



NOVEMBER 2024

# Decoding China's AI-Powered 'Algorithmic Cognitive Warfare'

Libby Lange, Director for Intelligence

---

As the strategic rivalry between the People's Republic of China (PRC) and the United States deepens, Chinese military and political scholars are pushing a new concept of information warfare that aims to leverage the capabilities of AI-powered algorithms to target, influence, and divide foreign populations. Dubbed "algorithmic cognitive warfare," this framework encompasses both the artificial intelligence (AI) algorithms used to analyze and track individuals, as well as the powerful recommendation algorithms embedded within social media platforms that drive content consumption. At the heart of algorithmic cognitive warfare's success lies the granular, comprehensive data about target populations needed to conduct individualized warfare.<sup>1</sup> The PRC military and intelligence agencies will need to collect and process immense amounts of personal data to achieve the level of tailored content delivery they envision. Policymakers and the public alike must recognize this shift in the PRC's strategic thinking to protect themselves better online both today and in the technological landscape of the future.

---

<sup>1</sup> [Offset-X: Closing the Deterrence Gap and Building the Future Joint Force](#), Special Competitive Studies Project (2023).



AI-powered  
analytic  
algorithms

Algorithmic Cognitive Warfare:  
Using granular data to exert precise,  
individualized influence

Social media  
recommendation  
algorithms



This article analyzes scholarly works and editorials written by authors affiliated with the People's Liberation Army (PLA) and defense-focused institutions, published in military-affiliated outlets, or supported by research grants focusing on national security that explicitly discuss “algorithmic cognitive warfare” or the use of algorithms to enhance the efficacy of cognitive operations. It is important to note that a significant gap often exists between PLA doctrine and the effectiveness of their capabilities. It is unclear whether the PLA currently has the capabilities to leverage the tools and techniques they propose fully. However, these works provide an unfiltered insight into strategic thinking about the methods and functions of algorithmic cognitive warfare, as well as offering forward-looking assessments of how emerging technologies such as large language models (LLMs) and virtual reality could all become attack surfaces in the future cognitive domain.

## What is Cognitive Warfare?

The PLA conceives of warfare across multiple domains. These domains span the physical and digital worlds, including what Chinese scholars and military thinkers refer to as the “cognitive domain” (认知域). According to authors at China's National Defense University, “cognitive domain operations” first appeared in Chinese scholarship as early as 2010,<sup>2</sup> but later authors have firmly situated the concept within existing PLA military thought.<sup>3</sup> In the words of one scholar, cognitive warfare is an aggregate of “public opinion warfare, psychological warfare, legal and trade warfare, diplomatic warfare, technological warfare, and thought warfare.”<sup>4</sup> More concretely, the goal of cognitive warfare is to use selective messaging to interfere with and control the beliefs of the enemy, here meant to include both warfighters and civilian populations.<sup>5</sup> Chinese military scholars view control of enemy cognition as crucial to victory: one group writing

---

<sup>2</sup> 余远来, 陈茜, 认知域作战的致效机理与策略选择, 思想理论战线 (2022).

<sup>3</sup> 陈昌孝, et al., 认知域作战主要样式演进与发展趋势, 国防科技 at 137 (2024).

<sup>4</sup> 梁晓波, 认知域作战是语言对抗新的主战场, 人民军事网 (2022).

<sup>5</sup> 余远来, 陈茜, 认知域作战的致效机理与策略选择, 思想理论战线 (2022).

陈昌孝, et al., 认知域作战主要样式演进与发展趋势, 国防科技 at 137 (2024).

for the military journal *National Defense Technology* described it as potentially more beneficial than “destroying by firepower, seizing control of troops, or conquering cities and territory.”<sup>6</sup> In practice, the PRC’s cognitive warfare efforts appear to be divided across military, law enforcement, and intelligence agencies. The dispersal of cognitive operations across multiple civilian and military agencies aligns with PLA conceptions of cognitive warfare as “eliminating the boundaries between peacetime and wartime, soldiers and civilians,” where operations are “used before military measures, launched in tandem with military measures, and wrapped up after military measures.”<sup>7</sup> For example, the now-reorganized PLA Strategic Support Force was once home to “Base 311,” a unit believed to be specifically responsible for cognitive warfare campaigns targeting Taiwan.<sup>8</sup> The group may have been subsumed under the newly established Information Support Forces. The U.S. Department of Justice has tied PRC influence campaigns targeting Chinese dissidents abroad and the U.S. government to China’s Ministry of Public Security, an agency responsible for both law enforcement and intelligence collection.<sup>9</sup> In its 2023 report to Congress, the Department of Defense also accused the Ministry of State Security, the PRC’s primary intelligence agency, of conducting influence operations against the U.S.<sup>10</sup>

