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" (杀手链)—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]

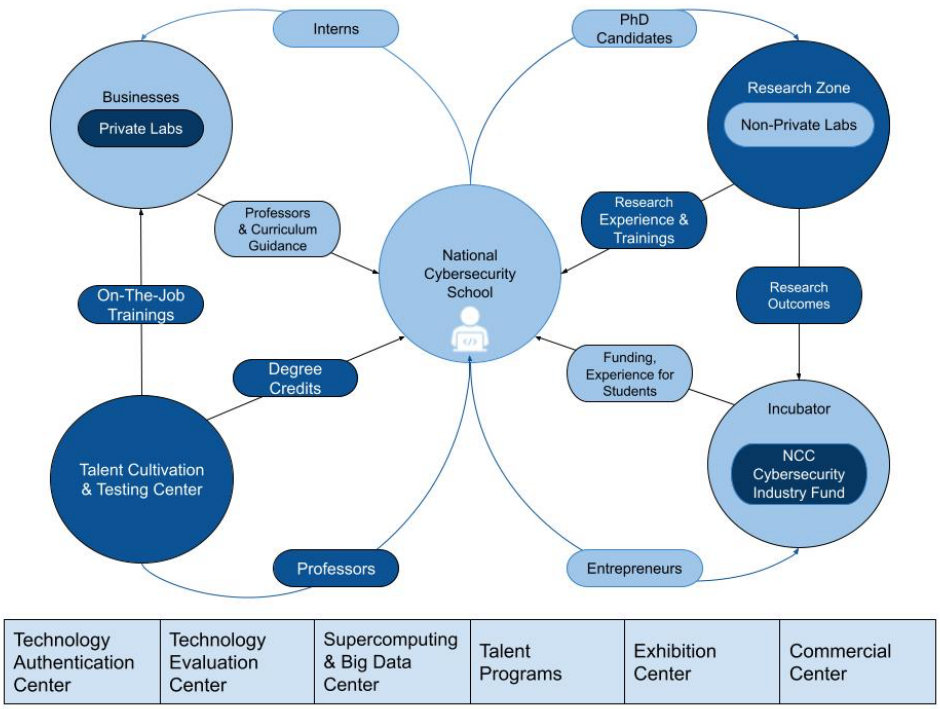
Third, China aims to reduce its reliance on foreign cyber technology.[9] The Snowden revelations reinforced PLA concerns that foreign technology facilitates espionage. Leaked documents revealed occasional close cooperation between the U.S. government and technology companies. The CCP wants indigenous 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.

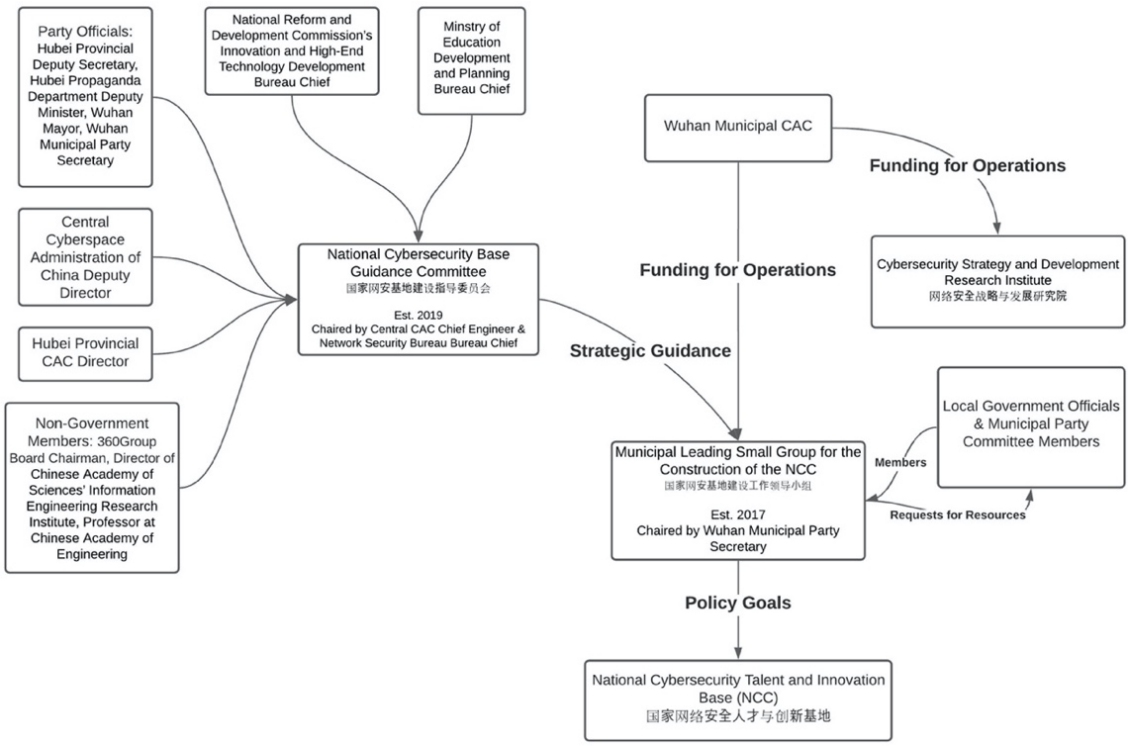
Governance Structure

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.