POLICY PAPERS

Borrowing a Boat Out to Sea:
The Chinese Military’s Use of Social Media for Influence Operations

Nathan Beauchamp-Mustafaga
Michael S. Chase
BORROWING A BOAT OUT TO SEA:
THE CHINESE MILITARY’S USE OF
SOCIAL MEDIA FOR INFLUENCE OPERATIONS

NATHAN BEAUCHAMP-MUSTAFAGA AND MICHAEL S. CHASE
For 75 years, students have come to the Johns Hopkins University School of Advanced International Studies (SAIS) to build their professional networks, learn from renowned faculty, train with policy practitioners, and gain hands-on work experience.

The school was founded in 1943 by Paul H. Nitze and Christian A. Herter who sought new methods of preparing men and women to cope with the international responsibilities that would be thrust upon the United States following the end of World War II. Scholars and professionals were assembled to teach an academic curriculum emphasizing international relations theory, international economics, regional studies, and foreign languages. That education, combined with skills training and experiential learning, would prepare students for impact-oriented work in policy and other sectors. In 1955, a campus in Bologna, Italy was established, and in 1986 the school initiated a unique joint degree program with Nanjing University in the People’s Republic of China.

Today, guided by the vision of its founders, the school’s cadre of expert faculty prepares students for exciting careers across sectors and around the world. The school is complemented by research and outreach organizations such as the Foreign Policy Institute (FPI), which unites scholarship and policy in the search for realistic answers to international issues facing the United States and the world. Established in 1954 as the Washington Institute for Policy and renamed the Foreign Policy Institute in 1980, FPI has served as Johns Hopkins SAIS’s link to the policy world for over six decades as the school has developed innovative thinkers and problem solvers to address today’s most pressing challenges.
## Table of Contents

Preface ........................................................................................................................................ v

Executive Summary .................................................................................................................... vii

**Section 1**
Introduction and Overview ....................................................................................................... 1

**Section 2**
Influence Operations on Social Media from the Chinese Military Context ....................... 7

**Section 3**
Leadership Guidance and Military C2 for Social Media ....................................................... 25

**Section 4**
Chinese Lessons Learned from Other Countries ................................................................. 33

**Section 5**
PLA Messaging, Engagement, and Targeting Strategies for Social Media ...................... 43

**Section 6**
PLA Interest in a Twitter Account .......................................................................................... 67

**Section 7**
How the PLAAF Uses Social Media for Deterrence ............................................................. 73

**Section 8**
Taiwan is the Canary in the Coal Mine for Chinese Political Interference ...................... 81

**Section 9**
Indications of PLA Interest in U.S. Elections ....................................................................... 89

**Section 10**
AI and Big Data Loom on the Horizon .................................................................................. 101

**Section 11**
Conclusion and Recommendations ......................................................................................... 107
Nathan Beauchamp-Mustafaga is a Policy Analyst at the RAND Corporation, where he focuses on Asian security issues.

Michael S. Chase is a Senior Political Scientist at RAND. He is also a fellow at the Foreign Policy Institute and an adjunct professor in the China Studies program at Johns Hopkins SAIS. He was previously an associate professor at the U.S. Naval War College.

The opinions expressed in this report are the authors’ and do not necessarily reflect the views of the non-profit, nonpartisan RAND Corporation, its research clients and sponsors, the Foreign Policy Institute, or Johns Hopkins University.
Shortly before this report went to print, Twitter, Facebook, and YouTube all publicly announced they had suspended accounts on their platforms that they believe were operated by the Chinese government. On August 19, Twitter said it had identified a “significant state-backed information operation...originating from within the People’s Republic of China (PRC)” with “large clusters of accounts behaving in a coordinated manner” that 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.”¹ The scale of this effort on Twitter alone included 936 active accounts and 200,000 “spammy” accounts, plus another 4,302 accounts Twitter identified and suspended in September 2019.² Most importantly, this represents the first public attribution of specific hostile political interference on foreign social media to the Chinese government.

Our analysis so far suggests these accounts were not run by the Chinese military but instead likely run by the Propaganda Department and/or United Front Work Department (UFWD). Early research into the data released by Twitter reveals it was a “relatively small and hastily assembled operation” using second-hand accounts that were likely bought from marketing firms overseas.³ The lack of any relevant activity targeting Taiwan’s 2018 elections suggests the revealed operation is a separate line of effort from the broader Chinese social media disinformation campaign against Taiwan, which the Taiwanese government and media have mainly attributed to the Chinese military. Moreover, the apparent hasty nature of this effort targeting Hong Kong suggests it may have been a minor operation to “check the box” for domestic bureaucratic purposes on guiding foreign public opinion on an important political crisis for the Chinese leadership. More research is needed to better understand this initial data trove of activity, and hopefully more information will be released in the future. Regardless, this highlights the fact that the PLA is only one actor within China’s broader influence operations, a growing cause for concern for countries around the world.

Executive Summary

The Chinese military, known as the People’s Liberation Army (PLA), is positioning itself as one of the leading actors for hostile Chinese influence operations on social media. It is already reported to be surreptitiously using Facebook and other platforms to undermine the democratic process in foreign countries, including Taiwan, and recent developments indicate the United States could be next. The PLA uses social media not just for overt influence operations, such as external propaganda via PLA Daily and Xinhua to achieve narrative dominance as well as psychological warfare for deterrence purposes, but also conducts covert hostile political interference operations targeting foreign countries.

The Chinese Communist Party’s (CCP) PLA-led efforts to interfere with Taiwan’s November 2018 elections through spreading disinformation on social media already reveal one Chinese tactic. Military technical writings on “cognitive domain operations” [renzhiyu zuozhan, 认知域作战] explain that the PLA is developing technologies for subliminal messaging, deep fakes, overt propaganda, and public sentiment analysis on Facebook, Twitter, LINE, and other platforms. Other articles also suggest that the PLA could blackmail or tarnish the reputation of politicians as well as coopt individual influential civilian social media users to extend the reach of Chinese propaganda while obfuscating its Party origins. Since the Chinese military does not see a clear distinction between peacetime and wartime, it is possible that it will employ these active interference efforts whenever China feels its interests are sufficiently threatened.

As the PLA seeks to expand the reach of its influence operations around the world and continues its overt propaganda campaign to influence the global conversation about China and future PLA operations abroad, there is substantial evidence the PLA is considering opening official social media accounts on Western platforms, most likely Twitter. PLA researchers refer to exploiting existing channels to reach previously untapped audiences, such as using Western social media platforms, as “borrowing a boat out to sea” [jiechuan chuhai, 借船出海], which is a long-standing Chinese government strategy to exploit foreign media to deliver Chinese propaganda. Although the PLA does not yet have an official presence on

Western social media, it already has a public presence throughout the West and much of the world through foreign citizens’ use of Chinese platforms such as Sina Corporation’s Weibo and Tencent Corporation’s WeChat. Moreover, the PLA has a de facto presence on Western platforms through Chinese state-run media accounts on Facebook, Twitter, YouTube, Instagram, and others that relay its messages to unwitting audiences and help the military collect data on its effectiveness. Taiwanese reports further assert that the PLA already has covertly opened fake accounts on Western social media for its disinformation operations.

Official PLA accounts on Western social media platforms would afford the military direct access to its intended foreign audiences. This then would allow for better messaging and data analytics to actively facilitate ongoing influence operations and help it prepare for hostile interference operations against more countries. Opening an official PLA account on Western social media may appear to fall under an acceptable category of influence operations because it would be transparent public diplomacy. However, this report argues that consideration should be given to the national security risks involved in the PLA’s holding accounts on Western social media platforms, which could allow the PLA to gather more analytic data on individual users to enhance future political interference operations, for example with improved targeting of tailored messages.

As the awareness and debate over Chinese influence operations targeting Western democracies grow, it is critical for the U.S. government and the wider policy community to understand how the Chinese military views social media as a tool for influence and broader information operations at home and abroad. Most attention on Chinese influence operations has focused on the United Front Work Department (UFWD), but this report argues that the PLA should be recognized as another key driver of these Chinese efforts. Although there is no evidence that the PLA or other parts of the Chinese government are currently following Russia’s model for interfering

in the U.S. democratic process, it is important to watch for signs of such operations in the future.\textsuperscript{6} Indeed, former Director of National Intelligence (DNI) Daniel Coats warned the U.S. Congress in January 2019 about “hostile states and actors’ intensifying online efforts to influence and interfere with elections here and abroad,” including in the upcoming 2020 U.S. elections. He also specifically noted that China “is improving its cyber-attack capabilities and altering information online, shaping Chinese views and potentially the views of U.S. citizens.” Recent events in Taiwan as well as writings and patents filed by Chinese military researchers suggest that the PLA is increasingly interested in leveraging social media for such political interference in foreign countries, including in the United States.


The People’s Liberation Army (PLA) views social media through the prism of information dominance and influence operations, using tailored messaging to shape the perceptions and decisions of its target audience. Social media is a “double-edged sword” for the military, bringing both immense benefits and vulnerabilities for its influence operations.

The PLA initially was very concerned by the advent of social media as a vector for social disruption and political interference by other countries, especially the United States. Eventually, the PLA realized that the scariest thing about the Internet—that it gave a voice to those who could previously only receive CCP propaganda—could actually be turned into an asset. Social media users’ interactions with Chinese propaganda on social media—in the form of replies, reposts, and favorites—allowed it to refine and improve its message in real time, bringing it one step closer to realizing a twenty-first century authoritarian’s dream of information control.

According to an October 2018 report by the Hoover Institution, “while Americans are well acquainted with China’s quest for influence through the projection of diplomatic, economic, and military power, we are less aware of the myriad ways Beijing has more recently been seeking cultural and informational influence, some of which could undermine our democratic processes.” Chinese influence operations span a range of activities, including lobbying and cultivating politicians, injecting Chinese narratives into the foreign education systems, paid propaganda inserts in newspapers, selective funding of pro-China research, conditioning academic and think tank researchers’ access in China, dominating Chinese language media abroad, and challenging free-
Freedom of speech of those in the United States, including Chinese citizens and U.S. citizens of Chinese descent. Some of these activities, such as public diplomacy, are considered legitimate and normal by many countries, while others are considered illegitimate and unacceptable, such as those that are “covert, coercive or corrupting,” in the words of former Australian Prime Minister Malcolm Turnbull. China is motivated to invest in influence operations in part because, as this report relates, there is a "growing body of evidence that the Chinese Communist Party views the American ideals of freedom of speech, press, assembly, religion, and association as direct challenges to its defense of its own form of one-party rule." The Hoover report emphasizes that U.S. responses should be based on transparency, integrity, and reciprocity. We concur and adopt these as core principles for our own recommendations at the end of this report.

To understand the role of the PLA in China’s influence operations, it is necessary to understand that it is the armed wing of the CCP. As such, the PLA’s primary purpose is to ensure the Party’s continued rule, so the CCP’s influence operations are targeted at both domestic and foreign audiences.10 Domestically, the PLA focuses its influence operations on protecting and improving its image to maintain public support for the military and Party. Internationally, the PLA’s more traditional tactics for favorably shaping public perceptions and policies are better documented than are its nontraditional ones. For example, the China Association for International Friendly Contact (CAIFC), known to be under the Political Work Department (PWD), reportedly has facilitated access to the U.S. Congress.11

The PLA also engages in academic exchanges, such as sending researchers to other countries and hosting conferences for foreign scholars, including through the China Foundation for International Strategic Studies (CFISSL) and the Chinese Institute for International Strategic Studies (CIISS). This report will focus on nontraditional influence operations, not only how the PLA uses social media to shape public perceptions in its favor, but also how it uses social media for deterrence purposes and hostile political interference operations.

Social media has firmly established itself as a powerful tool for empowerment and disruption around the world. The Chinese government has cautiously tolerated the explosion of social media use within its borders as an almost inevitable evolution of Chinese society. Yet, the government obviously remains wary about social media’s impact and has invested enormous resources in censoring, controlling, and injecting its own viewpoints into the public conversation. Chinese government organizations have had to adapt to this newfound public square, and they have also sought to exploit its benefits while minimizing their exposed vulnerabilities. As Chinese citizens take to social media to criticize the government, identify corrupt officials, and rally public pressure for improved policies, the Chinese government has paid propagandists to guide public opinion by steering users away from these topics and distracting them from unflattering breaking news.12 Even as China has banned Western social media plat-

11 Diamond and Schell, “Chinese Influence & American Interests: Promoting Constructive Vigilance.”

forms, such as Facebook and Twitter, from operating in China, the Chinese government has opened up accounts on those same platforms to spread its propaganda to foreign audiences and purchased fraudulent followers to boost its reach. The Chinese military, as perhaps the organization most skeptical and fearful of social media, has slowly embraced social media platforms as the next stepping stone for improving its influence operations in foreign countries as well as at home.

The rise of the Internet fundamentally has changed the PLA’s approach to information control at home within Chinese society, for better or for worse. For the first time, the PLA can speak directly to its audience with a uniquely tailored message to each individual user; but this also means that anyone can respond to or even cut the military out of the conversation altogether. Domestically, the two-way communication enabled by the Internet and turbocharged by social media has changed the traditional power dynamic between the people as consumer and the Party as producer, requiring even more resources and focus in order to maintain control of the PLA's narrative. Social media has accelerated the pace of agenda setting and public opinion formation, causing the PLA to shift from a strategy of defensive reaction to one of proactive engagement.

A major component of safeguarding the Party domestically is controlling the narrative about the military and the Party, which traditionally has rested upon the PLA’s directing the release and dissemination of information about the military, first through print media in the PLA Daily and then through television with CCTV. However, this ability now is substantially challenged by the Internet and the newest platform of mass communication, social media. First came bulletin boards (BBS) and cell phones, which enabled individual citizens as users to respond to and even initiate discussions about the military in the online public square in real time. More recently, social media and smartphones have taken this a step further, broadly reaching all corners of society and garnering an increasing share of the public’s attention. In China, social media is now dominated by Weibo, similar to Twitter, and WeChat, which provides private messaging, group chats, and also public accounts and has surpassed Weibo in popularity.

According to the PLA, China is already in constant battle over the narrative of China’s rise and the PLA’s intentions with other nations, both inside and outside of China, and, most prominently, against the United States. The


16 This report will focus on the PLA’s use of Weibo because it is more publicly accessible than WeChat, even though WeChat is much more popular than Weibo in many areas. See Lily Kuo, “Sina Weibo Just Lost 28 Million Users to Censorship and WeChat,” Quartz, January 17, 2014, https://qz.com/168119/sina-weibo-just-lost-28-million-users-to-censorship-and-wechat/; and Wang Tianyi, “Military Social Media Accounts Draw Both Praise and Concern” [“军营公众号的喜与忧”], PLA Daily [解放军报], February 20, 2017, 5, http://www.81.cn/jfjbmap/content/2017-02/20/content_169866.htm.
PLA believes that the United States utilizes its inherent and substantial advantages on the Internet—such as its ownership of Internet architecture and infrastructure, U.S. companies’ dominance of Internet websites and services, U.S. media’s readership around the world, and even English’s status as the global lingua franca—to shape and control the global narrative. This puts China on the defensive in this “public opinion warfare” against the United States and its allies, who are presumed to be on an unrelenting offensive to smear, discredit, and contain China from its rightful position of glory.

From China’s perspective, influence operations are undertaken by all countries, and it is other countries, especially the United States, that use social media to interfere in the political processes of countries like Iran and in the Middle East. Whatever actions the PLA takes to counter this perceived subversion are considered “defensive” and necessary to protect and defend the military and the Party. Whether targeted against Chinese citizens or foreign citizens in other countries, there are no boundaries to China’s desire to shape public opinion. PLA authors agree that “online public opinion warfare” [wangluo yulunzhan, 网络舆论战], in their parlance, is already a constantly confrontational domain, although certain circumstances such as actual war perhaps warrant even more aggressive tactics.

Yet, even the most aggressive tactics discussed by PLA authors are not labeled as “offensive” actions. This reflects PLA doctrine and rhetoric that nothing it does can be construed as an unprovoked attack on others.

A Note on Sources

This report is based on extensive Chinese language source research, especially Chinese military writings including PLA Daily, the PLA’s official newspaper, and Military Correspondent, the PLA’s premier academic journal on propaganda. Articles in Military Correspondent are written by a range of PLA researchers and propagandists (journalists), so these articles are not individually authoritative as stand-alone declarations of policy, but rather should be considered a useful window into ongoing debates and discussions within the military on various topics. The language of social media is constantly evolving, and so too is the PLA’s terminology for such analysis. The lack of consistent terminology means we were only able to capture a slice of the discussion about social media both in the analysis and the data presented.


19 For our purposes here, social media is translated as 社交媒体, but it has also been referred to as “social websites” [社交网站], among other translations, and is also sometimes encapsulated under “new media” (新兴媒体 or 新媒体), “network media” (网络媒体), “personal media” (自媒体), or “omni media” (全媒体). For example, Facebook is generally translated as “face book” (脸书) within China, and this was the most frequent translation for PLA authors, but the 2015 Science of Military Strategy oddly refers to it as “facial makeup or mask” (脸谱), a less widely used translation. Our dataset does not include the latter 脸谱, mentioned in 58 Military Correspondent articles since 2010, because it is a word used in everyday conversation and would otherwise distort our data.


This report includes Chinese materials published through August 1, 2019, though the data provided in the charts below is current through December 2017, the latest issue of *Military Correspondent* available on the China National Knowledge Infrastructure (CNKI) database. The sources reflect the number of articles published per year, usually in *Military Correspondent* unless otherwise noted. They should be considered a bare minimum of articles referencing these topics, which means PLA interest is likely much higher. Also, it is important to note that from China’s point of view, the Western concept of “strategic communications” is the same as the Chinese concept of “propaganda,” since both seek to release information with the goal of influencing public discussion. PLA experts argue that labeling Chinese messaging as “propaganda” unfairly maligns its intent since the term carries a negative connotation in the West. This report will use “propaganda” because that is the term used in PLA writings, and, similarly, will use “influence operations” to encapsulate Chinese military thinking on a range of related concepts such as the “three warfares” [sanzhan, 三战] (defined as psychological warfare [xinli zhan, 心理战], public opinion warfare [yulun zhan, 舆论战], and legal warfare [falü zhan, 法律战]); political warfare; external propaganda; online public opinion warfare; and cognitive domain operations.

### Organization of the Report

This report covers the Chinese military’s approach to social media for influence operations against both domestic and foreign audiences. Section 2 explains how influence operations and social media fit into the PLA’s military strategy, addresses PLA objectives using social media, and describes some motivating concepts. Section 3 covers leadership guidance to the PLA on social media and assessment of the command and control (C2) structure for the PLA’s use of social media. Section 4 explores what the PLA has learned from other countries around the world about influence operations and military uses of social media. Section 5 presents data and analysis on the PLA’s strategies for messaging, engagement, and targeting on different social media platforms. Sections 6 and 7 explore these communication strategies by presenting case studies on the PLA’s interest in joining Twitter and how the PLA Air Force (PLAAF) uses Weibo for deterrence. Section 8 covers how the PLA used social media for disinformation against Taiwan, especially in the November 2018 elections, and Section 9 applies these lessons to the PLA’s apparent interest in interfering with U.S. elections. Section 10 covers future trends to watch, including artificial intelligence (AI), big data, and deep fakes. The report concludes in Section 11 with some recommendations for U.S. policymakers.

---


Section 2
Influence Operations on Social Media from the Chinese Military Context

China has long thought about how to use information to shape the perceptions and decisions of other countries’ leaders and populations. It is unsurprising, therefore, that the PLA’s overarching approach to warfare increasingly focuses on the information domain including information and influence operations, which the PLA views as integral components of its approach to victory in modern, high-tech wars. Although the PLA does not have a specific term for influence operations, the closest concept would be the “three warfares,” a combination of psychological warfare, public opinion warfare, and legal warfare, and the related concept of “cognitive domain operations.” This section will outline how influence operations fit into the PLA’s approach to information operations and the role envisioned for social media.22

Role of Influence Operations in China’s Military Strategy

PLA influence operations are intimately connected to the broader concept of information operations. Information operations, in turn, are critical to the PLA’s ability to seize information dominance on the battlefield and considered necessary to winning modern wars. Authoritative Chinese publications highlight this: the 2015 Defense White Paper asserts that the “world revolution in military affairs (RMA) is proceeding to a new stage…. Outer space and cyber space have become new commanding heights in strategic competition among all parties. The form of war is accelerating its evolution to informationization.”23 This trend led the PLA to revise its military strategy to be “winning informationized local wars,” the latest iteration since the PLA embraced the critical role of information in the early 2000s in response to the United States’ military successes in Iraq, Kosovo, and Afghanistan.24 The 2013 *Science of Military Strategy* similarly emphasizes that “information dominance is the foundation for seizing battlefield initiative,” along with sea and air superiority and that controlling these domains “requires achieving a balance of offense and defense.”25 From the PLA’s perspective, seizing information superiority requires a holistic approach to information operations that in-

---

22 The authors would like to thank Kristen Gunness for her feedback on this section.

cludes use of cyber, space, and psychological warfare or influence operations.

Although these capabilities are targeted at wartime operations, in practice, they also require application in peacetime. The 2015 Defense White Paper explains that “a holistic approach will be taken to balance war preparation and war prevention,…deterrence and warfighting, and operations in wartime and employment of military forces in peacetime.”

The PLA has worked to better integrate its influence operations, or psychological warfare capabilities, into its broader military strategy, most notably through the creation of the Strategic Support Force (SSF) in 2015. According to analysts Joe McReynolds and John Costello, “the SSF combines assorted space, cyber, electronic, and psychological warfare capabilities” that were previously in siloed isolation across the PLA in order to “build new synergies between disparate capabilities that enable specific types of strategic information operations (IO) missions expected to be decisive in future wars.” Specifically, they note that the “SSF also appears to have incorporated elements of the PLA’s psychological and political warfare missions [such as Base 311], a result of a subtle yet consequential PLA-wide reorganization of China’s political warfare forces. This may portend a more operational role for psychological operations in the future.”

This enhanced integration would allow the PLA to better exploit the nexus between cyber and psychological warfare operations, which is the perfect combination necessary to create more effective influence operations on the Internet, including on social media. Indeed, there is already evidence that the SSF has been employed for just this purpose in Taiwan, and indications suggest it is tasked with targeting other countries.

PLA Strategy and Concepts for Influence Operations

PLA influence operations are best understood as part of the “three warfares” concept. McReynolds and Costello explain the three warfares as “a unique Chinese political warfare model that calls for the coordinated use of psychological warfare, public opinion warfare, and legal warfare to establish ‘discursive power’ [huayu quan, 话语权] over an adversary—that is, the power to control perceptions and shape narratives that advance Chinese interests and undermine those of an oppo-

---

26 Information Office of the State Council, *China’s Military Strategy*.
30 McReynolds and Costello, China’s Strategic Support Force: A Force for a New Era, 5.
32 Mattis, “China’s ‘Three Warfares’ in Perspective.”
nent.” 33 The 2011 Military Dictionary defines public opinion warfare as “creating a favorable public opinion environment for political initiative and military victory” through the “comprehensive use of various media means and information resources to fight the enemy,” while psychological warfare is “using specific information and media [for] combat actions that affect the psychology and behavior of the target audience.” 34

The PLA Daily in 2004 articulated public opinion warfare as the “integrated use of newspaper, radio, television, the Internet, and other news media” in a “planned and targeted manner” to encourage “the combat morale of its own side” and cause “the combat will of the enemy [to] collapse” as well as “guide international public opinion.” In explaining the nuanced difference between public opinion warfare and psychological warfare, it notes that public opinion warfare occurs all the time and “during peacetime pays more attention to long-term infiltration into the objects of the society’s and culture’s deep structure, changing the awareness and conviction of the enemy masses,” whereas “psychological warfare is more focused and concentrated in wartime” and can be more tailored and targeted. 35 The 2013 Science of Military Strategy places great faith in the three warfares’ ability to ensure that the “influence of our possible and just underway military activities is fully enlarged, weakened, or shifted, causing them to have a powerful psychological deterrent force against the enemy officers and men, and achieving the effect of yielding twice the result with half the effort.” 36 Thus, from the above, influence operations clearly play a large role in China’s military strategy.

Operationally, the PLA envisions warfare as a confrontation between systems, and influence operations are part of a “psychological attack” under the “information-confrontation system.” 37 This attack has four components—undermining enemy morale, confusing enemy decision-makers, convincing countries not to fight, and using disinformation to degrade enemy decision-making. First, psychological propaganda inducement “pressures and influences the ‘feelings and behaviors’ of both enemy and friendly populations to either weaken morale or enhance popular support, respectively…[by distributing] detrimental information to the enemy.” Second, psychological deterrence “confuses enemy decisionmaking as a way to undermine its military power.” Third, psychological influence “encourages a potential adversary to be cautious about


37 For more on the PLA’s systems confrontation approach to warfare, see Jeffrey Engstrom, Systems Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare (Santa Monica: RAND, 2018).
joining a war or, ideally, to be opposed to fighting in a particular war” by using tailored narratives that would most resonate with the target audience and finding common ground.

Fourth, psychological deception “adversely impacts its decision-making” by using “false information.”

A 2013 Academy of Military Science (AMS) book provides more details on the offensive employment of psychological warfare, including disinformation. It calls for making “full use of modern media, electronic information operations platforms and special operations methods” to support “the overall operational effectiveness of psychological warfare.” These methods include “information deprivation, 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.” Special operations in this context specifically include “point and click’ attack, ‘decapitation’ operations, ‘silver bullet’ and driving a wedge.” The book presents psychological warfare as an ever-present aspect of warfare, even in peacetime: “Psychological warfare exceeds the boundaries between peacetime and wartime, exceeding the boundaries between the front and the rear, exceeding the boundaries between open and secret channels.”

There is a role for social media to play in each of these components. Under psychological warfare, a related concept for the PLA’s influence operations is “cognitive domain operations” [renzhi yu zuozhan, 认知域作战]. Cognitive domain operations are framed as the next evolution in warfare, moving from the natural and material domains—land, maritime, air, even electromagnetic—into the ephemeral, namely the human mind. The goal of cognitive domain operations is “mind superiority” [zhi nao quan, 制脑权], namely using psychological warfare to shape or even control the enemy’s cognitive thinking and decision-making. Similar to cognitive domain operations representing the next frontier of warfare domains, mind superiority is the next step beyond the traditional PLA concept of the three superiorities—sea superiority, air superiority, and information dominance, all of which are nec-


necessary to seize in a conflict to enable victory.\textsuperscript{42} Cognitive domain operations is the real-world operational concept to carry out psychological operations across a range of domains, including social media, under the larger framework of the “three warfares.”

