March 2021

The Public AI Research Portfolio of China's Security Forces

A High-Level Analysis

CSET Data Brief

AUTHORS
Dewey Murdick
Daniel Chou
Ryan Fedasiuk
Emily Weinstein

Executive Summary

The overwhelming majority of Chinese artificial intelligence and machine learning, or simply AI, research coauthored by People's Republic of China (PRC) security force organization affiliates is published in Chinese, not in English. Despite the general decrease in the number of security force papers in all topics, AI research bucks the trend and continues to increase in volume. Computer vision is the most active subfield of AI research, much more so than natural language processing or robotics. The PRC security force organizations discussed in this brief include two police-like forces (the Ministry of Public Security and People's Armed Police Force) and the various components of the People's Liberation Army (PLA). The military components produce the largest share of AI research output by volume and each specializes in mission-relevant AI applications, such as multi-target tracking and targeting, and air/surface/underwater autonomous systems, among others. The policing organizations, likewise, have mission-specific areas of emphasis in facial recognition, gait recognition, forgery detection, fingerprint recognition, and steganography, among others.

Introduction and Overview

The PRC has set about prioritizing AI technologies and applications as part of its larger military modernization and economic competitiveness efforts. Chinese President Xi Jinping has spoken at length about the importance of AI, arguing in May 2019 that AI is the "driving force for scientific and technological development, industrial optimization and upgrading … and major productivity improvements."[1] In the military space, in its drive for "intelligentized" (智能化) warfare, the PLA is pursuing various types of AI-enabled weapons systems, including unmanned vehicles and intelligent software.[2]

The "New Generation Artificial Intelligence Development Plan" (新一代人工智能发展规划) is the seminal policy that lays out China's AI aspirations, spanning AI education, technology standards, military advancements, agriculture, talent, and many other fields.[3] The plan lays out incremental goals for the improvement of China's AI capabilities through 2030, in conjunction with large-scale industrial policies like China's 13th Five-Year Plan[4] and the Strategic Emerging Industries lists.[5]

China's security forces are also incorporating AI into their logistics and combat operations. The PRC maintains police, military, paramilitary, and intelligence organizations to enforce law, maintain domestic order, serve domestic communities, engage in foreign military relations, and otherwise protect national security interests.[6] The high-level PRC security force organizations considered in this data brief include the following:

1. Ministry of Public Security (MPS), the national police agency that exercises oversight of the nation's day-to-day law enforcement and security.[7]

2. People's Armed Police Force (PAP), a PRC paramilitary organization that is responsible for maintaining domestic order during periods of unrest in the face of riots, terrorism, and disaster response and otherwise "has the duty to assist other law enforcement forces in arrest, pursuit, and escort

operations."[8] The PAP also supports the military during wartime.[9]

3. People's Liberation Army, the armed forces of the PRC, including the Air Force (PLAAF), Ground Force, and a mix of other miscellaneous organizations that are part of the PLA (PLAGF/M), Navy (PLAN), and Rocket Force (PLARF).

All of these organizations maintain research capabilities of some sort, which have some unknown mix of openly discussed and undisclosed projects. This data brief describes the publicly disclosed research activity of individual researchers as aggregated at the organizational level. It also analyzes scholarly papers* authored by researchers that claim a direct working affiliation to the above security force organizations or their components.[10] We informally refer to such papers as "authored" by the organizations if one or more authors of the paper are affiliated with that organization; however, this does not mean that each of these research papers reflects the official position of the affiliated organization. After a review of the English and Chinese scholarly literature, we omit the Ministry of State Security from our analysis, which authored less than 50 public papers.†

We analyze publication activity from 2010 to 2019 and find, perhaps unsurprisingly, that most security force agencies openly published scholarly papers in Chinese-language venues, as included in the Chinese National Knowledge Infrastructure (CNKI).[11] Specifically, 83 percent (597,753 papers) of the PRC security force affiliated papers are published in Chinese venues.‡

---

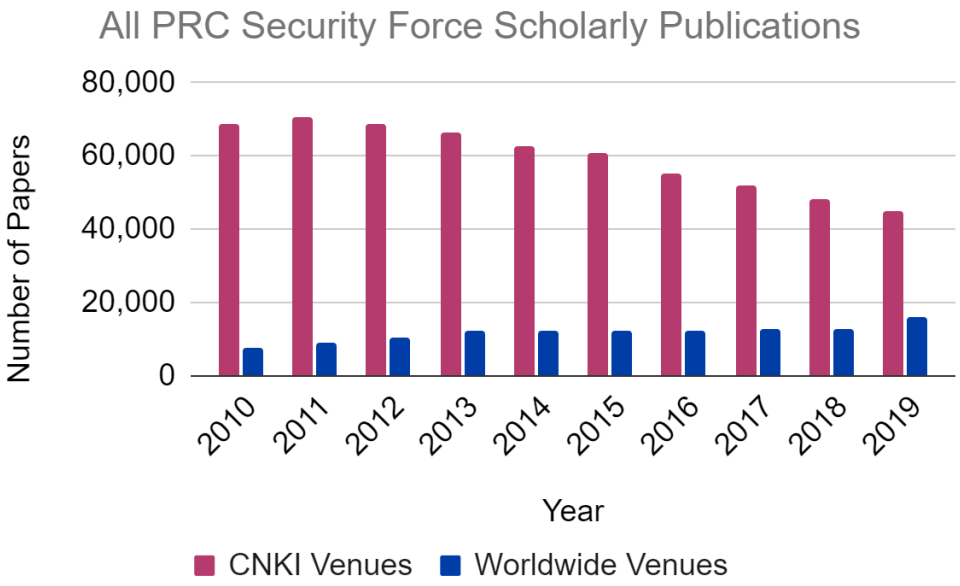
* We consider a paper to be a scholarly paper if (a) it is included in a preprint archive or one of CSET's publication databases and (b) contains references that cite other papers.

