

## Issue Brief

# China's Military AI Wish List

**Command, Control,  
Communications, Computers,  
Cyber, Intelligence, Surveillance,  
Reconnaissance, and Targeting  
(C5ISRt)**

---

### Authors

Emelia Probasco  
Sam Bresnick  
Cole McFaul

## Executive Summary

This report examines thousands of open-source requests for proposal (RFPs) published by China's People's Liberation Army between January 1, 2023, and December 31, 2024. The RFPs we reviewed offer insights into the PLA's priorities and ambitions for AI-enabled military technologies associated with C5ISR: command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance, and targeting.

In analyzing these RFPs, we find that the PLA is pursuing AI-enabled capabilities across all domains. The applications include AI-enabled decision support systems (AI-DSS), sensor enhancement tools, data fusion algorithms, and much more.

The RFPs reflect China's desire to generate, augment, and fuse increasing quantities of data to speed military decision-making and improve the precision and efficacy of the PLA's operations. Specifically, we found requests for AI-DSS that can leverage open-source data for strategic decision-making. We also came across requests for AI-DSS to support tactical decisions, such as for targeting. While many militaries are investing in AI-DSS, these systems are of particular importance to the PLA, which views them as a means of compensating for perceived weaknesses in its officer corps.

More specifically, we found an emphasis on AI applications that would counter perceived U.S. military advantages. This emphasis was especially apparent in numerous requests for technologies to detect U.S. naval assets on and under the sea, as well as technologies that could counteract U.S. space-based systems.

Outside of the maritime and space domains, the PLA's RFPs reveal that it aims to acquire increasingly sophisticated surveillance and cognitive domain capabilities. RFPs for facial and gait recognition systems, digital surveillance tools capable of recovering deleted data, and technologies for generating and detecting deepfakes point to ongoing efforts to better secure military installations and develop AI-enabled psychological warfare and cognitive targeting tools.

These documents, which are published by the PLA, are strikingly explicit in their requests for sensitive capabilities, including those related to operations in the space, cyber, and cognitive domains. The level of specificity is notable and likely reflects an effort to access advanced capabilities from nontraditional, commercial vendors outside China's traditional defense industrial base. Moreover, most of the RFPs involve relatively small budgets and short acquisition timelines—often three to six months—suggesting an emphasis on experimentation, prototyping, and rapid iteration.

The PLA's C5ISRT-related AI acquisition efforts have several implications for U.S. policymakers and defense planners. First, Washington must respond to China's interest in AI-enabled sensing and surveillance, especially in the maritime and space domains, with investments in counter sensing, deception, and resilience against China's increasingly capable ISR systems.

Second, the United States should prepare to counter emerging Chinese AI-DSS while pursuing dialogue with China on the responsible use of these systems to reduce the chances of miscalculation and escalation. While it is unlikely that Washington and Beijing will make binding commitments, continued discussions could help establish technical minimum standards and norms around the use of these systems.

Third, the PLA's interest in AI systems that ingest and process vast volumes of open-source data for strategic decision-making demands a rethink of approaches to military signaling, deterrence, and crisis management. Increasing reliance on AI to interpret global events could complicate previous approaches to escalation control.

Fourth, China's military appears ready to use AI to greatly expand its surveillance and information-manipulation capabilities, including more systematic use of deepfakes. Washington should counter with stronger public awareness efforts and public-private collaboration, as well as develop technical standards and tools to detect and blunt these tactics.

Fifth, China's embrace of prototyping and rapid acquisition timelines should further motivate U.S. leaders to support defense acquisition reform, fund a diverse research portfolio, and set the conditions for rapid experimentation and responsible AI adoption in the operating forces.

Sixth, access to advanced AI hardware developed by U.S. companies enables the PLA's modernization. Evidence that the PLA is seeking advanced U.S.-designed semiconductors, as well as leveraging Chinese large language models trained on U.S. GPUs, suggests that relaxing export controls will facilitate China's development and use of AI-enabled C5ISRT technologies.

Finally, the breadth and diversity of the PLA's AI wish list reinforce the importance of conducting sustained open-source monitoring to track capability development, detect shifts in priorities, and identify early signs of operational deployment. Such analysis helps to right-size current challenges to U.S. national security.

## Table of Contents

|  |    |
|--|----|
| Executive Summary .....  | 1  |
| Introduction .....   | 4  |
| Background .....   | 5  |
| The PLA’s Intelligentization Focus .....   | 5  |
| Methodology .....  | 7  |
| Enabling the PLA’s Command and Control: AI-Enabled Decision Support Systems (AI-DSS) ..... | 9  |
| Strategic, Multi-Domain, and Cross-Echelon Command and Control .....                       | 9  |
| Support for Targeting in the Air, Sea, and Space Domains .....                             | 10 |
| Cognitive Domain Operations .....  | 14 |
| Deepfake Requests .....  | 14 |
| Cognitive Targeting and Information Campaigns .....  | 15 |
| Intelligence, Surveillance, and Reconnaissance .....                                       | 17 |
| Cross-Cutting Intelligence and Sensing Capabilities .....                                  | 17 |
| Maritime Sensing .....   | 18 |
| Undersea Sensing .....   | 19 |
| Space Sensing .....  | 20 |
| Surveillance .....   | 20 |
| Communications, Computers, and Cyber .....   | 24 |
| Communications .....   | 24 |
| Cyber .....  | 25 |
| Takeaways .....  | 29 |
| Implications for the United States .....   | 31 |
| Conclusion .....   | 33 |
| Authors .....  | 34 |
| Acknowledgments .....  | 34 |
| Appendix: Methodology to Identify AI-related RFPs .....                                    | 35 |
| Endnotes .....   | 36 |

## Introduction

China now boasts world-class artificial intelligence (AI) capabilities. It is a leader in facial recognition technologies, competitive with the United States in developing large language models (LLMs), and pushing the boundaries in robotics. While some areas of China's AI ecosystem are much studied and well understood, others, such as the Chinese military's development and deployment of AI-enabled capabilities, are not.

This report attempts to address this gap and provide information on the People's Liberation Army's (PLA) drive to adopt AI for various military applications. In writing this paper, we examined more than 9,000 unclassified PLA requests for proposal (RFPs) to glean a partial yet detailed view of the Chinese military's efforts to acquire AI for C5ISR in the land, air, sea, space, cyber, and cognitive domains. These AI-related efforts include the employment of generative AI but also other related and enabling AI techniques, such as natural language processing, computer vision, data fusion algorithms, and more.

In brief, our analysis of the RFPs published in 2023 and 2024 indicates that the PLA is experimenting broadly with AI-related technologies across a range of applications, including decision-making; intelligence, surveillance, and reconnaissance (ISR); cyber offense and defense; and many more. This analysis is part of a series that will focus on China's requests for AI and related technologies across all domains of warfare.

## Background

### *The PLA's Intelligentization Focus*

The PLA considers information the decisive element of modern warfare. Its doctrine holds that success in any domain depends on achieving information dominance, which underpins all combat operations.<sup>1</sup>

As such, Chinese leaders and authoritative government sources have framed the PLA's modernization efforts as a transition from mechanization (the incorporation of advanced machinery and equipment), to informatization (the use of networks, information systems, and data), to intelligentization (the utilization of emerging technologies like AI).<sup>2</sup> Today, the PLA's focus is on informatization and intelligentization, whereby it aims to gather vast amounts of data and use AI and other emerging technologies to analyze it to speed military decision-making and conduct more precise operations.

PLA doctrine links this information-centric view of modern conflict to its concepts of system destruction warfare and multi-domain precision warfare.<sup>3</sup> The former, which the Pentagon notes is likely China's "principal theory guiding its way of war," specifies that the PLA should aim to paralyze an adversary by striking critical nodes such as communication networks and sensors, as well as command and control systems.<sup>4</sup> The latter serves as China's "core operational concept," whereby the PLA aims to use AI to help identify and strike weak points in its adversaries' military operational systems.<sup>5</sup>

According to the Pentagon, many of the capabilities the PLA needs to execute multi-domain precision warfare are a part of nine technological and functional areas known collectively by the acronym C5ISRT, which stands for command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance, and targeting.<sup>\*6</sup> Together, the technologies and people that perform C5ISRT functions enable military action through networks of sensors to perceive the battlespace, fuse data, identify objects, and guide precision strikes, and could help the PLA to seize the advantage.<sup>7</sup> USAF Colonel John Boyd's "Observe, Orient, Decide, Act," or OODA Loop, is a streamlined conceptualization of this information process. Like the U.S. military, the PLA is experimenting with AI to both accelerate and improve its OODA Loop.<sup>8</sup>

---

\* Other similar acronyms are also used to describe this grouping of capabilities, including C4ISR (which excludes Cyber and Targeting). NATO uses a related though less-comprehensive term, ISTAR, which stands for Intelligence, Surveillance, Target Acquisition and Reconnaissance.

China's defense conglomerates have historically struggled to develop the technologies necessary for intelligentization, so the PLA is increasingly seeking solutions from the Chinese commercial sector through Beijing's military-civil fusion strategy (MCF).<sup>9</sup> Previous CSET research found China's AI defense industrial base has indeed diversified, potentially fueling advances in China's military capabilities.<sup>10</sup>

The majority of this paper focuses on the PLA's AI-enabled C5ISRT-related RFPs. Certain sections, however, go beyond the typical U.S. conception of C5ISRT components. This is particularly true for surveillance, where the relevant RFPs indicate an embrace of expansive surveillance of individuals. Furthermore, this paper will cover technologies intended for the "cognitive domain"—namely, the domain of emotions, perceptions, beliefs, values, and reasoning that shape decision-making, according to the PLA.<sup>11</sup> We included RFPs for population surveillance and cognitive domain operations for two reasons. First, AI-fueled psychological warfare technologies and surveillance capabilities are key aspects of China's defense and internal security strategies, making them highly relevant to this study. Second, the technologies that support psychological warfare and population surveillance can be applied for both international and domestic uses.\*

---

\* While the PLA is primarily tasked with guaranteeing the Chinese Communist Party's and China's external defense and executing combat operations, many of the documents we reviewed include requests for technologies aimed at internal security missions. These include population and digital surveillance technologies as well as security systems for domestic military installations. We include information and analysis on these requests because they could also be used in international operations.