The PLA conception of cognitive space and mind superiority paints an expansive view of the battlefield domain that, in theory, applies to civilians in what the West would consider peacetime. This expansive view mirrors the similarly broad threat perception invoked in China’s 2015 National Security Law: “National security refers to the relative absence of international or domestic threats to the state’s power to govern, sovereignty, unity and territorial integrity,” among other issues.\textsuperscript{43} According to a 2017 \textit{PLA Daily} article, this “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,” and collectively includes many “intangible factors” such as “leadership, morale, cohesion; training level and experience; situational awareness and public opinion.” Drawing from the United States’ subversive psychological operations intended to collapse 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 of the target countries.” More broadly, “the goal of psychological warfare is to manipulate the perception of a particular group of people and to serve a larger operational goal. Perceptual manipulation is designed to influence the perception of others, affecting their emotions, reasoning, determination, and ultimately their behavior. It can target individuals, groups, countries, and even people around the world.”\textsuperscript{44} This aligns well with the general role of psychological warfare within PLA strategy as described above, especially the \textit{Science of Military Strategy’s} reference to the “information–belief–thought” process as a target for the three warfares.\textsuperscript{45} Observing real-world application in Taiwan, Rachael Burton argues “the PRC’s disinformation campaigns against Taiwan is a form of cognitive warfare that targets the people’s decision-making process, but also that of Taiwan’s elected leaders, and represent a national security threat for its ability to sow discontent, mistrust, and fear.”\textsuperscript{46}

The Role of Social Media in PLA Influence Operations

The PLA understands that social media, as the latest version of the Internet’s public square, can play a key role in psychological warfare and contribute to information superiority. McReynolds and Costello argue the SSF’s creation reflects the fact that the “Chinese Communist Party and PLA thinkers have long understood cyber operations to be a primary vehicle for psychological manipulation, a point not fully grasped by the U.S. Government, particularly the defense establishment, until the recent discovery and analysis of Russian interference in the U.S. Presidential

\begin{flushright}
43 Quoted in Mattis, “China’s ‘Three Warfares’ in Perspective.”
44 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”], \textit{PLA Daily} [解放军报], October 17, 2017, http://www.81.cn/jfjbmap/content/2017-10/17/content_189879.htm.
\end{flushright}
election in 2016.”47 The 2013 Science of Military Strategy asserts that “the rapid development of new media as represented by the Internet has made the right of speech become yet another form of expression of seizing and holding the initiative.”48 This is because “the Internet covers almost every corner of the entire world, and has become the fundamental means by which people regularly understand the world and connect with one another.”49

Authoritative Chinese discussions of social media are rare, but generally frame the platforms as a force for destabilization and political interference. The PLA Encyclopedia and PLA Military Dictionary do not mention social media nor do any of China’s military white papers. The first direct mention of social media appears to be the National Defense University’s (NDU) 2015 version of Science of Military Strategy. It states,

Since the beginning of the 21st century, cyberspace has been used by some countries to launch ‘color revolutions’ against other countries. The political turmoil that has erupted in the Middle East and North Africa in recent years is often dominated by behind-the-scenes operations using social networking sites such as Twitter and Facebook as the engine, from manufacturing online public opinion to inciting social unrest. As a result, national governments lacking the strategic means for cyberspace military struggle have continued to collapse.50

PLA awareness of the power of social media can be dated to 2009, especially the role of Western platforms in facilitating protests in Iran. A 2009 China Defense News article on that year’s Iranian election highlighted Chinese concerns of this new threat vector: “[Through] Twitter, Facebook, YouTube and other websites, the United States, Britain and the Israeli intelligence agency spread sensational news to ‘poison’ the Iranian people...the CIA also directed Iranian anti-government activists...to create greater turmoil and cause internal strife among the Iranian people.”51 For social media, “the crisis in Iran proved that Twitter had become a powerful political instrument.”52 Looking back to other events in 2009, then-Secretary of Defense Robert Gate’s comment that social media was a “strategic asset” of the United States and the creation of U.S. Cyber Command reinforced the PLA’s belief that the U.S. government was already using social media for malicious purposes.53 This concern about social media among some in the PLA was brought to the troops in September 2015, when the PLA Daily carried a full-page spread on “social media warfare,” highlighting various ways for adversaries to exploit it.54 This likely reflects the CCP’s concerns over domestic stability, but also provides insights into

47 McReynolds and Costello, China’s Strategic Support Force: A Force for a New Era, 48.


51 Chi, “Cyber Subversion: Security Threats That Must Not Be Taken Lightly.”

52 Chi, “Cyber Subversion: Security Threats That Must Not Be Taken Lightly.”

53 Li Weiqian [李玮倩], “New Media and Military External Propaganda” [新媒体与军事对外宣传], Journal of News Research [新闻研究], no. 9 (2017): 117. The author is affiliated with the National University of Defense Technology’s School of Humanities and Social Sciences.

54 Chen Hanghui [陈航辉], Fang Peng [方鹏], Yang Lei [杨磊], and Xia Yuren [夏育仁], “Social Media Warfare: A New Dimension to Warfare in the Information Age” [社交新媒体战：信息时代战争新维度], PLA Daily [解放军报], September 25, 2015, http://www.81.cn/jfjbmap/content/2015-09/25/content_124476.htm.
how the PLA conceptualizes the powerful impact of these platforms as conduits of foreign influence against other countries. Thus, it was only a matter of time before the PLA learned how to turn this vulnerability into a weapon against other countries.

Although PLA attention to social media as an offensive weapon has only intensified in the last couple years, some PLA researchers understood its power early on. A May 2011 article on social media emphasized its “potential for psychological warfare applications,” including expanding the available vectors, combat effectiveness, and innovation for psychological warfare.\(^55\) It argued that Facebook and Twitter can be used to gather information on intended psychological targets from user data, and opinion leaders can expand the reach of messaging through retweets and shares to a broader audience without distorting the original message. The article touts the value of subliminal messaging as being more powerful than overt propaganda and continues:

> In social media such as ‘Facebook’ and ‘Twitter,’ whether it is a president of a country, a celebrity, a CEO, workers and peasants, or teachers and students, they are [all] just ordinary users, and they all have the right to speak and communicate in an equal manner. Their own views, opinions and attitudes are derived from life, objective reality, and can imperceptibly stimulate the audience’s audio-visual feelings, and silently cause a psychological reaction for the audience. Using social media as a platform, psychological warfare information can be subtly disguised, and psychological warfare can become a ‘sugar-coated pill,’ which affects the target’s psychology without knowing it, and can maximize the impact and achieve the goals of psychological warfare.\(^56\)

Based on Taiwan’s experience and Chinese writings, disinformation is a key part of the PLA’s approach to influence operations on social media.\(^57\) Although the Science of Military Strategy does not directly discuss disinformation operations, its emphasis on psychological warfare combined with the discussion of cyber-attacks provides insight into what value a cyber-psychological attack could have for the PLA: “One successful [round of] network warfare can cause the collapse of the adversary’s economy, and paralysis of his operational systems. Within future war, the side holding the superior position in computer network operations will seize the initiative in war and generate powerful psychological awe in the enemy.”\(^58\) This source also noted that “computer network operations thus have the prominent characteristics of low cost, high benefit, and low risk.”\(^59\)

Although social media rarely is discussed directly in authoritative sources, non-authoritative articles by Chinese military researchers

---


\(^{56}\) Wu and Mei, “Some Inspirations Drawn from the Application of Booming Social Media in Psychological Warfare.”


can provide insights into how the PLA could conceive of a disinformation campaign. One 2006 article argued this could include “false information fabricated through careful consideration to launch attacks on the minds of the enemy leaders, misleading them to make wrong assessments or causing their psychological collapse,” since “mixing up true and false information can achieve a result of making it hard for people to distinguish.” 60 Other articles argued for the PLA to “incessantly disseminate false and focused information to the enemy” in order to “interfere with and disrupt the enemy side’s perception, thinking, willpower, and judgement.” 61 A 2007 article on the role of blogs noted that online media “could achieve twice the results for half the effort in conducting information deception and confusion.” 62 Such disinformation can be accomplished through explicit and direct statements or through subconscious messaging. 63 We believe the PLA is more likely to use semi-official or covert accounts with plausible deniability, like it reportedly did in Taiwan, instead of its official social media accounts, to conduct a disinformation campaign on social media. It is easy to imagine how the PLA would explain to the Chinese leadership that a deniable social media disinformation campaign is something akin to a low-cost high-reward cyber-attack, especially since so far it has faced no consequences for its employment against Taiwan.

PLA Objectives with Social Media

As a consequence of the PLA’s views of social media’s role in its larger military strategy and its status as the armed wing of the CCP, the PLA has three broad objectives for use of social media. First, it seeks to achieve narrative dominance through the use of official social media accounts to overtly spread Chinese propaganda and, thereby, shape public perceptions and policies toward China and its military. Second, the PLA seeks to use official social media accounts for deterrence purposes to communicate deterrence signals, which specifically demonstrate China’s capabilities and credibility while also undermining an enemy’s resolve through psychological warfare. Third, the PLA seeks to leverage social media for political interference in order to degrade the credibility of a foreign political system, undermine support for a foreign government and its policies, as well as support China’s preferred political candidates in an election. These objectives are neither mutually exclusive nor exhaustive, but provide a framework for PLA influence operations on social media.

Narrative Dominance

One of the PLA’s objectives is to control the narrative about China and its military on social media, especially for domestic audiences but also for foreign audiences. 64 The 2013 Sci-
THE CHINESE MILITARY’S USE OF SOCIAL MEDIA FOR INFLUENCE OPERATIONS

Table 1. PLA’s Objectives for Social Media

<table>
<thead>
<tr>
<th></th>
<th>Domestic</th>
<th>Foreign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrative Dominance</td>
<td>• Protect PLA image</td>
<td>• Improve and defend PLA image</td>
</tr>
<tr>
<td></td>
<td>• Maintain support for PLA as Party Army</td>
<td>• Win support for PLA actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Correct “misperceptions” by addressing negative reporting</td>
</tr>
<tr>
<td>Deterrence</td>
<td>• Build public support for war as function of resolve</td>
<td>• Communicate capabilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Communicate credibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Undermine enemy resolve</td>
</tr>
<tr>
<td>Political Interference</td>
<td>N/A</td>
<td>• Undermine credibility of foreign political system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Undermine support for government and policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support preferred political candidates</td>
</tr>
</tbody>
</table>

ence of Military Strategy explains the objectives of the PLA’s engagement on the Internet: protecting China’s image, winning “sympathy and support” from the international community, and maintaining domestic support for the war. The PLA realized early on that social media would play a role in defining Chinese domestic public opinion of the military, as a 2010 article notes: “As we grasp the new trend of an increasingly diversified and targeted social media...we need to actively occupy the public cultural service platform, so as to promote and display a positive military image.” Several authors argued that most negative news about the PLA comes from social media, damaging the PLA’s image because it does not control the narrative. The other aspect is that the PLA is always sensitive about its status as the armed wing of the CCP and strenuously opposes the “hostile” idea that the military should be under the national government.

66 Liao Yiwen [廖毅文], “Promoting National Interests and Building a New PLA Image” [“国家利益拓展与中国军队新形象塑造”], Military Correspondent [军事记者], no. 7 (2010).
Internationally, as the PLA increases its military activities abroad, it wants to create a favorable environment for its operations. Similar to its domestic goals, it seeks to improve and defend its image abroad. However, because the CCP does not have a monopoly over foreign media coverage, the PLA also has to correct “misperceptions” by addressing negative reporting. The last related objective is to gain support for PLA actions and operations abroad, which will increasingly be important as the PLA increases its operations abroad beyond humanitarian assistance/disaster relief (HA/DR) into more power projection, such as foreign deployments. This is reflected in Chinese writings; for example, one National University of Defense Technology (NUDT) author characterized social media as an opportunity to fix the PLA’s negative image abroad.69 She believed that traditional media is ill-suited for today’s narrative needs, and Ministry of National Defense (MND) spokespeople and PLA Daily do not suffice, especially in a time of crisis, when a fast response is needed.

The PLA’s biggest tool for achieving narrative dominance is its domestic and foreign propaganda. This includes not only the PLA’s own propaganda outlets, such as PLA Daily and its main English-language website China Military Online, but also state-run media that extend the reach of PLA propaganda, such as Xinhua, China Daily, and Global Times. These are all critical tools for addressing China’s perceived influence gap with foreign countries, especially the United States. Reducing the United State’s “narrative dominance” is often framed as improving China’s “discursive power” (or “right to speak”) in both the domestic and international arena. Achieving this “discursive power” will support China’s ability to have its voice heard and thus exert its “soft power” or influence in global affairs.70 Social media is one key aspect of the broader media and public opinion landscape in which China wages this battle. Doing its part, the military desires to shape how people around the world discuss China and the PLA. This interest is evident in the charts below, which draw data from CNKI.

This propaganda aspect of the PLA’s influence operations generally falls under the legitimate public diplomacy category outlined in the Hoover Institution’s report because these actions generally are transparent. However, as will be detailed in Section 5, the PLA is also very interested in disguising its propaganda through non-transparent means, such as coopting influential users on social media to spread its message. Reflecting this, one PLA author argued for the need to control influencers on social media who are critical of the PLA, because, according to them, 3 percent of Weibo comments are supportive of the military while 15 percent are negative.71 The PLA’s strategies for social media engagement will be covered in Section 5 and its consideration of opening a propaganda account on Twitter are covered in Section 6.

69 Li Weiqian, “New Media and Military External Propaganda,” 117.
Deterrence

The PLA takes a more comprehensive and, perhaps, more offensive approach to deterrence than the Western conception it is based upon. For China, the key components, similar to the West, are capabilities, credibility, and signaling, with an emphasis placed on the psychological aspect of resolve, that is both maintaining the will to fight and undermining the enemy’s resolve. The 2001 *Science of Military Strategy* says that one aspect of deterrence is to “display clearly one’s deterrent force for bringing about psychological pressure on and fear to the opponent and thus force him to submit.”\(^7^2\) Similarly, the 2011 *PLA Encyclopedia* defines “deterrence strategy” as “the display of military power, or the threat of use of military power, in order to compel an opponent to submit.”\(^7^3\) The 2013 *Science of Military Strat-

---


\(^7^3\) Quoted in Dean Cheng, “Chinese Views of Deterrence: Celebration of 50th Anniversary of PLA Navy’s North Sea Fleet as It Pursues Capability to Operate from Indian Ocean to Western Pacific,” *Joint Force Quarterly*, no. 60 (2011).
nergy expanded on the psychological connection to deterrence: “the carrier for deterrence to produce an effect is the opponent’s psychological activities. Deterrence is a military notion, and also a psychological-political notion. The deterring side strives with various modes to let the deterred side imagine or speculate the horrible consequence that might be produced by this type of threat, so as to incite psychological fear in the deterred side.” It further hinted at the importance of undermining enemy resolve through psychological warfare, noting that “transmission channels...have a feature of diversification,” so to maximize results the PLA should treat “the masses of the people as the most basic medium for amplifying fear, [manufacture] various strike results to disrupt popular sentiments of the people, weaken the nation’s will to resist, and form a scope of influence that proliferates gradually and strengthens continuously.” Social media can be useful for all three, but an underappreciated application is the role social media can play in undermining enemy resolve through psychological warfare.

Most simply, the Internet and social media are channels to transmit information for deterrence, and the PLA Rocket Force (PLARF) appears to be leading the way. It has been asserted that “whether to say something, how to make relevant statements, by whom to make the statements must all be brought into line with and serve the needs of the state’s political and diplomatic struggle.” Furthermore, “a propaganda campaign related to missiles and nuclear weapons” should support “expressing our strategic intention, demonstrating our strategic postures, and strengthening our strategic deterrence.” In the end, “the combination of official and unofficial propaganda,” which includes social media, “may produce better effects in deterring opponents by manifesting our power, thus boosting influence and momentum for the development and employment of our strategic power.” For example, a photo of a PLA Air Force (PLAAF) bomber flying above disputed features in the South China Sea released on social media can demonstrate China’s capability to defend its claims militarily, and accompanying official statements reinforce China’s credibility to do so. This and the more nuanced role of social media for psychological operations will be explored further in Section 7.

**Political Interference**

The PLA has always been engaged in political warfare but only recently has the rest of the world realized how the Chinese military has modernized it—with hostile political interference through disinformation and other tactics on social media. According to Russell Hsiao, “political warfare employs strategic influence operations as a means of influencing policies in favor of Chinese core interests.” Specifically, “political warfare in the Chinese context seeks to undermine the legitimacy of Taiwan, challenge the liberal democratic order, shore up CCP authority domestically, challenge international rules of the road, and promote alternatives to widely accepted universal values.” Hsiao was writing in 2013 before the revelations about PLA disinformation on so-

---


76 Lü Hongjun [吕红军], “Boosting the Use of the Strategic Force through External Propaganda” [“以外宣传助推战略力量运用”], *Huojianbing Bao* [火箭兵报], March 7, 2017, 3.

77 Lu, “Boosting the Use of the Strategic Force through External Propaganda.”

cial media against Taiwan, but in practice, it is the same objective using a new medium, perhaps more effectively. This can be accomplished through a range of tactics, including using covert or unofficial accounts to spread disinformation and amplifying true but negative news released by others. China reportedly has coupled its political interference with cyber-attacks to gain damaging or sensitive information both in Cambodia and in Taiwan.79

There are two explanations for the PLA’s role in political interference operations. First, the PLA believes political interference is important for accomplishing its military objectives. This may be true in a long-term sense for Taiwan since the PLA’s top mission is unification, but this logic weakens when applied to other countries. Second, the CCP leadership can turn to the PLA for its technical expertise and manpower to conduct an aspect of the broader Chinese government strategy. We believe the latter explanation is more likely and is also the case for Taiwan.

PLA authors also are very interested in the role of social media for intelligence collection, including for strike targeting and classified information. One article noted that the U.S. military has worked with the intelligence community to identify and monitor social media accounts to garner intelligence. It recounted that the U.S. government was able to strike a physical ISIS site within twenty-two hours after a photo was posted online that revealed its location, implicitly recognizing the operational security dangers of using social media in wartime.80 A September 2015 PLA Daily article analyzed the dangers of “catfishing” on social media, namely using fake accounts to pretend to be someone else to befriend strangers, because social media account registration requires a lot of personal information.81 This article stated that U.S. Marines on deployment had fallen victim to such an experiment and released sensitive information via social media, and that such contacts can enable sending malicious emails. It mentioned that Weibo and WeChat offer similar vulnerabilities for Chinese troops, such as revealing classified equipment or base locations through photos, and concluded that further controls were required on troops’ use of social media. Other Chinese military media addressed the use of the Strava exercise-tracking application’s open data set to identify foreign military presence around the world.82 While these discussions were couched in defensive terms, understanding the inherent vulnerabilities of social media is a critical step in turning them into an offensive weapon.


81 Chen, Fang, Yang, and Xia, “Social Media Warfare: A New Dimension to Warfare in the Information Age.”

A Closer Look at Cognitive Domain Operations

Although the concepts of cognitive domain operations and mind superiority may seem far-fetched or to be propaganda gibberish, they are very real. The terms first appeared in PLA Daily in December 2013, the same year as General Secretary Xi Jinping’s screed against Western ideological subversion that indicated China was exhibiting a sense of fear and defensive reaction against a perceived onslaught by the West. Subsequently, PLA authors argued the struggle for “mind superiority” already was underway. In 2014, a book was published by a NUDT professor on the topic and in 2018 PLA writings began to appear on the hardware requirements for such operations. Our assessments that cognitive domain operations is indeed a new operational concept for the PLA is reinforced by 2018 Taiwanese media reporting that cognitive domain operations was the operational principle driving the PLA’s election interference.

The leading intellectual work on “mind superiority” is a January 2014 book by Professor Zeng Huafeng, Dean of the School of Humanities and Social Sciences at NUDT. In a June 2014 interview for the book’s release with PLA Daily, Zeng said the cognitive domain was the most recent evolution of warfare, past the natural domain—land, maritime, and air—and material domain—electromagnetic. The “cognitive space” is defined by Zeng as “the scope and field of human cognitive activities, which are intangible spaces that reflect human emotions, wills, beliefs, and values, and exist in the minds of the participants in the struggle.” “Mind superiority” is defined as:

...using spiritual/psychological information carried by the propaganda media, national language, cultural products, etc. as a weapon to infiltrate, influence and even lead the cognition, emotion and consciousness of the pub-


84 The cognitive domain was discussed as a domain of operations in earlier PLA texts, such as Ye Zheng, Lectures on the Science of Information Operations.


89 Huang, “Seizing Mind Superiority in Future Wars.”
lic and the nation’s elites. The ultimate [goal] is to manipulate a country’s values, national spirit/ethos, ideologies, cultural traditions, historical beliefs, etc., to prompt them to abandon their theoretical understanding, social system and development path, and achieve strategic goals without victory.90

Zeng envisions the cognitive domain as “unbounded, invisible, shadowless” and existing “wherever spiritual information can be transmitted.”91 These concepts embrace this boundless domain in an era of global media where “an individual is both a recipient of information and a publisher of information. In theory, any individual or group can instantly transmit specific information processed and produced in the world and influence specific target objects.” This is both a direct threat to China: “Today, Western hostile forces seek to inculcate and infiltrate Western values and ideas of ‘democracy’ and ‘freedom’ through normal academic information exchanges through political, economic, scientific, cultural and other academic exchanges,” but also an implicit opportunity. Thus, Zeng identifies four ways Western countries are winning the fight for “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. For Zeng, cognitive warfare is the highest form of winning without fighting.92

Mirroring China’s broader approach to influence operations, cognitive domain operations are usually framed as a wartime psychological warfare mission, but clearly also are applicable in peacetime. Other Chinese analysts have argued that on the battlefield, the goal is to “make the opponent unable to perceive or perceive spam and false information,” while maintaining one’s own perception of the battlefield, as well as “disturb and destroy the opponent’s cognition by interfering with brain-machine [integration] function and affecting people’s ideology, value judgment, psychological emotion, etc., and can also gain recognition by attacking, destroying auxiliary decision-making and autonomous weapon equipment information data processing hardware.”93 Zeng similarly has framed cognitive space as the domain for psychological warfare, which includes “three links, namely information generation, information transmission and information influence, while information influence is the least controlled part.”94 While historically psychological warfare has not been very effective, “the rapid development of brain science and technology has enabled human beings to make breakthroughs on the road of self-knowledge, which will inevitably bring new opportunities for future psychological warfare.”95 However, the PLA’s expansive view of wartime conditions suggests cognitive domain operations likely are employed whenever necessary, such as evidenced by their use in Taiwan’s elections.

90 Huang, “Seizing Mind Superiority in Future Wars.”
91 Huang, “Seizing Mind Superiority in Future Wars.”
92 Huang, “Seizing Mind Superiority in Future Wars.” Other authors have placed mind superiority alongside psychological warfare. See Pan Guang-

93 Shen and Zhang, “Intelligent Knowledge Operations.”
94 Huang, “Seizing Mind Superiority in Future Wars.”
95 Huang, “Seizing Mind Superiority in Future Wars.”
PLA researchers began publishing articles in 2018 about the hardware requirements for cognitive domain operations, reinforcing our belief that this is an operational concept. In October 2018, the PLA's leading psychological warfare force known as Base 311 (Unit 61716) under the SSF, which very likely was responsible for spreading disinformation during the Taiwan election, delineated the hardware necessary to support such operations in peacetime and wartime. The article explicitly references Facebook, Twitter, and LINE, describing social media as “a constantly open system that is highly inclusive and transcends the boundaries of national borders, cultural barriers and media.” The authors point out several shortcomings the PLA is facing: not enough high-level planning, not enough joint integration across the other domains, and not enough innovation. It specifically notes that the PLA has “little research on the technology and equipment for cognitive domain operations on mainstream social networking platforms,” and it needs to improve its big data, natural language processing, and deep learning capabilities. The goal is to be able to conduct subliminal messaging [yuxia xinxi zhiru, 阈下信息植入], “voice information synthesis technology” (one version of deep fakes) [yuyin xinxi hecheng, 语音信息合成], “network propaganda” and to analyze Internet users’ sentiments. The article also raises the prospects of buying or renting equipment through military-civil fusion to reduce costs while at the same time “ensuring secrecy.” Lastly, in June 2019, another article co-authored by a Base 311 researcher explicitly suggested the PLA should use artificial intelligence (AI) to run its bot network on social media, which would be able to create content based on human guidance, select the appropriate time to post on social media, and be able to coordinate between these “sockpuppet” [majia, 马甲] accounts. Although the article did not explicitly mention cognitive domain operations, its origins with Base 311 suggest it is linked. The PLA has also begun patenting technologies dealing with the cognitive domain since at least 2018, again reinforcing the real-world


99 Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Yao [熊尧], “Intelligent Agent Model For Online Public Opinion Guidance” [“网络舆情引导智能代理模型” no. 3], National Defense Science & Technology [国防科技], June 2019, 73-77.

100 The article used the concept of “online public opinion warfare” (wangluo yulunzhan, 网络舆论战), which it also described as “online public opinion struggle (wangluo yulun douzheng, 网络舆论斗争) and “online public opinion confrontation” (wangluo konqijian yulun duikangzhan, 网络空间舆论对抗战).
 application of this concept. Beyond the hardware, PLA articles also reference “professional cognitive domain operations forces” and “professional forces for offensive psychological warfare.” This clearly indicates the PLA is developing technologies to manipulate foreign social media platforms.

There are several other related terms that are difficult to distinguish in practice. “Online public opinion warfare” has been used to describe how the Internet can be used for influencing public opinion. Another term, “cyber-psychological warfare” [wang xinzhan, 网心战], appears to be a more accessible rendering of “cognitive domain operations” and was coined by NDU Professor Dai Xu, a famous PLA commentator known for hawkish positions. Dai has mirrored Zeng’s framing of the term to prioritize psychological warfare as the natural evolution of warfare and next domain of great power competition by a poetic return to China’s ancient strategy roots from the Three Kingdoms. Dai likens it to a modern-day Trojan Horse by arguing that “in the deformed domain shaped by the interweaving of people’s minds into the ‘Net’, the main form of the strategic competition between major powers has shifted to ‘information-driven mental warfare’” [xinxi sixiang zhan, 信息思想战].

Dai outlines two versions of cyber-psychological warfare: “hard control” [ying kongzhi, 硬控制] for deterrence and wartime employment and “soft kill” [ruan shashang, 软杀伤] for constant offensive peacetime operations, although he notes that the line between these two is blurred. “Hard control” uses “chips and components equipment, in peacetime, to control the adversary’s strategic facilities by cyber means, gather the adversary’s intelligence, have command of the adversary’s data (in the age of big data); and in wartime, to

---


103 Xiao and Li, “Theoretical Analysis of Online Public Opinion Warfare.” For one applied example, see Li, Hu, and Xiong, “Intelligent Agent Model for Online Public Opinion Guidance.”


