THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

June 1, 2023

Private Eyes:

China's Embrace of Open-Source Military Intelligence

Information about the author, Zoe Haver, can be found at the end of this report.

Executive Summary

The People's Liberation Army (PLA) is using new collection, processing, and analysis technologies to exploit the massive amount of open-source information[1] available from the internet and other sources for military intelligence purposes. A growing ecosystem of private companies, state-owned enterprises, state-run research organizations, and universities is supporting the PLA's push to leverage open-source intelligence[2] (OSINT) by providing research services, platforms, and data. China's military and defense industries are using automated web crawlers, algorithms, machine learning, artificial intelligence, and other tools to extract intelligence from foreign governments, militaries, social media platforms, news media organizations, companies, research organizations, and individuals. The PLA very likely employs OSINT alongside other, more sensitive forms of intelligence to support decision-making at the strategic, operational, and tactical levels. The PLA's use of OSINT very likely provides it an intelligence advantage, as the West's open information environment[3] allows the PLA to easily harvest large quantities of open-source data, whereas Western militaries must contend with China's closed information environment. This report offers an overview of Chinese views on military OSINT, details how the PLA applies and collects OSINT, and profiles several private companies that provide OSINT to the PLA.

Key Findings

- The PLA almost certainly views OSINT as an increasingly valuable source of military intelligence that can support decision-making and necessitates the use of new collection, processing, and analysis technologies, which the PLA and China's defense industry are actively developing.
- The PLA uses OSINT to gain insight into foreign military capabilities, facilities, doctrine, decision-making, weapons, equipment, science and technology, exercises, training, intelligence, and deployments, which very likely helps the PLA prepare for future conflicts.
- In an effort to leverage external capabilities and expertise, the PLA increasingly acquires OSINT research and analysis services, platform and database products, and remote sensing data from private Chinese companies as well as from Chinese state-owned enterprises, state-run research organizations, and universities.
- The PLA and China's defense industry almost certainly take advantage of other countries' open information environments to extract OSINT from foreign governments, militaries, universities, defense industry companies, scientific research organizations, think tanks, news media outlets, social media platforms, forums, individuals, commercial data providers, print media, radio broadcasts, satellites, and other sources.
- The PLA very likely tries to learn from other countries' OSINT programs while also seeking to prevent foreign countries from collecting military OSINT from Chinese sources, which very likely helps preserve the PLA's advantage over the West in OSINT.

Table of Contents

Methodology

This report draws from an original data set of PLA and Chinese defense industry procurement records that we built using the Recorded Future® Intelligence Cloud and other tools. To create this data set, we collected military OSINT-related procurement records that were published between January 2019 and January 2023. The data set, which identifies 50 projects, can be viewed in Appendix A.

In addition to procurement records, our analysis draws from a variety of other publicly available Chinese-language sources, including academic writings and articles published in PLA media outlets. For academic sources, we focused on academic papers that discuss military or general OSINT and were authored by individuals affiliated with the PLA, China's defense industry, or other relevant institutions. For media sources, we focused on articles published in PLA-run publications like PLA Daily (解放军报), China National Defense News (中国国防报), and Military Reporter (军事记者). The sources cited throughout the report do not necessarily represent official PLA, Chinese Communist Party, or Chinese government policies; rather, they demonstrate how individuals situated within these institutions likely view and engage with OSINT. This analytical approach is necessary because the Chinese party-state is a paranoid and secretive system that does not readily release information about its internal concepts, regulations, and decision-making, particularly regarding intelligence.

Chinese Views on OSINT

PLA personnel and other observers in China almost certainly consider OSINT to be an increasingly valuable form of military intelligence that requires harnessing new technologies, and acknowledge that China can draw lessons from the development of OSINT in the United States (US). Some observers believe that China should mobilize civilian organizations to support OSINT efforts, while others have highlighted the need for China to guard against foreign countries' OSINT collection. These themes are detailed below.

- **OSINT is an increasingly valuable form of military intelligence**. The PLA and other entities in China have long valued OSINT,[4] particularly for science and technology intelligence.[5] However, PLA personnel and other Chinese observers have almost certainly recognized that the dawn of the internet era, as well as the commercialization of technologies like remote sensing and automatic identification systems (AIS), have produced new opportunities to expand and improve military OSINT.[6] For example, according to a 2020 paper by personnel affiliated with Unit 31008 (31008部队) of the Central Military Commission (CMC; 中央军事委员会) Joint Staff Department (JSD; 联合参谋部), the development of information technology has facilitated continuous, automated military OSINT collection from internet sources such as government, military, scientific research, and higher education organizations as well as from companies and individuals.[7] They argue that this internet-based OSINT is an effective source of information on operational forces, equipment construction, operational capabilities, military exercises, battlefield environments, and other topics.[8] The authors claim that this intelligence helps improve operational capabilities and supports command decision-making.[9] The CMC JSD is responsible for command and control, planning and strategy, intelligence collection and analysis, and other such missions;[10] we observed multiple instances of Unit 31008 researching or procuring OSINT.[11]

- **Effective OSINT requires harnessing new data collection, processing, and analysis technologies**. PLA personnel and other Chinese observers almost certainly understand that China must apply new data collection, processing, and analysis technologies to effectively capitalize on the massive amount of open-source information that is available on the internet.[12] For example, in 2017, researchers affiliated with the China Academy of Electronics and Information Technology (CAEIT; 中国电子科学研究院) published a paper titled "Study of Web Open Source Intelligence Topic Mining in Military Domain", in which they argue traditional methods of manual intelligence processing and analysis are insufficient for dealing with the quantity of open-source data collected from the internet.[13] As such, they propose a method of using a web crawler to collect information from the internet, employing technical means to extract key information, and then leveraging an algorithm to generate intelligence topics.[14] Using their method, they generate example intelligence topics like "China-Japan Air Forces East China Sea Confrontation", "THAAD [Terminal High Altitude Area Defense] Deployment in South Korea", and "US Air Raid on Syrian Base".[15] CAEIT is a subsidiary of China Electronics Technology Group Corporation (CETC; 中国电子科技集团公司), a major state-owned defense contractor.[16]

- **China can learn from the development and application of OSINT in the US**. PLA personnel and other observers are very likely studying the development and use of OSINT in the US to inform China's own OSINT efforts.[17] For example, in 2022, a PhD candidate and lecturer affiliated with the PLA National Defense University (NDU) College of Politics Department of Military Information and Internet Public Opinion (国防大学政治学院军事信息与网络舆论系) published a paper that repeatedly cites various US and North Atlantic Treaty Organization (NATO) regulations, standards, handbooks, and other materials in an effort to promote military OSINT standards development in China.[18] The author argues that China needs such standards to address issues like insufficient quantitative intelligence analysis, intelligence system integration, and intelligence planning.[19] The author's goal is to make intelligence work more systematic, standardized, and scientific.[20] NDU is subordinate to the CMC and is the PLA's only "comprehensive joint command university"; it is responsible for high-level leadership training and its staff have used data platforms to collect "international defense" data to produce OSINT reference materials in support of teaching and research.[21]

- **Civilian organizations should contribute to China's OSINT work**. Some specialists in China have suggested mobilizing civilian organizations (such as think tanks and private companies) to provide OSINT support for China's intelligence system, which includes military intelligence.[22] For example, in 2019, national security intelligence and national security researchers affiliated with the University of International Relations (国际关系学院) published a paper in which they argue that China's intelligence system should integrate OSINT contributions from the government, the military, intelligence agencies, and organizations in the civilian space.[23] They suggest that OSINT has high information technology requirements and that, when the technologies of the government and intelligence agencies are insufficient, China's national security intelligence system should turn to "business outsourcing", "technical customization", and "market procurement",[24] practices which the PLA has already adopted in its drive to mobilize civilian companies.[25] The authors note that, while the participation of civilian organizations in China's OSINT work can make China's intelligence sources more extensive and comprehensive, the government and intelligence agencies should still guide this intelligence system to ensure secrecy.[26] The University of International Relations is allegedly affiliated with the Ministry of State Security (MSS), China's primary civilian intelligence agency.[27]

- **China must be vigilant against foreign OSINT collection efforts**. Some observers in China have expressed concerns related to the threat of foreign entities collecting OSINT from Chinese sources.[28] For example, in 2020, the deputy director of the PLA News Propagation Center Department of Public Opinion Information (解放军新闻传播中心舆情信息部) published an article warning that foreign intelligence agencies collect and analyze "military secrets" from public media reports.[29] The author suggests that this risk has grown in recent years because, in the current digital media era, intelligence can easily be collected through comprehensive analysis of big data.[30] They identify a handful of security mistakes that enable foreign OSINT collection such as not distinguishing between internal and external propaganda; publishing unprocessed pictures and video of equipment sites and internal structures; speculating about the parameters and performance of high-precision weapons; using satellite imagery to analyze military bases and equipment construction; and analyzing equipment specifications and testing processes.[31] The PLA News Propagation Center is subordinate to the CMC Political Work Department (政治工作部) and oversees PLA publications like PLA Daily, China National Defense News, and Military Reporter.[32]

OSINT Applications

The PLA very likely uses OSINT to support decision-making,[33] which is in line with how the PLA applies other forms of military intelligence.[34] When doing so, the PLA very likely integrates OSINT with human intelligence, signals intelligence, measurement and signature intelligence, imagery intelligence, and other kinds of intelligence.[35]

The aforementioned 2020 paper by CMC JSD personnel offers insight into how the PLA very likely uses OSINT to support decision-making.[36] The authors argue that military intelligence collected from the internet provides big data support for commanders' "comprehensive judgements" and "command decision-making", and that it is relevant to the strategic, campaign (operational), and tactical levels of war.[37] At the strategic level, they claim that OSINT offers insight into areas like military strategy, political trends, and social and economic factors.[38] At the campaign level, the CMC JSD personnel suggest that OSINT provides information on topics such as military intentions, command and coordination, and organization.[39] At the tactical level, the authors state that OSINT is relevant to subjects like order of battle, deployment, weapons, and equipment.[40]

Beyond supporting decision-making, Chinese observers have suggested more specific uses for military OSINT as well, such as carrying out long-range maritime target tracking,[41] enabling early warning of crises,[42] supporting precision strikes,[43] countering enemy propaganda,[44] facilitating domestic science and technology innovation,[45] and supporting training and talent development.[46]

Our original data set of PLA and Chinese defense industry OSINT-related procurement records, which is available in Appendix A, provides additional insight into how the PLA uses OSINT. Trends that we observed in PLA entities' procurement of OSINT are identified below.

- PLA entities pursue OSINT on foreign military capabilities, facilities, doctrine, decision-making, weapons, equipment, science and technology, exercises, training, intelligence, and deployments.

- PLA entities also seek OSINT on geopolitical trends, foreign think tanks, foreign defense industry companies, general science and technology developments, and other non-military topics.

- Specific subjects of PLA interest include the US military's distributed ground intelligence equipment; US and German main battle tanks; armored equipment used by the US, India, and Taiwan; the operational concepts and equipment of the US Marine Corps and Taiwan Marine Corps; foreign military cyber and electromagnetic domain technologies; foreign unmanned aerial and ground vehicles; the strategies, equipment, and technologies of foreign navies and coast guards; and foreign research on hypersonics, artificial intelligence, quantum information, and other strategic technologies.

- PLA entities are interested in OSINT related to specific targets, subjects, and issues in countries like the US, Taiwan, Japan, Australia, South Korea, the United Kingdom (UK), France, Germany, India, and Russia.

- PLA entities procure OSINT platform and database products, research and analysis services, data from private and state-owned Chinese providers, foreign commercial data providers, and foreign primary source documents.

