July 2021

China's National Cybersecurity Center

A Base for Military-Civil Fusion in the Cyber Domain

CSET Issue Brief

AUTHOR
Dakota Cary

Executive Summary

China wants to be a "cyber powerhouse" (网络强国).[1] At the heart of this mission is the sprawling 40 km^2 campus of the National Cybersecurity Center. Formally called the National Cybersecurity Talent and Innovation Base (国家网络安全人才与创新基地), the NCC is being built in Wuhan. The campus, which China began constructing in 2017 and is still building, includes seven centers for research, talent cultivation, and entrepreneurship; two government-focused laboratories; and a National Cybersecurity School. The NCC enjoys support from the highest levels of the Chinese Communist Party (CCP). The Party's Cyberspace Affairs Commission established a committee to oversee the NCC's operations and policies, giving it a direct line to Beijing.

International competition forged China's commitment to growing its cyber capabilities. Despite a deficit of 1.4 million cybersecurity professionals, China is already a near-peer cyber power to the United States. Still, the current shortfall leaves China's businesses and infrastructure vulnerable to attack, while spreading thin its offensive talent. The NCC will likely bolster China's capabilities, making competition in the cyber domain fiercer still. U.S. policymakers should expect that China's increased capabilities will threaten the U.S. advantage in cyberspace.

China's path to becoming a "cyber powerhouse" is not free of obstacles. Japan's National Institute for Defense Studies identified three issues China's military must overcome to build an effective cyber force: talent, innovation, and indigenization.[2] These cyber-specific challenges likely extend to China's civilian intelligence service, the Ministry of State Security, and its internal security agency, the Ministry of Public Security.

First, China's military faces a shortage of cyber operators.[3] The country's deficit of 1.4 million cybersecurity professionals weighs on the military's ability to recruit qualified candidates.[4] In the same way a shortage of pilots would ground planes, China's shortage of cybersecurity professionals prevents the military from operating effectively. Two of the NCC's 10 components directly target talent cultivation. The NCC's "leading mission" is the National

Cybersecurity School, whose first class of 1,300 students will graduate in 2022. CCP policymakers hope to see 2,500 graduates each year. The length of time it will take to reach full capacity remains unclear. The Talent Cultivation and Testing Center, the second talent-focused component, offers courses and certifications for early- and mid-career cybersecurity professionals. The Talent Cultivation and Testing Center has the capacity to teach six thousand trainees each month, more than seventy thousand in a year at full capacity. Combined, both components of the NCC could train more than five hundred thousand professionals in a single decade. Even half that number would still help overcome the talent gap.

Second, China's current system for innovation in the cyber domain will not meet its strategic goals.[5] Chinese military strategists view cyber operations as a possible "Assassin's Mace" (杀手锏)—a tool for asymmetric advantage over a superior force in military confrontation.[6] Advanced militaries rely on interconnected networks to operate as a unified system, or "system of systems." Chinese strategists argue that disrupting communications within these systems is key to deterring military engagement.[7] No single tool will establish an asymmetric advantage. Instead, China must reliably produce attack types for each system targeted. There are no silver bullets, but a workforce capable of significant innovation is critical to implementing the strategy.

Three of the 10 components directly support innovation at the NCC. Students and startups can solicit business guidance and investment funds at the NCC's Incubator. Besides supporting private-sector innovation, two other components of the NCC support government-focused research. The NCC hosts two non-private laboratories, the Combined Cybersecurity Research Institute and the Offense-Defense Lab. Both institutions likely conduct cybersecurity research for government use (see component analysis below). Other components indirectly support innovation. The NCC's Exhibition Center, for example, hosts events that attract inventive talent from across the country. China's Military-Civil Fusion strategy ensures that the People's Liberation Army (PLA) can harvest new tools that come from the NCC,

regardless of who develops it, which may help China develop asymmetric advantage.[8]

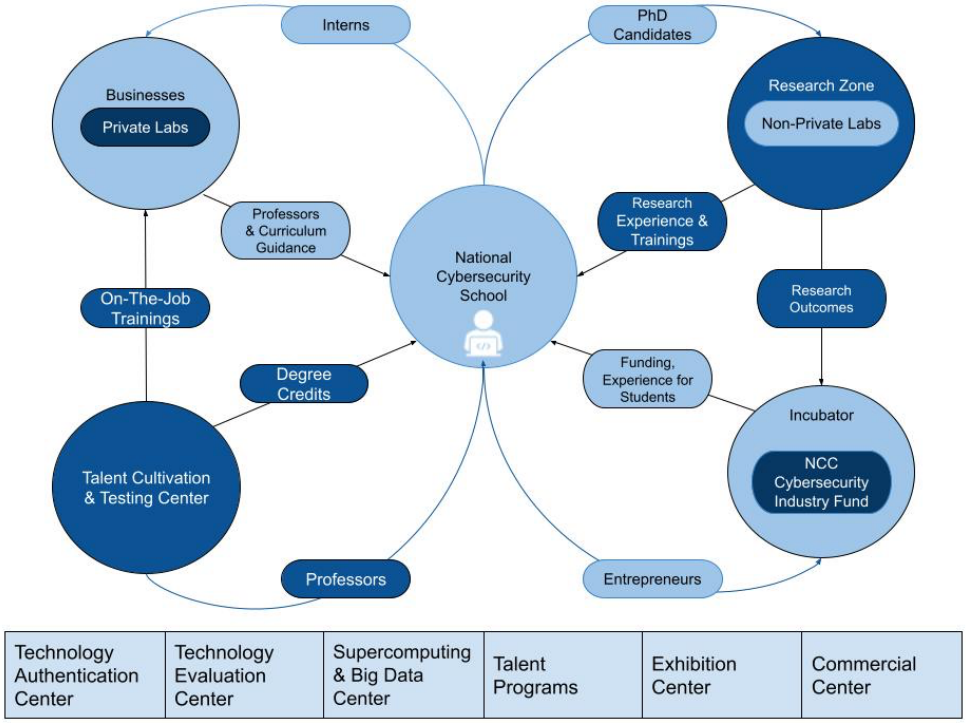
Third, China aims to reduce its reliance on foreign cyber technology.[9] The Snowden revelations reinforced PLA concerns that foreign technology facilitates espionage. Leaked documents revealed occasional close cooperation between the U.S. government and technology companies. The CCP wants indigenous replacements for foreign software to protect its military and critical infrastructure from foreign interference. Indigenization will also allow China to become more aggressive. If the PLA uses the same foreign-made software they are attacking, then their attack against that software leaves Chinese networks vulnerable to counterattack through replication. By attacking the software, they prove its vulnerability. If a capability is reciprocal, it is not asymmetric. Replacing foreign software would go a long way to remediate the Party's concerns about foreign espionage and remove constraints on policy choices.

A local government report shows that policymakers intend to harvest indigenous innovation from the NCC. Citing important Party organs, the report states that "leaders have repeatedly made it clear that the National Cybersecurity Base must closely monitor independent innovation (自主创新) of core cybersecurity technologies, promote Chinese-made independently controllable (自主可控) replacement plans, and build a secure and controllable information technology system…"[10] Local officials serve as a pipeline between the NCC's ecosystem and the needs of the Party by targeting nascent technologies. If the NCC is successful at spurring innovation, the pipeline may ease adoption of indigenous products and facilitate the replacement of foreign technology.

The CCP has high expectations for the NCC, and policymakers and businesses are making the necessary investments to be successful. But the prospects for the NCC's impact on China's cyber capabilities are uneven. On talent cultivation, the NCC is sure-footed. The National Cybersecurity School and Talent Cultivation and Testing Center already educates students and certifies trainees. Successive classes of NCC graduates and trainees will slowly fill the ranks of China's state-backed hackers and private-

sector defenders. The NCC's impact on innovation will only become clear over the next decade. Key stakeholders are making investments in research and development (R&D) facilities, talent programs, and the NCC's Incubator. But innovation is fickle. Following best practices, like concentrating talent and capital in a tightly defined area, creates a supportive environment but cannot guarantee the development of new technology. Over the long run, the NCC's talent cultivation efforts will likely impact the dynamics of nation-state cyber competition. The tools these operators use may well be designed by NCC graduates, too. China's competitors should be prepared to respond to these developments.

Figure 1: Concept Map for Components of the NCC



Source: CSET.

Table of Contents

Introduction

China has a cybersecurity problem. Each year the demand for cybersecurity professionals dwarfs the supply. Only 5 percent of open positions are filled annually.[11] A 2017 article projected that by 2020 the deficit of cybersecurity graduates would grow by fifteen thousand positions each year.[12] In 2020, Chen Doudou (陈斗斗), the leader of China's boldest new cybersecurity initiative—the National Cybersecurity Talent and Innovation Base (国家网络安全人才与创新基地, NCC), claimed that the country lacked 1.4 million cybersecurity professionals.[13] In an attempt to fill the gap, some private-sector companies—such as DAS-Security (安恒信息) and others—founded their own cybersecurity schools.[14] Other companies partnered with the China Information Technology Security Evaluation Center (CNITSEC)—the Ministry of State Security's 13th bureau—to train employees in cybersecurity.[15] These stop-gap measures helped some companies meet their own needs. But companies outside of the information technology sector lack the talent to train their own professionals. The result is a weak, fragmented cybersecurity environment. Widespread vulnerability slows the country's ascent to the status of "cyber powerhouse" (网络强国).[16]

But China's cybersecurity problems extend beyond civil society, impacting the People's Liberation Army (PLA) and civilian hacking teams. The National Institute for Defense Studies, a think tank affiliated with Japan's Ministry of Defense, identified three obstacles that the PLA Strategic Support Force (PLA SSF) must overcome to build its desired cyber corps.[17] First, China's lack of cybersecurity professionals stymies the military's use of cyber capabilities. Without qualified operators to defend networks and conduct attacks, the PLA SSF cannot fully meet its mission requirements. Second, Chinese military strategists think the cyber domain can provide the PLA with an asymmetric advantage over stronger militaries, often called an "Assassin's Mace." But without adequate talent and resources, the necessary innovation is lacking. Though no single technology can provide such an advantage, a well-resourced corps of cyber operators should be able to deploy novel attacks that can achieve the deterrent effect strategists

desire. PLA commanders conceptualize such cyber effects on par with nuclear deterrence or anti-satellite capabilities.[18] Third, China must promote the replacement of foreign technology with domestically produced equivalents. This "indigenization" has two purposes. The CCP worries that foreign technology facilitates espionage on sensitive networks.[19] Replacing foreign software with indigenous equivalents eliminates the possibility that another government has co-opted the technology. Besides improving China's defense, indigenization could unleash China's offensive capabilities. When operators attack a particular software, they often do so by exploiting a vulnerability. If China's networks include the same software they are attacking, then they are vulnerable to counterattack. This symmetric playing field impacts the software that nations choose to exploit and prevents China from creating the asymmetric advantage its strategists seek. If China can develop and deploy indigenous replacements, the tempo of offensive campaigns may increase. For now, these three hurdles constrain China's cyber capabilities.

The National Cybersecurity Talent and Innovation Base is a major component of China's response to its cybersecurity problem. The NCC will improve China's cyber capabilities by focusing on two goals: cultivating talent and spurring innovation. The "base" is more of a sprawling industrial park than a gated military installation. Although there are four smaller cybersecurity parks and industrial bases in Chengdu, Shanghai, Shanxi, and Tianjin, none are on par with the NCC, which is being built in Wuhan.[20] The other four combined are less than a quarter of the NCC's size, and many orders of magnitude smaller by investment. The breadth of the initiative is indicative of its importance. China's policymakers argue that the NCC is the only "base" to merge government, industry, academia, research, and application of technology (政产学研用).[21]

Expectations are high. The Central Party School, which trains current and future top Party leaders, said that the NCC was critical to the "conscientious promotion of the national cybersecurity defense capability."[22] The Central Party School's endorsement of the NCC reflects the high-level attention the project receives.

The NCC's impact will soon be felt—the National Cybersecurity School opened to students in August 2020. Its first class of graduates will cross the stage in June 2022. From there, they will go on to join the ranks of China's cyber operators, whether in the public or private sphere. No matter where they go, the Party will have continued access to NCC's graduates and innovations.