105 The authors of this report were unable to find any other references to this term in Chinese language sources, suggesting it is Dai’s own interpretation of another concept, which we argue is cognitive domain operations. For more on Dai, see David Lague, “Special Report: China’s Military Hawks Take the Offensive,” Reuters, January 16, 2013, https://www.reuters.com/article/us-china-hawks/special-report-chinas-military-hawks-take-the-offensive-idUSBRE90G00C20130117.

directly attack the opposing state’s strategic nodes, paralyze its networks, and destroy the adversary’s resistance will within a short time.” “Soft kill” involves “launching ideological offensives through cyberspace, mounting strategic ideological warfare directly against the opponent (the state or the whole nation, individuals) by transcending the military domain, so as to achieve the effect of subduing the enemy without fighting.” Dai envisions several missions that could fall under this operational concept, such as “protracted external infiltration, internal disintegration, collaboration between forces from within and forces from without, [and] clandestine and silent struggle.”107 This would appear to align quite well with what is known about PLA strategy for cognitive domain operations, and it provides stark language about its intended objectives.

107 Chu, “Dai Xu: Listening to the Door Knocking Sound of Future Warfare.”
Section 3
Leadership Guidance and Military C2 for Social Media

Chinese Leadership Guidance for Social Media

To Chinese leaders, the Internet and social media are vulnerabilities to be managed domestically, but the PLA increasingly sees them as weaknesses to exploit abroad. Chinese leaders Hu Jintao and Xi Jinping have long spoken about the danger of the Internet to China and the Party’s continued rule, and their sensationalist rhetoric on the U.S. threat to the Party via the Internet is reflected both explicitly and indirectly in writings by many PLA authors. In October 2011, then-President Hu said, “We must clearly see that international hostile forces are intensifying the strategic plot of Westernizing and dividing China, and ideological and cultural fields are the focal areas of their long-term infiltration.”

In April 2013, Xi similarly stated that, “Western forces hostile to China and dissidents within the country are still constantly infiltrating the ideological sphere,” and called for the Party to “strengthen guidance of public opinion on the Internet [and] purify the environment of public opinion on the Internet.”

Adopting this tone, one article bombastically warned about the “sinister intention of the Western hostile forces’ media” by specifically citing Voice of America, and claimed “they try to use ‘heavy cyber bombs.’” Its author added that “Western hostile forces painstakingly created…a batch of ‘big Vs’ and ‘public intellectuals’ on Weibo” to attack the PLA and China on social media.

---


111 Big Vs are social media accounts that have enough followers to lead the platform, for example Weibo, to verify the user’s identity.
General Secretary Xi has pushed the CCP to improve its foreign influence operations and has used social media at least once when he sent a New Year’s message to the troops using the PLA Daily’s Weibo account during a December 2015 visit to its offices. In his remarks on the changes brought by the Internet to “the public opinion environment, target audiences and communication technology,” Xi encouraged extending the military’s propaganda reach to “wherever the audience is.” He told PLA Daily staff to “provide thought and public opinion support for realizing the Chinese Dream and the Strong Army Dream.” When touring the online propaganda center, he also told personnel that they should strengthen their communications capability and that “the military press is surnamed Party,” which presaged his February 2016 call for the rest of the state-run media to be loyal to the Party. Xi’s 19th Party Congress November 2017 speech called for China to be “a global leader in terms of composite national strength and international influence” by 2050 and gave guidance to the broader Chinese propaganda apparatus: “We will...strengthen the penetration, guidance, influence, and credibility of the media. We will provide more and better online content and put in place a system for integrated Internet management to ensure a clean cyberspace.” The PLA interpreted this as “strengthening the military online media’s dissemination power, guidance power, influence power, and public trust.”

Reinforcing this desire for information control, Xi in January 2019 visited Xinhua to discuss more effective public opinion guidance and recommended boosting “integrated media


development and amplifying the mainstream voice,” by developing “websites, Weibo, WeChat, electronic newspaper bulletins, mobile newspapers, IPTV and other forms of new media.” Xi also applied this thinking to foreign social media, as is evident in his book of speeches on the Party’s media strategy in June 2018. He called for “winning international discursive power” and “optimizing international communication strategy and posture,” including “telling China’s story well and molding a positive national image” and “actively using overseas social media platforms.”

PLA Command and Control of Social Media

The PLA controls a range of social media accounts, but there does not appear to be a coherent management structure for its overt social media engagement, with many different organizations’ running their own accounts, research, and operational use spread across the military. As will be discussed later, military-affiliated accounts can have different levels of authoritativeness depending on the unit, but the PLA’s overt social media propaganda accounts appear to be run primarily, or even exclusively, by the PLA propaganda system and ultimately under the Political Work Department. Many, if not all, military media organizations, as well as most services and theater commands, have their own Weibo and WeChat accounts for domestic propaganda. Since the PLA does not yet have its own foreign accounts, it relies for external propaganda on Xinhua, China Daily, and other state-run media to repost military-related content to Facebook and other platforms. Chinese military thinking and analysis about social media generally are under the propaganda system’s research units, but there also appears to be broad interest in social media from different components of the PLA. For example, based on PLA patent filings and PhD dissertations, social media textual analysis research has been conducted at the SSF’s Information Engineering University (IEU) and NUDT.

We assume there is some coordination mechanism to ensure the smooth operation of the PLA’s social media assets, but the specifics of this are far from clear. In the early years of the military’s embrace of social media, such coordination may have fallen to the Central Military Commission (CMC) General Political Department (GPD) Liaison Bureau. However, now that the PLA is reorganized into a more operationally-focused structure, there are multiple moving parts. At the highest levels, China’s information warfare on social media


120 All-Military Military Terminology Administration Commission, People’s Liberation Army Military Terminology.

121 For example, see Xie Songxian [谢松县], “Opinion Mining and Application in Social Media” [“社交媒体中观点信息分析与应用”] (PhD Dissertation, National University of Defense Technology [国防科技大学], 2014).

122 The authors would like to thank Morgan Clemens for his feedback on this topic.
likely is coordinated by the Central Cyber-space Affairs Commission [zhongyang wangluo anquan he xinxihua weiyuanhui, 中央网络安全和信息化委员会], chaired by Party Secretary Xi.123 For the PLA operationally, the SSF appears to be the leading actor, but in wartime it will have to manage at least three categories of accounts: 1) China’s acknowledged civilian propaganda accounts on social media (such as Xinhua on Twitter); 2) the PLA’s own public propaganda accounts (such as the PLAAF’s Weibo account); and 3) the PLA’s covert accounts on Western social media for disinformation. Additionally, if the PLA adopts the Ministry of State Security’s (MSS) approach to hiring Chinese civilian “hacker” contractors to do perhaps the more sensitive and exposed foreign activities, in this case to run a social media campaign like Russia’s Internet Research Agency (IRA), the PLA, likely the SSF, would have to manage these contractors as well.124

The PLA also may coordinate with Chinese “content farms” that produce fake news, where each user is reportedly paid between 100–1,000 renminbi per post depending on length and from which the PLA developed much of its disinformation content for its Taiwan interference.125 For China’s acknowledged propaganda accounts on social media, the SSF likely coordinates with civilian outlets for propaganda through the All-Army Political Work Network [quan jun zhenggong wang, 全军政工网] under the new PWD. For the PLA’s own public social media accounts, the SSF probably gives directives to the relevant units, possibly coordinating with the PWD since it has peacetime responsibility for them. One move toward better integration and coordination for at least overt propaganda appears to be the establishment in 2018 of “service propaganda culture centers” [junzhong xuanchuan wenhua zhongxin, 军种宣传文化中心], which are intended to bring together the management of print, internet, and social media propaganda under one roof for cross-domain synergies.126 For the PLA’s covert accounts, all information and informed assumptions so far point to the SSF owning and commanding those assets itself, likely housed under the Network Systems Department (NSD).

The leading SSF unit most likely is Base 311 (Unit 61716) for hostile influence operations.

---

123 For an article on the Commission, see “Xi Outlines Blueprint to Develop China’s Strength in Cyberspace,” Xinhua, April 21, 2018, http://www.xinhuanet.com/english/2018-04/21/content/137127101.htm.


125 Li Ruobing [李若冰], “China’s Astroturf and Cyber Army Train Mind Superiority with 2020 Elections as Target” [“中國水軍、網軍九合一練兵「制腦權」，目標2020大選”], Storm [風傳媒], November 23, 2018, https://www.storm.mg/article/643412.

on social media. This is “the PLA’s sole organization that is publicly known to focus on psychological warfare.” Although Base 311 was under the GPD in the pre-reform era, it is now assigned to the SSF, likely the NSD, which means that the NSD is “in command of the full spectrum of information operations—not only cyber but also electronic and psychological warfare. The move itself appears to remove organizational impediments to coordination across the information operations disciplines, integrating them in peacetime to ease their transition into a wartime structure.” Some researchers believe that the SSF may have overarching responsibility for information operations in cooperation with the relevant theater commander in wartime.

However, one important unanswered question is who actually would run these accounts for the SSF, especially for foreign social media, since there have been limited SSF writings on actual social media content and strategy. The SSF may have enough people familiar with Taiwan’s information environment and society to permit using its own staff. Indeed, the Taiwanese media reported that “China’s fake news...generally gets published first by Chinese outlets such as the Global Times, Straits Today and Taihai Net” targeted at Taiwan, and is then tailored by the SSF and reposted to social media. In a future conflict that involves targeting foreign countries, however, it is unclear that the PLA would have sufficient expertise in-house. One option is that staff from Xinhua and other state-run media with peacetime expertise in Western social media could either be seconded to the SSF, or the SSF could simply give them instructions through the All-Army Political Work Network. However, since it may be difficult for the SSF to facilitate access to these covert accounts outside SSF facilities, it seems more likely the SSF would host civilian staff. If this staff expertise situation is accurate, this may motivate the SSF to develop its own in-house expertise on foreign social media in order to streamline future disinformation operations.

Although social media lives in a virtual world, the PLA, drawing in part on observing the U.S. military’s heavy emphasis on training cyber personnel since at least 2007, knows it needs dedicated professionals to shape its message. A May 2015 article calls for “combining specialized public opinion monitoring software and professional public opinion analysts.” The author argues that the PLA has so far largely ignored public opinion guidance.


during crises and instead relied on “deleting, blocking and blacking out information,” which does not actually publicize the PLA’s message. Social media and personal blogs are now the most influential forms of media, followed by blogs and forums, then local media, and lastly official media. But, ultimately, the goal is to “weaken the influence of the Western concept of values through a cumulative effect of propagation over time.” Another author argues that the PLA needs its own dedicated social media team, and content will have to be original and tailored, not simply translating Xinhua or PLA Daily articles meant for domestic audiences. The 2018 articles by Base 311 and NUDT researchers on cognitive domain operations suggest the PLA is already developing such forces, as the Base 311 article called for “improving the overall operational capabilities of professional cognitive domain combat forces.”

It appears that the PLA already is improving its online public opinion management via “commenting teams,” content monitoring, and “positive” propaganda. In 2017, the PLA established an “online public opinion management bureau” and Xinhua also works to guide public opinion on the military as well.

This would align with a greater push to hire younger and more social media-savvy Chinese propagandists to maintain the Party’s grip on the narrative. Another, often implicit, component of building a professional social media warfare team is training linguists who can seamlessly employ native or near native language to engage with target audiences, as the SSF is expected to do for operational security reasons. One source noted that the U.S. Department of Defense’s Boren Scholarship and Fellowship program under the National Security Education Program (NSEP) trains students in critical foreign languages and helps the U.S. military translate “language capability into operational capability,” which is a necessary component for foreign military operations and offensive psychological warfare. This source called learning foreign languages a “smoke-less weapon” for the PLA.

One way to assess the PLA’s social media management and bureaucratic interests is by examining who authors its social media analysis. The vast majority of the PLA’s social media experts come from the PLA’s propaganda and political warfare system. The Military Correspondent published 147 articles with 155 unique authors through December 2017 which mentioned “social media.” Fifty-three authors (37 percent) were from the PLA’s Nanjing Political Institute, the home of its research and training for political warfare (now reorganized into NDU’s Political College), and 45 authors (31 percent) were from PLA Daily, along with 7 authors from the PLA’s TV studio (5 percent).

134 Xiao Fei [肖飞], “Analysis on the Countermeasures to Strengthen the Construction of Our Military’s New Media Power” [“加强我军新媒体力量建设的对策探讨”], Military Correspondent [军事记者], no. 1 (2017): http://www.81.cn/jsjz/2017-01/06/content_7440635.htm; and Sun and Dong, “The Characteristics and Insights from U.S. Military on Online Public Opinion Control.”
135 Zheng, “How Official Chinese Propaganda Is Adapting to the Social Media Age as Disaffection Spreads Among Millennials.”
Less than 5 percent of the authors were from Xinhua or military region and service newspapers. There also were some authors from NDU (8 percent), as well as unidentified units from the Army, Rocket Force, and Strategic Support Force (SSF). These authors without explicit propaganda-focused affiliations still could be their units’ respective propaganda officers, but this is not certain. This breakdown is similar for Military Correspondent articles mentioning Western social media platforms such as Twitter (70 articles) and Facebook (58 articles). Authors from the Nanjing Political Institute wrote 42 percent of articles mentioning Twitter and 48 percent of those mentioning Facebook, while the PLA Daily produced 26 percent of articles mentioning Twitter and 14 percent of those mentioning Facebook. The majority of authors from the PLA’s political warfare institutions reflected the PLA’s view that social media is for influence operations.
Section 4
Chinese Lessons Learned from Other Countries

The PLA released its first guidance for public opinion warfare in December 2003 and over the next few years conducted research on the topic, including at the Academy of Military Science and PLA Nanjing Political Institute.137 The PLA's work on external military propaganda was highlighted in June 2008 with the first seminar on the topic and a follow-on conference with the director of the General Political Department that October.138

137 The PLA was tasked with “conducting public opinion warfare, psychological warfare, and legal warfare; developing work to disintegrate the enemy military; developing work to counter psychological warfare and the inciting of internal rebellion.” See Regulations on Political Work in the People’s Liberation Army” [“中国人民解放军政治工作条例”], CCP Central Committee [中共中央], revised December 5, 2003; and Li Jian [李健], Li Xuehong [李雪红], and Bao Guojun [包国俊], “Military Transformation with Chinese Characteristics Is Underway” [“中国特色军事变革在行动”], China Youth Daily [中国青年报], April 11, 2004, http://zqb.cyol.com/content/2004-04/11/content_853658.htm. For analysis, see: Mattis, “China’s ‘Three Warfares’ in Perspective.”

138 Xiang Fei [项飞] and Yan Manwei [严满伟], “Seminars on Theory and Practice of External Military Propaganda Held in Nanjing Institute of Politics” [“军事对外宣传理论与实践研讨会在南京政治学院召开”], PLA Daily [解放军报], June 28, 2008; and Ding Haiming [丁海明], and Li Donghang [李东航], “First Session of All-Army Advanced Seminar on Foreign-Oriented Propaganda Held in Beijing: Xu Caihou Lays down Requirements for Holding All-Army Advanced Seminar on Foreign-Oriented Propaganda, Li Jinai Meets, Addresses All Seminar Enrollees” [“首期全军对外宣传高级研讨班在京举办 NATO campaign against Muammar Gaddafi in Libya in 2011 (mentioned in thirteen Military Correspondent articles) further emphasized the value of public opinion warfare and how the Internet could play a role in military operations.139 A September 2015 PLA Daily article asserted that “from Libya to Iraq, from Ukraine to Syria, social networks have already become a new battlefield that all parties in a conflict intensely engage” and detailed the evolution of social media through the 2009 Iranian protests, 2011 Arab Spring protests, Israel’s 2012 war in Gaza, to the ongoing wars in Syria and Ukraine.140 The PLA has been proactive about learning from others and sent teams to visit Russia and Israel to discuss directly their operations and experience on social media. Making clear the continued value of learning from the West, one researcher at the Nanjing Political Institute wrote in 2014 that “offense is the best defense...new media has the characteristic of strong penetration, and since Western countries can infiltrate [us], we can infiltrate [them] in the same way.”141

139 For example, see Sun and Dong, “The Characteristics and Insights from U.S. Military on Online Public Opinion Control.”

140 Chen, Fang, Yang, and Xia, “Social Media Warfare: A New Dimension to Warfare in the Information Age.”

141 Miao Jian [苗健], “With the Help of Overseas Open Internet Information Platforms: Seeking Equal
United States

China has learned the most from the United States about how to use social media for influence operations, since the PLA clearly believes the United States is the best at this in the world. Through December 2017, 2,143 articles in Military Correspondent mentioned the United States, including 188 that specifically cited public opinion warfare and 76 that referred to social media. This compares with 326 articles that mentioned Russia, 88 that referenced Israel, and 8 that cited ISIS. Before the advent of social media, China’s interest in public opinion warfare began with “Operation Iraqi Freedom” in 2003 and the United States’ successful use of mass media to shape public and elite opinion in both the United States and Iraq.142

Social media has gravitated from an afterthought in studies of public opinion warfare to a central focus on influence operations in the information domain. These lessons now are being applied by the PLA to the role of social media in shaping public opinion.143 A May 2017 article noted that the U.S. military uses its skills for “public opinion manipulation” to control the public opinion narrative at home and abroad and, therefore, can expand its political influence and “willpower-destructive power,” or ability to undermine enemy morale, for military operations and even to support deterrence.144 This article argued that public support was necessary to support a nation at war, and that the dominant factor in swaying public opinion for the Iraq War nowadays has shifted from TV to online media. The Chinese article’s authors count 113 Twitter accounts operated by the U.S. military, along with others on Facebook, YouTube, and Flickr, and argue that these accounts are “an important weapon for concentrating, guiding, utilizing, shifting and creating international and domestic public opinion” and are enabled by dedicated social media professionals.145 Similarly, PLA authors have learned from NATO’s embrace of social media and “strategic communications.”146 Reflecting thorough research, these authors cite


143 For just a sample of articles on the United States in 2018, see Guo Yunfei [郭云飞] and Zhu Jianwei [朱建微], “Insights from the U.S. Military’s News and Public Opinion Control for Our Military’s Network Propaganda” [“美军新闻舆论管控对我军网络

144 Li Lin [李林] and Li Zezhong [李泽中], “Perspectives on NATO’s Use for Its Military Strength in Libya” [“透视北约在利比亚的军力使用”], PLA Daily [解放军报], October 31, 2011; and Sun and Dong, “The Characteristics and Insights from U.S. Military on Online Public Opinion Control.”

145 Sun and Dong, “The Characteristics and Insights from U.S. Military on Online Public Opinion Control.”

146 Mou Shan [牟珊], “Analysis of NATO’s Strategic Communication Strategy” [“北约战略传播策略探析”], Military Correspondent [军事记者], no. 2 (2016): 44–45, http://www.81.cn/jsjz/2016-06/17/content_7106856.htm; and Zhang Ming[张明], Mou Shan [牟珊], and Huang Xiaowei [黄晓伟], “Analysis of NATO’s Strategic Communication Strategy” [“北约战略传播运行机制探析”], Theoretical Studies
numerous U.S. military regulations on social media use in operations, such as the July 2011 Department of Defense (DOD) “Strategy for Operating in Cyberspace,” and take inspiration for regulating PLA troops’ social media use from U.S. guidelines, such as the January 2011 “U.S. Army Social Media Handbook.”

An example of how U.S. cyber operations concern the PLA is the U.S. military’s use of online anonymous accounts to counter ISIS and other terrorist groups. The PLA is very concerned by reports that the United States already is using fake social media accounts to combat terrorism online. One Military Correspondent article interpreted this as the United States fighting bad press by using anonymous fake accounts to create the illusion of grassroots authenticity.

This was interpreted as part of broader U.S. hypocrisy about using “Internet freedom” to force other countries to open their Internet and, thereby, enable the United States to manipulate public opinion in order to secretly fix its broken reputation. The article contends that it is likely that other countries will copy the United States and then nothing online will be authentic, which is a curious interpretation from a country that routinely censors, misleads, and even buys social media followers on Western social media. The article argues that the Chinese government should defend against this U.S. “astroturfing” through building new software to detect fake IP addresses and censor negative discussions and by increasing control of social media, including strengthening the monitoring of Twitter, Facebook, and YouTube in order to understand what is trending, guide public opinion on these platforms, and respond to “fake news.” It notably did not say that China should copy the U.S model for anonymous accounts. Rather, it proposes that the PLA should build a team which includes famous scholars for public opinion guidance on the foreign Internet. This article clearly assumed the worst about U.S. intentions and interpreted actions targeted at terrorists in the Middle East as also against China. Yet, reports...
of the PLA using fake social media accounts to influence Taiwanese politics suggest that whatever restraint was evidenced by some in the military was not shared by senior PLA leadership.

The PLA’s interest in, and justification for, cognitive domain operations is also tied to Chinese beliefs about U.S. and Russian activities on social media for political interference around the world. The October 2018 SSF Base 311 article consistently references U.S. and Russian capabilities as the model for China’s development of its own capabilities, noting that recent U.S. military operations have demonstrated that they are increasingly important for modern warfare “before, during, and after the war, especially for mainstream social networks.” It adds, “with the rapid development of communication and network technologies, the major countries represented by the U.S. military have vigorously developed cognitive domain operations network equipment and cognitive intervention weapons.” A similar April 2018 article by NUDT and other researchers argued that Western countries used Twitter and other social media for cognitive domain operations during the Arab Spring. Clearly, China feels it has much to learn in this domain: “due to [China’s] late start, short development time and low investment, there are many difficult problems...Our army’s follow-up research in this area is insufficient.”

Russian

Russia’s recent propaganda resurgence and use of social media during foreign military operations also have provided China with a model to emulate, with the main takeaway being the importance of actively promoting one’s own narrative to counter the West’s negative spin before and during a conflict. One Chinese article by a General Staff Department (GSD) author on Russia’s “public opinion warfare” in Ukraine drew three lessons: take the offensive by pushing your narrative first, make your legal arguments, and back it up with hard power. On the last point, he writes, “all actions of media warfare, psychological warfare and legal warfare, must, in the final analysis, rely on the comprehensive national power, especially the nation’s hard power with the military as the core.” The most authoritative article on Russia’s deployment

151 Liu, Xiong, Wu, and Mei, “Several Thoughts on Promoting the Construction of Cognitive Domain Operations Equipment in the Whole Environment.”


153 For Chinese lessons drawn from Russia’s recent actions in Ukraine and Syria, including for public opinion warfare, see Wang Jichang [王继昌], “Main Experience of Russia’s Military Operations in Syria” [“俄罗斯在叙利亚军事行动的主要经验”], China Military Science [中国军事科学], no. 5 (2016): 119–126; and Zhu Ningning [朱宁宁], “An Analysis of Russia’s Unfolding of Media Warfare Tactics Amid the Turbulent Political Situation in Ukraine” [“乌克兰政局动荡中俄对乌舆论战谋略运用探析”], Military Correspondent [军事记者], no. 5 (2014). For an article drawing on the White Helmets’ use of social media, see Liu, “Do Agenda Setting Well, Seize International Communication Discursive Power.” For a summary of a NATO report on how to counter adversary uses of social media, based on Russia’s use of social media in Ukraine, see Kuang Xiaoqin [匡晓沁], “Analysis on the Coping Strategies for Social Media Information Warfare: Taking Russia’s Approach to the Ukraine Crisis as an Example” [“社交媒体信息战应对策略探析：以俄罗斯应对乌克兰危机为例”], Military Correspondent [军事记者], August 22, 2018, http://www.81.cn/jsjz/2018-08/22/content_9260460.htm.

154 Zhu, “An Analysis of Russia’s Unfolding of Media Warfare Tactics Amid the Turbulent Political Situation in Ukraine.”
to Syria noted that Russia worked to counter “smearing speech” from the United States and the West through information transparency and promoting its own narrative.\textsuperscript{155} Furthermore, an August 2016 article in \textit{PLA Daily} by a deputy commander of the Northern Theater Command, the most senior officer we observed drawing lessons from Russia, argued that Putin was successful because he seized the informational advantage before the conflict began. He noted that,

...before launching the war, the Russian military used a diplomatic offensive and guiding public opinion as the main method. They took seizing the control of the Internet as the fundamental [policy], and controlled information through multi-dimensional linkage. In order to occupy the position of public opinion, Russia carefully designed and implemented the public opinion war to seize the moral and psychological high ground.\textsuperscript{156}

A September 2015 \textit{PLA Daily} article focused on Ukraine’s use of social media to push back against Russia, calling the 2014 protests “a classic ‘Facebook revolution’” and noting its low-cost and immediate results.\textsuperscript{157} Although these articles do not draw explicit operational lessons for the PLA’s use of social media, it is clear that such platforms could support the envisioned proactive propaganda strategy.

Another aspect of influence operations the PLA has learned from Russia is how to exploit the fallacy of balanced and objective reporting for injection in Chinese propaganda narratives. A September 2018 \textit{Military Correspondent} article drew explicit lessons about exploiting the U.S. audience’s desire for truth amidst worsening faith in media by wrapping propaganda and Russian values within “objective” coverage from the \textit{Russia Today} (RT) coverage of U.S. air-strikes on Syria. It said that “we can study RT’s communication method….At the same time as not losing ‘objectivity,’ [we] can silently influence the audience’s emotions and inclinations, and make them become dependent on information from our country’s media.”\textsuperscript{158} Another article analyzed the U.S. media’s façade of balanced reporting.\textsuperscript{159} It found that when the

\textsuperscript{155} Wang, “Main Experience of Russia’s Military Operations in Syria.”

\textsuperscript{156} Li Qiaoming [李桥铭], “Analysis of Modern Warfare Development Based on Russia’s Two Conflicts” [“从俄罗斯两场战事看现代战争新发展”], \textit{PLA Daily} [解放军报], August 16, 2016, http://www.81.cn/theory/2016-08/16/content_7208644_3.htm. The article was originally published in \textit{Guangming Daily} [光明日报]: Li Qiaoming [李桥铭], “Studies on Russia’s Modern War Practice—Study Russia’s Strategic Transformation Based on Its Two Military Actions and What the Actions Have Taught Us” [“俄罗斯现代战争实践研究:从俄两次军事行动看其战略转型及对我的启示”], \textit{Guangming Daily} [光明日报], no. 11 (2016): http://epaper.gmw.cn/gmrb/html/2016-08/10/nw.D110000gmrb_20160810_1-11.htm.

\textsuperscript{157} Deng Xiumei [邓秀梅], Yan Zhenhua [严振华], and Zhang Jiayu [张佳璐], “The Social Media War in the Ukraine Crisis” [“乌克兰危机中的社交媒体战”], \textit{PLA Daily} [解放军报], September 25, 2015, http://www.81.cn/jmywyl/2015-09/25/content_6697523.htm.