## Methodology

This report draws from a dataset of more than 9,000 AI-related RFPs published by the PLA between January 2023 and December 2024. The documents were publicly disseminated by the Chinese military with the intent of soliciting bids from Chinese companies, especially vendors that have not historically worked with the PLA. Many of the requests are for relatively small amounts, indicating that they may be for experimental research and development projects. We did not identify any requests for major weapons systems among the documents. Within our dataset, we identified the AI-related RFPs from a larger set of procurement documents using a combination of keyword searches and LLM-assisted methods.

We classify an RFP as “AI-related” if it supports the development or deployment of AI-enabled or autonomous technologies. As a result, the more than 9,000 AI-related RFPs in this dataset encompass a broad range of goods and services, including language and vision models, autonomous vehicles, virtual and augmented reality platforms, data collection and management systems, smart manufacturing and robotics, and more. For more on our methodology to classify AI-relatedness, please see the appendix.

From the more than 9,000 AI-related RFPs, we used an LLM to translate each document into English and extract relevant project information. We then manually reviewed a large subset of the documents to identify and analyze AI-related RFPs applicable to C5ISRT use cases. For this report, we largely excluded RFPs related to robotics, autonomous vehicles, semiconductors, and satellites, as well as RFPs related to AI applications for engineering, education, and training. Analysis of these requests will appear in future CSET research. Where a robotic or autonomous system was explicitly connected with a specific C5ISRT task, such as serving as a communications relay or reconnaissance platform, we included the RFP in our analysis as appropriate. During our manual review and analysis of C5ISRT-related RFPs, we referenced the original Chinese text to ensure the faithfulness of LLM translations.

Two limitations warrant mention. First, this dataset of AI-related RFPs only includes publicly available sources and does not include classified documents. Second, this study does not attempt to quantify the number of RFPs by AI technique or military task. Some RFPs do not provide enough detail to do so, and others involve multiple techniques or tasks, making quantifying RFPs by technique or application difficult and potentially misleading. Due to these categorization challenges, rather than quantify the RFPs by certain categories, we mention areas where we noted a concentration of effort.

Using this approach, this report aims to describe the main themes, trends, and priorities within the RFPs for the PLA's AI projects related to C5ISRT in 2023 and 2024. Our results provide an unclassified snapshot of the PLA's AI-related modernization efforts.

Throughout this report, we include direct quotes from certain RFPs in our dataset to add greater specificity to our analysis. Unfortunately, because the RFPs are no longer accessible online and due to the sensitive nature of these documents, we omit citations and references to specific source documents. Please reach out to us directly if you have questions about sources or citations.

The paper proceeds first with an examination of requests for AI-related technologies that support command and control, decision-making, and targeting. This is followed by an examination of RFPs related to cognitive domain operations and population and digital surveillance, as well as sensing and surveillance tasks. Finally, we summarize RFPs for other enabling technologies, such as those related to cybersecurity and communications. Altogether, our aim is to give the reader a sense of the breadth and character of the PLA's ambitions to develop and acquire AI-related goods and services applicable to C5ISRT.

## Enabling the PLA’s Command and Control: AI-Enabled Decision Support Systems (AI-DSS)

Senior military officers and political leaders alike maintain significant interest in AI-enabled decision support systems (AI-DSS), given the high-stakes nature of their decisions and the proliferation of battlefield sensors and information.<sup>12</sup> At all levels, decision-makers are burdened with the responsibility of managing and integrating vast and disparate sources of information to support strategic, operational, and tactical decisions. Analysts have long believed that AI could revolutionize military decision-making, and militaries around the world are pursuing AI-DSS, as evidenced by the U.S. Maven Smart System, Israel’s Lavender and Gospel systems, and Ukraine’s Delta system.<sup>13</sup> Our evaluation of PLA RFPs demonstrates that China is also pursuing the development of these systems in myriad ways.

### ***Strategic, Multi-Domain, and Cross-Echelon Command and Control***

The RFPs reveal that the PLA seeks to leverage AI and big data to maintain comprehensive awareness of everything from global events to tactical military movements. Two primary objectives emerge from these requests. First, the PLA aims to improve forecasting capabilities for world events and technological developments by assimilating and analyzing news, social media, and business data to predict social unrest, political tensions, and natural disasters. Second, the RFPs emphasize using AI and related technologies for decision-making support—allocating resources, setting military objectives, and coordinating efforts across different warfare domains.

To achieve these goals, the requested AI-DSS tools would dynamically display “the development of major international and domestic events, supporting situation analysis” while integrating geographic data and maps with location information from public news reports, commercial vendors, and government sources. The RFPs often emphasize open-source data collection, specifying that solutions should use “technologies such as deep web crawling and big data mining.”

Beyond data collection and display, several RFPs indicate the PLA’s interest in developing predictive algorithms. One sought “trend prediction for certain types of events, sorting through and tabulating the time, location, and circumstances of events, and predicting the future direction of such events.” Another appeared to pursue the orchestration of “general and domain-specific intelligent models,” using “large foundation models” to establish a “multi-model collaborative environment using video,

image, speech, text and code” from news and government sources.\* Finally, at least one RFP aimed to assist operational-level commanders in “programmatic planning” in response to “major international and domestic events.”

While AI-DSS can support general strategic or situational awareness and decision-making, they can also be used to centralize command and coordinate the activities of multiple weapons platforms, especially autonomous systems. In the dataset, we found a request for a system that would enable “multi-domain support fire and reconnaissance” with “low response latency, and high reliability” communications for a “collaborative tactical cloud,” as well as an RFP for a system that would, among other capabilities, “provide automatic correlation of multi-source intelligence based on target location.” We also saw evidence that the PLA is pursuing systems for controlling and coordinating autonomous systems, including one that would “support typical deep reinforcement learning algorithms, and support online feedback on human or agent scheduling simulation models, control, and data,” and one that would enable the simultaneous control of more than 80 airborne assets over distances of greater than 200 miles. This sort of command and control can coordinate surveillance, the rapid passing of information from sensor platforms to weapons platforms (sensor to shooter), and missile engagements. Of note, we also noticed RFPs for AI-related DSS to support satellite and space operations “under different space weather risk conditions.”

Overall, the AI-DSS RFPs for global situational awareness or multi-domain and cross-echelon support substantiate previous statements by the Chinese government that encourage the PLA to “strengthen a new generation of AI technology as a strong support to command and decision-making, military deduction, defense equipment, and other applications.”<sup>14</sup>

### ***Support for Targeting in the Air, Sea, and Space Domains***

Advanced militaries are increasingly deploying AI-DSS for targeting. They are using computer vision (CV) models to quickly locate objects of interest; identify tanks, ships, and other potential targets amid terabytes of imagery collected by satellites, drones, or ground-based cameras and videos; and track moving objects. Beyond CV, militaries use other AI techniques to refine, correlate, and fuse information from multiple heterogeneous sensors, including electromagnetic sensors, spectrometers, and synthetic aperture radar, as well as social media, research databases, and more.<sup>15</sup>

---

\* “Multi-model” is the correct translation.

While many militaries around the world discuss using AI for military targeting, China's RFPs are especially specific: The PLA is openly experimenting with AI-enabled targeting across all domains—air, land, maritime, space, cyber, and cognitive. This transparency reflects the PLA's information-centric approach to warfare, which positions data fusion and analysis as foundational to future military capabilities. The ability to collect, enhance, and analyze vast quantities of information will enable the PLA's evolving strategy of rapidly translating AI-generated battlefield insights into action. Our review of RFPs reveals that the PLA is experimenting with AI to extract actionable insights from troves of battlefield information.

We discuss each domain in the following subsections. In the United States, "targeting" involves six steps: finding, fixing (locating and identifying), tracking, selecting engagement weapons and timing, engaging, and finally assessing the impact of a strike.<sup>16</sup> Of the RFPs we found, most were focused on the tasks of finding, fixing, and tracking targets, though a few also sought to conduct battle damage assessments.\* For example, we found a number of general RFPs related to target recognition through the synthesis of optical remote sensing data, satellite synthetic aperture radar (SAR) data, and video. There was one request for a product focused on adapting "existing technological achievements in target detection, recognition, and time-series change analysis, placing emphasis on using theories such as AI and computer vision," as well as a request for an "optical convolutional neural network target recognition classifier." Other general target recognition requests included one to "enhance operational capabilities for target recognition and de-camouflaging of camouflaged personnel," and one to enable "target perception analysis" based on "multi-viewpoint video target trajectory fusion." With respect to battle damage assessment algorithms, we found requests for an "airborne damage assessment platform," as well as algorithms to measure structural damage based on panoramic images from drone cameras.

## Maritime Targeting

The PLA is soliciting AI solutions to enhance and analyze sensor data to find, identify, and track ships or other maritime targets. Several RFPs solicited data fusion technologies that could correlate information from multiple sensors across domains to assist in the accurate and comprehensive tracking of potential targets on the ocean surface. This is a common application and mirrors public statements from other

---

\* We distinguish targeting from surveillance RFPs by identifying requests that explicitly mention "target" or describe systems designed to find, identify, and track specific objects. For unclear cases, we classified RFPs as related to targeting based on indicators like data quality requirements, which are usually higher for munitions guidance purposes.

militaries looking to apply AI.<sup>17</sup> It is an especially critical capability for the PLA Navy, which must track the locations of ships and submarines if it hopes to be successful in conflicts at sea, including a potential invasion of Taiwan.

