Issue Brief

Downrange: A Survey of China's Cyber Ranges

Author
Dakota Cary

CSET CENTER for SECURITY and EMERGING TECHNOLOGY

September 2022

Executive Summary

China is rapidly building cyber ranges that allow cybersecurity teams to test new tools, practice attack and defense, and evaluate the cybersecurity of a particular product or service. Nineteen of China's 34 provinces are building, or have built, such facilities. Their purposes span from academic to national defense. In short, the presence of these facilities suggests a concerted effort on the part of the government, in partnership with industry and academia, to advance technological research and upskill its cybersecurity workforce—more evidence that China has entered near-peer status in the cyber domain. This report examines five of these 19 facilities that have demonstrable ties to the military or security services. China's investment in these facilities is in line with what is known about other efforts to bolster the country's hacking and cybersecurity capabilities. As these facilities mature, network defenders who find themselves in the crosshairs of China's hacking teams may be subject to attacks that have been rehearsed, tested, and sometimes practiced on replicas of their own networks.

This report finds:

1. China's cyber ranges facilitate joint exercises between the People's Liberation Army (PLA) and civilians. One competition hosted each year in Chengdu aims to replicate the North Atlantic Treaty Organization's (NATO) Locked Shields exercise. Teams include representatives from the military, private cybersecurity firms, and critical infrastructure operators. Separately, a defense state-owned enterprise (SOE) makes a "comprehensive space scenario range" available to civilians at an annual cybersecurity competition. Each of these examples demonstrates China's implementation of military-civil fusion in the cyber domain.

2. Some cyber ranges allow hackers to practice attacking and defending critical infrastructure systems. Two ranges covered in this report provide users with training on industrial control systems within the cyber range; one of which purportedly engages in "national offensive and defensive exercises." The Office of the Director of National Intelligence's 2022 unclassified annual threat assessment found that China was "almost certainly [...] capable of launching cyber attacks that would disrupt critical infrastructure services." These ranges could allow rehearsals and testing of these types of attacks in the future.[1]

3. Peng Cheng Laboratory in southern China is using a supercomputer to research artificial intelligence's (AI) application to cybersecurity. The lab's partners include the National University of Defense Technology, China's Key Laboratory

of Science and Technology for National Defense, and Shanghai Jiao Tong University, a university with ties to military hacking teams. The lab has quickly earned the respect of longtime experts in China's cybersecurity community.

China's cybersecurity posture will be enhanced by the use of cyber ranges in several ways. First, China's critical infrastructure, massive data troves, and government agencies will be better defended. Cybersecurity teams with years of experience and hours of practice on a range will be better able to defend against a variety of threats. Second, China's attacks are likely to increase in efficacy and capability. While there are no indications to date that China has launched a physically destructive or disruptive cyberattack against another country's critical infrastructure, the ranges covered in this report suggest such a lack of action may be based in policy rather than from a lack of capabilities. Besides making attacks on industrial control systems more feasible, other types of attacks will improve as well. For example, hacking teams have more opportunities to try new tactics, techniques, and procedures.

The cyber ranges discussed in this report are important components of China's cybersecurity talent pipeline. These ranges' operators and partners should be monitored, as they include a coterie of offensive and defensive talent that governments must contend with. In considering its "defend forward" mission,[2] the U.S. government should devote additional scrutiny to the cyber ranges with industrial control systems discussed in this report, as the offensive techniques and tools used on those networks could be deployed against U.S. systems in any future conflict. Technology analysts should monitor the research published by affiliates of these institutions, as these publications may illuminate the development of technologies of interest.

Introduction

Cybersecurity depends on a talented workforce. Professionals with years of experience are sought after by information technology teams. Graduates from the best schools often get competing offers for employment. And in a tight U.S. labor market, chief information security officers can earn seven-figure salaries. The same is true for government hackers—talent and experience drive recruitment and hiring.

But not everyone comes into government cybersecurity jobs with the right skills. The needs of the government and businesses are too different for schools to always teach the right skills. Government agencies know this and often provide years of supplemental education. For operators who have their hands on the keyboard, practice is key to their success.

Cyber ranges can help these agencies provide the experiential learning that hackers need. A set of virtual machines—software that creates a computer within a computer—comprise most cyber ranges. Because virtual machines are cheap software to license, a cyber range can quickly grow in size but with little additional cost.[3] The operator can design the range to his or her needs, specifying how the machines are connected, what operating system they use, and even the range's defenses. The best cyber ranges aim to simulate real computer networks. Few achieve this high standard, and for most users "close" is good enough. The best government-funded cyber ranges can simulate millions of connections.

But cyber ranges do not only let users learn new tools, they also let them practice. Offensive teams that hope to damage or impair physical systems with precision often need to rehearse. Attacking an electrical substation or gas pipeline requires deep knowledge about the target. A cyber range built to emulate that target can help attackers make sure that they are on the right path. Past CSET research demonstrates that industrial networks can be recreated from stolen data; AI may even help attackers understand how to attack these systems.[4]

This survey aligns with other research that demonstrates China's efforts to solidify its cybersecurity talent pipeline, conduct research on applying AI to computer network attack and defense, and improve China's overall operational capabilities.[5] Until now, there have been no publicly attributed attacks on cyber-physical systems—like electrical grids, water treatment plants, or other industrial systems—by China. The U.S. Cybersecurity and Infrastructure Security Agency warned about Chinese hacking campaigns against U.S. pipelines between 2011 and 2013, but did not say they attacked the pipelines.[6] Separately, a rumored attack by Chinese hackers against an

electrical grid in India was quickly dispelled.[7] Some reporting suggests China's hackers are nevertheless still active on parts of India's electrical grid, likely allowing them to conduct reconnaissance that would facilitate future attacks.[8] New research on Chinese procurement records and research publications shows Chinese interest in such destructive attacks, following the 2015 attack on Ukraine's electrical grid.[9] Cyber ranges with relevant hardware would allow Chinese hacking teams to practice attacks on these systems.

This survey analyzes five cyber ranges in China with ties to the PLA or security services; it finds cyber ranges with military influence funded by provincial governments, large strategic investments in supercomputers for AI and cybersecurity research, and an interest in using smart-city technologies and their accompanying cyber ranges to train PLA and civilian teams to work together.