- Numerous different entities within China's armed forces procure OSINT, including entities belonging to the CMC JSD, PLA Strategic Support Force (PLASSF), PLA Ground Force (PLAGF), PLA Navy (PLAN), PLA Air Force (PLAAF), PLA Academy of Military Science (AMS; 军事科学院), and PLA National University of Defense Technology (NUDT; 国防科技大学).

OSINT Collection

When carrying out military OSINT collection on the internet, Chinese entities very likely prioritize automated collection methods such as the use of web crawlers. Using such technical collection methods, these entities very likely collect intelligence from targets like foreign governments, militaries, universities, think tanks, media outlets, social media platforms, and commercial data providers.

Collection Methods

PLA and Chinese defense industry specialists have been actively developing and researching the use of web crawlers to address the challenges of OSINT collection. In addition to the aforementioned paper by CAEIT researchers on OSINT internet collection and topic generation, we observed several other instances of similar research.

- In 2022, researchers affiliated with the Nuclear Power Research Institute of China (中国核动力研究设计院), which is subordinate to state-run defense contractor China National Nuclear Corporation (中国核工业集团),[47] published a study on building an open-source military nuclear intelligence collection system based on an open-source web crawler framework.[48]

- In 2021, researchers associated with the Jiangsu Automation Research Institute (江苏自动化研究所), also known as the China State Shipbuilding Corporation (CSSC) 716th Research Institute (第七一六研究所),[49] published a paper in which they propose a method of tracking foreign aircraft carriers, submarines, destroyers, and other naval vessels using an OSINT system that combines a web crawler, entity recognition tools, AIS data from foreign providers, and other inputs.[50]

- In 2020, a senior engineer affiliated with the Navy Equipment Department Maritime Equipment Comprehensive Planning Bureau Equipment Finance Office (海装综合计划局装备财务处) published a study on a big data-based OSINT feature extraction algorithm that uses text, image, audio, and video data collected by a web crawler.[51]

- In 2019, researchers affiliated with the Army Service Academy (陆军勤务学院), a logistics-focused institution within the PLAGF,[52] published a paper in which they propose collecting OSINT from the internet using a web crawler, processing this data using machine learning, and then organizing it into a foreign military OSINT database.[53]

In addition to researching new OSINT collection methods, the PLA and China's defense industry are also almost certainly already applying similar technical methods. For example, in September 2020, an entity associated with AMS published a tender for a "science and technology intelligence research methods and capabilities improvement" project.[54] The entity wanted to use "advanced and mature technologies" such as web crawlers, data mining, machine translation, and natural language processing to complete “overall automated service process construction” for the comprehensive collection, automatic translation, and intelligence analysis of internet science and technology intelligence information.[55] The entity indicated that these improvements would change the current situation of traditional intelligence, which relies on methods such as manually browsing domestic and foreign websites, manually pasting and downloading information, manual translation, and single data statistics.[56] The project was intended to “help intelligence researchers have a comprehensive, accurate, and in-depth grasp of intelligence information in fields that they follow”.[57] It would also shorten the intelligence collection, processing, and analysis cycle; improve the efficiency and level of intelligence research work; and improve existing science and technology research capabilities.[58]

In April 2022, an unspecified PLAGF entity published a tender for a “foreign military XX [redacted] weapons and equipment development trend tracking and analysis system”, which demonstrates how the PLA is almost certainly applying OSINT collection technologies, as well as processing and analysis technologies, to monitor and assess foreign military capabilities.[59] The entity was trying to obtain a system that uses OSINT collected from the internet to realize “automated monitoring and tracking, collection and acquisition, and data processing, distribution, and use”.[60] It wanted “a software system that integrates internet open-source intelligence data collection, analysis and retrieval, automatic translation, and local area network [LAN]-integrated distribution”.[61]

The project included both an OSINT data collection system and a LAN management and distribution system.[62] The collection system was supposed to be able to automatically capture website information; support RSS news collection and HTML news collection; collect multiple types of data from websites including text information, URL, numbers, dates, pictures, PDF files, audio, and video; and support functions such as the automatic cleaning and translation of data.[63] The LAN system involved the integrated distribution of data to a LAN system after having gone through formatting conversion, data importing, and other processes.[64] It also involved a data retrieval function that allows front-end users to perform unified queries of collected data; to directly obtain full texts, translations, and attachments of sources; and to narrow queries using keywords, websites, classifications, and other modifiers.[65]

Collection Targets

The PLA and PLA contractors almost certainly collect OSINT from foreign governments, militaries, universities, defense industry companies, scientific research organizations, think tanks, media outlets, social media platforms, forums, individuals, commercial data providers, print media, radio broadcasts, satellites, and other such sources.[66] The aforementioned 2019 study by China’s Army Service Academy researchers includes a table (translated below) of foreign military OSINT information sources, which provides examples of likely PLA OSINT collection targets.[67] The sources are organized into the categories of international organizations, government departments, military organizations, scientific and teaching organizations, published media, intelligence consulting, and global security and defense think tanks. Target sources identified in the table are located in the US, Japan, European Union, Israel, Russia, and elsewhere.[68] Specific targeted entities include the United Nations Security Council (UNSC), NATO, European Defense Agency (EDA), US Congress, White House, National Aeronautics and Space

Administration (NASA), US Department of Defense (DOD), US National Defense University, US Defense Acquisition University, US Army University, US Army War College, US Marine Corps University, US Naval War College, ProQuest, Janes, and the Center for Strategic and International Studies (CSIS), among others.[69]

International Organizations	Government Departments	Military Organizations	Scientific and Teaching Organizations	Published Media	Intelligence Consulting	Global Security and Defense Think Tanks
UNSC	US military laws compilations	US military regulations	US National Defense University	Open-source military books	IQPC weapons systems conferences	US Center for International and Strategic Studies [likely referring to CSIS]
UN treaty compilations	US Congress military and national security bills	US DOD supervision publications	US Defense Acquisition University	Foreign open-source military periodicals and materials	SMI weapons systems conferences	US Global Security Institute
NATO standard terms	US signed international treaties	US DOD budget information	US Army University	Taiwan military periodicals	DMS defense market services reports	Russian International Affairs Council
NATO military standards	US White House	US DOD	US Army War College	EBSCO military periodicals	TEAL weapons and equipment technology analysis reports	Carnegie Europe Center
EDA	US national strategy documents	US military standards	US Marine Corps University	Russian military and security periodicals	Janes CBRN weapons evaluation intelligence	Israeli Institute for National Security Studies
NATO organizational publications	NASA reports	US DOD military terms dictionaries	US Naval War College	ProQuest military periodicals	Janes military and technology intelligence	Japan Institute of International Affairs
NATO defense reports	PB reports [likely referring to "Program / Budget"]	US military orders	US Army University [repeat]	DDN defense periodicals	Janes defense periodicals	Indian Centre for Land Warfare Studies

***Table 1**: Translated foreign military OSINT information sources table (Source: Wang and Xia, "Analysis and Implementation of Foreign Military Open Source Intelligence Database Based on MADL")*

In addition to the 2019 paper from the Army Service Academy researchers, we observed further evidence of the PLA using foreign commercial data for OSINT. For example, in 2019, AMS sought to procure foreign military information from UK-based Janes,[70] and an unspecified PLAN entity sought such information from Janes in 2021.[71] Likewise, in the same year, AMS appears to have pursued OSINT on strategic emerging technologies like artificial intelligence, quantum information, and hypersonics using data from Clarivate,[72] a company headquartered in the UK.[73] Moreover, the aforementioned OSINT-based maritime target tracking system that CSSC 716th Research Institute researchers proposed in 2019 integrated AIS data from foreign providers like MarineTraffic, FleetMon, and

VesselFinder.[74] Unlike the PLAN, US Navy vessels sometimes broadcast AIS signals, allowing observers in China to track them.[75]

The PLA is also possibly using remote sensing data from foreign government and commercial satellites for OSINT. In November 2020, the PLA Navy Submarine Academy (海军潜艇学院) published a single-source procurement announcement for synthetic aperture radar (SAR) data from foreign satellites.[76] The academy was trying to acquire this data through the Chinese Academy of Sciences Aerospace Information Innovation Institute (中国科学院空天信息创新研究院) and specifically wanted "directional observational survey data" on a specific area.[77] Whether the Navy Submarine Academy wanted this SAR data for OSINT purposes is unclear, but it likely could have used the data to assess foreign military facilities or analyze maritime operating environments.[78] Similarly, in October 2020, an unspecified PLASSF entity sought to acquire SAR remote sensing data from the TerraSAR-X, RADARSAT-2, and "ALOS" (almost certainly referring to the ALOS-2) satellites.[79] TerraSAR-X is a commercial SAR observation satellite operated by the German Space Center (DLR) and Germany's Federal Ministry of Education and Research (BMBF), with a European space industry company managing the satellite's commercial operations.[80] RADARSAT-2 is a commercial Earth observation radar-imaging satellite funded by the Canadian Space Agency (CSA) and operated by MacDonald, Dettwiler and Associates Ltd (MDA).[81] ALOS-2 is an earth observation satellite that serves both commercial and scientific users and is operated by the Japan Aerospace Exploration Agency (JAXA).[82] It is unclear how the PLASSF entity wanted to use this SAR remote sensing data.[83] Recorded Future has previously observed PLA entities using commercial remote sensing data for the explicit purpose of supporting OSINT.[84]

OSINT Providers

Over the past decade, private companies have almost certainly become increasingly important participants in China's military OSINT ecosystem. This section profiles 5 private Chinese OSINT providers that serve the PLA, including providers that mainly sell platform and database products, providers that primarily offer research and analysis services, and providers that specialize in remote sensing data. These 5 companies and their respective corporate networks do not constitute the entirety of China's military OSINT ecosystem (which also includes state-owned enterprises, state-run research institutes, and universities) but they do offer examples of the growing role of private companies in this space.

Platform and Database Products

DataExa

DataExa, also known as Xiamen Yuanting Information Science and Technology Co., Ltd (厦门渊亭信息科技有限公司; 渊亭科技), is a privately owned Chinese defense contractor that serves as an OSINT platform provider for the PLA.[85] The company's OSINT platform appears to integrate artificial intelligence, machine learning, deep learning, and other elements to provide foreign military intelligence, as well as foreign science and technology intelligence, to platform users.

DataExa uses advanced technologies to support military clients in China. DataExa claims to be a pioneer and leader in “cognitive decision-making intelligence”.[86] The company says it has core technical advantages and leading engineering capabilities in knowledge graphs, image computing, reinforcement learning, machine learning, and deep learning.[87] It focuses on the industries of national defense, finance, government affairs, and industrial internet, and its clients reportedly include over 200 major organizations such as the CMC Science and Technology Commission, the CMC Equipment Development Department, PLA theater commands, the PLASSF, PLAN, and PLAGF.[88] The company reportedly began in 2013 with the “founding team” participating in “major cognitive graph construction work” for an unspecified national defense client,[89] and the company was then formally founded the next year in 2014.[90]

DataExa offers an OSINT platform oriented toward military intelligence as well as science and technology intelligence. This platform, called the “Tianji Intelligence Information Center Platform” (天机情报信息中心平台), is a “distributed strategic intelligence analysis platform” focused on foreign military intelligence collection and analysis.[91] The platform reportedly integrates crawler, automatic feature extraction, knowledge graph, deep learning, and intelligence question and answer technologies to “broaden open-source intelligence collection” and build a “high-quality intelligence logic information graph”.[92] It is intended to provide functions like intelligence archive materials management; foreign military intelligence collection; and intelligence mining, analysis, and determination.[93] These functions are designed to serve intelligence technical support units, intelligence organizations, and intelligence analysts, among other users.[94] In addition to foreign military intelligence, the platform also appears to include foreign scientific intelligence from targets like the US’s Defense Advanced Research Projects Agency (DARPA).[95]

DataExa claims that its OSINT platform can support operational decision-making.[96] The company emphasizes that its platform can help predict and analyze events, improve the efficiency of intelligence analysis, reduce labor costs, and increase analytical empiricism.[97] The company’s website highlights the joint staff department of an unspecified PLA theater command as a successful customer case for the platform, discussing how the platform facilitated big data intelligence analysis based on image, text, video, audio, and electromagnetic information.[98]

We observed at least 1 recent instance of DataExa winning an OSINT contract. On November 2, 2022, an unspecified entity likely belonging to the PLA announced that DataExa had come in first place during bidding for the “Open-source Information Normalization Services” project detailed in Appendix A, which focused on the regulations and capabilities of foreign ground forces.[99]

DataExa also owns numerous patents, including some with very likely OSINT applications.[100] The examples listed below, all of which were filed in 2021 or 2022, demonstrate DataExa’s ongoing efforts to improve its OSINT collection, processing, and analysis capabilities.