Aside from tracking ships on the surface of the ocean, there were many requests for technologies to find undersea targets. For example, several documents included requests for AI-enhanced underwater acoustic target recognition, or the use of sonar data to identify an adversary's subsea assets. There were also RFPs for AI-supported data enhancement technologies to improve the acoustic detection of submarines and the target-homing performance of torpedoes. We even identified requests to use AI to render 3D images of small underwater targets and identify them based on multi-sensor fusion. These underwater detection and data fusion capabilities are critical to undermining the U.S. advantages in undersea warfare, particularly U.S. submarines, unmanned underwater vehicles, and underwater detection networks.<sup>18</sup>

## Land Targeting

The RFPs aimed at ground targets mostly focused on fusing legacy or AI-enhanced sensor data to recognize and track targets. These RFPs sought solutions that would dynamically fuse data from multiple, heterogeneous platforms, a technically difficult but important task given the growing diversity of sensors across most militaries, including those on ships, aircraft, satellites, and other platforms.

Some of the details in the PLA's ground targeting RFPs included efforts to apply AI to segment land features, detect and recognize targets, and conduct spatial and time-based analysis of objects on the ground (spatiotemporal analysis). There were also applications aimed at the fusion of satellite, video, and presumably ground-based static images for target identification and tracking. Other niche but important requests included AI applications for the removal of background clutter in sensor returns and for technologies to help missiles distinguish among targets and background clutter. Relatedly, we found interesting combinations of technologies, such as UAV-mounted laser collimation systems, that could be used to provide high-definition video to find, track, and ultimately pinpoint (illuminate) targets for missile guidance.

## Space Targeting

Despite China's public statements that it "always advocates the peaceful use of outer space" and "opposes the weaponization of an arms race in outer space," China has demonstrated an ability to destroy satellites in orbit.<sup>19</sup> Furthermore, the 2025 *Annual Threat Assessment of the U.S. Intelligence Community* claimed that "China has

counterspace-weapons capabilities intended to target U.S. and allied satellites.”<sup>20</sup> Our dataset includes surprisingly specific requests for space targeting capabilities, both for targets on land and in space, adding more supporting evidence to warnings about China’s offensive space ambitions.<sup>21</sup>

For example, we found multiple inquiries for space-specific target detection and feature enhancement algorithms to help determine the nature of space objects and their three-dimensional orientation, as well as to support more precise targeting. Notably, there were several requests for research on algorithms that would determine a satellite’s orbit for more precise tracking and, potentially, targeting. Moreover, we observed requests for algorithms that could detect anomalies in a satellite’s orbit, a capability useful for offensive and defensive operations in space, as well as those for space target detection algorithms that low-Earth orbit satellites would use to observe satellites in higher orbits.

Of note, the space targeting-related RFPs were noticeably shorter than other RFPs and contained fewer details. Accordingly, it was difficult to determine if the use of the term “algorithm” referred to an AI technique or simply orbital mechanics, and we erred on the side of inclusion for this analysis. Similarly, several of these RFPs used the term “target” (目标) or “target detection” (目标检测) in the title. However, in this context the term may also refer to surveillance or object-detection tasks rather than to operational targeting.

## Cognitive Domain Operations

The PLA views psychological warfare, or shaping an adversary's perceptions, decision-making, and behavior, as a critical aspect of future conflicts.<sup>22</sup> Chinese military theorists frame cognitive domain operations, the PLA's main operational concept for the cognitive domain, as a means to shape narratives, erode public morale, manipulate social cohesion, and influence elite decision-making. These strategists emphasize controlling the information environment and exploiting vulnerabilities in human cognition as essential to seizing the strategic initiative. This approach also extends to peacetime influence campaigns aimed at shaping foreign perceptions of China's power and intentions and weakening alliances, as well as undermining democratic resilience.<sup>23</sup>

Beijing has undertaken a range of cognitive domain operations, including those focused on influencing the Taiwanese public. For example, China has executed disinformation and influence campaigns aimed at Taiwan's elections to cast doubt on politicians and democratic processes.<sup>24</sup> It is now reportedly using generative AI to supercharge these campaigns.<sup>25</sup> Moreover, Beijing aims to use military signaling through air and naval drills and blockade rehearsals, coupled with narrative messaging, to convince the Taiwanese public of the futility of resisting China's eventual takeover of the island.<sup>26</sup>

AI will likely play a critical role in advancing China's psychological warfare ambitions, in part by enhancing the scale and sophistication of influence operations.<sup>27</sup> Our data reveals that the PLA is requesting AI systems capable of generating persuasive synthetic media, automating content production, and tailoring disinformation to specific audiences. In general, machine learning models also support the rapid analysis of massive datasets, including social media behavior, public sentiment, and demographic patterns, to identify perceived cognitive vulnerabilities and optimize messaging strategies. Combined with advances in natural language processing and deepfake generation, these capabilities could allow Beijing to conduct more sophisticated cognitive domain operations. Ultimately, the PLA sees AI-enabled psychological warfare not only as a support tool but also as a decisive means of shaping the strategic environment and achieving political objectives without resorting to open conflict.<sup>28</sup>

## Deepfake Requests

One notable finding was the presence of RFPs for the development, installation, and testing of AI-enabled, or "intelligent," deepfake systems. One request called for the creation of an "intelligent deepfake system" that would identify and collate open-source video, audio, images, and text (in at least ten languages) to create a "fake

sample library.” The library would support keyword searches for images and video, as well as cross-modal retrieval of content based on descriptions of objects, attributes, and behaviors. It would also allow for the faces and heads of people in videos to be replaced with samples from the library, as well as generate synthetic scenes with both video and voice audio. The information in this request reveals the sophistication of the PLA’s deepfake-related efforts, as a deepfake library would make it easier to create manipulated content quickly and efficiently, smoothing the way for its use in future conflicts.

While deepfake generation may attract more attention, the PLA also requested deepfake detection capabilities. A request for a deepfake detection module specified that the system should be able to detect deepfakes of people in both images and videos, as well as identify when heads and faces have been replaced. Interestingly, the RFP also called for four different deepfake detection models and three deepfake detection benchmark datasets, which appear aimed at creating a system of interlocking capabilities and technologies to better detect a wide range of synthetic, manipulated content.

In addition to systems that could be easily used in international contexts, the dataset also included requests for deepfake systems for domestic applications. For example, one request solicited portable deepfake systems for use in Tibet, a region where local authorities have invested heavily in surveillance technologies.<sup>\*29</sup> The use of artificial media could presumably be used to manipulate public opinion in Tibet. There were also a number of requests for the use of deepfakes as part of larger propaganda systems. One document requested portable deepfake systems for use alongside AI-enabled translation loudspeakers, drones for public address, and vehicle-mounted speakers. While the PLA focuses primarily on external security tasks, there is evidence that it provides technology to police and local officials who conduct surveillance and enforcement in regions such as Tibet.<sup>30</sup>

## **Cognitive Targeting and Information Campaigns**

Aside from deepfakes, our dataset reveals the PLA’s ongoing interest in developing a range of technologies to identify and target adversaries’ perceived cognitive domain vulnerabilities. One request called for LLM-powered gathering of internet-wide “cognitive domain information,” including deep analysis of targets for cognitive domain operations. The system appears aimed at performing comprehensive analyses of

---

\* A number of RFPs requested technologies for use in Tibet and Xinjiang, regions about which the Chinese government has long had security concerns.

various targets' online footprints in order to influence them. It could also, however, be used to perform analysis of specific populations' reactions to various events or situations, thus helping the PLA, or Chinese government, guide and shape public perceptions and sentiments. Such technologies could aid the Chinese military in influencing public, as well as elite, perceptions of various events, a key aspect of psychological warfare as outlined by the PLA.<sup>31</sup> China is already experimenting with cognitive targeting campaigns. It recently doxxed nearly 20 Taiwanese military officers whom Beijing accused of disseminating "separatist" propaganda by publishing the officers' sensitive personal information, including names and identification numbers.<sup>32</sup>

Another document requested a social engineering technique simulation platform. Social engineering is the use of psychological manipulation to cause people to divulge sensitive information or otherwise compromise security. This system, consisting of multi-agent and parallel simulation capabilities, is aimed at developing social engineering techniques and behavior simulation capabilities to identify and exploit adversarial vulnerabilities. While social engineering is often associated with cyber operations, we include it here due to its potential utility for accessing sensitive information that could then be used for cognitive domain operations.

The PLA's efforts extend beyond sentiment analysis to modeling future cognitive domain operations. For instance, there was a request for an advanced cognitive operations platform designed to model, simulate, and visualize activities in cyberspace. The system aims to support "cognitive countermeasure" tasks, likely information and influence operations, by creating scenario-based models and visualizations of information dissemination within online social networks. The RFP included requests for "network traces, social circle topology," security configurations, and communication patterns to map online communities, hierarchies, individual and group behaviors, and social connections. The system is aimed at displaying how information spreads across networks, how public opinion evolves, and how influence campaigns unfold. It appears as though the system is intended to give operators tools for understanding, predicting, and shaping behavior in the information domain.

In sum, the dataset reveals that the PLA is investing in a range of technologies and tools to manipulate public opinion, identify cognitive vulnerabilities in various groups, and then target those perceived weaknesses in a variety of ways.