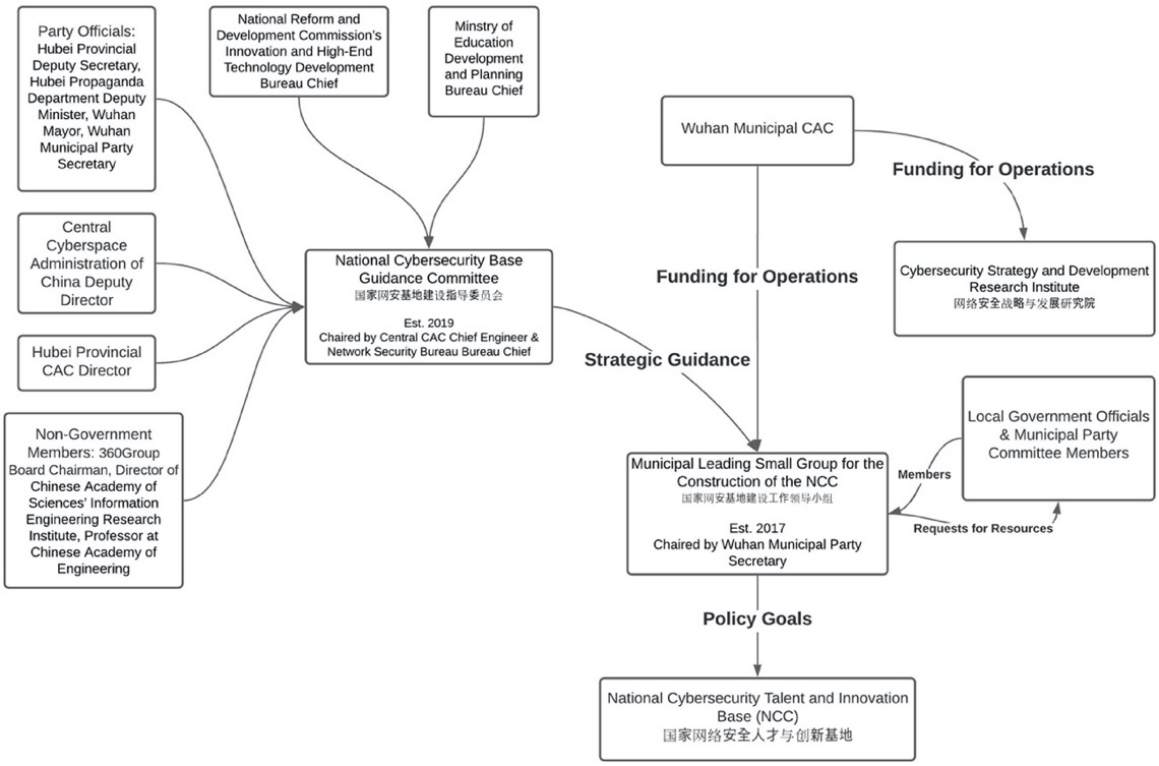
Governance Structure

National Cybersecurity Base Guidance Committee

The Chinese Communist Party's two highest policy bodies are "the National Congress and the Central Committee which it elects."[23] The Central Committee's 204 members are the Party's elite politicians. They concurrently serve as military generals, provincial secretaries and the like.[24] Members of the Central Committee sit on committees and commissions, overseeing issues ranging from finance to foreign affairs.[25] The CCP Central Committee Cyberspace Affairs Commission (中共中央网络安全和信息化委员会办公室) is one of 16 such committees.[26] The Cyberspace Affairs Commission handles many cyber related policies. Its remit includes everything from approving cybersecurity competitions to "maintaining the security and defense of China's critical information infrastructure."[27]

The Cyberspace Affairs Commission established the National Cybersecurity Base Guidance Committee (国家网安基地建设指导委员会) to oversee the NCC in 2019. The Guidance Committee allows central government organizations to provide input on policies governing the NCC. The committee's broad membership reflects the multidisciplinary approach of the NCC. Cybersecurity professionals, government officials, industry leaders, university professors, and research scientists sit on the Guidance Committee.[28]

Figure 2: NCC Oversight Organizations



Source: CSET.[29]

The Municipal Leading Small Group

Wuhan's municipal government established the Municipal Leading Small Group (LSG) for the Construction of the NCC in 2017. Local government officials and an initial fund of RMB 15 billion helped get the NCC integrated into municipal services.[30] The LSG's responsibilities include land management, special tax zones, and municipal waste disposal.[31] Once the NCC began operations in 2019, the CCP Central Committee Cyberspace Affairs Commission established the National Cybersecurity Base Guidance Committee (above).

The Cybersecurity Strategy and Development Research Institute

The Cybersecurity Strategy and Development Research Institute, a third, nebulous body, also contributes to policy at the NCC. The Wuhan Cyberspace Administration of China funds the institute, at

least in part.[32] The institute lacks a web page, publications, or references besides the Wuhan CAC budget line of RMB 400,000 in 2019, but purportedly acts as a think tank to guide the development of the NCC.[33] The work it undertakes and its avenues for influence are unclear.

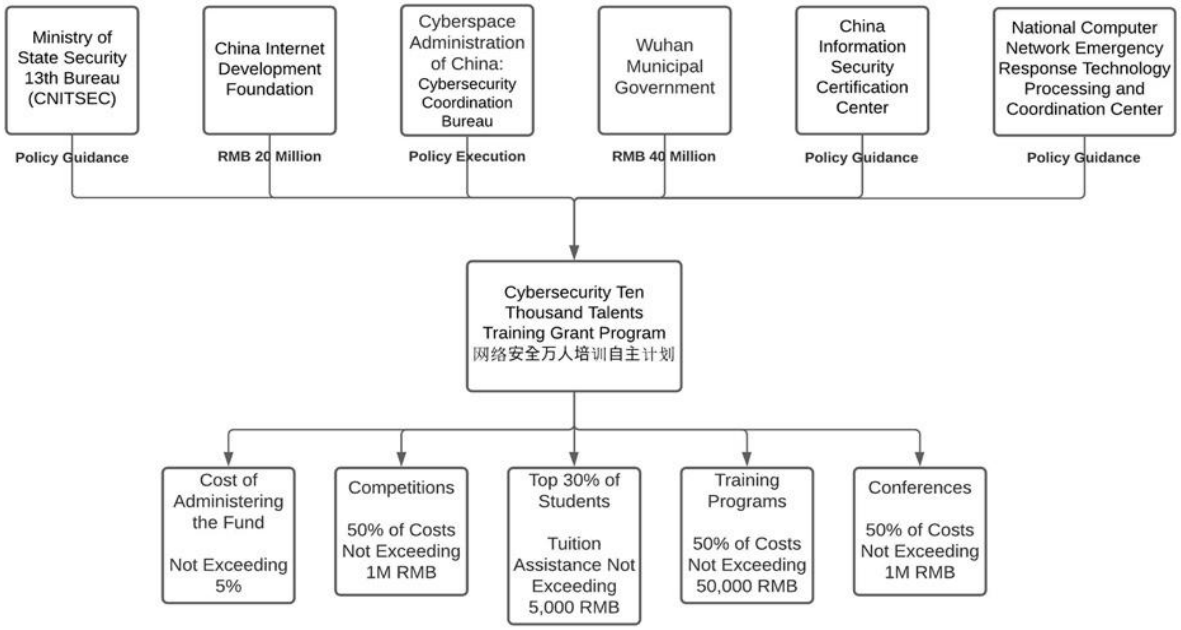
Attracting Talent to the NCC

Attracting China's top cybersecurity professionals to work at the NCC is crucial to its success. CCP policymakers' vision for luring the country's top cyber talent with housing and employment opportunities is something akin to the cybersecurity version of an old U.S. "company town," but with greater investment in compensation packages.

Wuhan Municipal Cyberspace Administration and the National Cybersecurity School will use research subsidies and talent awards to attract talent to the NCC. The Wuhan Party Committee and municipal government will offer a one-time sum of RMB 2 million (approximately $309,000) to attract highly-qualified cybersecurity professionals to teach at the school.[34] This represents between 10- and 20-years' worth of the median annual salary in the cybersecurity field—a staggering sum that falls on the more generous side of China's talent programs.[35] A separate program targets teams of researchers whose work is deemed critical to cybersecurity. The Wuhan municipal government will provide up to RMB 100 million to support their move to the NCC.[36] These two policies act in tandem to attract the best practitioners without disrupting ongoing innovation. Professionals who accept teaching positions at the school can expect to receive twice the normal university salary, twice the normal research funding, and subsidized housing, childcare, and spousal employment benefits.[37] Taken together, the policies designed to attract cybersecurity professionals to the NCC make a compelling offer—more income, fewer expenses, and a sizeable signing bonus. The benefits on offer illustrate the importance policymakers attach to the NCC and the National Cybersecurity School in particular.

The NCC also uses another program, the Cybersecurity Ten Thousand Talents Training Grant Program (CT4GP), to attract talent to the NCC for short-term visits. Under the guidance of five central government agencies, CT4GP subsidizes the costs of training programs, student tuition, conferences, and competitions held at the NCC.

Figure 3: The Cybersecurity Ten Thousand Talents Training Grant Program



Source: CSET.[38]

The CCP envisions these talent programs attracting a wide range of cybersecurity professionals to the NCC. The Party has high aspirations. Policymakers want "strategic scientists" to teach students and make breakthroughs in "core technologies" at the same time.[39] The talent programs also seek to attract experts in "various offensive and defensive techniques" to teach hands-on classes.[40] The drive to hire both researchers and practitioners reflects the two goals of the NCC—talent and innovation. On the one hand, hiring scientists focused on applied cybersecurity research will guide the doctoral talent pipeline, while allowing those same "strategic scientists" to work on projects of their own. On the other hand, having seasoned practitioners teach offensive and defensive techniques hones students' practical abilities. A deep talent pool with competency in such skills is crucial to international competition.

Students, too, receive benefits from talent policies as the NCC seeks to attract them. Besides the CT4GP initiative, the Wuhan municipal government separately promises to double the normal

sums for scholarships and provide money for students to turn school research projects into startup companies.[41] Students-turned-entrepreneurs will receive subsidized office space and preferential tax treatment for businesses set up within the NCC.[42] Policymakers hope to entice students to stay at the NCC after graduation, turning startups into mature cybersecurity businesses without needing to leave the NCC's ecosystem.

NCC Organization Structure and Analysis

Figure 4: Phase I of the NCC in October 2020, 4 km^2

Source: Apollo Mapping.

Accounts of the NCC's organizational structure vary, but many of its components are consistently described across different sources. The original 2017 proposal from the Wuhan government shows the National Cybersecurity School, eight centers, a research lab, and an innovation base.[43] An article written by three PLA officers in 2020 states that the NCC includes "two institutions, one laboratory, ten centers" (两院一室十中心).[44] A company working with the NCC reports yet another structure—two institutions, one laboratory, and seven centers.[45] The latter is likely the most accurate version of the NCC's current structure. The "two institutions" are the National Cybersecurity School and the Combined Cybersecurity Research Institute, the "laboratory" is the

Offense-Defense Laboratory, and the seven remaining organizations are the “centers.”[46] The analysis that follows reflects this assessment and may change as the NCC is further constructed or more definitive information comes to light.[47]

Wuhan municipal government dedicated 40 km^2 to the NCC, split into two parts, known as "phases."[48] Phase I occupies around 4 km^2 and groups institutions into “zones” based on their purpose. Phase II consists of the Cybersecurity Industrial Park, occupying the remaining 36 km^2.[49] The five zones of Phase I offer a framework to understand the structure of the NCC.[50]

Table 1: The Five Zones of the NCC

Zone	Components
Education Zone	National Cybersecurity School
On-the-Job Training Zone	Talent Cultivation and Testing Center
Research Zone	Offense-Defense Laboratory, Combined Cybersecurity Research Institute
Shared Services Zone	Technology Certification Center, Technology Evaluation Center, Conference Center, Exhibition Center, Commercial Center
Industrial Development Zone	Supercomputing and Big Data Center, Incubator

Education Zone (学历教育区)

National Cybersecurity School (国家网络安全学院)

Figure 5: National Cybersecurity School

Source: Apollo Mapping.

The Education Zone will host the planned National Cybersecurity School—currently its campus is shared by Wuhan University and Huazhong University of Science and Technology (HUST).[51] The School is at the center of the CCP's effort to train a new generation of cybersecurity professionals, and is described as the NCC's "leading mission."[52] In 2017, the Wuhan Municipal Cybersecurity Administration said that the school had attracted around RMB 5 billion in investment and would occupy around a quarter of Phase I, at 1 km^2.[53] However, a 2019 article by HUST suggests that the initial figures that were announced may have been overly

optimistic, reporting a later total investment of RMB 2.68 billion into the school.[54]

Prior to creating the National Cybersecurity School, Wuhan University and HUST worked with the PLA to varying degrees. The 6th bureau of the PLA SSF Networks Systems Department, which likely has a training mission, is headquartered in Wuhan, halfway between the two schools' original campuses.[55] Although both universities are overseen by the State Administration of Science, Technology and Industry for National Defense, a civilian agency that funds commercial and academic research in support of PLA requirements, Wuhan University maintains closer ties to PLA hacking teams than HUST.[56] Past reports find that Wuhan University operates a Cyber Offense-Defense Center (网络攻防中心) in collaboration with the PLA.[57] Separately, in 2015, Taiwanese intelligence officials alleged that Wuhan University hosted a PLA hacking team which conducted operations against Taiwan.[58] Like HUST, Wuhan University also hosts defense laboratories that research technology for the PLA.[59] Both institutions hold Secret clearances, allowing university labs and professors to work on sensitive military technology development. China Aerospace Science and Industry Corporation (CASIC), a manufacturer of PLA rockets, sponsored Huazhong University undergraduates for the National Defense Science and Technology Scholarship in 2020, focusing on information and communications technology degree holders.[60] Past collaboration with the PLA, including an allegation by U.S. officials that a Wuhan University research center conducted cyberattacks for the PLA, emphasize the importance of both the National Cybersecurity School and the NCC to China's military.[61]

The Central CAC and Wuhan Municipal CAC identified a number of responsibilities for the National Cybersecurity School to ensure the school serves the national interest.[62] The institution is expected to: 1) make decisions in accordance with China's National Cybersecurity Strategy, 2) hire professors from "various research institutions, universities and corporate R&D institutions nationwide", and 3) "recruit graduate students with master's degrees or higher from among domestic universities[…], overseas

undergraduate students, and top contestants in cybersecurity attack and defense competitions."[63] Rather than teaching basic content, the school aims to ensure that experienced professionals and innovative researchers are teaching promising students. Currently, the school falls short of expectations. Only students from Wuhan University and Huazhong University may apply to attend the National Cybersecurity School for their junior and senior years.[64] It is unclear whether enrollment at the National Cybersecurity School will expand to third- and fourth-year undergraduate students from other universities. This change is a prerequisite for a truly "national" cybersecurity school.

Policymakers redesigned the traditional model of university governance for the National Cybersecurity School. The school's board of trustees includes representation from "relevant state ministries, the nation's top cybersecurity experts, the local Party committee and government, sponsoring units from society, and the host universities."[65] Policymakers want the revamped structure to keep the NCC's curriculum aligned with national strategic goals and up to the standards of China's leading "national champion" cybersecurity and information technology companies.

The NCC instituted a nontraditional system for evaluating the performance of students and teachers. The school's system favors quantifiable metrics for technical competencies over academic publications and grades. The school evaluates professors on their ability to teach students practical cybersecurity skills, encourage entrepreneurship and innovation, and put solutions-focused research at the core of classroom instruction.[66] Similar flexibility is also afforded to students. The school counts "training programs, scientific competitions, published papers, inventions and patents obtained, and professional certificates" towards degree credits.[67] The goal of this system is to encourage hands-on learning and foster entrepreneurialism among the student body.