- Knowledge graph data extraction method and device based on web crawler (一种基于网络爬虫的知识图谱数据抽取方法及装置)[101]

- Visual integration device and method based on geographic information system (GIS) and knowledge graph and computing equipment (基于gis与知识图谱的可视化整合装置、方法及计算设备)[102]

- Military intelligence analysis visualization method and device and computer readable storage medium (军事情报分析可视化方法、装置以及计算机可读存储介质)[103]

Knowfar

Knowfar, also known as Beijing Nuofang Zhiyuan Information Science and Technology Co., Ltd. (北京诺方知远信息科技有限公司), is a private Chinese defense contractor that serves as an OSINT database provider for the PLA. The company offers a proprietary military OSINT database that very likely includes raw data, translations, and finished intelligence. We observed multiple instances of PLA units, including a PLASSF psychological warfare base, describing Knowfar as a well-known and uniquely qualified OSINT provider.

Knowfar, which was founded around 2009,[104] has business involving both research and databases. Knowfar's main research arm is the Knowfar Institute for Strategic and Defense Studies (KISDS; 知远战略与防务研究所).[105] The institute has a military translation center and intelligence data services center, and has research centers focused on maritime security; land-based forces; aerospace strategy; network-electromagnetic strategy; nuclear, biological, and chemical strategy; counterterrorism and overseas security; and national defense strategy.[106] The institute claims to engage with foreign universities and research organizations.[107] KISDS has published analyses on subjects like the US DOD Office of Net Assessment's research reports on China, Russia's efforts to implement national defense education in primary and middle schools, and radar stations in Japan's air early warning reconnaissance system.[108] KISDS also oversees the Knowfar Open-Source Center (知远开源中心),[109] which focuses on building a military data information platform and intelligence database with the goal of systematic, scientific, and standardized open-source defense data collection.[110] It aims to provide systematized and structured "strategic-campaign-tactical" OSINT database services to defense researchers and organizations.[111]

Knowfar's main OSINT database offering is very likely its "Foreign Military and Defense Open-Source Intelligence Database" (外军防务开源情报数据库).[112] This database, or at least its current website, appears to have been launched on September 28, 2020.[113] Though the database cannot be accessed without registration, it very likely includes modules like "personnel", "organizations", "meetings", "documents", "regulations", "open-source intelligence fusion", "military translated texts", "Knowfar periodicals", "defense periodicals", "Knowfar paper materials", and "situation map".[114] In addition to the aforementioned database, the website of the Knowfar Open-Source Center discusses 2 additional databases: the "Global Military Situation Intelligence Database" (全球军事态势情报数据库) and the

“Global Strategic Situation Intelligence Database” (全球战略态势情报数据库).[115] The links provided for these databases link directly to the Foreign Military and Defense Open-Source Intelligence Database website, which suggests that they are likely subcomponents of Knowfar’s main OSINT database product.[116] The Global Military Situation Intelligence Database reportedly covers the organizational structures, officers, weapons, equipment, and facilities of foreign militaries and can provide structured data support for wargames, academic research, and other use cases.[117] The Knowfar Open-Source Center reportedly covers political, military, economic, social, information, and infrastructure (PMESII) data for foreign countries.[118] Both the military and strategic situation intelligence databases use GIS technology to visually display structured data and support incident playback, situation plotting, and game demonstration functions.[119]

We observed numerous examples of Knowfar bidding on PLA OSINT contracts, as well as 2 instances in which PLA entities selected Knowfar via single-source procurement. These instances of single-source procurement indicate that the company provides unique and valuable OSINT to the PLA.

- **Knowfar Institute for Defense Studies Documents and Information**. According to a May 2019 single-source procurement announcement from Unit 61716 (61716部队), the unit was seeking information on military thought, strategy and tactics, force building, education and training, operational research, military history, military technology, weapons, and equipment from Knowfar and KISDS.[120] Unit 61716 is very likely a PLASSF psychological warfare organization known as 311 Base, which is reportedly responsible for targeting Taiwan.[121] The base wanted to install Knowfar’s defense translation database onto its LAN and access content through its LAN.[122] The base was interested in translated foreign military OSINT materials from the US, Russia, Japan, the UK, Australia, South Korea, and other major military countries.[123] It wanted the translated materials to cover the strategic, campaign, and tactical levels of war, as well as the sea, land, air, space, and cyber domains.[124] 311 Base justified its use of single-source procurement by stating that KISDS is highly professional and authoritative on military issues; has unique advantages; and has exclusive translated, researched, and copyrighted products.[125]

- **A Knowfar Database**. In March 2021, an unspecified PLA unit announced that it had selected Knowfar to provide a “Knowfar [unspecified] database” via single-source procurement.[126] According to the announcement, the database was independently developed and copyrighted by KISDS, which it describes as a well-known domestic military think tank.[127] The announcement further claims that KISDS is the only “social think tank” in China that has received “defense think tank qualification”.[128] As such, the entity decided to pursue single-source procurement with Knowfar.[129]

Additional examples of OSINT projects that Knowfar has bid on are listed below, with further details available in Appendix A.[130]

- Foreign Military OSINT Software Platform and Data Resources
- Documents and Materials Analysis Services Related to Intelligent Processing Equipment
- Foreign Military Intelligence Information Data Collection
- XX [redacted] Science and Technology Information Services[131]

Research and Analysis Services

Lanhai Changqing

Beijing Lanhai Changqing Information Science and Technology Co., Ltd. (北京蓝海长青信息科技有限公司), previously known as Beijing Lanhai Changqing Think Tank Science and Technology Consulting Co., Ltd. (北京蓝海长青智库科技咨询有限公司), is a privately owned PLA contractor that provides OSINT research services.[132] The company has bid on numerous contracts to provide the PLA with intelligence on the capabilities of the US military and other foreign militaries.

Beijing Lanhai Changqing Information Science and Technology Co., Ltd. is a new self-described think tank that provides research support to military clients. The company says it focuses on military-civil fusion innovation development as well as major issues related to military, security, science and technology, industry, and management.[133] It carries out theoretical research, strategy research, policy research, science and technology evaluation, and other similar activities to serve party, state, and military customers, as well as enterprises and social institutions.[134] The company claims to be "committed to becoming China's most influential military-civil fusion innovation think tank".[135] The company appears to be part of a broader "Beijing Lanhai Changqing Group" (北京蓝海长青智库) and has departments dedicated to research consulting, intelligence information, and expert coordination.[136] Corporate records indicate that it was established in March 2017.[137]

Beijing Lanhai Changqing Information Science and Technology Co., Ltd. almost certainly carries out research on foreign military and defense industry topics. Through at least September 2020, articles on "military-civil fusion", "strong military trends", and other subjects were posted to a website associated with Beijing Lanhai Changqing Information Science and Technology Co., Ltd.[138] For example, in June 2020, the website posted an analysis of the MK-48 Mod 7 Common Broadband Advanced Sonar System, a US Navy heavyweight torpedo.[139] In September 2020, it published an article on how Japan leverages civilian companies to develop its defense industry.[140] In March 2020, the website posted a piece on Russia's plans to develop a robot combat force.[141] We also observed an up-to-date "Lanhai Changqing Think Tank" blog hosted on NetEase,[142] which actively posts military capabilities and defense industry analyses and other similar content.[143]

We observed numerous instances of Beijing Lanhai Changqing Information Science and Technology Co., Ltd. bidding on likely PLA OSINT contracts, including contracts focused on the US military.[144] Examples of these projects are listed below, with further details available in Appendix A.

- US Military Standard Unmanned Aerial Vehicle In-Network Applications Information Organization and Analysis
- US Military Distributed Ground Intelligence Processing Equipment Technical Intelligence Information Special Topic Research
- Open-Source Intelligence Support Related to Network-Electromagnetic Confrontation Domain Strong Enemy Research
- US, Japan, India, and Australia Geostrategic Intelligence Collection and Analysis
- Foreign Country Ground Forces Unmanned Combat Equipment Intelligence Research
- World's Main Countries' Think Tanks Construction Situations and Operation Mechanisms Research
- Foreign Military Intelligence Information Data Collection
- 2022 Foreign Military Network-Electromagnetic Confrontation Domain Scientific and Technical Information Research

Techxcope

Techxcope, also known as Beijing Yuanwang Think Tank Science and Technology Consulting Co., Ltd. (北京远望智库科技咨询有限公司; 远望智库), is a privately owned PLA OSINT research services provider.[145] The company, which brands itself as a think tank, has a relatively prominent media presence.

Techxcope describes itself as integrating intelligence, consulting, and assessment.[146] According to its website, the company focuses on national security strategy, military strategy, and innovation strategy.[147] It also claims to prioritize "frontier technology" and "helping invigorate the country through science and technology, and strengthening the military through science and technology".[148] It has a future war and military requirements research center, high-level defense research institute, weapons and equipment development research center, future forecasting center, technology early warning center, net assessment center, and cyberspace research center.[149] It claims to provide decision-making consulting services and intellectual support to military organizations and the defense industry.[150]

Techxcope offers intelligence research services.[151] These services include source collection, translations, summaries, trend tracking, briefs, and research reports.[152] Techxcope also appears to produce written products with titles like "Electromagnetic Spectrum Warfare Research", "DARPA and Science and Technology Innovation", "Unmanned Aerial Vehicle Swarm Operations Technical Research", "Artificial Intelligence and National Security", "US Department of Defense Unmanned Systems Comprehensive Roadmap", "Hypersonic Weapons", and "6th Generation Fighters".[153] In addition to these services, the company claims to offer several platforms, including Military Resources Net (军事资源网), which appears to be a list of foreign military, defense industry, defense news, and security research entities and their publicly accessible websites, with short descriptions of each entity.[154]

Using its brand as a think tank, Techxcope has maintained a public media profile. Chinese media outlets have quoted Techxcope experts on topics like the communications capabilities of the Russian military, US Navy missile defense capabilities, and Russia's transfer of the S-400 surface-to-air missile (SAM) system to China.[155] PLA Daily, the PLA's official newspaper, has also cited Techxcope's data on the weapons imports and exports of the US, Russia, France, Japan, Australia, and other foreign countries.[156] PLA and state media have also published and republished articles authored by Techxcope personnel.[157] South China Morning Post, a Hong Kong-based outlet, has quoted Techxcope researchers and otherwise mentioned the organization.[158] Techxcope-affiliated researchers have also published publicly available research on subjects like the US Army's "multi-domain battle" concept and DARPA's technological innovation efforts.[159]

Techxcope has bid on numerous likely PLA OSINT contracts, in some cases competing with companies like Beijing Lanhai Changqing Information Science and Technology Co., Ltd. and Knowfar. Examples of projects that Techxcope has bid on are listed below, with more details available in Appendix A.