## Intelligence, Surveillance, and Reconnaissance

The term intelligence, surveillance, and reconnaissance refers to a military's efforts to understand the operating environment—especially the capabilities and activities of adversaries, but also of neutral or civilian actors in an area of ongoing or potential operations. ISR is enabled by military and civilian sensor data obtained from many sources, such as satellite sensor data, electromagnetic sensor data from drones, or text or video from social media websites. Given the vast amount of information available to commanders, ISR tasks are a promising application area for AI. The sections that follow give a sense of the PLA's widespread efforts to enhance sensing and surveillance using novel data gathering and sensor fusion approaches, as well as emerging techniques, including AI.

Among the RFPs, we noted several themes such as common sensor modalities, the importance of maritime and undersea sensing, and an emphasis on sensing objects in space. We discuss observations for each of these themes below.

### ***Cross-Cutting Intelligence and Sensing Capabilities***

The PLA is pursuing AI applications to make better use of diverse data types—text, quantitative data (including financial information), video, audio (including speech recognition and synthesis, specifically), infrared data, hyperspectral imagery, radio signals, and more. Critically, many of the RFPs made clear the PLA's intent to use AI to fuse information across sources and data types.

While most AI applications in our analysis focused on specific military domains (air, sea, ground, space, cyber, or cognitive), several RFPs had a cross-domain scope. For example, we identified RFPs for AI systems to “achieve rapid intelligent translation of Ukrainian language texts, documents, and images,” as well as to translate English-language documents and images.<sup>33</sup> We also found proposals for AI-enabled synthesis of open-source, text-based information, either purchased or otherwise acquired, with a focus on policy changes, technological trends, foreign laboratory research, think tank reports, epidemic dynamics, or “special events.”

In addition to textual analysis, there were detailed RFPs seeking AI-enabled audio and video analysis that listed English translation as a key capability. These included translating streaming audio and video content in real time, extracting text from audio and video for further analysis, comparing video subtitles and AI-generated translations, automating video and audio annotation, assisting audio and video searches, recognizing logos in videos, recognizing the voices of key leaders in audio

recordings, and automating monthly and weekly reports on gathered information. Additionally, one RFP specified a need for “business data resource aggregation and storage” as well as “access and storage of key open-source data resources” on businesses.

Beyond common open-source data types like text, audio, and video, we identified numerous requests for AI applications to process data from military and commercial sensors—including optical, infrared, hyperspectral, radio frequency, and geomagnetic. These RFPs fall into three categories of increasing sophistication. First, the PLA seeks to use AI to enhance weak or degraded returns from individual sensors. Second, it wants systems that combine data from multiple sensors to locate and identify objects, particularly ground targets viewed from air or space platforms, as discussed in the previous section. Third, and most ambitiously, it is pursuing multi-modal fusion capabilities that integrate results across different sensor types, including drone-mounted cameras, thermal imagers, as well as military, civilian, and even foreign-owned satellite optical sensors, to achieve a more fulsome understanding of military platforms and even multiple moving objects (such as drone swarms).

### ***Maritime Sensing\****

Of the PLA RFPs related to ISR, a notable number focused on maritime domain awareness (MDA). MDA is concerned with “the effective understanding of anything associated with the maritime domain that could impact security, safety, the economy or the marine environment.”<sup>34</sup> These applications are dual-use; the task of tracking undersea fish migrations overlaps with that of detecting undersea vehicles, just as the task of mapping the seabed can be useful for environmental research, as well as deep sea mining or mapping undersea cables.<sup>35</sup> Given China’s long coastline, territorial claims in the East China Sea, South China Sea, and Taiwan, and the threat Beijing may perceive from U.S. naval forces, one of the PLA’s most vital missions is to monitor and counter threats at sea. It is difficult, if not impossible, to know if a maritime-associated RFP might be used for research, routine safety, or military purposes; however, since each solicitation is a request from the PLA, and the fact that China has a strong interest in ocean surveillance for military operations, we assume that there is an intended military or security application.

---

\* While surveillance and targeting tasks have some overlap, we distinguish targeting from surveillance RFPs by identifying requests that explicitly mention “target” or describe systems designed to find, identify, and track specific objects. For unclear cases, we classified RFPs as related to surveillance where they mentioned information gathering or did not make an explicit link to targeting tasks or the need for target quality data.

AI-related RFPs that sought to improve China’s MDA were mostly concerned with establishing a baseline for normal operations. These included the characterization, measurement, and mapping of the maritime environment—tasks that are useful to both civilian and military operations, and are essential for detecting anomalies. Many of the proposed applications we found are relevant to conducting safe operations at sea. Weather prediction for vessels on the ocean, for example, is a widely discussed application for AI and one that we saw repeatedly in the PLA’s requests. We also identified several RFPs for machine learning models that support predictions of tides, currents, waves, and fog. Furthermore, we observed many requests seeking to characterize routine traffic patterns at sea based on the international maritime Automatic Identification System (AIS).\*

### ***Undersea Sensing***

China is concerned about the superior capabilities of U.S. submarines, which tend to be more difficult to detect than their Chinese counterparts.<sup>36</sup> The quantity of AI-related RFPs we found concerned with underwater detection and the undersea environment seemed to echo what we know of China’s interest in capabilities to counter U.S. submarines, which could play a significant role in a Taiwan contingency.<sup>37</sup> These RFPs included MDA-related big data collection and AI projects to characterize the steady state of underwater ocean noise, enable oceanographic mapping, determine underwater salinity profiles, map global ocean surface temperatures, and predict underwater temperatures and thermoclines (the latter two are important for sonar operations and underwater communications in addition to maritime research, fishing, and weather prediction). The quantity of data required to establish these baselines and the compute required to use it for prediction and anomaly detection are substantial enough that we also saw specific requests for data storage and computing resources to support these projects. While in some cases the use of AI techniques to analyze the data collected was not explicit, we included these requests because of the clear potential for current or future AI applications.

Beyond general maritime awareness projects, we also found specific AI-enabled detection RFPs, including algorithms to help identify and track objects in the ocean using sonar data. Other documents revealed the PLA’s ambition to develop a “global underwater marine environment dynamic analysis system” that utilizes satellites to collect sea surface height and temperature data. The combination of AI-enabled maritime domain awareness and object identification and tracking could pose a

---

\* AIS data is typically used for safety of navigation at sea. Most, but not all, vessels will broadcast their location, course, and speed using the AIS system.

substantial challenge to international navies seeking to respond to the PLA's maritime operations with submarines and unmanned underwater vehicles.

### ***Space Sensing***

As with maritime domain awareness, militaries, commercial firms, and global research institutes also conduct space domain awareness (SDA) to find and track objects in space and perform space weather forecasting. Both sensors in orbit and on the ground enable SDA. While we did not identify many requests to apply AI to SDA, those we found were largely focused on collecting data that could support AI training or to which AI could eventually be applied. These included fusing data collected by satellites to create better awareness of objects in space, to help project orbits of satellites, and to predict the likely capabilities and payloads of satellites on orbit. The interest in knowing or predicting the capabilities of satellites in orbit goes beyond the technical specifications of the satellites to also include information on the capacities for commercial and military satellite systems for sensing and/or communication. Additionally, we found a handful of initiatives to improve space weather and coronal mass ejection (solar flare) predictions. As discussed earlier, there were also a number of RFPs for space targeting.

### ***Surveillance***

Over the past several years, China has spent more on internal security than defense.<sup>38</sup> Focused on suppressing dissent and ensuring social stability, the Chinese Communist Party has become a pioneer in a range of mass surveillance techniques and technologies, many of which it has aimed at religious and ethnic minorities in Tibet and Xinjiang, among other areas. While these regions rightly receive most of the international community's attention, since they are where advanced technologies are commonly deployed to facilitate extensive human rights violations, it is worth noting that most, if not all, large Chinese cities are blanketed in surveillance cameras replete with facial and gait recognition capabilities for broader social control, law enforcement, and public security measures.<sup>39</sup>

Analysis of China's internal surveillance often concentrates on its population control practices, which is not a primary mandate of the PLA. That said, many RFPs we reviewed reveal that the PLA is utilizing a range of technologies to secure military installations, monitor the internet, and surveil individuals—possibly its own soldiers—as part of its efforts to counter insider threats.

## Security Systems and Surveillance

The PLA is seeking a range of AI-enabled security systems. Several RFPs related to military installation security featured everything from basic perimeter alerts to an integrated system for identifying individuals and their movements on or around those installations.\* These surveillance systems, the requirements for which were strikingly similar to one another, featured a range of cameras and sensors aimed at identifying and surveilling vehicles and personnel entering, navigating around, and exiting military installations. Several requested license plate readers, vehicle chassis inspection technologies, facial recognition cameras, fingerprint scanners, and vehicle and pedestrian access gates, as well as enabling equipment such as data collection devices, IT systems, and requisite power supplies.

Other RFPs concerned multi-faceted security systems. For example, one request specified the need for over 1,000 cameras of varying types, including “wearable pinhole” cameras and those equipped with infrared night vision capabilities. On top of this, it requested over 250 drones and over 130 pairs of smart translation glasses. Another document called for a perimeter warning subsystem that would include multiple drones and intrusion alarms, while another “smart monitoring subsystem” would feature video surveillance, data collection, and emergency command capabilities. Other documents requested the integration of electromagnetic shielding products and signal jammers to protect military installations. Should bases be infiltrated, another RFP called for the provision of different alarms indicating an intrusion, attack, or hijacking, among other emergencies.

## Identifying and Surveilling Individuals and Vehicles

Many RFPs requested advanced facial recognition technologies. One document called for technologies that could perform facial recognition on people wearing masks, while another solicited facial recognition capabilities complete with “anti-spoofing features” powered by high-resolution, night vision-enabled cameras.