† Note that only 21 papers are authored by researchers with Ministry of State Security affiliations from January 2005 to June 2020 in the CNKI database; therefore, this organization is excluded from this analysis.

‡ This data brief only includes papers authored by individuals directly affiliated with security force organizations rather than reviewing academic work funded by these organizations or all the content in journals dedicated to research regarding their mission. This provides the most direct public signal of institutional research activity. A full analysis would be comprehensive if it included all these methods, but that is beyond the scope of this paper.

The remaining 17 percent (118,131 papers) are published in worldwide venues, see Figure 1. When we specifically review AI-relevant papers, we found that this phenomenon is even more pronounced, with 93 percent (51,602 papers) of the total AI-related PRC security force-authored papers only available in CNKI.

Figure 1. Total number of papers authored from 2010 to 2019 by researchers with PRC security force affiliations in all topics, across Chinese- and English-language venues.



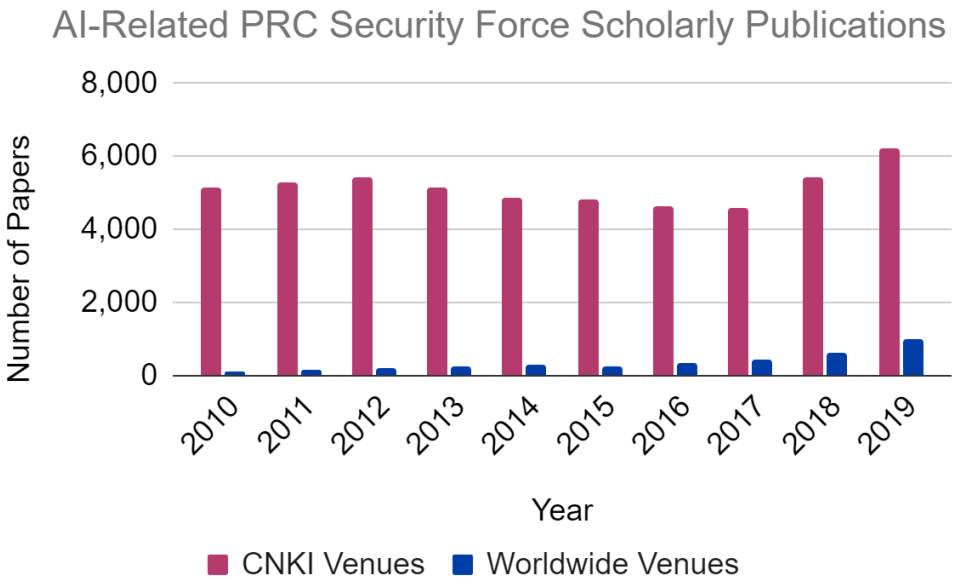
Sources: CSET Merged Corpus and CNKI, queried October 2020.

Although the overall annual number of Chinese-language security force papers has been decreasing in all topics, PRC security forces are bucking that trend and becoming more active in openly published AI research, as depicted in Figures 1 and 2. The overall quantity of papers in all venues and authored by PRC security force researchers drops roughly 3 percent per year (or just under 1,900 papers per year) from 2017 to 2019.* This stands in stark contrast with the number of security force papers published on the topic of

* The total number of papers published worldwide dropped by just under 2 percent by year from 2017 to 2019. These include unique paper records from three worldwide paper databases and one Chinese paper database. The PRC security force drops 1.56 times faster than the worldwide average during this same time.

AI in 2017–2019, which has grown on average 18 percent per year (1,116 papers per year), see Figure 2.

Figure 2. Total number of AI-relevant papers authored from 2010 to 2019 by researchers with PRC security force affiliations across Chinese- and English-language venues.



Sources: CSET Merged Corpus and CNKI, queried October 2020.

Topical Analysis with Research Clusters

We start our analysis with 49,105 AI PRC security force authored papers in CNKI between 2010–2019, which are distributed over 14,238 topical research clusters.* As we filter these clusters further for AI-relevance,[12] we use this research structure to find and explore especially active research topics and from there, infer the publicly accessible view of the high-level research agenda for the PRC security community.†

These clusters organize the global scientific research activity into groups of documents that are similar, meaning they tend to cite one another more than papers outside their cluster. Each group of related papers tend to focus on specific research problems, not groups of people, and are not intended to represent personal or professional relationships or networks. We analyze the high-level research agenda through the lens of these topical research groups. Table 1 provides a high-level summary of the topical areas in which the PRC security forces publish their AI-related papers. Unsurprisingly, the vast majority of AI-related papers are published in computer science, but AI applications are also evident in engineering, medicine, biology, physics, and materials science, among others.

---

* The topical research cluster structure is created by CSET's global research model and is constructed out of over 104.8 million papers and 127 thousand research cluster groupings dating back to 2005. This represents more than 90 percent of the world's scientific literature based on conservative estimates. Note that an AI paper can be clustered into a topical research cluster that does not meet the threshold to be an AI-relevant research cluster.