- Foreign XX [redacted] Equipment Key Materials Assessment and Evaluation Technical Information Summary and Analysis Research

- Science and Technology Information Normalization Services

- XX [redacted] Science and Technology Information Services[160]

- Foreign Military Typical Armored Equipment Operational Effectiveness Evaluation Basic Models and Data Resources System Construction Research

- Foreign Military Intelligence Information Data Collection

Remote Sensing Data

Kantian

Beijing Kantian Science and Technology Co., Ltd. (北京瞰天科技有限公司) is a privately owned remote sensing company that serves the PLA.[161] The company was founded in July 2017 and reportedly focuses on national defense and national security services, with an emphasis on integrating artificial intelligence with remote sensing big data.[162] The company claims to implement fusion processing, mining analysis, and research applications for geospatial information data.[163]

Beijing Kantian Science and Technology Co., Ltd. is actively working to integrate remote sensing with neural networks, a field closely related to artificial intelligence.[164] We identified 2 pending patents that belong to the company. The first, which the company filed in August 2019, is for "a kind of remote sensing target object identification method" that uses neural networks to "effectively improve the precision of target identification".[165] The second, which the company filed in September 2020, "relates to the field of image processing technologies" and uses a neural network model to improve the accuracy of maritime target recognition, with specific targets of interest including aircraft carriers, cruisers, destroyers, landing vessels, and submarines.[166]

The leadership of Beijing Kantian Science and Technology Co., Ltd. has included a former PLA officer who participated in likely English-language propaganda work. On 2 occasions, the company's then-general manager, Jiang Yanchuan (姜艳川), published articles with the South China Sea Strategic Situation Probing Initiative (SCSPI; 南海战略态势感知计划) that attempted to counter US narratives about the South China Sea disputes.[167] In both instances, Jiang used satellite imagery or ship tracking data in an effort to discredit claims about China's maritime militia operations published by the US-based Asia Maritime Transparency Initiative (AMTI), which is part of CSIS.[168] Prior to joining Beijing Kantian Science and Technology Co., Ltd., Jiang had reportedly served as the commander of Unit 96635 (96635部队) of the PLA Rocket Force (PLARF).[169] This unit is reportedly a remote sensing entity that may be associated with the PLARF Technical Reconnaissance Bureau (火箭军技术侦察局) and the PLARF Staff Department Intelligence Bureau (火箭军参谋部情报局).[170]

We observed at least 2 instances of Beijing Kantian Science and Technology Co., Ltd. bidding on likely PLA OSINT projects, both of which were in 2022. The projects are listed below, with additional details available in Appendix A.

- "Geospatial Environment Analysis and Judgement of Global Major Hotspots High-Resolution Satellite Remote Sensing Imagery"
- "Target Knowledge Bank Construction and Target Change Detection Software"

Outlook

The PLA and Chinese defense contractors will almost certainly continue developing and applying collection, processing, and analysis technologies to facilitate effective OSINT. Governments, militaries, research organizations, companies, news media organizations, social media platforms, and individuals should be aware that China's military and defense industry are using new technologies to collect, process, and analyze massive amounts of their publicly-available data for intelligence purposes, and should consider taking steps to mitigate these intelligence collection efforts. Commercial data providers should also be aware that China's military and defense industry could be purchasing their data for intelligence purposes, and should consider carrying out due diligence when selling their data to entities in China. The PLA very likely uses this data to support decision-making and better understand the military capabilities, operational concepts, and equipment of potential foreign adversaries in preparation for future conflicts. Given that China is very unlikely to open up its information environment, and that Western countries are very unlikely to close off their information environments, the PLA will very likely maintain its advantage over Western militaries in OSINT.

Appendix A: Chinese Military OSINT Procurement

This appendix provides a list of 50 PLA and Chinese defense industry projects very likely related to OSINT that we observed between January 2019 and January 2023. The list offers a sample of relevant procurement activity and should not be interpreted as an exhaustive catalog of PLA and defense industry OSINT projects. The dates provided for each project are the most recent documents, such as tenders or winning bid announcements, associated with each project that we observed.

Entity	Date	Project / Details
CSSC 714th Research Institute	January 2023	**Foreign Military Intelligent Recognition and Image Collection Specialized Network Technology Services**[171] The project aimed to support the collection of machine learning content for military science and technology intelligence recognition. It included the use of specialized network technologies to solve the issue of inaccessible internet addresses.
AMS	January 2023	**XXX Knowledge Base Software System**[172] The entity was looking to acquire a knowledge base on the operational applications of the intelligentized equipment of the world's major countries. Specific areas of interest included operational concepts, technology development, equipment development, and operational applications. The knowledge base was required to have data collation, multi-dimensional classification, and organic affiliation features, among others.
Unspecified PLAGF entity (very likely Unit 63963)	January 2023	**Foreign Military In-Service Main Battle Tank Upgrades, Remodeling, and Development Research**[173] The entity was seeking a report and a database on the US' M1A2 Abrams and Germany's Leopard 2 main battle tanks. Specific areas of interest include these tanks' propulsion systems, weapons systems, defensive systems (both passive and active), electrical systems, and communications systems (or integrated electronic information systems). The entity wanted the analysis to address these tanks' technical development, research history, and application tests.
Unspecified entity (very likely PLASSF)	December 2022	**A Data Analysis System**[174] The system needed to carry out collection, cleaning, fusion, and storage for open-source information. It also needed to have functions like "data display", "graph distribution", "relationship exploration", and "trend early warning".
Unspecified entity (very likely PLASSF)	December 2022	**Foreign Network [Cyber] Space Security Open-Source Research Electronic Information**[175] No additional project details observed.
Unspecified PLA entity	December 2022	**Foreign XX Equipment Key Materials Assessment and Evaluation Technical Information Summary and Analysis Research**[176] No additional project details observed.

Unspecified entity (likely PLA or defense industry)	November 2022	**Foreign Military Equipment Systems Contribution Rate Open-Source Intelligence Information**[177] The entity was seeking research reports on several foreign military joint war planning, hybrid warfare, complex systems, and other topics.
Unspecified entity (likely PLA or defense industry)	November 2022	**Open-Source Information Normalization Services**[178] The entity was seeking collection and organization of the "legal compliance information" of the ground forces of foreign militaries. Specific information of interest included policies, regulations, research reports, standards, specifications, writings, and papers, among others. The entity was interested in various information formats, including text, picture, table, and video. Focus areas included "overall construction", "informatization construction", "network information systems", "value engineering", and "simulation and evaluation".
Unspecified PLAGF entity	September 2022	**World's Main Countries' Think Tanks Construction Situations and Operation Mechanisms Research**[179] No additional project details observed.
Unspecified entity (very likely PLAGF)	August 2022	**XXXX Open-Source Intelligence Tracking Research**[180] The entity was interested in development plans, military theory, equipment construction, technology applications, organization and personnel, training and exercises, and logistics related to a redacted target. It wanted daily OSINT information tracking, collection, translation, and publishing, as well as comprehensive research. An unspecified PLAGF entity initiated a different project with the same name but different requirements in March 2022.
Unspecified PLAGF entity	June 2022	**Science and Technology Information Normalization Services**[181] The project involved subcontracts focused on coordinated innovation mechanisms, frontier combat concepts, intelligent unmanned technology, network information and electronic technology, new materials and advanced manufacturing, big data and advanced computing, and other topics. Though the project documents did not specify foreign targets, the participation of OSINT providers and foreign military translation companies in the project bidding process suggests that this project likely had foreign-oriented elements.
NUDT	June 2022	**Target Knowledge Bank Construction and Target Change Detection Software**[182] No additional project details observed.
Unit 93184 of the PLAAF	April 2022	**Foreign Military War Decision-Making and War Preparations Relevant Information Collection and Analysis**[183] No additional project details observed.
Unspecified PLAGF entity	April 2022	**Foreign Military XX Weapons and Equipment Development Trend Tracking and Analysis System**[184] See the "Collection Methods" section above for details.

Unspecified PLAGF entity	April 2022	**Foreign Squad-Level Ground Unmanned Equipment Materials Collection, Translation, and Collation**[185] The project aimed to produce a report based on foreign-language sources that includes the pictures; functions; technical indicators; procurement; and participation in exercises, tests, and operations of foreign military ground unmanned equipment and control terminals. The report should have covered the following systems, which were listed in a mix of English and Chinese: “Packbot、FCS-SUGV、310 SUGV、Dragon runner、MK4 Mod 0、XM1216、Scorpion、FirstLook110、Recon scout 、MARCbot、M160、Talon、Warrior 710、MAARS、MTRS Inc II、先进爆炸物处理机器人 [Advanced Explosive Ordnance Disposal Robot]、MUTT SMSS、J8 Atlas XTR、CAMEL、MULE、、[sic] Gladiator、Crusher、Laska 2.0 UGV、"模块化武装机器人" [Modularized Armed Robot]、Hunter Wolf、RS2-H1、Cobra-1600、RS1A3 Min Rex、ASENDRO、MTGR、MINI、MK Caliber、MK.8、Cutlass排爆机器人 [Cutlass Explosive Ordnance Disposal Robot]、tEODor、OSCAR、KAPLAN、MARS A-80、Ironclad、平台-M [Platform-M]、argo、寄生者 [Parasite]、Guardium、IZCI、Adunok-M、THeMIS 、涅列赫塔 [Nerekhta] 、山猫 [Lynx, Bobcat, or Leopard]、Probot、Rambow、Phantom、TITAN、Mission Master Multi-Mission UGV”.
Unspecified PLAAF entity	April 2022	**Foreign Military New Quality Combat Forces Construction and Emerging Technologies Development Relevant Data Collection and Analysis**[186] No additional project details observed.
Unspecified PLAGF entity	April 2022	**Foreign Military New-Generation Tracked Armored Vehicles Technological Development Documents and Data Resources Services**[187] This project aims to produce 2 reports and a set of databases related to new-generation tracked armored vehicles from countries like the US, Germany, Russia, the United Kingdom, and France. The research will address subjects such as intelligentized operational concepts, ground equipment operational mission planning systems, ground equipment target autonomous identification technology, tactical communications technology, power and drive technology, and protection technology.
AMS	April 2022	**General Field Science and Technology Intelligence Monitoring Platform**[188] The entity wanted a monitoring platform with functions such as intelligence data processing, intelligence analysis, report generation, and user management.
Unspecified PLAGF entity	March 2022	**2022 Foreign Military Network-Electromagnetic Confrontation Domain Scientific and Technical Information Research**[189] No additional project details observed. An unspecified PLAGF entity initiated a project with a very similar name in 2021.
Unspecified PLASSF entity	March 2022	**Geospatial Environment Analysis and Judgement of Global Major Hotspots High-Resolution Satellite Remote Sensing Imagery**[190] No additional project details observed.
Unspecified PLAGF entity	March 2022	**XXXX Open-Source Intelligence Tracking Research**[191] The project involved tracking relevant domestic and foreign media, targeting a redacted target, and carrying out daily OSINT tracking, collecting, translation, and compilation, and conducting relevant comprehensive research. An unspecified entity initiated a project with the same name but different requirements in August 2022.

