The JAMESTOWN FOUNDATION
Global Research & Analysis (https://jamestown.org/)

Search ..

CHINA BRIEF

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

Publication: China Brief Volume: 19 Issue: 16

By: Nathan Beauchamp-Mustafaga (https://jamestown.org/analyst/nathan-beauchamp-mustafaga/)

September 6, 2019 04:51 PM Age: 3 years

Introduction

As information becomes ever more central for Chinese warfighting, the People’s Liberation Army (PLA) is developing a new concept for psychological warfare in the information era called “cognitive domain operations” (认知域作战, *renzhiyuzuozhan*). **[1]** This next-generation evolution of psychological warfare seeks to use information to influence an adversary’s cognitive functions, spanning from peacetime public opinion to wartime decision-making. The concept is largely inspired by the U.S. military’s emphasis on the cognitive domain’s decisive role in modern warfare, and the belief among the leaders of the Chinese Communist Party (CCP) that the U.S. government has already used social media to foment political revolutions against authoritarian governments during events such as the Arab Spring. After several years of concerns over China’s vulnerabilities in the cognitive domain, the PLA is now developing offensive strategies and capabilities to influence adversary public opinion—as recently evidenced in its political interference in Taiwan’s November 2018 elections, and its summer 2019 disinformation campaign against Hong Kong protesters (China Brief (https://jamestown.org/?post_type=program&p=83770&preview=true), September 6).

Overview of Cognitive Domain Operations

Broadly speaking, cognitive domain operations fall under the rubric of psychological warfare, which is

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

itself a part of the PLA's concept of information operations. China already has a wide range of concepts that relate to Western definitions of influence operations, to include: the "three warfares" (三战, *sanzhan*), consisting of psychological warfare (心理战, *xinlizhan*], public opinion warfare (舆论战, *yulunzhan*], and legal warfare (法律战, *faluzhan*); political warfare (政治战, *zhengzhizhan*); and external propaganda (对外宣传, *duiwai xuanchuan*). **[2]** The PLA is very likely in the early stages of its development of this new capability, based on relatively inconsistent terminology and the PLA's writings on its own perceived shortcomings. What began as fundamentally a wartime concept focused on impacting the adversary's military decision-making process now extends to peacetime operations against entire societies—enabled by the wide reach of modern information technology, and especially social media.

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

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

Three Phases of PLA Research on Cognitive Domain Operations

Like many developments in the PLA, cognitive domain operations find their roots in U.S. military operations and doctrine. **[7]** The 2001 Department of Defense report to Congress on "network centric warfare" first introduced the concept of the cognitive domain to go along with the physical and information domains. **[8]** *Information Warfare* (Joint Publication 13-3, released in 2006) further explained that the United States would seek to target the cognitive domain through psychological operations to "influence" adversaries, and further employ military deception to "mislead" them. **[9]** More recently, the U.S. military's "multi-domain operations" explicitly seek to gain the advantage in the cognitive domain. **[10]** In 2005, early PLA writings conceptualizing the first phase of "operations in the cognitive domain" largely focused on decision-makers' cognitive process and ability in wartime, and did not consider the internet the most significant vector. **[11]**

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

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

A Framework for Cognitive Domain Operations

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

<u>Cognitive influence technologies</u>:

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

<u>Subliminal cognitive influence technologies:</u>

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

messaging.

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

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

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

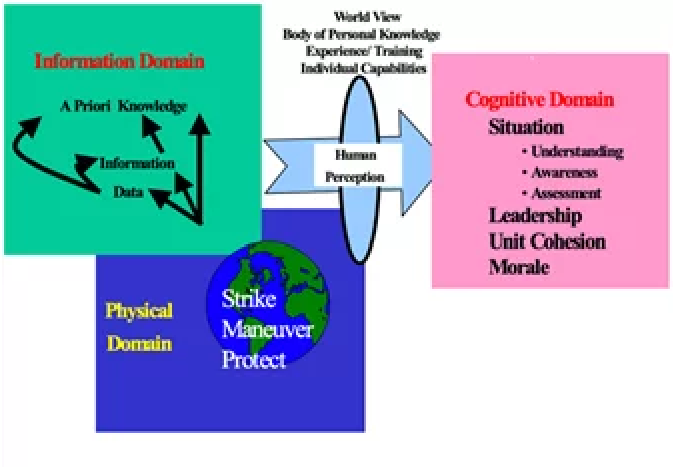


Figure 3-2. Domains of Warfare

Image: Initial U.S. Conception of Cognitive Domain in Warfare. (Source: Department of Defense report to Congress (http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf), July 27, 2001.)

