

2018

China's Quantum Quandary

Elsa B. Kania

Center for a New American Security, EKania@cnas.org

Follow this and additional works at: <https://scholarcommons.usf.edu/mca>

Part of the [International Relations Commons](#)

Recommended Citation

Kania, Elsa B. (2018) "China's Quantum Quandary," *Military Cyber Affairs*: Vol. 3 : Iss. 2 , Article 10.

Available at: <https://scholarcommons.usf.edu/mca/vol3/iss2/10>

This Article is brought to you for free and open access by Scholar Commons. It has been accepted for inclusion in *Military Cyber Affairs* by an authorized editor of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

China's Quantum Quandary¹

Elsa B. Kania²

China aspires and possesses the potential to lead a new quantum revolution.³ Over more than a decade, Chinese researchers have demonstrated consistent advances in the research, development, and operationalization of a range of quantum technologies. China's launch of the world's first quantum satellite in August 2016 captured headlines, not only possessing great prestige but also representing an important experimental milestone that is now enabling practical progress.⁴ To date, China is at the forefront of implementing quantum key distribution (QKD), a technique to enable provably secure communication that involves a cryptographic protocol in which keys are exchanged in quantum states through entanglement.⁵ The Chinese government is investing in the continued construction of a national quantum communications infrastructure, which will integrate local networks and a national backbone of optical fibers with an expanding constellation of satellites to enable security and scalability.⁶ Already, these systems have started to be employed for military, government, and commercial applications.⁷ Joining in the global

¹ Please cite as: Kania, Elsa B., "China's Quantum Quandary," in Demchak, Chris C. and Benjamin Schechter, eds. *Military Cyber Affairs: Systemic Cyber Defense* 3, no. 2 (2019).

² Elsa Kania is an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security.

³ For the initially articulation of the concept of the "second quantum revolution," see: Jonathan P. Dowling and Gerard J. Milburn, "Quantum Technology: the Second Quantum Revolution," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 361 no. 1809 (2003), 1655-1674, <https://arxiv.org/pdf/quant-ph/0206091.pdf>.

⁴ In fact, there was a dedicated campaign of media and publicity or "propaganda" work (新闻宣传工作) undertaken at the time, with the guidance of the Central Propaganda Department News Bureau and the Strategic Support Force Political Work Department. These efforts were seen as successful in ensuring extensive coverage across a range of media, setting off a "quantum storm" (量子风暴). See: "Space Science Guiding Special Projects Communication Strategy Analysis" [空间科学先导专项传播策略分析],

<http://webcache.googleusercontent.com/search?q=cache:4cnBI74GPecJ:www.bsc.cas.cn/jlyd/ywyj/201706/P020170622527613667684.docx+&cd=1&hl=en&ct=clnk&gl=gr>.

⁵ For a useful explainer, see: Martin Giles, "Explainer: What is quantum communication?", *MIT Technology Review*, February 14, 2019, <https://www.technologyreview.com/s/612964/what-is-quantum-communications/>

⁶ For USTC's description of this backbone and their involvement in it, see: "Quantum communication backbone network (Beijing-Shanghai),"

<https://web.archive.org/web/20190311195803/http://quantum.ustc.edu.cn/web/en/node/350>.

⁷ For some of the latest updates on this program: "'Mozi' expected to continue working for over 2 years" ["墨子号"预计超期工作2年以上], *Xinhua*, February 15, 2019,

https://web.archive.org/web/20190311192343/http://www.xinhuanet.com/tech/2019-02/15/c_1124120351.htm

“race” to develop a quantum computer,⁸ Chinese scientists notably established a new world record through achieving entanglement among 18 qubits (i.e., ‘quantum bits’) in July 2018.⁹ In the future, quantum computing will introduce immensely powerful capabilities that could be leveraged for a range of impactful applications, including to break public key cryptography. At a time when international competition in quantum science and technology is intensifying, China’s advances and ambitions have often provoked concerns.¹⁰ Evidently, influenced by intense anxieties over cyber security and recognition of the potential strategic advantages, Chinese leaders prioritize this agenda for quantum innovation at the highest levels.