Unspecified PLAGF entity	March 2022	**Information Collection and Translation Related to Strong Enemy Marine Corps Operational Concepts Development and Equipment Construction Situation**[192] The project required translation of “NATO operational concept development manuals” and “US Marine Corps internal force operational concepts”. It also involved retrieving and translating “strong enemy” operational concepts development, experimental verification, and evaluation documents. Additionally, it included retrieving and translating US Marine Corps and Taiwan Marine Corps operational concept designs and equipment construction documents.
Unspecified PLA entity	November 2021	**Open-Source Comprehensive Research and Study Platform**[193] No additional project details observed.
Unspecified entity (likely PLA or defense industry)	October 2021	**Foreign Military OSINT Software Platform and Data Resources**[194] No additional project details observed.
Unit 93209 of the PLAAF (very likely affiliated with Air Force Research Institute)	September 2021	**US Military Standard Unmanned Aerial Vehicle In-Network Applications Information Organization and Analysis**[195] The project involved analysis of unmanned aerial vehicle communication and data link networks in the US. This analysis was to be based on intelligence information pertaining to the large-scale unmanned aerial vehicles that the US military currently uses, such as the RQ-4 and MQ-9. The project also involved a series of research reports that would summarize the basic processes, communications network organization methods, and other key factors of US unmanned aerial vehicle reconnaissance and surveillance, reconnaissance and strike integration, damage assessment, and coordination.
NUDT College of Computers	August 2021	**Documents and Materials Analysis Services Related to Intelligent Processing Equipment**[196] No additional project details observed.
Unspecified PLAGF entity	August 2021	**Foreign Military XX Unit Intelligence Data Collection and Translation Compilation**[197] The entity was seeking information on a redacted foreign military unit’s development history, development direction, operational use, and deployment situation. The project included translating and compiling key materials and producing atlases.
Unit 93204 of the PLAAF (almost certainly the Engineering and Design Research Institute of the Air Force Research Institute)	June 2021	**World’s Major Countries Overseas Support Facilities Comprehensive Research**[198] No additional project details observed.

AMS	May 2021	**Strategic Emerging Technologies International Cooperation Scientific Measurement and Analysis**[199] The project was intended to produce a research report on international cooperation between 10 countries including China, the US, Germany, and Japan in emerging technical fields like artificial intelligence, quantum information, advanced materials, advanced manufacturing, 5G, hypersonics, unmanned systems, aerospace, aviation, and brain-computer interfaces. The tender associated with this project appears to have instructed the winning bidder to focus on using the “Clarivate Web of Science Core Database” and “Derwent Patent Database”. Both databases are almost certainly products from commercial data provider Clarivate, a multinational analytics company based in the US and UK.[200]
Unit 63920 of the PLASSF	May 2021	**XX Robotic Arm Teleoperation Intelligence Research**[201] No additional project details observed.
Unit 93209 of the PLAAF (very likely affiliated with Air Force Research Institute)	May 2021	**US Military Distributed Ground Intelligence Processing Equipment Technical Intelligence Information Special Topic Research**[202] No additional project details observed.
Unspecified PLAAF entity	April 2021	**XX Data Collection Services**[203] No additional project details observed.
Unspecified PLAGF entity	April 2021	**Open-Source Intelligence Support Related to Network-Electromagnetic Confrontation Domain Strong Enemy Research**[204] The project appears to have also been known as “foreign military network-electromagnetic confrontation domain scientific and technical information research”.[205] An unspecified PLAGF entity initiated a project with a very similar name in 2022.
Unit 91054 of the PLAN (likely affiliated with the Naval Research Academy)	April 2021	**XX Science and Technology Information Services**[206] The unit was seeking research on the strategies, equipment, technologies, logistics, operational theories, regulations, combat operations, exercises, training, and education of the world’s major naval and coast guard forces, as well as defense industry enterprises and technologies. It was also interested in research on the domestic development of artificial intelligence, new technologies, and new materials. The entity managed a very similar project in 2020.
Unspecified PLAN entity	March 2021	**2021 Foreign-Language Original Version Periodicals**[207] The project involved acquiring editions of “C4ISRNET”, “Undersea Warfare”, “Journal of Electronic Defense”, “Asian Defence Journal”, “Unmanned Systems”, “Jane's Defence Weekly”, “Jane's Navy International”, “Jane's Intelligence Review”, “Jane's International Defense Review”, “Jane's Fighting Ships”, “Asian Military Review”, “Military Technology”, “United States Naval Institute Proceedings”, “Sea Power”, “Naval Forces”, “Naval Engineers Journal”, “Naval Architect, with Warship Technology”, “Signal”, “軍事研究/Japan Military Review”, “世界の艦船/Ships of the World”, “世界の艦船増刊”, “Морской сборни”, “尖端科技軍事雜誌/Defense Technology Monthly”, “軍事家/Defence International”, “Warship World”, “Marine Corps Gazette”, “Naval Aviation News”, and “Indo-Asia-Pacific Defense Forum”.

Unspecified PLA entity	March 2021	**A Knowfar Database**[208] See the “Knowfar” section above for more details.
Unit 61540 of the PLASSF	February 2021	**US, Japan, India, and Australia Geostrategic Intelligence Collection and Analysis**[209] The unit was seeking collection and collation of geostrategic intelligence information pertaining to the US, Japan, India, and Australia (the members of the Quadrilateral Security Dialogue or “Quad”). The unit wanted analysis of the historical evolution of US-Japanese-Indian-Australian geostrategies and their geostrategic trends in recent years, with assessment of future trends and their impact on “us”, presumably referring to China, the PLA, the PLASSF, or Unit 61540.
Unspecified PLAGF entity (likely Unit 32181)	October 2020	**Porous Materials Air Water Intake Intelligence Collection and Comprehensive Analysis Research**[210] The project involved collection of comprehensive intelligence from the past 20 years, from both domestic and international sources, on “porous absorbent materials air water intake materials performance” and “water intake current application status, rules and theories, and equipment principles and applications”. It also included analysis of scientific and technological progress in the past 10 years, translation of primary source documents and key foreign language materials, and submission of analytical research reports.
AMS	September 2020	**Science and Technology Intelligence Research Methods and Capabilities Improvement Conditions Construction**[211] See the “Collection Methods” section above for more details.
Unspecified PLAGF entity	September 2020	**Foreign Military Typical Armored Equipment Operational Effectiveness Evaluation Basic Models and Data Resources System Construction Research**[212] The project involved research related to the typical armored equipment used by the militaries of the US, India, and Taiwan. It included analyzing the simulation basic models, data systems, operational evaluation systems, and operational applications of typical operational forces, and carrying out research on simulation model data standardization.
Unit 92859 of the PLAN (almost certainly the Naval Hydrographic Surveying and Charting Research Institute)	July 2020	**Polar Silk Road Land-Sea Intermodal Transportation Geospatial Intelligence Data Compilation**[213] The entity was seeking analysis of the feasibility of Polar Silk Road land-sea intermodal transportation by compiling geographic, legal, and international relations materials related to Polar Silk Road land-sea intermodal transportation passages. This research was further intended to enrich the “concept implications” of the Polar Silk Road, strengthen the connective capabilities of the Polar Silk Road, and promote better global economic integration.
Unit 91054 of the PLAN (likely affiliated with the Naval Research Academy)	June 2020	**XX Science and Technology Information Services**[214] The project involved research on the strategies, equipment, technologies, logistics, operational theories, regulations, combat operations, exercises, training, and education of the world’s major naval and coast guard forces, as well as defense industry enterprises and technologies. It also included research on the domestic development of artificial intelligence, new technologies, and new materials. The entity managed a very similar project in 2021.

Unspecified PLAN entity	March 2020	**Foreign-Language Original Version Periodicals and Yearbooks**[215] No additional project details observed.
Unit 32179 of the PLAGF	December 2019	**Foreign Military Intelligence Information Data Collection**[216] No additional project details observed.
Unit 63963 of the PLAGF	September 2019	**Foreign Country Ground Forces Unmanned Combat Equipment Intelligence Research**[217] The unit wanted research on the development status and combat applications of foreign military ground unmanned combat equipment, foreign military airborne unmanned combat equipment, military water-area unmanned combat equipment, and foreign military manned-unmanned coordination command information systems.
CSSC 701st Research Institute	August 2019	**Foreign Electromagnetic Spectrum Combat Equipment Situation Research**[218] No additional project details observed.
AMS Military Science Information Research Center	July 2019	**IHS-Jane's Defense Databases**[219] The project involved procurement of "IHS/Jane's Defense Forecast Database", "IHS/Jane's National Defense and Security Periodical Database", and "IHS/Jane's Yearbook", among other data sets.
Unit 61716 of the PLASSF (likely 311 Base)	May 2019	**Knowfar Institute for Defense Studies Documents and Information**[220] See the "Knowfar" section above for more details.
Unit 31008 of the CMC JSD	February 2019	**Internet Data Collection and Analysis System Software**[221] The project involved an internet data collection and analysis system with 2 subsystems: a data collection and cleaning subsystem and a data analysis and management subsystem.
AMS	January 2019	**Science and Technology Intelligence Mining Technical Text Annotation**[222] No additional project details observed.

Table 2*: Likely PLA and Chinese defense industry OSINT procurement activity between January 2019 and January 2023 (Source: Recorded Future*[223]*)*

About the Author
Zoe Haver
Threat Intelligence Analyst, Insikt Group®

Zoe Haver is part of Insikt Group's Global Issues team. Her research focuses on the People's Liberation Army, maritime security, the South China Sea disputes, and other China-related security issues. She has worked on these topics for Radio Free Asia, the Center for Advanced China Research, SOSi's Center for Intelligence Research and Analysis, the US Naval War College China Maritime Studies Institute, C4ADS, and other organizations. She received her BA from George Washington University and is proficient in Mandarin Chinese.

About Insikt Group®
Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

Endnotes

[1] The US Department of Defense (DOD) defines open-source information as “information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access”. *DOD Dictionary of Military and Associated Terms* (US Department of Defense, 2021).

[2] The US DOD defines OSINT as “relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements”. *DOD Dictionary of Military and Associated Terms*.

[3] The US DOD defines the information environment as “the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information”. *DOD Dictionary of Military and Associated Terms*.

[4] Zhang Xiaojun [张晓军], Li Naiguo [李耐国], Shen Hua [申华], and Liu Xinming [刘心铭], *The Science of Military Intelligence* [军事情报学] (Military Science Press [军事科学出版社], 2001), pp. 22-25.

[5] Anna B. Puglisi, James C. Mulvenon, and Wm. C. Hannas, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (Routledge, 2013), pp. 18-51; Wm. C. Hannas and Huey-Meei Chang, China’s STI Operations (Center for Security and Emerging Technology, 2021), https://cset.georgetown.edu/publication/chinas-sti-operations/.