## The Emergence of ‘Algorithmic Cognitive Warfare’

**“Explore the use of artificial intelligence in news collection, production, distribution, reception, and feedback, using mainstream value orientations to drive ‘algorithms,’ comprehensively enhancing discourse leading capabilities.”**

PRC President Xi Jinping, 2019<sup>11</sup>

With the rise of social media and other technologies that facilitate online interaction, Chinese military scholars have begun to advocate for a new form of cognitive warfare, one that is fundamentally algorithmic in nature. Some of the most prolific scholars to write on this subject appear to be affiliated with the PLA Air Force Early Warning Academy, which the official PLA

---

<sup>6</sup> 陈昌孝, et al., 认知域作战主要样式演进与发展趋势, 国防科技 at 140 (2024).

<sup>7</sup> 陈昌孝, et al., 认知域作战主要样式演进与发展趋势, 国防科技 at 140 (2024).

<sup>8</sup> Elsa B. Kania, [The Role of PLA Base 311 in Political Warfare against Taiwan \(Part 3\)](#), Global Taiwan Institute (2017).

<sup>9</sup> [34 Officers of People's Republic of China National Police Charged with Perpetrating Transnational Repression Scheme Targeting U.S. Residents](#), U.S. Attorney’s Office, Eastern District of New York (2023).

<sup>10</sup> [Military and Security Developments Involving the People’s Republic of China](#), U.S. Department of Defense (2023).

<sup>11</sup> 习近平：加快推动媒体融合发展 构建全媒体传播格局, 中国共产党新闻网 (2019).

news website refers to as a “base for military information capabilities training.”<sup>12</sup> While these authors trace the fundamental tenets of cognitive operations as far back as philosophers like Sun Tzu, they view the emergence of algorithms as a transformative factor in their importance. In their words, AI can “create a flexible cognitive setting and shape the adversary’s thoughts and cognition without them knowing through the precise delivery of tendentious messaging.”<sup>13</sup> Their belief in the fundamental importance of algorithms is shared by others in the PRC’s cognitive warfare community, where researchers have described algorithms as everything from “controllers” to “gatekeepers” to the creators of “information cocoons.”<sup>14</sup> One author highlights the Cambridge Analytica controversy revealed in 2018, in which data from millions of Facebook profiles were harvested for use by political campaigns, as proof of the power of algorithms to sway political outcomes.<sup>15</sup> According to these scholars, whereas previous propaganda and cognitive warfare paradigms relied on broad mass communication techniques to spread pro-China messaging, algorithms have unlocked a “bottom-up” ability to influence populations at an individual level through data-driven methods.<sup>16</sup>

Russia’s full-scale invasion of Ukraine in February 2022 marked a clear turning point in PLA thinking about cognitive warfare and the key role algorithms play in their success. Many algorithmic cognitive warfare articles specifically discussed algorithms’ impact on global opinions on the Russia-Ukraine war. One such article, co-authored by Qiushi Distinguished Professor<sup>17</sup> and member of UNESCO’s Information for All Program Information Ethics Working Group Fang Xingdong, called the war a “paradigm shift” in public opinion warfare. The author contrasted Russia’s attempts to establish a “grand narrative” rooted in history to Ukraine’s more effective use of social media to establish a “narrative of difference” with Russia. The key, the author argues, was Ukraine’s ability to use this tactic to “seize the ‘moral heights’” of the war.”<sup>18</sup> Interestingly, the article highlights TikTok as a particularly prominent forum where this new paradigm has taken shape.