The National Cybersecurity School pays special attention to its doctoral program. To help doctoral candidates conduct and monetize applied research, the school provides "dual mentors", one "strategic scientific" mentor and one "innovative entrepreneurship" mentor.[68] The school recruits mentors from NCC stakeholders,

including businesses. Together with the other NCC policies and institutions, such as the Incubator, the dual mentor program is intended to drive doctoral candidates and their research into the cybersecurity market.

China's policymakers originally intended for Wuhan University's Cybersecurity College and Huazhong University's School of Cyber Science and Engineering to combine and form the National Cybersecurity School. So far, this approach has proven unsuccessful. In an apparent attempt to smooth over differences, the Central CAC published a notice in 2020 stating the two schools would implement a "partially independent, partially shared" model.[69] The compromise is at odds with all prior documentation on the school—which indicate the two universities' NCC operations would merge. The inability to resolve political infighting is likely the reason the National Cybersecurity Base Guidance Committee's first meeting revolved around facilitating the universities' integration.[70]

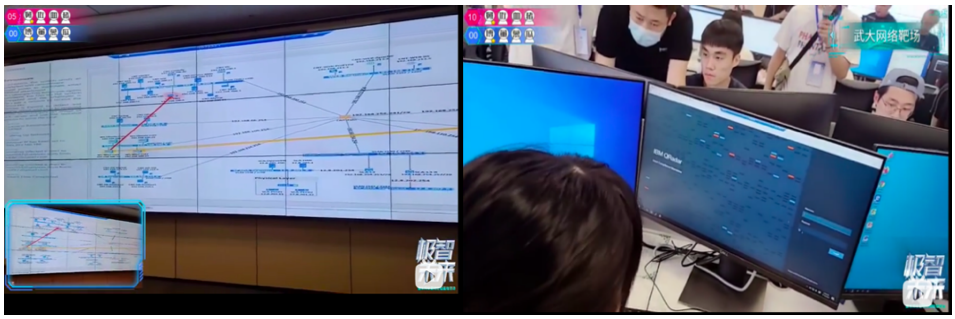
Figure 6: University Signs in Separate Buildings; Wuhan University (Left), Huazhong University of Science and Technology (Right)[71]

Source: 天天风行-录制组, Bilibili.

At present, each college is under the leadership of its respective university. The two schools use separate education buildings and dormitories, but share other facilities, including cafeterias, libraries, sports facilities, and parking garages.[72] The two schools claim "different" educational objectives. Wuhan University focuses on developing "comprehensive cybersecurity talent", while HUST concentrates on cultivating "the world's most effective defensive cybersecurity professionals."[73] Joint university-enterprise facilities constructed at the NCC reflect these separate institutional foci. Huazhong University and Beijing Topsec, a company that trains

PLA hackers, partnered to build the university's "cyber range" (网络靶场)—a platform used to simulate network confrontation.[74] Separately, Wuhan University partnered with Qi'anxin Technologies and Tencent to build its own cyber range.[75] These two cyber ranges meet policymakers' requirement that the NCC "introduce real, high-level actual combat confrontations."[76] Though not a fully integrated National Cybersecurity School, the different descriptions of each school's educational objective are likely just branding. Educating "defensive cybersecurity professionals" and "comprehensive cybersecurity talent" requires the same curriculum. Moreover, the Guidance Committee will likely ensure the split institution meets its obligations to the central government. Based on all prior documentation and its high-level oversight by the CCP, it is likely that the two universities will resolve outstanding issues and merge.

Figure 7: Wuhan University, Tencent, and Qi'anxin Technologies' Cyber Range



Source: 天天风行-录制组, Bilibili.[77]

Figure 8: Huazhong University and Beijing TopSec's Cyber Range

Source: 天天风行-录制组, Bilibili.[78]

The number of staff and students at the NCC was lower than planned in 2020 due to the COVID-19 pandemic, but will likely grow. In its first graduating class, the school enrolled 1,300 students, slightly less than half of the original NCC proposal's stated capacity.[79] As of September 2020, the school employed 140 teaching and administrative staff, around 50 of whom were professors.[80] As the program expands, the number of faculty is expected to double to around 100.[81] It is unclear how many of these professors were already employed by the two universities, and how many were poached through talent recruitment programs. The NCC director recently reiterated the importance of involving the "specialized talents" to teach classes; whether the school has yet put this into practice is unknown.[82]

On-The-Job Training Zone (在职培训区)

Talent Cultivation and Testing Center (人才培训与考试中心)

Figure 9: Talent Cultivation and Testing Center, original proposal (left), actual construction (right).

Source: City of Wuhan Land Use and Urban Space Planning Research Center; Apollo Mapping.[83]

The On-The-Job Training Zone hosts the Talent Cultivation and Testing Center (人才培训与考试中心).[84] The center offers technical courses, network security certifications, professional development classes, training on specific products, and some general cybersecurity awareness programs for nonexperts.[85] Students from the National Cybersecurity School can receive degree credits for

certifications. But the center focuses on providing early- and mid-career cybersecurity professionals seeking career advancing certifications.[86] The formal certification of skill sets is part of the CCP's strategy to professionalize the cybersecurity sector.[87] On-site training and testing allows the NCC to support that goal.[88] To expand its reach beyond Wuhan, the center is also developing an online education platform.[89] CCP policymakers hope the Talent Cultivation and Testing Center's business-led approach will help trainings keep pace with industry standards. The center started accepting applications for its first batch of trainees in May 2020.[90]

As with other components, the NCC made companies responsible for running the center's programming. Policymakers hope to ensure training programs respond to market demand and are updated at the speed of business, not government.[91] The talent center is administered by a joint venture between the district government and TUS Holdings, a company also involved with the tech Incubator.[92] The main companies operating at the center are IntegrityTech (北京永信至诚科技)[93] and Qi'anxin Technology (奇安信集团).[94] In 2017, IntegrityTech claimed that it would train up to three thousand people per year in-person, and three hundred thousand people per year online—though this online number likely reflects the company's total corporate training capacity, not just that built at the NCC.[95] The training capacity and investment of Qi'anxin Technology is unclear but likely constitutes a significant proportion of the center's capacity. The company made the NCC its headquarters in central China.[96] Qi'anxin Technology's status as the cybersecurity provider of choice for 90 percent of the central government, state-owned enterprises, and major banks, explains its involvement. Trainees can easily move from the NCC into Qi'anxin Technology and on to government-focused cybersecurity careers.[97] Though none of the supporting documentation specifically mentions China's Military-Civil Fusion strategy, the relationship between Qi'anxin Technology, the NCC, and the government nonetheless exemplifies this strategy.[98]

The Talent Cultivation and Testing Center will improve China's cybersecurity talent pool. As of late 2019, the center's estimated training capacity was six thousand people per month.[99] However,

highly-skilled cybersecurity professionals will still take years of investment and training to cultivate—a task better suited to the National Cybersecurity School. The center also conducts specialized research as directed by the central, provincial, and municipal cyberspace administrations.[100] What this research includes, and how it interacts with other components of the NCC, is unclear.

Businesses involved in the NCC may offer preferential hiring to certificate holders from the talent center. Almost 30 companies gave trainees from the center's inaugural class with a particular certification preferential treatment and early access to job postings.[101] This preferential hiring system, if extended to future classes, would solidify the NCC's importance within China's cybersecurity ecosystem. Such a policy would support the feedback loop between the NCC, businesses, and government sought by China's policymakers.

Research Zone (*研究院区*)

Figure 10: Research Zone

Source: Apollo Mapping.

The Research Zone hosts the NCC's two quasi-public research laboratories, the Offense-Defense Laboratory (攻防实验室) and the Combined Cybersecurity Research Institute (网络安全联合研究院).[102] The zone may also lease office space to companies that move onto the NCC campus but do not build their own facilities.[103] Companies that have committed to building their own R&D facilities (see appendix) will construct them in Phase II.[104]

Both labs' goals, leadership, and responsibilities are unclear. Neither are private-sector laboratories—though both have corporate partners. There is also no documentation explicitly stating that they are government-run. The labs are likely government-directed but not government-operated, embodying China's Military-Civil Fusion strategy.

The Offense-Defense Laboratory (攻防实验室)

The Offense-Defense Lab likely tests cyber tools for government use. Provincial propaganda departments describe the Offense-Defense Lab as a network simulation center with three purposes: to host personnel training, to offer "practical combat drills" (实战攻防演练), and to support research and innovation.[105] But it is unclear who will receive training, what constitutes "practical combat drills," and what research or innovation will be supported. The Talent Cultivation and Testing Center already has ample resources to run training programs, and the companies known to work with that center (Integrity Tech and Qi'anxin Technologies) are not mentioned in relation to the Offense-Defense Lab. Additionally, the National Cybersecurity School, in its current bifurcated form, already has two cyber ranges for students to train on. The question of who needs to use the Offense-Defense Lab for activities that could be hosted elsewhere, remains unanswered.

And what of innovation and research? Again, the answer is fuzzy. Other components of the NCC have named corporate partners, with each party's responsibilities well defined. The Offense-Defense Lab has only one known partner. In September 2020, the Hubei Government announced that Wuhan Anyu Information Security Technology (武汉安域信息安全技术) had invested RMB 20 million in a network simulation training platform (仿真实训平台).[106] Wuhan Anyu's corporate website makes no mention of offering a network simulation platform, but does highlight its information security services—network monitoring, penetration testing, and risk analysis.[107] These services help organizations assess their defenses and protect networks from attack. The cybersecurity firm has provided these services to many government entities. The Hubei provincial office of the Ministry of Public Security, China's government agency for internal security, is a longtime customer.[108] These relationships make selecting Wuhan Anyu as a partner for the Offense-Defense Lab an easy choice. But the firm's focus on network security, not training platforms, raises questions about the services provided. Even if Wuhan Anyu runs and operates the lab's simulated network, there is still no clear sign of who is procuring the offensive and defensive tools that are tested there. The

similarly-named Cyber Offense-Defense Center (网络攻防中心) operated by Wuhan University in collaboration with the PLA may offer one explanation, but no sources yet confirm any relationship between the PLA and the Offense-Defense Lab.[109]

Figure 11: Offense-Defense Lab in the Original Proposal in Pink

Source: City of Wuhan Land Use and Urban Space Planning Research Center.[110]

The Combined Cybersecurity Research Institute (网络安全联合研究院)

The Combined Cybersecurity Research Institute (网络安全联合研究院) likely serves as an avenue for government-directed research on new cybersecurity technologies.[111] While the Offense-Defense Lab focuses on the application and testing of new cyber tools, the research institute appears to focus on developing those tools. Originally designed as a joint effort between Wuhan University and Qihoo360,[112] the institute later expanded to include 12 companies.[113] Two of those companies, Beijing Topsec and Qihoo360, train PLA hackers.[114] The research direction, methods of cooperation, and distribution of resources within the research

institute are unclear from available materials. Given that other companies are establishing their own R&D laboratories in the NCC and have a market incentive to develop defensive cybersecurity tools, it is possible that the work of the research institute will also be government-focused and used for offensive purposes.

R&D Facilities

Several companies are establishing R&D facilities within Phase II of the NCC. A few businesses stand out for their known ties to state-sponsored hacking teams and their focus on achieving China's strategic goals.[115] Beijing Topsec invested in a new research lab and moved four hundred research staff to the NCC.[116] Besides training PLA hackers, the company likely provides technical capabilities to the Party. Another leading cybersecurity firm, Qihoo360, will employ two hundred research staff at its secondary headquarters on the NCC.[117] Qihoo360—which has a seat on the guidance committee overseeing the NCC[118] and leads China's Cybersecurity Military-Civil Fusion Cybersecurity Innovation Center[119]—identified its automated software-vulnerability discovery tools as an "Assassin's Mace" for China's military.[120] While the technical merit of the CEO's comments are debatable, his remarks and the company's relationship to the PLA demonstrate that the company intends to fulfill China's strategic needs; namely, an asymmetric advantage in the cyber domain. Technical innovation from all companies at the NCC, not just Beijing Topsec and Qihoo360, will likely benefits China's state-backed hacking teams.

Shared Services Zone (共享服务区)

The Shared Services Zone includes the Technology Certification Center, Technology Evaluation Center, Exhibition/Conference Center,[121] and the Commercial Center. These four centers are designed to provide common services and event spaces for businesses and institutions at the NCC.

Figure 12: Shared Services Zone, Original NCC Proposal

Source: City of Wuhan Land Use and Urban Space Planning Research Center.[122]

Technology Certification Center (网络安全审查技术与认证分中心)

The Technology Certification Center is run by the China Information Security Certification Center (ISCCC, 中国网络安全审查技术与认证中心), a government agency responsible for the certification of basic cybersecurity for products, licensed personnel, management systems, and information security services.[123] The ISCCC performs similar functions to the American National Standards Institute's National Accreditation Board and American Association for Laboratory Accreditation, charged with implementing NIST's standards for cybersecurity systems.[124] The Technology Certification Center will likely perform the same services for on-site technology systems, providing cybersecurity evaluation for new products and services developed at the NCC.[125]

Technology Evaluation Center (测试中心)

Information about the Technology Evaluation Center's role is sparse, but its presence is confirmed by four government documents and one private company's website.[126] Some documents show it co-located with the Technology Certification Center.[127] But, unlike the latter, there are no sources indicating who is responsible for the Technology Evaluation Center. This ambiguity likely stems from the Center's relationship with its namesake organization, the China Information Technology Security Evaluation Center (CNITSEC)—also known as the 13th bureau of the Ministry of State Security.[128] The 13th bureau oversees the cybersecurity posture of government agencies and offices. But at least one of its regional offices—Guangdong ITSEC—has been linked to a state-sponsored hacking group (APT3).[129] The Technology Evaluation Center may provide security and defensive services for the Supercomputing/Cloud Computing Center, the National Cybersecurity School, and NCC laboratories.