Relatedly, one request included facial recognition cameras and “liveness” detection systems, as well as visitor registration terminals that could connect to and exchange real-time information with the Ministry of Public Security’s Mobile Police System private networks. Finally, some requests called for technically sophisticated cameras capable of detecting the presence of humans and small UAVs in real time at a distance

---

\* Most of the documents we reviewed related to base security suggested the installations were in Mainland China, but the technologies could also be useful in international contexts.

of greater than three kilometers. The same document requested vehicle detection capabilities at greater than 10 kilometers. Detecting was a common request, but so too was tracking. Some requests noted the need for technologies to track the trajectory, in real time, of at least 350 vehicles at once. Others requested cameras with an “erroneous capture rate” of less than one in 10 million and the ability to identify someone through a picture of the side of their face (at 60 degrees) with up to 97 percent accuracy.

On top of the recognition technologies, several RFPs called for vast quantities of storage for face- and vehicle-related data. For example, one request called for the capacity to store at least five million vehicles and five million faces.

While facial recognition and vehicle detection were quite frequently mentioned across the documents, there were also examples of requests for audio and speech recognition capabilities, as well as gait analysis systems.

### **Digital Surveillance**

On top of these surveillance applications, which were primarily geared toward military installations and base security, there were a number of requests for technologies to surveil computers, phones, and other electronic devices more broadly. It is difficult to discern, however, whether the intended targets of digital surveillance are PLA employees, Chinese civilians, or other individuals.

One RFP, for example, called for “deep inspection” capabilities that could delete or recover information from phones and apps. More interestingly, the document requested the capability to extract information on cloud-stored data from “uninstalled” or “irrecoverable” applications, as well as to analyze WeChat and Alipay financial data to detect whether owners had engaged in gambling. Finally, it solicited AI-enabled automatic recognition of “illegal” images stored on phones.

A different document called for an AI-powered tool to screen the online footprints of thousands of people, which could be for monitoring PLA personnel’s digital activities. Such capabilities, however, could be used for more general surveillance. The request included real-time scanning of WeChat Moments, Douyin, and Weibo, among other popular Chinese apps and websites, to collect information on users’ posts and videos. Moreover, the request asked for identifying information like phone numbers and registration traces to track whether people are participating in online gambling and gaming, as well as using VPNs.

One of the most interesting requests was for the use of generative models to monitor the internet for indications of another COVID-like virus outbreak. One RFP specified the requirements for an LLM-powered system to “detect early signs and related signals of infectious disease events...based on network data.” Another document requested a “pathogen monitoring and early warning algorithm.”

Finally, there were a number of requests for surveillance drones, but those will be covered in greater depth in a forthcoming paper. Of particular interest here, however, are the surveillance-focused robotics systems that appear in our dataset. Alongside general solicitations for a “surveillance robot,” some requests called for robotic dogs for observation and surveillance.

## Communications, Computers, and Cyber

For modern militaries, communication networks, computers, and cyber operations are related and essential to achieving and maintaining information dominance. Together, these systems allow for the collection, distribution, and processing of information that ranges from simple emails to the high-fidelity data streams required for precision strikes.

### ***Communications***

Modern militaries depend on robust communication networks for critical functions, from video teleconferences to rapid data transfers in remote locations. These networks must work across multiple domains and mediums. Because these communication networks are so critical to successful military operations, the networks themselves are often targeted, including by electromagnetic energy, directed energy, and cyberattacks.

One particular challenge for military communications is the rapid and secure transfer of high-quality sensor information across the networks of different platforms. Differing hardware and messaging formats between platforms or allies, as well as the need to add or remove network participants as they may join or leave an operation—to say nothing of enemy efforts to jam or disrupt communications—create ongoing and complex configuration issues and security concerns in the midst of already stressful scenarios. Similar challenges arise when coordinating drone swarms—a technically demanding task requiring robust, agile communications between drones and their controlling units so they can operate as a cohesive force.

The PLA, like other militaries, is pursuing solutions to these communications challenges. We found requests for several specific applications that may be leveraging AI: enabling distributed and cooperative battlefield networks for both platforms and individual soldiers, creating autonomous broadband networks for data transfer between surface and airborne platforms, and developing AI for collaborative engagements, as well as data transfers by and within heterogeneous unmanned swarms and satellite constellations. We also saw requests for technical solutions for managing and moving data across different networks. While solutions to these network-switching RFPs may not involve the use of AI (it was difficult to discern from the RFP language), solving the challenge of network management for multiple autonomous platforms is a key enabler of battlefield autonomy and future AI applications.

## Communication Interference and Electronic Warfare

While AI offers powerful applications that enhance communications, it equally presents opportunities to interfere with an adversary's comms networks. For example, the PLA requested an AI-enabled communication monitoring system that might find and correlate enemy transmissions. Similarly, it solicited AI solutions to help detect and analyze ultra-shortwave communication signals using weak supervision, a machine learning technique.

Beyond mere detection, some AI-related RFPs fell into the category of electronic warfare, where militaries attempt to degrade enemy operations by intercepting, jamming, or destroying communication signals and devices.<sup>40</sup> As one example of these types of applications, the PLA has requested AI-enabled tools to detect and interfere with satellite communication signals. It has also requested the development of a library of algorithms for communication interference, research on signal identification for interference purposes, and intelligent algorithms that would counteract jamming or interference activities by an enemy.

## *Cyber*

According to the Pentagon, China aims to use offensive cyber operations to degrade adversarial command and control (C2) systems, hamstring logistics operations, and disable critical infrastructure to hamper an enemy's decision-making and slow its pace of operations.<sup>41</sup> States also use cyber espionage to collect information and copy valuable technologies, develop countermeasures to new technologies, understand and counteract enemy war plans, establish baseline activity patterns, and collect intelligence on specific individuals. Cyber operations are key enablers of China's "system destruction" concept, and succeeding in cyberspace could lead the PLA to realize multiple advantages across other domains.<sup>42</sup> The recent Salt and Volt Typhoon cyber campaigns indicate that China is already using advanced cyber capabilities to monitor U.S. telecommunications and, potentially, disrupt U.S. critical infrastructure.<sup>43</sup>

At the same time, fortifying cyber defenses is equally important, and many cyber intrusions are difficult to detect before it is too late. Given that AI relies on computer networks, the importance of protecting these networks will only grow. Chinese scholars often note the difficulty of guaranteeing network and cyber security in peace and wartime, and the PLA appears to be investing in technologies that it hopes will afford its computer networks a greater chance of survival in future conflicts.<sup>44</sup>

To be successful, China must use cyber offense and defense together to degrade

adversarial military systems while denying its opponents the same opportunity.

We found a number of RFPs related to offensive and defensive cyber activities. Many of the RFPs described sophisticated software systems, and we cannot be sure that the PLA is applying AI in all of these cases. Where RFPs mentioned an intent to collect large amounts of data to use in cyber offense or defense, we erred on the side of inclusion in our analysis based on what we know of modern efforts to apply AI for cyber operations, though more detailed studies of the PLA's application of AI to the cyber domain are warranted.<sup>45</sup>

### **Secure Network Operations and Maintenance**

Before considering exquisite cyber capabilities, it is important to note that there is a tremendous amount of routine work that must be done by any military to establish, maintain, and secure the communications and cyber networks that enable everything from back-office operations to precision strikes. A number of RFPs in the dataset highlighted the importance of network operations and maintenance tasks and seemed to indicate early experimentation with AI to help with data fusion, data visualizations, and anomaly detection. Many of these tasks can already be addressed, at least in part, with modern cybersecurity software. The RFPs we reviewed for network operations and maintenance seldom mentioned AI techniques explicitly, but the vast majority included requests for big data collection and analysis.

Some examples of the RFPs related to secure network operations and maintenance included:

- Systems that provide intrusion detection and “intrusion prevention capabilities, as well as capabilities for monitoring, detecting, seeking out, and destroying network viruses;”
- Systems to intelligently enhance communication networks;
- Requests to visualize network traffic data so that human operators can better identify anomalies or make more informed decisions when managing and securing networks;
- Requests to develop AI tools to detect cyber backdoors; and
- Requests to automatically collect data on network activity and take defensive actions against a discovered vulnerability.

The PLA also sees an opportunity to use AI to monitor or surveil network accounts for suspicious behavior. Many of the RFPs relevant to network surveillance are routine for cybersecurity purposes. The capabilities described could also be used to monitor any user's activities, be they PLA personnel who may pose insider threats, Chinese citizens, or foreign spies. For example, we found requests to monitor mobile phones and establish users' potential to pose a risk to the PLA, but it was unclear from the RFP if "users" referred to PLA employees or other individuals. One such request sought to establish "scoring of and early warning about personnel, based on the number or severity of dangerous websites they are registered on," as well as "monitoring of risky app installation and use, and of risky websites." The websites of concern included those where malware and scams are prevalent but are also sites that might make a person vulnerable to extortion, such as online gambling, online loans, and adult content platforms. One request included a proposal to apply AI to content monitoring of livestreamed videos. Several projects requested the monitoring of any VPN activities as well as any efforts by a user to access overseas content.<sup>46</sup>

## **Cyber Offense and Defense**

In addition to the passive monitoring and scanning of networks to detect intrusions or suspicious activities, there is a category of cyber activities often described as active defense. One document requested an "active cyber defense" platform that could execute tasks including "threat hunting," or searching for intruders on a network, using "honeypots" to lure intruders to observe their habits and targets, tracing intruders back to their point of origin, and other aggressive countermeasures. The RFP also sought a platform that included "network deception [and] attack origin tracing...that effectively withstands cyberattacks and provides technical verification to improve network cyber defense capabilities." Moreover, the same request sought to "support dynamically generating and issuing strategy templates based on active defense plans and tasks"—in other words, helping operators select appropriate defenses against intruders and illuminate different future cyber actions based on an intruder's past behavior.

