Evaluating China's Road to Cyber Super Power

The Chinese Communist Party's (CCP) 14th Five Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 unambiguously states the aspiration of maturing into a cyber superpower.[1] This paper examines recent publications to evaluate the CCP's path to reaching cyber superpower status. It asks where does China stand relative to the United States' cyber power in the short-, medium-, and long-term?

CCP elites emphasize the primacy of regime stability, and a yawning cyber security gap with the United States or other competitors sits uneasily with CCP leadership and the People's Liberation Army (PLA). In the near-term of the next five to ten years, the United States will likely retain its position of preeminence in cyber power. Investment, structural reform, elevating cyber in policy and strategy documents, and domestic demand will propel China to a peer competitor status in the long-term. As of now, Chinese cyber power should not be exaggerated even if popular perception may assume China already is a cyber superpower.

Headlines carry the potential of inflating China's cyber capacity, perhaps to Beijing's delight. The institution of a free press in the United States opens numerous channels for unclassified leaking of information as well as publication of breaches. One could survey the large number of stories in print media, podcasts, or blogs that chronicle an aggressive cyber assault on the United States by Chinese advanced persistent threat (APT) actors and conclude that China's cyber power towers above a beleaguered, inferior United States.

A Chinese cyber leviathan figures large in Elliot Ackerman and James Stavridis' book *2034: A Novel of the Next World War*. The authors imagine a scene in the White House situation room where the gravity of China's cyber intrusion punctures the balloon of impregnability. In the onset of a crisis, and the book, Chinese defense attaché Lin Bao flexes Chinese cyber muscle for bewildered National Security Council officials Chowdhury and Hendrickson.

> Then Lin Bao's exasperated voice: "We do have a counterproposal….."
> "Good," interjected Chowdhury, but Lin Bao ignored him, continuing on.
> "If you check, you'll see that it's been sent to your computer—"
> Then the power went out. It was only a moment, a flash of darkness. The lights immediately came back on. And when they did, Lin Bao wasn't on the line anymore. There was only an empty dial tone. Chowdhury began messing with the phone, struggling to get the White House operator on the line, while Hendrickson attempted to log back on to his computer.
> "What's the matter?" asked Chowdhury.
> "My log-in and password didn't work"
> Chowdhury pushed Hendrickson aside. His didn't work either.[2]

[1] Ben Murphy, editor, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," Georgetown Center for Security and Emerging Technology (translated May 12, 2021). https://cset.georgetown.edu/publication/china-14th-five-year-plan/. A detailed explanation of the translation of "cyber superpower" can be found here: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/.

[2] Elliot Ackerman and James Stavridis, *2034: A Novel of the Next World War* (New York: Penguin Press, 2021), 40.

The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense, Lawrence Livermore National Laboratory, or the US Government.

Chowdhury and Hendrickson stammer in formulating a coordinated response under the weight of a nearly decapitating Chinese cyber attack, and *2034* unfolds with the premise of China's near-cyber hegemony. Although impossible to gauge, it raises the question of potential accuracy. Could life imitate fiction?

The near- and medium-term ability of China to deploy cyber weapons for a strategic effect on the national security apparatus appears unlikely based on open-source analysis. Chinese APTs developed a talent for pilfering intellectual property, cyber espionage, and culpability for marquee intrusions such as the 2016 mass exfiltration of data from the Office of Personnel Management (OPM) or the 2021 Microsoft Exchange server breach. As of mid-2021, Chinese APTs do not appear to parallel Russian APTs' sophistication in using cyber for myriad purposes, nor do threat intelligence firms link Chinese APTs to cyber attacks such as NotPetya. Although China has used Taiwan as a test bed for information and cyber attacks, it is unclear if these intrusions culminated in China inflicting measurable damage in Taiwan.

Cyber power indices stand apart from popular or fictional perception of relative cyber power. The 2021 International Institute for Strategic Studies' (IISS) "Cyber Capabilities and National Power: A Net Assessment" and the 2020 Harvard Kennedy School Belfer Center's "National Cyber Power Index 2020" place the United States atop a list comparing whole of nation-state cyber capabilities.[3] Both indices place China in the second tier but closing fast. The qualitative appraisals find that China's numerous deficiencies prevent it from competing on a peer status with the United States. Innovation, however, may position China to compress the time required to sit equally in terms of cyber power.

