Chinese Efforts in Quantum Information Science: Drivers, Milestones, and Strategic Implications

Testimony for the U.S.-China Economic and Security Review Commission

March 16th, 2017

John Costello

We are in the midst of a "second quantum revolution," one that enables disruptive new technologies that have the potential to change long-held dynamics in commerce, military affairs, and strategic balance of power.[1] Within the foreseeable future, the realization of quantum computing will result in revolutionary computing power, with wide-reaching applications. The employment of quantum cryptography can create quantum communications systems that are theoretically unbreakable and unhackable. Quantum sensing enables the capability to conduct extremely precise, accurate measurements for new forms of navigation, radar, and optical detection.

Although the future trajectory of quantum technologies is hard to predict, their revolutionary potential and promise has intensified international competition. The U.S. remains at the forefront of quantum information science, but its lead has slipped considerably as other nations, China in particular, have allocated extensive funding to basic and applied research. Consequently, Chinese advances in quantum information science have the potential to surpass the United States.[2] Once operationalized, quantum technologies will also have transformative implications for China's national security and economy. As the United States has sustained a leading position in the international affairs due in part to its technological, military, and economic preeminence, it is critical to take swift action to reverse this trend and once again place the United States as a frontrunner in emerging technologies like quantum information science.

This testimony will address the following topics:

---

[1] Jonathan P. Dowling and Gerard J. Milburne, "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

[2] This testimony builds upon prior research and writings by the author, including: Elsa Kania and John Costello, "Quantum Leap (Part 1): China's Advances in Quantum Information Science, *China Brief*, December 5, 2016. Elsa Kania and John Costello, "Quantum Leap (Part 2): The Strategic Implications of Quantum Technologies, *China Brief*, December 21, 2016.

- Part I offers a basic overview of the underlying technology, applications, current status, and challenges in quantum computing, quantum encryption, and quantum sensing.
- Part II details drivers behind China's investment in quantum information science, national R&D plans, and efforts and milestones.
- Part III compares U.S. and Chinese efforts and delineates the critical factors in play.
- Part IV details the commercial and strategic implications of quantum information science technologies.
- Part V provides a conclusion and final thoughts on the information presented.
- Part VI gives recommendations to the U.S. Congress on how the United States may regain its lead in quantum information science and other critical emerging technologies.

Part I. Overview of Quantum Information Science Technologies:

Quantum information science harnesses the power of uncertainty and the strange – often counterintuitive – properties of quantum states. Taken together and scaled, these technologies establish exciting new paradigms in every aspect where information is used, stored, processed, or collected, providing vastly more powerful instruments of computation, security, and measurement.

General Principles

Quantum information science can be broadly broken up into quantum computing, quantum encryption, and quantum sensing. While each of these technologies differ wildly in technological basis and applications, all rely on two fundamental properties of quantum phenomena: superposition and entanglement. Superposition refers to the ability of a particle, like a photon, to exist in all possible states at the same time. Entanglement refers to sharing this state across two or more particles. Observing the particle will "collapse" the state, resulting in its reversion to one of the two states. So too, for entangled pairs, even if separated across a great distance, the observation of either particle will "collapse" the state, immediately reverting one particle to one state and the other to a corresponding, opposite state. It is these strange properties of superposition and entanglement, the latter of which Einstein famously referred to as "spooky action at a distance," that give these technologies their unique power.

Quantum Computing

Traditional or "classical" computers perform calculations using standard "bits" which exist in states 1 or 0. Quantum computing, through its employment of "qubits" (i.e., a quantum analogue of the “bit,” which simultaneously exists in a superposition of the states of 0 and 1), will convey an extreme advantage in computing power. Qubits, which exist in a superimposed state and entangled together are able to execute vast numbers of calculations simultaneously. In the future, quantum computers will be able to resolve complex algorithms, including those integral to most standard encryption methods. Computations that would be impossible or infeasible for classical computers to perform can be performed by quantum computers at sufficient scale.

The commercial promise of a full-scale general quantum computer is largely driving both state-level and commercial funding into these technologies. The commercial and military applications of these technologies are nearly endless, appropriate wherever speed and processing power are at a premium. Some commercial applications that have been suggested include large-scale simulations for weather, complex and chaotic systems, protein folding and modeling, genomics, big-data, intelligence processing, and artificial intelligence. For the military, as the information age ends and a new age based on automation and machine learning takes hold, the processing power of quantum computers promises to play a critical role.

Currently, a general-purpose, full-scale quantum computer does not exist. D-Wave, a Canada-based company, does produce what has been called the world’s first quantum computer. However, this computer uses “quantum annealing” a form of computation that, strictly defined, is not considered “true” quantum computing. Google, IBM, and NASA, among others, on the U.S. side and Alibaba and Chinese Academy of Sciences (CAS) on the Chinese side are each establishing public-private or private research groups with the object of developing a general-use quantum computer. The goal is to achieve “quantum supremacy” or a quantum computer that is able to outperform a traditional, or classical computer in every way.

There are significant technological barriers that need to be overcome to realize a fully capable quantum computer. It will be challenging but necessary to scale quantum computers to achieve quantum supremacy. In addition, designing the algorithms and software on which these calculations could be run presents a further challenge. Since quantum computers do not perform calculations like classical computers, newer approaches to software and programming are another factor to consider in developing the capacity necessary to exploit these technologies.

Nonetheless, security researchers have become concerned that quantum computers could undermine certain prevalent encryption standards currently in use. Using Shor’s algorithm, a quantum computer of sufficient scale would be able to crack encryption keys for many modern forms of encryption, an endeavor that by today’s classical computing standards would be impossible or infeasible within a practical time frame. In 2015, likely in response to progress in quantum computing, the National Security Agency (NSA) updated their "Suite B" encryption methods towards ones that focused on "quantum resistant" encryption, or encryption standards that would be beyond a quantum computer's ability to break.[3] The National Institute of Standards and Technology (NIST) has also launched a competition in response to develop a set of "quantum resistant" encryption standards.[4] Other forms of encryption, such as lattice-based encryption, are less efficient but resistant through cracking from quantum computers.

Quantum Cryptography:

There are three qualities of quantum states that give quantum encryption and communications their protective power, according to SANS.[5] First, the "no-cloning" theorem states that an unknown quantum state cannot be copied. Second, in a quantum system, which is a complex of two or more particles in a shared "entangled" state, an attempt to measure or observe will disturb the system, revealing an eavesdropper to the sender and recipient. Third, disturbing the system is irreversible, meaning an interloper wouldn't be able to cover up evidence of the interception.