Another RFP identified an interest in using AI for stress-testing and measuring the performance of various encryption techniques. This capability could be leveraged to better secure Chinese networks. However, there is also potential for offensive applications. Notably, at least one of the encryption standards mentioned in the RFP text (MISTY) is probably a reference to MISTY1, a cryptographic standard used by the government of Japan from 2003 through 2013. The RFP also refers to Feistel, a cryptographic technique that underlies many widely used encryption algorithms, both outdated (Lucifer, DES, Skipjack, CAST, MISTY1) and current (Blowfish, Twofish, LOKI, KASUMI). Of note, the current U.S. encryption standard, AES, is not a Feistel-based

algorithm. This interest in Feistel and MISTY1 suggests the PLA's desire to gain access to not only current encrypted communications material, but perhaps also historical collections of encrypted material.<sup>47</sup>

Relatedly, we observed two quantum-related cyber defense RFPs. One request sought quantum-resistant cryptography algorithm testing capabilities, likely aimed at discerning whether cyber defense software could withstand quantum-based cyberattacks. The second request was for a measurement system for quantum computer software. Together, these RFPs indicate the Chinese military's interest in preparing for quantum-enabled threats, both by testing the resilience of existing cryptographic systems and developing tools to assess emerging quantum software capabilities.

Altogether, our review of RFPs related to communications and cyber demonstrates that China is actively seeking and experimenting with a wide variety of solutions to protect their networks and probe the networks of others. These findings further substantiate cybersecurity professionals' warnings about the potential for AI to render cyberspace less secure and the urgent need to adopt AI solutions for cyber defense.<sup>48</sup>

## Takeaways

Our review of these PLA RFPs provides a partial but detailed view of how the Chinese military's rhetoric on AI is translating into specific AI system acquisition requests. The information and trends in these documents will help guide strategic responses to the challenges posed by the PLA's ongoing AI adoption. Although the RFPs we reviewed offer insights on the technologies and capabilities the PLA is interested in developing or acquiring, they do not reveal whether the proposals produced workable solutions that were adopted. Measuring the PLA's AI adoption is beyond the scope of this paper, but we hope that our RFP analysis provides other researchers with some indication of where to look for adoption trends. These limitations aside, our analysis reveals several notable takeaways:

- **The PLA is actively pursuing AI-related technologies for a broad range of C5ISRT applications.** There are RFPs to apply AI to C5ISRT tasks in all domains, including space, cyber, and cognitive. Requests range from large, multi-modal strategic decision support systems to narrow sensor-enhancement tools, and ISR-related data processing tasks, among other applications. The PLA is seeking to fuse diverse data sources from proliferated sensors through the use of multiple models with an eye toward speeding and improving military decision-making. Its extensive pursuit of AI for C5ISRT reflects Beijing's continued emphasis on military intelligentization.
- **Many of the RFPs are likely trial procurements or reflect prototyping efforts.** Their smaller budget values may indicate that the PLA is trying out certain experimental systems and has low expectations for each project's success. At the same time, the PLA is likely using these publicly available RFPs to rapidly procure AI-related capabilities from vendors outside of China's traditional defense industrial base. It is not surprising that Beijing would look to the commercial sector for advanced technologies given China's rise as a global technology powerhouse.<sup>49</sup>
- **Some of the PLA's public RFPs are surprisingly transparent and specific, even regarding domains and use cases that are usually opaque and secretive.** These documents reveal the Chinese military's intent to adopt cutting-edge capabilities, including for orbital warfare, offensive cyber operations, population and digital surveillance, and cognitive domain targeting. The Chinese government and military usually restrict information about sensitive technologies and military capabilities, so it is notable that the PLA publishes thousands of RFPs that illustrate the specifics of its AI-related priorities. This

openness is likely aimed, at least in part, at sourcing advanced capabilities from vendors beyond China's traditional defense industrial base.<sup>50</sup>

- **The PLA appears to be emphasizing AI applications to counter U.S. military advantages.** There was, for instance, a persistent focus on using AI-related technologies to improve China's maritime domain awareness capabilities, which could help the PLA counter U.S. naval power. Moreover, we analyzed a number of documents related to the use of emerging technologies in space, including those aimed at augmenting China's space-based capabilities and blunting the U.S. military's advantages in that domain.
- **Requests related to AI-enabled decision support systems (AI-DSS) indicate the PLA's interest in machine-aided decision-making.** While many militaries are developing such systems, the PLA may be particularly interested in using AI-DSS to address its lack of trust in the decision-making skills of its officer corps.<sup>51</sup> Furthermore, the RFPs demonstrate an interest in expansive tools for predicting, discerning, and reacting to political events and social movements for a broad range of contingencies, capabilities that could be useful in both domestic and international contexts. For example, we came across several requests aimed at performing internet-wide sentiment analysis to inform responses to emergencies and other unforeseen events.
- **The PLA is seeking ever-more sophisticated technologies to surveil individuals in the physical and digital domains and execute cognitive domain operations.** There were a number of RFPs for facial, gait, and vehicle recognition technologies, as well as digital surveillance tools to monitor individuals' online presence and even recover previously deleted information from mobile devices. Moreover, the preponderance of requests for deepfake generation and detection systems, as well as cognitive targeting technologies, reveals the PLA remains intent on developing emerging technology-enabled psychological warfare tools.
- **Relatedly, many RFPs specify rapid acquisition timelines, often of only three to six months.** The speed at which the PLA requires some contractors to provide technologies and capabilities suggests that it is experimenting widely and is eager to understand what works or fails in various operational environments. Such accelerated timelines could aid the PLA in prototyping and experimentation, which might lead to faster iteration and adoption of cutting-edge AI-related technologies. That said, many (though not all) RFPs mandate that bidding companies have operated for at least three years, sidelining potentially innovative newcomers.

## Implications for the United States

Our analysis suggests that China is taking meaningful steps to advance the development and adoption of military AI. While myriad Chinese government documents and military strategists discuss the importance of AI in bolstering China's comprehensive power and relative strengths, these documents demonstrate that Beijing is backing up its words with concrete steps in technology acquisition, though we do not have information on the technical quality or performance of these systems in testing or operational environments. This has several implications for U.S. policymakers and defense planners:

**First, the PLA's efforts to use emerging technologies to redress perceived capability gaps with the U.S. military underscore the importance of the United States' efforts to maintain its lead in the space and undersea domains, as well as in sensing technologies.** Many of the RFPs we reviewed focused on sensing and surveillance applications, especially related to maritime domain awareness and space, where enhanced Chinese capabilities could directly challenge U.S. naval and space superiority. This emphasis highlights the need to monitor PLA technical experimentation in these domains and rapidly innovate to maintain U.S. advantages in space and at sea.

**Second, while Beijing believes that AI-DSS could improve the PLA's military decision-making, an overreliance on such systems could augment the risks of miscalculation and escalation.** Despite the difficulties associated with discussing responsible military AI use with Beijing, the U.S. government should engage Chinese officials in dialogue on the responsible use of AI-DSS. While it is unlikely that the two sides will strike binding agreements, discussions could eventually contribute to the establishment of norms around AI-DSS use. Such discussions could help prevent or at least mitigate AI-induced misunderstandings that might inadvertently lead to miscalculations or escalations.

**Third, the United States may need to rethink how to send credible military and diplomatic signals to China as the PLA expands its use of AI-DSS.** The PLA is experimenting with AI systems that ingest vast quantities of open-source data to assess international political and social conditions, anticipate potentially consequential geopolitical events, and inform its responses. Should the Chinese military and/or government come to rely on these systems to interpret and respond to geopolitical events, the United States will have to develop new approaches to conducting diplomatic and military signaling to maintain deterrence and avoid miscalculation in an AI-enabled age.

**Fourth, AI seems poised to supercharge the PLA’s investments in surveillance and cognitive domain operations.** The Chinese military continues to invest in AI-enabled surveillance and cognitive targeting technologies. The PLA’s apparent embrace of deepfakes and deepfake management systems should spur policy action and R&D on detection technologies and countermeasures for cognitive domain operations in peacetime and in crises. Public education and public-private partnerships are a critical first step, but Washington could also amplify efforts to develop technical standards and forgery detection technologies as counters to the PLA’s efforts.

**Fifth, China’s pursuit of commercial technologies on rapid acquisition timelines should reinforce the Pentagon’s efforts to reform its own acquisition process.<sup>52</sup>** Numerous RFPs required project completion within three to six months after contract signing. These quick turnaround times reflect Beijing’s intent to quickly determine which technologies and capabilities are viable and which are not. They also promote rapid iteration and experimentation, which could lead to improved military capabilities in short timeframes, much as we have seen in Ukraine. Unlike in Ukraine, however, many RFPs include a requirement for bidding firms to have at least three years of operating experience. In contrast, Western militaries have established ties with startups through initiatives like the U.S. Defense Innovation Unit (DIU) and NATO’s Defence Innovation Accelerator for the North Atlantic (DIANA).\*

**Sixth, relaxing export controls on advanced, U.S.-origin AI chips will make it easier for the PLA to develop and deploy AI-enabled C5ISR technologies and capabilities.** The dataset contains evidence that the PLA is seeking advanced chips designed by U.S. companies, including NVIDIA and AMD. Moreover, RFPs include requests to deploy LLMs trained using U.S. hardware, including those developed by DeepSeek.<sup>53</sup> Giving Chinese entities access to cutting-edge AI chips smooths the way for the PLA’s intelligentization efforts. Future CSET analysis will characterize the extent of PLA requests for technologies from U.S. semiconductor companies.