[6] An Hui [安辉], Gu Linuo [顾丽娜], and Liu Jian [刘剑], “Internet Open-Source Military Intelligence Data Collection Strategies and Reliability Research” [互联网开源军事情报数据采集策略与可靠性研究], *All Circles* [各界前沿理论] 7 (2020); Zheng Lingsha [曾令沙], Liu Wei [刘伟], and Xu Zhenbei [许振北], “Methods of Open Source Geospatial Intelligence Gathering” [开源地理空间情报的搜集方法], *Geomatics & Spatial Information Technology* [测绘与空间地理信息] 43, no. 2 (2020); Wang Jingshi [王景石], Qiao Hui [乔慧], He Jiazhou [何佳洲], and Jiang Bingdong [蒋丙栋], “Detection and Recognition of Large and Medium-sized Marine Targets Based on Open Source Intelligence” [基于开源情报的海上大中型目标检测与识别], *Ship Electronic Engineering* [舰船电子工程] 41, no. 7 (2021); Zhang Meng [张猛], “An Open Source Intelligence Feature Extraction Algorithm Based on Big Data Framework” [基于大数据框架的开源情报特征提取算法], *Ship Electronic Engineering* [舰船电子工程] 40, no. 9 (2020); Wang Sijia [王思佳] and Xia Shaomo [夏绍模], “Analysis and Implementation of Foreign Military Open Source Intelligence Database Based on MADL” [基于MADL的外国军事开源情报数据库的分析与实现], *Command Control & Simulation* [指挥控制与仿真] 41, no. 3 (2019); Su Min [苏敏], Zhang Ping [张萍], and Luo Wei [罗伟], “Open-Source Intelligence Value Primary Analysis” [公开源情报价值浅析], *Legal System and Society* [法制与社会] 14 (2013); Huang Sheng [黄胜], Guo Jiguang [郭继光], Lu Zejian [陆泽健], Chen Long [陈龙], and Pan Yue [潘越], “Study of Web Open Source Intelligence Topic Mining in Military Domain” [面向军事领域的Web开源情报主题挖掘研究], *Journal of China Academy of Electronics and Information Technology* [中国电子科学研究院学报] 12, no. 4 (2017); Qi Shiqian [漆世钱] and Meng Chunning [孟春宁], “Research and Application of Open Source Intelligence Based on Social Networking” [基于网络社交的开源情报研究与应用], *Information Security and Communications Privacy* [信息安全与通信保密] 1 (2021); Song Jiwei [宋继伟], “Model Construction of Military Intelligence Early Warning Based on Open Source Intelligence” [公开源情报视角下的军事情报预警模型构建], *Proceedings of 17th Cross-Strait Information Management Development and Strategy Forum* [第十七届海峡两岸信息管理发展与策略学术研讨会论文集] (2011); Wang Feiyue [王飞跃] “‘AlphaGo’ Wins, Indicating Big Data Will Become a Military Weapon?”[“阿法狗”胜出，预示大数据成为军事武器？], China Military Net [中国军网], March 17, 2016, https://archive.ph/7LbEH; Yang Zuo [杨佐], “Use Information Concept to Pry Open the Door of Military Theory Innovations” [用信息理念撬开军事理论创新之门], *PLA Daily* [解放军报], December 9, 2021, https://archive.ph/I5uc9; Wang Yingjie [王英杰], “China Should Improve Intelligence Work, Aviation Industry Shoulders Heavy Responsibility” [中国应提升情报工作 航空工业肩负重任], China Military Net [中国军网], July 29, 2014, https://archive.ph/i7KrN.

[7] An, Gu, and Liu, “Internet Open-Source Military Intelligence Data Collection Strategies and Reliability Research”.

[8] Ibid.

[9] Ibid.; Gao Kai [高凯], Huo Xinlei [霍鑫磊], and Xu Mingyang [徐明阳], “Pay Attention to Degree of Data Depreciation” [关注数据“折旧度”], *PLA Daily* [解放军报], December 13, 2022, https://archive.ph/DbvM8.

[10] Joel Wuthnow and Philip C. Saunders, “Introduction”: Appendix: Central Military Commission Reforms, in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, ed. Philip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N.D. Yang, and Joel Wuthnow (National Defense University Press, 2019), pp. 32-33, https://ndupress.ndu.edu/Publications/Books/Chairman-Xi-Remakes-the-PLA/.

[11] An, Gu, and Liu, “Internet Open-Source Military Intelligence Data Collection Strategies and Reliability Research”; Tian Zhong [田仲], Bi Yuhui [毕于慧], and Hou Dongfeng [侯东风], “Open-Source Intelligence Analysis System Planning Research for the Military Domain” [面向军事领域的开源情报分析系统设计研究], *Information Systems Engineering* [信息系统工程] (2019); see Appendix A.

[12] An, Gu, and Liu, “Internet Open-Source Military Intelligence Data Collection Strategies and Reliability Research”; Zhang, “An Open Source Intelligence Feature Extraction Algorithm Based on Big Data Framework”; Wang and Xia, “Analysis and Implementation of Foreign Military Open Source Intelligence Database Based on MADL”; Huang Yu [黄禹], Lan Yang [兰洋], Zhang Yue [张玥], Hu Jiaquan [胡家全], and Huang Can [黄粲], “Open-Source Nuclear Intelligence Collection System Construction Based on Scrapy”, [基于Scrapy的开源核情报采集系统构建], *Science & Technology Vision* [科技视界] 17 (2022); Huang, Guo, Lu, Chen, and Pan, “Study of Web Open Source Intelligence Topic Mining in Military Domain”; Tian, Bi, and Hou , “Open-Source Intelligence Analysis System Planning Research for the Military Domain”; Wang, Qiao, He, and Jiang, “Detection and Recognition of Large and Medium-sized Marine Targets Based on Open Source Intelligence”; Wang Mingqian [王明乾], Ni Lin [倪林], and Zhang Bin [张斌], “An Open Source Military Intelligence Aquisition Method Based on Text Classification” [基于文本分类的开源军事情报获取方法], *Information Research* [情报探索] 7 (2021); Chen Chunyan [陈春燕], “Research on Semantic Aggregation Framework of Open Source Intelligence Based on Linked Data” [基于关联数据的开源情报语义聚合框架研究], *Journal of Library and Information Science* [图书情报导刊] 5 (2021); Zhou Yang [周洋], “Preliminary Research on the Application of Computational Propaganda in Intelligentized Warfare” [计算宣传在智能化

战争中的应用研究初探], *Military Reporter* [军事记者], May 6, 2022, https://archive.ph/DcVIn; Wu Xiangrong [武向荣] and Lu Bin [吕彬], “Actively Respond to Data-Centric Warfare” [积极应对数据中心战], *PLA Daily* [解放军报], October 18, 2019, https://archive.ph/tymyJ; Li Wenqing [李文清] and Liang Jinlong [梁金龙], “Put Science and Technology to Good Use Enabling Combat Command” [善用科技为作战指挥赋能], *PLA Daily* September 28, 2021, https://archive.ph/9Xd0C; Hao Fei [郝飞], Shao Huiwen [邵惠文], and Wang Lili [王利利], “Pay Attention to New Trends in Firepower Precision Combat” [关注火力精打作战新趋势], China Military Net [中国军网], March 18, 2021, https://archive.ph/BHDUs; Lu Tiange [陆天歌] and Zhang Aimin [张瑷敏], “Artificial Intelligence ‘Thrown Into’ Intelligence Community” [人工智能“投身”情报界], *PLA Daily* [解放军报], August 3, 2018, https://archive.ph/A1eUj.

[13] Huang, Guo, Lu, Chen, and Pan, “Study of Web Open Source Intelligence Topic Mining in Military Domain”.

[14] Ibid.

[15] Ibid.

[16] “Company Introduction” [企业简介], China Electronics Technology Group Corporation Academy of Electronics and Information Technology [中国电子科技集团公司电子科学研究院], https://web.archive.org/web/20200304201945/http://caeit.cetc.com.cn/caeit/319315/319303/index.html.

[17] Huang Yongqin [黄永勤], “Research on Standards Construction for Open Source Military Intelligence” [刍议开源军事情报工作的标准构建], *Technology Intelligence Engineering* [情报工程] 8, no. 1 (2022); Ma Zengjun [马增军] and Wang Jing [王净], “The US Military Development and Task Management System of Open Source Intelligence” [美军开源情报发展历程及任务管理体系综述], *Journal of Modern Information* [现代情报] 35, no. 7 (2015); Me Zengjun [马增军], Geng Wei [耿卫], and Wang Chuan [汪川], “The US Open Source Intelligence System Analysis and Development Trend” [美国开源情报制度分析及发展趋势], *Innovation Science and Technology* [创新科技] 211, no. 9 (2017); Wang Mingmin [王明敏] and Wan Kuo [万阔], “US Think Tank Open-Source Intelligence Analysis on China’s Defense Concept Research” [美国智库对华防务开源情报分析理念研究], *Journal of Intelligence* [情报杂志] (2022); Su, Zhang , and Luo, “Open-Source Intelligence Value Primary Analysis”; Bao Changhuo [包昌火], Ma Dehui [马德辉], Li Yan [李艳], and Zhang Wei [张薇], “Challenges, Opportunities and Responses of Chinese National Intelligence Activities” [我国国家情报工作的挑战、机遇和应对], *Journal of Intelligence* [情报杂志] 35, no. 10 (2016).

[18] Huang, “Research on Standards Construction for Open Source Military Intelligence”.

[19] Ibid.

[20] Ibid.

[21] “General Information of NDU”, PLA NDU International College of Defense Studies, https://web.archive.org/web/20220216001524/http://www.cdsndu.org/en/index.php/daxuegaikuang.html; “National Defense University”, China Defense Universities Tracker, https://unitracker.aspi.org.au/universities/national-defense-university/; Yan Xiaoqiang [闫晓强], Deng Chaoxing [邓朝鑫], Zhan Xiaobei [湛小贝], Sai Zongbao [赛宗宝}, “Come for War, Go to War” [为战而来 向战而行], *PLA Daily* [解放军报], May 15, 2019, https://archive.ph/Xx8TW.

[22] Bao, Ma, Li, and Zhang, “Challenges, Opportunities, and Responses of Chinese National Intelligence Activities”; Yang Jianying [杨建英] and Yu Zhicheng [余至诚], “An Analysis of the Position and Function of Open Source Intelligence in China's National Security Intelligence” [试析开源情报在中国国家安全情报中的地位和作用], *Journal of Intelligence* [情报杂志] (2019); Qi and Meng, “Research and Application of Open Source Intelligence Based on Social Networking”.

[23] Yang and Yu, “An Analysis of the Position and Function of Open Source Intelligence in China's National Security Intelligence”.

[24] Ibid.

[25] Marcel Angliviel de la Beaumelle, Benjamin Spevack, and Devin Thorne, *Open Arms: Evaluating Global Exposure to China’s Defense Industrial Base* (Center for Advanced Defense Studies, 2019, https://c4ads.org/wp-content/uploads/2019/10/OpenArms-Report.pdf.

[26] Yang and Yu, “An Analysis of the Position and Function of Open Source Intelligence in China's National Security Intelligence”.

[27] “University of International Relations”, China Defense Universities Tracker, https://unitracker.aspi.org.au/universities/university-of-international-relations/; David Shambaugh, “International Relations Studies in China: History, Trends, and Prospects”, *International Relations of the Asia-Pacific* 11 (2011); “Notice on Issues Relating to Zhejiang Province Personnel Department, Public Security Department, State Security Department Recruiting Graduates frp, People’s Police from Public Security and State Security System Schools” [浙江省人事厅、公安厅、国家安全厅关于从公安、安全系统院校应届毕业生中录用人民警察有关问题的通知], Ningbo City Human Resources and Social Suport Bureau [宁波市人力资源和社会保障局], June 23, 1997, https://archive.fo/3HRE4.

[28] Ma Hongsheng [马宏省], “Mistakes and Preventions that Easily Occur in Military-related New Media” [涉军新媒体容易出现的差错及防范], *Military Reporter* [军事记者], March 9, 2020, https://archive.ph/RALc1; Qi and Meng, “Research and Application of Open Source Intelligence Based on Social Networking”.

[29] Ma, “Mistakes and Preventions that Easily Occur in Military-related New Media”.

[30] Ibid.

[31] Ibid.

[32] “About Us” [关于我们], PLA News Propagation Center Press [中国人民解放军新闻传播中心出版社], https://archive.ph/NkwhW; “Military News Propagation Center 2022 Civilian Staff Recruiting Official Begins! (Unit Introduction)” [解放军新闻传播中心2022年文职人员招考正式开始！（单位介绍篇）], PRC Ministry of National Defense [中华人民共和国国防部], December 6, 2021, https://archive.ph/oY21r.

[33] An, Gu, and Liu, “Internet Open-Source Military Intelligence Data Collection Strategies and Reliability Research”; Huang, Guo, Lu, Chen, and Pan, “Study of Web Open Source Intelligence Topic Mining in Military Domain”; Wang and Xia, “Analysis and Implementation of Foreign Military

Open Source Intelligence Database Based on MADL"; Song, "Model Construction of Military Intelligence Early Warning Based on Open Source Intelligence"; Wang, "'AlphaGo' Wins".