Quantum key distribution can be accomplished through fiber-optic networks as well as over the electromagnetic spectrum in "free space" quantum communications. Sending through fiber-optic networks limits range of QKD, while quantum free-space communications allows for more long-distance key exchange but opens it open to other forms of interference, such as debris, noise, and jamming. These technologies have considerable technological and logistical challenges and, according to some researchers don't confer enough information security advantages to warrant the added complexity necessary for their use. The Air Force Scientific Advisory Board stated that classical alternatives offer the same advantages without the headache of additional equipment and complexity.[6]

Concerns over information security and privacy of communication may be driving significant state-level investment in this field. China, in particular, has drawn a direct line between state-level programs in quantum encryption and revelations of massive U.S. espionage alleged by

---

[3] Bruce Schneier, "NSA Plans for a Post-Quantum World," Lawfare, August 21, 2015, https://www.lawfareblog.com/nsa-plans-post-quantum-world

[4] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone, "Report on Post-Quantum Cryptography," *National Institute of Standards and Technology Internal Report* 8105 (2016).

[5] Bruce R. Auburn, "Quantum Encryption–A Means to Perfect Security," *SANS Institute*, 2003, https://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986

[6] USAF Scientific Advisory Board, "Utility of Quantum Systems for the Air Force," August 19, 2016, http://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230.

Edward Snowden. These technologies have apparent, but untested, military applications as well. Quantum teleportation and communication not only conceals the content of the message, but also alerts the recipient and sender if the signal is intercepted. This is a major potential disruptive feature in the world of global intelligence, surveillance, and reconnaissance capabilities.

Quantum Sensing

Quantum sensing, broadly defined, is the ability to use quantum phenomena like entanglement for extremely precise and accurate measurements, also known as quantum metrology. This discipline of quantum information science is a collection of techniques and applications of quantum metrology in sensors, rather than a specific technology in its own right. More accurate quantum clocks, quantum imagery, radar, navigation, and compasses are all discussed under this discipline.

Quantum sensors for use in gravimetric readers have commercial and military applications in subsurface sensing and detection (such as in oil-drilling) and inertial navigation systems, which would allow for high-precision navigation without global position satellites (GPS). This so-called “quantum navigation” or “quantum compass” would be useful for submarines and other maritime platforms. Quantum radar could nullify stealth technologies and advanced forms of radar jamming. Quantum imagery can allow for more precise optical capabilities that would have applications to space-spaced intelligence, surveillance, and reconnaissance and awareness in the space domain.

Of quantum information science disciplines, quantum sensing has the most direct and obvious military applications. As such, there is comparatively little openly available research on these topics when compared to quantum computing and encryption, which appear to be largely privatesector and academic affairs, respectively. As further research into this field evolves, more information will give a better picture of the relative progress made by the United States and China in the development of these technologies.

Part II. Chinese Quantum Information Science Efforts:

Under the leadership of Xi Jinping, China’s prioritization of quantum information science has intensified. From the Chinese leadership’s perspective, quantum technologies have become integral to national security, particularly information security, and to strategic competition. This research agenda has taken on increased importance ever since the leaks by former NSA contractor Edward Snowden. In fact, this incident was so fundamental to Chinese motivations that Snowden has been characterized as one of two individuals with a primary role in this scientific ‘drama,’ along with Pan Jianwei himself.[7]

There are three fundamental factors driving China’s investment into quantum information science R&D:

1. Information Security: The use of quantum encryption and communication for information security is a primary driver for China’s increased investment in that field. Chinese scientists and media have drawn a direct linkage between the need for progress in quantum information science and the Snowden leaks. As Chinese authorities grow more concerned about potential for spying in their ICT systems, the advantages that quantum encryption confers will be se This will be especially critical as Chinese society grows more informatized and connected, potentially making it even more vulnerable to foreign adversary spying, sabotage, and influence.

2. Economic Competition: There is a recognition that current U.S. dominance in information technology may not confer any substantial advantages in pursuit of quantum information science, essentially placing China on par with the United States and putting it in a unique strategic position to corner the market on these technologies. If so, China would benefit from first-to-market advantage that, when coupled with its manufacturing and human capital base would allow it to achieve and sustain global leadership in quantum information solutions and the next information revolution.

3. Strategic Military Competition: Quantum computing has very real military applications in the fields of big data analytics, artificial intelligence, complex systems simulation, and advanced robotics. The widespread adoption of quantum technologies for military or government communications would hinder an adversary’s ability to conduct surveillance and signal intercepts, as any attempt to do so would be detectable. Additionally, use of quantum sensing for inertial navigation, stealth detection, high-resolution space-based surveillance and reconnaissance, and submarine detection each challenge current military paradigms built on technological and intelligence superiority, although in different ways. These would disrupt current military paradigms in which the United States has a distinct advantage.

---

[7] “China Will Establish a Global Quantum Communications Network By 2030” [中国将力争在2030年前后建成全球量子通信网], *Xinhua*, August 16, 2016, http://news.sina.com.cn/c/sd/2016-08-16/doc-ifxuxnpy9658879.shtml.

For these reasons, quantum technology has attracted the attention of the Chinese leadership at the highest levels, and Xi himself has emphasized the strategic importance of quantum technologies to national security and particularly cyber security. In September 2013, Xi Jinping and other Politburo members visited Anhui Quantum Communication Technology Co. Ltd. for a collective learning session, meeting with Pan Jianwei and the company's general manager, before viewing a demonstration of quantum communication technology.[8] In November 2015, at the 18th Party Congress' 5th Plenum, Xi Jinping included quantum communications in his list of major science and technology projects that are prioritized for major breakthroughs by 2030, given their importance from the perspective of China's long-term strategic requirements.[9] In April, Xi visited the University of Science and Technology of China, where he met with Pan Jianwei and praised his progress.[10] During the 36th Politburo study session on cyber security, Xi also emphasized the importance of advancing indigenous innovation in quantum communications and other critical cyber information technologies.[11]

Chinese National R&D Planning

At the highest level, the 13th Five-Year Plan (2016-2020), formulated in the aftermath of the Snowden leaks, intensifies the prioritization of quantum information science, including "quantum control" in the category of "basic research related to national strategic requirements."[12] Following from this, China's national research and development plans for science and technology have translated the increasing national prioritization of quantum technology into action through funding research in this domain. The National Key R&D Plan (国家重点研发计

---

[8] "Anhui Quantum Communications Innovation Successfully 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.

[9] "Xi Jinping: Explanations Regarding the "CCP Central Committee Suggestions Regarding the Formation of the National Economic and Social Development Thirteenth Five-Year Plan" [习近平:关于《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》的说明], *Xinhua*, November 3, 2015, http://news.xinhuanet.com/politics/2015-11/03/c_1117029621_3.htm.