---

<sup>12</sup> 任爽, 2017军校巡礼第十五站: 空军预警学院 (附报考指南), 中国军网 (2017).

<sup>13</sup> 陈昌孝, et al., 认知域作战主要样式演进与发展趋势, 国防科技 at 141 (2024).

<sup>14</sup> 张智伟, 智能化视阈下的认知域作战, 解放军报 (2022);

蔡翠红, 社交媒体‘算法认知战’与公共外交的新特点, 人民论坛 at 22 (2022).

The concept of “information cocoons” was first proposed by American legal scholar Cass Sunstein. See Cass Sunstein, [Infotopia: How Many Minds Produce Knowledge](#), Oxford University Press (2006).

<sup>15</sup> 蔡翠红, “社交媒体‘算法认知战’与公共外交的新特点.” 人民论坛 at 21 (2022).

<sup>16</sup> 方兴东, 钟祥铭, 算法认知战: 俄乌冲突下舆论战的新范式, 传媒观察 at 7 (2022).

<sup>17</sup> Qiushi is the Chinese Communist Party’s official theoretical journal. For more details, see [Qiushi](#), Center for Strategic and International Studies (last accessed 2024).

<sup>18</sup> 方兴东, 钟祥铭, 算法认知战: 俄乌冲突下舆论战的新范式, 传媒观察 at 7 (2022).

The parallels between the authors' lessons learned from the war in Ukraine and the PRC's approach to Taiwan are clear. President Xi Jinping himself has repeatedly invoked historical narratives to create a sense of inevitability around the PRC's proposed annexation of Taiwan.<sup>19</sup> Conversely, Taiwanese policymakers and civil society groups have worked to emphasize the island's connections to global democracies, in contrast to the PRC, and their desire to further integrate into the international community – Taiwan's own "narrative of difference." While Fang's article stops short of criticizing specific PRC-promoted narratives, the author urges a shift away from "ideology and propaganda" in cognitive shaping efforts. Researchers in Taiwan noted a shift in PRC efforts to influence Taiwan's elections in 2024 that aligns with these suggestions, with an increased focus on inauthentic and unattributed accounts amplifying localized narratives related to livelihood and corruption, rather than official state channels pushing overtly ideological narratives.<sup>20</sup> This could indicate increasing alignment with the stance that in an online world driven by algorithmic amplification, the CCP's cognitive operations need to meet people where they are online, rather than trying to get them to engage with overtly ideological narratives. Instead of trying to get audiences to engage with explicit narratives that democracy is a lost cause, opportunistic cognitive warfare operations can target discrete issues salient to various audiences – such as natural disasters<sup>21</sup> or alleged corruption<sup>22</sup> – to more effectively reach the same result.

## Breaking Down Algorithmic Cognitive Warfare

While the concept of algorithmic cognitive warfare is still nascent, an article titled "An Exploration of Effective Mechanisms and Critical Technologies in Algorithmic Cognitive Warfare," published in the journal *Information Security and Communications Privacy*,<sup>23</sup> lays out a clear framework for how algorithms "empower" each stage of a cognitive operation. The authors divide cognitive operations into six stages: user portrait, attracting attention, suggesting reference, inducing reaction, timely intervention, and supervising gratification.<sup>24</sup>

---

<sup>19</sup> Jude Blanchette, et al., [What is Beijing's Timeline for 'Reunification' with Taiwan?](#), Center for Strategic and International Studies (2023).

<sup>20</sup> [2024 Taiwan Elections: Foreign Influence Observation – Preliminary Statement](#), Digital Intelligence Team, Doublethink Lab (2024).