Cyber Ranges in China

Background and Recent Policies

The Chinese Academy of Sciences established China's first national cyber range in 2010.[10] CAS worked in partnership with universities in Beijing with relevant degree programs (有关高校), but the outcome of the project, its university partners, and location are unknown. This appears to be China's first publicly-acknowledged, government-led effort to establish such a facility. Some of China's best universities, military hacking teams, and private cybersecurity firms likely already had access to cyber ranges, as was the case in the United States before Defense Advanced Research Projects Agency's (DARPA) 2008 project to establish the United States' National Cyber Range.[11]

Cyber ranges within China featured prominently in 2021 in two important ways. First, the Ministry of Industry and Information Technology began soliciting public opinions on the drafted *Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023)* in July 2021. MIIT policymakers called on the government and industry to build "AI security cyber ranges," promote research on cyber ranges, use cyber ranges for training, and invest in cyber ranges that can be used to train defenders of China's futuristic smart cities.[12] MIIT frequently allocates money for research on cyber ranges, including allotments to research partnerships between universities and the PLA Strategic Support Force—the service branch responsible for computer network operations and space systems. In 2019, for example, Guangzhou University and the PLA SSF Information Engineering University received money to create a method to evaluate the efficacy of malware in a cyber range environment.[13]

China issued its second policy addressing cyber ranges a few months later in October 2021.[14] The National Industrial Information Security Development Research Center（国家工业信息安全发展研究中心），a research institute of the MIIT, published a document whose contents were only summarized publicly.[15] In the policy document, titled "Industrial Cyber Range Platform Technology Capability Evaluation Criteria"（工业网络靶场平台技术能力评价标准), policymakers lay out the standards that China's Industrial Control System cyber ranges should aspire to meet. Available summaries reference standards from companies such as Dragos, KPMG, EY, and Deloitte. Without access to the full document, it is difficult to determine the specificity, enforceability, or the applicability of these standards. What little information is publicly available stresses the close connection between industrial security and China's future as an automated manufacturing powerhouse.

Figure 1: MIIT slide on Non-Chinese, Private-Sector Cyber Ranges

Source: China's Ministry of Industry and Information Technology.[16]

China, like many countries, has a robust market for cyber range providers. Private sector companies sell services to universities so cybersecurity students can practice their skills. Some companies specialize in supporting critical infrastructure operators, helping electrical grid operators learn how to defend their networks. And still some companies focus on training other private sector employees. Similarly, it is well known that China's premier military university for hackers—the PLA Information Engineering

University—has a cyber range. This report ignores this range and general-purpose cyber ranges in favor of examining specific ranges with ties to the military and security services.

Potential Cyber Range Uses in China

There are a number of potential uses of cyber ranges. The following have been observed in China:

- Training on new tools and techniques in a controlled environment.
- Practicing attacking and defending industrial control systems.
- Evaluating product cybersecurity—smart cars, Internet of Things (IoT) devices, etc.
- Evaluating the efficacy of cybersecurity/antivirus products. Such evaluations can determine whether the products will detect new attack methodologies or malware. These evaluations can also help attackers evade a target's defenses. China's military has been observed purchasing such systems.[17]
- Recreating networks to allow defenders to practice defending those systems and attackers to practice attacking targeted systems.
- Planning attacks using attack graphs, which recreate a network and determine which pathways to a target are least likely to pique the interest of defenders. Some researchers are using an AI technique, reinforcement learning, to determine and optimize these attack paths.
- Replicating smart-city networks for defenders to practice protecting internet-connected infrastructure and surveillance systems.

Smart Cities and Cyber Ranges

One application of cyber ranges observed in China is the development of ranges that represent the city in which they are located. The Chinese Communist Party's goal to establish smart cities is driving development of these technically impressive cyber ranges.[18] Smart cities are composed of intelligently managed IoT devices, ranging from cars and public transportation to trash receptacles and closed-circuit television cameras, all reporting back to a single "cloud brain." Although no Chinese city has yet achieved full operational capability, many are making progress.[19]

As China's municipal leaders realize their goal of creating smart cities, they will also have created an incredibly complex computer network. Successfully defending this

network, where many obscure and insecure IoT devices are connected and managed, will be an incredibly complex task. Cybersecurity professionals already have a difficult time defending corporate networks, which often include only computers, servers, printers, network switches, and the like. A smart city with potentially millions of devices, or hundreds of millions in the case of a city like Shanghai, is much more difficult. While China is undoubtedly concerned about a range of potentially disruptive attacks such as ransomware groups holding an internet-connected city hostage, the ability of foreign governments or dissidents to interfere with its ubiquitous surveillance system is likely another significant concern.

Since 2016, at least six provinces have built smart-city cyber ranges: Chengdu, Tianjin, Zhejiang, Jiangsu, Guiyang, and the Guangdong Bay area (a special zone including Hong Kong and Macau).[20] China's policymakers are increasingly emphasizing the importance of creating "digital twin ranges" (数字孪生靶场).[21] These "digital twin ranges" replicate the smart city's actual network structure, rather than just creating a generic model. Defenders can then use this cyber range to train against all kinds of potential attacks.

Beijing Integrity Technologies (IntegrityTech), a state-backed leader in cyber range technology, is the leading firm helping cities develop these ranges.[22] After winning a contract to build a cyber range at China's National Cybersecurity Center in Wuhan, IntegrityTech's operations have spread across the country. IntegrityTech is the cyber range provider of choice for operators of critical infrastructure, like utility providers.[23] An article in the magazine, *China Information Security*, published by the Ministry of State Security bureau responsible for hacking operations promoted IntegrityTech's cyber ranges and featured an interview with its Chief Technical Officer. In discussing previous exercises held on its platform, the CTO noted how "various functional sectors, such as the government, the military, critical information infrastructure operators, and security enterprises, quickly perceive threats in intense confrontational environments, and through coordination and cooperation . . . jointly respond to and deal with security attacks rapidly."[24] Besides demonstrating the value of cyber ranges, the article drives home the point about China's cyber strategy. Smart city cyber ranges prepare defenders to respond to threats across large swaths of society's most critical networks. The CTO's comments, while illustrative of the cyber range's capabilities, also demonstrate interest in uniting the military, civilians, and critical infrastructure operators to defend from attacks.

Ranges of Interest

Table 1: Guiyang National Big Data Cyber Range

Guiyang National Big Data Cyber Range (贵阳国家大数据安全靶场)	
The Guiyang National Big Data Cyber Range is praised by elements of the PRC defense establishment for its offensive-defensive exercises and national security work.	
Notable Cyber Range Characteristics	
Facilitates Military-Civil Fusion	Central Government Level Cyber Range
Cyber + Physical Systems (ICS)	Talent Certification
Research (AI, Product Verification)	Conducts Offense-Defense Exercises
Hosts Cybersecurity Competitions	

Source: CSET analysis.

A large complex of four buildings sits at No.1 Data Security Road in Guiyang, China. The Guiyang provincial government started construction of the facility in 2015 and opened it for use in 2016.[25] At the time, the facility was just a provincial policy initiative—there was no central planning that required it to be built. In its first year of operation, the facility hosted an inaugural "Big Data Cybersecurity Competition," which it has held each year since.[26] After two years of successful operation, competitions, and partnerships, the Cyberspace Administration of China (CAC) designated the facility as the National Big Data Cyber Range.[27] It was a sign that central party officials were impressed by the work of the facility. The CAC's websites and publications now only use its new title, signifying its adoption by the central party into the national apparatus of government administration.[28] The State Administration for Science, Technology and Industry for National Defense (SASTIND) has lauded the cyber range on its website for Guiyang's commitment to deepening military-civil fusion.[29]

Figure 2: Image of the Guiyang National Big Data Cyber Range

Source: Qihoo 360.[30]