Exhibition and Conference Center (会议中心)

Figure 13: Exhibition and Conference Center

Source: Apollo Mapping; JJW.com.[130]

The Exhibition and Conference Center hosts large-scale events and promotes investment in the NCC.[131] The Exhibition Center is 100 m^2 with three exhibition halls.[132] Since opening in July 2019, it has hosted several events, including signing ceremonies for new participants in the NCC; the opening of the "Yellow Crane Cup," a

cybersecurity competition; and a conference for the Shanghai Cooperation Organisation's Information Security Working Group.[133] In its 2019 budget, the Wuhan Municipal Cyberspace Administration announced plans to host a global cybersecurity conference at the facility, referring to it as a "Chinese Black Hat Conference." The name is a nod to the U.S.-based Black Hat—an industry leading cybersecurity conference. The event was likely disrupted by the COVID-19 pandemic, but may restart in 2021.[134]

Figure 14: Competitors in the 2019 Yellow Crane Cup

Source: 中国网络安全审查技术与认证中心.[135]

Commercial Center (商务中心)

The Commercial Center is made up of two office buildings, currently housing 42 companies in residence.[136]

Industrial Development Zone (产业发展区)

The Industrial Development Zone includes the Supercomputing and Big Data Center, the Incubator, and the Cybersecurity Industrial Park.

The Cybersecurity Industrial Park

The original project proposal for the NCC cites North Carolina's Research Triangle Park as a model to replicate for research-fueled economic development.[137] The goal of both parks is to concentrate businesses and capital, incorporate talent from nearby universities, and move scientific research towards commercialization.[138] The NCC's industrial park includes business headquarters, private R&D facilities, "a national cybersecurity research center," an innovation and entrepreneur incubator (located on Phase I), and "strategic enterprises in military-civil fusion (军民融合) and cybersecurity."[139] The industrial park is massive. At 36 km^2, it is one-third of the size of San Francisco.[140]

Illustrating CCP policymakers' commitment to reducing red tape, the NCC cut business taxes, provided subsidies for entrepreneurs, and removed regulatory barriers to incorporating businesses. The proposed tax structure for the NCC would only tax businesses after "cash gains are generated" and would pay entrepreneurs' income taxes before businesses are profitable.[141] These policies aim to build a cybersecurity industrial park fueled by local talent, concentrated business R&D, and easy access to capital markets. Policymakers' willingness to cut burdensome regulations demonstrates the importance of the NCC to a country that otherwise ranks 31st on the World Bank's Ease of Doing Business Index.[142] It is a commonly-used playbook in a country littered with special economic zones.

Supercomputing and Big Data Center (超算中心/大数据中心)

The NCC relies on two facilities, one on-site and one off-site, to provide cloud computing and data storage solutions.[143] The Supercomputing and Big Data Center is, confusingly, the smaller of the two and is located just south of Phase I. The second site, Data Valley, is located on Phase I and is far larger and more powerful.

Figure 15: The Supercomputing and Big Data Center, south of the NCC

Source: 武汉新闻广播, Sohu.[144]

The Supercomputing and Big Data Center, a joint effort between Centrin Data Systems and Huawei, is neither all that "super" nor even particularly "big" compared to other data centers.[145] The center was the first project established under the umbrella of the NCC, opening in December 2016 as a stopgap for the NCC's cloud computing services, and scaling its capabilities as construction progressed.[146] As of November 2020, it contained more than two thousand servers, a 60,000-core vCPU, 8 petabytes (PB) of RAM, and 80PB of data storage.[147] It is reportedly the largest container data center in China.[148] That title is, at best, a stretch—drop the word "container", which only means that servers are stored in shipping containers, and the facility is small by comparison to other data facilities. Amazon Web Services' Snowmobile, a semitruck outfitted to transport data, boasts 100PB of storage capacity—20PB more than the facility—and costs only $500,000 per month for data storage.[149] Besides being more capable than the Supercomputing and Big Data Center, the Amazon Snowmobile is just a single container.

Figure 16: Data Valley concept art (left). Current construction progress (right).

Source: City of Wuhan Land Use and Urban Space Planning Research Center; Apollo Mapping.[150]

Data Valley, the second site—also constructed by Centrin Data Systems—is a sprawling complex of three large and four medium-sized data storage buildings, an operation and maintenance center, a control center, and dedicated backup power supplies.[151] Once complete, Data Valley's total storage capacity will reach 10 exabytes at a total cost of RMB 10.5 billion.[152] This is relatively small given the size of modern cloud computing—Data Valley's total storage capacity may be on par with just one of Amazon Web Services' approximately 80 data centers.[153] Besides serving the NCC, Data Valley is committed to supporting the Wuhan City Cloud Platform, a smart city initiative, and the Hubei provincial government—both of which will take up space.[154] The storage capacity for the NCC will likely be enough to keep any research and development data on-site.

Along with normal storage capacity, Data Valley touts an adequate, but by no means "super," computational capacity of 1 petaflops.[155] This is enough to manage a data center, but is not enough to rank among the Top 500 Supercomputers.[156] If OpenAI tried to train their famous GPT-3 language model at the Data Valley facility, it would take nearly 10 years at full tilt.[157] Alphabet, Google's parent company, rents five times as much computational power for $24 per hour.[158] Based on the cloud computing and data storage services offered by Data Valley, the facility's computational

capacity seems to align with the structure of a traditional data center, rather than a supercomputer.

The Supercomputing and Big Data Center and Data Valley may yet live up to its name if a claim on Centrin Data Systems' website proves true. Centrin claims that Data Valley will be constructed in two phases, and that Phase I of construction began in May 2018.[159] While there are no other mentions of a two-phase plan, the current structures on the NCC match what Centrin refers to as "phase I."

The Wuhan government provides matching land grants to companies establishing data centers in the NCC, with a minimum fixed investment of RMB 3 billion.[160] So far, only the Centrin Data System's Supercomputing and Big Data Center (including Data Valley) meets this threshold. Qualifying companies who buy land to build data centers are given the same amount of land for free, to be used for residential and commercial purposes, though the location is subject to local government planning approval. This will likely have three major impacts. First, benefits accrue only to companies able to spend RMB 3 billion on data centers, stifling competition. Second, policymakers' plans to create a shared "data trough" for startups and businesses in the NCC will serve as a valuable resource as companies chase innovation in AI. Third, companies that open data centers will be incentivized to open more local offices. Free land from an initial investment transforms into an anchor for the business's development.

Incubator (孵化器)

Figure 17: Incubator

Source: Apollo Mapping.

The NCC's Incubator is one of the largest cybersecurity incubators in China according to the Hubei provincial government.[161] The facility has attracted investment of more than RMB 3 billion.[162] Led by Tsinghua University's TUS Holdings, the Incubator will help commercialize research and fund startups.[163] Besides these services, the Incubator will help scale up existing enterprises by providing accelerator programs for small businesses.[164] These programs extend support to the full early lifecycle of companies, and aim to attract nascent companies to the NCC from elsewhere in China. The construction bid for the Incubator estimated that construction would finish near the end of 2021.[165]

Besides providing financial support and office space to startups, policymakers want the Incubator to be a point of collaboration for aspiring innovators, entrepreneurs, and established businesses. Like other business incubators across the world, shared spaces and programs facilitate the exchange of ideas between stakeholders.[166] China's policymakers hope the cross-fertilization of students and experts will contribute to the development of new technologies and new applications for existing technologies. According to government announcements, more than two hundred companies are involved with the Incubator.[167] What counts as "involved" is unclear, however. Most companies are likely to supply employees as mentors and help participants hone their business skills.

Figure 18: Sign for the NCC Incubator

Source: 北京云峰数展, Sohu.[168]

For the Incubator to achieve its main goal of commercializing research, money must flow from investors to startups. The local government has turned these investment funds into tools of the state. Government documents outline an NCC-specific industry fund to allocate money collected from state-owned enterprises (SOEs) and private investors[169] to companies within the Incubator.[170] The governance structure of these funds is opaque, so it is unclear how much influence private investors have in the process of capital allocation. But the fund's money is not unlimited. To ensure that the government might recover its funds, the Wuhan

municipal government will incentivize startups to list on stock exchanges.[171] This allows the investment fund to cash out its equity positions and reinvest in other startups. In some cases, however, the government may choose to not cash out. Though the Chinese government does not need to have an equity stake in order to access any particular technology, some corporate ownership is likely to facilitate conversations with businesses whose products are put to use by the state. A December 2020 report that claimed Chinese tech giants help process data from state espionage operations also found that company employees are sometimes peeved by the additional work.[172] Being tasked by a government official might be irksome; getting the same task from a shareholder may be more palatable.

Businesses and the NCC

Businesses are at the core of policymakers' strategic plans and objectives for the NCC.[173] The private sector influences the curriculum of the National Cybersecurity School, provides training sessions offered by the Talent Cultivation Center, and administers many of the NCC's functions.

Though the NCC is still under construction, businesses are lining up to claim a slice of land. As of September 2020, 114 companies had agreed to establish a presence in the NCC, promising more than $71.5 billion in investment.[174] Commitments range from secondary company headquarters—as is the case for Qihoo360 (北京奇虎360 有限公司)[175]—to national R&D headquarters or regional offices.[176] In its 2019 annual report, Wuhan municipal government reported vast investments by companies. Registered capital—the sum that shareholders commit to a firm within a specific local administration[177]—totaled RMB 28.7 billion.[178] Sixteen business projects already underway totaled RMB 200 billion. Separately, companies inked deals worth RMB 273.4 billion to start 58 more projects within the NCC.[179]

However, China's government has exaggerated commitments to technology development in the past. A much vaunted $150 billion government fund to support the indigenous development of advanced semiconductor manufacturing only allocated $12 billion over its first four years.[180] Moreover, in the same year that Wuhan municipal government reported massive investments in the NCC, Dongxiu District Government (the level below municipal government) published an annual report citing difficulties in attracting "a large number of projects" to the base.[181] Similarly, it is unclear just how far the "committed capital" which accounted for more than half the NCC's $71.5 billion investment can be relied upon.[182] For example, Hongxin Semiconductors (武汉弘芯半导体) built a chip fabricator at the NCC and planned to invest over RMB 120 billion on manufacturing capabilities across China. In early 2021, the business declared bankruptcy and collapsed.[183] Nevertheless, more mature companies with plans to move into the NCC may be less prone to this kind of turbulence.

Attracting companies to the NCC is critical to its success. China's deficit of 1.4 million cybersecurity professionals is coupled with a concentration of talent in a handful of technology and telecommunications companies. Less than one-fifth of cybersecurity professionals work for the government, public institutions, or research institutions.[184] If well-staffed companies do not move to the NCC, it will be difficult to reach the critical mass—the tipping point at which the NCC becomes so important that it is costly for companies to not take part. To attract investment to the NCC, Wuhan municipal government promises subsidies—eight percent of the investment total, up to RMB 8 million—for businesses investing more than RMB 50 million in a project that meets the city's "cybersecurity industry development plans."[185] The district government also promises subsidies—2-8 percent of the fixed asset investment—for "key projects in the production chain."[186] These high capital requirements encourage established companies to relocate or make significant investments in the NCC. The municipal and district governments have also waived administrative fees associated with investment ventures, construction projects, and relocation of businesses to the NCC.[187]

Some of the companies committed to moving to the NCC (see appendix) receive more attention than others. From the private sector, Qihoo360, Beijing Topsec, NSFocus, and DeepBlue AI (深兰科技) are often touted for their commitment to the NCC. Qihoo360—a cybersecurity company listed for "presumption of denial" on the U.S. Bureau of Industry and Security's Entity List, a trade blacklist—committed to building its secondary headquarters at the NCC.[188] Similarly, Beijing Topsec, a company that was tied to the 2015 hack of Anthem Insurance, moved more than four hundred employees into its R&D center on the NCC.[189] Another firm connected to state-sponsored hacking and the military, NSFocus, is also constructing and R&D and Operations Center at the NCC.[190] DeepBlue AI, a tech unicorn and national AI champion supplied palm scanners for dorms and technology for smart classrooms.[191] The company is also setting up a less well-publicized project to research AI's application to cybersecurity.[192] DeepBlue AI incorporated a subsidiary, DeepBlue AI Network

Security Technology (Wuhan) Co. (深兰网安科技(武汉)有限公司), in the NCC to conduct R&D on the technology.[193]

Figure 19: A palm scanner provided by DeepBlue AI (left). Students submit palm prints for use (right).

Source: *我要发大财财*, *Bilibili;*[194] 机智的王小鹏, Bilibili.[195]

Defense SOEs, such as China Aerospace Science and Industry Corporation and China Electronics Technology Group Corporation, have also received government plaudits for work related to the NCC. Both CASIC and CETC are party to a 2017 strategic cooperation framework with the PLA Strategic Support Force.[196] According to state media, CASIC and CETC (among seven other institutions) will "concentrate on training high-end talents for new combat forces, building innovation teams, and conducting cutting-edge S&T research."[197] These SOEs are committing resources to the NCC to help develop the talent and innovation the PLA SSF needs. CASIC is the parent company of Hubei Aerospace Information Technology Co., which changed its address of incorporation to the NCC in August 2018.[198] Together, Hubei Aerospace Information Technology and CASIC committed RMB 6 billion to build an "intelligent cybersecurity industrial base" (智能网安产业基地) within the NCC.[199] CASIC's Second Academy, which is listed on the U.S. Department of Commerce's Bureau of Industry and Security Entity List, will operate the research facility on the NCC.[200] The facility, its location on the NCC, and the strategic cooperation framework agreement with the PLA SSF make the "intelligent cybersecurity industrial base" a great way to track local innovations that could serve as the CCP's "assassin's mace" in the cyber domain.