These aspirations for leadership in this new frontier of innovation indicate China’s continued trajectory towards becoming a true “science and technology superpower” (科技强国). In many respects, China’s recent progress in innovation has been uneven and seemingly contradictory. China has continued to struggle with catching up in a number of cases, from aeroengines to semiconductors.¹¹ At the same time, China is starting to emerge as a true leader in certain technologies, including artificial intelligence, which could enable disruptive capabilities in the cyber domain and beyond.¹² Under the 13th Five-Year Plan (2016-2020), China has launched a series of new ‘megaprojects,’ with quantum computing and communications among

⁸ As I have argued elsewhere, this competition to advance quantum computing is more of a marathon than a race, given the timeframes that are likely required: “China’s challenge to US quantum competitiveness,” *The Hill*, June 30, 2018, <https://thehill.com/opinion/technology/394894-the-chinese-challenge-to-us-quantum-competitiveness>

⁹ See: Wang, Xi-Lin, Yi-Han Luo, He-Liang Huang, Ming-Cheng Chen, Zu-En Su, Chang Liu, Chao Chen et al. “18-qubit entanglement with six photons’ three degrees of freedom,” *Physical Review Letters* 120, no. 26 (2018): 260502.

¹⁰ At the same time, the field does remain fairly open and collaborative in ways that advance global innovation. Nonetheless, the trend towards increased competition among key companies and countries is undeniable. For instance, in the United States, concerns over China’s quantum ambitions contributed to the decision by the U.S. Congress to pass the National Quantum Initiative Act in December 2018, which will launch a new ten-year plan and provide at least \$1.2 billion in funding for future research. See: “H.R.6227 - National Quantum Initiative Act,” 115th Congress (2017-2018), <https://www.congress.gov/bill/115th-congress/house-bill/6227>

¹¹ For an academic assessment of the challenges of catching up, particularly in contemporary technologies of greater complexity, see: Andrea Gilli and Mauro Gilli, “Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage,” *International Security* 43, no. 3 (2019): 141-189.

¹² For a more detailed evaluation of these trends, see: Elsa B. Kania, “Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power,” Center for a New American Security, 2017, <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.

them,¹³ aiming for major advances by 2030.¹⁴ This state-driven approach to innovation often involves the mobilization of talent and massive amounts of resources.¹⁵ Increasingly, there are also active efforts from dynamic technology companies, particularly Baidu and Alibaba, that are pursuing their own extensive investments in this field.¹⁶ For instance, Alibaba became the second company after IBM to launch an 11-qubit quantum computing cloud service, in partnership with the Chinese Academy of Sciences in February 2018,¹⁷ and Baidu has entered the race with the launch of its Institute for Quantum Computing in March 2018.¹⁸ China is seeking to progress beyond the imitation and absorption of foreign technologies to pursue truly original innovation,¹⁹ including through increased investments in basic research,²⁰ while continuing to leverage international technologies and collaborations in the meantime.²¹ It is too soon to evaluate the

¹³ “Notice of the State Council on the Printing and Distribution of the “Thirteenth Five-Year” National Science and Technology Innovation Plan” [国务院关于印发“十三五”国家科技创新规划的通知], State Council, August 8, 2016, http://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm.

¹⁴ “China’s “Science and Technology Innovation 2030 Megaprojects Will Newly Add “Artificial Intelligence 2.0”” [中国“科技创新 2030—重大项目”将新增“人工智能 2.0”], Ministry of Science and Technology of the People’s Republic of China, February 16, 2017, https://web.archive.org/save/http://www.most.gov.cn/ztlz/lhzt/lhzt2017/hkjlhzt2017/hkj_fbh02/201702/t20170228_131502.htm

¹⁵ This concept of a ‘brute force’ approach involving mobilization comes from and is informed by a number of conversations with Dr. Tai Ming Cheung on the topic. For a more extensive discussion of these dynamics, see: Elsa B. Kania and John K. Costello, “Quantum Hegemony? – China’s Ambitions and the Challenge to U.S. Innovation Leadership,” Center for a New American Security, September 2018, <https://www.cnas.org/publications/reports/quantum-hegemony>

¹⁶ However, relative to the U.S. quantum industry, there does not yet appear to be an extensive ecosystem of start-ups pursuing research in quantum computing in China, which is recognized as a relative weakness. See: CAICT [中国信通院], “Research Report on Quantum Information Technology Development and Industrialization” [量子信息技术发展与应用 研究报告], December 2018, <http://www.caict.ac.cn/kxyj/qwfb/bps/201812/P020181221551983008723.pdf>.

¹⁷ “Alibaba Cloud and CAS Launch One of the World’s Most Powerful Public Quantum Computing Services,” March 1, 2018, <https://www.alibabacloud.com/press-room/alibaba-cloud-and-cas-launch-one-of-the-worlds-most>

¹⁸ “Baidu has entered the race to build quantum computers,” *MIT Technology Review*, March 8, 2018, <https://www.technologyreview.com/the-download/610449/baidu-has-entered-the-race-to-build-quantum-computers/>.