Chinese military seized a U.S. military unmanned underwater vehicle (UUV) in 2016, the Chinese state-run media cited the Chinese government more than the U.S. media cited the U.S. government. This made the U.S. media look more “balanced” even though the author still believed U.S. news was delivering propaganda on behalf of the government. Reducing quotes from the Chinese government, the article argued, would resonate better with Western audiences who prefer “objective” news they think is independent from the government.

RT also has been a model for leveraging social media and using disinformation against the West. NDU analysts called RT a “propaganda aircraft carrier” for its engagement on Twitter, Facebook, YouTube, and Instagram. They argued that “in the Internet age, public opinion propaganda has risen to an important means of safeguarding national interests,” and the contest is between “whoever has the stronger external propaganda media,” with Russia’s use of RT serving this role. They highlighted RT’s presence on YouTube, where it “provides a large number of topics with sharp video content for audiences to watch. In Russia and even in the West, it attracts a large number of netizens (Internet users) to pay attention and become an important ‘mouthpiece’ for public opinion propaganda in Russia.” Another recent article has focused on RT’s value for disinformation, reflecting a shift in the PLA’s discussion of offensive uses of social media.

Despite clear PLA focus on learning from Russia’s social media strategy, there has been a noticeable absence of analysis of Russia’s use of social media to interfere with the 2016 U.S. presidential election. For Chinese military authors monitoring global developments of social media, the 2016 election would have been impossible to overlook. Yet, until the summer of 2018, there were very few, if any, articles about Russia’s actions in the election. This will be covered in depth in Section 9.

**Israel**

The PLA also has closely followed the Israeli military’s use of social media in its ongoing struggle against Hamas. The PLA saw the early value of Western social media as a deterrent in Israel’s psychological operations during its 2009 conflict in Gaza. Focusing on Israel’s “psychological deterrence against Hamas militants,” a PLA Daily article noted that “besides using traditional means of psychological warfare such as dropping leaflets and battlefield messages, the Israeli army also set up a dedicated website on the Internet… in an attempt to win the understanding and support of domestic and international publics from all walks of life,” specifically mentioning Twitter, YouTube, and Israeli-run webpages in

---

160 Ma, Zhang, and Zhang, “Russia’s New Front for Defending Internet Media.”

Arabic and English.\textsuperscript{163} Another article noted that before Israel’s November 2012 bombing of Gaza, “the information office of the Israeli Defense Force set up accounts with main social media, including YouTube, Facebook, Flickr, Twitter and made announcements there.”\textsuperscript{164} During the conflict, Israel streamed “live battle scenes,” making “the influence of the new media war completely [overcome] the actual firepower war.”\textsuperscript{165}

The PLA has also learned from Israel’s use of multiple languages to reach specific international target audiences on social media. Another article on the 2012 war concluded that “social media played an important role....the two sides collected intelligence and conducted propaganda” for public opinion warfare.\textsuperscript{166} Other reports noted that Israel has accounts on the top 10 most used Western social media platforms with a total of 57 million followers, including 14 million on Twitter.\textsuperscript{167} Most recently in October 2018, an article in \textit{Military Correspondent} highlighted Israel’s civil-military coordination of offensive public opinion warfare in wartime and how the Israeli government was able to force Western social media platforms, such as Facebook, Twitter, and YouTube, to censor anti-Israeli posts and delete accounts run by Hamas through domestic legislation.\textsuperscript{168} The PLA appears to have absorbed Israel’s use of multiple languages into its social media playbook in Chinese air force propaganda, for example, in its use of Chinese dialects spoken in Hong Kong and Taiwan. However, it will be much harder for China to force Western social media companies to enforce Chinese censorship edicts since they have no market in China.\textsuperscript{169}

---


\textsuperscript{164} Wang Xuchao [网旭超] and Zhang Dongdong [张东东], “Cyber Attacks Step onto the Front” [“网络攻击走上前台”], \textit{People’s Army News} [人民军队报], May 16, 2013, 4.

\textsuperscript{165} Wang and Zhang, “Cyber Attacks Step onto the Front.”

\textsuperscript{166} Yan Shiqiang [颜士强], “Strive to Cultivate Military Reporters Who Adapt to the New Media Ecology” [“努力培养适应新媒体生态的军事记者”], \textit{Military Correspondent} [军事记者], June 22, 2017, http://www.81.cn/jsjz/2017-06/22/content_7648406.htm. See also Li Shuhong [李树宏], “Gaza Microblog War’ Notice” [‘加沙微博战’及启示], \textit{Leadership Science} [领导科学], no. 16 (2013).

\textsuperscript{167} Zhou Lei [周雷] and Meng Chaojie [蒙超杰], “The Era of Social Media Mobilization and Impact on War Has Arrived” [“社交媒体动员并影响战争的时代到来”], \textit{National Defense} [国防], no. 7 (2016) 22–23.


ISIS

Meanwhile, ISIS’ deft use of social media for incitement and recruitment has caught the attention of the Chinese. One analysis of ISIS’ social media strategy focuses on its “mass strategy” that overcomes U.S. counter-terrorism efforts by using a mix of official and semi-official accounts, with one central account releasing a message and then having foreign supporters around the world spread this message if its accounts are blocked. This article highlights four aspects of ISIS’ strategy. First, ISIS targets public figures, because if public figures are brainwashed, they can amplify the message to a broader audience. Second, ISIS has special software that can identify and target youth when they register on social media. Third, ISIS tailors content for social media and phones, using photos and videos in different languages to target different audiences. Fourth, ISIS employs hashtags to become trending topics and expand influence. The PLA also has mentioned U.S. cyber operations against ISIS, specifically targeted at the group’s propaganda capabilities by disrupting and closing its social media accounts, including by pressuring Facebook, Twitter, and Google to contain ISIS’ online presence.

These articles generally treat ISIS as a threat. This likely is driven by Chinese military fear about ISIS recruitment of Uyghurs, although this reason is never explicitly mentioned. However, another explanation of Chinese interest could be that the PLA is seeking to learn from ISIS’ ability to covertly recruit otherwise ordinary foreign citizens to a cause that is opposed in their home society—an ability that would be useful before or during a conflict with other countries for China. Another explanation would be that learning from ISIS’ ability to broadcast its message on U.S.-run platforms such as Twitter, despite U.S. pressure and even censorship, and successful targeting of susceptible populations, are both key goals for PLA propagandists, even though the articles do not explicitly draw any lessons.

Foreign Cooperation on Social Media Strategy?

Beyond researching from afar, the PLA has directly engaged with some of its leading role models for further lessons about how to use social media for military information operations by sending delegations to at least Russia, Israel, Belarus, and Germany. Likely in 2017, an MND press team visited Russia and related that the Russians view information operations as a “force multiplier.” Likely sometime during 2018, the SSF branch director for PLA Daily visited Israel’s military press office and reported that its social media presence includes six languages, which gives it direct communication with its audience and thereby avoids media distortion. In April 2019, the


deputy head of the PWD’s information and propaganda office visited Belarus to “share… best practices in organizing information and propaganda work” though it ostensibly was focused on military museums.¹⁷⁵ There is no evidence that any of these engagements focused on disinformation or election interference, but since these known engagements all occurred after 2016 and given Beijing’s deepening security cooperation with Moscow, it is something that bears further scrutiny.

PLA Messaging, Engagement, and Targeting Strategies for Social Media

The PLA is constantly considering how best to increase the effectiveness of its influence operations at home and abroad through better engagement and targeting strategies on social media. Military researchers realize its current reach on social media, especially in foreign countries, is insufficient to achieve its three objectives: narrative dominance, deterrence, and political interference. Several core tenets drawn from its traditional communications strategy drive the PLA’s approach to social media, including rapid response, agenda setting, and adaptive messaging, as well as finding common ground and targeting users with tailored messages. The PLA has adapted several tactics for social media, including more active engagement from its overt accounts, coopting influential individual users with a preexisting large audience to spread its propaganda and obfuscate the Party origins of the message, and manipulating foreign media organizations to do the same. The PLA believes targeted and tailored messaging will be a key part of its success, but all available evidence so far suggests little nuanced understanding of what this would entail and limited appeal of PLA propaganda to foreign audiences. Although these strategies are geared toward the PLA’s official overt accounts, they are equally applicable to its covert, or unofficial, accounts for political interference.

PLA Social Media Accounts by the Numbers

The PLA manages a broad range of overt official accounts that can be used for narrative dominance through propaganda and for deterrence through psychological warfare. By February 2017, PLA Daily reported there were 700 military-run accounts on Chinese social media out of over 800 million Weibo users and one billion WeChat users. The first PLA account on social media appears to have been the PLA Daily’s Weibo account in March 2010, and the military’s propaganda organs, PLA Daily and China Military Online, registered accounts before the PLA Army, Navy, and Air Force. PLA authors have proposed different ways to conceptualize these various military-run accounts.


177 One author claims that the PLA Rocket Force (PLARF) joined in 2011, but this report’s authors were unable to find any such account. See Wu, “The Status Quo and Development Suggestions of Military Social Media.” Of note, the PLARF has actually been the service to write the most on foreign signaling. See Lu, “Boosting the Use of the Strategic Force through External Propaganda.”
counts. One divided these accounts into three categories: “authoritative official military public accounts” that are verified on social media and directed by the respective propaganda units; public military accounts that are not verified but still run by propaganda units; and individual soldiers’ personal public accounts that are not verified but are still somewhat controlled by virtue of their duty.\(^\text{178}\) Other authors have suggested they be segmented into media accounts, government accounts, and individual soldiers’ accounts.\(^\text{179}\) Another account type worth noting that was not explicitly addressed is those of PLA propagandists, most famously Major General Luo Yuan, whose primary job is to guide public opinion.\(^\text{180}\) Regardless of category, the PLA has many accounts under its control with various ways to employ these account types, especially unofficial accounts, for deniable disinformation operations.

Since the PLA’s expansive number of accounts and intensive efforts to develop them have not necessarily led to influence and success, some experts are critical of the PLA’s effectiveness on social media. One author argued the PLA still does not have enough accounts nor enough followers.\(^\text{181}\) He claims that there is no control system in place, so the accounts are of varying quality, with some unused “corpse accounts” that clearly are not fulfilling their mission to guide public opinion.\(^\text{182}\) A 2018 article argues the PLA still undervalues social media by treating it like traditional media without being sufficiently targeted.\(^\text{183}\) Another factor is that the PLA’s direct presence on social media is only on Chinese platforms, as there are no known accounts on Twitter run by the Chinese military. Instead, Chinese propaganda efforts on Twitter are directed by Chinese government offices and state-run media. This means that the Chinese military’s reach to foreign audiences is limited and reliant on other Chinese government actors.

**History of PLA Influence Operations on the Internet**

To understand the PLA’s social media strategy, it is helpful to look at its leading precursor, the *China Military Online* website, which it closely resembles. *China Military Online* is the PLA’s English-language website that was started in 2003, and the website’s own introduction

---

\(^\text{178}\) Song Mingliang [宋明亮] and Huang Yumin [黄裕民], “What Kind of Media Are the Military’s Public WeChat Accounts” [军队微信公众号是怎样的媒体], *Military Correspondent* [军事记者], no. 5 (2017): http://www.81.cn/jsjz/2017-05/10/content_7595213.htm. Although this article’s categorization is for WeChat accounts, this reflects broader PLA discussions of all social media accounts. PLA-run accounts are not verified if the “user” cannot be publicly identified due to secrecy regulations. Another category of accounts not listed would be military enthusiasts, who are Chinese netizens who post military-related news but are not soldiers.

\(^\text{179}\) Wu, “The Status Quo and Development Suggestions of Military Social Media.”


\(^\text{181}\) Xiao, “Analysis on the Countermeasures to Strengthen the Construction of Our Military’s New Media Power.”

\(^\text{182}\) For similar criticism, see Wu, “The Status Quo and Development Suggestions of Military Social Media.”

\(^\text{183}\) Wu, “The Status Quo and Development Suggestions of Military Social Media.”
explains it is intended to “[build] up the online international communication capacity of the Chinese military” with its “main tasks” as “leading online public opinion and setting a good image of China’s military abroad.”

Visits by General Secretary Hu Jintao and other CMC members to China Military Online’s office indicate the high-level support it enjoys for external propaganda and its desire to be an authoritative platform. Similar support was shown by China’s then-Minister of Defense, Liang Guanglie, in 2011, when the website was updated. He said that he “hoped” the China Military Online and MND websites, including mobile phone versions, “could play a bigger role in publicizing and expanding the influence of the PLA,” and the PLA Daily hailed its iPhone-specific website as “[bringing] ease and convenience...to a wider population of smartphone users.” This appears to have been realized, as one article explained that 85 percent of China Military Online’s audience is overseas, including over 20 percent from the United States and 15 percent from India.

Some military authors clearly frame extending the PLA’s propaganda reach in terms of influence operations. One concluded his recommendations by saying that “if foreign public opinion work is the same as public opinion warfare struggle, then China Military Online’s English service has the capacity to be an airborne insertion of paratroopers and shock troops into the enemy’s rear.”

Articles in Military Correspondent paint a clearer picture of China Military Online’s purpose and strategy. A 2007 article outlined the goals of the website as supporting the PLA’s “three warfares,” including “wartime minimum operating measures” with a “target network address database”; cooperating with “foreign militaries to open up new channels for external military propaganda work,” pending approval by the relevant leadership; and supporting the development of a professional staff for Internet propaganda. A 2013 article provided more details on its communications strategy by explaining its founding assumption that “the Western world’s aggressive culture carries out a containment-centered strategy on our country, which severely interferes with the strengthening of our country’s international influence,” and that China’s “international discursive power” is “weak.”

According to the authors, this is because “more than 80 percent of the important international news in the world is provided by a few major news outlets of the developed nations in the

186 Chen, “Create a Shock Team for Military External Propaganda.”
Western world” and that rises to 90 percent online. They acknowledge that “China Military Online would usually seek a different angle” than domestic propaganda, since it “must understand what the target audience wants” in order to tailor the message to the “thinking and reading habits of the Western audience.”

China Military Online’s content is heavily scripted and “actively engaged in topic planning and selection to effectively respond to the concerns of the international community as well as the doubts of the international public opinion.” To expand its attraction, the website began promoting English-language videos and also recommended incorporating “civilian media outlets’ work on foreign affairs into our military’s foreign publicity system.”

A 2018 article on the website’s future argued that it should expand its services to include “important targets” such as Vietnamese and Japanese, and because of the Belt and Road Initiative (BRI) also open Arabic, French, and Spanish services. Perhaps the biggest crossover account run by the PLA is China Military Online’s account on Weibo, which brings external propaganda to a domestic audience.

These writings on China Military Online reflect the military’s desire to use the Internet to extend the reach of the PLA’s propaganda and psychological warfare abroad with a targeted message to foreign audiences through finding common ground and leveraging extant foreign dissemination channels through cooperation with foreign partners. However, there clearly is a broader external propaganda strategy at work. The PLA almost seems to have desired the benefits of social media before it even became a reality, and such thinking is now a recurring theme in PLA strategy for social media.

PLA authors paint a stark picture of the control exerted by the Chinese government over the country’s media, including private news portals and social media companies. One article noted that when the United States indicted PLA officers for hacking in 2014, “all major portal websites…promptly pushed the messages to the interface of the cell phone and tablet users, thus shaping a media posture of ‘airing the same voice in an overspread way’ [and] on social media platforms, media and opinion leaders published commentaries in their individual names, and many accounts also relayed the commentaries of the mainstream media.” The overall Party line was set by the traditional media, but this narrative was spread and amplified to the broader public on social media. Its general strategy was to denounce and deny, change the topic, and conduct a “media counteroffensive.” This “counteroffensive” utilized “multiple opinion-voicing entities to carry out all-directional counterattacks,” and asserted that “unofficial opinion leaders, such as Weibo VIPs and cyberspace commentators” were used to more subtly influence public opinion.

The close ties between the PLA, civilian state-run media, and even non-government media were evident in a forum hosted by the PLA following General Secretary Xi’s 19th Party Congress speech in 2017 that discussed the topic of improving PLA propaganda. The PLA forum’s participants included Director Hu

---


191 Chen, “Create a Shock Team for Military External Propaganda.”

192 Weibo [微博] account, China Military Online [中国军网], https://m.weibo.cn/profile/5996312730.

Changming of the CMC International Military Cooperation Office, Deputy Editor-in-Chief Wang Yizhen of the People’s Daily, Vice President Liu Xinyang of Xinhua News Agency, President Li Xiubao of the PLA Daily, Chairman and CEO of 360 Group Zhou Hongyi, President Chen Hao of Phoenix Network, Professor Zhang Zhaozhong from NDU, and Dean Yang Shuzhen from China Cyberspace Research Institute. This reflected PLA efforts to recruit and control influencers as a way to obfuscate the Party origins of its message.

**General PLA Communication Strategies Applied to Social Media**

The PLA’s general propaganda strategy is guided by several tenets: rapid response, agenda setting, and adaptive messaging—all while seeking to find common ground with its audience. As one author argued, the PLA’s social media strategy should be to “attract people with ‘hot topics,’ touch them with [personal stories] and keep them with sentiment.” The PLA also has embraced public opinion monitoring to support these tenets, and even talks about developing an “early warning” system so it can get ahead of the discussion and shape it in its favor or censor it altogether, if necessary.

The first tenet of the PLA’s communication strategy is rapid response—to be the first, or at least the loudest, in response to breaking events, since the military knows public opinion forms quickly. Chinese experts suggest the propaganda system should prioritize responding to sensitive topics. Several authors agree that public opinion guidance is most important for “incidents” related to CMC leaders, such as Xi Jinping. Others argue this should extend to senior officers, as well as the PLA budget, military policies, military operations, and all major foreign activities. Early PLA writings focused on integrating social media into the broader propaganda system, and how it could augment traditional media strategies. These early writings also grappled with the challenges between balancing control of social media against speed for a timely, but perhaps uncoordinated, response. However, more recent articles have moved beyond this tension between traditional and social media and instead focused on social media as a separate channel for propaganda.

The utility of PLA engagement on social media during “hot-spot events” is detailed in a 2012 article reflecting on the Scarborough Shoal standoff with the Philippines, which considers how to seize “the preemptive position in influ-

---


encing public opinion.” Newspapers such as PLA Daily are supposed to provide the government line and proper interpretation of events, but since social media has accelerated the formation of public opinion, the article asserted that there is a “‘golden 24-hour rule’ for the response to an emergency event.” Thus, government-orchestrated social media campaigns can shape early public opinion before the print media is able to finalize its broader propaganda strategy. Early social media work should “stress that news released must be timely, and the government should make its voice heard at the first opportunity [...] and be] the ‘first to give definition’ to the emergency event.”

A 2014 article echoed this, saying “those who can be the first to release information may win an advantageous position influencing public opinion as first impressions are often strongly entrenched in people’s minds. Those who can be the quickest in setting up the agenda may win the control of public opinion and dominate public discourse.” Reflecting the quickening pace of online discussion, a 2018 article claimed that the “24-hour rule” now has turned into the “four-hour rule.”

The second tenet of the PLA’s social media strategy is agenda setting. This entails “selectively and continuously reporting news on a certain subject,” and as one article contends, “we need to carefully pre-set our own agenda from beginning to end so to direct the general public’s attention at home and abroad.” Echoing classic Western research on agenda setting, the author argued “there exists a kind of causality as ‘the priority subjects in the news media will become the priority subjects of public concern.’” The article’s authors contended that the West already employs this strategy to turn public opinion against China. They argued that the U.S. amplifies “human rights, Taiwan, threats from China, military expenditure, and China trade” while the UK media focuses on “the so-called ‘3T’ subjects, namely, the Tiananmen Incident, the Taiwan issue, and the Tibet issue.” Chinese military media employ agenda setting to develop not only long-term messaging but also immediate crisis response at the request of the government, and when the PLA feels it is fighting a losing narrative battle, it will shift topics to something more positive, such as focusing on the hard-working researchers who developed new military hardware instead of the threatening aspects of such hardware. This agenda setting can be strongly reinforced at a subconscious level if it is repeated, a process sometimes referred to as brainwashing or stealth propaganda.

198 Yu Chunguang [于春光], “Enhancing Public Opinion Guidance Capability for International Hotspot Events” [提升国际热点事件舆论引导能力], Military Correspondent [军事记者], July 2012.
199 A 2014 article echoed this, saying “those who can be the first to release information may win an advantageous position influencing public opinion as first impressions are often strongly entrenched in people’s minds. Those who can be the quickest in setting up the agenda may win the control of public opinion and dominate public discourse.”
200 Chen, “Preliminary Thoughts about Strengthening Cyber News Media in Wartime.”
201 Zhao, “Reflections on Creating a Weibo Military Image.”
205 For references to subconscious messaging, see Zhang Fang [张芳], “External Propaganda of Military Affairs in China’s Military Diplomacy” [“中国军事外交中的军事对外传播”], Military Correspondent [军事记者], January 2, 2014, http://www81.cn/jkhc/2014-01-02/content_5716684.htm, 38–40; and Xu Sen [许森], “Communicating Our Military’s Advanced Military Culture to the World” [“向世界传
authors specifically have referenced the value of agenda setting for driving the conversation on social media and drawn inspiration from General Secretary Xi’s favorable recommendation during a 2016 Politburo study session.\textsuperscript{206}

The third tenet of the PLA’s social media strategy is to adapt its narrative if it is not gaining traction with the general public. If the PLA determines it cannot control the public discussion, then its last resort is to censor the discussion. One author suggested the PLA adopt a top-down iterative and adaptive feedback loop for propaganda based on “creation–employment–evolution.”\textsuperscript{207} The author added that the PLA needs more centralized and empowered propaganda teams to enable this quicker and more targeted response, because the PLA currently lacks a centralized approach to make PLA propaganda organs speak with one voice. Others have argued that the PLA should use domestic social media (without mentioning foreign social media) and leverage opinion influencers to create a “feedback mechanism” to control public opinion.\textsuperscript{208} Some authors have suggested that the PLA should develop and test theories of how best to guide public opinion, “even proactively triggering public opinion to verify and assess the effectiveness of the theories,” in part by adding negative content to a “black list” and monitoring “key regions and key people” to develop data for these predictive theories.\textsuperscript{209}

These three communication tenets drive the PLA’s desire to develop a public opinion monitoring system to quickly identify and address “sudden incidents” before they get out of hand, often referred to as “early warning,” and to support a rapid feedback loop to further refine propaganda messages.\textsuperscript{210} An NUDT professor stated at a 2013 PLA forum on online public opinion that “China has 93 companies with 104 versions of online public opinion systems,” but maintained that these systems were not yet fused together and had poor analytic functions.\textsuperscript{211} PLA interest also
applies to monitoring foreign social media. PLA patents reveal an intent to build a public opinion monitoring system. Several patents relate to sentiment analysis on Chinese social media, including detecting hot events based on sentiment analysis. Separately, another patent supports early warning and censorship by finding pre-determined information if it appears on the Internet, and others can trace information back to the source and create an information dissemination model. It is clear that the PLA is serious about developing these capabilities, and, while the patents so far do not appear focused on Western social media, it would be a natural outgrowth of a PLA presence on those platforms.

PLA propagandists advise finding common ground with their audience, especially when they do not feel comfortable engaging on the substance of an issue such as PLA intentions. As one article explained,

"With regard to Western audiences, we need to conscientiously filter the content of communication, finding more points of resonance and common ground… even in the case of positive propaganda we also need to be adept at ‘softening’ the content. For example, using stories to convey things, ‘translating’ viewpoints into stories, and concealing them in stories,… we should adopt open and emotional methods."

This is also another way to compensate for failed agenda setting. For example, another article concluded that the best way to counter the West’s China-threat theory is to “enhance the affinity of Chinese culture and values,” rather than engaging the substance of the argument. Similarly, others suggested that highlighting common values, such as the hard work of individuals, also can bridge the cultural gap that otherwise would leave a foreign audience uninterested or wary of the Chinese military. Another suggested method is to highlight human stories with broad appeal, such as the 2015 evacuation of Chinese citizens from Yemen as it descended into civil war, when Chinese social media focused on human stories of evacuating from the war-torn country,

212 Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda.”


215 Xu, “Communicating Our Military’s Advanced Military Culture to the World.”

and the side benefit was showing PLA Navy strength (instead of arousing fear from a show of force).217

The PLA is clearly aware of the challenges it faces with reaching Western audiences, spanning from linguistic, rhetorical, and cultural differences to simply not being able to attract their attention. One suggestion from an NDU propaganda researcher was to follow Hollywood’s model and use China’s entertainment industry and Chinese culture “to improve the image and the foreign influence of our military,” as well as talk about the good things China does and find common ground—like hardworking soldiers.218

The use of “reasonably plain language” and consistent messaging was recommended in order to get “the overseas audience to accept our viewpoints subconsciously,” with specific guidance to find common ground with Western audiences. The emphasis on translation was evident in a July 2012 article that stated, “Frankly speaking, how much of our voice can be transmitted to the opponent in the public opinion warfare and whether our propaganda can really reach foreign countries relies to a great extent on whether our voice and our propaganda are translated into the language that the opponent can understand or at least to English, the current lingua franca.” 219 The article noted that English articles are easier for Western media to pick up and carry, and so could be utilized to transmit China’s narrative.

Yet, even translation cannot completely bridge the divide, as the burden is on the PLA to understand and tailor the message to its targeted audience accordingly. As an example, the dragon, a positive symbol of power in traditional Chinese culture, is a poor image for China to use in propaganda for Western audiences, since it could carry a negative and scary connotation. Such tailoring for customs and culture, not only language, is a challenge the PLA is aware of and is attempting to adapt to.220 A mark of progress in the PLA bridging the culture gap was the PLA’s 2016 release of a hip-hop recruitment video on its website, 81.cn, called “Battle Declaration,” which garnered online attention from Western media, though PLA researchers still found Western media’s coverage was biased against China.221


218 Xu, “Communicating Our Military’s Advanced Military Culture to the World”; and Dong Tao [董涛], “Advancing International Communications for Military News [Toward] Differentiated Audiences” [“推进军事新闻分众化的国际传播”], Military Correspondent [军事记者], no. 7 (2012).

219 Guo Jiquan [高吉全], “Give Play to Dagger Role of Commentaries on Current International Affairs in Public Opinion Warfare: Thoughts on Writings of Several Recent Commentaries on Current International Affairs” [“发挥国际时评在舆论战中的尖刀作用: 近期几篇国际时评的撰写体会”], Military Correspondent [军事记者], no. 6 (2018).