† To accomplish this topical analysis, the authors leverage CSET's comprehensive network of the world's scholarly publications that are connected by paper-to-paper citation links. The primary sources used include CNKI (Tongfang Knowledge Network and distributed by East View), Dimensions (Digital Science), Microsoft Academic Graph (Microsoft), and Web of Science (Clarivate) data repositories. The resulting set of over 104.8 million papers have over 1.4 billion citation links, which are used to create 127 thousand research clusters.

Table 1. Breakdown of PRC security force participation in high-level subject areas.

Subject Area	Number of Research Clusters	Total AI Papers	PLA Total AI Paper Count	MPS Total AI Paper Count	PAP Total AI Paper Count
Computer Sci.	5,095	27,786	25,783	1,638	805
Medicine	2,065	3,268	3,062	78	187
Engineering	1,824	7,192	6,959	172	144
Mathematics	852	3,139	3,004	104	59
Biology	849	1,465	1,394	45	47
Materials Sci.	842	1,455	1,408	33	27
Chemistry	501	858	754	89	49
Psychology	412	613	528	70	28
Enviro. Sci.	361	697	656	31	15
Physics	349	793	769	14	16
Business	318	546	476	60	20
Geology	236	497	462	7	38
Economics	211	285	257	28	4
Sociology	104	144	115	30	5
Geography	98	190	165	25	8
Political Sci.	86	139	120	18	5
Unknown*	16	17	16	1	0
Art	8	10	5	5	2
Philosophy	7	7	4	3	0
History	4	4	3	1	0
Total	14,238	49,105	45,940	2,452	1,459

Source: CNKI, summary statistics are current as of October 2020.

* The high-level topical categories are determined by finding the most common Microsoft Academic Graph's high-level topical label for papers in each cluster. Note that 16 research clusters have no label because there are an insufficient number of papers included by Microsoft Academic Graph to accurately assign the high-level category.

Publication activity is not uniform across the security forces. We see that PLA researchers author the largest number of papers with 94 percent of the total AI security force papers in CNKI, followed by MPS (5 percent) and PAP (3 percent).* Interestingly, 12 percent of AI-relevant papers are coauthored by PRC security force researchers affiliated with hospitals or other organizations of an obviously medical nature.† The smaller number of papers published by PAP-affiliated authors would seem to indicate that a larger fraction of PAP research is not public, as compared to MPS.

We know that AI is not a 'thing' or a 'widget' and that the landscape of AI is not homogenous. Chinese and U.S. experts generally agree on descriptions of how artificial intelligence (人工智能) could be applied to weapon systems, envisioning numerous applications related to intelligent command and control systems; autonomous vehicles; and intelligence, surveillance, and reconnaissance software, among others.[13] In order to better understand the actual impact of subdomains within the scientific field of AI research, we break down this classification further into three broad application types: computer vision (how computers process and interpret images and videos), natural language processing (how computers process, interpret, and use human language), and robotics (how programmable machines use AI to interact with their environment). A fourth category is added for General AI/ML (machine learning), which collects papers that are not strongly related to these three areas.‡ This breakdown enables analysis of topical research areas strongly associated with coherent AI-relevant research communities and focuses our attention on 13,093 papers in these research clusters.

---

* Note that the percentages do not sum to 100 percent because some papers are coauthored by individuals from a combination of PLA, MPS, and PAP researchers.

† The PAP (21 percent) and PLA (13 percent) have the largest fraction of medically-relevant AI research papers, while MPS has a very small fraction of its work in this domain (2 percent).

‡ Each research cluster is classified into one of the four bins when at least 25 percent of its papers are tagged as relevant and it is the most common classification.

The computer vision category is the largest focus area of research for the PRC security forces. This work includes, but is not limited to: target detection, object tracking, hyperspectral imaging, facial recognition, gait recognition, vehicle detection, forgery detection, and fingerprint recognition. This emphasis on AI-based computer vision is also seen more broadly in Chinese paper and patenting activity across the entire country.[14] Natural language processing garners considerably less attention overall, and often focuses on areas such as sentiment analysis, analysis of online social media, and text classification. Robotics likewise attracts relatively less attention and covers areas such as control systems, unmanned aerial vehicles (UAVs), underwater autonomous systems, surface autonomous vehicles, robotic exoskeletons, and humanoid robotics research. The General AI/ML category contains a mixed group of application areas and covers topics such as, path planning, targeting, multi-target tracking, intrusion detection, computer network operations, steganography, and other application areas (e.g., data analysis, medicine, electrical or mechanical engineering, advanced materials engineering, etc.). Table 2 shows this breakdown by AI-relevance for each PRC security force.* The table also disaggregates the PLA into PLAAF, PLAGF/M,† PLAN, and PLARF components.

* We tabulate based on author-reported affiliations in each paper. In particular, we did not investigate whether an author holds multiple appointments.

† PLA Miscellaneous Organizations refer to PLA-affiliated entities outside of combatant command units. Examples: Academy of Military Science (军事科学院), National University of Defense Technology (国防科技大学), General Armaments Department/Equipment Development Department (总装备部/装备发展部), Strategic Support Force (战略支援部队).

Table 2. Count of PRC security force-authored AI papers and number of AI-relevant topical research clusters (RCs) over which they are distributed by broad application type.