The world sits at the precipice of what may register as one of the most profound periods of technological innovation since the industrial revolution. Converging emerging technologies carry the potential to speedily disrupt the present order, and cybersecurity is one among many sectors that could be revolutionized. Advances in artificial intelligence (AI), quantum computing, and 5G connectivity could quickly erase the United States' advanced status in cybersecurity by altering the cyber offense and defense threat landscape in the coming years.[4] Integrating private sector cybersecurity and AI technologies—where the heart of innovation lies—with the United States government will be crucial for retaining a competitive national security advantage with China. The CCP is investing heavily in AI, and AI's multiplying effects for cybersecurity could drastically erode the time China needs to reach its stated goal of reaching cyber superpower status.

[3] International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment" (June 2021). https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power; Julia Voo, Irfan Hermani, Simon Jones, Winnona DeSombre, Dan Cassidy, Anina Schwarzenbach, "National Cyber Power Index 2020" (September 2020), Harvard Kennedy School Belfer Center. https://www.belfercenter.org/publication/national-cyber-power-index-2020

[4] For a sober analysis of the benefit for cyber offense and defense, see Micah Musser and Ashton Garriot, "Machine Learning and Cybersecurity Hype and Reality," Georgetown Center for Security and Emerging Technology (June 2021). https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity/

Definitions, Sources, and Methodology

For the purposes of this report, cyber power is defined capaciously to encompass institutional capabilities, human capital, and private sector capacity, ideally to repel attacks and develop the indigenous talent and software to prevent an adversary's cyber predations across society. This document is not an authoritative analytical product on the entirety of Chinese cyber power—such a net assessment would likely be an exercise in futility. Rather, it seeks to illuminate the current state of Chinese cyber capabilities with a sober accounting of open-source data. As such, the materials consulted for this report rely on recent publications and not a historic dive into doctrine, workforce development, a chronology of cyber campaigns, or technological gain.

This report examines open source, non-classified qualitative analysis to evaluate China's current cyber maturity. Evidence for this document draws on materials from academia, private cybersecurity companies, and national security research institutions. Private sector threat intelligence firms produce high quality analysis on Chinese APTs tactics, techniques, and procedures (TTPs), and investigation from companies such as FireEye illuminate China's ability to wield cyber means for its security ends. None of the materials cited in this assessment originate from classified United States or foreign government sources. Any references to United States government sources are sourced entirely to unclassified information.

On the Road to A Cyber Superpower

For understanding China's contemporary vision of national security and cybersecurity, 2015 stands as a pivotal year for institutional reforms within the PLA that heralded a new era of cyber sophistication. Xi Jinping announced reforms in 2015 and 2016 to reorganize the services for joint operations alongside a heavy blanket of CCP oversight to guarantee the military's subservience to the party. The PLA reorganized commands and its bureaucratic structure, forming a new institution to handle conceptual domains like cyber. The 2015 "China's Military Strategy" White Paper dubbed cyber as one of the "'new commanding heights in strategic competition'" and declared that the CCP would establish a cyber force. Sweeping reforms to China's services in 2015 and 2016 birthed the Strategic Support Force (SSF). [5]

The SSF consolidated disparate cyber offices or functions within the PLA and housed them under one roof for offensive and defensive cyber operations and intellectual property (IP) theft. SSF cyber units are tasked with preparing the battlefield of the future to use offensive cyber attacks to degrade adversary command and control, communication, intelligence collecting, and decision making. One of the SSF's primary objectives entails disrupting information and leveraging it to overwhelm an adversary early in the conflict to support the doctrine of informatized warfare. Since its founding, the SSF continues to support the services and integrate cyber effects in exercises, war games, and planning. Statements by Xi in 2019 signaled a shift away from informatized warfare to intelligentized war that will feature the

[5] Caitlin Campbell, "China's Military: The People's Liberation Army (PLA)," Congressional Research Service (June 4, 2021), 10, 24. https://crsreports.congress.gov/product/pdf/R/R46808

merging of cyber with cognitive domains driven by AI. All told, in the PLA, the advancements are impressive but are equally matched by the Chinese Ministry of State Security (MSS).[6]