220 Sun and Dong, “The Characteristics and Insights from U.S. Military on Online Public Opinion Control.”

Gaining Influence Through Coopting Existing Channels

The PLA is interested in recruiting or coopting “influencers” to tout the Party’s propaganda line to address this perceived lack of sway on social media and obfuscate the Party origins of the message. This is part of a long track record, dating at least to the mid-2000s with the advent of popular blogs, of PLA propaganda leveraging existing “opinion leaders” in various media forms. As the editor of Military Correspondent wrote in 2010, the PLA must “expand external military propaganda positions outside official channels” because “at present, our country still does not have an unofficial media in the real sense. And the main targets of our military’s external propaganda are overseas audiences….The more official the news and information is, the less they tend to believe it.”

The answer is to “focus on overseas audiences’ psychological state of receiving information and with an appropriate degree expand our military’s external propaganda position beyond the official channel. By doing so, we will be able to enhance the efficiency of our military’s external propaganda.” Recognizing that users may not trust official channels, the writer advised seeking “influencers” to amplify PLA messaging through unofficial channels and voices. A July 2013 article noted that “with the rise of the microblog as the cyber media instrument with the ‘greatest killing power,’ the role of Internet ‘opinion leaders’ in influencing public opinions has become increasingly prominent.”

This desire for “influencers” has migrated now from TV to blogs to social media. A May 2015 article noted that on Weibo, “about 300 ‘opinion leaders’ control agenda setting to obtain considerable discursive power,” drawing an analogy to the relative dominance of the most popular Twitter accounts. The article revealed that the PLA “hosted two workshops on Chinese military community cooperation and development [and] the participants were all moderators and ‘opinion leaders’ of each major military community” in the hopes that they could “smooth propagation channels.”

A March 2017 article further argued that “for guidance on public opinion incidents relating to the military, only using official media are far from enough…. [We] must strengthen our cultivation of online opinion influencers.” A December 2013 article drew lessons from U.S. public diplomacy that exploiting celebrities was a good way to shape the conversation by utilizing their preexisting influence and fan base, for example, promoting badminton champion Lin Dan’s love of the PLA.

---

223 Zhu Jinping [朱金平], “Create Maximum Efficiency of our Military’s External Propaganda” [“创造军事对外宣传效益的最大值”], Military Correspondent [军事记者], no. 11 (2010).
227 Wu Bing [吴兵] and Liu Wei [刘炜], “The Revelations of Public Diplomacy to Raising the Dissemination Force of External Propaganda” [“公共外交
emphasis on opinion leaders on social media led the PLA, since the blog era when authors called for “skillfully establishing blog information spokespersons,” to seek to develop its own propagandists into online stars. Others have noted that PLA commentators can play this role because “experts” have more “freedom in expressing opinions,” so they can be “an effective strategy for public opinion guidance.”228 This has carried over more recently into social media, as several articles suggested that the PLA needed more “Big V” accounts (accounts with so many followers their identity is verified by the platform).229 This means that the PLA should cultivate and coopt these opinion leaders, including interviewing them, as a way to grab their audience.

These influencers also can be foreigners, whether wittingly supporting the Party line or having PLA media cite unwitting foreign experts whose views conveniently align with China’s narrative. One article argued that “making use of the viewpoints and opinions of third party media and experts, amplifying voices advantageous to our side, can be effective.”230 Another article provided the example that, as part of public opinion guidance, Chinese media amplified a Western expert’s skepticism of the evidence presented in the May 2014 U.S. indictment of PLA officers for hacking in order to counter the U.S. narrative that China was behind the cyber-attacks.231 A different source added that “only by cultivating some opinion leaders with influence on the international community can we make sure that their voices will be loudly heard in foreign affairs issues,” and noted that Chinese media should amplify foreign analysis that accords with the Party line.232

Similarly, another author added that “for some well-known and influential foreigners, [we] can use their visits to China or interviews through other means to deliver statements that are beneficial to us and easy to be received by Western audiences.”233 Most recently, a July 2017 article on how the PLA handled foreign public opinion guidance for the launch of China’s second aircraft carrier argued that the PLA should “quickly coordinate and mobilize the resources of China’s accounts on import ant international social media to broadcast official explanations and information, as well as retweet [forward] third party positive comments about the carrier by third parties and

---


229 Zhang Jiaqi [张珈绮], “Improve the Military’s External Propaganda Capability and Tell the Chinese Military’s Story Well” [“提高军事外宣能力讲好中国军队故事”], Military Correspondent [军事记者], no. 11 (2016): http://www.81.cn/jsjz/2016-12/01/content_7387398.htm; and Jiang, “Use Media to Create a New Type of Combat Force.”

230 Pu Duanhua [濮端华], “An Analysis of China’s Public Opinion Strategy in the Diaoyu Islands Dispute” [“钓鱼岛争端中的我舆论斗争策略探析”], Military Correspondent [军事记者], no. 10 (2012).

231 Hou Lei [侯磊], “The Handling of Public Opinions in Negative Incidents in International Communications: Taking the U.S.Media’s Hype of ‘Chinese Hacking’ as an Example” [“国际传播中负面事件的舆论应对与思考：以美媒炒作‘中国网络黑客’话题为例”], Military Correspondent [军事记者], June 2013.

232 Hou, “The Handling of Public Opinions in Negative Incidents in International Communications: Taking the U.S.Media’s Hype of ‘Chinese Hacking’ as an Example.”

233 Chen, “Create a Shock Team for Military External Propaganda.”
give play to ‘third-party authoritative and trustworthy’ pro-China media and academics.” Furthermore, “[we] should plan to invite them to comment on the carrier’s launch, and use many parties to reduce the ‘Chinese military threat’ theory.”234 Therefore, for Western social media, the PLA could woo influential users to promote its Party line.

Cooperating with, or really coopting, foreign media organizations and using Western social media platforms are the other main approaches mentioned in PLA writings to easily gain influence. This is often referred to as “borrowing a boat out to sea” [jiechuan chuhai, 借船出海], and seeks to exploit existing channels to reach previously untapped audiences.235 This phrase represents a long-standing Chinese government approach to exploit foreign media to deliver Chinese propaganda.236 One author stated that the PLA should cooperate with foreign media to use their “existing channels to quickly enter the target market through paid or free article placement, content exchanges or custom distribution,” as these are “effective methods to quickly elevate the Chinese military media’s ‘landing rate’ and ‘delivery rate.’”237 Other writers have simply suggested that, since the PLA’s messaging still reaches international audiences through Western media,

Figure 2. Rising PLA Interest in Controlling Online Influencers

![Graph showing rising PLA interest in controlling online influencers](source: CNKI)


236 James Jiann Hua To, Qiaowu: Extra-Territorial Policies for the Overseas Chinese, 177.

the Chinese military should embrace this and try to have the Western media “magnify” its talking points about international military exchanges, military competitions, and military visits.238 The chart above shows the growth of Military Correspondent articles referencing Big Vs and interest in coopting others, in contrast with declining references to more traditional opinion leaders [yulun lingxiu, 舆论领袖] as the attention shifted to social media for public opinion guidance.239

If the PLA is unable to coopt influencers on foreign social media, another tactic discussed is to try to exploit platforms’ own rules to silence undesirable voices. One 2018 article by PAP researchers recommends, in response to the anti-China criticism of Uyghur activists on Twitter, that China should cooperate with Twitter on “counter-terrorism” to get Twitter to close the activists’ accounts.240 Drawing from Twitter’s cooperation with the United States to close terrorist accounts, the authors argue China should petition Twitter to abide by international counter-terrorism conventions to monitor the accounts and to be more responsive to “reports” about them. If this fails, the article also suggests discrediting them, using patriotic “Big Vs” and opinion leaders to counter their narrative, and opening more official accounts across multiple foreign platforms to better reach overseas Uyghurs. This follows PLA discussions of Israel’s consideration of domestic laws to force Twitter and other social media platforms to censor foreign content.241 Of note, the accounts of over 100 anti-China dissidents on Twitter were suspended ahead of the 30th anniversary of Tiananmen in June 2019, though Twitter apologized and reopened their accounts, citing its own spam filters and denying they were reported by China.242

Some PLA authors have applauded ostensibly independent self-organization by enthusiastic civilian netizens who circumvent the Great Firewall to vent nationalist opinions against foreign targets. The most prominent example is a January 2016 effort to post critical comments on President Tsai’s official Facebook page.243 Although there was no evidence this was conducted by bots, according to research by Oxford University, state-run media positively reviewed the event.244 Although military researchers similarly could not officially condone this behavior since it was technically


239 Also rendered as 意见领袖 (yijian lingxiu).


against the law in China, they nevertheless described this favorably as a grassroots movement for “online ideological struggle” and a modern form of the “people’s war.” 245 One even implied it could be “normalized” over time. 246 Even if this instance was not organized, it is not hard to imagine some government or military encouragement for similar efforts in the future as a semi-deniable way to generate authentic comments on foreign social media.

One tactic not explicitly discussed by PLA authors but used by Chinese state-run media is to artificially inflate the number of followers for their social media accounts. Reports exploring the unexpected surge of followers of Chinese state-run media accounts on Facebook and other platforms date back to 2015. 247 But it was a January 2018 New York Times report that first detailed how an “editor at China’s state-run news agency, Xinhua, paid [a company] for hundreds of thousands of followers and retweets on Twitter.” 248 Despite this spotlight, a 2019 Economist report suggested state-run media’s follower counts were still artificially high. 249 This tactic aligns well with PLA interest in cultivating opinion leaders, in this case simply building themselves into opinion leaders, and would certainly be one possible approach if the Chinese military does open accounts on foreign social media in the future (see Section 6 below for more).

Targeting Audience with Tailored Messages

The PLA has long sought to improve its propaganda effectiveness through targeted and tailored messaging, and social media makes this even easier. PLA researchers suggest, at the most basic level, to differentiate between the two sides of a conflict and neutral countries, reflecting the 2013 Science of Military Strategy’s goal to win “sympathy and support” from the international community. 250 The 2013 AMS book on information operations states that, “Psychological warfare targets include key enemy military and political officials, participating soldiers, ordinary people, the enemy’s allies and even the international community.” 251 One article developed a matrix approach to targeting, breaking people into four groups: one’s own people, one’s allies, the enemy’s people, and neutral countries; and three levels: leadership, troops, and the common people. 252 Another article explained that “intermediate forces and neutral third parties are important forces that need to be unified for our public opinion struggle.” 253 Articles have similarly

---

245 Li Yuanyuan [李媛媛], “Fight against Attacks in the Online Ideology Battle” [“打好网络意识形态斗争进攻仗”], Political Workers [政工导刊], no. 4 (2017): 15–16; and Liu Weichao [刘伟超] and Zhou Jun [周军], “New Ideas to Improve Our Army’s Online Public Opinion Capability” [“新理念提升我军网络舆论引导能力”], New Media [网络传播], no. 7 (2018): 88–90.


247 Grundy, “Did China’s State-Run News Agency Purchase Twitter Followers?”; and Olesen, “Where Did Chinese State Media Get All Those Facebook Followers?”

248 Confessore, Dance, Harris and Hansen, “The Follower Factory.”


253 Sun Wenjing [孙文静] and Wang Lin [王林], “The Scarborough Shoal Incident in the Eyes of Foreign Media and Revelations for our Propaganda
explained that targeting can be based on people’s beliefs, value systems, or inclinations in order to influence people from different countries, political parties, or cultural groups.\textsuperscript{254} One argued it could be done based on social, political, economic, cultural, religious, or even psychological characteristics.\textsuperscript{255} This strategy has been part of the PLA’s response to crises over the Scarborough Shoal, South China Sea, and Senkakus, and even in its approach to overseas basing.\textsuperscript{256} This builds on the PLA tactic of finding common ground as described above.

One specific demographic that is mentioned as a target for influence is younger audiences, including foreigners.\textsuperscript{257} One early article by the editor of Military Correspondent argued that “After the bullet train of the times abruptly ushered humankind into the microblog era by means of the Internet, disruptive changes were made to the concepts, modes, and channels by which the news audience—and the youth audience in particular—receives public opinion propaganda.”\textsuperscript{258} Another article explained that,

the channels and methods for youth to receive communication are undergoing significant changes.\ldots internet technology has changed the way people, especially the younger generation, consume information.\ldots Military propaganda should enhance its effectiveness and influence. It must also face up to the changes in the way audiences, especially young people, receive information, innovative forms and methods, broaden the channels of voice, respond to audience concerns, and enhance audience participation and enthusiasm.\textsuperscript{259}

This attention on younger audiences is not just domestic, as some Chinese articles on ISIS and Russia have focused on their ability to win over foreign youths, and others have detailed U.S. social media use by age bracket, noting that while nearly 70 percent of U.S. adults have social media accounts, 88 percent of young adults do.\textsuperscript{260} This aligns with the broader Chinese propaganda thinking that shaping opinions in younger foreign

\textsuperscript{254} Dong, “Advancing International Communications for Military News [Toward] Differentiated Audiences.”

\textsuperscript{255} Wu and Mei, “Some Inspirations Drawn from the Application of Booming Social Media in Psychological Warfare,” 77–80.


\textsuperscript{257} For how China is targeting younger audiences domestically, including by the PLA, see Minnie Chan, “China’s Military Newspaper PLA Daily to Cut 240 Jobs as It Targets Online Audience, Sources Say”; and Zheng, “How Official Chinese Propaganda Is Adapting to the Social Media Age as Disaffection Spreads among Millennials.”

\textsuperscript{258} Zhu Jinping [朱金平], “A Brief Exploration of Model Propaganda Tactics in the Microblog Era” [“微博时代的典型宣传策略浅探”], Military Correspondent [军事记者], no. 7 (2011).

\textsuperscript{259} Wang Jinyao [王锦尧] and Li Jiaxin [李嘉鑫], “Cultivation of New Media Audience in Military Culture Communication” [“军事文化传播中新媒体受众的培养”], Military Correspondent [军事记者], no. 2 (2016): http://www.81.cn/jsjz/2016-02/19/content_6919237.htm.

audiences is easier and has longer-lasting effects. Moreover, some of the social media platforms mentioned in Military Correspondent are disproportionately more popular among younger audiences, such as YouTube (94 percent of 18–24 year olds vs. 56 percent of 50+ year olds), Snapchat (78 percent vs. 7 percent) and Instagram (71 percent vs. 16 percent). Although these articles generally do not reference their specific value for targeting younger audiences, a passing familiarity with U.S. social media would make this clear. Indeed, at least some PLA propagandists understand this targeting, as one praised Xinhua’s foreign social media accounts on Twitter and Facebook for “accurately, immediately and effectively” spreading China’s message, especially to foreign youths. This interest in foreign social media as a vector to reach younger audiences again underlines the PLA’s interest in changing international attitudes toward China through narrative dominance, which is one component of its influence operations.

Yet such theorizing so far falls short. Despite the universal agreement that the PLA should improve its audience targeting and narrative tailoring to increase the impact of its propaganda for influence operations, there is little nuance or substantial recommendations to be found in these writings beyond this basic message tailoring. One article detailing China Military Online’s audience only provided very basic statistics on visitors’ IP addresses with no basic analysis. Furthermore, there was no discussion of the differences between the website and social media, and no analysis of social media discussion.

PLA patents also appear to support improved targeting of domestic and foreign social media users. A 2017 patent from the SSF’s IEU claimed to enable the PLA to associate nominally unaffiliated Twitter, Facebook, and Instagram accounts to a single (hidden) user behind the seemingly separate accounts. Although the patent filing did not explicitly frame this for targeting, it did say this was for public opinion guidance and network security, specifically for detecting malicious users. It claimed that based on “basic information, hobbies, friends, relations and historical activities,” it could identify “a malicious attack with a large number of accounts on multiple platforms” in order to “maintain social stability.” This also could be aimed at identifying bots of the type the PLA suspects the United States uses to fight terrorists and fears could be turned on China. Additional patents claim to identify on improving foreign propaganda that lacks detailed proposals.

261 For example, see Cai Yintong [蔡印同], “Overseas Students: An Important Force for People-to-People External Propaganda” [“留学生: 民间外宣的重要力量”], International Communications [对外传播], no. 3 (2009).


263 Li, “How Does Chinese Military News ‘Go Out.’”

264 For one sample, the September 2018 edition of Military Correspondent [军事记者] has a whole section

265 While it made the claim that normal people just wanted to read about their own country, it provided no analysis to prove this, such as simply showing that Indian IP addresses read mostly India-related articles. See Chen, “Create a Shock Team for Military External Propaganda.”

opinion leaders and leadership groups in support of public opinion guidance.267

Other patents claim to identify communities on social media, specifically mentioning Facebook and Twitter, and measure social media influence.268 Two similar patents from researchers at the SSF’s IEU in early 2018 estimated a Weibo user’s influence based on the probability the user’s followers retweeted or spread their posts.269 Lastly, NUDT patents have focused on improving estimates of social media users’ age and gender based on network mapping, while referencing Twitter.270 Perhaps facilitating all of this, SSF Base 311 researchers created a data crawler program to scrape information from inside Sina Weibo, including automatically handling the required log-in and verification process.271 Coupled with a 2011 PLA article expressing interest in scraping Facebook, this could be one approach to gathering this data with covert accounts.272 Perhaps to be expected, these patent filings by science and technology schools indicate a much more in-depth understanding of social media analysis and software code for analytic tools than the discussions by propaganda experts writing in Military Correspondent, but this also suggests that there is limited cross-over of true expertise between different parts of the PLA bureaucracy.

References to Social Media Platforms Reveal Targeting Preferences

The PLA’s use of social media and an analysis of social media platforms referenced in Chinese military writings illustrate that social media is intended primarily to shape domestic public opinion, or at least users of Chinese-controlled platforms, such as ethnic Chinese abroad, a key target of Chinese influence operations. Military Correspondent and PLA Daily both began discussing social media in 2009 but greatly expanded coverage over 2012–2014. Domestic platforms Weibo and WeChat comprise over 90 percent of the references.273


Within mentions of Western social media, Twitter and Facebook predominate, followed by YouTube. This somewhat aligns with the popularity of social media platforms in the United States and the broader developed world. According to a 2018 Pew Research Center survey, the most popular social media platforms in the United States are YouTube (used by 73 percent of respondents), Facebook (68 percent), Instagram (36 percent), Pinterest (29 percent), Snapchat (27 percent), LinkedIn (26 percent), Twitter (24 percent), and Whatsapp (22 percent).274 There has been some coverage

274 Smith and Anderson, “Social Media Use in 2018.”

Figure 5. Chinese Military References to Western Social Media Platforms

SOURCE: CNKI
in *Military Correspondent* in the last few years of newer platforms such as Instagram, Snapchat, and Pinterest, but *PLA Daily* has never mentioned these. Other Western platforms mentioned as recently as 2017 include some that are no longer popular such as Flickr and Google+, which suggests an outdated understanding of the evolving landscape of Western social media.

**PLA Social Media Analytics**

This raises the question of how the PLA gauges the effectiveness of its social media outreach and what data and analytic tools it has at its disposal.275 *Military Correspondent* articles have mentioned Tweet Binder and BuzzSumo tools for analysis, but they simply provide basic statistics such as retweets and the number of people reached.276 One author used BuzzSumo to analyze PLA-related discourse on Twitter, Facebook, LinkedIn, Google+, and Pinterest, among others.277 He found that *Xinhua*’s most

Table 2. Comparison of Chinese Government, Media, and Military Accounts on Social Media Platforms

<table>
<thead>
<tr>
<th>Account</th>
<th>Weibo Account Created (Year)</th>
<th>Weibo Followers</th>
<th>Twitter Account Created (Year)</th>
<th>Twitter Followers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>China Daily</strong></td>
<td>Nov. 2009</td>
<td>43.3 million</td>
<td>Nov. 2009</td>
<td>4 million</td>
</tr>
<tr>
<td><strong>PLA Daily</strong></td>
<td>Mar. 2010</td>
<td>20.5 million</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Global Times</strong></td>
<td>Feb. 2011</td>
<td>24.5 million</td>
<td>Jun. 2009</td>
<td>1.4 million</td>
</tr>
<tr>
<td><strong>China Military Online (English)</strong></td>
<td>Apr. 2011</td>
<td>6</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>People’s Daily</strong></td>
<td>Jul. 2012</td>
<td>100+ million</td>
<td>May 2011</td>
<td>7 million</td>
</tr>
<tr>
<td><strong>Ministry of National Defense (MOD)</strong></td>
<td>May 2015</td>
<td>7.1 million</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>PLAAF</strong></td>
<td>Oct. 2015</td>
<td>2.8 million</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>PLAA</strong></td>
<td>May 2018</td>
<td>1.7 million</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>PLAN</strong></td>
<td>Apr. 2019</td>
<td>880,000</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>SSF</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>State Council Information Office (SCIO)</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>Sept. 2015</td>
<td>2</td>
</tr>
</tbody>
</table>

---

275 For how the PLA assesses its broader online public opinion efforts, see Wu Jie [伍杰] and Liao Dongsheng [廖东升], “Analysis of the Effectiveness of Online Public Opinion Warfare” [“网络舆论战效能评估探析”], *National Defense Science & Technology* [国防科技] no. 2 (2014), 21-23.

276 Zhou, “An Exploration of U.S. Military Operations on Social Media to Fight ISIS”; and Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda.”

277 Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda.” For an analysis of the PLA Army’s Weibo strategy and related engagement statistics, see Wang Jian [王健], “Preliminary Exploration of Military Weibo Communication Results: Taking ‘People’s Army’ Weibo Account as an Example” [“军队微博传播效果初探:
popular PLA-related tweet got 900 retweets, which would seem to represent limited reach. Other articles have criticized the PLA’s domestic social media accounts for having lots of followers but few retweets, revealing a continued lack of nuanced analytics of social media data. A Military Correspondent article by a civilian academic used reposts, likes, video views, and Baidu searches for related topics as a way to gauge the impact of Weibo posts by the PLAAF. While this would hint at the concept of “engagement,” that term did not appear in PLA writings. It is clear the PLA is still learning how to utilize social media, and based on the track record of other Chinese propaganda organs, the fruit of these endeavors may take time to grow. Such basic recommendations about using more images, GIFs, videos and even simply hyperlinks are made by NDU graduate students, not established researchers, which suggests a possible generational disconnect of senior thinkers not actually understanding the nuances of social media. Yet, there is still the ambition, as one article set the goal of over 100,000 retweets as the new standard for PLA social media. One further complicating factor for the PLA is that because only state-run media have accounts on foreign social media, PLA researchers are forced to rely on data from Xinhua’s China International Communication Research Center or People’s Daily Online’s Public Opinion Data Center.

This is not to say that the broader Chinese security establishment completely lacks social media analytics. A 2018 article by PAP researchers demonstrated at least some proficiency with basic analytics, representing the best we could find. The article focused on foreign human rights activists’ use of Twitter to raise awareness of China’s treatment of the Uighur ethnic minority in Xinjiang, where over a million people have been put into what U.S. officials have referred to as “mass imprisonment of Chinese Muslims in concentration camps.” The article uses many different types of social media metadata to identify and analyze the key members of the Uyghur activ-


281 This was intended as a goal for WeChat, which is more plausible. See Lin, Liu, and Tan, “From ‘100,000+’ to See How the WeChat Public Account Won the Audience: Take the ‘No. 1 Post’ WeChat Public Account as an Example.”

282 For example, see Zhao, “Thoughts on the Creating the Image of the Military on Weibo”; and Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda.”

283 For an early example of advanced social media analytics by Chinese Academy of Sciences researchers written in 2007, see Qiang Liu, Feng Yu, Shu Wu, and Liang Wang, “Mining Significant Microblogs for Misinformation Identification: An Attention-based Approach,” ACM Transactions on Intelligent Systems and Technology 9, no. 4 (2010).

284 Wang and Mei, “A Study of ‘East Turkistan’ Terrorist Patterns on the Twitter Platform and Countermeasures.”

ist community on Twitter, including when the accounts were created, the type of platform the users use to post to Twitter, the location of their followers by city, and the numbers of posts, likes, and followers of different users. For specific tweets, it analyzes the time of day they were posted, their content (by word frequency), and hashtags used. They were even able to create a network diagram based on interactions with one of the most prominent accounts, @UyghurCongress. However, even this much broader analytic approach has serious shortcomings, because the PAP researchers did not refine their data to make it useful—the most frequent word they found in one of their content analysis graphics was “http,” so it is difficult to draw any conclusions about what topics were being discussed. Nevertheless, with the PAP now officially under the CMC, it is possible these enhanced analytics could be shared across the PLA.

**Offensive Psychological Warfare: Sensationalist or Revealing?**

Some PLA writings on influence operations and the role of social media focus on explicitly offensive employment and more aggressive tactics. While these non-authoritative articles may appear as sensationalist posturing, consistency over the years suggests there is at least a stream of thought within the Chinese military that believes certain conditions warrant an even more aggressive approach than the day-to-day overt propaganda for influence operations China already undertakes.

One of the most explicit discussions comes in a May 2006 article on “public opinion decapitation,” which focuses on undermining enemy leadership.286 This aligns with what the 2013 AMS book could be categorized under the first component of wartime information operations, “psychological propaganda inducement.” The article describes this as “dealing effective attacks on the leader of the enemy side by means of mass media,” and draws lessons from U.S. rhetoric against Saddam Hussein in the Iraq War. This reflects PLA thinking on how to use influence operations or psychological warfare for deterrence by undermining enemy resolve and leadership, either by discrediting the leader or disintegrating enemy troops’ will to fight through “shock and deter.” The article argues that “propaganda for ‘demonizing’ the leader of the enemy side, and by means of disseminating information that sows discord or produces deterring effects…cripples the enemy leader’s command authority and weakens his command and control ability.” The point is to use a “decapitating opinion offensive…as an instrument of large-scale propaganda and brain-washing for the government, to guide the voice of all the mainstream media at home and abroad and then influence the audience so that public opinion in war can serve one’s war purposes.” This can be targeted at the enemy leader, which requires a psychological assessment of the leader to detect weaknesses, or the broader public and troops, which requires prior research and analysis to support tailored messaging. According to the authors, “public opinion decapitation” should be part of a broader media offensive for public opinion warfare and can be preemptive, although the attackers should prepare for retaliation. Even though this article was written before the advent of social media, it clearly would be a part of such a campaign undertaken today. The authors’ discussion of the U.S. military’s efforts to target Iraqi officers’ email and cell phones with propaganda before the war to encourage defection could easily be applied by the PLA.

---


to targeted social media appeals to foreign troops.

A November 2013 article highlights the important role of psychological and public opinion warfare to “subdue the enemy without fighting” on social media. The author lists several methods, including “creating information chaos,” brainwashing (defined as extreme public repetition of one’s views), and “exaggerating the conflict of interests within the enemy camp.” Most notably, he also discusses “using public scandal or revelation of personal secrets to defame the enemy leaders, and weakening their leadership ability,” and “using prisoners of war for counter-propaganda,” as well as “spreading all kinds of rumors and information.” There is a focus on the growing importance of social media for shaping Chinese public opinion, but he bemoans the role of “Big Vs” on Chinese social media in promoting liberal values, and claims that “enemies” want to “cause internal strife and civil war to subjugate China and cause China to collapse.”