PRC Security Force Organization	General AI/ML *Papers (RCs)*	Computer Vision *Papers (RCs)*	Natural Language Processing *Papers (RCs)*	Robotics *Papers (RCs)*
MPS	285 (183)	470 (195)	47 (28)	9 (7)
PAP	151 (100)	189 (110)	6 (5)	11 (11)
PLAAF	1,217 (354)	650 (196)	14 (13)	45 (29)
PLAGF/M	3,190 (667)	2,963 (423)	283 (78)	304 (104)
PLAN	1,122 (339)	628 (206)	26 (20)	123 (44)
PLARF	696 (250)	603 (173)	7 (6)	54 (33)
Grand Total	**6,661**	**5,503**	**383**	**546**

Source: CNKI, summary statistics are current as of October 2020.*

PRC security force organizations tend to be relatively small players in the larger research clusters. This is expected due to the applied nature of their work and the likelihood that discussion of specific AI applications is most likely avoided in public.

* To avoid double counting, research cluster totals are not summed. It is possible that a research cluster contains papers from more than one organization or PLA component.

As we conclude our high-level review of the PRC security force public research portfolio, let us turn our attention back briefly to the 3,734 AI-relevant papers (7 percent of the total PRC security force AI output) published outside of CNKI in largely English-language venues. We find that the vast majority of these papers written in English are published in the same topical research clusters as those published in CNKI. Of the 1,690 unique AI-relevant research clusters containing papers from CNKI, all but one also have PRC security force authored papers in English. Additionally, the papers written in English expand the PRC security force presence thinly across an additional 742 topical areas (31 percent expansion). The largest relative increase in topical coverage is in the area of natural language processing.[*]

[*] The expansion in topical research cluster (RC) coverage with the inclusion of English-language venues beyond those in CNKI is as follows: adds 169 RCs for a total of 702 RCs (24 percent of total) in computer vision, 89 RCs for a total of 186 RCs (48 percent of total) in natural language processing, and 93 RCs for a total of 272 (34 percent of total) in robotics.

Exploring Specific Research Clusters

Digging deeper into particular research clusters can offer additional insights. An example of such analysis is provided in the following sections to highlight the utility of this analytic approach. What follows highlights one or two research clusters per organization and is not designed to be a comprehensive review of the literature published by each organization.

Ministry of Public Security

The MPS has long leveraged data mining and AI research to improve its surveillance and intelligence capabilities.[15] Two of MPS' key AI research clusters deal with visual object tracking, data mining, and counterterrorism intelligence (反恐情报). Of the 127 papers authored by PRC security forces on visual object tracking, 11 are by authors affiliated with MPS, which has a small public research footprint, relative to the other security forces assessed in this study.*

This cluster activity connects to broader signals and priorities seen in Chinese media and government documents. For example, in 2017, the MPS Internet of Things Technology R&D Center (物联网技术研发中心)—which sponsored two of MPS' AI research papers in this cluster—unveiled an "Airport Public Security Intelligence Big Data Research, Analysis, and Decision Support System" (机场公安情报大数据研判分析系统) for deployment in airports in Nanjing and Chengdu.[16] The system is designed to collect and integrate information from video surveillance cameras, mobile terminals, and passengers' social media profiles into a database that security officers can search and apply to real time video feeds. The ultimate goal is to identify suspicious passengers, track pedestrians, or monitor crowd formation. These types of research activities continue into 2021.[17]

Beyond its in-house research and development, MPS is also contracting with private companies to develop advanced

* Note that 2,470 (5 percent) of the scientific papers in this study were by MPS authors.

surveillance tools. The company Henan 863 Software, for example, is marketing an “Anti-Terrorism Big Data Visualization Command Platform” (反恐大数据可视化指挥平台), which it calls “a support platform for the management departments of public security organs.”[18] These kinds of data streams also contribute to the formation of China’s “smart cities,” which integrate and manage data related to traffic, energy usage, and crime.[19]

People's Armed Police Force

The PAP appears to be heavily invested in applying AI to steganography (a practice for concealing a message within a public message or image).[20] Two research clusters in particular have a significant PAP presence; first on steganography images and methods (22 papers by PAP authors), and steganalysis—the analysis of steganographic images (27 papers by PAP authors). With its primary focus in internal security, this indicates that the PAP may be conducting AI-related steganographic research in the context of monitoring and surveilling Chinese citizens. In 2017 and 2018, the PAP underwent “the most profound restructuring since its establishment in 1982,” coming under the centralized control of Xi Jinping.[21] Over the past decade, the PAP has been involved in the construction and management of China’s broad surveillance apparatus, most notably in Xinjiang Uyghur Autonomous Region, where the PAP have been involved in augmenting local police forces, deploying facial recognition and surveillance technology, and opening and overseeing “re-education camps.”[22]

There is evidence beyond the scientific literature that further suggests the PAP’s interest in steganography. For example, in 2015, the PAP filed a steganography-related patent entitled “A kind of image latent writing analysis method and its device” (一种图像隐写分析方法以及其装置).[23] In addition, the PAP Engineering University in 2020 won five awards from the Chinese Ministry of Education for projects associated with steganography, including “Identity authentication system based on implicit learning” (基于内隐学习的身份认证系统) and "Image code system based on SM9 and steganography” (基于 SM9 和隐写术的“图像码”系统).[24]

People's Liberation Army, Air Force

The PLAAF is most active in a research cluster focused on AI papers, methods, and evidence theory. Within this cluster, the PLAAF-affiliated authors wrote 106 papers. The PLAAF papers indicate a focus on AI at a theoretical level, as Chinese experts believe that AI will be applicable to many air-related technologies, including UAVs and air defense systems.[25] Many of the papers in this cluster appear to relate to target recognition evidence and theories, spanning as early as a 2006 paper on "Intelligent target recognition method of sequential images based on DSmT" and a 2007 paper entitled "Target recognition system based on D-S theory of conflict evidence."