Besides investing in on-site research and development, CASIC launched its Intelligent Cloud 3.0 Platform during an event at the NCC in late 2020.[201] Attendees included a diverse group stakeholders, including political representation from the Wuhan municipal government and the National People's Congress, as well as national security stakeholders from the Ministry of Public Security, the Cyberspace Administration of China, and the State Administration for Science, Technology and Industry for National Defense.[202] Other SOEs, such as China Electronics Technology Group Corporation and China Electronic Information Industry Group Corporation, have been involved in the NCC since its launch in 2016, but have been less public about their support.[203]

Figure 20: CASIC launches Intelligent Cloud 3.0

Source: 中国航天科工.[204]

Prior to 2020, the NCC aimed to attract foreign investments. Announcements from the NCC's launch ceremony in 2016 lauded Cisco, Kaspersky, and Microsoft for "lining up to invest."[205] Attracting foreign investment was likely eliminated as a goal in 2020, however.[206] A district government report requesting the cancelation of a foreign capital performance metric cited the CCP Central Committee Cyberspace Affairs Commission, stating that: "leaders have repeatedly made it clear that the National Cybersecurity Base must closely monitor independent innovation (自主创新) of core cybersecurity technologies, promote Chinese-made independently controllable (自主可控) replacement plans, and build a secure and controllable information technology

system… we must be cautious about foreign investment projects."[207] The elimination of foreign capital investment is a sign that China's government plans to monitor, control, and implement new technologies from the NCC's labs and Incubator. The view that a "purely domestically funded" (纯内资) corporate structure is important on projects related to national security now permeates much of the technology development ecosystem.[208] The exclusion of foreign firm is particularly important to PLA SSF, since the force views foreign technology as a potential Trojan horse for foreign spies.[209] The prohibition of foreign firms at the NCC aligns well with PLA SSF development priorities.

Cisco's involvement on the NCC provides one example. Early documentation shows that some of the NCC's training facilities are likely operated on Cisco's Cyber Range platform.[210] Multiple sources claim that Cisco's platform opened for use in December 2017, but questions remain unanswered about its exact location.[211] Satellite imaging from early 2018 does not indicate any significant construction in Phase I, but a no-longer-available Hubei government web page touted the training of its first class of personnel in December 2017.[212] The lack of sources on the use of Cisco's Cyber Range Platform after 2017, and the removal of a government web page before researchers could archive it, illustrates the change in the NCC's approach to foreign companies.

The CCP's propensity to co-opt nongovernment resources extends to businesses located at the NCC. While businesses are free to innovate and commercialize research conducted, it is likely that much of their research is driven by China's national interests. As with the National Cybersecurity School and the Talent Cultivation and Testing Center, businesses operating within the NCC are meant to work towards China's strategic goals. Reports published in late 2020 demonstrated how China's National Security Law can turn corporate titans into data processing centers for the security services—essentially receiving taskings from intelligence agencies.[213] With its concentration of talent and resources, co-opting the structures of the NCC seems like a natural progression in China's pursuit of becoming a "cyber powerhouse."

Conclusion

China wants to be a "cyber powerhouse."[214] A deficit of cybersecurity professionals in China—1.4 million, by some accounts[215]—limits the country's cybersecurity capabilities, leaving businesses and infrastructure vulnerable to attacks while spreading offensive talent thin. Despite this, China is already a near-peer cyber power to the United States. But it does not want to be second best. By 2030, the NCC aims to have contributed to the training of over five hundred thousand cybersecurity practitioners, alleviating the shortage of talent. The NCC will bolster China's already potent cyber capabilities, making competition in the cyber domain fiercer still. U.S. policymakers should anticipate that increased Chinese capabilities will threaten the U.S. advantage in cyberspace, a vulnerability which will likely be to the detriment of core U.S. interests.

The NCC will advance China's offensive and defensive cyber capabilities. Unlike the tools for cyber defense, where there is a well-developed market in which companies innovate and compete for profits, offensive cyber capabilities have only one legal market in China: the government. Though offensive techniques are not the sole focus of the NCC's training or development, the evidence suggests that they are not a mere byproduct of studying cyber defense either. The NCC aims to advance China's cybersecurity capabilities in two strokes—bolstering the talent pipeline, and supporting innovation and entrepreneurship.

Certifying seventy thousand cybersecurity practitioners each year through the Talent Cultivation and Testing Center and graduating four thousand to six thousand students of the National Cybersecurity School would significantly improve the cybersecurity environment in China. That the NCC's core mission is the National Cybersecurity School suggests that the primary impetus for the project was to increase the quality and quantity of students in the talent pipeline.[216] The school's focus on practical, hands-on learning and the substitution of school course credits with certifications from the Talent Cultivation and Testing Center makes its graduates particularly attractive for government and private

sector employers seeking to bolster their cyber capabilities. Students at the NCC can build relationships with companies they will eventually work for, solicit support from the Incubator for their new startup, or attain certifications that give them preferential treatment when applying to jobs. Online programs targeted at broader audiences may further expand the talent pool. Together, the National Cybersecurity School and Talent Cultivation and Testing Center will create a rigorous learning environment, increase connectivity between stakeholders in the cybersecurity ecosystem, and represent a broad-based attempt to expand the talent pool.

The NCC's commitment to supporting innovation will improve China's capabilities in the cyber domain. Innovative tools can increase the automation of cybersecurity, generate new offensive and defensive techniques, and shape the operational environment of cyberspace. The CCP aims to harness future innovation from the NCC's school, businesses, and startups in service of the Party's strategic interests. Some of the students and technology will go on to support the PLA SSF's hacking teams. The NCC has already hosted a competition for automated hacking systems, like the kind tested at DARPA's 2016 Cyber Grand Challenge, demonstrating it will attract the type of innovations sought by the PLA.[217] Policy statements prohibiting foreign companies contributing to the NCC also make clear that the state will track and target new technologies as they are created at the NCC.[218] This will allow the Party, its military, and the security services to rapidly adopt new replacement technology. The NCC's focus on innovation aims to make China stronger, richer, and more self-sufficient.

While bringing together government, academia, and the private sector is far from a new strategy, the NCC is unique in China for its focus on cybersecurity, the depth of the private-sector connections, and the extent of government direction. In the long run, the NCC will likely prove to be a foundation for technological progress and talent cultivation that significantly impacts the dynamics of nation-state cyber competition. The NCC will help the PLA make progress on the three obstacles constraining its capabilities: talent, innovation, and indigenization.[219] China's corps of military cyber

operators, private sector mercenaries, and state security services' hackers will slowly be filled by successive classes of NCC graduates. The cyber tools they use may well be designed by NCC graduates, too. China's competitors in cyberspace should be prepared.

Author

Dakota Cary is a research analyst at CSET, where he works on the CyberAI Project.

Acknowledgments

For feedback and assistance, thanks to John Bansemer, Jennifer Melot, Kayla Goode, Hannah Stone, Jeffrey Ding, Emily Weinstein, Ryan Fedasiuk, Ben Murphy, Shelton Fitch, Scott Harold, Kady Arthur, and Benjamin Pollack.

Document Identifier: doi: 10.51593/2020CA016

Endnotes

[1] Translator's note: For a more in-depth discussion in English of the Chinese term 网络强国, which can be rendered as "cyber powerhouse" or "cyber superpower," see Rogier Creemers et al., "Lexicon: 网络强国 Wǎngluo Qiángguó," *New America*, May 31, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/.

[2] "NIDS China Security Report 2021: China's Military Strategy in the New Era" (National Institute for Defense Studies, Japan, 2020), https://perma.cc/C7KK-DF6N.

[3] "NIDS China Security Report 2021: China's Military Strategy in the New Era."

[4] "对话国家网安基地办主任：网络安全人才要放到 '战场' 上培养," *北京报*, September 18, 2020, https://perma.cc/H5DB-W3V4 or https://web.archive.org/web/20200925071040/https://new.qq.com/rain/a/20200918A07VH5.

[5] "NIDS China Security Report 2021: China's Military Strategy in the New Era."

[6] "China's AI Strategy and Development: A Glossary of Key Terms" (Center for Security and Emerging Technology, forthcoming).

[7] M. Taylor Fravel, "China's New Military Strategy: "Winning Informationized Local Wars," *China Brief* 15, no. 13 (July 2, 2015): https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/; Elsa B. Kania and John Costello, "Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power," *Journal of Strategic Studies* 44, no. 2 (May 12, 2020): 218-264.

[8] The U.S. Department of Defense 2020 China Military Power Report offers a comprehensive, six-part definition of China's MCF Strategy. "MCF encompasses six interrelated efforts: (1) fusing the China's defense industrial base and its civilian technology and industrial base; (2) integrating and leveraging science and technology innovations across military and civilian sectors; (3) cultivating talent and blending military and civilian expertise and knowledge; (4) building military requirements into civilian infrastructure and leveraging civilian construction for military purposes; (5) leveraging civilian service and logistics capabilities for military purposes; and, (6) expanding and deepening China's national defense mobilization system to include all relevant aspects of its society and economy for use in competition and war." See Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2020* (Washington, D.C.: Department of Defense, 2020), vi, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF. The CCP Central Committee Cyberspace Administration Commission's own interpretation is published here:

Office of the Central Cyberspace Affairs Commission, "网络信息体系军民融合战略的思考," Cyberspace Administration of China, November 12, 2018, https://perma.cc/8V6R-LSRQ.

[9] "NIDS China Security Report 2021: China's Military Strategy in the New Era."

[10] CSET original translation of "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office" [现代服务产业建设管理办公室 2019 年工作总结及 2020 年计划], October 28, 2019, https://cset.georgetown.edu/wp-content/uploads/t0255_service_industry_office_EN.pdf. Original text in Chinese can be found here: https://perma.cc/9KJ6-467J.

[11] 李墨, "360'第二总部'落子武汉 在光谷设研发运营中心." *湖北日报*, November 25, 2017, https://perma.cc/QME4-YV9U.

[12] 李墨, "360'第二总部'落子武汉 在光谷设研发运营中心."

[13] 许雯, "对话国家网安基地办主任：网络安全人才要放到'战场'上培养," *新京报*, September 20, 2018, https://perma.cc/H5DB-W3V4.

[14] 崔光耀, "漫说网络安人才的热点和难点," *中国信息安全* 12 (2018): 48-49, CNKI:SUN:CINS.0.2018-12-023.

[15] 崔光耀, "漫说网络安人才的热点和难点"; Peter L. Mattis and Matthew J. Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis, Maryland: Naval Institute Press, 2019). Attribution as MSS13th.

[16] 赵银平, "建设网络强国--习近平一直'在线,'" *新华网*, March 22, 2019, https://perma.cc/JK49-Y5W5.

[17] These cyber-specific challenges likely extend to China's civilian intelligence service, the Ministry of State Security, and its internal security agency, the Ministry of Public Security. See "NIDS China Security Report 2021: China's Military Strategy in the New Era."

[18] "China's Cyber Power in a New Era," in *Asia Pacific Regional Security Assessment 2019* (International Institute for Strategic Studies, 2019), 77–90, https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5.

[19] 习近平, "习近平在网信工作座谈会上的讲话全文发表," *新华网*, April 25, 2016, https://perma.cc/V9ZF-UZLH.

[20] (Although the NCC's operations were impacted in 2020 by Covid-19, the facility's construction and use now continues unabated.) "陕西国家信息安全产业园," *百科*, captured October 7, 2020,

https://web.archive.org/web/20201007142054/https://baike.baidu.com/item/%E9%99%95%E8%A5%BF%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E4%BA%A7%E4%B8%9A%E5%9B%AD/2521683?fr=aladdin; "战略合作伙伴," 天津国家信息安全产业基地，captured August 16, 2018, https://web.archive.org/web/20180816163106/http://www.nisib.cn/NewsList_18.aspx; "Home Page." 天津国家信息安全产业基地，captured August 16, 2018, https://web.archive.org/web/20180816171658/http://nisib.cn/Default.aspx; 崔光耀, "漫说网络安人才的热点和难点," *China Information Security* 12 (2018): pg. 48-49, CNKI:SUN:CINS.0.2018-12-023; "国信安基地," *百科*, captured June 1, 2021, https://perma.cc/HM6T-FRR5; "国家信息安全成果产业化（西部）基地," 前瞻产业研究院, captured June 1, 2021. https://perma.cc/K4WJ-LZJX; 叶国标 and 刘颖, "国家信息安全成果产业化(东部)基地初具规模," *新华网*, July 7, 2002, https://perma.cc/L4SZ-26Q3.

[21] "国家网络安全人才与创新基地基本概况," Huazhong University of Science and Technology School of Cyber Science and Engineering, August 2019, https://perma.cc/TVB2-XB6Z.

[22] 庄荣文, "把握信息时代机遇 推进网络强国建设 为实现中华民族伟大复兴中国梦贡献力量," 时事报告(党委中心组学习) 5 (2019), CNKI:SUN:SBDX.0.2019-05-005 [切实提升网络安全防护能力].

[23] *Constitution of the Communist Party of China*, Chapter 2, Article 10, Section 3, revised October 24, 2017, http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf.

[24] Damien Ma et al., "About The Committee," Macro Polo, October 2017, https://macropolo.org/digital-projects/the-committee/about-the-committee/.

[25] CSET original translation of Chinese Communist Party (CCP) Central Committee, "CCP Central Committee Publishes Plan for Deepening the Reform of Party and State Agencies" [中共中央印发《深化党和国家机构改革方案》], *Xinhua News Agency*, March 21, 2018, https://cset.georgetown.edu/wp-content/uploads/t0280_PRC_reform_plan_2018_EN.pdf.

[26] The CCP Central Committee Cyberspace Affairs Commission is also called the Cyberspace Administration of China, which is the corresponding government office to the Cyberspace Affairs Commission under a different name. "Bilingual State Council Organizational Chart," NPC Observer, last updated May 13, 2021, https://npcobserver.com/resources/bilingual-state-council-organizational-chart/; CSET original translation of Chinese Communist Party (CCP) Central Committee, "CCP Central Committee Publishes Plan"; State Commission for Public Sector Reform, "Committees and Commissions of the CCP's Central Committee," https://perma.cc/D43L-BHF6.