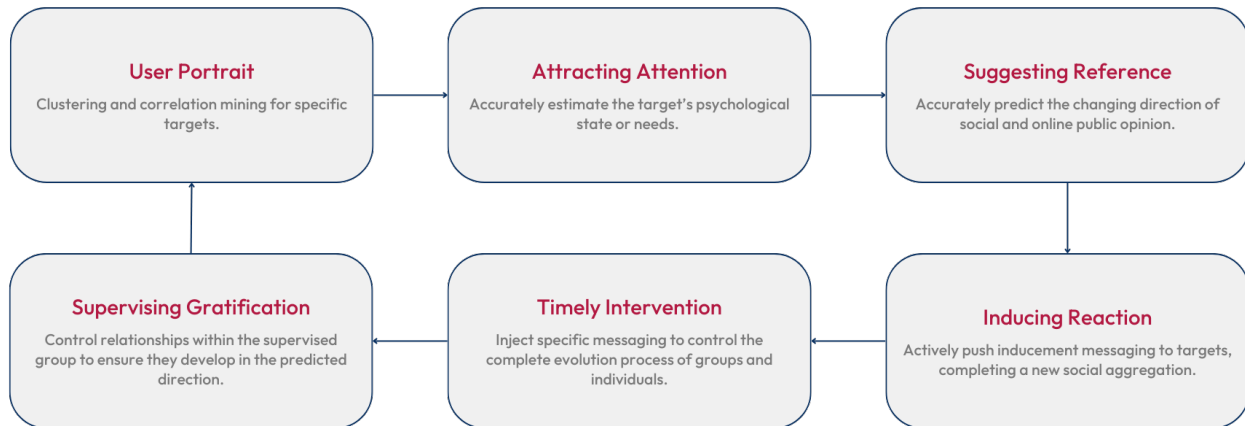
<sup>21</sup> [Same targets, new playbooks: East Asia threat actors employ unique methods](#), Microsoft Threat Intelligence at 6 (2024).

<sup>22</sup> [Russia, China, and Iran continue influence campaigns in final weeks before Election 2024](#), Microsoft Threat Intelligence at 7 (2024).

<sup>23</sup> *Information Security and Communications Privacy* is supervised by the Ministry of Industry and Information Security and hosted by a research institute affiliated with China Electronics Technology Group that was added to the Entity List in 2020 for "engaging in activities contrary to U.S. national security interests." See [Addition of Entities to the Entity List, and Revision of Entries on the Entity List](#), Federal Register (2020).

<sup>24</sup> 陈昌孝, et al., 算法认知战的致效机理与关键技术探析, 信息安全与通信保密 at 76-78 (2023).

## Theoretical Model of Algorithmic Cognitive Warfare



A translated infographic from the article “An Exploration of Effective Mechanisms and Critical Technologies in Algorithmic Cognitive Warfare” details the authors’ theoretical model of algorithmic cognitive warfare. Source: 陈昌孝, et al., 算法认知战的致效机理与关键技术探析, 信息安全与通信保密 at 76 (2023).

- **User Portrait.** Algorithms offer a technologically-enabled means to identify target audiences at scale. On an individual level, the authors describe algorithms as being able to sketch out a person’s psychological state; at a societal level, they see algorithms as mapping “societal ideological distributions, psychological tendencies, [and] psychological structures.” More concretely, algorithms can perform grouping and relationship mapping on specific targets to segment audiences and identify linkages between them. A narrative or piece of content that may resonate with one audience may be interpreted completely differently by another.
- **Attracting Attention.** The authors see a role for algorithms in both monitoring audiences and powering the AI models that can automatically generate content that will capture their attention. They argue that the key to attracting attention is not just tailoring content to “static” attributes such as interests or political leanings, but instead a target’s real-time psychological state and needs. Large language models (LLMs) powered by algorithms will be able to rapidly create content addressing those needs and engage in precise dissemination to encourage targets to “explore” an issue further. This stage sets users on a path to engage with new narratives, destabilizing their existing “cognitive framework.”
- **Suggesting Reference.** Algorithms are uniquely capable of making the appearance and virality of certain issues appear natural, allowing targets to believe they are making “independent judgments” in favor of the adversary. According to the authors, algorithms are responsible for both “fanning the flames” of an issue and “managing” discussions in the desired direction. Here, again, the authors foresee a need for vast amounts of data to

fine-tune the algorithm to parse and predict public opinion so that the algorithm's role in the debate is not revealed.