Notably, 56 papers in this cluster are written in conjunction with any one of China's Seven Sons of National Defense (国防七子), a group of seven Chinese universities under the Ministry of Industry and Information Technology that play an important role in Chinese defense research and development (R&D).[26] Of the 56 papers written with Seven Sons universities, almost all are written in conjunction with Northwestern Polytechnical University (NWPU; 西北工业大学).* According to the Australian Strategic Policy Institute, NWPU research focuses on aviation and space technology and is known for UAV R&D.[27] NWPU is also heavily involved in target recognition-related research in AI and ML and has published significantly on this subject.[28] Furthermore, NWPU has filed at least two related patents, including a 2010 patent entitled "A method for detecting and tracking infrared dim and small targets in a complex background" (一种复杂背景下红外弱小目标检测和跟踪方法)[29] and a 2017 patent on "Spatial target recognition method based on deep learning" (基于深度学习的空间目标识别方法).[30] These findings are consistent with prior assessments of PLAAF-sponsored research, which has noted a focus on AI-enabled air defenses.[31]

* It is important to note that NWPU has a deep-rooted history with military aeronautics, as it is the result of the merging of three Chinese research entities: Northwestern Engineering Institute, the East China Aeronautics Institute (also referred to as the Xi'an Aeronautic Institute), and the PLA Military Engineering Institute.

People's Liberation Army, Ground Force / Miscellaneous

PLA universities, specifically the National University of Defense Technology, appear interested in applying AI to unmanned ground and all-terrain vehicles, as demonstrated in a research cluster focused on terrain, robots, and methods. Of the 18 papers in this cluster, 10 are written by NUDT. The remaining eight papers are coauthored with researchers from various Seven Sons and civilian universities, and one is written by a PLA unit likely associated with Central Military Commission's Logistics Support Department.

The majority of papers in this cluster assess ways to improve an unmanned or robotic systems' ability to navigate difficult terrain. For instance, a 2017 paper from Tianjin University of Technology proposes a classification algorithm to facilitate a robot's movement abilities by perceiving the surrounding environment, and a NUDT paper from 2011 looks for ways to build an automated navigation system for an off-road environment. Others in this cluster look to improve a robot's ability to detect hazards, such as a 2014 piece entitled "A summary of water obstacle recognition technology in complex field environments" (复杂野外环境下水障碍识别技术综述).

All of the work done by NUDT in this cluster comes out of the Key Laboratory of Electrical Engineering and Automation (国防科大机电工程与自动化学院重点实验室), which is housed within the School of Intelligence Science. According to the school's description, over 300 million RMB has been invested to focus on R&D in weapon equipment automation and simulation, unmanned combat, and precision guidance, among other topics.[32]

People's Liberation Army, Navy

The PLAN envisions several applications of AI, but two of the most prominent explore remote sensing and autonomous underwater vehicles (AUV). Specifically, two research clusters focus on decluttering radar to detect underwater objects, and modulating and classifying radar signals. Of the 206 papers authored by PRC security forces in the radar signal cluster, 23 are by authors affiliated with the PLAN.

Most PLAN papers in these clusters discuss using ML methods to improve undersea radar detection and object identification—typically by calculating and applying mathematical filters in real time to reduce unintentional clutter or noise,[33] and fusing those signals to create radar signature libraries comprising a wide array of targets.*

The PLAN authors frequently partner with other research institutions, and one of the most common is the Shenyang Institute of Automation (SIA; 沈阳自动化研究所) within the Chinese Academy of Sciences. Since its founding in 1958, SIA has been a forerunner of China's underwater autonomy and AI research. The institute has signed strategic cooperation agreements with most prominent Chinese defense companies—including the world's largest shipbuilding conglomerate, China Shipbuilding Industry Corporation—and frequently coauthors research with the PLAN.[34] In the 1990s, SIA unveiled its first AUV, the CR-01 Explorer. Over the past 25 years, it has made gains in the fields of undersea object detection and unmanned vehicle navigation. As of 2020, SIA plans to develop two series of AUVs, capable of traversing long ranges or diving to deep-sea depths.[35]

People's Liberation Army, Rocket Force

The PLARF is looking to leverage AI primarily to improve missile guidance and target discrimination. Its two largest research clusters focus on using ML in celestial navigation and control systems to improve missile guidance, and to help missile defense systems discriminate between objects in an intercontinental ballistic missile (ICBM) threat cloud.[36]

The PLARF's chief application of AI is to help missile seekers detect and recognize targets. In 2020, the PLARF launched a $1.1 million competition entitled "Intelligence Rocket, Fire Eyes" ("智箭•火眼"),[37] in which it sponsored teams of Chinese university researchers to

* PLAN papers included titles such as "Modulation Classification of Communication Signals Based on Broad First Search Neighbors Clustering," "Novel method for extracting features of MPSK signal," and "An Algorithm for Automatic Identification of Digital Modulation Types."

develop AI applications useful for ballistic missile guidance systems.[38] Specifically, the competition focused on image recognition and remote sensing applications capable of operating in cluttered environments.[39] Intelligence Rocket, Fire Eyes is one of many research and entrepreneurship competitions the PLA is leveraging to innovate in AI.[40] But much of the PLARF's own AI research has focused on celestial guidance systems—using machine learning to recognize and calculate a missile's position in space relative to certain stars.