¹⁹ Often, Chinese “indigenous” innovation has been enabled through the acquisition, including by means of espionage, of foreign technologies, but China’s results in quantum science appear to reflect the start of a shift towards more truly original innovation. For authoritative analyses of this trajectory, see: William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology acquisition and Military Modernization*, Routledge, 2013. Jon R. Lindsay and Tai Ming Cheung, “From Exploitation to Innovation: Acquisition, Absorption, and Application,” in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (2015): 51-86.

²⁰ For recent reporting on this priority, see: Meng Jing, Celia Chen, and Jane Cai, “China calls on private sector to beef up investment in basic science as it seeks to become tech powerhouse,” *South China Morning Post*, March 11, 2019, <https://www.scmp.com/tech/policy/article/2189445/china-reiterates-it-will-step-investment-basic-science-and-call-industry>

²¹ For instance, the world’s first quantum satellite was enabled by cooperation between the Chinese and Austrian Academies of Sciences, a detail that China’s state media often does not mention. In addition, the joint venture between ID Quantique and China Quantum Technologies (QTEC), through which this company, founded as a spin-

prospects of these initiatives with confidence, given the considerable uncertainties regarding the trajectory of future technological developments. Moreover, certain weaknesses persist in Chinese quantum innovation, including institutional impediments to interdisciplinary cooperation and challenges in the complex engineering that is required.²² However, China clearly aspires to contest traditional American leadership in innovation in ways that may have far-reaching implications for today's great power rivalry.

The Imperative of Innovation

China's quest for innovation is at the heart of its agenda for national rejuvenation. As a rising power, the pursuit of innovation also constitutes a core element of China's challenge to American dominance.²³ Chinese leaders recognize today's emerging technologies as a unique chance to achieve a strategic advantage. In particular, a new national strategy of "innovation-driven development" emphasizes, "Disruptive technologies are constantly emerging, continually reshaping the world's competitive landscape, changing the balance of power among states... Our nation is not only facing a rare historic opportunity to catch up and leapfrog ahead but also confronting the serious challenge of a gap that could widen."²⁴ In certain respects, this powerful commitment to innovation is influenced by the historical memory of China's past weaknesses during the "Century of Humiliation," which are often attributed to its relative technological backwardness at that time.²⁵ Such intense anxieties about the perils of failing to keep pace have combined with an enthusiasm for new strategic technologies in which China is starting from the same point as the U.S. — and may thus have the chance to be a first-mover in innovation, rather than a latecomer seeking to catch up. Although these objectives have remained relatively

off from the University of Geneva, has provided QKD solutions and Quantum Random Number Generators (QRNGs) to the China market, may also be worth noting. See: "ID Quantique & China Quantum Technologies (QTEC) Announce Joint-Venture," December 14, 2016, <https://www.idquantique.com/idq-qtec/>

²² This white paper provides a fairly balanced and, at times, even pessimistic assessment, relative to the hype and enthusiasm often characteristic of media reporting: CAICT [中国信通院], "Research Report on Quantum Information Technology's Development and Industrialization" [量子信息技术发展与应用 研究报告], December 2018, <http://www.caict.ac.cn/kxyj/qwfb/bps/201812/P020181221551983008723.pdf>.

²³ For a theoretical and empirical treatment of the topic, see: Andrew B. Kennedy and Darren J. Lim, "The Innovation Imperative: Technology and US-China rivalry in the Twenty-First Century," *International Affairs* 94, no. 3 (2018): 553-572.

²⁴ "CCP Central Commission and the State Council Release the "Outline of the National Innovation-Driven Development Strategy" [中共中央 国务院印发《国家创新驱动发展战略纲要》, Xinhua, May 19, 2016, http://news.xinhuanet.com/politics/2016-05/19/c_1118898033.htm.

²⁵ Ibid.

consistent across recent generations of Chinese leadership, Xi Jinping has placed his own imprimatur upon innovation in a way and to an extent that implies that this concept could be considered a core element of his ideology. By his assessment, “If China wants to be strong and to rejuvenate, we must vigorously develop science and technology, striving to become the world’s premier center of science and high ground of innovation.”²⁶