[10] "Xi Jinping Inspected USTC: Must Advance Independent Innovation in the Process of Opening" [习近平考察中科大：要在开放中推进自主创新], *Xinhua*, April 27, 2016, http://news.xinhuanet.com/politics/2016-04/27/c_1118744858.htm

[11] "Xi Jinping: Accelerate the Advancement Independent Innovation in Cyber and Information Technology, Unrelentingly Strive towards the Objective of Constructing a Cyber Power" [习近平：加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力], *Xinhua*, October 9, 2016, http://news.xinhuanet.com/politics/2016-10/09/c_1119682204.htm

[12] ""Thirteenth Five-Year" Plan Guidelines" ["十三五"规划纲要], *Xinhua*, March 18, 2016, http://economy.china.com/news/11173316/20160318/22110334_all.html

划), a large-scale reorganization of China's national-level research and development planning, including the consolidation of the 863 and 973 plans, has strengthened and focused development of quantum information science.[13]

Although the Chinese focus on quantum technology can be largely attributed to information security concerns, this also reflects the successes achieved through the research undertaken so far. This has become a self-reinforcing cycle in which national-level interest in quantum technology has proceeded alongside and been reinforced by progress that Chinese researchers have achieved.

National Key R&D Plan

In February 2016, the National Key R&D Plan (国家重点研发计划) included quantum control and quantum information among its prioritized projects. [14] The available guidance for the project in 2016 and 2017 emphasized six particular research tasks: related electronic systems, small quantum systems, artificial band-gap systems, quantum communications, quantum computing and simulations, and quantum precision measurement.[15]

13th Five-Year National Science and Technology Innovation Plan

In August 2016, the new 13th Five-Year National Science and Technology Innovation Plan (国家科技创新规划), urged China to seize the "high ground" (制高点) in international scientific development, included an intensified focus on multiple forms of quantum technology.[16] The plan included quantum control and quantum information as among the top "major strategic

---

[13] "Quantum Control and Quantum Information Key Special 2016 Annual Project Reporting Guidelines" [量子调控与量子信息"重点专项2016年度项目申报指南], Ministry of Science and Technology, February 16, 2016, http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2016/201602/t20160214_124104.htm

[14] "Quantum Control and Quantum Information Key Special 2016 Annual Project Reporting Guidelines" [量子调控与量子信息"重点专项2016年度项目申报指南], Ministry of Science and Technology, February 16, 2016, http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2016/201602/t20160214_124104.htm

[15] Quantum Control and Quantum Information Key Special 2017 Annual Project Reporting Guidelines and Suggestions [量子调控与量子信息重点专项2017年度项目申报指南建议], Ministry of Science and Technology, August 1, 2016, http://service.most.gov.cn/2015tztg_all/20160801/1146.html

[16] "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 |

prospective scientific issues" and called for China to achieve breakthroughs in quantum communication and the quantum anomalous Hall effect.

For the 2030 timeframe, the plan also called for choosing a new round of major science and technology projects that "embody national strategic intent," including quantum communication and quantum computing. In particular, this major project was to include metropolitan and inter-city free space quantum communications technology, the development and manufacture of common-use quantum computing prototypes, and the development and manufacture of actual-use quantum simulators. To develop air and space exploration, the plan called for advancing technologies for quantum navigation and also "the completeness of quantum mechanics."

Made in China 2025

China has also made the commercialization of these technologies as a priority. As of May 2015, the new "Made in China 2025" (中国制造2025) plan included advances in quantum computing among its priorities, in the category of the "next generation information technology industry."[17] The extent to which these efforts may hinder foreign quantum computing efforts ability to compete against Chinese firms within China is unknown.

Chinese Quantum Milestones

Currently, the PRC is hurtling headlong towards the quantum era, placing its bets on the disruptive, even revolutionary potential of quantum technology. These recent breakthroughs have been preceded and enabled by long-term efforts and investments in quantum information science, all enthusiastically backed at the highest levels of Chinese leadership. As a result, Chinese scientists have succeeded in progressing towards the operationalization and commercialization of unhackable quantum communications, while seeking supremacy in quantum computing and concurrently progressing in quantum sensing.

Quantum Computing

While Chinese advances in quantum cryptography have achieved multiple world records and seemingly outpaced parallel global efforts, Chinese quantum computing efforts remain relatively nascent. Nonetheless, Chinese scientists have increasingly kept pace with global progress in

---

[17] "The State Council's Notice on the Printing and Distribution of "Made in China 2025" [国务院关于印发《中国制造2025》的通知], Ministry of Industry and Information Technology, May 19, 2015, http://www.miit.gov.cn/n11293472/n11293877/n16553775/n16553792/16594486.html

quantum computing and also achieved notable advances in this domain.[18] As leading quantum scientist Guo Guangcan has emphasized, “Chinese scientists have been going all out to win the worldwide race to develop a quantum computer.”[19] For instance, in August, USTC scientists announced their successful development of a semiconductor quantum chip, which could enable quantum operations and information processing.[20] Later that month, researchers also from USTC announced their breakthrough in the preparation and measurement of six hundred pairs of entangled quantum particles.[21] In October, USTC researchers announced significant progress in quantum control that could enable future advances in quantum computing based on more precise quantum logic gates.[22] As Pan Jianwei has noted, the eventual development of a quantum computer with 50 qubits could achieve “quantum supremacy” (量子称霸), including the capability to overcome most conventional encryption capabilities.[23] However, Pan anticipates that the creation of a “truly programmable, universal” quantum computer might ultimately require between 30 and 50 years.

Relative to quantum communication, China’s quantum computing efforts have a much greater degree of private sector involvement and investment. This phenomenon is mirrored in Western nations where there is heavy private sector involvement in research on quantum computing. In China, the most visible and mature effort has occurred at the Alibaba Quantum Computing Lab, a collaboration between Alibaba’s cloud computing arm, Aliyun, and CAS that was established in 2015. According to Pan Jianwei, who also serves as its chief scientist, the team will “undertake frontier research on systems that appear the most promising in realizing the practical applications of quantum computing.” Their pursuit of quantum computing will take advantage of “the combination of the technical advantages of Aliyun in classical calculation algorithms, structures and cloud computing with those of CAS in quantum computing, quantum analogue computing

---

[18] “Present Status and Development Trends of Quantum Computers” [量子计算机的发展现状与趋势], CAS, 2010, http://www.bulletin.cas.cn/ch/reader/view_full_html.aspx?file_no=20100507&flag=1

[19] Zhu Lixin, “Progress made in development of quantum memory,” *China Daily*, August 20, 2016, http://usa.chinadaily.com.cn/epaper/2016-08/20/content_26559829.htm

[20] “China Successfully Develops Semiconductor Quantum Chip,” Chinese Academy of Sciences, August 12, 2016, http://english.cas.cn/newsroom/news/201608/t20160812_166433.shtml.