**Finally, the PLA’s acquisition programs demand continued open-source monitoring and analysis in order to better discern the strengths and weaknesses of China’s efforts, any changes in focus or direction, and indications that certain AI capabilities are already in use.** Such analysis is essential not only for tracking technological progress, but also for understanding how acquisition patterns reflect organizational learning, risk tolerance, and the PLA’s evolving concepts of operation.

---

\* Not every RFP contract includes a three-year requirement. We know from the RFPs, for example, that China is requesting models from DeepSeek, which was founded in 2023.

## Conclusion

This paper makes use of a novel dataset of more than 9,000 RFPs published by the PLA in 2023 and 2024. These RFPs cover a broad range of goods and services related to AI, including language and vision models; autonomous vehicles; virtual and augmented reality platforms; data collection, management, and analysis systems; smart manufacturing and robotics; and more.

This first paper in our series about the PLA's AI-related RFPs focuses on those related to C5ISRT in the air, sea, ground, space, cyber, and cognitive domains. We find that the PLA is experimenting with AI across all domains and a wide range of applications, including the use of some systems for population and digital surveillance, as well as cognitive domain operations. We cannot, however, ascertain the extent to which the PLA is successfully adopting these technologies to gain a competitive advantage. At a minimum, it is clear from our analysis that the PLA is broadly experimenting with and prototyping potential AI-related solutions in support of its military modernization objectives.

The findings in this paper demonstrate that, despite trailing the United States in frontier AI model development, China is working to adopt a suite of AI technologies for military use. Just because U.S. AI companies continue to lead the world with the most advanced generative AI models does not mean the U.S. military will out-compete the PLA in AI deployment. This paper should serve as further encouragement to military leaders to stay ahead in responsible AI adoption, as well as in responsible AI innovation.

## Authors

**Emelia Probasco** is a senior fellow at CSET.

**Sam Bresnick** is a research fellow and an Andrew W. Marshall fellow at CSET.

**Cole McFaul** is a senior research analyst and an Andrew W. Marshall fellow at CSET.

## Acknowledgments

The authors would like to thank Igor Mikolic-Torreira, John Bansemer, Drew Lohn, Julie George, Lauren Kahn, Mike Brown, Nathan Beauchamp-Mustafaga, and an anonymous reviewer for their feedback on this report. They also thank Matt Mahoney for fact-checking, Daniel Chou for data support, Danny Hague, Lauren Lassiter, Shelton Fitch, and Susan Moynihan for editorial support, Ben Murphy for translation assistance, and Jason Ly for help with graphic design.



© 2026 by the Center for Security and Emerging Technology. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc/4.0/>.

Document Identifier: doi: 10.51593/20250006

## Appendix: Methodology to Identify AI-related RFPs

This report draws from a dataset of over 9,000 AI-related RFPs published by the PLA between January 2023 and December 2024. Almost all of the documents in this dataset were Procurement Announcements (采购公告), Public Disclosures of Procurement Intent (采购意向公开), Request for Quotations (询价), and Open Tenders (公开招标). These documents all concern the PLA's solicitation of proposals for a set of defined capabilities from potential suppliers, so we use the term RFP throughout this report to encompass these documents.

To determine the AI-relatedness of a document, we employed the methodology developed for our first report using AI-related procurement documents, "Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage."<sup>54</sup> We used a combination of human-curated AI-related keywords and an LLM model with a standardized system prompt to assess whether each procurement document was AI-related. We used OpenAI's GPT-4.1-mini model for this project. For more on this methodology and for the full list of AI-related keywords used, see Appendix B1 in "Pulling Back the Curtain on China's Military-Civil Fusion."

We use the following definition for an AI-related procurement document:

"Excluding medical systems, any award notice that may involve the development or deployment of AI-enabled systems (such as machine learning or decision-making software), hardware that may incorporate or enable AI-enabled systems (such as autonomous vehicles or specialized AI chips), or data collection, processing, or labeling."

For each AI-related RFP, we used the GPT-4.1-mini model to translate the title and text into English, and extracted key details about the project from the text of the document. We manually validated the accuracy of the LLM translations and data extraction for a subset of the documents.

## Endnotes

<sup>1</sup> *Science of Military Strategy 2020*, Translation, In Their Own Words (China Aerospace Studies Institutes, 2022), <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf>; J. Michael Dahm, *China C4ISR and Counter-Intervention: Hearing on China's Evolving Counter Intervention Capabilities and Implications for the U.S. and Indo-Pacific Allies and Partners*, U.S.-China Economic and Security Review Commission, 2024, <https://www.mitchellaerospacepower.org/app/uploads/2024/03/03.21.24-PLA-C4ISR-USCC-Testimony.pdf>.

<sup>2</sup> Josh Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," *Cyber Defense Review*, Fall 2024, [https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Baughman\\_CDRV9N3-Fall-2024.pdf](https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Baughman_CDRV9N3-Fall-2024.pdf).

<sup>3</sup> Mark Cozad, Jeffrey Engstrom, Scott W. Harold, Timothy R. Heath, Sale Lilly, Edmund J. Burke, Julia Brackup, and Derek Grossman, *Gaining Victory in Systems Warfare: China's Perspective on the U.S.-China Military Balance* (RAND Corporation, 2023), [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RRA1500/RRA1535-1/RAND\\_RRA1535-1.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1500/RRA1535-1/RAND_RRA1535-1.pdf); Stew Magnuson, "SPECIAL REPORT: China Pursues Its Own Version of JADC2," *National Defense*, July 13, 2023, <https://www.nationaldefensemagazine.org/articles/2023/7/13/china-pursues--its-own-version-of--jadc2>.

<sup>4</sup> *Military and Security Developments Involving the People's Republic of China 2022*, Annual Report to Congress (Office of the Secretary of Defense, 2022), 39, <https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>.

<sup>5</sup> *Military and Security Developments Involving the People's Republic of China 2024*, Annual Report to Congress (Office of the Secretary of Defense, 2024), 30, <https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF>.

<sup>6</sup> *Military and Security Developments Involving the People's Republic of China 2022*, Annual Report to Congress (Office of the Secretary of Defense, 2022), 39, <https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>.

<sup>7</sup> Jacob Stokes, *Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition*, Center for a New American Security, 2024, <https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition>.

<sup>8</sup> B.A. Friedman, "Finding the Right Model: The Joint Force, the People's Liberation Army, and Information Warfare," *Journal of Indo-Pacific Affairs* 6, No. 3 (March–April 2023): 1–17.

<https://www.airuniversity.af.edu/JIPA/Display/Article/3371164/finding-the-right-model-the-joint-force-the-peoples-liberation-army-and-informa/>.

<sup>9</sup> Cole McFaul, Sam Bresnick, and Daniel Chou, “Pulling Back the Curtain on China’s Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage” (Center for Security and Emerging Technology, September 2025), <https://cset.georgetown.edu/publication/pulling-back-the-curtain-on-chinas-military-civil-fusion/>.

<sup>10</sup> McFaul et al., “Pulling Back the Curtain on China’s Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage.”

<sup>11</sup> Nathan Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States* (RAND Corporation, 2023), [https://www.rand.org/pubs/research\\_reports/RRA853-1.html](https://www.rand.org/pubs/research_reports/RRA853-1.html).

<sup>12</sup> Emelia Probasco, Helen Toner, Matthew Burtell, and Tim G. J. Rudner, “AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks” (Center for Security and Emerging Technology, April 2025), <https://cset.georgetown.edu/publication/ai-for-military-decision-making/>.

<sup>13</sup> Emelia Probasco, “Building the Tech Coalition” (Center for Security and Emerging Technology, August 2024), <https://cset.georgetown.edu/publication/building-the-tech-coalition/>.

<sup>14</sup> Graham Webster et al., “Full Translation: China’s ‘New Generation Artificial Intelligence Development Plan’ (2017),” *DigiChina*, August 1, 2017, <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>.

<sup>15</sup> Patrick Tucker, “AI Is Helping the Pentagon Go from Finding Targets to Predicting Threats,” *Defense One*, May 13, 2025, <https://www.defenseone.com/technology/2025/05/ai-helping-pentagon-go-finding-targets-predicting-threats/405279/>; Kateryna Bondar, “Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare,” Center for Strategic and International Studies, March 2025, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250306\\_Bondar\\_Autonomy\\_AI.pdf?VersionId=E2h8uqROea77udoc\\_og82HWsrfgfJRTZ](https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250306_Bondar_Autonomy_AI.pdf?VersionId=E2h8uqROea77udoc_og82HWsrfgfJRTZ); Elizabeth Dwoskin, “Israel Built an ‘AI Factory’ for War. It Unleashed It in Gaza,” *The Washington Post*, December 29, 2024, <https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/>.

<sup>16</sup> Office of the Chairman of the Joint Chiefs of Staff, “Joint Publication 3-60: Joint Targeting,” September 28, 2018, [https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint\\_Staff/21-F-0520\\_JP\\_3-60\\_9-28-2018.pdf](https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/21-F-0520_JP_3-60_9-28-2018.pdf).

<sup>17</sup> Naval Air Systems Command, “Virtual Agent for Data Fusion and Understanding,” Navy SBIR 25.2 Topic N252-089 (pre-release), April 2, 2025, [https://navysbir.com/n25\\_2/N252-089.htm](https://navysbir.com/n25_2/N252-089.htm).

<sup>18</sup> Ryan D. Martinson, “Exposed Undersea: PLA Navy Officer Reflections on China’s Not-So-Silent Service,” Center for International Maritime Security, June 24, 2025, <https://cimsec.org/exposed-undersea-pla-navy-officer-reflections-on-chinas-not-so-silent-service/>.