A separate 2017 article analyzed the United States’ “public opinion decapitation” specifically against Muammar Gaddafi by releasing negative propaganda online to dissolve his military’s resolve. The relationship between psychological warfare and cyber operations was explained in one article as information suppression during war which includes “soft suppression” of public opinion guidance and “hard suppression” of “directly attacking the enemy’s command and control system via measures like virus spreading, hacker attack…to sink the enemy into a situation of chaos, fear and dread.” This aligns nearly perfectly with Dai Xu’s cyber-psychological warfare uses of “soft kill” and “hard control,” suggesting these are not random musings but revealing glimpses of at least elements of PLA thinking.

A July 2014 article provides the clearest writing on the role of social media in PLA offensive psychological operations by focusing on the role of “cyber media warfare” to deter and undermine an enemy’s will to fight. The article explains that it is a kind of combat operation with the internet as the platform….targeted information infiltration is made through the internet media for influencing the convictions, opinions, sentiments, and attitudes of the general public so as to effectively control the public opinion condition, shape strong public opinion pressure and deterrence over the adversary, and win an overwhelming public opinion posture for one’s own side.

This influence operation clearly summarizes the PLA’s goals for using social media and the Internet more broadly against adversaries. It recommends “carrying out ‘point-to-point’ targeted ‘bombing’ against small groups of recipients by using such media as email, Weibo and WeChat messages, and cell phone text messages.”

---

288 Wu, “Be on Guard against Other Kinds of Soft Warfare.”

289 Sun and Dong, “The Characteristics and Insights from U.S. Military on Online Public Opinion Control.”


291 Chu, “Dai Xu: Listening to the Door Knocking Sound of Future Warfare.”

292 Chen, “Preliminary Thoughts about Strengthening Cyber News Media in Wartime.” For a similar analysis of the role of online public opinion warfare for “smearing” and “demonizing” enemy leaders through releasing negative information about them, see Xiao and Li, “Theoretical Analysis of Online Public Opinion Warfare.”
messages, so as to achieve the purposes of undermining and bringing down the morale of the military forces and the civilian people on the enemy side, and deliver ‘soft killing’ for forcing the enemy to surrender,” drawing lessons from U.S. and allied information operations in Iraq and Libya. The author argues that the PLA should seek to set the narrative agenda around its absolute military power, relative and asymmetric military advantages, and deterrence power, all to “daunt the enemy troops.” Supporting this offensive action, China also will need to monitor and censor online discussions domestically. The author calls for “traditional media” to “set up their Weibo and WeChat accounts...[to] dominate the ‘micro-communication market,’ drive the agenda and content interaction as quickly as possible, and closely integrate the ‘official’ and ‘unofficial’ opinion circles.” Of note, the author also argues “it is necessary to pertinently carry out technical reconnaissance against the enemy’s cyber media attacks,” although it is unclear if the author was suggesting hacking foreign social media platforms.293 As a real world example, a September 2015 PLA Daily article noted that Israel used Twitter to threaten the Hamas leadership during the 2012 Gaza war for “psychological intimidation.”294 There already has been a link to such Chinese activity. Allegedly, one motivation for China’s reported hacking of a Singaporean health care company was to “blackmail prominent politicians or business leaders who have embarrassing conditions such as sexually transmitted diseases.”295

293 Chen, “Preliminary Thoughts about Strengthening Cyber News Media in Wartime.”

294 Chen, Fang, Yang, and Xia, “Social Media Warfare: A New Dimension to Warfare in the Information Age.”

Section 6
PLA Interest in a Twitter Account

PLA authors have been explicitly and publicly lobbying for the PLA to join Twitter since at least 2014, which is a natural extension of the PLA’s desire to shape the global narrative about China and the military. We found at least eight instances of PLA propagandists and researchers making detailed arguments for the necessity of this choice, but did not discover any public arguments against such a move. However, the fact that the PLA has not yet opened accounts on foreign social media suggests high-level resistance to this idea despite growing interest within the ranks. We predict that the ranks will eventually win out, and the PLA will join Twitter and perhaps other Western social media platforms, but the timing still is not clear. While the PLA’s interest in opening an official account on Western social media on the surface would appear to fall under the legitimate and acceptable category of influence operations that are transparent public diplomacy as proposed by the Hoover report, there are national security considerations at play. Direct PLA control over Western social media accounts likely would enable the PLA to gather more analytic data on individual users that could be used for future political interference operations, for example, improved targeting of tailored messages.

An official PLA account on Twitter would further all of the military’s objectives on social media. Most obviously, this would help the PLA towards its goal of narrative dominance by enabling it to directly inject military propaganda into foreign countries. Second, it would enable the related goal of psychological warfare for deterrence by enabling broader reach of its messaging to target audiences to undermine enemy resolve. Third, while the PLA is very unlikely to engage in hostile influence operations from its own official accounts, it would be able to directly collect data on foreign engagement with its messaging, and potentially improve its targeting using other covert accounts in the future.

Among the arguments for opening accounts on Twitter, Facebook, YouTube, and Instagram that are made by PLA authors include having direct access to its intended audiences, avoiding misinterpretation by Western media, being able to respond to negative stories abroad, and generally monitoring foreign discussions about the PLA. As early as 2014, it was suggested that the PLA should use social media for external propaganda, and should get accounts on Facebook, Twitter, Instagram, and YouTube. This early article maintained that the PLA should use official and unofficial accounts on social media, customize content, and adopt local vocabulary to blend in as part of “information stealth dissemination.”

An editor from the PLA Daily’s online communications center argued in 2015 that the PLA should open Western social media accounts to target foreign audiences. The author ar-

296 Liu and Xu, “Social, Mobile and Publication of Military External Propaganda.”
297 Chen, “Create a Shock Team for Military External Propaganda.”
gued that it is hard to attract visitors to the PLA’s website, but if it created Western social media accounts instead, it could target audiences with tailored content and draw them back to China Military Online with hyperlinks. He added that the PLA can use Western social media to correct misperceptions and broadcast positive propaganda.298

Similar calls for joining Facebook, Twitter, and YouTube were made in 2016.299 In early 2017, a professor at the Nanjing Political Institute argued that the PLA should “explore” getting Twitter, Facebook, and other accounts in order to “directly influence overseas audiences and international public opinion,” and that PLA schools should lead this effort.300 In late 2017 at a forum discussing the implications of the 19th Party Congress for PLA propaganda, Chen Tong, formerly a co-president of Phoenix Media and a vice president at Chinese smartphone maker Xiaomi, asked, “I wonder if it’s possible for us or other civilian forces to open accounts on English language social media on a large scale, such as Twitter, YouTube and Facebook.”301 Some of these authors exhibited narrow parochial interests, as when the PLA professor argued military schools should lead the charge, and a Xinhua author pointed out that Xinhua already was well-placed to help.

Other PLA authors have been inspired by U.S. President Donald Trump’s popularity on Twitter. In 2018, a PLA graduate student referred to the United States to make the case:

For example, U.S. President Trump uses Twitter to post and through a constant presence he has gathered a huge fan base. Therefore, our military should also leverage foreign social media’s power […] and announce authoritative information on social media, utilize the advantages of online communication’s speed and large influence to expand our military’s influence in international media.302

The writer embraced newer platforms, such as streaming on Facebook Live, Twitter Periscope, or Google Connect, and argued that the PLA could reach foreign audiences through finding common ground and leveraging opinion leaders, although it still needed to improve targeting and reduce the propaganda flavor. Earlier in 2017, another source concluded that the 2016 U.S. election illustrated that social media was better than traditional media and so the PLA should use foreign media—not only Facebook, Twitter, and Instagram but also Russia’s VKontakte—and adapt to each different platform.303 Some authors indicated that they see extending the PLA’s propaganda reach on social media in terms of influence operations, or in their words, “public opinion warfare.”304

298 Chen, “Create a Shock Team for Military External Propaganda.”
300 Xiao, “Analysis on the Countermeasures to Strengthen the Construction of Our Military’s New Media Power.”
303 Li Yuqian, “New Media and Military External Propaganda,” 117.
304 Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda”; and Chen, “Create a Shock Team for Military External Propaganda.”
Other analysts believe that the PLA does not need its own accounts, but can better utilize its preexisting arrangements with Chinese state-run media to use their foreign accounts. One author pointed out that the PLA needs to use foreign social media accounts because Weibo does not attract foreigners. He added that since the Chinese media is not trusted by foreigners, the PLA also should use social media accounts owned by overseas Chinese students and overseas Chinese. However, he believed that the PLA could suffice with using others’ accounts, like China Daily on Facebook, and, in general, it should promote the good things China does to foreign audiences.

A military reporter at Xinhua stated that the PLA should “incorporate overseas social media that relates to the PLA’s broadcasts into the public opinion monitoring system,” to support responses to negative public opinion, even though he did not specifically argue for joining those platforms. He believed that the PLA “overlooks” foreign social media, especially since its direct broadcasting to an audience cannot be twisted by Western media, and notes that Twitter and Facebook are very popular, especially among youth. The author argues that the PLA “cannot avoid” the topic of joining foreign social media, which could be used to respond quickly to negative stories. His desire to monitor foreign social media was echoed by another author who wrote that the PLA does not yet do this, but that it should monitor foreign social media sites in order to respond and “help win momentum in our public opinion struggle on overseas social media.”

Citing the problem that articles published by non-authoritative news sources trending popular on Twitter, such as The Fiscal Times (as opposed to The Financial Times), are often critical of the PLA, the author cautioned that the PLA should “strengthen […] monitoring, control and early warning” for “explosive topics” and respond to specific negative tweets to set the record straight and spread the good news in part by weakening the propaganda flavor. Another author suggested that the PLA join foreign social media in emphasizing the value of directly communicating with its audience. He argued that the PLA could expand its presence by sending PLA reporters to the United States and other countries and, in the meantime, could use PLA defense attachés or state media for this propaganda role.

The reason the PLA has yet to open a Twitter account appears to be the lack of high-level approval. Several authors mentioned that such approval was needed. This restriction on the PLA’s online presence dates back to limits on websites, reflecting deep-seated PLA skepticism of the Internet. However, there has been at least some bureaucratic support for this idea, as an officer from the MND’s International Communications Bureau argued at a PLA seminar on online public opinion in June 2013 that “for major military actions,” the PLA should “open temporary micro-blogs to disseminate information dynamically and in real time,” though it is unclear if he meant foreign accounts. More importantly, one would


306 Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda.”

307 Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda.”

308 Li, “How Does Chinese Military News ‘Go Out.’”

309 Chen, “Create a Shock Team for Military External Propaganda.”

310 Zhang, “21-Point Suggestion to Strengthen, Expand Military Networks, Websites.”

311 Liu, “Thinking Technologies and Mechanisms for Study of Online Public Opinion on Military Af-
think General Secretary Xi would approve because he told the PLA in December 2015, “Wherever the reader is, wherever the audience is, the propaganda reports should reach there,” and his 2018 book argued for “actively using overseas social media platforms.” This leads us to believe the PLA will eventually secure this necessary approval for accounts on foreign social media. Although Twitter is the most likely, interest in Facebook and YouTube is also quite apparent and could be useful for reaching different audiences.

PLA authors frequently point to the fact that other Chinese state-run media have accounts on foreign social media and that other militaries around the world already have embraced social media. Two articles point to the presence of the American, British, and Canadian militaries on social media and the fact that Xinhua first joined Twitter in 2015, followed by the People’s Daily, CCTV, and China Daily. These calls by the PLA propaganda system for its own Twitter account suggest the PLA does not trust Xinhua or other state-run media to accurately communicate its message. Indeed, this report has found a People’s Daily Online post on Twitter that wrongly claimed to “reveal” a DF-41 missile, perhaps providing evidence that civilians lack the nuance to conduct deterrence signaling in wartime.

Despite apparent PLA skepticism about outsourcing foreign social media to China’s civilian state-run media, it does at least provide some value for the PLA. Xinhua reportedly has 50 million followers on overseas social media, giving the Chinese government a broad reach that the PLA is unlikely to match anytime soon, even after joining these platforms. Xinhua also appears to have a public opinion monitoring center, which found that foreign social media platforms discuss the PLA’s reforms, anti-corruption campaign, budget, the South China Sea, and new equipment. The deputy of Xinhua revealed in late 2017 that it has a team dedicated to guiding PLA topics and has some data on public opinion.

For now, the PLA has accepted state-run media as conduits for military propaganda on Western social media, as evident in the PLA’s approach to promoting the International Army Games. In 2017, China Daily promoted China’s participation on Facebook, reaching nearly 1.2 million people, according to later analysis by PLA propagandists. In 2018, China’s participation was broadcast on 17 foreign social media platforms, including

---

312 Xi, “Xi Jinping: Wherever the Audience Is, Propaganda Reporting Should Extend There”; and Speeches on Xi Jinping’s Media Thought (2018 Version), People’s Press.


315 Zhang, “Actively Use Overseas Social Media to Participate in Military External Propaganda.”


YouTube and Twitter, by 116 journalists from 51 outlets organized by the Army’s Political Department.\textsuperscript{318} The 2018 audience exploded to 120 million people, including Chinese citizens, with 35 million comments on social media.

For now, there are no indications the PLA officially has joined Western social media. Moreover, the Taiwanese government has provided no details of specific accounts operated by the PLA. However, the PLA already has a de facto presence via state-run media, although this is not likely to satisfy the PLA’s growing desire to influence public opinion abroad. One looming question is how sensitive the PLA would be to criticism on foreign social media, since it would be unable to censor this “inaccurate” information like it does at home.

After an international tribunal ruled against Chinese claims in the South China Sea in July 2016, China decided to send its People’s Liberation Army Air Force (PLAAF) H-6K strategic bomber to fly over the disputed islands as a signal of its resolve to defend its territorial claims. The announcement of this flight was not made by China’s Ministry of Foreign Affairs (MFA) or MND, nor was it announced by the state-run media, or even military fan sites that often break military stories. Instead, the PLAAF posted a photo of the bomber flying over Scarborough Shoal on Weibo, and the photo was quickly reposted on Twitter by the State Council Information Office (SCIO).

This is only one example of the Chinese military increasingly turning to social media for deterrence purposes. The PLAAF has used social media to demonstrate its growing power to domestic audiences as part of its quest for narrative dominance at home, but it has also used social media for deterrence, demonstrating its capabilities and credibility as well as undermining enemy resolve using psychological warfare.

Based on the content, languages, and platforms used in its social media posts, the PLAAF so far has targeted at least Taiwan, the Philippines, Japan, and the United States.

**PLAAF’s Social Media Strategy**

The PLAAF opened its Weibo and WeChat accounts in November 2015. According to a speech given by PLAAF spokesperson Shen Jinke in December 2017 at the 2017 Military Weibo Summit, which celebrated the service’s Weibo account as one of the military’s best, the intent was to “improve [the service’s] real-time provision of information, broadcasting, influence and guidance.” Shen asserted that the “internet media era is an ‘information starved’ era,” so the military must “optimize the information supply and guide public opinion,” and that by mastering the release of information, the PLAAF can control the “discursive power,” or achieve narrative dominance. He

---


added that “in public opinion related to the military, information is power, information is a weapon, information is confidence, information is position, and information is guidance [of public opinion].” Shen argued three principles should guide social media strategy: 1) seizing discursive power by controlling the release of information and guiding public opinion through “positive energy,” namely promoting the Party line and not letting foreigners or netizens speak for the Chinese government; 2) operational security; and 3) promoting appealing content to help with agenda setting.

This follows traditional PLA strategy for public opinion guidance outlined above, and Shen noted that the PLAAF’s Weibo account has been the first to release information on important steps in the service’s modernization, such as J-20 training and bomber flights over Scarborough. The Scarborough post reached 19.2 million people, and another on younger service members reached 12.6 million people. The PLAAF account also reposts relevant coverage from CCTV and other TV channels, improving its “secondary broadcasting,” and sometimes reaching 10 million to even 18.6 million people. Another strategy has been to post scenic photos with PLAAF planes, which people then use as their screensaver, such as the widely circulated shot of a PLAAF bomber purportedly flying in front of Taiwan’s Jade Mountain. The PLAAF also memorializes pilots who die in the line of duty, presumably to promote a sense of sacrifice and patriotism.

There are two ways to interpret the PLAAF’s reliance on Weibo for its social media outreach. The PLAAF’s posts clearly intend to show the power and successful modernization of the PLA to a domestic audience, reflecting the PLA’s primary concern about promoting a positive image domestically of the military. The importance of cultivating public support is evident in an April 2018 post that said, “Whether you are a worker, a farmer, a science and technology worker, a cleaner, or a courier, the strength of the motherland needs your commitment! The strength of the army requires your support!”

Moreover, the PLAAF also wants to broadcast this support back to the general public, evident in a CCTV documentary that highlighted netizen support for its bombers. Yet the PLAAF’s use of Weibo also could be considered a weakness in its deterrence strategy. Some posts are clearly meant for deterrence purposes since they are targeting foreign audiences and cross-posted to Twitter by the SCIO, but the PLA’s restriction to Chinese social media severely limits the reach of its deterrence messages and ability to undermine adversary resolve.


The PLAAF has tried to bridge this gap by relying on state-run media to extend its reach overseas. Shen described a November 2017 video entitled “Chinese Air Force Flies into New Era” as an “external propaganda product,” which was first posted on Weibo. The four-minute video is about the implications of the 19th Party Congress for the PLAAF and has both Chinese and English subtitles, indicating its targeting includes a foreign audience. The video presents images of China’s newest planes and lists the PLAAF’s mission areas in English. However, it also reveals how unpolished the PLAAF’s external propaganda team remains, as it has no voiceover and contains heavily stilted Party rhetoric that is difficult to read. Reflecting its reliance on other state-run media, CGTN reposted the video on YouTube under the title, “PLA Air Force promotional video gone viral in China,” which garnered 275,000 views.

The PLAAF purposely has shifted its strategy for the bomber flights in recent years by more proactively releasing information and translating its message into foreign languages in service of deterrence. While previously the PLAAF often would wait to release flight details until after they were reported by the Japanese government, since circa 2017 the PLAAF has released the information first via Weibo. This led one commentator to remark that the service now has adopted an “active” approach to better sway public opinion. The PLAAF also has begun sharing promotional videos, mainly touting its bomber flights, but even including a short cartoon that was clearly meant for children. Some of these videos have been recirculated by state-run media on Twitter.

Mirroring other PLA analysts about the importance of translation, the PLAAF has dubbed these videos and provided other information in Cantonese, English, Japanese, and Southern Min (Taiwanese). These languages align


well with the obvious targets for the PLAAF’s deterrence purposes. One PLAAF Weibo post explained translating materials “allows the people of all nationalities across the country and the compatriots in Taiwan and overseas to understand and see more clearly” that “every inch of territory of our great motherland cannot and absolutely must not be separated from China.”

The one surprising language was Cantonese, but a December 2018 Military Correspondent article explained that it was intended to demonstrate China’s “power and prosperity” to Hong Kong and the broader Chinese diaspora around the world. This article included detailed demographic information about the use of the Southern Min dialect in Taiwan and argued that using local dialects and languages is much more effective in reaching people to bridge domestic and international cultural gaps. This clearly demonstrates an evolving desire and effort to reach foreign audiences, and a tangible step toward tailored messages for different targeted audiences. The question remains: how effective are these efforts?

The PLAAF account also reveals that not all PLA social media posts are part of an elaborately orchestrated behind-the-scenes propaganda campaign. An April 2018 PLAAF Weibo post of a propaganda video dubbed in English of a H-6K flight around Taiwan prompted a response by China Military Online’s Weibo account for an original copy of the video so it could be posted to the English-language China Military Online. Later that month, after another flight around Taiwan, the PLAAF Weibo account proactively tagged other military media-run and state media-run Weibo accounts, likely in an attempt to get them to repost the video and reach a broader audience. This public coordination of PLAAF social media has not been observed since, so it is unclear if a coordination mechanism actually was created.

**Flights for Signaling China’s Capabilities and Credibility**

The 2016 Scarborough Shoal flight is a good example of how the PLAAF uses social media to demonstrate its capabilities and credibility for deterrence. The photo of the H-6K bomber over Scarborough demonstrated China had the capability and intent to defend its territorial claim in the South China Sea.

---

332 “The People’s Air Force Rounded off the Motherland’s Island Memorial and the Promotional Film Released in Fujian” [“人民空军绕飞祖国宝岛纪念封及宣传片在福建发布”], People’s Liberation Army Air Force [中国人民解放军空军 (空军发布)], Weibo [微博], April 23, 2018, https://m.weibo.cn/status/4231887629616281; “The People’s Air Force Rounded off the Motherland’s Island Memorial and the Promotional Film Released in Fujian” [“人民空军绕飞祖国宝岛纪念封及宣传片在福建发布”], People’s Liberation Army Air Force [中国人民解放军空军 (空军发布)], Weibo [微博], April 28, 2018, https://m.weibo.cn/status/4233758188413527; and “Air Force Organizes Bidirectional Flight around the Island! Su-35 first Flight through the Strait!” [“空军组织航空兵双向绕飞台岛巡航！苏-35首飞巴士海峡！”]. People’s Liberation Army Air Force [中国人民解放军空军 (空军发布)], Weibo [微博], May 11, 2018, https://m.weibo.cn/status/4238484057813485.


335 “The People’s Air Force Flies around the Island of the Motherland!” People’s Liberation Army Air Force.

Indeed, in light of the Philippines’ poor maritime domain awareness (MDA), it is possible that they learned about the flight from social media, since the Philippine defense secretary could not confirm the flight even after it happened. Making China’s resolve clear, PLAAF spokesperson Shen Jinke said, “The PLA Air Force will firmly defend national sovereignty, security and maritime interests, safeguard regional peace and stability, and cope with various threats and challenges.” Such flights have continued sporadically since, and China increased pressure by landing a bomber on Woody Island in May 2018. State-run media quoted a Chinese defense analyst as saying, “After the Air Force’s bombers are able to be deployed on islands in the South China Sea, their operational range as well as China’s maritime defense parameters will be tremendously extended, adding to existing prowess to deter any plots to compromise China’s territorial integrity from the sea.”

Although the PLAAF has generally avoided explicit discussions of the flights’ value for deterrence, some articles have made this clear. A 2015 PLA Daily piece described the flights as showing “China’s conventional military deterrence capability,” and another argued that, “The existence of a bomber force with strategic implications imposes deterrence to the enemy; more importantly, it is a commitment to peace.” More recently, Wang Mingliang, a professor at the PLAAF Command College, explained how these flights are utilized as deterrence by China:

It is undeniable that this is also a special language for China’s security communication on the international stage. The information transmitted is that the PLAAF is determined to be able to maintain the sovereignty, unity, and territorial integrity of the country in a broader space. It also [says that China] has the resolve and capability to show the PLAAF’s legal existence in international public airspace. This helps maintain regional stability and peace.

341 Lin Yuan [林源], Yu Hongchun [余红春], Yan Guoyou [闫国有], Chi Yuguang [迟玉光], Bai Zhongbao [白仲宝], and Mou Xingguang [缪星光], “Bombers Take Action” [“轰炸机出动”], China Air Force [中国空军], no. 7 (2015): http://kj.81.cn/content/2015-08/18/content_6636892.htm.
Flights Around Taiwan for Undermining Enemy Resolve

The PLAAF’s use of social media to broadcast bomber flights around Taiwan is a prime example of the role of psychological warfare for deterrence purposes. As noted earlier, the *Science of Military Strategy* and other authoritative Chinese military books argue that psychological warfare can serve deterrence by undermining the enemy’s resolve. The most specific operational applications are psychological propaganda inducement, which “pressures and influences the ‘feelings and behaviors’ of both enemy and friendly populations to either weaken morale or enhance popular support”; and psychological influence, which “encourages a potential adversary to be cautious about joining a war or, ideally, to be opposed to fighting in a particular war” by using targeting narratives and finding common ground.\(^{343}\) Similar to the flights into the South China Sea, these bomber flights certainly support Chinese deterrence by communicating capabilities and resolve. However, they also serve a third purpose more focused on psychological warfare—undermining Taiwan’s resolve. Arguably, China’s flights in the South China Sea, close to Japan or toward Guam, could theoretically similarly seek to undermine enemy resolve, but the PLAAF has played up only the intimidation factor for its flights around Taiwan. For example, following an April 2018 flight circumnavigating Taiwan, the MND spokesperson referred to Taiwan as “China’s island,” and warned “Taiwan independence separatist activities are the biggest real threat to the peace and stability across the Strait, and damage the fundamental interests of our compatriots in Taiwan,...promoting ‘Taiwan independence’ is leading to nowhere....

We are willing to strive for the peaceful reunification with utmost sincerity and efforts.”\(^ {344}\) In addition, the PLAAF has been very active in reposting CCTV clips of PLA commentators analyzing the flights as warnings against Taiwanese moves toward independence.\(^ {345}\)

The PLAAF has done more than just talk about the flights. The service’s Weibo account released and frequently reposts several photos claiming to show H-6K bombers flying near Taiwan’s Jade Mountain, although the Taiwan MND denies they flew close enough for the photos and suggested that these were disinformation.\(^ {346}\) This also happens on social media, as “state-run China Central Television has aired footage of old military exercises to lend credence to a false report that the Chinese People’s Liberation Army Air Force conducted a live-fire exercise in waters off southwest China.”\(^ {347}\) According to one analysis of the bomber flights around Taiwan,

The photos send a message...to Taiwan’s citizens, to highlight the inability of their government to stop such flights.... Taiwanese media also reported on a possible effort by China

---

343 For more on the PLA’s systems confrontation approach to warfare, see Engstrom, *Systems Confrontation and System Destruction Warfare.*


to weaken Taiwan’s will through psychological warfare. When two H-6Ks entered Taiwan’s Air Defense Identification Zone (ADIZ) during the July 20 flight, the Chinese pilots said they and the Taiwanese were the ‘same people,’ an illustration of Chinese claims to Taiwan and a way to undermine enemy resolve by convincing Taiwanese not to declare independence. The Taiwanese government denied the incident. 348

A December 2018 Military Correspondent article examining the PLAAF’s social media strategy for flights around Taiwan added that they show China’s “resolve and strength” for opposing Taiwanese independence and served as a “strong warning” to those independence forces. 349

The PLA also has employed social media for broader influence operations to reinforce its pressure campaign against President Tsai Ing-wen. According to one report, “In the past year, Taiwanese media have extensively covered stories about the People’s Liberation Army (PLA) of China sending aircraft and ships to patrol Taiwan. These stories were sparked by social media accounts run by the Chinese military, which released pictures and videos about the PLA operation that were widely shared within Taiwan.” Part of China’s success is with the support, intentional or not, of some Taiwanese media: “Before long, seven 24-hour news channels were delivering breaking news about the Chinese operations every hour, using the photos and videos made by the PLA—but without having verified whether or not they were true.” Moreover, popular news websites dramatised the PLA’s military operations. For example, Apple Daily presented the operations as a hyper-real film, creating animations and composite photos in which the leaders of Taiwan and China confronted each other. This approach helped Apple Daily online attract a large number of page views.” 350

PLAAF messaging fits well with recent PLA rethinking of how to target the island for influence operations. A 2011 article argued that “the main objective is to win over the hearts of the military and the will of the people [so] the best tone is…confident, sincere, natural, frank, firm, and like an iron fist in a velvet glove.” 351 Similarly, in November 2013 the director of the Voice of the Taiwan Strait broadcasting station, which is run by the UFWD, maintained that social media can play a role by not only “improving upon the mono-voice communication model of traditional broadcasting but also [by giving] more participation options to the Taiwanese audience.” Furthermore, it “enables real-time, prompt, and interactive exchanges between the transmitting and the receiving ends, thus breaking the limits of time, space, and regions and better realizing simultaneous communication deep in to the island.” 352 This


352 Zhong Zhigang [钟志刚], “New Explorations on Military Propaganda toward Taiwan under the
comes with a recognition that Taiwan requires a unique influence operations strategy that includes positive messaging, informing civilians that the PLA does not target them, and focusing on common interests with Taiwanese troops and common territorial disputes in the East and South China Seas, all the while deterring Taiwanese separatists.