[21] “China Makes New Breakthrough in Quantum Communications,” Chinese Academy of Sciences, August 26, 2016, http://english.cas.cn/newsroom/mutimedia_news/201608/t20160826_166818.shtml.

[22] “Our Nation’s Scholars Achieved the “Fastest” International Quantum Control, Laying the Foundation for Multi-Bit Quantum Computing” [我国学者实现国际“最快”量子控制 为多比特量子计算基础], *Xinhua*, October 26, http://www.81.cn/gnxw/2016-10/26/content_7328567.htm

[23] “Pan Jianwei: “Quantum Supremacy” Will Become a Milestone in Physics and Computer Science” [潘建伟:"量子称霸"将会成为物理学和计算机科学的里程碑], *Science and Technology Daily* [keji ribao | 科技日报], November 6, 2016, http://www.stdaily.com/index/kejixinwen/2016-11/06/content_310018.shtml

and quantum artificial intelligence, so as to break the bottlenecks of Moore's Law and classical computing."[24] For quantum computing, the Alibaba Quantum Computing Lab has articulated equally ambitious goals. Their team seeks by 2020, to achieve the coherent manipulation of 30 qubits; by 2025, to develop quantum simulation with calculation speeds that match those of today's fastest supercomputers; and by 2030, to succeed in the "comprehensive realization of common-use quantum computing functions" through a quantum computer prototype with 50 to 100 qubits.[25]

Quantum Cryptography and Communications

The launch of the world's first quantum satellite, *Micius* (墨子) in August 2016 drew international attention to the PRC's rapid progress in quantum communications.[26] *Micius* established a quantum key distribution network with the transmission of quantum information between the satellite and multiple ground stations. [27] This recent launch is a component of Quantum Experiments at Space Scale (QUESS), a roject initiated in 2011, which has involved collaboration between a team led by leading Chinese quantum scientist Pan Jianwei from the University of Science and Technology of China (USTC), the Chinese Academy of Sciences (CAS), and the Austrian Academy of Sciences. The *Tiangong*-2 space station, launched in September, will also engage in quantum key distribution experiments.[28] As of mid-October, *Micius* was reportedly in good condition, with experiments ongoing and expected to be completed in November.[29] The satellite has successfully completed links with multiple ground stations, as well as teleportation optical links. *Micius* is only the first of what Chinese scientists

---

[24] "Aliyun and Chinese Academy of Sciences Sign MoU for Quantum Computing Laboratory," Alibaba, July 3, 2015, http://www.alibabagroup.com/en/news/article?news=p150730

[25] 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. "Chinese Academy of Sciences - Alibaba Quantum Computing Lab" [中国科学院—阿里巴巴量子计算实验室挂牌], Chinese Academy of Sciences, September 2, 2015, http://www.bsc.cas.cn/gzdt/201509/t20150902_4419884.html.

[26] "China Will Establish a Global Quantum Communications Network By 2030" [中国将力争在2030年前后建成全球量子通信网], *Xinhua*, August 16, 2016, http://news.sina.com.cn/c/sd/2016-08-16/doc-ifxuxnpy9658879.shtml.

[27] Ibid.

[28] "Tiangong-2: Lays a Foundation for China's Space Station Age" ["天宫二号"：奠基中国空间站时代], *People's Daily*, September 18, 2016, http://military.people.com.cn/n1/2016/0918/c1011-28720954.html

[29] "Our Nation's Quantum Satellite Smoothly in Orbital Testing, Will Start Scientific Testing in Mid-November" [我国量子卫星在轨测试顺利 11月中旬开始科学实验], *Xinhua*, October 12, 2016, http://www.81.cn/jwgz/2016-10/12/content_7297405.htm

intend will be a future constellation of multiple quantum satellites.[30] According to Anton Zeilinger of the University of Vienna, one of the lead scientists involved in the project, this is not only the initial test of the feasibility of quantum communication via satellite but also constitutes a "a very significant step towards a future worldwide quantum internet."[31]

The *Micius* satellite reflects the culmination of nearly two decades of steady progress on free space quantum teleportation, which uses the transmission of quantum states "over-the-air" to distribute quantum cryptographic keys. In 2005, Pan Jianwei's team first confirmed the feasibility of a quantum satellite in the world's first free space quantum communications experiment.[32] Since then, Chinese scientists have progressively increased the distance at which free space quantum communications can be operationalized, breaking several world records in the process. In 2010, a team of researchers from Tsinghua University and USTC published a paper describing their successful demonstration of quantum teleportation across 16 kilometers of free space.[33] Then, in 2012, Pan Jianwei and his colleagues demonstrated successful quantum teleportation and entanglement across 100-kilometer free-space channels.[34] These experimental achievements have since extended beyond the laboratory, with the launch of *Micius*, and this gradual, sustained progress in techniques for quantum entanglement and quantum teleportation continues. In September 2016, a paper by Pan Jianwei and his team described their success in the "full" quantum teleportation of photons through an optical fiber network 12.5 kilometers apart, such that the teleported photons were destroyed in one laboratory and recreated in another.[35] This research reportedly constitutes a notable step towards the development of a future "quantum Internet," which would be radically more secure than existing systems.

---

[30] "China Will Establish a Global Quantum Communications Network By 2030" [中国将力争在2030年前后建成全球量子通信网].

[31] "China launches world's first quantum science satellite," Physics World, August 16, 2016, http://physicsworld.com/cws/article/news/2016/aug/16/china-launches-world-s-first-quantum-science-satellite

[32] Cheng-Zhi Peng et al., "Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication," *Physical Review*, April 22, 2005, http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.94.150501

[33] Matthew Luce, "China's Secure Communications – A Quantum Leap," *China Brief*, August 19, 2010. Xian-Min Jin et al., "Experimental free-space quantum teleportation," *Nature Photonics*, May 16, 2010, http://www.nature.com/nphoton/journal/v4/n6/full/nphoton.2010.87.html

[34] Xian-Min Jin et al., "Experimental free-space quantum teleportation," *Nature*, August 8, 2012, http://www.nature.com/nature/journal/v488/n7410/full/nature11332.html

[35] Qi-Chao Sun et al., "Quantum teleportation with independent sources and prior entanglement distribution over a network," *Nature Photonics*, September 19, 2016, http://www.nature.com/nphoton/journal/v10/n10/full/nphoton.2016.179.html