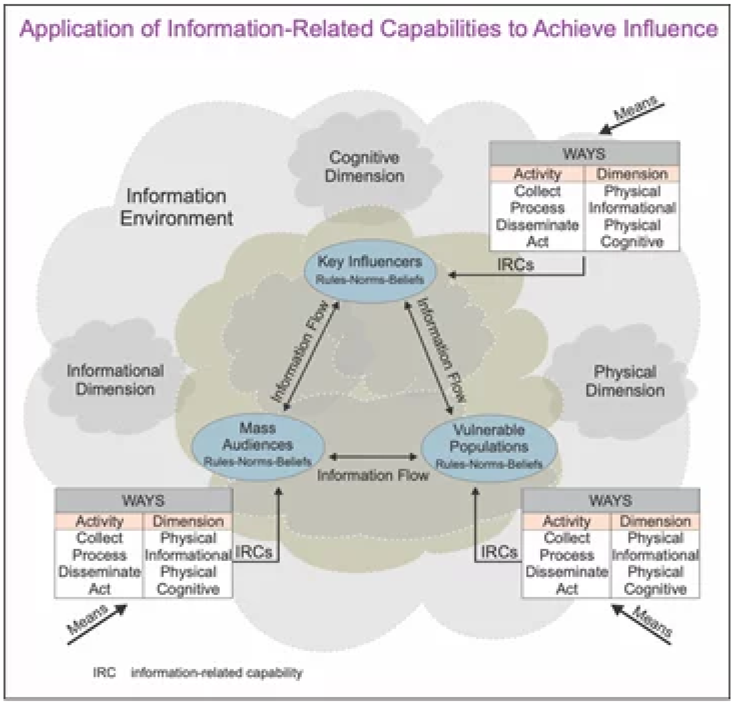


Image: Recent U.S. Conception of the Role of the Cognitive Domain in Influence Operations. (Source: Joint Chiefs of Staff (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf), November 2012.)

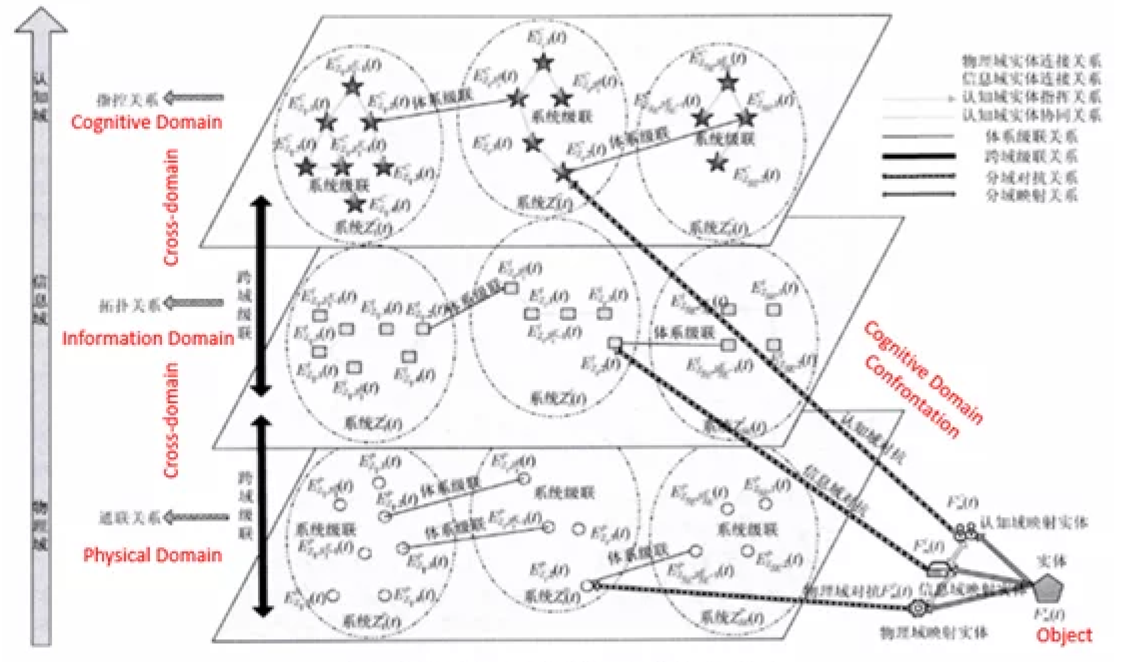


图 6 基于"机理+表现"的网络空间作战效果模型

Fig. 6 Cyberspace operation effect model based on "mechanism + performance"