[27] Rogier Creemers et al., "China's Cyberspace Authorities Set to Gain Clout in Reorganization," *New America*, March 26, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/; "Bilingual State Council Organizational Chart"; John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, DC: National Defense University Press, 2018), 53, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

[28] "国家网络安全人才与创新基地," *新华网*, August 19, 2020, https://perma.cc/YL3D-DCG6.

[29] 武汉市互联网信息办公室, "国家网安基地建设指导委员会第一次工作会议在武汉召开," April 22, 2019, https://perma.cc/79YQ-FWRN?type=image; "国家网络安全人才与创新基地," 新华网, August 19, 2020, https://perma.cc/YL3D-DCG6"; "市国家网络安全人才与创新基地建设工作领导小组组成人员调整," *武汉市人民政府公报* 13 (2017); 谢慧敏, "湖北召开省国家网络基地监视工作领导小组会议,", *湖北日报*, January 13, 2020, https://perma.cc/MVF9-JN8H?type=image; "Wuhan Municipal CAC 2019 Budget," 武汉市互联网信息办公室, captured January 28, 2021, https://perma.cc/CY76-4UV8.
Dakota Cary, "*China's National Cybersecurity Center: A Base for Military Civil Fusion in the Cyber Domain*." June 29, 2021.

[30] "市国家网络安全人才与创新基地建设工作领导小组组成人员调整," *武汉市人民政府公报* 13 (2017).

[31] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation," *China Information Security* 10 (2017), *CNKI:SUN:CINS.0.2017-10-041*.

[32] "Wuhan City Cyberspace Administration 2019 Budget." **武汉市互联网信息办公室**, captured January 28, 2021, 50, https://perma.cc/CY76-4UV8.

[33] "国家网络安全人才与创新基地," *新华网*, August 19, 2020, https://perma.cc/YL3D-DCG6.

[34] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation." Currency valuation as of June 21, 2021.

[35] Original CSET Translation of "Research Report on the Status of China's Information Security Professionals (2018-2019)" [中国信息安全从业人员现状调研报告（2018-2019 年度）], China Information Technology Security Evaluation Center, September 6, 2019, https://cset.georgetown.edu/wp-content/uploads/t0231_cyber_employment_report_EN.pdf. This 2019 employment survey of cybersecurity professionals published by CNITSEC found

the median income for practitioners to be between RMB 100K-200K, with 91.3 percent of respondents making less than RMB 300K annually. Emily Weinstein, "Chinese Talent Program Tracker," Center for Security and Emerging Technology, https://chinatalenttracker.cset.tech/.

[36] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[37] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation." The document does not stipulate a dollar amount for these figures. "国家网络安全人才与创新基地," *新华网*, August 19, 2020, https://perma.cc/YL3D-DCG6. Apartment blocks adjacent to the NCC and built between 2017 and 2020 advertise low-cost "Cybersecurity Apartments." A subsidiary of TUS Holdings (a leading player at the NCC) is listed as the developer of the apartment complex. This subsidiary is registered at the same address as many other NCC-related enterprises (武汉临空港经济技术开发区五环大道 666 号(10)), suggesting that these apartments are at least one element of the subsidized housing program. It is unclear whether these off-campus apartments constitute a completed "Talent Community," or if on-campus housing is still under development. "网安合寓," 安居客, captured June 1, 2021, https://perma.cc/TCN9-P2ZH; "43 平 2 室 2 厅 2 卫 三轨交汇 数万高端商业精英大学旁公园边," 安居客, captured February 3, 2021, https://perma.cc/5X44-26Q7; "启迪网安和众科技发展（武汉）有限公司," 企查查, captured June 1, 2021, https://perma.cc/AJ55-AN6M.

[38] Wuhan Airport Development Zone Committee (武汉临空港开发区管委会) and Wuhan City Cyberspace Administration, "Notice on Special Fund Management Rules for the Cybersecurity Ten Thousand Talents Grant Program (Trial)," January 14, 2020; 袁胜, "网安人才培养进入'快车道'," *China Information Security* 10 (2017): 50-53, CNKI:SUN:CINS.0.2017-10-038; "Industry Trends," *China Information Security* 8 (2017): 24-25, CNKI:SUN:CINS.0.2017-08-015; General Office (办公厅) of the Wuhan City People's Government, "Notice of the [Wuhan] City People's Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base," March 3, 2017, https://perma.cc/74PC-APS7; 中国网络安全审查技术与认证中心, "信安中心进入'网络安全万人培训资助计划'" August 1, 2018, https://perma.cc/B4NU-C6J7?type=image.

Dakota Cary, "*China's National Cybersecurity Center: A Base for Military Civil Fusion in the Cyber Domain*." June 29, 2021.

[39] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[40] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[41] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation." The document does not stipulate a dollar amount for these figures.

[42] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation." The document does not stipulate a dollar amount for these figures.

[43] City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计," 百度文库, February 2017, https://drive.google.com/drive/folders/11ZX2xxFRUmhUxLY7XyQALKIBbFERvWSr?usp=sharing.

[44] 张雪峰, 安凯军, and 刘平, "浅析信息网络安全新形势及对策," *数字通信世界* 1 (2020): 156, 158.

[45] Centrin Data Systems, "国家安全网络安全人才与创新基地," Wuhan Supercomputing Center, https://perma.cc/C5QH-T4FD.

[46] Centrin Data Systems, "国家安全网络安全人才与创新基地."

[47] When the Cyberspace Administration of China announced the NCC in 2016, central government policymakers also enumerated "five innovations" that should guide its development and ensure it achieved the CCP's original intentions. The CAC's "five innovations" did not provide much guidance when originally announced; they were essentially a collection of commandments left open to interpretation. The "five innovations" are: "Innovate New Methods for Administering Cybersecurity Schools, Innovate New Ways of Assembling Cybersecurity Talent, Innovate New Methods of Cultivating Cybersecurity Talent, Establish a System for Evaluating and Certifying Cybersecurity Talent, and Construct a Top-Class Cybersecurity Industrial Park." Within a year of the NCC's announcement and its accompanying "five innovations," the Wuhan Municipal CAC expanded on these broad concepts. The "Wuhan Model'' of Cybersecurity Talent Cultivation described how major components of the base are to be operated with varying levels of specificity. Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation"; Office of the Central Cyberspace Affairs Commission, "国家网络安全人才与创新基地吸引众多知名企业," Cyberspace Administration of China, September 19, 2016, https://perma.cc/N98W-5VWU.

[48] 胡曙光, "突破性发展网络安全产业 建设国家网络安全港," *湖北政协* 3 (2019): 21-22, CNKI:SUN:SJXT.0.2019-03-011.

[49] 胡曙光, "突破性发展网络安全产业 建设国家网络安全港."

[50] “国家网络安全人才与创新基地基本概况,” Huazhong University of Science and Technology, School of Cyber Science and Engineering, August 2019, https://perma.cc/TVB2-XB6Z.

[51] Office of the Central Cyberspace Affairs Commission, “武汉市委网信办：加快建设国家网络安全人才与创新基地,” Cyberspace Administration of China, August 25, 2020, https://perma.cc/9W9H-84PE?type=image; 中共中央网络安全和信息化领导小组办公室, “国家网络安全人才与创新基地吸引众多知名企业,” September 19, 2016, https://perma.cc/N98W-5VWU?type=image; a translation of Wuhan municipal government policies designed to support the establishment of the National Cybersecurity School published in 2017 is available here.

[52] “国家网络安全人才与创新基地基本概况,” Huazhong University of Science and Technology, School of Cyber Science and Engineering.

[53] 武汉市互联网信息办公室, “国家网络安全人才与创新基地六大重点项目正式开工建设,” August 28, 2017, https://perma.cc/96M5-2BM8?type=image.

[54] “国家网络安全人才与创新基地基本概况,” Huazhong University of Science and Technology, School of Cyber Science and Engineering.

[55] Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure.” Project 2049 Institute, November 11, 2011. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf The location of the sixth bureau is determined by using the MUCD, 61726 Unit. A daycare advertises itself to members of the sixth bureau, providing its on-site address. https://perma.cc/Y46E-PTVP

[56] Joske, Alex et al. “Wuhan University.” China Defence Universities Tracker. Australian Strategic Policy Institute, November 18, 2019. https://unitracker.aspi.org.au/universities/wuhan-university/

Joske, Alex et al. “Huazhong University of Science and Technology.” China Defence Universities Tracker. Australian Strategic Policy Institute, November 18, 2019. https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology/

[57] Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure.” Project 2049 Institute, November 11, 2011. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

[58] Lo, Tien-pin and Jason Pan. “PLA cyberunit targeting Taiwan named.” Taipei Times, March 10, 2015.

https://web.archive.org/web/20170820041946/http://www.taipeitimes.com/News/taiwan/archives/2015/03/10/2003613206

Gertz, Bill. "Network Effects: Chinese university lab linked to PLA cyber attacks." May 14, 2013. https://freebeacon.com/national-security/network-effects/

[59] Joske, Alex et al. "Wuhan University." China Defence Universities Tracker. Australian Strategic Policy Institute, November 18, 2019. https://unitracker.aspi.org.au/universities/wuhan-university/

Joske, Alex et al. "Huazhong University of Science and Technology." China Defence Universities Tracker. Australian Strategic Policy Institute, November 18, 2019. https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology/

[60] Huazhong University of Science and Technology. "关于面向全校本科生选拔国防科技生的通知." December 2, 2020. https://webcache.googleusercontent.com/search?q=cache:28VqhKtPgnYJ:https://job.hust.edu.cn/notice/1083435.htm+&cd=1&hl=en&ct=clnk&gl=us

[61] Gertz, Bill. "Network Effects: Chinese university lab linked to PLA cyber attacks." May 14, 2013. https://freebeacon.com/national-security/network-effects/

[62] Office of the Central Cyberspace Affairs Commission, "国家网络安全人才与创新基地吸引众多知名企业," Cyberspace Administration of China, September 19, 2016, https://perma.cc/N98W-5VWU; Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[63] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[64] Shao Lan and Sue Liu, "Institute for State Cybersecurity to be completed next year," *Changjiang Weekly*, April 20, 2018, https://www.pressreader.com/china/changjiang-weekly/20180420/page/1/textview.

[65] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[66] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[67] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[68] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[69] Office of the Central Cyberspace Affairs Commission, "武汉市委网信办：加快建设国家网络安全人才与创新基地," Cyberspace Administration of China, August 25, 2020, https://perma.cc/9W9H-84PE?type=image.

[70] "国家网络安全人才与创新基地," *新华网*, August 19, 2020, https://perma.cc/YL3D-DCG6; https://perma.cc/VX9Q-NECL?type=image.

[71] 天天风行-录制组, "TD 丶正直博_2020-09-12 13 时 16 分【极智未来】- 国家网安基地主题直播活动_哔哩哔哩_bilibili," September 9, 2020, https://www.bilibili.com/video/BV1WK411K748/.

[72] 柳洁 and 彭吉松, "武大华中大正式入驻国家网安基地网络安全学院," *经济日报*, August 9, 2020, https://perma.cc/Y2E6-5YJ5; Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation"; Li Jiancheng (李建成), vice dean at Wuhan University's Chinese Academy of Engineering, will serve as dean of the Cybersecurity College. Hu Ruimin (胡瑞敏), dean of Wuhan University's School of Computer Science, will serve as deputy dean. Huazhong University's School of Cyber Science and Engineering is led by university Executive Vice President Shao Xinyu (邵新宇) as dean, and Dean of the School of Computer Science Feng Dan (冯丹) as deputy dean.

[73] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[74] People's Government of Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office," https://web.archive.org/web/20210114142151/http:/www.dxh.gov.cn/ZWGK/QZFXXGKML/GHJH/202005/P020200514097399996987.pdf.

[75] People's Government of Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office."

[76] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[77] 天天风行-录制组, "TD 丶正直博_2020-09-12 13 时 16 分【极智未来】- 国家网安基地主题直播活动_哔哩哔哩_bilibili."

[78] 天天风行-录制组, "TD 丶正直博_2020-09-12 13 时 16 分【极智未来】- 国家网安基地主题直播活动_哔哩哔哩_bilibili."

[79] 柳洁 and 彭吉松, "武大华中大正式入驻国家网安基地网络安全学院"; "国家网络安全人才与创新基地," *新华网*, August 19, 2020, https://perma.cc/YL3D-DCG6; City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计," 百度文库, February 2017, https://drive.google.com/drive/folders/11ZX2xxFRUmhUxLY7XyQALKIBbFERvWSr?usp=sharing.

[80] 柳洁 and 彭吉松, "武大华中大正式入驻国家网安基地网络安全学院"; "国家网络安全人才与创新基地," *新华网*, August 19, 2020, https://perma.cc/YL3D-DCG6.

[81] "国家网络安全人才与创新基地," *新华网*.

[82] 彭瑶, "国家网络安全人才与创新基地办主任陈斗斗：拉近网安人才培养和企业实际应用之间的距离," 中国网信网, September 15, 2020, https://perma.cc/T6QS-53QC?type=image.

[83] City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计."

[84] 崔光耀, "漫说网络安人才的热点和难点," *中国信息安全* 12 (2018): 48-49, CNKI:SUN:CINS.0.2018-12-023.

[85] National Cybersecurity Center Talent Cultivation Center, "Home Page," captured November 15, 2019, https://perma.cc/EX5V-BYHV?type=image.

[86] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[87] National Cybersecurity Center Talent Cultivation Center. "Home Page"; Office of the Central Cyberspace Affairs Commission, "武汉市委网信办：加快建设国家网络安全人才与创新基地."

[88] The Center hosts training programs for several different certifications, including:

- Certified Information Security Professional—standard developed by MSS 13th Bureau, CNITSEC (注册信息安全专业人员)
- Certified Information Security Manager (注册信息安全员)
- Information Security Management Auditor (ISO/IEC27001 and ISO/IEC20000-1)
- Network Security Authentication Certification Engineer (NSACE)—standard developed by the Ministry of Industry and Information (工信部 NSACE 网络安全工程师认证)

- Information Security Protection Evaluator—standard developed by the Ministry of Public Security (公安部信息安全等级保护测评师)

- Certified Information Security Assurance Worker (CISAW)—standard developed by the China Cybersecurity Review Technology and Certification Center (信息安全保障从业人员认证)

National Cybersecurity Center Talent Cultivation Center, "Home Page."