[34] Peter Mattis, "Modernizing Military Intelligence: Playing Catch-Up (Part One)", *China Brief* 16, no. 18 (2016), https://jamestown.org/program/modernizing-military-intelligence-playing-catch-part-one/; Peter Mattis and Elsa Kania, "Modernizing Military Intelligence: Playing Catchup (Part Two)", *China Brief* 16, no. 19 (2016), https://jamestown.org/program/modernizing-military-intelligence-playing-catchup-part-two/.

[35] Su, Zhang , and Luo, "Open-Source Intelligence Value Primary Analysis"; Yang Longxi [杨龙溪], "Aim at Future Warfare, Fight Well the Cognitive '5 Battles'" [瞄准未来战争打好认知"五仗"], China Military Net [中国军网], August 23, 2022, https://archive.ph/ix3Mb.

[36] An, Gu, and Liu, "Internet Open-Source Military Intelligence Data Collection Strategies and Reliability Research".

[37] Ibid.

[38] Ibid.

[39] Ibid.

[40] Ibid.

[41] Wang, Qiao, He, and Jiang, "Detection and Recognition of Large and Medium-sized Marine Targets Based on Open Source Intelligence".

[42] Song, "Model Construction of Military Intelligence Early Warning Based on Open Source Intelligence".

[43] Hao, Shao, and Wang, "Pay Attention to New Trends in Firepower Precision Combat".

[44] Zhou, "Preliminary Research on the Application of Computational Propaganda in Intelligentized Warfare".

[45] Wang and Xia, "Analysis and Implementation of Foreign Military Open Source Intelligence Database Based on MADL".

[46] Ibid.

[47] "About NPIC" [关于NPIC], Nuclear Power Research Institute of China, https://archive.ph/z8kUq.

[48] Huang, Lan, Zhang, Hu, and Huang, "Open-Source Nuclear Intelligence Collection System Construction Based on Scrapy".

[49] "Group Website Group" [集团网站群], China State Shipbuilding Corporation Limited, https://archive.ph/1Idtk; "CSSC 716th Research Institute Spring Recruitment Brochure" [中国船舶第七一六研究所2022届春招简章], January 30, 2022, https://archive.ph/f0KyG; "Unit Basic Information" [单位基本信息], Shandong University Student Career and Entrepreneurship Center, https://archive.ph/TcF63.

[50] Wang, Qiao, He, and Jiang, "Detection and Recognition of Large and Medium-sized Marine Targets Based on Open Source Intelligence".

[51] Zhang, "An Open Source Intelligence Feature Extraction Algorithm Based on Big Data Framework".

[52] "Army Service Academy", China Defense University Tracker, https://unitracker.aspi.org.au/universities/army-service-academy/.

[53] Wang and Xia, "Analysis and Implementation of Foreign Military Open Source Intelligence Database Based on MADL".

[54] Source documents held by Recorded Future.

[55] Source documents held by Recorded Future.

[56] Source documents held by Recorded Future.

[57] Source documents held by Recorded Future.

[58] Source documents held by Recorded Future.

[59] Source documents held by Recorded Future.

[60] Source documents held by Recorded Future.

[61] Source documents held by Recorded Future.

[62] Source documents held by Recorded Future.

[63] Source documents held by Recorded Future.

[64] Source documents held by Recorded Future.

[65] Source documents held by Recorded Future.

[66] An, Gu, and Liu, "Internet Open-Source Military Intelligence Data Collection Strategies and Reliability Research"; Wang and Xia, "Analysis and Implementation of Foreign Military Open Source Intelligence Database Based on MADL"; Song, "Model Construction of Military Intelligence Early Warning Based on Open Source Intelligence"; Su, Zhang, and Luo, "Open-Source Intelligence Value Primary Analysis"; Huang, Lan, Zhang, Hu, and Huang, "Open-Source Nuclear Intelligence Collection System Construction Based on Scrapy"; Wang, Qiao, He, and Jiang, "Detection and Recognition of Large and Medium-sized Marine Targets Based on Open Source Intelligence"; Zheng, Liu, and Xu, "Methods of Open Source Geospatial Intelligence Gathering"; Qi and Meng, "Research and Application of Open Source Intelligence Based on Social Networking".

[67] Wang and Xia, "Analysis and Implementation of Foreign Military Open Source Intelligence Database Based on MADL".

[68] Ibid.

[69] Ibid.

[70] "About Janes", Janes, https://www.janes.com/about-janes/what-we-do, https://www.janes.com/about-janes/what-we-do; "Jane's Information Group Ltd.", Bloomberg, https://www.bloomberg.com/profile/company/2564378Z:LN.

[71] Source documents held by Recorded Future; see Appendix A for more details.

[72] Source documents held by Recorded Future; see Appendix A for more details.

[73] “About Us”, Clarivate, https://clarivate.com/about-us/; “Clarivate PLC”, Bloomberg, https://www.bloomberg.com/profile/company/1713669D:US.

[74] Wang, Qiao, He, and Jiang, “Detection and Recognition of Large and Medium-sized Marine Targets Based on Open Source Intelligence”.

[75] SCS Probing Initiative, social media, February 19, 2023, https://archive.ph/Gkuxu; SCS Probing Initiative, social media, January 28, 2023, https://archive.ph/LMZI7; Ben Werner, “After Deadly Collisions Navy will Broadcast Warship Locations in High Traffic Areas”, USNI News, September 19, 2017, https://news.usni.org/2017/09/19/deadly-collisions-navy-will-broadcast-warship-locations-high-traffic-areas; Jonathan Saul and Eduardo Baptista, “Off the grid: Chinese data law adds to global shipping disruption”, Reuters, November 17, 2021, https://www.reuters.com/world/china/off-grid-chinese-data-law-adds-global-shipping-disruption-2021-11-17/.

[76] Source documents held by Recorded Future.

[77] Source documents held by Recorded Future.

[78] Source documents held by Recorded Future.

[79] Source documents held by Recorded Future.

[80] “TSX (TerraSAR-X)”, eoPortal, https://www.eoportal.org/satellite-missions/terrasar-x;

[81] “What is RADARSAT-2”, Government of Canada, https://www.asc-csa.gc.ca/eng/satellites/radarsat2/what-is-radarsat2.asp.

[82] “ALOS-2 Project / ALOS-2 Overview”, Japan Aerospace Exploration Agency Earth Observation Research Center, https://www.eorc.jaxa.jp/ALOS-2/en/about/overview.htm; “ALOS-2 (Advanced Land Observing Satellite-2) / Daichi-2”, eoPortal, https://www.eoportal.org/satellite-missions/alos-2; “ALOS-2”, PASCO, https://alos-pasco.com/en/alos-2/.

[83] Source documents held by Recorded Future.

[84] Source documents held by Recorded Future.

[85] Source documents held by Recorded Future.

[86] Here, “intelligence” (zhineng; 智能) is the same word used in “artificial intelligence”, rather than the “intelligence” (qingbao; 情报) used in “open-source intelligence”; “About Yuanting Science and Technology” [关于渊亭科技]], Yuanting Science and Technology [渊亭科技], https://archive.ph/TlzrF.

[87] “About Yuanting Science and Technology”.

[88] “About Yuanting Science and Technology”; “About Us” [关于我们], DataExa, https://archive.ph/IBNcV; “Tianji - Intelligence Information Center” [天机·情报信息中心], Yuanting Science and Technology [渊亭科技], https://archive.ph/MMSi9; “Illuminating Central China, AI Empowerment | Hunan Yuanting Intelligent Technology Co., Ltd. Formally Established” [点亮华中，AI赋能丨湖南渊亭智能科技有限公司正式成立], Zhihu [知乎], June 28, 2022, https://archive.ph/H648z.

[89] “About Yuanting Science and Technology”.

[90] Ibid.

[91] “Tianji - Intelligence Information Center”.

[92] Ibid.

[93] Ibid.

[94] Ibid.

[95] “Tianji Intelligence Information Center” [天机情报信息中心], DataExa, https://archive.ph/XUSh1.

[96] “Tianji - Intelligence Information Center”.

[97] Ibid.

[98] Ibid.

[99] Source documents held by Recorded Future.

[100] “assignee:厦门渊亭信息科技有限公司”, Google Patents, https://archive.ph/4aVsY.

[101] “Knowledge graph data extraction method and device based on web crawler”, Google Patents, https://archive.ph/DV8UU.

[102] “Visual integration device and method based on GIS and knowledge graph and computing equipment”, Google Patents, https://archive.ph/3gKfU.

[103] “Military intelligence analysis visualization method and device and computer readable storage medium”, Google Patents, https://archive.ph/wip/tWJFX.

[104] Source documents held by Recorded Future.

[105] “About Us” [关于我们], Knowfar [诺方知远], https://web.archive.org/web/20090608181610/http://www.Knowfar.org.cn/cmsfile/about/index; “About Us” [关于我们], Knowfar Institute for Strategic and Defense Studies [知远战略与防务研究所], https://web.archive.org/web/20190101181207mp_/http://www.Knowfar.org.cn/about/index.html.

[106] “About Us”, Knowfar Institute for Strategic and Defense Studies.

[107] Ibid.

[108] Shang Zijie [尚子絜], “Categories Analysis of US Department of Defense Office of Net Assessment Research Reports Related to China (1988-2015)”, [美国国防部净评估办公室涉华研究报告类型分析 （1988-2015）], Knowfar Institute for Strategic and Defense Studies [知远战略与防务研究所], October 31, 2018, https://web.archive.org/web/20181103224112/http://www.knowfar.org.cn/html/zhanlue/201810/31/838.htm; Li Jian [李健], “Basic Situation of Russia Implementing Middle and Primacy Students National Defense Education” [俄罗斯实施中小学生国防教育的基本情况], Knowfar Institute for Strategic and Defense Studies [知远战略与防务研究所], September 27, 2018, https://web.archive.org/web/20181103224936/http://www.knowfar.org.cn/html/zhanlue/201809/27/829.htm; “Japan Southwest Sea Air Reconaissance Early Warning Core Node: Fuke Island Radar Station” [日本西南海空域侦察预警核心节点之：福江岛雷达站], Knowfar Institute for Strategic and Defense Studies [知远战略与防务研究所], September 2018, https://web.archive.org/web/20181103224106/http://www.knowfar.org.cn/html/zhanlue/201809/29/834.htm.

[109] “About the Knowfar Open-Source Center” [关于知远开源中心], Knowfar Open-Source Center [知远开源中心], https://archive.ph/BlHem.

[110] Ibid.

[111] Ibid.

[112] “Knowfar Foreign Military and Defense Open-Source Intelligence Database” [知远-外军防务开源情报数据库], Beijing Nuofang Zhiyuan Information Science and Technology Co., Ltd. [北京诺方知远信息科技有限公司], https://archive.ph/eWIDL.

[113] “Homepage” [首页], Knowfar Institute for Strategic and Defense Studies [知远战略与防务研究所], archived May 2021, https://web.archive.org/web/20210520154410/http://www.Knowfar.org.cn/.

[114] “Homepage”, Knowfar Institute for Strategic and Defense Studies, archived May 2021; “Homepage” [首页], Knowfar Open-Source Center [知远开源中心], https://archive.ph/pprLE.

[115] “Homepage”, Knowfar Open-Source Center.

[116] Ibid.

[117] Ibid.

[118] Ibid.

[119] Ibid.

[120] Source documents held by Recorded Future.

[121] John Costello and Joe McReynolds, *China’s Strategic Support Force: A Force for a New Era, China Strategic Perspectives 13* (Center for the Study of Chinese Military Affairs, 2018), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf; Mark Stokes and Russell Hsiao, *The People’s Liberation Army General Political Department: Political Warfare with Chinese Characteristics* (Project 2049 Institute, 2013), https://project2049.net/wp-content/uploads/2018/04/P2049_Stokes_Hsiao_PLA_General_Political_Department_Liaison_101413.pdf; Nathan Beauchamp-Mustafaga and Jessica Drun, “Exploring Chinese Military Thinking on Social Media Manipulation against Taiwan”, *China Brief* 21, no. 7 (2021), https://jamestown.org/program/exploring-chinese-military-thinking-on-social-media-manipulation-against-taiwan/.