Responsibility for the marquee intrusions in recent history can be traced to the MSS, such as the OPM hack, and the trajectory for advancements in cyber capabilities points upward. The MSS manages China's domestic surveillance but also empowers its hackers and contractors to launch offensive cyber campaigns to exfiltrate data from foreign actors. A July 2021 Department of Justice indictment documented the MSS officers' TTPs who committed global economic espionage targeting an array of companies, governments, and universities.[7] The Biden administration along with allies attributed blame to the MSS for the destructive Microsoft Exchange Server hack that capitalized on a previously unknown vulnerability, known as a zero day, to steal data and leave back door access points for future access.[8] MSS hackers' growth beginning with the OPM intrusion until 2021 evidenced impressive development of TTPs. Operating separately from the SSF, MSS invested in its human capital alongside improved malware quality for cyber espionage. MSS hired hackers as contractors to circumvent talent shortages, and has proven agile in its ever-growing brazen campaigns in spite of China's growing vulnerabilities.[9]

The digitization of China's economy over the past decade forced the CCP to adopt a new and active posture in cyberspace for intelligence collection, domestic surveillance, and security. China's 2017 Cybersecurity Law of the People's Republic of China erected the legal scaffolding to codify the party's vision of cyber sovereignty.[10] The elastic Cybersecurity Law creates numerous opportunities for the party to access data. Under military-civil fusion and the 2017 law, Chinese telecommunication and technology companies must submit data to the government in addition to sharing cybersecurity technology.[11] The CCP links cybersecurity and 5G connectivity—likely born from the party's domestic surveillance needs. Meanwhile, the government promotes telecommunication companies such as Huawei to developing and advanced countries that opens a host of cyber and data vulnerabilities. 5G sales generate revenue for domestic champions while also broadening the reach of the CCP's access to foreign networks. The authors of a 2021 Brookings report write "Beijing intentionally dilutes discussions

[6] "'Intelligentization' and a Chinese Vision of Future War," Mad Scientist Blog (December 19, 2019). https://madsciblog.tradoc.army.mil/199-intelligentization-and-a-chinese-vision-of-future-war/

[7] Department of Justice Office of Public Affairs, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

[8] The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

[9] "China's Cyber Power in a New Era" in *Asia-Pacific Regional Security Assessment 2021: Key Developments and Trends*," The International Institute for Strategic Studies, editor (May 2019). https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

[10] A full translation is available here: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[11] Lauren Maranto, "Who Benefits from China's Cybersecurity Laws?," Center for Strategic & International Studies New Perspectives on Asia Blog (June 25, 2020). https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws

of its ambitions in order to not alarm foreign audiences." Concealing aims serves the party's domestic and foreign progress to prepare for a future of cyber war or sustained cyber competition with indigenous expertise to establish cyber autonomy.[12]

In 2021 to facilitate the cyber superpower ambition, China's National Cybersecurity Center (NCC) matriculated its first class of approximately 1,500 cybersecurity graduates to anticipate a new era of indigenous talent and cybersecurity software innovation. The CCP ordered the opening of the Wuhan-based institute to remedy domestic cyber expertise shortfalls. Students receive generous compensation packages to attend the institute, and it is envisioned to fill a pipeline for China's public and private sectors. In the short-term, annual graduates will total to 2,500. The NCC will operate as an incubator for China's cybersecurity sector where students, graduates, and instructors flow in and out of government under military-civil fusion. The hub is intended to materialize the CCP's security dreams—producing a new generation of cyber leaders to serve as the vanguard of a cyber superpower that can compete against the United States.[13]

Chinese Perception of Cyber Competition & Cooperation with the United States

The United States sits atop China's list cyber adversaries where they could seek to compete but also cooperate with Washington. This report turns to recent writings to comprehend thought leaders' analysis or Chinese nationals who speak with audiences in the United States. Future translation projects will likely improve the speed and number of Chinese writings in English on cybersecurity and cyber competition.

China is susceptible to attacks on its prestige that are inflicted by adversaries who publicly name and shame China's bad cyber behavior. One Chinese expert, Lu Chuanying, castigated the United States and allies' public attribution of the Microsoft Exchange hack for damaging trust. Lu is a Fellow and Secretary-General of the Research Center for the International Governance of Cyberspace at the Shanghai Institutes of International Studies. Lu asserts that the attribution was made with no evidence and is associated with a number of hollow claims originating from Washington regarding China's malicious cyber behavior, espionage, and intellectual property theft. "'Unsupported accusations'," in his words, degrade trust when two sides should cooperate on data sharing to accurately attribute blame.[14]

One of the most authoritative voices for a policy audience on Chinese cyber thinking belongs to Lyu Jinghua. Lyu retired from the PLA in 2016 with the rank of colonel, and was a visiting scholar at the Carnegie Endowment for International Peace's Cyber Policy Initiative. Her 2021 contribution to the chapter "Strategic Stability in Cyberspace" in the United States Institute