- **Inducing Reaction.** Humans are social creatures and will naturally seek out others who share their beliefs and values. Once targets have engaged in the desired way with suggested narratives pushed as part of a cognitive operation, algorithms further the process of fragmentation by regrouping individuals into new clusters, creating what multiple articles refer to as “information cocoons.”<sup>25</sup> Here, the authors see in-platform algorithms as key; they specifically name multiple types of recommendation algorithms (that have largely replaced chronological content delivery systems) used on social media platforms as capable of crossing the “threshold” needed to regroup users.
- **Timely Intervention.** Once a cognitive operation has formed new groupings, the authors warn against allowing these groups to evolve unchecked. The purpose of “timely intervention” is to use specific messaging to ensure these “cliques” develop in the operators’ desired direction.
- **Supervising Gratification.** Finally, algorithms can help to measure the social gratification of targets once they have entered into new groupings. They describe people as deriving “extreme gratification” from supervising both others and themselves within an in-group. At this stage, they also urge cognitive operators to test the “black box” of these new social groupings by using specific messaging and monitoring the group’s outputs to create a model of that group’s internal dynamics.

## Data-Driven Manipulation

Precise data is fundamental to the new paradigm of algorithmic cognitive warfare detailed above. In fact, one article argues that “although algorithms are the core [of algorithmic cognitive warfare], intelligence information is the key” to their effectiveness.<sup>26</sup> Whereas previous influence efforts sought to achieve the dissemination of content to the largest audience possible, the algorithmically-enabled “user portraits” algorithmic cognitive warfare proponents envision would be able to design content tailored precisely to an individual’s unique cognitive terrain, as well as their psychological state at any given time. To accomplish this, the PLA and PRC intelligence agencies would need to collect and process vast amounts of personal data on foreign targets to carry out a truly “algorithmic” cognitive operation.

---

<sup>25</sup> For example, see 蔡翠红, 社交媒体“算法认知战”与公共外交的新特点, 人民论坛 (2022).

<sup>26</sup> 李灵芝, 李浩 & 冯讯, 面向算法认知战的开源情报智能化分析, 军事文摘 (2024).

## Hypothetical Data Pipeline for Algorithmic Cognitive Warfare



Early indications suggest PRC-linked actors are already collecting this kind of information at both broad and granular levels. In its first public threat report on covert influence operations, OpenAI noted that a persistent online influence campaign that researchers dub “Spamouflage,” which both Meta<sup>27</sup> and the U.S. government have linked to Chinese law enforcement, used ChatGPT to “summarize and analyze the sentiment” of posts by overseas Chinese dissidents the operation sought to target with harassment.<sup>28</sup> In a July 2024 court filing, the U.S. Department of Justice revealed that TikTok collected and stored data about users’ views on divisive topics such as abortion and gun control that was accessible by employees located in China.<sup>29</sup>

The data these authors hope to collect, however, goes far beyond just publicly available social media data. For example, multiple articles discuss the potential for algorithms to establish correlations between people and events using disparate data points such as a person’s shopping history or travel habits – what they call “finding relationships or correlations between hidden data points within a sea of data.”<sup>30</sup> Much of this data is not publicly available and would need to be acquired commercially or stolen from internal systems. Massive hacks attributed to the Chinese government, including the U.S. Office of Personnel Management (OPM), Marriott, and Equifax, closely align with this desire to create comprehensive profiles of U.S. citizens.<sup>31</sup> While much previous reporting has focused on the potential of that data to be used for intelligence targeting or blackmail, the scholarship on algorithmic cognitive warfare paints this data collection in a new

<sup>27</sup> Ben Nimmo, et al., [Second Quarter Adversarial Threat Report](#), Meta at 12 (2023).

<sup>28</sup> [AI and Covert Influence Operations: Latest Trends](#), OpenAI at 24 (2024).

<sup>29</sup> Georgia Wells, [TikTok Collected U.S. Users’ Views on Gun Control, Abortion and Religion, U.S. Says](#), The Wall Street Journal (2024).


<sup>30</sup> 李灵芝, 李浩, & 冯讯, 面向算法认知战的开源情报智能化分析, 军事文摘 (2024).

<sup>31</sup> Garrett M. Graff, [China's Hacking Spree Will Have a Decades-Long Fallout](#), Wired (2020).



light: rather than searching for the needle, the Chinese government may be able to use the entire haystack.