[89] National Cybersecurity Center Talent Cultivation Center. "Home Page"; "永信至诚与武汉临空港开发区合力共建国家网安基地," Chinese Software Developer Network, February 24, 2017, https://perma.cc/8UA4-W34D?type=image.

[90] 国家网安基地培训中心, "武汉临空港网安基地培训学校 CISP 认证开班啦！扶持期间享优惠," *CNBlogs.com*, May 27, 2020, https://perma.cc/75N3-AHBK?type=image. Including Qianxin Technology, NSFocus Technology, Beijing TopSec, Cybersecurity Center Technology Services, and TUS Cybersecurity.

[91] Office of the Central Cyberspace Affairs Commission, "武汉市委网信办：加快建设国家网络安全人才与创新基地."

[92] "武汉临空港网安基地职业培训学校有限公司," 爱企查, captured January 28, 2021, https://perma.cc/3BM2-P3ZT; "启迪控股股份有限公司," 爱企查, captured January 28, 2021, https://perma.cc/ZL6J-ZP7U. The center is administered by Cybersecurity Center Training and Education Ltd., which is fully owned by Cybersecurity Center Technology Services Ltd.—a joint venture established by the Wuhan Airport Development Zone Investment Corporation (a district government entity) and TUS Holdings (a key player in the NCC's technology incubator).

[93] "永信至诚与武汉临空港开发区合力共建国家网安基地," Chinese Software Developer Network.

[94] Eudora Wang, "Chinese State-Owned Electronics Firm CEC Pays $547M For Stake In Network Security Giant." *China Money Network*, May 10, 2019, https://perma.cc/3WYS-HSXM?type=image. In May 2019, China Electronics Corporation, a state-owned telecom equipment producer, acquired a 22.59 percent stake in Qianxin to become the second largest shareholder in the company, behind only its chairman and CEO. People's Government of Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office."

[95] "永信至诚与武汉临空港开发区合力共建国家网安基地," Chinese Software Developer Network.

[96] 消费日报网, "奇安信华中总部将落户武汉国家网安基地," *中国日报网*, July 20, 2019, https://perma.cc/2Y96-U9BM?type=image; People's Government of

Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office."

[97] 消费日报网, "奇安信华中总部将落户武汉国家网安基地," *中国日报网*, July 20, 2019. https://perma.cc/2Y96-U9BM?type=image.

[98] Alex Stone and Peter Wood, "China's Military-Civil Fusion Strategy: A View from Chinese Strategists" (China Aerospace Studies Institute, June 15, 2020), https://static1.squarespace.com/static/5e356cfae72e4563b10cd310/t/5ee37fc2fcb96f58706a52e1/1591967685829/CASI+China%27s+Military+Civil+Fusion+Strategy-+Full+final.pdf.

[99] National Cybersecurity Center Talent Cultivation Center. "Home Page."

[100] National Cybersecurity Center Talent Cultivation Center. "Home Page."

[101] 国家网安基地培训中心, "武汉临空港网安基地培训学校 CISP 认证开班啦！扶持期间享优惠." Including Qianxin Technology, NSFocus Technology, Beijing TopSec, Cybersecurity Center Technology Services, and TUS Cybersecurity.

[102] General Office (办公厅) of the Wuhan City People's Government, "Notice of the [Wuhan] City People's Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base."

[103] General Office (办公厅) of the Wuhan City People's Government, "Notice of the [Wuhan] City People's Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base."

[104] In 2017, the Wuhan government committed to providing free offices and research facilities for a limited number of years to companies that conducted R&D at the base, including the use of the Offense and Defense Laboratory; the total subsidy was capped at RMB 100 million.

General Office (办公厅) of the Wuhan City People's Government, "Notice of the [Wuhan] City People's Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base."

[105] 汪甦 and 姜珊, "争分夺秒为企业"搭台"，网安基地首个网络安全攻防实验室本月建成," *Hubei Daily*, September 17, 2020, https://perma.cc/HM78-DGSQ?type=image; 石菲, "国家网络安全人才与创新基地落地武汉," *中国信息化* 12 (2016), CNKI:SUN:IGXN.0.2016-12-034.

[106] 黄金 and 郭淞冰, "以网安基地为引领，临空港五大产业蓄势腾飞," 武汉临空港报, September 19, 2020, https://perma.cc/B63Z-8NKG, https://web.archive.org/web/20200925075641/http://www.dxh.gov.cn/XWZX/LKGYW/202009/t20200918_1451935.shtml.

[107] Wuhan Anyu Information Security Co., Ltd, "Home Page," captured May 26, 2021, https://perma.cc/KU4R-TSB6.

[108] Wuhan Anyu Information Security Co., Ltd., "湖北省网络安全主管部门领导莅临武汉安域调研指导工作," December 30, 2019, https://perma.cc/7L8C-GBGQ.

[109] Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute, November 11, 2011. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

[110] City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计."

[111] General Office (办公厅) of the Wuhan City People's Government, "Notice of the [Wuhan] City People's Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base"; 崔光耀, "漫说网络安人才的热点和难点."

[112] "360 携手武汉市政府、武汉大学共建国家网络安全研究院," *Science China*, September 19, 2016, https://perma.cc/53D5-BWRW?type=image.

[113] "国家网络安全人才与创新基地基本概况," Huazhong University of Science and Technology, School of Cyber Science and Engineering; Office of the Central Cyberspace Affairs Commission, "双高聚焦网络安全人才培养与产业发展 全力推进国家网络安全人才与创新基地建设," Cyberspace Administration of China. 中国网信网, March 27, 2019. https://perma.cc/K4L2-JXAQ. Qihoo360 Attribution: Elsa B. Kania and Lorand Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy" (Center for a New American Security, January 28, 2021), https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy. Beijing TopSec Attribution: "US Embassy Cables: China Uses Access to Microsoft Source Code to Help Plot Cyber Warfare, US Fears," *The Guardian*, December 4, 2010, http://www.theguardian.com/world/us-embassy-cables-documents/214462.

[114] Qihoo360 Attribution: Kania and Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy." Beijing TopSec Attribution: "US Embassy Cables: China Uses Access to Microsoft Source Code to Help Plot Cyber Warfare, US Fears."

[115] A complete list of companies and their R&D projects is located in the appendix.

[116] 黄金 and 郭淞冰, "以网安基地为引领，临空港五大产业蓄势腾飞"; CSET original translation of "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office" [现代服务产业建设管理办公室 2019 年工作总结及 2020 年计划].

[117] 李墨, "360'第二总部'落子武汉 在光谷设研发运营中心."

[118] Kania and Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy."

[119] Jiang Jie, "China Unveils Its First Civil-Military Cybersecurity Innovation Center," *People's Daily Online*, December 28, 2017, https://perma.cc/R8QB-VK4J.

[120] Office of the Central Cyberspace Affairs Commission, "360：自觉担当责任维护网络安全," Cyberspace Commission of China, November 6, 2018, https://perma.cc/ENA2-WZ3F.

[121] (originally 发布中心, also referred to as 展示中心)

[122] City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计."

[123] China Information Security Certification Center, "Development and Prospect of China's Information Security Certification Scheme," September 10, 2017, https://perma.cc/S3JY-LGNX?type=image.

[124] National Institute of Standards and Technology, "National Voluntary Conformity Assessment Systems Evaluation (NVCASE)," U.S. Department of Commerce, May 3, 2021, https://www.nist.gov/nvcase; FedRAMP, "3PAO Obligations and Performance Standards," Version 3.1, GSA, May 18, 2021, https://www.fedramp.gov/assets/resources/documents/3PAO_Obligations_and_Performance_Guide.pdf.

[125] The Center will help carry out examinations under new regulations for reviewing software and services deemed critical to national security, introduced in early 2020. Zhuang Rongwen (庄荣文), director of the Cyberspace Administration of China (CAC, 国家互联网信息办公室, 网信办), He Lifeng (何立峰), director of the National Development and Reform Commission (NDRC, 和改革委员会国家发展, 发改委), Minister of Industry and Information Security (MIIT et al., "网络安全审查办法," China Cybersecurity Review Technology and Certification Center (中国网络安全审查技术与认证中心), May 11, 2020, https://perma.cc/S6A3-257H; 中金数据(武汉)超算技术有限公司, "网安基地," Wuhan Supercomputing Center, accessed June 2, 2021, https://web.archive.org/web/20201206094001/http:/www.centrincloud.com/wuhan/03.html; 胡曙光, "Spur Breakthrough Development of the Cybersecurity

Industry by Building a National Cybersecurity Port, 突破性发展网络安全产业 建设国家网络安全港," *Hubei Zhengxie* (*湖北政协*), March 21–22.

[126] 中金数据(武汉)超算技术有限公司, "网安基地"; 胡曙光. "突破性发展网络安全产业 建设国家网络安全港." *湖北政协* 3 (2019): 21-22, CNKI:SUN:SJXT.0.2019-03-011 (This source uses an incorrect name for CNITSEC, uses 国家网络安全测试中心, a name not used in any other document and unconnected to any other organization); General Office (办公厅) of the Wuhan City People's Government. 2017. "Notice of the [Wuhan] City People's Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base"; City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计"; "Industry Trends," *China Information Security* 8 (2017): 24-25, CNKI:SUN:CINS.0.2017-08-015.

[127] City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计."

[128] Mattis and Brazil, *Chinese Communist Espionage: An Intelligence Primer*.

[129] INSIKT GROUP, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," Recorded Future, May 17, 2017, https://perma.cc/UD5K-FQL7.

[130] 吉家网武汉新房, "【奥山汉口澎湃城：千亿大道上的天生野心家，住宅 8 月首开在即！】武汉吉家网," JJW, August 2, 2019, https://perma.cc/8WMW-QPGG?type=image.

[131] 武汉市互联网信息办公室, "国家网络安全人才与创新基地六大重点项目正式开工建设."

[132] http://www.hubei.gov.cn/zwgk/rdgz/rdgzqb/201907/t20190719_1403117.shtml, source was deleted before successfully archived.

[133] http://www.hubei.gov.cn/zwgk/rdgz/rdgzqb/201907/t20190719_1403117.shtml, source was deleted before successfully archived; 中国日报网, "奇安信华中总部将落户武汉国家网安基地," Baidu, July 22, 2019, https://perma.cc/87XX-3FE8?type=image; 佚名, "恒安嘉新落户武汉国家网安基地，将建立'国嘉网信研发运营中心,'" *环球财富网*, accessed June 2, 2021, https://perma.cc/L28T-QM4F?type=image; 新华网, "2020'黄鹤杯'网络安全人才与创新峰会在武汉召开," *新华网*, accessed June 2, 2021, https://perma.cc/5JLD-XM5F?type=image; "国家网络安全人才与创新基地基本概况," Huazhong University of Science and Technology, School of Cyber Science and Engineering.

[134] 武汉市互联网信息办公室, "武汉市互联网信息办公室 2019 年部门预算," accessed June 2, 2021, https://perma.cc/GT7V-QFMV.

[135] 中国网络安全审查技术与认证中心, "2019'黄鹤杯'网络安全人才与创新峰会暨网络安全服务与创新能力大赛圆满结束," September 20, 2019, https://perma.cc/57J5-NZLT?type=image.

[136] 华中科技大学网络空间安全学院, "国家网络安全人才与创新基地基本概况," 网络空间安全学院, August 2019, https://perma.cc/78U8-6M49?type=image.

[137] City of Wuhan Land Use and Urban Space Planning Research Center, "国家网络安全人才与创新基地规划方案设计."

[138] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation"; "See How RTP Moves North Carolina Forward," Research Triangle Park, accessed June 2, 2021, https://perma.cc/BGM8-29U4.

[139] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[140] U.S. Census Bureau, "QuickFacts: San Francisco County, California," U.S. Department of Commerce, accessed June 2, 2021, https://www.census.gov/quickfacts/fact/table/sanfranciscocountycalifornia/PST045219.

[141] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation"; "See How RTP Moves North Carolina Forward," Research Triangle Park.

[142] "Ease of Doing Business Index - China." The World Bank, accessed June 2, 2021, https://data.worldbank.org/indicator/IC.BUS.EASE.XQ?locations=CN.

[143] 石菲, "国家网络安全人才与创新基地落地武汉," *iChina* (*中国信息化*), *PRC Ministry of Industry and Information Technology* (*MIIT*; *工业和信息化部*), December 10, 2016.

[144] 武汉新闻广播, "谁是武汉'最强大脑'?" *Sohu*, December 11, 2018, https://perma.cc/WD2E-GG94.

[145] 武汉市互联网信息办公室, "国家网络安全人才与创新基地先导项目武汉超算暨云计算中心落成启用," December 14, 2016, https://perma.cc/2CW3-WW4G; 中金数据集团有限公司, "武汉超算暨云计算(数据)中心," accessed June 2, 2021, https://perma.cc/N27Y-PYLQ?type=image; 石菲, "国家网络安全人才与创新基地落地武汉."

[146] 武汉市互联网信息办公室, "国家网络安全人才与创新基地先导项目武汉超算暨云计算中心落成启用"; 石菲, "国家网络安全人才与创新基地落地武汉."

[147] 中金数据集团有限公司, "武汉超算暨云计算(数据)中心."

[148] 石菲, “国家网络安全人才与创新基地落地武汉.”

[149] “AWS Snowmobile,” Amazon Web Services, accessed June 1, 2021, https://aws.amazon.com/snowmobile/; “AWS Snowmobile Pricing,” Amazon Web Services, accessed June 1, 2021, https://aws.amazon.com/snowmobile/pricing/.

[150] 中金数据集团有限公司, “中金武汉数谷大数据中心 Pg. 2,” accessed June 2, 2021, https://perma.cc/3BGL-WNY2?type=image.