[12] Rush Doshi, Emily De La Bruyère, Nathan Picarsic, John Ferguson, "China as a 'Great Cyber Power': Beijing's Two Voices in Telecommunications," Brookings Report (April 2021). https://www.brookings.edu/research/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/

[13] Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," Georgetown Center for Security and Emerging Technology, CSET Issue Brief (July 2021), 1-4, 12. https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/

[14] Amanda Kerrigan, "Views from the People's Republic of China on US-China Relations since the Beginning of the Biden Administration," CNA Information Memorandum (September 2021), 5. https://www.cna.org/CNA_files/PDF/Views-from-the-Peoples-Republic-of-China-on-US-China-Relations-since-the-Beginning-of-the-Biden-Administration.pdf

of Peace's *Enhancing U.S.-China Strategic Stability in an Era of Strategic Competition: U.S. and Chinese Perspectives* neatly explains the Chinese cyber perspective and directions for improvement. She identifies three challenges to cooperation: the difficulty of attribution, mistaken estimates of capabilities and intention, other states or non-state actors inflaming tensions by masquerading as either the United States or China. She goes on to summarize two interrelated risks impinging on strategic stability in the bilateral relationship. The first, digitization of nuclear command and control, presents an unclear future for the security of nuclear weapons. Second, there exists a high opportunity for spillover into kinetic or nuclear combat due to accidental penetration testing of nuclear systems.[15]

Lyu's steps to build stability concentrate on establishing trust. "Mutual suspicion," she writes, imperils the bilateral relationship and facilitates deterioration of the cyber domain. In the event of crisis, offensive operations in cyberspace may deteriorate further, and she argues for discussions on crisis management to preserve communication to ward off a cyber spiral that could bleed into a kinetic attack. Joint restraint in probing nuclear systems or civilian critical infrastructure is another avenue for stability. She closes her confidence building recommendations by imploring both parties to cooperate on norms to prevent cyber escalation.[16]

Speedbumps on the Road to Cyber Superpower Status

Achieving cyber superpower status in the near- and medium-term will prove challenging based on prevailing trends. The CCP faces several obstacles in attaining cyber superpower status, both unique and common among contemporary nation-states. China's domestic workforce falls far short of projected need for its dream of cyber autonomy in and outside the government. Bureaucratic overlap may further hinder synergies that one might expect from an authoritarian state. In addition to the human and bureaucratic elements, vulnerabilities lurk throughout China's internet architecture with technology sourced to the United States.

Earlier this year, China's inaugural class of 1,500 cybersecurity experts matriculated from the Wuhan-based National Cyber Center (NCC). The NCC shows promise for establishing an incubator to offset indigenous talent and technology deficiencies. Nevertheless, 2,500 graduates from NCC are a fraction of necessary professionals to fuel innovation. The Japanese National Institute for Defense Studies' 2021 *China Security Report* notes that 15,000 Chinese cyber experts enter the labor force annually. To keep pace with demand, the report authors assess, 700,000-1.4 million cyber experts would need to join China's labor pool.[17] 95 percent of cybersecurity openings go unfilled every year.[18] In other words, China's human capital gap is vast, and driving innovation will prove challenging.

[15] Lyu Jinghua, "Chinese Perspective," in *Enhancing U.S.-China Strategic Stability in an Era of Strategic Competition: U.S. and Chinese Perspectives*, edited by Patricia M. Kim, United States Institute of Peace (April 2021), 40-42. https://www.usip.org/publications/2021/04/enhancing-us-china-strategic-stability-era-strategic-competition

[16] Lyu, *Enhancing U.S.-China Strategic Stability*, 42, 43.

[17] National Institute for Defense Studies, *NIDS China Security Report 2021: China's Military Strategy in a New Era* (Tokyo, Japan: National Institute for Defense Studies), 35.

[18] Cary, "China's National Cybersecurity Center," 6.