The PLARF also supports autonomous flight research. Its fourth largest AI research cluster focuses on improving autonomous navigation in missile systems. Of the 123 papers authored by PRC security forces within this cluster 25 papers are by authors affiliated with the PLARF. The PLARF research into autonomous flight has already paid dividends for China's cruise missile industry. In 2018, the China Aerospace Science and Technology Corporation unveiled the CH-901—an autonomous, loitering munition similar to the Israeli IAI Harpy.[41] Achieving fully autonomous cruise missile navigation would significantly improve the PLA's anti-access/area-denial capabilities.

Conclusions

It has been well established that the Communist Party under Xi Jinping is seeking to make AI a national priority for China.[42] That priority naturally extends to its security forces and defense industry. But the actual status of AI research in China has been less clear, especially where security is concerned.[43]

Analysis of the scientific literature has long been discussed as a useful resource in understanding activities in technical advances around the world.[44] However, it is often difficult to provide analysis that can be contextualized in any meaningful way. Here we show that not only can our comprehensive approach to clustering worldwide scientific literature into topical networks be useful, it can even shed light on communities once viewed as difficult to explore using publicly available information.

This analysis uses new analytic methods and clearly shows that publicly available research information can give us a useful signal into military, paramilitary, and law enforcement research portfolios around the world. The Chinese security forces are openly publishing in their own language, and while this is clearly not a comprehensive representation of their work, it is a signal that should not be ignored.

Beyond the security forces themselves, ostensibly-civilian institutions like the Seven Sons of National Defense and the Chinese Academy of Sciences likely play a significant role in security- and defense-related scientific research. Policies like China's military-civil fusion (MCF; 军民融合) strategy are looking to the civilian sector to develop new and innovative ideas. Although this report briefly touches on examples of coauthorship between the PLA and these universities, further research is required to assess what role these institutions play in overall security research.

Public scientific literature shows an increasing emphasis on AI research in the Chinese security forces against the backdrop of an overall drop in open publication. Within AI, the PRC security forces are focusing on a variety of research areas that support policing and military-relevant activities that go beyond facial recognition to

include capabilities such as target detection, object recognition, and hyperspectral imaging. Lastly, we find that much of this openly published work is consistent with higher level doctrine and activities, which suggests that this is a valuable tool for better understanding Chinese military priorities.

Authors

Dewey Murdick is the interim director at CSET, where Daniel Chou is a data scientist, and Ryan Fedasiuk and Emily Weinstein are research analysts.

Acknowledgments

For feedback and assistance, we would like to thank Catherine Aiken, Melissa Deng, Shelton Fitch, Melissa Flagg, Igor Mikolic-Torreira, Ilya Rahkovsky, and Joel Wuthnow. The authors are solely responsible for the views expressed in this data brief and for any errors.

Document Identifier: doi: 10.51593/20200057

Endnotes

[1] Yang Cheng, Fan Feifei, and Ouyang Shijia, "President stresses AI's role in growth," *China Daily*, May 17, 2019, https://www.chinadaily.com.cn/a/201905/17/WS5cddb746a3104842260bc1f9.html.

[2] Elsa Kania, "'AI Weapons' in China's Military Innovation" (Brookings Institution, April 2020), https://www.brookings.edu/research/ai-weapons-in-chinas-military-innovation/.

[3] Graham Webster, Rogier Creemers, Paul Triolo, and Elsa Kania, "Full Translation: China's 'New Generation Artificial Intelligence Development, Plan' (2017)," *New America*, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[4] "Outline of the 13th Five-Year Plan for National Economic and Social Development of the People's Republic of China" [中华人民共和国过敏经济和社会发展第十三个五年规划纲要], *Xinhua News*, March 17, 2016, http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm.

[5] Elsa Kania, Ngor Luong, Caroline Meinhardt, Ben Murphy, Dahlia Peterson, Helen Toner, Graham Webster, and Emily Weinstein, "New Chinese Ambitions for 'Strategic Emerging Industries,' Translated," *New America*, September 29, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/new-chinese-ambitions-strategic-emerging-industries-translated/.

[6] See for example: (1) Harvey W. Nelsen, *The Chinese Military System: An Organizational Study Of The Chinese People's Liberation Army*, 2nd ed (Routledge, 2019). (2) Michael Palmer, "Changing Policing in the People's Republic of China," *Taiwan in Comparative Perspective* 3 (March 2011): 66–98.

[7] The Ministry of Public Security of the People's Republic of China, official homepage, https://www.mps.gov.cn/ with a April 16, 2020 snapshot here.

[8] Xinhua, "Top Legislature Passes Armed Police Law," *China Daily*, August 27, 2009, http://www.chinadaily.com.cn/china/2009-08/27/content_8625494.htm. Ivan Y. Sun and Yuning Wu, "The Role of the People's Armed Police in Chinese Policing," *Asian Journal of Criminology* 4, no. 2 (November 11, 2008): 107, https://doi.org/10.1007/s11417-008-9059-y.

[9] Joel Wuthnow, "China's Other Army: The People's Armed Police in an Era of Reform," *China Strategic Perspectives* 14 (April 16, 2019), https://inss.ndu.edu/Media/News/Article/1815868/chinas-other-army-the-peoples-armed-police-in-an-era-of-reform/.