Although technical specifics about the National Big Data Cyber Range are hard to find, some core capabilities are identified by state-run media. One MIIT publication notes that the cyber range includes facilities that allow for network emulation of industrial hardware. These cyber and physical range facilities are particularly useful because operators can practice attacking and defending the specialized computers responsible for operating critical infrastructure and other internet-connected industrial processes.[31] *iChina* (中国信息化), an MIIT-affiliated publication, notes the facility's important contributions to "national offensive and defensive exercises with a focus on supporting the development of technology, product testing and verification, and technological innovation."[32]

Other publications highlight how the facility supports China's cybersecurity talent pipeline and strategic development. Officials credit the cyber range with increasing hands-on experience with computer network attack and defense,[33] and providing a place where cybersecurity students can receive certificates and licenses for standardized skills.[34] Increasing the availability and use of these certificates has been a significant push for the central government since 2015.[35]

Besides facilitating cybersecurity competitions and national strategic exercises, the National Big Data Cyber Range also supports cutting-edge research. One of the only publications available from the facility notes its support in offense-defense exercises for AI and using AI to plan attacks on computer networks.[36] Noticeably absent are any details of how this would occur. More speculatively, use of the cyber range could itself generate more training data to feed machine learning (ML) models and aid in their development.[37] The progress and value of such research is still unclear.

The National Big Data Cyber Range is now the anchor for a much larger cybersecurity park within Guiyang. One of China's state champions for the cybersecurity industry, Qihoo 360, opened an office in the park to provide services to the cyber range and other nearby businesses.[38] Since the expansion of the surrounding area beginning around 2018, more than 120 technology businesses have moved near the facility.[39] The collection of many like-minded businesses may yield intangible benefits such as collaboration, overlapping talent pools, and competition that breeds innovation.

Table 2: Chengdu's PeekGeek Competition & Guangcheng City Cyber Range

Chengdu's Peak Geek Competition & Guangcheng City Cyber Range	
The Guangcheng City Cyber Range has attracted significant interest from PRC policymakers seeking to boost military-civilian cooperation in cyberspace.	
Notable Cyber Range Characteristics	
Facilitates Military-Civil Fusion	Offense-Defense Exercises
Cyber + Physical (ICS)	Hosts Cybersecurity Competitions

Source: CSET analysis.

The "Guangcheng City" ("光城市") cyber range is Chengdu's smart-city cyber range. The range has hosted the "Peak Geek" Cyber Security Skills Challenge ("巅峰极客"网络安全技能挑战赛; 巅峰极客挑战赛) annually since 2019. Organized by SOEs such as China Electronics Technology Group Corporation, its local subsidiary—Chengdu National Information Security and Information Industry Base (成都国信安信息产业基地), and the provincial branch of the Cyberspace Administration of China, Peak Geek

attracted more than 30 participating teams for 32 hours of competition in 2021.[40] Teams competed for control over the cyber range's simulated "critical infrastructure industries such as electricity, transportation, water conservancy, e-government, and media."[41] Although the cyber range "simulates key city infrastructure," it is not clear if it is comprehensive enough to qualify as a "digital twin range."[42] Such progress would not be surprising, however, as Chengdu's municipal government subsidizes the development of public security technology platforms—including cyber ranges.[43]

Hype over Guangcheng City in Ministry of State Security publications suggests that the policymakers hope other cities will replicate Chengdu's success. One article by an MSS publication introduced the Peak Geek competition in the context of the NATO Cooperative Cyber Defense Center of Excellence cyber exercise Locked Shields. Another article published by the MSS referred to Guangcheng City as the "Zhurihe of cyberspace," a reference to the Zhurihe Combined Tactical Training Base（朱日和合同战术训练基地）in Inner Mongolia which is "the PLA's most technologically advanced combined tactical training base, combining computerized battlefield simulations with live-fire training exercises."[44] According to the CTO of IntegrityTech, Peak Geek participants included teams from civil society, public utilities, and the PLA.[45] The event showcased the capabilities of the Guangcheng City cyber range and demonstrated China's commitment to implementing military-civil fusion in the cyber domain.

Table 3. Peng Cheng Laboratory

Peng Cheng Laboratory (鹏城实验室)	
With government funding, massive computational capacity, and ties to the military, Peng Cheng Lab will likely be actively used by state hacking teams.	
Notable Cyber Range Characteristics	
Supercomputer	Research (AI, ICS, Smart Cars, etc.)
Facilitates Military-Civil Fusion	Hosts Competitions

Source: CSET analysis.

Led by the Guangdong Provincial Laboratory of Cyberspace Science and Technology and built with funding from the Guangdong provincial and Shenzhen municipal

governments, Peng Cheng Lab aims to provide computational power to groups conducting research on a large number of topics. Based on the lab's known partnerships (see below), these groups include academics, industry, and military researchers. Peng Cheng Lab enumerated areas of research extends to robotics, virtual reality, smart lasers, and "electromagnetic cognition."[46] Peng Cheng Lab has built a powerful supercomputer, Cloudbrain-II.[47] Based on available data, Cloudbrain-II is estimated to be half as fast as the world's fastest supercomputer, Fugaku in Japan. Its most famous contribution to China's public research so far has been the computational power it provided to train China's PanGu large language model.[48] Peng Cheng Lab aims to provide similar computation resources to work on cyber ranges and AI and cyber research.

Peng Cheng Lab also hosts cyber ranges for industrial control systems, smart cars, cybersecurity development, and AI.[49] The facility's work on industrial control systems appears aimed at securing IoT devices used to implement "smart manufacturing"—a policy goal formalized in a recent five-year plan.[50] Smart cars, part of the electric vehicle revolution and a topic of concern in *China's Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023)*, receive their own cyber range. The Internet of Vehicles Lab is being built in concert with central government regulators under the China Automotive Technology and Research Center in Tianjin.[51]

Peng Cheng Lab issued contracts to build its AI cyber range within months of opening in 2019.[52] The contracts were quickly followed with public events promoting research on AI in China.[53] The Shenzhen-based lab hosted China's National AI Competition in late 2020, which counted leaders from the Chinese Academy of Engineering, leading Chinese universities, and private firms among its participants.[54]

Projects focused on cybersecurity advanced just as quickly. Peng Cheng Lab hosted an inaugural conference on cyber range research in mid-2019 and has done so at least once since then.[55] After China's National Cybersecurity Center for Education and Innovation（国家网络安全人才与创新基地）opened in 2020, Peng Cheng Lab began partnering with the facility. In 2021, Peng Cheng Lab joined the National Cybersecurity Center, Sichuan University, and a cybersecurity park in Qingdao in jointly hosting a cybersecurity competition.[56] Qi An Xin Technology Group, a Chinese cybersecurity company active at the National Cybersecurity Center and one of China's 20 "invisible champions" of national security technology, may have facilitated Peng Cheng Lab's engagement—the company won a contract to construct Peng Cheng Lab's AI cyber range.[57] The lab's rapid integration into existing cybersecurity and AI research initiatives across the country by Qi An Xin indicate it is taken seriously by other leading

researchers in China. As of yet, such cooperation appears to be organic and not centrally dictated.