## Opportunities for Countering Algorithmic Cognitive Warfare

-  Enhance Analysis and Situational Awareness
-  Develop More Rapid Warning Mechanisms
-  Prepare Counter-Messaging
-  Protect U.S. Citizens' Data

U.S. policymakers will need to make full use of their research, policy, and communications toolkits to counter the persistent, pervasive nature of the PRC's algorithmic cognitive warfare.

### Enhance Analysis and Situational Awareness

First and foremost, U.S. intelligence and homeland security agencies should increase their focus – both collection and analysis – on PRC influence capabilities and aspirations, and educate policymakers about how algorithmic cognitive warfare is changing the game. Maintaining awareness of Beijing's doctrine, strategies, and tactics will be an ongoing task because algorithmic cognitive warfare remains a dynamic concept. For example, multiple PRC papers discuss the potential for emerging technologies – including LLMs, AR/VR, deepfakes, “human-machine integration,” and data produced by the increasing connectivity of everyday objects, sometimes referred to as the Internet of Things (IoT) – to further enhance both the data collection and delivery mechanisms of algorithmic cognitive warfare.<sup>32</sup> As these technologies develop, it will be important for U.S. intelligence to monitor if, and how, they are deployed in support of PRC influence efforts.

### Develop More Rapid Warning Mechanisms

U.S. security officials and policymakers must do a better job of communicating to the American public how PLA scholars discuss using social media and advanced technologies to manipulate, deceive, and misdirect. A broader understanding of the precision warfare Chinese scholars

---

<sup>32</sup> 陈昌孝, et al., 算法认知战的致效机理与关键技术探析, 信息安全与通信保密 (2023); 张智伟, 智能化视阈下的认知域作战, 解放军报 (2022).

envision on social media – and the data infrastructure needed to support it – could add significant weight to existing concerns around the safety of China-linked social media platforms, such as TikTok, and companies that collect and analyze vast amounts of user data, such as Shein.<sup>33</sup>

The U.S. Intelligence Community (IC), which is perhaps best positioned to detect and monitor these advanced influence campaigns as part of its national security mission, must also work to speed up, systematize, and potentially even automate the warnings it provides to policymakers and the public. While the IC's unclassified reports to Congress are a strong start, there is currently no home for reporting that is easily accessible to the public. Faster, broader warnings toward the public regarding threats posed by targeted disinformation campaigns and cyberattacks aimed at harvesting their personal data would help bolster the public's situational awareness and encourage better cyber hygiene practices.

### **Advance Our Own Strategic Messaging**

The PRC's cognitive warfare ambitions are a global threat that necessitates a global response. Armed with the knowledge that the PRC is working to undermine trust in our institutions and system of government, policymakers need to actively promote truthful, accurate messaging that aligns with our own strategic goals. We must reinvigorate our strategic communications efforts across traditional diplomatic and media channels, but also leverage the digital platforms where many people are now engaging with news and current events. This includes redoubling efforts to penetrate the PRC's information space, even as they seek to sequester it from the outside world. The U.S. IC can augment this reinvigorated strategic communications capability by expanding the sharing of findings related to disinformation and cognitive warfare campaigns with allies and like-minded nations.

### **Protect U.S. Citizens' Data**

Because Chinese algorithmic cognitive warfare is designed to acquire and exploit the private information of its targets, protecting and shielding U.S. privacy data will be even more essential. The U.S. government has already made encouraging progress to limit the transfer of U.S. data to China in the form of the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA) and Executive Order 14117.<sup>34</sup> More recently, the Department of Justice has built on EO 14117 by publishing a Notice of Proposed Rulemaking that would give it regulatory authorities over

---

<sup>33</sup> Nicholas Kaufman, [Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes](#), U.S.-China Economic and Security Review Commission at 2-3 (2023).

<sup>34</sup> [Public Law No: 118-50](#) (2024); [Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern](#), The White House (2024).

certain data transactions to countries of concern.<sup>35</sup> A deeper understanding of the data collection targets laid out in algorithmic cognitive warfare scholarship will help to determine whether the data types and entities restricted under these frameworks will need to be expanded.

---

---

<sup>35</sup> [Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons](#), Department of Justice (2024).