**Limited Reach to Foreign Audiences**

Analyzing the PLAAF’s efforts to use Western social media illustrates the PLA’s limited reach so far to foreign audiences. The SCIO tweet of the Scarborough Shoal flight in July 2016 only garnered twenty-two retweets and nine likes, not even a blip on Twitter.353 **People Daily**’s post on Twitter about the May 2018 landing on Woody Island generated 130 retweets, while a similar CGTN report posted on YouTube garnered 30,000 views. However, most relevant Twitter posts only have several thousand retweets.354 Others are even less successful. A SCIO report on the PLAAF posted on YouTube in October 2016 only received 145 views, and a CCTV report on a January 2018 MND press conference denouncing the “China Military Threat” received 387 views.355 Generic PLAAF propaganda may be more attractive, as its promotional video garnered 275,000 views.356 However, it would appear that PLA-related topics, as presented by Chinese propaganda outlets, garner little attraction, although reposts and videos produced by accounts not affiliated with the Chinese government promote the narrative further. This corroborates recent testimony to the U.S.-China Economic and Security Review Commission which found that “it would appear that for the most part, many Americans are not attracted to or convinced by Chinese government propaganda, particularly when its state-run origins are evident.”357 Thus, despite PLA intent to target propaganda to foreign audiences for its influence operations, it to date has failed to garner much interest, and it remains to be seen if the Chinese military will be able to successfully adapt its content for broader appeal. This further incentivizes the PLA to reduce the transparency about the Party origins of its messaging by outsourcing its messaging through coopting opinion leaders or even creating covert accounts.
Section 8
Taiwan is the Canary in the Coal Mine for Chinese Political Interference

The PLA’s offensive use of social media for hostile political interference operations is most evident in its efforts against Taiwan. China has long sought to subvert Taiwan’s political process and influence its society in the hopes of increasing public support for reunification, or at least prevent the Taiwanese government from declaring independence. Social media is only the newest vector for Chinese influence operations against Taiwan, and the Taiwanese government has accused China of using social media to interfere with the November 2018 elections. While the actual impact of China’s

---


360 Horton, “Specter of Meddling by Beijing Looms Over Taiwan’s Elections.”
purported interference is undetermined, this sets a precedent for Chinese political interference in other countries’ democratic elections.

The November 2018 Taiwan elections mark the first claims of direct PLA involvement in disinformation on social media for election interference. In early November before the elections, National Security Bureau Director-General Peng Sheng-chu told Taiwan’s Legislative Yuan that “Beijing and the PLA were behind a propaganda campaign to interfere with the nation’s democratic elections by creating disinformation and fake news targeting Taiwanese media outlets, radio and television programs and Web sites.” Then-Taiwanese Premier William Lai accused China of the “dissemination of disinformation through mass media and social media” as part of its broader election interference, comments reiterated by his successor, Su Tseng-chang in April 2019. The Taipei Times claimed that “China has been creating fake social media accounts to interfere with the Nov. 24 elections as practice for manipulating the 2020 elections to elect candidates favorable toward Beijing,” and that “China’s cyberwarfare specialists are familiar with social issues in Taiwan and inject divisive commentary into discussions on controversial topics in an attempt to create social strife.” To date, the Taiwanese government has not released any evidence to support its assertions, and the Chinese government has denied it.

The PLA appears to target its disinformation on popular social media platforms in Taiwan, especially PTT, a Reddit-like bulletin board. According to Taiwanese media, the PLA posts this disinformation on Chinese platforms like Weibo, Taiwanese platforms such as PTT, and foreign platforms such as LINE, Facebook, Twitter, and YouTube. Radio Free Asia similarly reported that “Chinese operatives are spreading disinformation through social media, including Weibo, Facebook, and YouTube, as well as targeting its mainstream print and broadcast media.” Targeting these platforms is rational, since Facebook (used by 75 percent of Taiwanese), LINE (73 percent), YouTube (73 percent), and PTT (29 percent) are the four most popular social media platforms in Taiwan, with WeChat not far behind (24 percent). PTT appears to be the main platform to host and spread Chinese disinformation. PTT was the source of a fake story about China evacuating Taiwanese citizens from the Osaka airport during a typhoon that

361 Chung and Hetherington, “China Targets Polls with Fake Accounts.”
363 Chung and Hetherington, “China Targets Polls with Fake Accounts.”
364 Horton, “Specter of Meddling by Beijing Looms Over Taiwan’s Elections.”
led to the suicide of a Taiwanese diplomat.\footnote{368 Lee Hsin-fang and William Hetherington, “Chinese Kansai Evacuation Story ‘Fake News’: DPP,” \textit{Taipei Times}, September 9, 2018, http://www.taipeitimes.com/News/taiwan/archives/2018/09/09/2003700087.} PTT also reported on a brief scandal in a key mayoral race in Kaohsiung in November 2018, where the leading DPP candidate was alleged to have cheated during an election debate.\footnote{369 J. Michael Cole, “That’s What ‘Fake News’ Looks Like and What it Does to Democracy,” \textit{Taiwan Sentinel}, November 12, 2018, https://sentinel.tw/fake-news-kaohsiung-democracy/.} China has been accused of spreading disinformation in both instances, but hard evidence so far is inconclusive. We only found one article referencing PTT and three articles referencing Line, perhaps suggesting the absence reflects the PLA’s efforts to maintain secrecy around its attack vectors.\footnote{370 For the articles referencing PTT, see 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”], \textit{Journal of News Research} [新闻研究], no. 21 (2017). For the article referencing LINE, see Wu and Mei, “Some Inspirations Drawn from the Application of Booming Social Media in Psychological Warfare,” 77–80; Sun Guangyong [孙广勇], “New Media: The Double Edged Sword in a Changing Southeast Asian Society” [“新媒体：东南亚社会转型的双刃剑”], \textit{Military Correspondent} [军事记者], no. 2 (2015): http://www.81.cn/jsjz/2015-02/15/content_6357230.htm; and Liu, Xiong, Wu, and Mei, “Several Thoughts on Promoting the Construction of Cognitive Domain Operations Equipment in the Whole Environment.”} Nevertheless, Chinese state-run media such as \textit{People’s Daily Online} and \textit{Global Times}, have mentioned PTT and the larger landscape of Taiwanese social media.\footnote{371 Drun, “Taiwan’s Social Media Landscape: Ripe for Election Interference?”} This gap can be explained by the high-level coordination in the Central Cyberspace Affairs Commission that can transfer this knowledge to other CCP organizations, such as the UFWD, that likely better understand Taiwan society.

The PLA does not appear to produce this content itself but recycle content from state-run media, and few details have been released about this coordination mechanism.\footnote{372 For an article about how the Chinese state-run media interacts with and supports suspected Chinese-manufactured disinformation in Taiwan, see Nick Aspinwall, “Taiwan: The Frontline of the Disinformation Wars,” \textit{Diplomat}, November 1, 2018, https://thediplomat.com/2018/10/taiwan-the-frontline-of-the-disinformation-wars/.} The content is usually drawn from existing “fake news” created by Taiwan-focused state-run media, such as \textit{Straits Today} and \textit{Taihai Net}, as well as the more well-known \textit{Global Times}. The \textit{Taipei Times’} source added,

There are a growing number of Chinese accounts aimed at Taiwan on YouTube, such as Jianghu Baixiaosheng (江湖百晓生) and Touhao Zhanjiang (頭號戰將), which both have nearly 30,000 Taiwanese followers.…These accounts have each published nearly 1,000 videos in the six months they have been active, and the content is largely commentary critical of Tsai and U.S. President Donald Trump sourced from the \textit{Global Times}.\footnote{373 Chung and Hetherington, “China Targets Polls with Fake Accounts.”} Another report added that “China has now established its own version of a troll factory.” Taiwanese government sources told the media that China has created a “government agency charged with disseminating disinformation in Taiwan for the purposes of influencing public morale and causing rifts within society.” The source further described it as a “Chinese government task force responsible for destabili-
bilizing the Tsai administration by spreading disinformation on everyday issues through social media and other online platforms.” 375 Although it is not identified, the committee could be the Central Cyberspace Affairs Commission, which is the organization most likely responsible for the high-level planning and coordination of China’s hostile political interference campaigns.

Taiwanese officials assert that the PLA devoted massive resources against Taiwan. Legislator Wang Ding-yu, according to the Taipei Times, “said that China has set up its fifth military branch, a ‘cyberforce’ that has 100,000 staff, of which 30,000 are deployed as part of ‘cyber-army units’ that are specifically focused on launching attacks against computer and mobile networks, as well as gathering intelligence and spreading of disinformation to destabilize other countries.” This NDB source told the Times that,

China’s information warfare efforts are an evolution of a PLA unit [the SSF] that was established at the end of 2015 to conduct intelligence gathering, attacks on servers and networks, cognitive hacking and psychological warfare, the source said, adding that the branch today has an estimated 300,000 personnel. Taiwan has long been a testing ground for Chinese cyberattacks, and last year the bureau intercepted an average of 100,000 online attacks from China per month. 376

The identification of the SSF as the driving force behind the PLA’s social media warfare against Taiwan reaffirms our assumptions of the SSF’s role outlined above. Although Taiwanese statements are vague about how much of the SSF is actually focused on Taiwan, the number of personnel devoted to disinformation on social media is certainly much smaller. For comparison, Russia’s IRA, according to the February 2018 grand jury indictment, had 80 employees assigned to “information warfare” operations against the United States for the 2016 election and overall “employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The organization’s annual budget totaled the equivalent of millions of U.S. dollars.” 377

One PLA article provides insight into how the Chinese military may have prepared for interference against Taiwan. A 2017 article by a graduate student at the Nanjing Political Institute, by then under NDU as the Political Academy, created a playbook for others in the Chinese military to “localize” their “targeted communications” toward Taiwan on social media. 378 The author explains how to alter the sentence structure and vocabulary used by Mandarin speakers, the language of most of mainland China, to sound more like that of Southern Min, the language used in Taiwan, because he is from Fujian, where the local dialect is closest to Taiwanese. He specifically focuses the article on PTT, the only known reference by any PLA author, and justifies his playbook by saying that sounding local will reduce the emotional distance between the

376 Pan, “China Subverting Elections: Premier.”
378 Lai, “An Analysis of the Minnan Language Sentence Patterns and Vocabulary Used on Taiwanese Social Media.”
two sides, otherwise it is “very easy to spot and will attract the attention of other Internet users, forming an invisible wall in the online community.” He adds that “achieving a sense of belonging requires to a certain extent encouraging Taiwanese netizens to communicate with others in Southern Min, so that they can be integrated into some online communities with a strong localized [Taiwanese] atmosphere.” Although the article is framed as about propaganda toward Taiwan, the specificity of the linguistic instruction and the emphasis on fitting in suggest it could have been intended to facilitate covert interference on social media against Taiwan.

Taiwan serves as a useful case study to show that social media is only part of China’s larger information campaign, which itself is only one segment of China’s comprehensive influence operations. China is widely suspected of covertly influencing Taiwanese media coverage through Chinese-controlled media and pro-China but Taiwanese-owned media, including directing news coverage and editorials. This was confirmed by a senior official in Taiwan’s NSB in May 2019. Beijing also strives to define the bounds of Taiwan’s own narrative, focusing on the “1992 consensus” and “one China policy” as a way to constrain Taiwan. Beyond the information domain, China is widely suspected of many conventional forms of election interference, including working with Taiwanese gangs to coopt minor political parties and employing numerous carrots to sway voters all year round. As Kevin McCauley argued, “Beijing is ramping up a multifaceted influence campaign employing overt and covert measures. The goal is to keep President Tsai from moving towards a formal declaration of independence, turn public opinion against her government before key elections, and improve Taiwan public opinion towards China.” Disinformation on social media was an increasingly important part of this campaign, but should be considered as a part of the whole effort.

China reportedly used several tactics on social media against Taiwan. China clearly targeted support for President Tsai and her policies, including spreading disinformation that pension reform would be much more severe than announced. Most notably for the

---

379 Lai, “An Analysis of the Minnan Language Sentence Patterns and Vocabulary Used on Taiwanese Social Media.”


382 Kathrin Hille, “Taiwan China’s ‘Sharp Power’ Play in Taiwan,” Financial Times, November 21, 2018, https://www.ft.com/content/5c272b90-ec12-11e8-89c8-d36339d835c0.


384 “Is Han Kuo-yu Popular across the Strait? Townspeople: Han Kuo-yu Is Searched For a Lot in China” [“韓國瑜紅到對岸？ 鄉民：「韓國瑜」在中國搜尋熱度高”], Liberty Times [自由時報], November...
election, China and the PLA seemed to have been more active in supporting the KMT candidate, Han Kuo-yu, for the Kaohsiung mayoral race, traditionally a DPP bastion. As noted above, disinformation spread on PTT that the DPP candidate, Chen Chi-mai, had cheated by using an earpiece to receive answers for questions. Other investigations by Taiwanese media similarly alleged that Han’s support on PTT was artificially manufactured by Chinese users. A June 2019 Foreign Policy report further found that suspected Chinese operators created fake Facebook accounts to create a fan group for Han and generate real enthusiasm against Taiwanese voters about his candidacy. Moreover, users in this group were accused of spreading fake news that ended up on LINE. The report traced the fake users to a further group of 249 fake LinkedIn accounts, which is known to be used by Chinese intelligence, that used Chinese language characters, a tell-tale sign of not being Taiwanese. The report did not definitely identify the specific Chinese organization responsible, suggesting that it could either be the SSF or could be private contractors supporting either Chinese intelligence or the military, and also identified the Propaganda Department as likely running other fake accounts. Regardless, the Foreign Policy report is the most specific research to date on pinpointing specific behavior on foreign social media attributed to China. A July 2019 report on China’s influence operations targeted at Taiwanese youth on social media argued, “China uses metadata, artificial intelligence and other technologies to analyze what content young Taiwanese consume and exploit the information to cultivate sympathy for Beijing.” The report added, “China’s short-term strategy is to mount an interference campaign targeting next year’s presidential election, while its long-term aim is to divide Taiwanese society to facilitate its ultimate goal of annexation.”

China likely will seek to improve its strategy before the 2020 Taiwan elections, and some believe changes already are underway. In July 2019, Han Kuo-yu became the KMT’s nominee for Taiwan’s presidential election, likely benefiting from China’s influence amongst traditional Taiwanese media. As the main contender against Tsai, Beijing will have an even greater incentive to boost his candidacy than during his mayoral race in 2018. Some Taiwanese analysts believe Chinese disinformation is easy to identify because it is written in the simplified characters of China, instead of in the traditional characters, which are used in Taiwan. According to one analysis,

[a] Taiwanese scholar purported that China’s Internet army has started a ‘localization’ [bentu hua, 本土化] cam-

---


386 Huang, “Chinese Cyber-Operatives Boosted Taiwan’s Insurgent Candidate.”


389 Tu and Chin, “Beijing Using Emergent Media to Attract Youth.”

390 Hille, “Taiwan Primaries Highlight Fears over China’s Political Influence.”
campaign, converting text on accounts and messages from simplified Chinese to traditional and imitating local Taiwan ways of speech. The same scholar also noticed a strategy focused on swaying swing voters, targeting pan-green pages to weaken perceptions of support, and adding Taiwanese friends and posting positive articles about the pan-blue camp, among others.391

However, questions remain over how effective China really was via social media, especially compared to more established traditional methods of Chinese interference, and whether Taiwan will be able to improve its defenses against Chinese disinformation before 2020.392 President Tsai vowed before the election that “Whether it be disseminating disinformation, ... intervening in the election process, or interfering with government operations, if there is irrefutable evidence of crime, the perpetrators will suffer serious consequences.” She called for international cooperation to combat “systematic dissemination of disinformation from specific countries,” including “not only experience sharing, but also setting up monitoring and notification mechanisms.” The goal would be to “respond to any damage or negative impact that disinformation has on social stability in various countries.”393

Such cooperation will be increasingly important if, moving forward, China continues its hostile political interference. Assistant Secretary of Defense for Asian and Pacific Security Affairs Randall Schriver stated in June 2019 that the United States indeed would assist Taiwan in responding to Chinese interference in its upcoming 2020 presidential election, without providing details.394 He stated that “There’s no question in our minds that China will try to meddle, as it has done in every previous election,” and specifically commented, “The sophistication on the PRC is growing, so what we expect this time is use of social media, cyber intrusions.”395

391 Drun, “Taiwan’s Social Media Landscape: Ripe for Election Interference?”


Section 9
Indications of PLA Interest in U.S. Elections

Despite the immense attention on Russia’s efforts to interfere with the 2016 U.S. presidential election and the likelihood of similar interference in 2020, there may be another threat that is being overlooked—China. Indications emerged in the summer of 2018 that the PLA was interested in hostile political interference operations against the United States, although there is no evidence so far that any actions have been taken. We believe that Taiwan’s experience demonstrates China has the capability and interest for interfering in foreign elections, warranting heightened vigilance for other countries, including the United States.

Accusations and Warnings of Election Interference but Only Evidence of Influence

The Trump administration already has accused China of interfering with U.S. elections, but no evidence has been released, and there are no indications this has extended to social media.\(^{396}\) In September 2018, President Trump claimed the Chinese government was interfering in the 2018 midterm elections, apparently based on Chinese state-run media paid advertisements in newspapers.\(^{397}\) These claims were furthered by others in the administration, most prominently Vice President Pence. Pence said in an October 2018 speech outlining the administration’s China policy,

Beijing is employing a whole-of-government approach to advance its influence and benefit its interests. It’s employing this power in more proactive and coercive ways to interfere in the domestic policies and politics of the United States…. China has initiated an unprecedented effort to influence American public opinion, the 2018 elections, and the environment leading into the 2020 presidential elections.\(^{398}\)

However, then-Secretary of Homeland Security Kirstjen Nielsen denied that there was any evidence to specifically suggest that


China was “attempting to undermine or alter the outcome of the 2018 midterm elections,” and the Chinese Foreign Minister denied it.\footnote{Joseph Marks, “DHS Secretary: No Sign China’s Trying to Hack Midterm Vote,” NextGov, October 2, 2018, https://www.nextgov.com/cybersecurity/2018/10/dhs-secretary-no-sign-chinas-trying-undermine-midterm-vote/151727/; For Chinese denial, see “Wang Yi: China Adheres to Non-interference in Other’s Internal Affairs and Other Countries Should Not Interfere in Other Countries’ Internal Affairs,” Ministry of Foreign Affairs of the People’s Republic of China, News, September 27, 2018, https://www.fmprc.gov.cn/mfa_eng/wjwb_663304/wjzb_663340/bmdyzs_664814/xwlb_664816/t1600130.shtml.} Therefore, if China were to use social media to influence or interfere with the 2020 U.S. elections, it apparently will be the first time.

China’s current efforts against the U.S. political process are better understood as part of Beijing’s broader influence efforts instead of direct election interference. According to Rush Doshi and Robert Williams, “China has long pursued a wide-ranging and very real campaign to influence the political and informational environment of other countries, including the United States,” but “these efforts by China differ in breadth, ambition and brazenness from those undertaken by Moscow in 2016.”\footnote{Rush Doshi and Robert D. Williams, “Is China Interfering in American Politics?” Lawfare, October 1, 2018, https://www.lawfareblog.com/china-interfering-american-politics.} Abigail Grace similarly has argued that “Chinese interference is played with the long game in mind” and different from Russia, because China focuses on “policy, rather than elections” with “highly targeted, diffuse, and scoped efforts to sway individual Americans who the Chinese perceive have sufficient influence to shape U.S. policy.”\footnote{Abigail Grace, “China’s Influence Operations Are Pinpointing America’s Weaknesses,” Foreign Policy, October 4, 2018, https://foreign-policy.com/2018/10/04/chinas-influence-operations-are-pinpointing-americas-weaknesses/.}

and Williams argue “China’s efforts in the United States appear less mature and flagrant than they are in Australia or Taiwan.”

While accepting the conclusions of Doshi, Williams, and Grace as generally accurate, we raise the question of whether or not Chinese efforts will advance to more active election interference in 2020.

There is concern that China can use its experience in Taiwan to improve its capabilities against other countries, including the United States. Shortly after Taiwan’s election, Yi-Suo Tzeng, acting director of the Cyber Warfare and Information Security division at the Taiwanese Ministry of National Defense’s Institute for National Defense and Security Research (INDSR) told Nikkei Asian Review that, “As they [China] accumulate knowledge and test their algorithms, I think within two years we will probably see China having the capability to use cybertools to intervene in the U.S. election.” Similarly, Jessica Drun has argued that, Chinese disinformation campaigns against Taiwan could be used as a blueprint against other democracies, particularly in sowing greater discord between segments of the population.... While any attempt against the United States would likely require a greater degree of sophistication, China has demonstrated a familiarity with popular Western social media networks, as well as an awareness of existing vulnerabilities within these systems.

Several U.S. senators have written to the Trump administration to ask it to investigate Chinese interference in Taiwan, and “if necessary, take swift action to deter future CCP interference in elections in Taiwan or elsewhere across the globe.”

Recent U.S. intelligence community statements warn of the growing Chinese threat to democratic institutions and provide more credibility to Taiwan’s assertions of Chinese political interference. The 2017 National Security Strategy (NSS) labeled China a “revisionist” actor that wants “to shape a world antithetical to U.S. values and interests” and asserted that “rival actors use propaganda and other means to try to discredit democracy. They advance anti-Western views and spread false information to create divisions among ourselves, our allies, and our partners.”

Former Director of National Intelligence (DNI) Daniel Coats has been the most outspoken about foreign threats to the U.S. democratic process. In January 2019, Coats for the first time testified to Congress that actors other than Russia could target the 2020 U.S. elections, asserting that “U.S. adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine U.S. alliances and partnerships, and shape policy outcomes.

405 Doshi and Williams, “Is China Interfering in American Politics?”
407 Horton, “China Uses Taiwan as R&D Lab to Disrupt Democracies.”
in the United States and elsewhere.” He warned that China “is improving its cyber-attack capabilities and altering information online, shaping Chinese views and potentially the views of U.S. citizens,...expanding its ability to shape information and discourse relating to China abroad,...[and] also capable of using cyber-attacks against systems in the United States to censor or suppress viewpoints it deems politically sensitive.”

Coats did not provide specific information on China’s activities, but it is clear that he assesses Beijing as a risk. He also hinted at China and others learning from Russia’s election interference: “Adversaries and strategic competitors refine their capabilities and add new tactics as they learn from each other’s experiences.” Former U.S. intelligence officials agree it is a concern, though evidence so far is absent.

Other U.S. government and allied officials have made similar statements. Assistant Secretary Schriver framed China’s approach to gray zone warfare as “coercive and aggressive in nature, deliberately designed to remain below the threshold of conventional military conflict.” Schriver asserted that China’s “gray zone activities include coordination of multiple tools, including political warfare, disinformation,...cooption, subversion and economic leverage.” These appear to be the first senior U.S. government officials’ explicit accusations of Chinese use of disinformation, and in June 2019 he said he expected China to interfere with Taiwan’s election on social media, providing more emphasis on China’s threat.

Similar statements have been made by the Australian Security Intelligence Organisation (ASIO), which warned in September 2018, “We have identified foreign powers clandestinely seeking to shape the opinions of members of the Australian public, media organisations and government officials to advance their country’s own political objectives,” and reportedly by late 2017 had found a “deliberate strategy by Beijing to wield influence through Australian politics.”

Echoing these government comments, a June 2019 report by the cybersecurity firm FireEye found that “Chinese groups have been targeting and monitoring elections in neighboring countries more closely than before, suggesting a more active effort to protect Chinese investments overseas, especially as the country seeks to expand its global influence.”

Recent research confirms that China is indeed interested in monitoring and influencing the U.S. political process, but not yet via social media. A July 2019 Microsoft report found that China was engaged in hacking U.S. polit-

410 Coats, “Worldwide Threat Assessment of the U.S. Intelligence Community.”

411 Coats, “Worldwide Threat Assessment of the U.S. Intelligence Community.”


413 Randall Schriver, “China’s Expanding Strategic Ambitions” (speech at George Washington University, Elliott School of International Affairs, February 7, 2019), https://www.youtube.com/watch?v=64aeoHqwxzw.


ical campaigns, but not at the scale of Russia, Iran, and North Korea. A May 2019 report on how Chinese state-run media engages on Instagram found that “Chinese influence accounts used paid advertisements to target American users with political or nationally important messages and distorted general news about China.” This aligns with a separate February 2019 report that found “Chinese government-funded media outlets used paid advertising in English on Twitter and Facebook. The advertisements told American social media users that the tariffs are hurting the American economy and called on the United States to make some concessions,” and were quickly removed from Facebook for violating the platform’s new political advertising rules. The May 2019 report found such paid advertising was part of a larger campaign where “the Chinese state has employed a plethora of state-run media to exploit the openness of American democratic society in an effort to insert an intentionally distorted and biased narrative portraying a utopian view of the Chinese government and party.” Compared to Russia, just the two Chinese accounts studied generated roughly one-sixth as much influence as the known IRA-linked accounts, in part because “the top 20 Xinhua repliers are either broadcast or spam bots.” However, the report did not find evidence of “a large-scale campaign to influence American voters.”