The lab's list of partners is growing rapidly. Since opening its doors in 2019, Peng Cheng Lab has formed research partnerships with other Chinese institutions. The lab partners with 21 universities, 13 research organizations, and 25 businesses or SOEs.[58] Among the organizations participating in the initiative, prominent institutions include several of China's premier universities, such as Peking University, Tsinghua University, and the Chinese Academy of Sciences. One school tied to state-sponsored hacking campaigns and co-located on a PLA base, Shanghai Jiao Tong University, also partners with Peng Cheng Lab.[59] Shanghai Jiao Tong University is also subject to a 2017 agreement with the PLA Strategic Support Force to develop "new combat forces" (新型作战力量). [60] Likewise, China's National University of Defense Technology and the Key Laboratory of Science and Technology for National Defense are listed among its partnerships with research organizations.[61] The collection of collaborators reads as a who's who of Chinese high-tech research talent. Peng Cheng Lab names entities like BGI, China Aerospace Science and Industry Corporation, China Electronics Corporation, China Electronics Technology Group, iFlyTek, and HiSense among its corporate and defense-SOE partners.[62] The US Department of Commerce has listed many of these businesses on its Entity List.[63]

Of the cyber ranges discussed in this report, Peng Cheng Lab stands out for its association with Li Jianhua (李建华), a professor at Shanghai Jiao Tong University. Li currently runs a PLA-affiliated lab which researches the applications of AI to cybersecurity research for both offensive and defensive purposes.[64] His work is also featured in Robot Hacking Games, China's version of DARPA's Cyber Grand Challenge.[65]

Li is one of China's leading experts on cyber policy. In 2018, he published an article extolling the importance of cyber ranges and offered a detailed path for successful development.[66] Li argued that the ability to rapidly recreate networks is critically important, a capability which can facilitate attack planning. He specifically suggested the use of AI to aid both defenders in detecting intrusions and in "decision making" during range operations.

Given Li's prominence, his involvement in Peng Cheng Lab suggests it is among the more sophisticated cyber ranges developed by China. His involvement, his school's history of working with China's security services, the technical capabilities of the lab, and the lab's partnership with military institutions indicate it may be used by the PLA to practice offensive operations. Li's institution, Shanghai Jiao Tong University, is listed

among the lab's strategic partners, alongside defense-SOEs and the PLA's National University of Defense Technology. Further, given Li's focus on AI and ties to the security services, Peng Cheng Lab is well-situated to enable AI-aided attack planning. One possible scenario would allow offensive operators to further hone their attacks by applying machine learning to attack simulations made possible by the range.

Table 4. Zhejiang Lab, Zhejiang Province

Zhejiang Lab, Zhejiang Province (之江实验室)	
The confluence of cybersecurity talent, funders of AI research, and military organizations points to significant work underway at the lab.	
Notable Cyber Range Characteristics	
Facilitates Military-Civil Fusion	Research (AI, Software Vulnerability Discovery)
Cyber + Physical (ICS)	

Source: CSET analysis.

Zhejiang Lab is an active participant in China's AI-research ecosystem and home to a cyber range. The lab hosts competitions for AI researchers, participates in collaborative research, and is a member of China's Artificial Intelligence Industry Alliance.[67] Zhejiang Lab operates as a partnership between the Zhejiang provincial government; Zhejiang University, a favored place for state hacking teams to recruit talent; and Alibaba.[68] A committee responsible for overseeing the lab's advancement of key technologies includes representation from the China Electronics and Technology Group Corporation, the same Guangdong provincial science and technology lab that funded Peng Cheng Lab, and China's National University of Defense Technology.[69]

Zhejiang Lab's work is varied, including both traditional cybersecurity work and more cutting-edge research at the intersection of AI and software security. Job postings on the Zhejiang provincial government's human resources website express the need for applicants to Zhejiang Lab to be able to create cyber ranges.[70] Cybersecurity company Qi An Xin, which established Peng Cheng Lab's AI cyber range, is working with Zhejiang Lab to research the attack and defense of industrial control systems.[71] These ICS-specific cyber ranges are particularly useful because they often include actual

industrial hardware, increasing the accuracy and reliability of their tests. Separately, Zhejiang Lab penned an agreement with one of two universities operating at China's National Cybersecurity Center in Wuhan to conduct research on AI for cybersecurity.[72] The two institutions will research the use of AI for software vulnerability discovery—a tool that is the focus of China's Robot Hacking Games and is a research focus for many schools tied to state hacking teams.[73]

Table 5. CASIC's Comprehensive Space Scenario

China Aerospace Science and Industry Corporation (CASIC)	
Provides civilian operators the opportunity to practice attack and defense on space assets built by one of China's Defense-SOEs and the PLA's leading supplier of space kit. The range likely supports research and exercises conducted by CASIC affiliated research institutes year-round.	
Notable Cyber Range Characteristics	
Facilitates Military-Civil Fusion	Hosts Cybersecurity Competitions

Source: CSET analysis.

China Aerospace Science and Industry Corporation (CASIC), a defense SOE, provided a comprehensive space scenario（航天综合场景）to competitors at an annual industrial security competition in late 2021.[74] Technical details about the cyber range in which the competition took place are sparse. It is unclear if the range includes a single satellite, a constellation of satellites, or other space assets, and whether these are on-orbit or simulated. CASIC provides China's military with satellites, microsatellites, missiles, anti-satellite systems, and other space or aerospace systems.[75] Teams from utility providers and the private sector practiced attacking the space assets, as well as electrical grids, water treatment plants, and transportation networks.

None of the competitors were from the PLA, but some cybersecurity firms that train PLA hackers, such as Beijing Topsec Technologies, as well as those who supported the construction of China's National Cybersecurity Center and have a history of patriotic hacking, such as NSFOCUS, did participate in the competition.[76] In China, where military strategists plan for civilian hackers to join forces with the military in the event of war, civilian access to a cyber range for attack and defense of space assets takes on new meaning.[77] Rather than just another exhibit at a public competition, the range

represents a tool of military preparedness and a potent example of China's military-civil fusion.

When the range is not being showcased at public events, it likely facilitates research done on the attack and defense of space-based assets by researchers working for CASIC. Two research institutes lead the way on such research. CASIC's 304 Research Institute hosts its "Space Flight Escort Team" (飞航护卫队), which competed in the public competition discuss above. The 304 Research Institute's organization chart shows departments like "Software Evalution Division, Cyber and Information Security Division, and Military Informatization Division."[78] Separately, CASIC's 706 Research Institute hosts its "Tianjun"（天钧）hacking team, which may be responsible for the cybersecurity and defense of China's space assets.[79] The Tianjun team wins national cybersecurity competitions and has attracted the attention of some poilcymakers.[80] The manager of Tianjun won Beijing's 2022 Capitol Labor Union Award for meritocratic service.[81] State media noted the manager's affinity for software vulnerability discovery.