Xi Jinping has personally indicated strong interest in quantum science, which may contribute a catalytic influence upon innovation in this field.²⁷ In September 2013, Xi Jinping and the Politburo members engaged with Pan Jianwei (潘建伟), China’s leading quantum physicist, and quantum communications companies founded on the basis of his research, viewing a demonstration of their technology.²⁸ It may not be coincidental that this visit occurred just a few months after leaks, called ‘Prism-gate’ in China’s state media, by former NSA contractor Edward Snowden, which had thrown in stark relief the extent of U.S. cyber espionage capabilities and Chinese relative vulnerabilities, thus heightening threat perceptions about the insecurity of Chinese information technology infrastructure. As a result, Snowden has been since described in Chinese media as one of two individuals with a key role in the ‘drama’ of China’s quantum agenda, along with Pan Jianwei himself.²⁹ Consequently, Chinese scientists have apparently possessed practically unlimited resources to pursue such projects, in the hope of creating a new “shield” for sensitive information and communications.³⁰ When he visited and inspected the University of Science and Technology of China in April 2016, Xi Jinping talked to Pan Jianwei and his team, praising their research in quantum communications as “very promising

²⁶ “Quantum’s On Fire; How to Reach Scientific and Research Results” [量子火了，科研成果如何落地], *Guangming Daily*, March 12, 2019, <http://news.sciencenet.cn/htmlnews/2019/3/423853.shtm>

²⁷ Tai Ming Cheung discusses the notion of catalytic factors as contributing to innovation in the framework that he has developed on the topic, which I have drawn upon and been influenced by in much of my research on these issues: Tai Ming Cheung, “Critical Factors in Enabling Defense Innovation: A Systems Perspective,” (2018)

²⁸ “Anhui Quantum Communications Innovations Successful; Featured in Politburo Collective Learning Activities” [安徽量子通信创新成果 亮相中央政治局集体学习活动], *Quantum CTek*, September 30, 2013, <http://www.quantum-sh.com/news/146.html>.

²⁹ “Quantum Revolution: Opening the ‘New Engine’ for Future Science and Technology” [量子革命：开启未来科技“新引擎”], *Economics Observer*, October 23, 2017, https://web.archive.org/save/http://www.xinhuanet.com/science/2017-10/23/c_136697748.htm

³⁰ “Ten Years Casting a Shield for Information Security” [十年铸就信息安全之“盾”], *China Science Report* [中国科学报], August 16, 2016, <http://webcache.googleusercontent.com/search?q=cache:r9cvBe52Y-8J:news.sciencenet.cn/htmlnews/2016/8/353791.shtm+&cd=1&hl=en&ct=clnk&gl=us>.

and very important.”³¹ During the Politburo study session on cyber security in October 2016, Xi again emphasized the criticality of advancing indigenous innovation in quantum communications, along with other critical cyber and information technologies.³² Reflecting on these trends, his remarks have highlighted, “Scientists are beginning to control the quantum world; this will greatly promote the development of information, energy, and materials sciences, bringing about a new industrial revolution.”³³

This fight to innovate is often characterized in highly martial terms by Chinese leaders and scientists. Chinese leaders often declare that China must “occupy the commanding heights” of “key and core technologies.” Xi Jinping has urged that China must “compose shock brigades and special forces to storm the passes” in pursuit of advances in the research and development of such critical and foundational technologies.³⁴ As teams around the world compete to be the first to achieve quantum supremacy (量子霸权), the symbolic milestone at which a quantum computer can outperform a classical computer, one prominent Chinese quantum scientist, Guo Guangcan of the Key Laboratory of Quantum Information at the University of Science and Technology of China, has argued, “If we want win the struggle for quantum supremacy, we must not be ‘guerrillas’—necessarily, we must organize a ‘group army.’”³⁵ Continuing this analogy, China’s battle for leadership in quantum computing has included a ‘war chest’ that amounts to and may exceed tens of billions of dollars in funding from the government and investments, along with the mobilization of ‘special forces’ of strategic scientists through active initiatives in education and talent recruitment. In particular, China has announced plans to establish a National

³¹ “Xi Jinping Inspects the University of Science and Technology of China: [We] Must Promote Independent Innovation in the Open” [习近平考察中科大：要在开放中推进自主创新], April 27, 2016, https://web.archive.org/web/20190311150413/http://news.ustc.edu.cn/mtgz/201604/t20160427_243894.html

³² “Xi Jinping: Accelerate the Advancement of Indigenous Innovation in Cyber and Information Technologies” [习近平：加快推进网络信息技术自主创新], Xinhua, October 9, 2016, http://news.xinhuanet.com/politics/2016-10/09/c_1119682204.htm.