<sup>19</sup> “Foreign Ministry Spokesperson Zhao Lijian’s Regular Press Conference on July 4, 2022,” People’s Republic of China Ministry of Foreign Affairs, July 4, 2022, [https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202405/t20240530\\_11347316.html](https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202405/t20240530_11347316.html).

<sup>20</sup> 2025 Annual Threat Assessment of the U.S. Intelligence Community, Intelligence Community Annual Threat Assessment (Office of the Director of National Intelligence, 2025), <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2025/4058-2025-annual-threat-assessment>.

<sup>21</sup> “Foreign Ministry Spokesperson Zhao Lijian’s Regular Press Conference on July 4, 2022,” People’s Republic of China Ministry of Foreign Affairs, July 4, 2022, [https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202405/t20240530\\_11347316.html](https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202405/t20240530_11347316.html).

<sup>22</sup> Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*.

<sup>23</sup> Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*.

<sup>24</sup> Huynh Tam Sang, Tong Thai Thien, and Le Thi Yen Nhi, “How Taiwan Fights the Disinformation War,” *The Interpreter*, by the Lowy Institute June 20, 2024, <https://www.lowyinstitute.org/the-interpreter/how-taiwan-fights-disinformation-war>.

<sup>25</sup> Yimou Lee, “Taiwan Says China Using Generative AI to Ramp Up Disinformation and ‘Divide’ the Island,” Reuters, April 8, 2025, <https://www.reuters.com/world/asia-pacific/taiwan-says-china-using-generative-ai-ramp-up-disinformation-divide-island-2025-04-08/>.

<sup>26</sup> Brian Kerg, “Think China Can Already Take Taiwan Easily? Think Again..,” *Atlantic Council*, April 14, 2024, <https://www.atlanticcouncil.org/blogs/new-atlanticist/think-china-can-already-take-taiwan-easily-think-again/>.

<sup>27</sup> Nathan Beauchamp-Mustafaga, Kieran Green, William Marcellino, Sale Lilly, and Jackson Smith, *Dr. Li Bicheng, or How China Learned to Stop Worrying and Love Social Media Manipulation* (RAND Corporation, 2024), [https://www.rand.org/pubs/research\\_reports/RRA2679-1.html](https://www.rand.org/pubs/research_reports/RRA2679-1.html).

<sup>28</sup> Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*.

<sup>29</sup> Congressional-Executive Commission on China, *The Human Rights Situation in Tibet and the International Response: Hearing before the Congressional-Executive Commission on China*, 116th Cong., 2nd sess., 2020, <https://www.congress.gov/event/116th-congress/joint-event/LC68497/text>.

<sup>30</sup> Ashu Mann, “Inside Tibet’s Digital Prison: PLA and Police Merge to Enforce China’s Grip – Analysis,” *Eurasia Review*, October 5, 2025, <https://www.eurasiareview.com/05102025-inside-tibets-digital-prison-pla-and-police-merge-to-enforce-chinas-grip-analysis/>.

<sup>31</sup> For more on this, see Brett V. Benson and Brett J. Goldstein, "The Fog of AI: What the Technology Means for Deterrence and War," *Foreign Affairs*, January 6, 2026, <https://www.foreignaffairs.com/china/fog-ai>.

<sup>32</sup> "China Offers Cash Bounties for Information on Taiwanese Military Officers," *Al Jazeera*, October 11, 2025, <https://www.aljazeera.com/news/2025/10/11/china-offers-cash-bounties-for-information-on-taiwanese-military-officers>.

<sup>33</sup> There were requests for translation systems for a number of languages, including Russian, Japanese, Korean, and Vietnamese, as well as Uighur and Tibetan, among others.

<sup>34</sup> "Maritime Domain Awareness," International Maritime Organization, n.d., accessed August 4, 2025, <https://www.imo.org/en/ourwork/security/pages/maritime-domain-awareness.aspx>.

<sup>35</sup> For more on the overlap between China's research and economic and defense activities in Maritime Domain Awareness, see Matthew P. Funaiole, Brian Hart, Aidan Powers-Riggs, "Surveying the Seas: China's Dual-Use Research Operations in the Indian Ocean," Center for Strategic and International Studies, January 10, 2024, <https://features.csis.org/hiddenreach/china-indian-ocean-research-vessels>.

<sup>36</sup> Martinson, "Exposed Undersea: PLA Navy Officer Reflections on China's Not-So-Silent Service."

<sup>37</sup> Gabriel Honrada, "China's AI Sea Grid Aims to Render US Subs Transparent," *Asia Times*, October 20, 2025, <https://asiatimes.com/2025/10/chinas-ai-sea-grid-aims-to-render-us-subs-transparent/>.

<sup>38</sup> "China Spends More on Controlling Its 1.4bn People than on Defense: Silencing Dissent Also Nips Innovation in the Bud," *Nikkei Asia*, August 29, 2022, <https://asia.nikkei.com/static/vdata/infographics/china-spends-more-on-controlling-its-1-dot-4bn-people-than-on-defense/>; Chris Buckley, "China Internal Security Spending Jumps Past Army Budget," *Reuters*, March 5, 2011, <https://www.reuters.com/article/world/china-internal-security-spending-jumps-past-army-budget-idUSTRE7222RA/>.

<sup>39</sup> Vivian Wang, "China's Security State Sells an A.I. Dream," *The New York Times*, November 4, 2025, <https://www.nytimes.com/2025/11/04/world/asia/china-police-ai-surveillance.html>.

<sup>40</sup> Electronic warfare also encompasses activities that go beyond communications; for example, jamming the homing devices on a missile to prevent it from striking a target. For more on the elements of electronic warfare, see: Office of the Chairman of the Joint Chiefs of Staff, "Joint Publication 3-13.1: Electronic Warfare," February 8, 2012, [https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional\\_Reading/1C4\\_Mod\\_5\\_JP\\_3-13-4\\_MILDEC.pdf](https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C4_Mod_5_JP_3-13-4_MILDEC.pdf).

<sup>41</sup> *Security Developments Involving the People's Republic of China* 2024, 86, 95.

<sup>42</sup> Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (RAND Corporation, 2018),

[https://www.rand.org/pubs/research\\_reports/RR1708.html](https://www.rand.org/pubs/research_reports/RR1708.html); Magnuson, “SPECIAL REPORT: China Pursues Its Own Version of JADC2.”

<sup>43</sup> Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*, In Focus IF12798 (Congressional Research Service, 2025), <https://www.congress.gov/crs-product/IF12798>; PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Joint Cybersecurity Advisory AA24-038A (Cybersecurity and Infrastructure Security Agency, 2024), [https://www.cisa.gov/sites/default/files/2024-03/aa24-038a\\_csa\\_prc\\_state\\_sponsored\\_actors\\_compromise\\_us\\_critical\\_infrastructure\\_3.pdf](https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf).

<sup>44</sup> Sam Bresnick, “China’s Military AI Roadblocks: PRC Perspectives on Technological Challenges to Intelligentized Warfare” (Center for Security and Emerging Technology, June 2024), <https://cset.georgetown.edu/publication/chinas-military-ai-roadblocks/>.

<sup>45</sup> Andrew J. Lohn, “Anticipating AI’s Impact on the Cyber Offense-Defense Balance” (Center for Security and Emerging Technology, May 2025), <https://cset.georgetown.edu/publication/anticipating-ais-impact-on-the-cyber-offense-defense-balance/>.

<sup>46</sup> Several requests that may be relevant to cyber defense efforts are included in our review of intelligence, surveillance, and reconnaissance RFPs.

<sup>47</sup> “A List of Cryptographic Algorithms to Be Referenced for Procurement in Electronic Government (CRYPTREC Cryptographic List) [電子政府における調達のために参照すべき暗号のリスト (CRYPTREC 暗号リスト)]”, Digital Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy Trade and Industry, March 30, 2023, [https://www.digital.go.jp/assets/contents/node/information/field\\_ref\\_resources/9ad4ff87-b673-4f3d-a2f5-8750525f9502/ae43fdf7/202330\\_get-involvedprocedure\\_outline\\_02.pdf](https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/9ad4ff87-b673-4f3d-a2f5-8750525f9502/ae43fdf7/202330_get-involvedprocedure_outline_02.pdf); “Overview of China’s Commercial Cryptographic Algorithm Standards,” Institute of Commercial Cryptography Standards, March 17, 2025, [https://niccs.org.cn/niccs/Notice/pc/content/content\\_1937429502295019520.html](https://niccs.org.cn/niccs/Notice/pc/content/content_1937429502295019520.html).

<sup>48</sup> See, for example, “Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign,” *Anthropic*, November 13, 2025, <https://www.anthropic.com/news/disrupting-AI-espionage>.

<sup>49</sup> McFaul et al., “Pulling Back the Curtain on China’s Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage.”

<sup>50</sup> McFaul et al., “Pulling Back the Curtain on China’s Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage.”

<sup>51</sup> Sam Bresnick, “The Obstacles to China’s AI Power,” *Foreign Affairs*, December 31, 2024, <https://www.foreignaffairs.com/china/obstacles-china-ai-military-power>.

<sup>52</sup> “Secretary of War Announces Acquisition Reform,” U.S. Department of Defense, November 10, 2025, <https://www.war.gov/News/Releases/Release/Article/4329487/secretary-of-war-announces-acquisition-reform/>.

<sup>53</sup> Sam Bresnick and Cole McFaul, “China Wants an AI-Powered Military Built with Nvidia Chips, and That’s a Problem,” *The Hill*, December 3, 2025, <https://thehill.com/opinion/technology/5630281-nvidia-china-military-chips/>.

<sup>54</sup> McFaul et al., “Pulling Back the Curtain on China’s Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage.”