CASIC is well-positioned to help the PLA. In 2017, CASIC signed an agreement with the PLA SSF to support the development of "new combat forces."[82] The agreement between CASIC, eight other institutions, and the military, aims to provide the PLA SSF with a talent pipeline for cybersecurity professionals. In the event of armed conflict, China could quickly call upon civilians in reserve, working at defense SOEs, critical infrastructure providers, or elsewhere, to work alongside the military to attack targets and defend assets, including satellites.[83]

Conclusion

The development of China's cyber ranges highlights how its military-civil fusion strategy is applied to the cyber domain, leveraging academic institutions, companies and government labs/entities to work toward a central goal. These ranges not only provide the opportunity for civilian organizations and the military to practice their skills together, but they also consistently engage in national security related research in areas such as applying machine learning frameworks to software vulnerability discovery, applying AI to cyber attack and defense, and developing attack and defense methodologies for industrial control systems.

The growth of China's cyber ranges is not accidental. Central policymakers signaled their interest in cyber ranges for education, training, AI development, and testing in China's most recent development plan for the cybersecurity sector. Consequently, municipal and provincial governments funded the development of cyber ranges with sometimes significant subsidies in alignment with Beijing's political mandate.[84] Other cyber ranges included in the appendix receive similar funding across China. The decentralized approach to investment supports innovation by provincial governments and increases opportunities for cooperation and collaboration between the military and civilians.

Cyber ranges are key to training the next generation of talent to defend, and potentially attack, critical infrastructure. China—through the development of its ranges—is providing a venue for testing and exercising the tools and techniques to attack and defend critical infrastructure while developing the technical talent to execute these operations. Although no cybersecurity firms or governments have yet attributed a disruptive or destructive attack on industrial control systems to China, this report on its cyber ranges demonstrates that the PLA has the capabilities to do active research in this area and could be postured to conduct such attacks in the future. New research on Chinese procurement records and research publications shows Chinese interest in procuring the capabilities for such destructive attacks, following the 2015 attack on Ukraine's electrical grid.[85] China's interest in having that capability is likely driving those requests.

As new cyber range capabilities develop and mature, the lessons learned from their use will provide more policy options to Beijing. Competition among states for influence and power in China's near-abroad will continue to shape Beijing's policy in the region. Besides positive incentives that induce cooperation, such as trade deals, disincentives—like potentially learning that Beijing has implanted destructive malware on your country's electrical grids—bolster China's ability to compel other countries.

Although the time and place of future cyber operations is hard to predict, the scope and scale of China's operational capabilities is growing. Investment precedes capabilities, and China has invested.

Author

Dakota Cary was a research analyst at CSET working on the CyberAI Project.

Acknowledgments

The author would like to thank John Bansemer, Perri Adams, Devin Thorne, Andreas D. Kellas, Ali Crawford, Kayla Goode, Dahlia Peterson, Ngor Luong, Emily Weinstein, Ryan Fedasiuk, Drew Lohn, Micah Musser, Shelton Fitch, and two anonymous reviewers.

Document Identifier: doi: 10.51593/2021CA013

Appendix: Other Cyber Ranges

Province	Link
Anhui	https://perma.cc/3E5G-TZBQ
Beijing	https://perma.cc/5QTH-THUS
Chongqing	https://perma.cc/Y2US-FYXP
Fujian	https://perma.cc/5LSX-AB8E
Guangdong	https://perma.cc/Z6RZ-ESAS
Henan	https://perma.cc/RD5S-XU5L
Hubei	https://perma.cc/DL3X-PBYE
Hong Kong SAR	https://perma.cc/EFP7-M83C
Jiangsu	https://perma.cc/4878-HKBE
Jiangxi	https://perma.cc/7NUZ-VSDP
Liaoning	https://perma.cc/86X8-E8YN
Shanghai	https://perma.cc/YCJ2-4QX7
Shaanxi	https://perma.cc/S298-EHGB
Sichuan	https://perma.cc/3VEL-KNJL https://perma.cc/N9BU-K594
Tianjin	https://perma.cc/986X-P72H https://perma.cc/YE75-AUUR
Tibet	https://perma.cc/8TQZ-GZRK

Endnotes

[1] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," 2002, https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Wstate-HainesA-20220308.pdf, 8.

[2] Generally considered the strategy of accessing adversary networks to collect intelligence that can be used for defensive purposes; U.S. Department of Defense, "Summary of the Department of Defense Cyber Strategy," 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[3] Some organizations do spend the extra money to recreate specific networks with real hardware—this type of cyber range is uncommon and referred to as an emulation.

[4] Dakota Cary and Daniel Cebul, "Destructive Cyber Operations and Machine Learning," Center for Security and Emerging Technology, November 2020, https://cset.georgetown.edu/publication/destructive-cyber-operations-and-machine-learning/

[5] Dakota Cary, "Robot Hacking Games," (Center for Security and Emerging Technology, September 2021), https://cset.georgetown.edu/publication/robot-hacking-games/; Dakota Cary, "China's CyberAI Talent Pipeline," (Center for Security and Emerging Technology, July 2021), https://cset.georgetown.edu/publication/chinas-cyberai-talent-pipeline/; Dakota Cary, "China's National Cybersecurity Center," (Center for Security and Emerging Technology, July 2021), https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

[6] Cybersecurity and Infrastructure Security Agency, "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," July 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-201a.

[7] David E. Sanger and Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *The New York Times*, February 28, 2021, https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html; *The Washington Post*, "Was China behind Last October's Power Outage in India? Here's What We Know," April 29, 2021, https://www.washingtonpost.com/politics/2021/04/29/was-china-behind-last-octobers-power-outage-india-heres-what-we-know/; Robert M. Lee, "Expert Opinion," Twitter, February 28, 2021, https://twitter.com/RobertMLee/status/1366187435617624064?s=20&t=pNzZLmrb_w7AoQbTT-0jlA.

[8] INSIKT Group, "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group," Recorded Future, April 6, 2022, https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets/.

[9] Zoe Haver, "China's Government Is Learning from Russia's Cyberattacks against Ukraine," Recorded Future, March 18, 2022, https://www.recordedfuture.com/chinas-government-is-learning-from-russias-cyberattacks-against-ukraine/.

[10] 科研成果年报中国科学院计算技术研究所, 2010, "科研成果年报," https://perma.cc/88W6-SUJY.

[11] DARPA Strategic Technology Office, "DARPA Broad Agency Announcement: National Cyber Range," *Wired*, May 5, 2008, https://www.wired.com/images_blogs/threatlevel/files/darpa_rfp_cyber_range.pdf.

[12] Cybersecurity Administration (网络安全管理局) of the PRC Ministry of Industry and Information Technology (MIIT, 工业和信息化部, and 工信部), "公开征求对《网络安全产业高质量发展三年行动计划（2021–2023 年）(征求意见稿)》的意见," 工业和信息化部, July 12, 2021, https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20217/0e5071815ec641be9e2154566c09fe33.wps.

[13] "第二批行业标准制修订计划," Ministry of Industry and Information Technology, August 2019. https://perma.cc/LW3T-6V9X.

[14] 国家工业信息安全发展研究中心, "《工业网络靶场平台技术能力评价标准》公开发布," 安全内参, October 20, 2021, https://perma.cc/MTA6-FF4G.

[15]工业和信息化部电子科学技术情报研究所, "国家工信安全中心 (工信部电子一所) 2022 年校招," 清华大学学生职业发展指导中心, October 3, 2021, https://perma.cc/8KWA-UK4Y.