Concurrently, since ground-based fiber-optic quantum communication networks have reached a much more advanced stage than their free space counterparts, the Chinese leadership is engaged in a massive effort to operationalize these technologies in order to secure their most sensitive networks. In 2009, USTC's CAS Key Laboratory of Quantum Information (量子信息重点实验室) established what it characterized as the world's first "quantum government network" (in Wuhu, Anhui.[36] Notably, in 2012, for the 18th Party Congress, Pan led a team of researchers to create quantum communications networks that securely connected the venue hosting the meeting, the delegates' hotel rooms, and *Zhongnanhai*.[37] At the local level, metropolitan quantum communication networks have been constructed in Hefei and Jinan.[38] As of 2016, Tianjin also planned to establish a metropolitan-level quantum encryption communication network in order to enhance the city's level of cyber security.[39]

At a larger scale, China has been building and will soon complete the world's largest ground quantum optical fiber communications system. The "Quantum Beijing-Shanghai Trunk" (量子京沪干线) will stretch approximately 1,240 miles between Shanghai and Beijing.[40] This project was enabled by prior research under the 863 Plan involving the demonstration of an integrated quantum communication fiber optic network.[41] According to Pan Jianwei, who is involved in the project, this quantum communications network will be used for the secure transmission of

---

[36] "USTC Establishes the First Quantum Government Service Network in Wuhu" [**中国科技大学在芜湖建成首个量子政务网**], *Guangming Daily*, May 20, 2009, http://www.gov.cn/fwxx/kp/2009-05/20/content_1319699.htm

[37] Yu Dawei, "In China, Quantum Communications Comes of Age," *Caixin*, February 6, 2015, http://english.caixin.com/2015-02-06/100782139.html

[38] "Hebei Establishes the First Metropolitan Quantum Communications Testing Demonstration" [合肥建成首个城域量子通信试验示范网Science Net, February 21, 2012, http://news.sciencenet.cn/htmlnews/2012/2/260041.shtm. "Jinan Quantum Communications Test Network" [*Jinan liangzi tongxin shiyanwang* | 济南量子通信试验网], Shandong Quantum CTek, November 21, 2013, http://www.quantum-sd.com/index.php?m=content&c=index&f=show&catid=3&l=1&id=5.

[39] "Tianjin Will Build a Quantum Secret Communications Metropolitan Network" [天津将建量子保密通信城域网], *Tianjin Daily*, July 22, 2016, http://www.tianjinwe.com/tianjin/tjsz/201607/t20160722_1031311.html.

[40] ""Quantum Beijing-Shanghai Backbone" To Be Built This Year, Quantum Internet Can Be Expected" ["量子京沪干线"今年建成"量子互联网"可期], *Xinhua*, March 3, http://news.xinhuanet.com/politics/2016lh/2016-03/03/c_1118225683.htm.

[41] "National 863 Project "Optical Fiber" Quantum Communication Integrated Application Demonstration Network" Project Successfully Received Acceptance" [国家863计划"光纤量子通信综合应用演示网络"项目顺利通过验收], SAICT, November 23, 2015, http://www.saict.org/kygl/kyjz/11/35053.shtml

information in government, finance, and other sensitive domains.[42] Within the next several years, the "Beijing-Shanghai Trunk" may be expanded nationwide and linked with multiple metropolitan-level quantum communications networks. China intends to create a quantum communications network between Asia and Europe by 2020 and ultimately a global network in 2030.[43] Future quantum communications networks will probably involve both terrestrial wide area networks and quantum satellites linked with ground stations.[44]

Quantum Sensing

Within a longer timeframe, various forms of quantum sensing, including quantum radar, may take advantage of quantum entanglement to enable highly sophisticated detection of targets, regardless of stealth.[45] Notably, in September 2016, a team of Chinese scientists from China Electronics Technology Group Corporation's (CETC) 14th Research Institute's Intelligent Sensing Technology Key Laboratory (智能感知技术重点实验室) publicized their progress towards creating a single-photon quantum radar that is capable of detecting targets up to 100 kilometers away with improved accuracy.[46] Their research was undertaken in collaboration with a team led by Pan Jianwei from the University of Science and Technology of China, CETC's 27th Research Institute, and Nanjing University.[47] The reported range of this quantum radar,

---

[42] Quantum Beijing-Shanghai Backbone" To Be Built This Year, Quantum Internet Can Be Expected" ["量子京沪干线"今年建成"量子互联网"可期].

[43] "China to build global quantum communication network in 2030," *Xinhua*, November 2, 2014, http://news.xinhuanet.com/english/china/2014-11/02/c_127169705.htm.

[44] "Our Nation Will Strive to Construct a Quantum Communications Network Around 2030" ["我国将力争在2030年前后建成全球量子通信网], *PLA Daily*, http://jz.chinamil.com.cn/n2014/tp/content_7209383.htm.

[45] In general, there are three primary forms of quantum radar, single-photon quantum radar (单光子量子雷达), interferometric quantum radar (干涉式量子雷达), and quantum entanglement radar (以及纠缠态量子雷达) that may be under development by Chinese scientists. Although there is limited information available, there have been patents filed for a "laser radar based on the principle of strongly correlated quantum imaging," quantum radar and target detection methods, and a "quantum entanglement radar."

[46] "The Coming of the Quantum Radar That Makes Stealth Fighter in Profile" [让隐形战机显形的量子雷达来了], *Science and Technology Daily*, September 13, 2016. "China's First Single-Photon Quantum Radar Successfully Developed," [中国首部单光子量子雷达系统研制成功], CETC, September 18, 2016, http://www.cetc.com.cn/zgdzkj/_300931/_300939/445284/index.html

[47] "CETC's First Single-Photon Quantum Radar System Successfully Developed" [中国电科首部单光子量子雷达系统研制成功], CETC 14th Research Institute, September 7, 2016, http://wmdw.jswmw.com/home/content/?1174-3887947.html.

which takes advantage of entanglement between photon pairs, is supposedly five times that of a laboratory prototype jointly created last year by an international team of researchers.[48]

Since the research openly published and available in international peer-reviewed journals likely only reflect a limited subsection of this research, it is difficult to evaluate the progress of this aspect of China's advances in quantum technology, especially the potential military applications, which may remain highly classified. For instance, CETC's release of information regarding its quantum radar may have been an overstatement or understatement of its actual capabilities. Potentially, the announcement of this advance in official media might have been intended as a signaling mechanism.[49] Nonetheless, the possibility that certain aspects of Chinese research on the military applications of quantum science could have advanced further than has been disclosed cannot be wholly discounted.

Part III. Comparing Chinese and United States Advances in Quantum Information Science:

The United States was once the leader in quantum information science, but the lack of funding, structural and institutional issues, and lack of government coordination have reduced both the levels and consistency of support that are necessary to maintain capacity in this critical research area. The resulting void has caused the locus of research in certain quantum information science areas – most notably quantum cryptography – to shift to other countries where funding and support for basic research are more reliable.