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

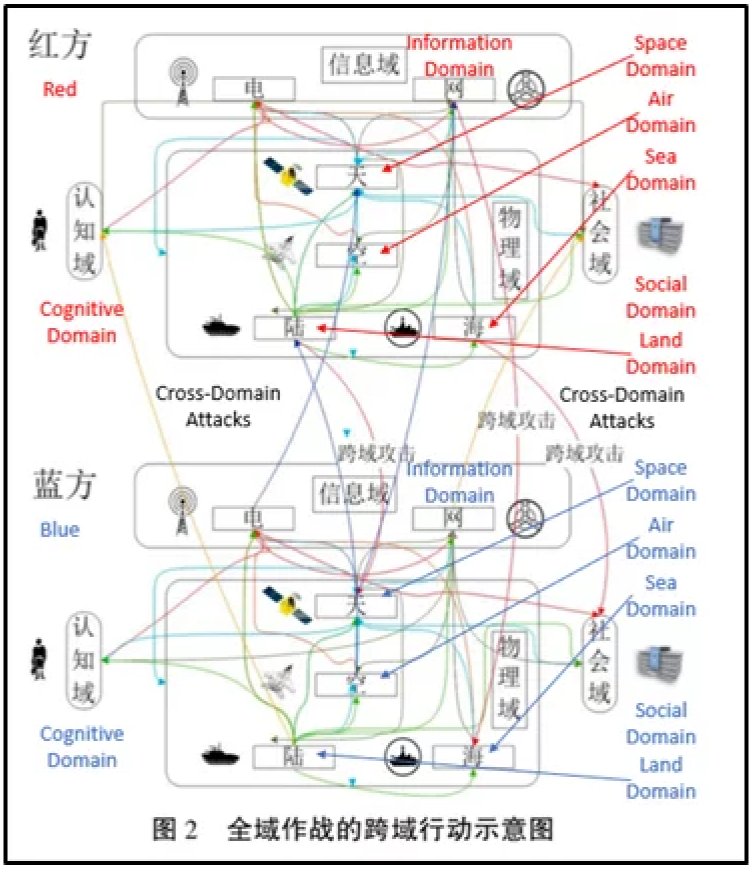


Image: Chinese Conception of Cognitive Domain Links to Other Domains. (Source: *Military Operations Research and Systems Engineering*, [军事运筹与系统工程], January 2018.)

Applications of Cognitive Domain Operations

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

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

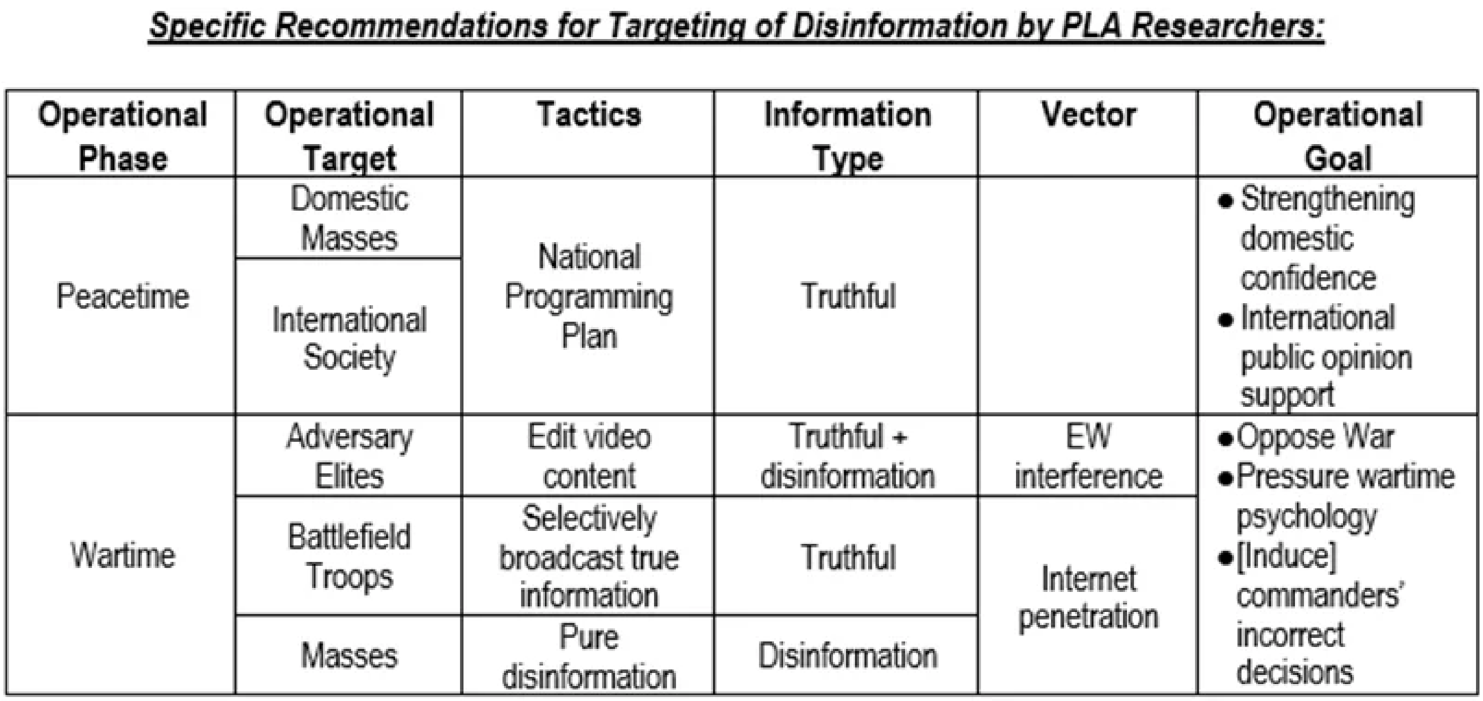
The PLA has also begun patenting technologies dealing with the cognitive domain since at least 2018, again reinforcing the real-world application of this concept. **[27]** These examples clearly indicate the PLA is developing specialized technologies and training personnel to manipulate foreign social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