### Indications of Chinese Interest

Although specific reports of direct Chinese manipulation on U.S. social media are rare, Chinese military analysts have taken a keen interest in Russia’s disinformation tactics against the United States on social media through RT, and in how Cambridge Analytica used covert social media accounts to target users for political influence. It is important to note that the Chinese articles are not definitive nor fully authoritative, but their publication in Military Correspondent and other PLA-run journals suggests that such topics are not taboo but of interest to the broader military and possibly could lay the groundwork for similar Chinese activities in the future. Overall, the PLA appears to be intentionally broadcasting that it understands the vulnerabilities of the U.S. political system, as the well-known propagandist Major General Luo Yuan said in December 2018, according to a news report, “the five cornerstones of the United States are its military, money, talent, voting system, and fear of adversaries […] Luo said that cuts in soybean

---


imports would hurt the states which voted for U.S. President Trump, such as Iowa.”

The only specific report of Chinese activity on U.S. social media is a March 2019 Buzzfeed report about Chinese trolls on Reddit. The journalists relay Reddit users’ suspicions that “Chinese government-sponsored users are engaging in a coordinated effort to spread propaganda and bury anti-China messages on Reddit,” based on their observations of “an increase in posts from newly created accounts that downvote anything critical of China, swarm threads to push pro-Communist Party views, or attack anyone criticizing the country.” However, Reddit denied any coordinated activity on the site and there was no consensus amongst Reddit users about whether the large-scale activity was accomplished via bots or human coordination, or whether these were outspoken Chinese individuals or government-directed propagandists. Other journalists have found a similar surge in pro-China accounts on Twitter around certain events, such as Marriott’s social media troubles in January 2018 and the arrest of Chinese Interpol President Meng Hongwei in April 2019, but have been equally unable to differentiate outspoken citizens vs. government-directed campaigns. A Chinese focus on Reddit would align closely with China’s alleged manipulation of PTT in Taiwan, but conclusive evidence is lacking. A review by Facebook and Twitter of social media activity during the November 2018 U.S. elections found no evidence of Chinese manipulation. One possible explanation would be the ‘organic’ mobilization of enthusiastic nationalistic netizens like those employed against President Tsai in January 2016.

The first positive and detailed PLA appraisal of Russia’s general disinformation campaign against the United States appeared in June 2018, although authoritative PLA analysts have so far avoided drawing explicit lessons from Russia’s disinformation campaign in the 2016 election. This is a change from articles written shortly after revelations about Russia’s interference in the election, which focused mostly on the cybersecurity risks, even though some articles did examine how disinformation spread within the United States. The authors of the June 2018 article asserted that


427 Sebenius, “Facebook, Twitter Can’t Find China Election Meddling Trump Claims.”

428 PLA analysts ignored the issue or simply focused on the downsides and cybersecurity implications. See Ma and Sun, “The Characteristics of Russian Public Opinion Propagation: Taking “Russt Today” TV Station as an Example.”

429 For example, see Chen Huihui 陈慧慧, “Commentary Analysis on ‘Artificial Intelligence Technology Manipulating the U.S. Election’ Research Report” [“人工智能技术操纵美国大选’研究报告的评述分析”], Information Security and Communications Privacy [信息安全与通信保密], no. 7 (2017).
Russia’s bots improved the effectiveness and lowered the costs of propaganda, and that RT spread disinformation on social media to confuse people.⁴³⁰ The article noted that RT targets “easily influenced people,” such as youths on YouTube. The article did not draw any lessons for China; however, such public acknowledgement of Russia’s effectiveness, coupled with the lack of warnings of consequences of U.S. retaliation, suggests some PLA thinkers are clearly monitoring Russian efforts.

A September 2018 article drew similarly explicit lessons from how RT exploits divisions in Western society to affect the audience’s judgment:

we can also fully exploit latent contradictions between different countries and the influence of the opposition factions within Western countries to prevent enemies banding together to form an anti-China battlefront, and emphasize the other side’s never-ending disputes and difficulty in achieving consensus contrasted against our unity to influence global audiences to acknowledge our public opinion prestige and power.⁴³¹

Another article by the same author several months later repeated these vulnerabilities to exploit within Western democracy but recommended that if China begins to lose the public opinion battle at a given moment, it should inject “conspiracy theories” into Western media via the Internet and think tanks. The author stated that China should “actively cultivate a group of media outlets and think tanks with small audiences that are ‘grey’ and peddle falsehoods, and establish a database of negative topics and conspiracy theories” to use against the adversary, with a special focus on targeting younger Western audiences’ distrust of mainstream media, politicians, and even values.⁴³² Although these articles are not by authoritative authors, in fact, the last author is a graduate student in the NDU’s public opinion warfare department, it is clear that the idea of Western society, including U.S. society, as ripe for influence operations with well-demonstrated vulnerabilities courtesy of Russia is pervasive within at least some institutions of the PLA.

Some in the PLA have drawn lessons from the use of social media for influencing the 2016 election. A September 2018 article in Military Correspondent by an NDU lecturer saw value in how Cambridge Analytica leveraged peoples’ data to influence their voting preferences: “[we] should draw insights from the ‘Cambridge Analytica’ incident,” where researchers “tricked” 50 million Facebook users to download an application and gathered data under false pretenses. The author argued that the PLA should learn from Cambridge Analytica’s ability to “exploit big data analysis, AI processes, bots and astroturfing, grasp the different personalities of voters and realize large-scale guidance of public opinion and changing their [political] orientation.”⁴³³ The

---

⁴³⁰ Ma and Sun, “The Characteristics of Russian Public Opinion Propagation: Taking “Russia Today” TV Station as an Example.”


author also emphasized the value of tailoring messages based on the beliefs, value systems, political orientation, and targeting of different countries, political parties, and cultural groups, among others. Similarly, a December 2016 article by a Nanjing Political Institute researcher found that U.S. political campaigns were using big data drawn from social media to tailor their communications to targeted voters, noting that more and more U.S. voters have engaged on social media involving elections since 2008. The article relayed U.S. research that found Facebook usage could influence voting and increase turnout. The article focused on Hillary Clinton’s use of social media, noting her campaign’s inclusion of Chinese-American figure skater Michele Kwan, but ignored the Trump campaign’s heavy use of Twitter. While none of these articles should be considered authoritative statements of PLA intentions, they are a stark admission written in clear terms that illustrate some in the PLA are interested in using social media and next-generation tools to influence voters in foreign countries.

Chinese military patents convey an interest in monitoring social media conversations about U.S. elections. A Chinese patent for monitoring social media discussion groups, filed by NUDT researchers in March 2017, explicitly raised the 2016 U.S. election and the two months leading up to it as an example event that would be worthy of monitoring, although it did not mention any specific social media platforms. A separate patent from December 2017 by another team of NUDT researchers focused on machine learning for sentiment analysis again mentioned the U.S. election as a test case for monitoring conversations, this time on Sina Weibo. Similarly, the PLA SSF Base 311 co-authored article on using AI for running a large-scale online bot campaign mentions that China should learn from a Western study of how U.S. public opinion forms during U.S. election campaigns. It may be mere coincidence that two separate Chinese military research groups filed patents on social media monitoring in 2017 that mention U.S. elections, and that an article on running a bot campaign by the PLA SSF organization likely responsible for election interference against Taiwan (Base 311) also mentioned the United States, since there is no evidence in the patents that such monitoring or analysis was ever actually conducted. However, the coincidence bears further scrutiny.

This interest extends beyond U.S. elections. A Nanjing Political Institute author studied the United Kingdom’s “Brexit” vote for the gender dynamics of political engagement


437 The other example given was the release of Apple’s iPhone 7. See Tong Yongzhi [童咏之] et al, “Topic Self-Adaption Microblog Sentiment Analysis Method Based on Transfer Learning” [“种基于迁移学习的话题自适应的微博情感分析方法”], Chinese Patent CN108021660A, December 4, 2017.


on social media. The October 2017 article specifically conducted textual analysis on a Facebook page that featured debate over the Brexit vote as a way to understand the political discussion. This was not a detailed study, as it only looked at seven posts, but it still reflected interest and understanding of where to find and how to track political conversations on Western social media.

**SSF Base 311 Writings on the United States’ Information Environment**

There are indications that the same unit likely responsible for China’s political interference against Taiwan, the SSF’s psychological warfare unit Base 311 (Unit 61716), now is researching the United States’ information environment. PLA authors have expressed concern over newfound challenges of broadcasting propaganda into the United States because of the U.S. Congress’ reaction to Russian interference in the 2016 election. Perhaps the most revealing is an article by a member of Base 311 about the negative effects of proposed U.S. legislation on counter-propaganda. The article revolves around the struggle for influencing public opinion and opines that while the United States is losing the battle, this newest U.S. legislation is an attempt by Washington to recover its advantage. Similarly, an NDU researcher suggested that a way to avoid being entrapped by the new regulations was to call it “communication” instead of “propaganda.” These articles provided detailed analysis of the bill in a way that went beyond the typical writings found in *Military Correspondent*. They focused on the impact on China and noted support for the U.S. Department of State’s Global Engagement Center counter-propaganda efforts in other countries. The fact that the PLA unit historically focused on targeting Taiwan is now writing about the U.S. information environment suggests the unit may be expanding its purview to target the United States as well.

---


441 Hu, “Decoding the U.S. ‘Murphy-Portman Counter-Propaganda Bill.’”

Beginning in 2019, other SSF researchers have specifically explored the role of social media in U.S. politics. A researcher from the SSF’s IEU Foreign Language Institute authored an in-depth February 2019 article on the psychological roots of American neo-populism, further reflecting SSF interest in U.S. politics. Another researcher from the same institute explored the role of social media in U.S. political polarization, finding Facebook and Twitter heightened polarization but called for further empirical research to understand the specific relationship. Of note, it addresses President Trump’s support on Facebook during the election and the “echo chamber effect” created by social media.

China Likely to Target Chinese Americans

We believe China is likely to first target Chinese Americans for any hostile influence operations, including political interference, against the United States. This is consistent with the experiences of other countries targeted by China, especially Australia.

One of the PLA’s main imperatives for specifically targeting Chinese Americans is their perceived ability to amplify CCP propaganda to the broader U.S. audience. A December 2013 article argued that the PLA should “connect with overseas compatriots,” defined as both Chinese nationals and ethnic Chinese with other citizenship, to “expand overseas military propaganda.” Citing the power of the Jewish community in the United States for Israel as a model for influencing national policy, the authors argued that “when engaging in public diplomacy in a country, they should be vigorously courted by the government of the motherland [China] so that they are able to play an active role in the areas of spurring the target country to ultimately change its diplomacy policies.” Specifically, overseas Chinese “can use their own modes to disseminate mainstream information from inside China to friends around them, subtly expand dissemination,…and explain China’s military culture of aversion to war and advocating peace.”

443 Zhang Wei [张伟], “The Role of Social Media in the Intensification of Contemporary American Political Polarization” (“社交媒体在当代美国政治极化加剧的作用”), Today’s Mass Media [今传媒], no. 6 (2019).


445 Zhang, “The Role of Social Media in the Intensification of Contemporary American Political Polarization.”


448 Wu and Liu, “The Revelations of Public Diplomacy to Raising the Dissemination Force of External Propaganda.”

Furthermore, PLA authors have discussed promoting Chinese-language media as a bridge for broadcasting Chinese propaganda to U.S. audiences.450 A 2012 article noted a Texas-based newspaper “has some influence in the overseas Chinese community” and has “energetically publicized and supported ethnic Chinese individuals participating in politics and running for public office such as mayor, state representative, city councilor, and district court justice.” The article stated that “one out of four ethnic minorities in the United States rely on media in their mother tongue to get information and express their feelings, and the influence of these media surpasses that of the media of the country in which they reside.” It argued that “overseas Chinese language media shoulder epochal missions in areas such as setting up ties between mainstream society and ethnic Chinese people and overseas Chinese.” Furthermore, the paper’s editor was quoted as saying “Publicizing Chinese culture to mainstream society...is one way to have a say in mainstream U.S. society.” Even more revealing of the author’s interest in targeting the United States is the fact that the article maintained that in 2006 the Chinese government hosted overseas Chinese-language media for a “training class,” and the newspaper “wrote an alternative version of the song ‘We are the Heirs of Communism’: We are the overseas news media, carrying forward the glorious traditions of our predecessors, viewing the world, loving China...”451 This would fit the broader PLA strategy of cultivating opinion leaders, but is a rare mention of U.S. targets.

Questions for Further Research

There are certainly many unanswered questions about China’s capabilities and intent. To date, China has targeted only Taiwan with a disinformation campaign on social media as part of its broader influence efforts, but Russia similarly began with its next-door neighbor, Ukraine, before it targeted the United States in 2016.452 There is little specific evidence of China seeking to sow social divisions with its disinformation campaign on anything like the scale that Russia did by targeting the U.S. African-American community, among others.453 This finding aligns with the common conception that China’s influence operations are more focused on long-term positive projects to improve China’s image and foreign behavior toward Beijing, while Russia seeks immediate results through divisive exploitation of social divisions. Yet, Taiwanese officials assert such intent is there, and Chinese military writings mention this tactic, so it is possible. For capabilities, Taiwan would clearly be a much easier target for several reasons than the United States or other countries. First, Taiwan’s language and culture are very similar to China’s, whereas Chinese operatives would have to bridge both linguist and cul-


tural barriers to target other countries (though machine translation could help the PLA solve this problem). Second, China has spent decades studying and already refining its influence operations against Taiwan on a large scale, whereas its more ambitious operations elsewhere are in a more nascent stage, which means that its messaging and targeting likely would be unrefined at first. In short, there are many challenges China will have to overcome, but none of this is to deny the potential threat of Chinese interference in U.S. and other political processes. Russian interference in the 2016 U.S. election accomplished many of its objectives, regardless of whether it actually impacted the outcome of the election.
Section 10
AI and Big Data Loom on the Horizon

Perhaps the next frontier for the PLA’s propaganda system lies in big data and AI. The Chinese government under General Secretary Xi has embraced AI and big data as a critical part of China’s economic growth and domestic social control programs. The PLA sees great opportunity for its own military capabilities, including the ability to improve its targeting and monitoring on social media. Articles in Military Correspondent mentioning big data rose from 7 in 2013 to 43 in 2017, and articles referencing AI rose from 1 in 2015 to 13 in 2017. Chinese state-run media already have capitalized on AI, as Xinhua created a video-editing tool that can automatically create a short news video based on its ability to “analyze and capture information” and “realizes data visualization, data-to-video transformation and video production automation.”

More famously, Xinhua has also created an AI-enabled digital news anchor. One Western research organization created an AI text generator that can “write authentic-sounding prose that could fool humans” so well it has not been released, suggesting this capability may be in reach for China down the road.

With growing capability for AI within China’s private sector, military, and media, generating synergies around next-generation disinformation such as deep fakes may quickly become part of the CCP’s hostile influence operations.

Big Data

PLA authors believe big data will provide a major improvement to public opinion monitoring, early warning, and targeting. This dates back to at least 2013, when one expert argued at a PLA conference on online public opinion that with 45 million military-related social media posts in the preceding six months, big data would enable “early warning” for public opinion crises. The Director of the Chinese

Institute for Cyberspace Studies said in late 2017 that the PLA can use AI and big data to improve public opinion detection, determination, and handling, especially for sensitive topics like the CMC leadership. While for a long time these interests appeared more theoretical than practical, the PLA has begun patenting ways to leverage big data to analyze social media. Indeed, recent writings on PLA propaganda embracing virtual reality (VR) suggest that not all topics are intended for immediate application, but the potential benefits of big data and AI surely will divert at least some resources towards these efforts. Furthermore, some of this research appears to be dominated by younger scholars, suggesting that another factor in the rate of adoption is the career progression of the next generation of PLA propagandists. This also could extend to PLA external propaganda and dovetails with the state-run media’s interest in AI for propaganda.

**Artificial Intelligence (AI)**

The same September 2018 *Military Correspondent* article that argued for influencing voters also hailed AI for subconscious manipulation. The author wrote that the PLA should “fully exploit AI technology to accurately recommend military information to broad media platforms, [and] for different audiences... make even more international audiences see our [PLA] reporting that they enjoy, thinking that they themselves chose the content.” Similarly, big data could be leveraged to “extract information consumption habits and cultural traits for different international audiences” and after “locking onto a target group, use targeted promotions and accurate advertising to make international audiences understand and support our [PLA] policies.”

**Deep Fakes**

Chinese military authors appear so far to have avoided explicit discussions of deep fake technology. This is certainly on the global...
horizon, however, as a December 2018 Foreign Affairs article explains, “Disinformation is an ancient art, of course, and one with a renewed relevance today. But as deep fake technology develops and spreads, the current disinformation wars may soon look like the propaganda equivalent of the era of swords and shields.”

The October 2018 SSF Base 311 article on the hardware requirements for cognitive domain operations did address the need for “voice information synthesis technology,” suggesting an interest in manipulating audio or video clips with revised speech, one form of deep fakes. Although it is difficult to determine how advanced the military’s technology is, Chinese tech giant Baidu has already created Deep Voice, which can clone voice audio in minutes, and under military-civil fusion could share this with the PLA. Any increase of discussion by PLA authors will be worthy of attention.


Liu, Xiong, Wu, and Mei, “Several Thoughts on Promoting the Construction of Cognitive Domain Operations Equipment in the Whole Environment.”


Increased Popularity of Chinese Social Media Platforms Abroad

Another positive trend for China is the advent of popular Chinese-controlled applications outside the country, such as TikTok’s popularity within the United States. While WeChat is used in foreign countries, its actual popularity is limited—only 10 percent of Americans are estimated to use it at least once a week. By comparison, TikTok was the most downloaded social media application in the United States for several months in late 2018 to early 2019, in part fueled by $1 billion in advertising spending. Although there have been no specific issues so far, TikTok’s privacy policy is lax; it has already been sued by the Federal Trade Commission for privacy violations, and the CCP’s heavy-handed approach to control of tech companies, even abroad, raises the possibility for the misuse of its data. At least one Chinese article claims TikTok has strategic cooperation agreements with local Chinese city governments to push their content and train their employees on how to use the platform.


472 Yang Jiao 杨姣, “The Role of Short Video in the Construction of Regional External Communication
The popularity of a Chinese social media platform abroad could potentially solve the PLA’s lack of presence on foreign platforms, since the target audience would come to them. Moreover, against the backdrop of a great desire for data, the opportunity for China to actually gather data from so many users is likely a dream come true, and many of these users are young, China’s favorite target demographic for propaganda. While a musical application may seem far removed from the PLA, Chinese military researchers have indeed followed and written on its propaganda value to China. Younger PLA propagandists increasingly realize the popularity of short videos online, and TikTok is the best example of this so far.\(^\text{473}\) Not everyone in the PLA is sold on TikTok, however, as one researcher wrote an article about how much he disliked TikTok and why he uninstalled it from his phone.\(^\text{474}\)

The benefits of Chinese-controlled platforms for political interference is already clear from Australia’s experience. Australian researchers found that in the run-up to the country’s May 2019 elections, WeChat “accounts aligned more closely with the Government in Beijing have a clear anti-Liberal (Government) story coming out of them,” but there was “little evidence of attacks on Bill Shorten and the Labor Party across their dataset.”\(^\text{475}\) Beyond broadly criticizing the government, journalists further found “Chinese-Australian voters are being targeted by a scare campaign” through a “series of political statements systematically distributed on WeChat which target Labor’s policies in a way that could influence critical marginal seats away from the scrutiny of the main campaign,” including disinformation.\(^\text{476}\) The power of WeChat, or any Chinese-controlled platform, is greatest when it is the main source of information, which it is in the case of 26 percent of Chinese Australians.\(^\text{477}\) The decision for Australian politicians to increase engagement with Chinese Australian voters via WeChat raises the possibility of self-censorship, whether intentional or subconscious, and also direct censorship by Beijing of foreign politicians.\(^\text{478}\)

---

\(^{473}\) Zhang Heyun [张贺云] and Wang Yiming [王一鸣], “TikTok Audience Identity Alienation and Communication Dilemma” [“抖音用户的身份认同异化与生产传播困境”], Youth Journalist [青年记者], no. 2 (2019); Yu Gentai [余亘泰], “Analysis of the Current Status of Short Video Communication Related to the Military from TikTok Short Videos” [“从抖音短视频探析涉军短视频传播现状”], Research on Transmission Competence [传播力研究], no. 8 (2019); and Hu Xujie [胡煦劼], “Military Propaganda Innovation Seen from TikTok Short Videos” [“从抖音短视频看军事宣传创新”], Military Correspondent [军事记者], August 22, 2018, http://www.81.cn/jsjz/2018-08/22/content_9260368.htm.

\(^{474}\) Meng Yuting [孟玉婷], “Why I Uninstalled the Short Video App: Take TikTok as an Example” [“我为什么卸载了短视频APP：以抖音为例”], Research on Transmission Competence [传播力研究], no. 23 (2018).


WeChat accounts in Australia published less news about China than those on other platforms.\textsuperscript{479} The further penetration of WeChat, or any other Chinese-controlled platform, into U.S. and other societies would improve China’s capabilities for manipulating the information environment on social media.

Section 11
Conclusion and Recommendations

The PLA’s embrace of social media is shaped by its view of warfare as increasingly driven by information operations and belief that its battlefield is nearly limitless. It seeks to further the military’s objectives of narrative dominance, deterrence, and political interference against foreign countries. The PLA’s employment of influence operations always will be in service of the military and Party’s larger strategic objectives in coordination with other military, diplomatic, and economic measures. Since China already believes it is in a cyber and information confrontation with other countries, the PLA’s influence operations should not be analyzed along the already-blurred continuum of peacetime versus wartime. China, including the PLA, always is engaged in a range of influence operations, ranging from constant overt propaganda to intensified actions with hostile influence operations, including spreading disinformation on social media. The most aggressive action is the targeted use of hostile interference operations during key political events, such as democratic elections. Taiwan’s experience of Chinese interference in its November 2018 election demonstrated China’s capabilities and should serve as a clarion call for greater vigilance by the United States, since Chinese military writings and patents suggest increased interest in the U.S. political process. There are not yet any indications of political interference, which means there is still time to prepare before the upcoming 2020 elections.

There are several “covert, coercive or corrupting” aspects of the PLA’s embrace of social media. First, the Chinese military seeks to wittingly or unwittingly coopt influential individual civilian users with a preexisting large audience to spread its propaganda and obfuscate the Party origins of the message. This violates the principle of transparency that would normally tolerate foreign propaganda as public diplomacy. Second, it uses social media as a way to target psychological warfare against foreign populations to undermine their resolve for deterrence purposes. Third, its efforts to undermine democratic elections through political interference means that allowing the PLA to open an official account on Twitter would likely enable the PLA to gather more analytic data on individual users that could be employed for future hostile operations on social media, such as improved targeting of tailored messages. This report has focused on Western social media platforms, but all of these concerns apply to Chinese-run platforms because they are already used across the world, including in the United States. WeChat played a small role in the 2016 U.S. election, and any Chinese political interference for 2020 is likely to start by targeting Chinese Americans on WeChat.

According to military writings and patents, the PLA seeks to improve its performance on domestic and foreign social media through improved targeting of specific audiences with tailored messaging for more effective influence operations, especially toward younger audiences. Although the PLA, along with the Chinese government, has often been behind
the curve on social media developments, it nonetheless has persisted and is advancing. Most attention is focused on Facebook and Twitter, but the PLA slowly is widening its focus to include other platforms popular with younger users such as Instagram. As China moves toward wider implementation of political interference, its core communication tenets—rapid response, agenda setting, and adaptive messaging while finding common ground—all align well with what is necessary for disinformation campaigns. AI, big data, and machine translation offer opportunities for major advancement in China’s capabilities on social media. Still, it remains to be seen if the PLA will be able to realize its vision and whether or not the offensive or defensive applications of the next-generation technology will succeed.

Recommendations

We offer three main recommendations for the U.S. policy community which are focused on preparation for possible Chinese interference in 2020, international cooperation to safeguard other democracies, and reconsidering the presence of Chinese state-run propaganda (media) on Western social media platforms.

1. The United States should begin to prepare for Chinese political interference in the 2020 elections. While Russia’s interference in the 2016 election generally surprised the U.S. government and analysts, the country now has an opportunity to protect against possible Chinese interference. Taiwan’s experience and the DNI’s warnings show that China is a credible threat and warrants increased attention for signs of a Chinese disinformation campaign on social media.

   a. Further research should be conducted to find evidence of covert Chinese accounts on Western social media. It may be possible to identify fake accounts like those that Russia established, although there are only a limited number of known Chinese examples.480

   b. Further research should be conducted on any possible cooperation between Russia and China on political interference against democratic societies.

2. The United States should cooperate with allies and partners to counter Chinese influence operations, especially the looming threat of greater Chinese political interference. While this report has focused on the PLA, China’s influence operations are launched across the whole government and responses similarly must engage all aspects of U.S. and allied resources and power.

   a. Beyond Taiwan, the United States should proactively engage with other democracies around the world that may be ripe targets for Chinese political interference. This includes

Australia, Canada, New Zealand and Singapore, among others. Any election interference against these countries would suggest China is escalating its global influence operations beyond Taiwan.

b. The Taiwanese government should release more information about Chinese interference in their 2018 and 2020 elections. This could follow the example of the U.S. House Intelligence Committee releasing Russian social media posts in November 2017 and the U.S. Senate Intelligence Committee’s reports on Russian disinformation in December 2018. Transparency is important for credible threat assessments and national awareness.

c. The United States should proactively engage Canada and Singapore, as they will hold elections before the United States and could be ripe targets for Chinese political interference. Any election interference against these countries would suggest China is escalating its global influence operations beyond Taiwan.

3. The United States, along with its allies and partners, should reconsider and constantly evaluate the presence of Chinese state-run media and other government-owned accounts on Western social media. Such access potentially provides critical data to support and improve PLA and broader Chinese government political interference in U.S. elections. We acknowledge these national security considerations should be weighed against the value of open communication between the two countries. However, since U.S. media organizations are in practice not able to have a presence on Chinese social media platforms, it is believed that, even if Xinhua and others are not blocked from Western social media on national security grounds, their continued operation should be conditioned on reciprocal access for U.S. media organizations on all Chinese social media platforms. If the PLA does join Western social media, the U.S. government should request reciprocal access to Weibo and WeChat for the U.S. military. Despite the fact that there are challenges to maintaining an independent presence on Chinese social media, as research has shown even foreign embassies are censored on Weibo,481 nevertheless, the presence of U.S. military accounts on Weibo and WeChat could reach the majority of the Chinese population and enable the U.S. military to tell the majority of the Chinese population and enable the U.S. military to tell its side of the story, and at least create reciprocity between the two countries.