Among the major limitations that the U.S. faces is the lack of high-level or long-term R&D plans and of a more comprehensive approach to scientific funding. China's current quantum information science programs reflect an "all-of-government" approach, whereas the White House has noted the lack thereof in the U.S. as a key factor for why the United State's funding levels are inconsistent. Indeed, China's quantum information science program is proceeding in lock-step with larger, national R&D and informatization plans, with a corresponding long-term strategy for commercialization of these technologies. This approach allows for more consistent levels of funding over time and is a clarion call to any scientists who hope to acquire funding for basic research - a mainstay for their careers.

---

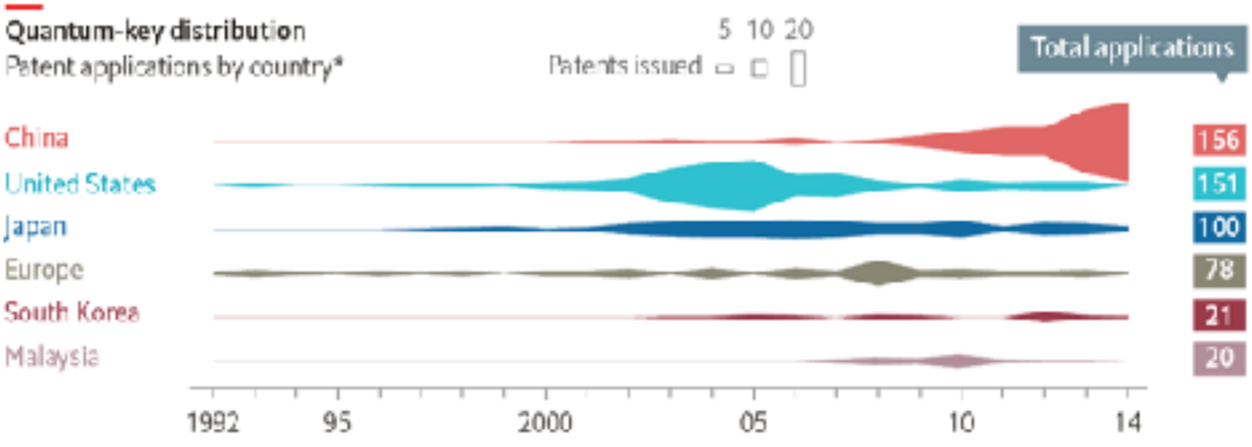
[48] "New research signals big future for quantum radar," Phys.org, February 26, 2015, http://phys.org/news/2015-02-big-future-quantum-radar.html.

[49] "Quantum Radar: "Clairvoyant" with Insight into the Future Battlefield" [量子雷达：洞察未来战场"千里眼"], *PLA Daily*, September 22, 2016, http://jz.chinamil.com.cn/n2014/tp/content_7271314.htm.

Overview:

One report from Massachusetts Institute of Technology (MIT) in 2015 reviews the state-of-play for emerging technologies, quantum included, and notes the U.S. lead has slipped considerably.[50] The report, titled "Future Postponed" studied critical areas where the United States was losing its technological dominance and leadership. The study suggested that a reduction in R&D funding threaten an "innovation deficit" with the U.S. lagging behind in emerging technologies. Quantum information science was listed as one of these critical areas, with the report noting that "U.S. leadership is not assured, especially given recent budget constraints, while the potential outcomes seem quite important both strategically and commercially."

A recent feature by the *Economist*, which offers a more comprehensive look at the state-of-the-art of quantum information science and comparative efforts internationally, gives useful metrics in the shift of QIS innovation to China.[51] While the U.S. has made considerable advances in quantum computing, encryption, and sensing, the economist report show the overall pace of innovation has slowed allowing other countries like China to catch up and in some ways pass the U.S. China's rapid advances in quantum encryption, for instance, are demonstrated below. The increase in patent applications is a function of increased funding and meaningful indicator for progress in Chinese programs, which, in this author's view has surpassed that of the United States.



Quantum-key distribution
Patent applications by country*

Sources: UK Intellectual Property Office; European Commission

*By location of corporate headquarters

---

[50] A Report by the MIT Committee to Evaluate the Innovation Deficit, "Future Postponed: Why Declining Investment in Basic Research Threatens a U.S. Innovation Deficit," April 2015, https://dc.mit.edu/sites/default/files/Future%20Postponed.pdf

[51] "Here, There, and Everywhere," *The Economist*, March 9, 2017, http://www.economist.com/technology-quarterly/2017-03-09/quantum-devices

Limitations on Progress in U.S. Quantum Information Science

A 2016 White House report titled "Advancing Quantum Information Science: National Challenges and Opportunities" gives an overview of the state of federally-funded quantum information science programs and challenges that remain in further progress in the field.[52] In addressing why this gap has narrowed, the report's recommendations provide a useful framework to compare the role of U.S. and Chinese structural and institutional factors.

According to the report, there are five major factors that need to be addressed to solidify and further U.S. dominance in this field: institutional boundaries within academic institutions, education and workforce training, technology and knowledge transfer, materials and fabrication, level and stability of funding. While a more comprehensive analysis of these factors in the context of U.S.-China economic and strategic competition is beyond the scope of this testimony, there is one factor in particular stick out as areas where China has a distinct advantage compared to the United States: stability of funding.

The report states that significant progress in quantum information science in the U.S. has been hindered by long-standing instability in both level and consistency of R&D funding. This has "negatively impacted both the pace of technical progress and development of a QIS workforce." According to the report:

> *Fluctuations in Federal and other U.S. funding led to discontinuities in university-based research programs and contributed to promising young as well as senior researchers choosing to pursue alternate careers or look for opportunities outside the United States.*

The lack of consistent funding at home, coupled with ample Chinese funding abroad, may persuade researchers to collaborate with China on larger projects or pursue their research in Chinese institutions. Inconsistency of funding in European institutions in part led to China's most prestigious and ambitious project to date, *Micius*, the world's first quantum satellite. Pan Jianwei, father of Chinese quantum information science and lead on the satellite project, partnered with his mentor and erstwhile rival, Austrian Scientist Anton Zeilinger. Although Zeilinger had the technical know-how and expertise, he had been unable to secure funding in Europe to launch and

---

[52] National Science and Technology Council (NSTC), "*Advancing Quantum Information Science: National Challenges and Opportunities*," July 22, 2017, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22 final.pdf

operate a quantum satellite.[53] Pan's connections with the Chinese Academy of Sciences (CAS) proved beneficial, and the satellite only became a reality through Chinese state funding.