[10] Please see GitHub for additional technical details regarding the queries and clusters, https://github.com/georgetown-cset/public-ai-research-portfolio-of-china-security-forces.

[11] CNKI was launched in 1988 as an electronic platform to integrate Chinese knowledge-based information resources. It has become the largest source of Chinese science and technology, humanities and social sciences, politics, and economics content and includes resources, such as, China Academic Journals (used in this study), China Core Newspapers, China Doctor/Master's Dissertations, and China Proceedings and Conferences. See https://global.cnki.net/index/ and https://www.eastview.com/resources/cnki-faq/ for more information.

[12] It is important to note that this analysis makes no attempt to characterize the quality of these research papers. A research cluster is designed as being AI-relevant if 25 percent of its papers contain either a set of Chinese AI-related keywords or are classified as AI-relevant by a modern machine learning-based classifier. The details of these approaches are explained in James Dunham, Jennifer Melot, and Dewey Murdick, "Identifying the Development and Application of Artificial Intelligence in Scientific Text," *arXiv [cs.DL]*, arXiv, May 28, 2020, https://arxiv.org/abs/2002.07143.

[13] Ryan Fedasiuk, "Chinese Perspectives on AI and Future Military Capabilities" (Center for Security and Emerging Technology, August 2020), https://cset.georgetown.edu/research/chinese-perspectives-on-ai-and-future-military-capabilities/.

[14] See Dewey Murdick, James Dunham, and Jennifer Melot, "AI Definitions Affect Policymaking" (Center for Security and Emerging Technology, June 2020); Patrick Thomas and Dewey Murdick, "Patents and Artificial Intelligence: A Primer" (Center for Security and Emerging Technology, September 2020); and Simon Rodriguez, Autumn Toney, and Melissa Flagg, "Patent Landscape for Computer Vision: United States and China" (Center for Security and Emerging Technology, September 2020).

[15] Elsa Kania, "Seeking a Panacea: The Party-State's Plans for Artificial Intelligence (Part 2)," *Center for Advanced China Research*, November 15, 2017, https://www.ccpwatch.org/single-post/2017/11/15/seeking-a-panacea-the-party-state-s-plans-for-artificial-intelligence-part-2.

[16] Zhao Xin, "The three institutes of the Ministry of Public Security strive to build an airport public security intelligence big data research and analysis system," *Airport* Security, June 26, 2017.

[17] MPS has spun up its AI research to develop and deploy AI-based surveillance tools nationwide. In March 2020, the China National Information Center (国家信息中心) outlined an advanced surveillance and policing system capable of integrating data from Chinese citizens' social media profiles and CCTV cameras,

among other platforms. MPS patented a similar tool designed to collect participatory GIS data in 2016. In terms of machine learning techniques employed, MPS system apparently uses online (Spark) and offline (MapReduce) processing, streaming processing (Storm), graph computing (Neo4j), full-text retrieval (SolrCloud), and natural language processing. See "Public Security data analysis platform construction under the background of big data" [大数据背景下公安数据分析平台建设], *National Information Center* [国家信息中心], March 12, 2020, https://web.archive.org/web/20201027190949/http://www.sic.gov.cn/News/612/10439.htm; "Police big data mining and analysis platform based on PGIS and cloud computing" [基于 pgis 和云计算的警务大数据挖掘与分析平台], *Changzhou Aegis Software Technology Co., Ltd.* [常州神盾软件科技有限公司], https://web.archive.org/web/20201027191030/https://patents.google.com/patent/CN106528809A/zh.

[18] "Anti-terrorism big data visualization command platform," [反恐大数据可视化指挥平台], *Henan 863 Software Co., Ltd.* [河南八六三软件股份有限公司], https://web.archive.org/web/20201027155708/https://www.863soft.com/cn/solutionContents-sub.html?id=fae8a1161ee84eb9b0d0d41e51a01673.

[19] Katherine Atha et al., "China's Smart Cities Development" (U.S.-China Economic and Security Review Commission, January 2020), https://www.uscc.gov/research/chinas-smart-cities-development.

[20] James Stanger, "The Ancient Practice of Steganography: What Is It, How Is It Used and Why Do Cybersecurity Pros Need to Understand It," CompTIA, July 6, 2020, https://www.comptia.org/blog/what-is-steganography.

[21] Wuthnow, "China's Other Army," 1–45.

[22] Wuthnow, "China's Other Army"; and James Millward and Dahlia Peterson, "China's System of Oppression in Xinjiang: How it Developed and How to Curb It" (Brookings Institution, September 2020), https://www.brookings.edu/research/chinas-system-of-oppression-in-xinjiang-how-it-developed-and-how-to-curb-it/.

[23] "An image steganography analysis method and its device" [一种图像隐写分析方法以及其装置], *Chinese People's Armed Police Force Engineering University* [中国人民武装警察部队工程大学], https://patents.google.com/patent/CN104636764B/zh.

[24] "The 13th National University Student Information Security Competition in 2020—Entries and Finalists" [2020 年第十三届全国大学生信息安全竞赛-作品赛 – 决赛作品获奖名单], *Ministry of Education College Cyberspace Security Professionals Teaching Steering Committee* [教育部高等学校网络空间安全专业教学指导委员会], https://drive.google.com/file/d/1BYm7tCEp7xT2gjBzRunfK0H4CVO4L7oE/view.