[122] Source documents held by Recorded Future.

[123] Source documents held by Recorded Future.

[124] Source documents held by Recorded Future.

[125] Source documents held by Recorded Future.

[126] Source documents held by Recorded Future.

[127] Source documents held by Recorded Future.

[128] Source documents held by Recorded Future.

[129] Source documents held by Recorded Future.

[130] Source documents held by Recorded Future.

[131] Both the 2020 and 2021 versions of the project.

[132] Source documents held by Recorded Future.

[133] “Company Introduction” [公司简介], Lanhai Changqing [蓝海长青], https://archive.ph/eEpeY.

[134] Ibid.

[135] Ibid.

[136] “Organizational Structure” [组织架构], Lanhai Changqing [蓝海长青], https://archive.ph/9YmuL; “Company Introduction”, Lanhai Changqing.

[137] Source documents held by Recorded Future.

[138] “Homepage” [首页], Lanhai Changqing [蓝海长青], https://archive.ph/M5MkS.

[139] “MK-48 MOD Heavy Torpedo: US Navy’s Most Advanced Underwater Strike Force” [MK-48 Mod 7重型鱼雷：美国海军最先进的水下打击力量], Lanhai Changqing [蓝海长青], June 30, 2020, https://archive.ph/jzPRo; “MK 48 Mod 7 Common Broadband Advanced Sonar System (CBASS) Heavyweight Torpedo”, Lockheed Martin, https://web.archive.org/web/20230227183758/https://www.lockheedmartin.com/en-us/products/mk-48-mod-7-common-broadband-advanced-sonar-system-cbass-heavyweight-torpedo.html.

[140] Du Renhuai [杜人淮], “Locating Military Potential in Civilian Capabilities Strategy in Japan’s National Defense Industry Development” [日本国防工业发展的寓军于民策略], September 28, 2020, https://archive.ph/Qt1Sv.

[141] Li Wei [李玮] and Lan Shunzheng [兰顺正], “Combat Robots Force: Russia Prepares to Complete Building Before 2025” [战斗机器人部队：俄罗斯准备在2025年前组建完成], March 10, 2020, https://archive.ph/wvdoB.

[142] “Lanhai Changqing Think Tank” [蓝海长青智库], https://archive.ph/Y06UW.

[143] “‘Crewed-Uncrewed’ Formations Are Driving Global Unmanned Aerial Vehicle Surge” [“载人-无人”编队正在推动全球无人机激增], NetEase [网易], October 4, 2022, https://archive.ph/iAme2.

[144] Source documents held by Recorded Future.

[145] Source documents held by Recorded Future.

[146] “Company Introduction” [公司介绍], Techxcope [远望智库], https://archive.md/SlQEu.

[147] Ibid.

[148] Ibid.

[149] Ibid.

[150] Ibid.

[151] “Homepage”, Techxcope [远望智库], https://archive.md/w3pyD.

[152] “Intelligence Research” [情报研究], Techxcope [远望智库], https://archive.md/nZfT8.

[153] Ibid.

[154] “Homepage”, Techxcope; “Expert Base” [专家库], Techxcope [远望智库], https://archive.md/a3wO4; “Military Resources Net” [军事资源网], Techxcope [远望智库], https://archive.md/wwdbE.

[155] Zhang Qiang [张强], “Russia Builds Military-Use Internet, Starts Virtual Space Defense Battle” [俄建设军用互联网，打响虚拟空间保卫战], China Military Net [中国军网], September 24, 2019, https://archive.ph/ogz65; Zhang Qiang [张强], “What is the US’ Intentions for Replacing Ship Anti-Missiles with Land-based Systems” [美陆基系统替代舰船反导意欲何为], China Military Net [中国军网], June 27, 2018, https://archive.ph/7pKFg; Zhang Qiang [张强], “Our Country’s Introduction of S-300 Systems Intended to Add Flowers to Brocade” [我国引进俄S-400系统意在锦上添花], China Military Net [中国军网], January 24, 2018, https://archive.ph/Pl0V1.

[156] Chen Zeliang [陈泽亮] and Yin Baorui [尹宝瑞], “Behind the Global Top 100 Military Industry Enterprises Ranking Data: ’Stage’ of Competition Has Much to Watch” [全球百强军工企业排行榜数据背后：“擂台”竞技看点多], China Military Net [中国军网], November 6, 2020, https://archive.ph/nUj6x.

[157] Lan Shunzheng, “NATO countries discuss on European Sky Shield Initiative for independent defense”, China Military Online, October 24, 2022, https://archive.ph/cH0Aa; Li Daguang, “PLA development steady and peaceful”, *China Daily*, August 1, 2022, https://archive.ph/XWu9J.

[158] Stephen Chen, “China’s top weapons scientist says nuclear fusion power is 6 years away”, *South China Morning Post*, September 14, 2022, https://archive.ph/GlJLz; Kristin Huang, “Chinese military’s potential in the South China Sea boosted by Hainan amphibious assault ship, say analysts”, *South China Morning Post*, May 8, 2022, https://archive.ph/G5FHU.

[159] Pan Letian [潘乐天], “The Ins and Outs of US Military ‘Multi-Domain Battle’” [美军“多域战”的实质及启示], *Science & Technology Review* [科学导报] 35, no. 21 (2017); Huang Zhicheng [黄志澄], “The Success and the Challenge of DARPA’s Technological Innovation” [DARPA 技术创新的成功与挑战], *Science & Technology Review* [科学导报] 36, no. 4 (2018).

[160] Botht the 2020 and 2021 versions of the project.

[161] Source documents held by Recorded Future.

[162] “Beijing Kantian Science and Technology Co., Ltd. Recruitment Information” [北京瞰天科技有限公司招聘信息], Beijing Haidian District People’s Government [北京市海淀区人民政府], February 8, 2023, https://archive.ph/8rz3D.

[163] Ibid.

[164] Eda Kavlakoglu, “AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What’s the Difference?”, IBM, May 27, 2020, https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks; “Artificial intelligence (AI) vs. machine learning (ML)”, Azure, https://azure.microsoft.com/en-us/solutions/ai/artificial-intelligence-vs-machine-learning/#introduction.

[165] “A kind of Remote Sensing Target object identification method, device and storage medium”, Google Patents, https://archive.ph/sGE25

[166] “Aquatic target identification method and device, electronic equipment and storage medium”, Google Patents, https://archive.ph/tglIH.

[167] Jiang Yanchuan, “So-called Evidence of Chinese Vessels ‘Engaged in Surveillance of Thitu Island’”, SCSPI, March 11, 2020; https://archive.ph/7Fw6l; Chen Xiangmiao and Jiang Yanchuan, “‘Fact’ and ‘Fiction’: The Thitu Island Crisis”, SCSPI, June 16, 2019, https://archive.ph/nCbk6.

[168] Jiang, “So-called Evidence of Chinese Vessels ‘Engaged in Surveillance of Thitu Island’”; Chen and Jiang, “‘Fact’ and ‘Fiction’: The Thitu Island Crisis”.

[169] Ma Xiu, *PLA Rocket Force Organization* (Blue Path Labs and China Aerospace Studies Institute, 2022), https://www.airuniversity.af.edu/CASI/Display/Article/3193056/pla-rocket-force-organization/.

[170] Ibid.

[171] Original Chinese: “外军智能识别图像采集专用网络技术服务”.

[172] Original Chinese: “XXX知识库软件系统”.

[173] Original Chinese: “外军在役主战坦克升级改造发展研究”.

[174] Original Chinese: “某数据分析系统”.

[175] Original Chinese: “国外网络空间安全开源研究电子资料”.

[176] Original Chinese: “国外XX装备关键材料考核评价技术资料汇总分析研究”.

[177] Original Chinese: “外军装备体系贡献率开源情报资料”.

[178] Original Chinese: “开源信息常态化服务项目”.

[179] Original Chinese: “世界主要国家智库建设情况与运行机制研究”.

[180] Original Chinese: “XXXX开源情报跟踪研究”.

[181] Original Chinese: “科技信息常态化服务”.

[182] Original Chinese: “目标知识库构建及目标变化检测软件”.

[183] Original Chinese: “外军战争决策与战争准备相关信息采集分析”.

[184] Original Chinese: “外军XX武器装备发展动态跟踪分析系统”.

[185] Original Chinese: “国外班组级地面无人装备资料收集、翻译及整理”.

[186] Original Chinese: “外军新质作战力量建设与新兴军事技术发展相关数据采集分析”.

[187] Original Chinese: “外军新一代履带装甲车辆技术发展文献数据资源服务”.

[188] Original Chinese: “通用领域科技情报监测平台”.

[189] Original Chinese: “2022年度外军网电对抗领域科技信息研究”.

[190] Original Chinese: “基于全球重热点地区高分辨率卫星遥感影像的地理空间环境分析研判”.

[191] Original Chinese: “开源情报跟踪研究”.

[192] Original Chinese: “强敌海军陆战队作战概念开发与装备建设情况相关资料检索与翻译”.

[193] Original Chinese: “开源综合研究学习平台”

[194] Original Chinese: “外军开源数据软件平台及数据资源”.

[195] Original Chinese: “美军典型无人机系统入网应用资料整理分析”.

[196] Original Chinese: “智能处理器相关文献和资料分析服务”.

[197] Original Chinese: “外军XX单元情报数据收集与翻译整编”.

[198] Original Chinese: “世界主要国家海外保障设施综合研究”.

[199] Original Chinese: “战略新兴技术国际合作科学计量分析”

[200] “Web of Science”, Clarivate, https://clarivate.com/webofsciencegroup/solutions/web-of-science/; “Derwent Innovations Index on Web of Science”, Clarivate, https://clarivate.com/webofsciencegroup/solutions/webofscience-derwent-innovation-index/; “Derwent World Patents Index (DWPI)”, Clarivate, https://clarivate.com/products/ip-intelligence/ip-data-and-apis/derwent-world-patents-index/.

[201] Original Chinese: “XX机械臂遥操作情报研究”.

[202] Original Chinese: “美军分布式地面情报处理装备技术情报资料专题研究”.

[203] Original Chinese: “XX数据采集服务”.

[204] Original Chinese: “网电对抗领域强敌研究相关开源情报支撑”.

[205] Original Chinese: “外军网电对抗领域科技信息研究”.

[206] Original Chinese: “XX科技信息服务”.

[207] Original Chinese: “2021年度外文原版期刊”.

[208] Original Chinese: “知远某某数据库”.

[209] Original Chinese: “美日印澳地缘战略情报搜集分析”.

[210] Original Chinese: “多孔材料空气取水情报收集与综合分析研究”.

[211] Original Chinese: “科技情报研究手段及能力提升条件建设”.

[212] Original Chinese: “外军典型装甲装备作战效能评估基础模型和数据资源体系建设研究”.

[213] Original Chinese: “冰上丝绸之路陆海联运地理空间情报资料整编”.

[214] Original Chinese: “XX科技信息服务”.

[215] Original Chinese: “外文原版期刊及年鉴拟”.

[216] Original Chinese: “外军情报资料数据采集”.

[217] Original Chinese: “外国陆军无人作战装备情报研究”.

[218] Original Chinese: “外军电磁频谱战装备情况调研”.

[219] Original Chinese: “IHS-Jane’s防务等数据库”.

[220] Original Chinese: “知远防务研究所文献资料”.

[221] Original Chinese: “互联网数据采集与分析系统软件”.

[222] Original Chinese: “科技情报挖掘技术文本标注”.

[223] Source documents held by Recorded Future.