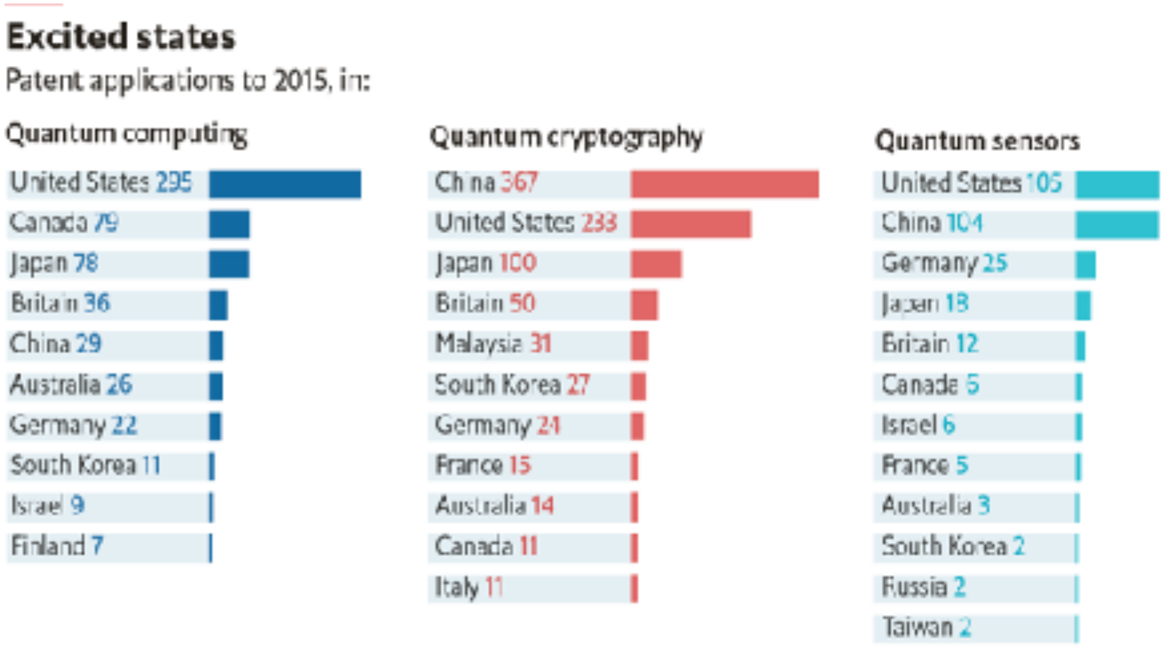
It should be noted that these factors do not account for the substantial advantages the U.S. enjoys over China in the area of overall quality and number of academic institutions, venture capital investment, industrial and technological base, and quality and speed of private innovation. However, these advantages are narrowed considerably by China rising economic dominance, multiple forms of tech transfer, talent recruitment programs, and comprehensive state-level R&D funding programs. Despite structural disadvantages in state-level funding, the United States has seemingly maintained its lead in quantum information science in general, but, as noted, this gap is narrowing.

Comparisons of U.S. and Chinese Progress

There is a general sense that China missed the first "information revolution" in the first Gulf War and has since struggled to catch up and surpass the United States. The leapfrogging strategy it has employed that uses a combination of state investment, technology transfer, and espionage has enabled only limited success in realms where the U.S. had traditionally been dominant, such as information technologies. This may not hold true for quantum. As such, quantum information science is one area where China feels it has a strategic advantage, and its leapfrogging strategy may pay off in commercial and military contexts. This has so far been true for quantum encryption, but it's unclear if that same success can be found in computing and sensing, which present different technical challenges.

---

[53] Elizabeth Gibney, "Chinese satellite is one giant step for the quantum internet," *Nature*, August 16, 2016, http://www.nature.com/news/chinese-satellite-is-one-giant-step-for-the-quantum-internet-1.20329



In quantum computing, China lags behind the United States both in progress as well as scale and size of effort, according to information available in open sources. The joint Alibaba-CAS effort is still nascent and is behind more mature efforts on the part of D-Wave (backed by In-Q-tel), Google, IBM, NASA, and LogiQ (an IARPA effort). This doesn't account for sizable efforts from Europe and the U.K. Unlike the quantum encryption program, it's not clear if academic exchanges, cooperation, and increased R&D investment will breed the same success in quantum computing as it has in quantum encryption. This begs the question whether China will have to pursue other means to achieve advances such as increased infusion of venture capital, foreign mergers and acquisitions, or commercial espionage. China benefits from high-levels of state funding and a growing venture capitalist market that is behind that of the United States. This is one area where the United States has a distinct financial advantage. The clear market applications of quantum computing have driven substantial amounts of private investment in these areas. As China's private investment ecosystem continues to mature, however, this U.S. advantage may narrow considerably.

China is the preeminent leader in quantum encryption and communication technologies. The combination of state R&D investment, academic exchanges, and commercial applications have placed it ahead of the United States. In the last few years, Chinese researchers have taken steps to overcome the very real technical and logistical hurdles preventing practical use of quantum encryption. In the last year alone, Chinese researchers have been able to execute "measurement device independent" quantum key distribution (MDI QKD) to overcome a potential vulnerability and have also solved the so-called "nocturnal problem" which limited free-space communication's use to nighttime.[54] China appears to be resolving the problems of scale and complexity endemic to large-scale quantum key distribution through creating a national quantum key distribution network that allows critical infrastructure companies, government agencies, and the military to plug in for their own super-secure quantum encryption networks.

Quantum sensing is perhaps the most unknown of these technologies, in terms of both the technological hurdles China may or may not have been able to surmount and how these efforts compare to those of Western nations like the United States. What is known is that both nations appear to recognize the applications that these technologies have in both commercial and military realm. While China claims to have tested the world's first quantum radar, it's not clear whether Chinese researchers have yet been able to surmount the technical problems that limit the technology's range and reliability. Otherwise, the United States and other Western countries, such as the United Kingdom certainly have an advantage in this area, already having realized basic quantum sensors for use in commercial and military applications.

Part IV. Strategic Considerations:

The balance of power between the U.S. and China is due in part to the former's long-held preeminence in information technologies and technological innovation. Indeed, the United States is the birthplace of information technologies, the Internet, and both the civil and military information revolutions. China's rise as a leader in quantum and related emerging technologies would therefore signal an eastward shift in the locus of international innovation.