[16] 国家工业信息安全发展研究中心, "《工业网络靶场平台技术能力评价标准》公开发布" 安全内参, October 20, 2021, https://perma.cc/MTA6-FF4G.

[17] INSIKT Group, "China's PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation," Recorded Future, May 5, 2021, https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation/.

[18] Katherine Atha, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Brian Lafferty, Joe McReynolds, James Mulvenon, Benjamin Rosen, and Emily Walz, "China's Smart Cities Development," 2020, Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf.

[19] Baptista, Eduardo, "China Uses AI Software to Improve Its Surveillance Capabilities," *Reuters*, April 8, 2022, https://www.reuters.com/world/china/china-uses-ai-software-improve-its-surveillance-capabilities-2022-04-08/.

[20] Guiyang (See Guiyang National Big Data Range), Zhejiang (https://archive.ph/saB5t), Tianjin (https://perma.cc/986X-P72H https://perma.cc/YE75-AUUR), Chengdu (https://archive.vn/NkBHM), and Guangdong (Hong Kong, Macau, Greater Bay Area); China Internet Information Center (中国互联网新闻中心, 中国网, and 网上中国), 2020; "Another Move in the 'Government + Enterprise' State of Play; Qihoo 360 and Zhuhai's Strategic Cooperation Gives Them a Foothold in the Digital Future," 新华社, September 17, 2020, https://perma.cc/34J2-DLQF.

[21] Cybersecurity Administration (网络安全管理局) of the PRC Ministry of Industry and Information Technology (MIIT, 工业和信息化部, and 工信部), "公开征求对《网络安全产业高质量发展三年行动计划 (2021–2023 年) (征求意见稿)》的意见," 工业和信息化部, July 12, 2021, https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20217/0e5071815ec641be9e2154

566c09fe33.wps; 李赟赵千, 李耀兵, 江浩, "网络靶场的建设现状、基本特点与发展思路." 中国信息化, no. June 2020: 62–64.

[22] "永信至诚完成 2 亿元融资," 中国信息安全, December 2020 issue, p. 97.

[23] 永信至诚, "案例分享 | 打造电力行业网络靶场 '样板间,'" Baidu, May 25, 2021, https://perma.cc/3PTA-GQKN.

[24] "前沿 | 网络靶场, 未来安全的基础设施," 中国信息安全, November 2021, https://www.integritytech.com.cn/html/News/News_438_1.html.

[25] 贵阳市政府办公室, "贵阳：打造国际一流的大数据安全产业集聚区 – 贵州省人民政府," 贵州省人民政府办公厅, April 6, 2021, https://perma.cc/68R8-R7U3.

[26] 贵阳市政府办公室, "2021 贵阳大数据及网络安全精英对抗演练启动," 贵州省人民政府, May 18, 2021, https://perma.cc/6W5C-RBHX.

[27] 贵州日报, "2018 贵阳大数据及网络安全攻防演练举行," Office of the Central Cyberspace Affairs Commission, November 27, 2018, https://archive.ph/lqjp5.

[28] 科技日报, "贵阳：全国首个国家大数据安全靶场升级," Office of the Central Cyberspace Affairs Commission, September 5, 2019, https://perma.cc/YU79-AKW6;
贵阳日报, "一场'赛事'带来的'蝶变'——贵阳经开区 '十三五' 期间发展成果之大数据安全产业篇," 中共中央网络安全和信息化委员会办公室, December 11, 2020, https://archive.vn/Cx6ta;
科技日报, "全国首个国家大数据安全靶场升级," 中共中央网络安全和信息化委员会办公室, August 31, 2019, https://archive.vn/bJDfu.

[29] 国家国防科技工业局, "贵州大数据战略结出军民融合硕果," 中国国防报, December, 2017, https://perma.cc/53KH-MTYT.

[30] 360 闲聊站, "【ISC 2021】360 政企安全集团赋能贵阳网络安全体系建设," Bilibili. August 27, 2022, https://www.bilibili.com/video/BV1H44y1m7aC.

[31] 李赟赵千, 李耀兵, 江浩, "网络靶场的建设现状、基本特点与发展思路," 中国信息化, June 2020: 62–64.

[32] *Ibid.*

[33] 贵阳大数据交易所, "全国首个：贵阳国家大数据安全靶场一期建成_提升," 搜狐, November 21, 2018, https://perma.cc/58RV-QSVM.

[34] 贵州日报, "贵阳抢占大数据创新制高点," 新华网, May 27, 2021, https://perma.cc/J57C-6Y66.

[35] Dakota Cary, "China's National Cybersecurity Center," (Center for Security and Emerging Technology, July 2021), https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

[36] 高升, 宋伟, 陈玉玲, 钱晓斌, 朱洪亮, 徐勤, 吴云坤, 吕虓, and 韩耀明, "国家大数据安全靶场关键技术与示范应用," 国家科技成果数据库, December 2019, https://perma.cc/2FW6-EFBZ.

[37] Thanks to an anonymous editor and friend for this comment.

[38]拉风的极客, "360 集团与「贵州四方」达成战略合作, 共建大数据产业示范城市," 极客公园, Accessed August 27, 2022. https://perma.cc/FTX2-SJKF.

[39] 贵阳筑诚人力资源服务有限公司, "2021 贵阳大数据及网络安全精英对抗演练启动 – 最新资讯 – 贵阳筑诚人力资源服务网," 贵阳筑诚人力资源服务, May 25, 2021, https://perma.cc/C6WU-ARCR.

[40] "成都国信安信息产业基地有限公司," 爱企查, 2002, https://perma.cc/G8YE-J76B?type=image; 成都日报, "网络安全明星战队齐聚成都," 成都市科学技术局主办, November 12, 2019, https://archive.vn/WQ2BE; "前沿 | 网络靶场, 未来安全的基础设施," 中国信息安全, https://www.integritytech.com.cn/html/News/News_438_1.html.

[41] 李炜, "网络安全人才培养的'3.0 时代,'" 中国信息安全, July 2020.

[42] 成都商报, "颠峰对决 12 支战队今天激战 '广诚市,'" 成都市科学技术局主办, November 13, 2019, https://archive.vn/NkBHM.

[43] 成都日报, "成都市出台 5 个方面 18 条支持政策加快网络信息安全产业高质量发展," 新闻-成都市人民政府, December 24, 2020, https://archive.vn/b5wna.

[44] 李炜, "网络安全人才培养的'3.0 时代,'" 中国信息安全, July 2020. Special thanks to Ben Murphy for his summation of Zhurihe in his translator's note.

[45] "前沿 | 网络靶场, 未来安全的基础设施," 中国信息安全, November 2021, https://www.integritytech.com.cn/html/News/News_438_1.html.

[46] Peng Cheng Laboratory, n.d, "Organizational Chart." Peng Cheng Laboratory. https://perma.cc/M7Z6-SXTS.