[25] Fedasiuk, "Chinese Perspectives on AI."

[26] Ryan Fedasiuk and Emily Weinstein, "Universities and the Chinese Defense Technology Workforce" (Center for Security and Emerging Technology, December 2020), https://cset.georgetown.edu/research/universities-and-the-chinese-defense-technology-workforce/.

[27] "Northwestern Polytechnical University," Australian Strategic Policy Institute – China Defence Universities Tracker, https://unitracker.aspi.org.au/universities/northwestern-polytechnical-university/.

[28] "Articles with keywords containing 'target recognition,'" [关键词中包含'目标识别'的文章," *Journal of Northwestern Polytechnical University* [西北工业大学学报], https://archive.vn/8l0jw.

[29] "A method for detecting and tracking infrared dim and small targets in complex backgrounds" [一种复杂背景下红外弱小目标检测和跟踪方法," *Northwestern Polytechnical University* [西北工业大学], https://patents.google.com/patent/CN102103748A/ko.

[30] "Method of spatial target recognition based on deep learning" [基于深度学习的空间目标识别方法], *Northwestern Polytechnical University* [西北工业大学], https://patents.google.com/patent/CN107316004A/zh.

[31] Richard Uber, "Penetrating Artificial Intelligence–enhanced Antiaccess/Area Denial: A Challenge for Tomorrow's Pacific Air Forces," *Journal of Indo-Pacific Affairs* (Winter 2020): 54–65, https://www.airuniversity.af.edu/JIPA/Display/Article/2425748/penetrating-artificial-intelligenceenhanced-antiaccessarea-denial-a-challenge-f/.

[32] "Introduction to the School of Intelligent Science" [智能科学学院简介], *National University of Defense Technology* [国防科技大学], https://archive.vn/jpSV0.

[33] Sharath Srinivasan, "The Kalman Filter: An algorithm for making sense of fused sensor insight," *Towards Data Science*, April 18, 2018, https://towardsdatascience.com/kalman-filter-an-algorithm-for-making-sense-from-the-insights-of-various-sensors-fused-together-ddf67597f35e.

[34] "Homepage>Robot Testing and Evaluation Center>Corporate Cooperation" [首页>机器人检测与评定中心>交流培训>企业合作], *Shenyang Institute of Automation, Chinese Academy of Sciences* [中国科学院沈阳自动化研究所], https://web.archive.org/web/20200525030543/http://www.sia.cas.cn/jczx/jlpx1/qyhz/; and "Shenyang Institute of Automation and China Aerospace Science and Industry Fourth Institute signed a strategic cooperation framework agreement" [沈阳自动化所与中国航天科工四院签订战略合作框架协议], *Shenyang Institute of Automation, Chinese Academy of Sciences* [中国科学院沈阳自动化研究所], https://web.archive.org/web/20201109213855/http://www.sia.cas.cn/jczx/jlpx1/qyhz/201604/t20160405_4579046.html.

[35] "Autonomous underwater robot technology research office" [自主水下机器人技术研究室], *Shenyang Institute of Automation, Chinese Academy of Sciences* [中国科学院沈阳自动化研究所], https://web.archive.org/web/20201109194235/http://www.sia.cas.cn/gkjj/zzjg/jgsz/kyxt/zzsxjqrjsysj/.

[36] "How It Works: Midcourse Discrimination (Video)," *Missile Threat*, CSIS Missile Defense Project, November 23, 2016, last modified February 4, 2020, https://missilethreat.csis.org/midcourse-discrimination/.

[37] "2020 Intelligence Rocket, Fire Eyes Artificial Intelligence Challenge starts" [2020 火箭军智箭·火眼人工智能挑战赛开赛], Tech.163, September 19, 2020, https://web.archive.org/web/20201111131842/https://tech.163.com/20/0919/22/FMTV8K2200097U80.html.

[38] "Intelligence Rocket, Fire Eyes artificial intelligence challenge begins" [火箭军智箭·火眼人工智能挑战赛开赛], https://web.archive.org/web/20201111132747/http://webcache.googleusercontent.com/search?q=cache%3Aon6TFzJ3mHUJ%3Ahttps%3A%2F%2Fwww.yuanwangfw.com%2Fhjjtzs%2F&hl=en&gl=us&strip=0&vwsrc=0.

[39] "2020 火箭军智箭·火眼人工智能挑战赛开赛," Tech.163.

[40] Marcus Clay, "The PLA's AI Competitions: Can the new design contests foster a culture of military innovation in China?" *The Diplomat*, November 5, 2020, https://thediplomat.com/2020/11/the-plas-ai-competitions/.

[41] "China defense industry presents CH-901 suicide drone at SOFEX 2018," Army Recognition, May 9, 2018, https://www.armyrecognition.com/sofex_2018_official_online_show_daily_news/china_defense_industry_presents_ch-901_suicide_drone_at_sofex_2018.html.

[42] Jeffrey Ding, "Deciphering China's AI Dream" (Centre for the Governance of AI, Oxford University, March 2018), https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.

[43] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *The New York Times*, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[44] For more suggestions on the use of open source information in strategic analysis, see Tarun Chhabra, William Hannas, Dewey Murdick, and Anna Puglisi, "Open-Source Intelligence for S&T Analysis" (Center for Security and Emerging Technology, September 2020), https://cset.georgetown.edu/wpcontent/uploads/CSET-Policy-Recommendation-OSINT-One-Pagers.pdf.