³³ “Excerpts from Xi Jinping's Discussions of Scientific and Technological Innovation” [习近平关于科技创新论述摘编], May 11, 2016, http://www.sjziam.cas.cn/dqyd/xyyd/201603/t20160311_4548759.html

³⁴ See this translation courtesy of Rogier Creemers: “Speech at the Work Conference for Cybersecurity and Informatization,” April 19, 2016, <https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/>

³⁵ “Observing the Global Battle for “Quantum Hegemony”” [全球“量子霸权”争夺战观察], Xinhua, February 14, 2018, http://www.xinhuanet.com/science/2018-02/14/c_136972095.htm

Here is the original phrasing for his remark, and I have taken some slight liberties with the translation to render it more colloquially in English: “要打赢量子霸权争夺战，不能做‘游击队’，一定要组织‘集团军’

Laboratory for Quantum Information Science that could receive billions of dollars in funding.³⁶ At present, its construction is underway, building upon an initial institute for quantum innovation at the University of Science and Technology of China towards a model that will combine this future headquarters in Hefei with branches in Beijing and Shanghai, plus a national network of partnerships.³⁷ Pan Jianwei highlighted the urgency of these efforts in response to the “fierce assaults” of international competition in his remarks as a delegate to the “Two Sessions” in March 2019.³⁸ This agenda also includes a number of local initiatives, such as Anhui Province’s creation of a fund for quantum science and industry with 10 billion RMB (over \$1.6 billion) to start,³⁹ the launch of a plan and special project in Shandong and Guangdong provinces respectively,⁴⁰ and even the city of Jinan’s plans to create a “Quantum Valley” that could promote industry development.⁴¹ China is also in the process of establishing a national technological commission for quantum technology that will promote industrialization and standardization.⁴²

As an initial evaluation, China’s approach to innovation in such emerging technologies could prove effective, but also inefficient and incongruent in certain respects. The critical

³⁶ “Anhui Reports on the Construction of the National Laboratory of Quantum Information Science, Total Investment 7 Billion Yuan” [安徽拟申报建设量子信息科学国家实验室，总投资约 70 亿元], July 11, 2017, <http://news.163.com/17/0711/15/CP2TJ9V7000187VE.html>.

³⁷ “The Anhui delegation proposed to approve the National Laboratory of Quantum Information Science and promote the province's efforts” [安徽代表团建议批复量子信息科学国家实验室，举全省之力推进], *The Paper*, March 8, 2019, https://m.thepaper.cn/wifiKey_detail.jsp?contid=3097278&from=wifiKey

³⁸ “Pan Jianwei: Suffering the fierce assault of international competition, it is necessary to substantially implement the construction of the National Laboratory for Quantum Information Science as soon as possible” [潘建伟：受国际竞争强烈冲击，需尽快实质性启动量子信息科学国家实验室建设], *China Daily*, March 10, 2019, <http://cn.chinadaily.com.cn/a/201903/10/WS5c8492eba31010568bdce87a.html>

³⁹ “One Hundred Hundred Million Yuan Anhui Quantum Science Industry Development Fund Launches Operations” [百亿元安徽量子科学产业发展基金启动运营], *China News Network*, December 12, 2017, <http://webcache.googleusercontent.com/search?q=cache:Yu9KlnNMReOJ:news.sina.com.cn/o/2017-12-12/doc-ifypnyqi4346545.shtml+&cd=4&hl=en&ct=clnk&gl=us>.

⁴⁰ Potentially, there may be more plans and initiatives launched across various provinces and municipalities going forward. See: “Shandong Province Quantum Technology Innovation and Development Plan (2018-2025)” [山东省量子技术创新发展规划], March 6, 2018, <http://www.sdsc.gov.cn/uploadfiles/ueditor/file/20180305/1520234573711015373.doc>. See also: “2018-2019 Guangdong Province Major S&T Special Project “Quantum Science and Engineering Application Guidance” [2018~2019 年度广东省重大科技专项 “量子科学与工程” 申报指南], <https://web.archive.org/web/20190312035513/http://www.gzzoc.com/xwzx/tzgg/zytz/201809/P020180912623719564172.pdf>

⁴¹ “Jinan Will Set the “National Standard” in Quantum Communications Security” [济南将为量子通信安全做“国标”], March 24, 2018, <http://news.takungpao.com/mainland/topnews/2018-03/3554886.html>.