Poor impression of government work hamstrings recruitment efforts and adds a level of complexity to bureaucratic stove piping. Private sector employers pay better without the rigors of qualifying to work with the PLA or MSS. Disinterest in a military culture hampers the SSF's recruitment and compels the SSF as well as the MSS to compete with the private sector or hackers for a limited pool of civilian cyber experts. Bureaucratically, MSS and SSF lines of effort conflict without a clear coordination mechanism to reduce friction or consolidate cyber campaign objectives. The Ministry of Industry and Internet Technologies maintains a cyber arm, and instead of creating synergies it contributes to silos.[19]

The supply chain for China's information technologies runs through the United States and China's cyber defense private sector is weak. Without a core of indigenous software, SSF and MSS forces rely on core technologies without an indigenous technology base to replace operating systems and design architectures compatible with those developed in the United States. The CCP acknowledges these shortcomings and urges Tencent and other companies to grow into cyber national champions for Made in China 2025.[20] Domestic growth in China's defense-oriented cyber companies grew progressively in the past five years. Nevertheless, they are far behind IBM, Norton, MITRE, or FireEye in developing a national cyber defense industry. Growth has yet to keep pace with private sector demand or the CCP's intention of robust cyber defense with indigenous software.[21]

U.S. Government Assessment of China's Cyber Power

The unclassified *2021 Annual Threat Assessment of the U.S. Intelligence Community* published by the Office of the Director of National Intelligence describes China as a sophisticated cyber adversary, principally in the terrain of cyber espionage. Intelligence professionals "continue to assess that China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure in the United States." The cyber threat against the United States' homeland stands to grow as China augments its cyber arsenal alongside the "proliferation of related technologies." These technologies further the CCP's ambition to surveil perceived threats to regime stability abroad and at home. China's domestic surveillance apparatus employs cutting-edge cyber tools to monitor dissidents and prevent the free flow of information. Chinese cyber espionage targets communication and software firms to extend the ambit of its intelligence collection net.[22]

The Department of Defense's 2020 *Military and Security Developments Involving the People's Republic of China* delves into the PLA's outlook on cyber war. PLA theorists consider cyber as a tool to manage escalation, deter, and degrade an adversary's war-fighting capacity by utilizing cyber weapons or intelligence gleaned through espionage. "Disruptive and destructive effects" achieved through warning or limited cyberattacks can shape an adversary's strategic

[19] Lin, Ying-Yu, "PLA Cyber Operations: A New Type of Cross-Border Attack," in *The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context*, Joel Wuthnow, Arthur S. Ding, Phillip C. Saunders, Andrew Cobell, Andrew N. D. Yang, eds. (Washington, D.C.: National Defense University Press, 2021), 305, 306.
[20] National Institute for Defense Studies, *NIDS China Security Report 2021*, 37.
[21] Greg Austin, "The Strategic Implications of China's Weak Cyber Defenses," *Survival* 62, 5 (October-November 2020), 122.
[22] Office of the Director of National Intelligence, *2021 Annual Threat Assessment of the U.S. Intelligence Community* (April 2021), 8.

calculus during conflict escalation. The PLA theorists believe that cyber tools can inflict pain at a low cost to prevent the United States from striking China. Cyberattacks against command and control or logistic networks, Chinese writings suggest, provide the PLA with the potential to incapacitate the United States or others from launching attacks. By knocking an adversary out of a conflict early via cyber attacks, the PLA articulates a vision for achieving strategic superiority by controlling an adversary's decision-making early in escalation.[23]

Conclusion

In the short-term, China will not eclipse the United States as the world's premier cybersecurity nation-state. MSS officers will, however, target the United States' data for exfiltration, and SSF forces will map foreign states' networks to achieve a military advantage in the event of crisis. Achieving economic or diplomatic gain from cyber espionage is attractive to the CCP, and cyber espionage campaigns will only accelerate. The CCP will drive state and private sector investment to nurture an indigenous cybersecurity personnel and technology base. Regardless, China's overwhelming cyber shortcomings cast aside the misperception that the United States has fallen behind the CCP's cyber campaigns or demographic advantages. Beijing's cyber deficits cannot be overlooked—a fact apparent to CCP senior leadership—but competing with the United States would require a national overhaul for China and the United States surrendering on cybersecurity.

2034's authors employ fear of cyber inferiority to illustrate the peril of inaction for the United States' strategic competitiveness. In the intervening thirteen years between the present and the fictional year depicted in the book, the United States will retain its advantages over a China that struggles to meet its basic, national cybersecurity obligations. Although galloping innovation may reverse this condition, the United States can look to remain competitive if its domestic private and public sectors cooperate and integrate the technologies that will transform the cybersecurity that protects the nation's critical infrastructure.

The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, Inc. LLNL-TR-829221

[23] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress* (September 2020), 83.