[151] 中金数据集团有限公司, “中金武汉数谷大数据中心 Pg. 2”; 武汉市互联网信息办公室, “国家网络安全人才与创新基地先导项目武汉超算暨云计算中心落成启用.”

[152] Data Valley will house 40,000 server racks (机架) containing more than 300,000 servers. 中金数据集团有限公司, “中金武汉数谷大数据中心 Pg. 2”; 中金数据集团有限公司, “武汉数谷大数据中心,” accessed June 2, 2021, https://perma.cc/4559-UAB8?type=image.

[153] This is a rough approximation based on information from the following sources: Pierr Johnson, “With The Public Clouds Of Amazon, Microsoft And Google, Big Data Is The Proverbial Big Deal,” *Forbes*, June 15, 2017, https://www.forbes.com/sites/johnsonpierr/2017/06/15/with-the-public-clouds-of-amazon-microsoft-and-google-big-data-is-the-proverbial-big-deal/?sh=72ad02522ac3; Mike Allen, “And The Title of The Largest Data Center in the World and Largest Data Center in US Goes To..,” DataCenters, June 14, 2018, https://www.datacenters.com/news/and-the-title-of-the-largest-data-center-in-the-world-and-largest-data-center-in#qualification; “Global Infrastructure,” Amazon Web Services, accessed June 10, 2021, https://aws.amazon.com/about-aws/global-infrastructure/; Raj Bala et al., “Magic Quadrant for Cloud Infrastructure and Platform Services,” Gartner, September 1, 2020, https://www.gartner.com/doc/reprints?id=1-242R58F3&ct=200902&st=sb.

[154] 武汉市互联网信息办公室, “国家网络安全人才与创新基地先导项目武汉超算暨云计算中心落成启用.”

[155] 中金数据集团有限公司, “中金武汉数谷大数据中心 Pg. 2.”

[156] “TOP500 Super Computer List,” TOP500, November 2020, https://perma.cc/9FFV-AP3Q.

[157] GPT-3’s 175B parameter model utilized 3,640 days of petaflop/s computational power. Tom B. Brown et al., “Language Models Are Few-Shot Learners,” *arXiv [cs.CL]* (May 28, 2020), arXiv, http://arxiv.org/abs/2005.14165.

[158] A 32-pod slice of the Cloud TPU v2 Pod provides 5,760 Teraflops, or 5.76 petaflops, for $24 an hour without a signed contract. Prices decrease with longer

contract periods. See “Cloud TPU – Pricing,” Google Cloud, https://cloud.google.com/tpu#tab1.

[159] 中金数据集团有限公司, “武汉数谷大数据中心.”

[160] General Office (办公厅) of the Wuhan City People’s Government, “Notice of the [Wuhan] City People’s Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base.”

[161] 湖北日报, “国家网络安全基地孵化器在汉奠基 该项目有望在 2020 年建成,” 湖北省人民政府门户网站, September 16, 2018, https://perma.cc/7JUT-GE9U?type=image; 武汉市互联网信息办公室, “国家网络安全人才与创新基地六大重点项目正式开工建设.”

[162] 湖北日报, “国家网络安全基地孵化器在汉奠基 该项目有望在 2020 年建成”; 武汉市互联网信息办公室, “国家网络安全人才与创新基地六大重点项目正式开工建设.”

[163] 湖北日报, “国家网络安全基地孵化器在汉奠基 该项目有望在 2020 年建成.”

[164] 湖北日报, “国家网络安全基地孵化器在汉奠基 该项目有望在 2020 年建成.”

[165] 湖北日报, “国家网络安全基地孵化器在汉奠基 该项目有望在 2020 年建成”; “国家网络安全基地孵化器 B 地块施工中标公告,” 湖北招标信息网, April 1, 2019, https://perma.cc/MPK7-EP4Y?type=image.

[166] 湖北日报, “国家网络安全基地孵化器在汉奠基 该项目有望在 2020 年建成.”

[167] 湖北日报, “国家网络安全基地孵化器在汉奠基 该项目有望在 2020 年建成”; 武汉市互联网信息办公室, “国家网络安全人才与创新基地六大重点项目正式开工建设.”

[168] 北京云峰数展, “【案例回顾】启迪网安基地孵化器企业展厅设计施工一体化_项目,” *Sohu*, February 7, 2020, https://perma.cc/B2U2-V8NW?type=image.

[169] Translator's note: The Chinese term 社会资本, translated literally as “social capital,” and its synonym 社会资金 “social funding,” refer to any source of funding outside of government budget outlays. These terms encompass investment by private individuals and private institutions. However, investment from state-funded entities such as state-owned enterprises (SOEs), including state-run banks, also falls under the umbrella of "social capital" or "social funding."

[170] General Office (办公厅) of the Wuhan City People’s Government, “Notice of the [Wuhan] City People’s Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base.”

[171] General Office (办公厅) of the Wuhan City People's Government, "Notice of the [Wuhan] City People's Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base."

[172] Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, December 23, 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

[173] Translation by Ben Murphy, Wuhan City Cyberspace Administration, "The 'Wuhan Model' of Cybersecurity Talent Cultivation."

[174] 黄金 and 郭淞冰, "以网安基地为引领，临空港五大产业蓄势腾飞," 武汉临空港报, September 19, 2020, https://perma.cc/NFM6-HAPE?type=image.

[175] Kania and Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy."

[176] 李墨, "360'第二总部'落子武汉 在光谷设研发运营中心."

[177] Sophie Mao, "What Does Registered Capital Mean?," China Law Help, June 1, 2019, https://perma.cc/UNW6-ERTA.

[178] 市政府督查室, "全年完成情况- 2019 年工作报告执行情况," 武汉市人民政府门户网站, April 1, 2020, https://perma.cc/6WBC-5A2U.

[179] 市政府督查室, "全年完成情况- 2019 年工作报告执行情况."

[180] Remco Zwetsloot, Helen Toner, and Jeffrey Ding, "Beyond the AI Arms Race," *Foreign Affairs*, November 16, 2018, https://www.foreignaffairs.com/reviews/review-essay/2018-11-16/beyond-ai-arms-race.

[181] People's Government of Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office."

[182] 陈先发 et al., "六个百亿级项目坍塌 '中国芯'遭遇烂尾潮," 瞭望, September 30, 2020, https://finance.sina.cn/chanjing/gdxw/2020-09-30/detail-iivhvpwy9799323.d.html?cre=tianyi&mod=wpage&loc=6&r=0&rfunc=51&tj=cxvideo_wpage&tr=214. Thanks to Jeffrey Ding's ChinAI translation of this piece.

[183] China Money AI, "Beijing Calls for 'Orderly Development' after Implosion of Six Massive Chip Projects," China Money Network, October 21, 2020, https://www.chinamoneynetwork.com/2020/10/21/beijing-calls-for-orderly-development-after-implosion-of-six-massive-chip-projects/amp; Han Wei, "Four Things to Know About China's $18.5 Billion Failed Chip Champ," *Caixin*, March 2, 2021, https://www.caixinglobal.com/2021-03-02/four-things-to-know-about-chinas-185-billion-failed-chip-champ-101668910.html; Taiwan News

Staff Writer, “China Gives up Ambitious $20 Billion Semiconductor Investment Project,” *Taiwan News*, February 28, 2021, https://www.taiwannews.com.tw/en/news/4138523.

[184] Original CSET Translation of "Research Report on the Status of China's Information Security Professionals (2018-2019)" [中国信息安全从业人员现状调研报告（2018-2019 年度）].

[185] General Office (办公厅) of the Wuhan City People’s Government, “Notice of the [Wuhan] City People’s Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base.”

[186] General Office (办公厅) of the Wuhan City People’s Government, “Notice of the [Wuhan] City People’s Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base.”

[187] General Office (办公厅) of the Wuhan City People’s Government, “Notice of the [Wuhan] City People’s Government on Certain Policies to Support the Development of the National Cybersecurity Talent and Innovation Base.”

[188] 李墨, “360‘第二总部’落子武汉 在光谷设研发运营中心.”

[189] Patrick Howell O’Neill, “How China Turned a Prize-Winning iPhone Hack against the Uyghurs,” *MIT Technology Review*, May 6, 2021, https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/; People’s Government of Dongxihu District in Wuhan City, “2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office.”

[190] People’s Government of Dongxihu District in Wuhan City, “2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office”; “US Embassy Cables: China Uses Access to Microsoft Source Code to Help Plot Cyber Warfare, US Fears,” *The Guardian*; Edward Wong, “Hackers Find China Is Land of Opportunity,” *The New York Times*, May 22, 2013, https://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html.

[191] Paco Zheng, “China AI Unicon at WAIC: Deepblue Technology- a Commercial Case That China AI Is Rising,” *Gizmodo*, September 4, 2019, https://perma.cc/RR6F-2JR9; AI 产业研究中心, “如何看待武汉大学国家网络安全学院引入深兰科技 AI 技术?,” 知乎, accessed June 1, 2021, https://perma.cc/4SFK-WRBK?type=image.

[192] People’s Government of Dongxihu District in Wuhan City, “2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office.”

[193] 爱企查, "深兰网安科技(武汉)有限公司," accessed June 1, 2021, https://perma.cc/E35K-B9HG.

[194] "华科网安基地女生宿舍的日常（十）——夜游归来," *我要发大财财*, October 10, 2020, https://www.bilibili.com/video/BV1Fp4y1k7E7.

[195] "Vlog#1 搬新校区 | 国家网安基地 | 宿舍 | 校园初探 | Day1," 机智的王小鹏, August 31, 2020, https://www.bilibili.com/video/BV1yV41127ag?from=search&seid=4647657823770949479.

[196] 新华网, "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," July 12, 2017, https://perma.cc/E352-K9A8.

[197] 新华网, "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."

[198] 爱企查, "湖北航天信息技术有限公司," accessed June 1, 2021, https://perma.cc/3PMS-XMJN.

[199] "国家网络安全人才与创新基地基本概况," Huazhong University of Science and Technology, School of Cyber Science and Engineering; 新华财经, "航天科工 6 款智慧产业产品亮相 2020 智慧产业高峰论坛," 中国航天科工二院, November 3, 2021, https://perma.cc/LT3B-MCFM?type=image.

[200] U.S. Bureau of Industry and Security, *Supplement No. 4 to Part 744 - ENTITY LIST* (Washington, DC: U.S. Department of Commerce, April 8, 2021), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file.

[201] 中国航天科工, "智能协同云技术与产业发展高峰论坛在鄂召开 重磅发布航天智云 3.0," 中国航天科工集团有限公司, December 14, 2020, https://perma.cc/94UU-7MMB?type=image.

[202] SASTIND is the key nexus between the PLA and China's defense industrial sector.

[203] 中共中央网络安全和信息化领导小组办公室, "国家网络安全人才与创新基地吸引众多知名企业," September 19, 2016, https://perma.cc/N98W-5VWU?type=image.

[204] 中国航天科工, "智能协同云技术与产业发展高峰论坛在鄂召开 重磅发布航天智云 3.0."

[205] 武汉市互联网信息办公室, "国家网络安全人才与创新基地先导项目武汉超算暨云计算中心落成启用."

[206] People's Government of Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office."

[207] People's Government of Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office."

[208] Translation by Jeff Ding, Wu Xi, "后浪可畏：云从科技获国家基金 18 亿元融资，距 A 股上市仅剩临门一脚] [Respect the Latecomer Wave: Cloudwalk receives 1.8 billion RMB in financing from national funds]," Synched, May 14, 2020, https://docs.google.com/document/d/1n07iJTVK_Hlhleztz4fuHBy2FX97nVXCoVqxiR_9FWQ/edit. This translation was brought to the authors' attention by CNAS' report on military-civil fusion (Kania and Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy.").

[209] "NIDS China Security Report 2021: China's Military Strategy in the New Era," 37.

[210] 搜狐湖北资讯, "中国武汉 Cyber Range 电子攻防实验室盛大开幕," Sohu, December 13, 2017, https://perma.cc/SXD6-F3YC?type=image.

[211] 搜狐湖北资讯, "中国武汉 Cyber Range 电子攻防实验室盛大开幕"; 中新社, "武汉建电子攻防实验室 助力网络安全人才培养," *中新网*, December 13, 2017, https://perma.cc/D2JS-BTMK; Jeff Reed (@jeffreed415), "@CiscoSecurity's CyberRange Lab is now open in China's Wuhan Cybersecurity Valley. From #innovation to sharing #threatintelligence, our goal is to provide #security solutions & #businessarchitecture integration for our global customers," Twitter, December 15, 2017, https://perma.cc/4QJA-225K?type=image; http://www.hubei.gov.cn/zwgk/rdgz/rdgzqb/201712/t20171218_1235491.shtml (page has been deleted and no archive exists).

[212] http://www.hubei.gov.cn/zwgk/rdgz/rdgzqb/201712/t20171218_1235491.shtml (page has been deleted and no archive exists).

[213] Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage."

[214] Office of the Central Cyberspace Affairs Commission, "《国家网络空间安全战略》全文," Office of Cyberspace Administration of China, December 27, 2016, https://web.archive.org/web/20200812173740/http%3A%2F%2Fwww.cac.gov.cn%2F2016-12%2F27%2Fc_1120195926.htm.

[215] 许雯, "对话国家网安基地办主任：网络安全人才要放到'战场'上培养."

[216] "国家网络安全人才与创新基地基本概况," Huazhong University of Science and Technology, School of Cyber Science and Engineering.

[217] 中国海洋大学, "中国海洋大学战队荣获 '黄鹤杯' RHG 机器人网络安全大赛季军," July 16, 2019, https://perma.cc/BG6R-FKMJ; 企鹅号 - 丁牛科技, "丁牛科技荣获"黄鹤杯"机器人网络安全大赛企业第一名，大赛第七名！," 腾讯云, September 21, 2019, https://perma.cc/3TSZ-W8VQ.

[218] People's Government of Dongxihu District in Wuhan City, "2019 Work Summary and 2020 Program for the Modern Service Industry Construction Management Office."

[219] "NIDS China Security Report 2021: China's Military Strategy in the New Era."