⁴² “China to establish national commission for quantum computing standards,” *Xinhua*, August 6, 2018, https://web.archive.org/web/20180818004101/http://www.xinhuanet.com:80/english/2018-08/06/c_137371729.htm

question has arisen and remains: Can China reconcile the apparent tension between innovation and authoritarianism? These seem to be core contradictions in China's current paradigm for development, yet China's Party-state has attempted to reconcile its assertion of increased ideological authority with the forceful promotion of innovation as a matter of national strategy, while seemingly providing relative autonomy to scientists involved in such major strategic initiatives. At the same time, China's tech companies have emerged as key leaders and new 'national champions' for innovation. For instance, Alibaba plans to invest over \$15 billion in disruptive technologies, including quantum computing,⁴³ through its DAMO Academy and aspires to fully realize a universal quantum computer by 2030.⁴⁴ The success of such players has often been enabled by their relative autonomy, but the space within which tech companies could operate with some independence seems to be becoming more constrained with the reassertion and expansion of Party control.⁴⁵ Consequently, the inextricability of nationalism that has been a core feature of science in China is becoming even more accentuated under Xi Jinping,⁴⁶ who has declared, "The Party leads everything."⁴⁷ The potential for costs to creativity or adverse impacts of interference can be difficult to evaluate but may introduce greater friction or create damaging incentives in practice. Among the negative externalities of these trends could be a distortion of incentives and assessments, which could extend to unrealistic expectations about these technological developments.⁴⁸

⁴³ "Alibaba Established "DAMO Academy"" [阿里巴巴成立 "达摩院"], Xinhua, October 11, 2017, http://www.xinhuanet.com/tech/2017-10/11/c_1121785713.htm

⁴⁴ "The Chinese Academy of Sciences, Hand in Hand with Alibaba, Will Establish a 'Quantum Computing Laboratory' in Shanghai" [中国科学院携手阿里巴巴在沪建立"量子计算实验室"], Xinhua, July 31, 2015, http://news.xinhuanet.com/2015-07/31/c_1116104188.htm. "CAS Quantum Innovation Research Center Collaborates with AliCloud to Launch a Quantum Computing Cloud Platform" [中科院量子创新研究院联合阿里云发布量子计算云平台], Xinhua, October 12, 2017, http://www.xinhuanet.com/science/2017-10/12/c_136673422.htm.

⁴⁵ For one thoughtful assessment of these trends, see: Christopher Balding, "China Is Nationalizing Its Tech Sector," *Bloomberg*, April 12, 2018, <https://www.bloomberg.com/opinion/articles/2018-04-12/china-is-nationalizing-its-tech-sector>.

⁴⁶ For a compelling discussion of the difficult considerations often confronting Chinese scientists, see: Yangyang Cheng, "For Science, Or The 'Motherland'? The Dilemma Facing China's Brightest Minds," *SupChina*, January 30, 2019, <https://supchina.com/2019/01/30/for-science-or-the-motherland-chinas-brightest-minds/>

⁴⁷ For a more theoretical assessment of what this declaration entails, including the decision to write it into the Party constitution explicitly, see: "How to Understand "The Party Leads Everything" Written Into the Party Constitution" [怎样认识"党是领导一切的"写入党章?], *People's Daily*, January 25, 2018, <http://webcache.googleusercontent.com/search?q=cache:vedWYvXBPFYJ:cpc.people.com.cn/n1/2018/0125/c123889-29787340.html+&cd=7&hl=en&ct=clnk&gl=us>

⁴⁸ For instance, there is extreme skepticism among many American scientists regarding the actual utility of quantum key distribution that appears to arise much more rarely in discussions of this technology in China.

Quantum Questions for Cyber Security

Today's parallel advances in quantum communications and computing may have significant implications for the future of cyber security and conflict. Already, the employment of new techniques of quantum cryptography to secure communications can enable improvements in cyber defense and information assurance, even if claims of “perfect security” may prove chimeric in practice. Chinese leaders are seeking to improve security through shifting sensitive information and communications to quantum networks, in the hope that this strong “shield” could mitigate vulnerability to adversarial espionage – and to a future quantum computer that could enable new assaults on encryption.⁴⁹ In practice, China's quantum networks are unlikely to prove truly ‘unhackable’ and instead might remain vulnerable to spoofing and interference, or the perhaps inevitable systemic and human weaknesses that may remain, despite attempts to develop measures for mitigation.⁵⁰ Moreover, recent research indicates even measurement-device-independent quantum key distribution (MDI-QKD), believed to be highly secure, is vulnerable to certain techniques of hacking with a high rate of success.⁵¹ This interplay of security measures and countermeasures, and between defenders and would-be hackers, will certainly continue going forward. Although Chinese leaders have appeared so far to be quite enthusiastic about the promise of quantum communications, there are indications of further debate emerging on the reliability and tradeoffs of extensive investments in these technologies, including apparent criticisms of quantum communications as a “pseudoscience” to which Pan Jianwei responded during the March 2019 at China's annual “Two Sessions.”⁵² Despite the recurrence of claims that quantum communications could enable “absolute security,” there appears to be increased awareness of the problems and technical bottlenecks, such as limited

⁴⁹ “Ten Years Casting a Shield for Information Security” [十年铸就信息安全之“盾”], *China Science and Technology* [中国科学报], August 16, 2016, <http://webcache.googleusercontent.com/search?q=cache:r9cvBe52Y-8J:news.sciencenet.cn/htmlnews/2016/8/353791.shtm+&cd=1&hl=en&ct=clnk&gl=us>.