[47] Fueled by 1,024 Huawei Atlas900 AI clusters, Peng Cheng Lab's CEO claimed that the facility surpassed 1,000 PFlops of computational power (see https://perma.cc/X58D-Q5PG). For context, the world's fastest, unclassified supercomputer, Fugaku in Japan, is twice as fast. Fugaku completed the semi-annual Top500 competition with just half the claimed power of Peng Cheng Lab's CloudBrain-II (see https://www.top500.org/lists/top500/2021/11/). But the organization behind the Top500 competition—which ranks supercomputers on a benchmark—notes that computers from China which claim to reach this ultra-high capacity have not yet been submitted for validation (see https://www.top500.org/lists/top500/2021/11/). When compared under the same conditions (half-precision), the Fugaku supercomputer can break the same 1,000 PFlops barrier and outperform Peng Cheng Lab's Cloudbrain-II. Until Peng Cheng Lab submits CloudBrain-II to the competition, their claims cannot be validated.

But some in China argue the lab has already proven itself capable by creating a new metric for success and then leading in that new metric. Researchers from Peng Cheng Lab and academics at Tsinghua University published a paper promoting a new benchmark for high-performance computing and AI. The paper reads as though the authors were compelled, perhaps by political pressure, to create the world's fastest supercomputer for AI, but that they were unable to do so. The paper argues that current metrics of performance like Top500 do not accurately reflect the variety of hardware and software architectures that AI computers represent. The authors contend that their new benchmark, AIPerf500, a reference to the current standard, MLPerf, and the Top500 competition, more accurately ranks the performance of High-Performance Computing and AI systems. Perhaps unsurprisingly, Peng Cheng Lab's CloudBrain-II ranks first on this new benchmark–although there is no independent verification of the results (see https://perma.cc/ZQ2R-PPWR). If the researchers were driven by a political goal to achieve the world's fastest AI supercomputer, the paper makes the case for their success. The paper was published in May of 2021, so the benchmark has not yet been adopted outside China. This may change overtime, however (see https://arxiv.org/pdf/2008.07141.pdf).

[48] Jeffrey Ding, "ChinAI #141: The PanGu Origin Story," ChinAI Newsletter, May 17, 2021. https://chinai.substack.com/p/chinai-141-the-pangu-origin-story?s=w; In February 2022, the central government announced an initiative to create eight national high-power computational centers and 10 large data centers across China. Guangdong Province is listed as one of the eight computational centers, but Peng Cheng Lab is not specifically named. The Lab may count towards this new initiative; Amanda Kerrigan, April Herlevi, Brian Waidelich, and Kevin Pollpeter, "The China AI and Autonomy Report - March 2022," CNA Corporation, March 2022, https://www.cna.org/archive/CNA_Files/centers/cna/cip/china/ai-newsletters/chinaai-autonomy-report-issue-10.pdf

[49] 李赟赵千, 李耀兵, 江浩, "网络靶场的建设现状、基本特点与发展思路," 中国信息化, June 2020: 62–64; Shandong University, "A Visit to Peng Cheng Laboratory," Joint SDU-NTU Centre for Artificial Intelligence Research, August 17, 2019, https://perma.cc/4BTD-EHBF; 鹏城实验室, "鹏城实验室 2018 网络靶场态势评估分析及工控安全仿真子系统测试服务项目中标公告," 鹏城实验室-中标公示, July 9, 2019, https://perma.cc/GU66-9W96; 鹏城实验室, "鹏城实验室与中汽中心举行项目合作签约暨鹏城靶场分靶场揭牌仪式," 科研动态-鹏城实验室, November 3, 2021, https://perma.cc/TEK5-EDAJ; 鹏城实验室, "'网络靶场'赋能智能汽车行业，国内首个应用项目落地鹏城," 科研动态-鹏城实验室, August 1, 2020, https://perma.cc/CK45-9M4G.

[50] 鹏城实验室, "鹏城实验室 2018 网络靶场态势评估分析及工控安全仿真子系统测试服务项目中标公告," 鹏城实验室-中标公示. July 9, 2019, https://perma.cc/GU66-9W96; Global Times Staff Reporter, "China Unveils 5-Year Plan for Robotics, Smart Manufacturing amid Global Race," Global Times, December 28, 2021, https://perma.cc/96EP-GTF4.

[51] 鹏城实验室, "鹏城实验室与中汽中心举行项目合作签约暨鹏城靶场分靶场揭牌仪式," 科研动态-鹏城实验室, November 3, 2021, https://perma.cc/TEK5-EDAJ; 鹏城实验室, "'网络靶场'赋能智能汽车行业，国内首个应用项目落地鹏城," 科研动态-鹏城实验室, August 1, 2020, https://perma.cc/CK45-9M4G.

[52] 鹏城实验室, "鹏城实验室 AI 靶场硬件设备采购项目中标公告," 中标公示-鹏城实验室, May 5, 2020, https://perma.cc/VW8R-SXZS; 鹏城实验室, "鹏城实验室 AI 靶场硬件设备采购项目公开招标公告," 招标公告-鹏城实验室, April 26, 2020, https://perma.cc/95EU-HHVU.

[53] 企鹅号-大信科, "'鹏城杯' 网络安全竞赛启动报名," 云+社区-腾讯云, November 16, 2018, https://perma.cc/7LXZ-NSPC.

[54] 鹏城实验室, "2020 年全国人工智能大赛在鹏城实验室圆满落幕 产学研用共促人工智能发展," 学术交流-鹏城实验室, December 12, 2020, https://perma.cc/UTH6-2AST.

[55] 鹏城实验室, "鹏城实验室召开网络靶场技术研讨会," 科研动态-鹏城实验室, May 16, 2019, https://perma.cc/6AVQ-4NN7.

[56] 鹏城实验室, "2021 年全国分布式网络安全对抗演练-深圳站成功举办," 科研动态-鹏城实验室, January 15, 2021, https://perma.cc/WU9J-TB7C.

[57] 奇安信集团, "恭喜！奇安信接连中标鹏城、之江两大实验室项目 - 全国政法装备展展商动态," 法安网, August 18, 2020, https://perma.cc/GSG5-LZRH; Jamie Tarabay and Sarah Zheng, "Chinese Firm That Accused NSA of Hacking Has Global Ambitions," *Bloomberg News*, May 31, 2022, https://www.bloomberg.com/news/articles/2022-05-31/chinese-firm-that-accused-nsa-of-hacking-has-global-ambitions.

[58] 鹏城实验室, "战略合作-鹏城实验室," 鹏城实验室, 2021, https://perma.cc/Y2WZ-ZRZS.

[59] Dakota Cary, "Academics, AI, and APTs: How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research," (Center for Security and Emerging Technology: March 2021), https://cset.georgetown.edu/publication/academics-ai-and-apts/

[60] 中华人民共和国国防部, "战略支援部队与地方 9 个单位合作培养新型作战力量高端人才," 中华人民共和国国防部, July 12, 2017, https://perma.cc/PM8L-3WU4.

[61] 鹏城实验室, "战略合作-鹏城实验室," 鹏城实验室, 2021, https://perma.cc/Y2WZ-ZRZS.

[62] *Ibid.*

[63] Bureau of Industry and Security, "Control Policy: End-User and End-Use Based, Supplement No. 4 to Part 744 - ENTITY LIST," Export Administration Regulations, August 24, 2022, https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file.