A New Holistic Concept Subsuming Previous Research

Cognitive domain operations now appear to be subsuming many previously distinct lines of effort under the PLA's psychological warfare program. For example, subliminal messaging is specifically referenced as a key technology for cognitive domain operations by the aforementioned 2014 AMS book, 2018 NUDT and 2018 SSF Base 311 articles. There has been a clear line of effort by NUDT over the last 10 years, following the broader PLA shift from a defensive to an offensive mindset, that included research on how to use subliminal messaging to reduce PLA soldiers' resistance to indoctrination. Some of these tactics were recently tested on NUDT students in a class on the "three warfares." **[28]** NDUT researched video manipulation during 2010-2011, and a December 2011 article proposed using " audio-visual technology to imitate the voice of the national leadership and battlefield commanders to mislead the adversary's decision-makers into wrong decisions." **[29]** This video editing required "sound-image synthesis technology" (声像合成技术, *shengxiang hecheng jishu*)—a term that resembles other PLA references to "voice information synthesis technology," and seems to indicate the development of building blocks for deep fakes. **[30]**

Disinformation is a Key Feature

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



Specific Recommendations for Targeting of Disinformation by PLA Researchers:

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

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

Real World Evidence

Taiwan is the best case study of the real-world applications of the PLA's cognitive domain operations, and highlights one clear vector: social media disinformation. The Taiwan government has claimed that China interfered with the island's November 2018 election through a variety of means, employing both traditional and social media. **[35]** Anonymous Taiwanese national security officials have claimed the SSF was the driving force behind the election interference campaign, and reports have identified Beijing artificially generating support for its preferred candidates on social media. **[36]** Researchers have suggested the CCP Propaganda Department, CCP United Front Work Department, and perhaps private contractors could have played a role as well. **[37]**

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

Conclusion

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

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

Notes

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

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

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

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

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

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

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

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

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

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

Army in Multi-Domain Operations 2028 (U.S. Army Training and Doctrine Command, December 2018), https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf (https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf).

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

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

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

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

[15] See: Shi Zhongwu [石忠武], "Considerations on Promoting the Transformation of the PLA Army" ["推进陆军转型建设的几点思考"], *China Military Science* [中国军事科学], December 2016; Zhang Fang [张芳] and Wei Jiying [魏际英], "Enhancing the aggressiveness and initiative of military strategy communication under the media fusion communication environment" ["媒体融合传播环境下增强军

事战略传播进取性和主动性问题”], *Course Education Research* [课程教育研究], March 2019; Lu Hongwei [路红卫], “Revisiting the Essential Feature of Modern War” [“再谈现代战争的本质特征”], *National Defense* [国防], May 2019.

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

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

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

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

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

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

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

Review [国防科技], October 2018.

[23] Ibid.

[24] Ibid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[39] Ibid.

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

Read-the-09-06-2019-CB-Issue-in-PDF.pdf (https://jamestown.org/wp-content/uploads/2019/09/Read-the-09-06-2019-CB-Issue-in-PDF.pdf)

1310 L St. NW, Suite 810
Washington DC, 20005

PHONE: 202.483.8888 (tel:202.483.8888)
FAX: 202.483.8337
E-MAIL: pubs@jamestown.org (mailto:pubs@jamestown.org)