⁵⁰ For instance, the PLA Information Engineering University, now under the Strategic Support Force, has been funded by the National Science Foundation of China for “Research on the Security of Quantum Cryptography and Other New-Type Measures Facing the Risks of Hacker Attack's Decoys” (面临黑客攻击风险的诱骗态量子密码及其新型方案的安全性研究), <http://npd.nsf.gov.cn/showOrganizationAction.action?orgCode=201202>.

⁵¹ For a less technical review of this research, see: “There's a new way to break quantum cryptography,” MIT Technology Review, March 6, 2019, <https://www.technologyreview.com/s/613079/theres-a-new-way-to-break-quantum-cryptography/>. For the paper itself as posted in arXiv, see: [Xiao-Ling Pang](https://arxiv.org/abs/1902.10423), Ai-Lin Yang, Chao-Ni Zhang, Jian-Peng, Dou, [Hang Li](https://arxiv.org/abs/1902.10423), Jun Gao, and Xian-Min Jin, “Hacking Quantum Key Distribution via Injection Locking,” February 27, 2019, <https://arxiv.org/abs/1902.10423>

⁵² “Is quantum communication a pseudoscience? Pan Jianwei responded like this” [量子通信是不是伪科学? 潘建伟这样回应], *Science and Technology Daily* [科技日报], March 11, 2019, https://web.archive.org/web/20190311152530/http://stdaily.com/index/fangtan/2019-03/11/content_754686.shtml

capacity and distance, remaining in China's operationalization of quantum communications, that persist for the time being.⁵³

It is reasonable nonetheless to raise the question of whether China could succeed in complicating or undermining the efficacy of U.S. cyber espionage and signals intelligence capabilities through these technological developments. Increasingly, it appears that sensitive information is being shifted over to these new, perhaps more secure systems. In particular, the Chinese People's Liberation Army (PLA) appears to be unique among militaries in the extent to which it is leveraging quantum communications within its C4ISR architecture. As early as 2015, Pan Jianwei had claimed, "China is completely capable of making full use of quantum communications in a local war. The direction of development in the future calls for using relay satellites to realize quantum communications and control that covers the entire army."⁵⁴ The PLA has also started testing mobile systems for QKD,⁵⁵ and the Chinese defense industry is exploring the extension of new techniques for quantum communications underwater to nuclear submarines and via satellite to ships at sea.⁵⁶ Potentially, if capable of improved shielding of sensitive information and communications against adversary intelligence collection, China could achieve an advantage in peacetime and wartime competition alike. Perhaps, such developments may even result in a "going dark" phenomenon that could increase the uncertainty of competitors about China's intentions. To the extent that accurate intelligence can constitute a stabilizing influence in great power rivalries, such a lessening of visibility could exacerbate the risks of surprise or misperception in U.S.-China relations going forward. However, it remains to be seen

⁵³ CAICT [中国信通院], "Research Report on Quantum Information Technology Development and Industrialization" [量子信息技术发展与应用 研究报告], December 2018, <http://www.caict.ac.cn/kxyj/qwfb/bps/201812/P020181221551983008723.pdf>. The China Academy for Information and Communications Technology is a research institute under the aegis of China's Ministry of Industry and Information Technology (MIIT) that has emerged as a notable player on these issues. For a more detailed assessment of its influence, see this profile from New America's DigiChina initiative: "China Academy for Information and Communications Technology (CAICT)," <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/profile-china-academy-information-and-communications-technology-caict/>

⁵⁴ Yu Dawei, "In China, Quantum Communications Comes of Age," *Caixin*, February 6, 2015, <https://www.caixinglobal.com/2015-02-06/101012695.html>

⁵⁵ "Chinese military-use quantum mobile phones will be entering trial usage" [中国军用量子手机将投入试用], *Military Observer*, June 29, 2018, <http://mil.news.sina.com.cn/china/2018-06-29/doc-ihqpwqy6243500.shtml>

⁵⁶ "CSIC promotes the industrialization of quantum technologies to seize the commanding heights of maritime defense applications" [中船重工推进量子技术产业化 抢占海防应用制高点], *China Securities News*, February 5, 2018, http://webcache.googleusercontent.com/search?q=cache:Hso1WYvBhhMJ:www.xinhuanet.com/fortune/2018-02/05/c_129805346.htm+&cd=1&hl=en&ct=clnk&gl=us.

how secure and resilient such nascent systems would prove under actual operational conditions. That is, there are reasons for concern, but not alarm, at this potential for “quantum surprise,” and such considerations will require more granular technical assessment going forward.