[64]Dakota Cary, "Academics, AI, and APTs: How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research," (Center for Security and Emerging Technology: March 2021), https://cset.georgetown.edu/publication/academics-ai-and-apts/

[65] Dakota Cary, "Robot Hacking Games" (Center for Security and Emerging Technology, September 2021), https://cset.georgetown.edu/publication/robot-hacking-games/.

[66] Li Jianhua (李建华), "Innovation and Practice of Pluralistic and Multi-Level Cyber Security Personnel Training," Journal of Information Security Research (信息安全研究), December 2018 issue, pp. 1073-1082.

[67] Ngor Luong and Zachary Arnold, "China's Artificial Intelligence Industry Alliance," (Center for Security and Emerging Technology, May 2021), https://cset.georgetown.edu/publication/chinas-artificial-intelligence-industry-alliance/; Lab, Zhejiang, "ZhejiangLab Cup Global AI Competition 2018 - Zero-Shot Learning Picture Recognition," Alibaba Cloud Tianchi, November 30, 2018, https://perma.cc/J2V6-GXYV; Maj Richard Uber, 2020, "China's Artificial Intelligence Ecosystem," National Intelligence University, https://perma.cc/P2V4-L2TX; Zixuan Ma, Jiaao He, Jiezhong Qiu, Huanqi Cao, Yuanwei Wang, Zhenbo Sun, Liyan Zheng, Haojie Wang, Shizhi Tang, Tianyu Zheng, Junyang Lin, Guanyu Feng, Zeqiang Huang, Jie Gao, Aohan Zeng, Jianwei Zhang, Runxin Zhong, Tianhui Shi, Sha Liu, Weimin Zheng, Jie Tang, Hongxia Yang, Xin Liu, Jidong Zhai, Wenguang Chen, "BaGuaLu: Targeting Brain Scale Pretrained Models with over 37 Million Cores," *PPoPP '22, April 2–6, 2022, Seoul, Republic of Korea*, accessed August 27, 2022, https://perma.cc/Q39R-G5CQ.

[68] 之江实验室, "Homepage." 之江实验室, 2021, https://perma.cc/4WRM-4EVU.

[69] 之江实验室, "之江实验室牵头的国家重点研发计划 '多模态智慧网络核心技术与原理平台' 通过中期检查," 之江实验室, July 25, 2021, https://perma.cc/HX64-CCKS.

[70] 浙江省人力资源和社会保障厅, "之江实验室科研工作站招聘启事," 浙江省人力资源和社会保障厅, Accessed August 27, 2022, https://perma.cc/4WUZ-KREJ.

[71] 奇安信集团, "恭喜！奇安信接连中标鹏城、之江两大实验室项目 – 全国政法装备展展商动态," 法安网, August 18, 2020, https://perma.cc/GSG5-LZRH.

[72] 之江实验室, "之江实验室牵手华中科技大学 共建图计算联合研究中心," 之江实验室, December 31, 2021, https://perma.cc/NUA4-7JNM; Dakota Cary, "China's National Cybersecurity Center" (Center for Security and Emerging Technology, July 2021). https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

[73] Dakota Cary, "Academics, AI, and APTs: How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research," (Center for Security and Emerging Technology: March 2021), https://cset.georgetown.edu/publication/academics-ai-and-apts/; Dakota Cary, "Robot Hacking Games," (Center for Security and Emerging Technology, September 2021 https://cset.georgetown.edu/publication/robot-hacking-games/.

[74] "「聚焦」2021 年工业信息安全技能大赛决赛在蓉成功举办," 163.com, October 18, 2021, https://perma.cc/C82A-U26F; 改革网, "2021 年工业信息安全技能大赛复赛落幕, 全国 30 强战队名单出炉," CFGW, September 22, 2021, https://perma.cc/4QDS-QJCB.

[75] Mark Stokes, Gabriel Alvarado, Emily Weinstein, and Ian Easton, "China's Space and Counterspace Capabilities and Activities," 2020, The U.S.-China Economic and Security Review Commission, https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf.

[76] "「聚焦」2021 年工业信息安全技能大赛决赛在蓉成功举办," 163.com, October 18, 2021, https://perma.cc/C82A-U26F; 改革网, "2021 年工业信息安全技能大赛复赛落幕，全国 30 强战队名单出炉," CFGW, September 22, 2021, https://perma.cc/4QDS-QJCB.

[77] Elsa Kania, "A Force for Cyber Anarchy or Cyber Order? —PLA Perspectives on 'Cyber Rules.'" Jamestown Foundation, July 6, 2016, https://jamestown.org/program/a-force-for-cyber-anarchy-or-cyber-order-pla-perspectives-on-cyber-rules/; Joe McReynolds "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," Jamestown Foundation, April 16, 2015, https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/.

[78] China Aerospace Science and Industry Corporation, "【聚焦发展】三院 304 所 '飞航护卫队' 在 2021 年工业信息安全技能大赛决赛中喜获佳绩," 中国航天科工集团公司, July 21, 2022, https://archive.ph/lNpH0; 中国航天科工集团第三研究院第三〇四研究所, "中国航天科工集团第三研究院第三〇四研究所图册-概述图册," 百度百科, July 21, 2022, https://archive.ph/CKXum.

[79] 中国航天报, "中国航天科工二院 706 所：创新引领自主 计算创造未来," 澎湃新闻, October 5, 2020, https://web.archive.org/web/20220721191858/https:/www.thepaper.cn/newsDetail_forward_4608254.

[80] 中国航天报, "中国航天科工二院 706 所：创新引领自主 计算创造未来," 澎湃新闻, October 5, 2020, https://web.archive.org/web/20220721191858/https:/www.thepaper.cn/newsDetail_forward_4608254.

[81] 今日精选, "他是 '2022 年首都劳动奖章'的获得者， 也是天钧战队的优秀成员," 网易公司版权所有, May 1, 2022, https://archive.ph/Sg7GF; "首都劳动奖章,"百度百科, Accessed August 27, 2022, https://web.archive.org/web/20220827135042/https://baike.baidu.com/item/%E9%A6%96%E9%83%BD%E5%8A%B3%E5%8A%A8%E5%A5%96%E7%AB%A0.

[82] 中华人民共和国国防部, "战略支援部队与地方 9 个单位合作培养新型作战力量高端人才," 中华人民共和国国防部, July 12, 2017, https://perma.cc/PM8L-3WU4.

[83] Joel Wuthnow, Arthur S. Ding, Phillip C. Saunders, Andrew Scobell, Andrew N.D. Yang, "The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context," 2021, https://ndupress.ndu.edu/Portals/68/Documents/Books/beyond-borders/990-059-NDU-PLA_Beyond_Borders_sp_jm14.pdf.

[84] Beijing often issues unfunded political mandates that require provincial and municipal governments to put up cash to back initiatives.

[85] Zoe Haver, "China's Government Is Learning from Russia's Cyberattacks against Ukraine," Recorded Future, March 18, 2022, https://www.recordedfuture.com/chinas-government-is-learning-from-russias-cyberattacks-against-ukraine/.