Moreover, China's early start on a quantum-secure architecture, through this nationwide construction of quantum networks, could provide a comparative advantage for adaption to the future disruption that will result from the advent of quantum computing. Indeed, quantum computers will introduce immensely powerful capabilities that could be leveraged to break public key cryptography, thus threatening the current foundations of our information technology ecosystem. Because information that may be collected today while encrypted could be decrypted in the future by a quantum computer, there are evident benefits to starting that process of transition to ‘quantum-proof’ cryptography, of which QKD is one approach, as early as possible, in order to minimize those risks of future exposure.⁵⁷ There are reasons for concern that the actor who first succeeds in the development of a quantum computer of sufficient capability could achieve an inestimable advantage on that ‘Q-Day,’ given the immense increases in computing that will result. By most estimates, the creation of a quantum computer with that capacity will require at least a decade, and a general-purpose quantum computer with full functionality may remain several decades in the future, but the timeframe is inherently uncertain. Even as recent developments in China, such as quantum chips and a control system, and worldwide indicate rapid advances,⁵⁸ this race could prove more of a marathon in the years to come, requiring further progress in such disparate difficulties as error correction for qubits and the development of new algorithms and software.⁵⁹

Going forward, the impact of this quantum revolution may prove more incremental than transformational,⁶⁰ insofar as the impact on the offense-defense balance in the cyber domain will

⁵⁷ The potential for quantum secure direct communication is also worth noting, including related advances in quantum memory. See, for instance: Zhang, Wei, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo. “Quantum secure direct communication with quantum memory,” *Physical Review Letters* 118, no. 22 (2017): 220501.

⁵⁸ “Quantum computer ‘backbone’ developed,” *Global Times*, December 12, 2018, <http://www.globaltimes.cn/content/1131612.shtml>

⁵⁹ For context on these requirements, see: Alán Aspuru-Guzik, “Algorithms for Quantum Computers,” *Scientific American*, September 14, 2018, <https://www.scientificamerican.com/article/algorithms-for-quantum-computers/>

⁶⁰ For an excellent analysis of reasons to question the claim that quantum computing in particular could be radically disruptive, see: Jon Lindsay, “Why Quantum Computing Will Not Destabilize International Security: The Political Logic of Cryptology,” June 29, 2018, <https://ssrn.com/abstract=3205507> or <http://dx.doi.org/10.2139/ssrn.3205507>

also depend upon a range of technical and organizational challenges. In the future, the extent to which the United States could prove relatively vulnerable to such future threats will depend on the extent to which the U.S. military and government succeed in updating their own legacy systems, whether through the use of quantum or “quantum-resistant” cryptography on the basis of standards currently under development by the National Institute of Standards and Technology (NIST), in anticipation of these risks.⁶¹ The U.S. National Cyber Strategy, released in September 2018, urged, “To protect against the potential threat of quantum computers being able to break modern public key cryptography...[t]he United States must be at the forefront of protecting communications by supporting rapid adoption of these forthcoming NIST standards across government infrastructure and by encouraging the Nation to do the same.”⁶² Hopefully, this exhortation will be implemented in practice. In the meantime, the expertise and experience that China is acquiring through the early implementation and standardization of quantum cryptography communications could provide an advantage in the next-generation of quantum networking,⁶³ even the possibility of a future “quantum Internet” that may be ‘made in China’ to be secure by design.⁶⁴ In this regard, the strategic implications of this quantum revolution for the U.S. and China will be shaped by their respective approaches to developing and operationalizing these technologies.

⁶¹ For the latest on this process, see: “NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto ‘Semifinals,’” January 30, 2019, <https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals>

⁶² “NATIONAL CYBER STRATEGY of the United States of America,” White House, September 2018, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

⁶³ The relevant research in China dates back nearly a decade at this point. See, for instance: Lu, Chao-Yang, Tao Yang, and Jian-Wei Pan, “Experimental multiparticle entanglement swapping for quantum networking,” *Physical Review Letters* 103, no. 2 (2009): 020501.

⁶⁴ For an interview in which Pan Jianwei discusses these objectives at some length, see: “The man turning China into a quantum superpower,” MIT Technology Review, December 19, 2018, <https://www.technologyreview.com/s/612596/the-man-turning-china-into-a-quantum-superpower/>