This testimony focuses largely on the military and strategic implications of China's quantum information science efforts. However, the economic impact these technologies are likely to have once matured and commercialized is substantial enough to have major implications for strategic competition. It is clear that for each of these technologies, the first-to-market advantage will be immense. For quantum computing in particular, any nation which first develops a general purpose, large-scale quantum computer will have nearly intractable market dominance, able to offer a high-powered, big data solution that are equally applicable in all industries where processing power would be useful. There are already commercially available solutions for quantum encryption to secure data at rest, and limited solutions for protecting data in transit. The effects in quantum sensing will be comparatively much less pronounced in the commercial domain, and may hold higher dividends in scientific research. The exact of quantum sensors

---

[54] Stephen Chen, "Chinese scientists solve quantum communication's 'nocturnal curse', paving way for sending of secure messages 24/7," *South China Morning Post*, January 3, 2017,http://www.scmp.com/news/china/article/2054219/chinese-scientists-solve-quantum-communications-nocturnal-curse-allowing

commercial applications are not fully clear, though may extend to oil-drilling, resource detection, neurology, and other areas. Due to the relative immaturity of these commercial markets, there doesn't appear to be currently substantial threat from China in usurping U.S. dominance in these areas.

If the United States does not maintain or regain its edge in these vital areas in the context of the pace and scale of China's research, China may eventually edge out the United States and dominate commercial sales of these technologies. This would be a major paradigm shift in today's information technology environment, where the locus of power is firmly planted in the United States.

Quantum Computing

Quantum computing may play a significant role in military strategy by virtue of its potential to provide a substantial source of portable processing power. Increasingly, military strategists and planners recognize that data processing may become one of the foremost resources for warfighting in the near future – comparable in importance to the role that data plays in today's information age, and the role that oil, coal, wind, and horsepower have played in previous eras of warfare.

The information age, which has put a premium on collection, processing, a dissemination of data and intelligence, may subside as traditional reliable areas of collection such as computer network and electromagnetic spectrum become more contested or unavailable through technical means. Quantum encryption, information security, and quantum sensors only accelerate this trend further. A corresponding increase in processing power brought through advancements in quantum computing and classical computer science will shift the focus of military advantage towards speed, precision, and timeliness of analysis and action in a limited information resources environment. Indeed, as a brilliant colleague of mine, Peter Mattis once observed, "analysis is the tool of last resort when efforts to collect the necessary information for decision-making have failed. Regardless of whether analysis sifts signals from noise or connects the dots, analysis attempts to provide by inference what cannot be known directly." As we shift from the current information age to a machine age of warfare, these dynamics will become more pronounced. In this regard, the portable processing power of quantum computing coupled with artificial intelligence represents a critical capability in this new paradigm.

Finally, though valid, concerns over quantum computing's ability to crack modern-day encryption are largely overblown. While estimates vary considerably, experts predict the first general purpose quantum computer will not be made available at least within the next decade, allowing standard bodies, public, and private sector plenty of time to innovate new methods that put encryption beyond quantum's reach. If anything, the rapid advancement of quantum computers demonstrate the need to move on to quantum resistant forms of encryption sooner rather than later. As such, military communications should use quantum-resistant encryption at a bare minimum, and operate at wider bandwidths to accommodate for less-efficient, though more secure algorithms.

Quantum Encryption and Communication

The widespread adoption of quantum encryption and communication would undercut U.S. advantages in intelligence surveillance and reconnaissance, potentially shielding some Chinese forces from intelligence collection. This would be especially pronounced in military signals intelligence, particularly of Chinese maritime operations in the East and South China Seas. Chinese space-based quantum communications networks enabled by satellites like *Micius* would ideally allow eavesdrop and hack-proof communications worldwide. This type of shield could extend to closed Chinese government and military fiber-optic networks, providing additional obstacles to executing computer network exploitation of these targets for strategic and operational intelligence and, more hypothetically, presenting a barrier to certain forms of computer network attack. The real operational implications of quantum encryption are unclear as a majority of these technologies are untested in a military context and have yet to be implemented in any practical way.

Utilizing these technologies does come with tradeoffs. It's not clear how quantum encryption would hold up in an operational context. The systems upon which it relies tend to be fragile and delicate. Quantum communications are also highly vulnerable to disruption and jamming as they relies on sensitive detection mechanisms to work properly. While there are methods to mitigate against jamming, they are unproven experimentally. Therefore, for radio communications and free-space quantum key distribution, these networks may only be useful for peacetime purposes and unable to meet the hard realities of an electromagnetically contested environment expected during war and conflict. For its part, the U.S. Air Force believes that both quantum encryption and communications "yield limited benefit...while adding significant complexity."[55] Quantum encryption "provides little advantage over the best classical alternatives."

---

[55] USAF Scientific Advisory Board, "Utility of Quantum Systems for the Air Force," August 19, 2016, http://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230.

Also, as noted before, the vulnerabilities of encryption - or any form of secure technology - are not derived from the theoretical concepts underpinning the technology, but rather the reality of their implementation. These systems would still be vulnerable to social engineering, side-channel attack, software vulnerabilities, and other forms of computer espionage that do not directly target the physical properties that give quantum encryption its advantage. SANS Institute perhaps put it best, stating:

> *Long encryptions keys might be compared, in military terms, to a mile-high mountain that that has an enemy behind it. The attacking army could go straight over the mountain to reach the enemy, or it might attack by going around the mountain. It has been said that quantum cryptography merely creates a higher mountain, and that the enemy has been concentrating for a long while not on defeating encryption schemes, but in attacking in other ways.*[56]

Despite these problems, there is no doubt that quantum encryption would hinder a highly-sophisticated, large-scale, global intelligence surveillance regime like that of the United States, if implemented at sufficient scale.

Quantum Sensing

As the electromagnetic spectrum becomes potentially crowded in times of peace and contested in times of war, the ability to ensure trust in sensors and operate independently of the spectrum's limitations will be critical. The Air Force Scientific Advisory Board specifically points out quantum clocks and quantum sensors as two areas that warrant further investment. The study states, "Better timing precision would enhance Air Force missions/capabilities such as signals intelligence (SIGINT), counter-DRFM (digital radio frequency memory), electronic warfare (EW), and more robust communications."[57] Regarding quantum magnetometers, which enable quantum navigation, the study states that "[these] sensors can be an important part of achieving GPS-denied advantage. Quantum inertial sensing (e.g., cold atom IMUs) can provide extremely low drift rates and is not susceptible to jamming."

Quantum imaging, a related technology to quantum radar just focused on the visible range, can substantially increase satellites optics, either for space object surveillance and identification

---

[56] Bruce R. Auburn, "Quantum Encryption–A Means to Perfect Security," *SANS Institute*, 2003, https://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986

[57] USAF Scientific Advisory Board, "Utility of Quantum Systems for the Air Force," August 19, 2016, http://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230.

(SOSI) or ground-based target tracking. The technology is able to reduce noise and loss caused by debris and weather. Researchers from the University of Missouri have suggested that these type of quantum sensors can be operationalized for use in the both space and maritime domains.

Quantum radar, which China claims to have developed, could overcome superior U.S. stealth capabilities if operationalized, enabling the PLA to undermine this critical pillar of U.S. military power. The commentary in PLA media at the time highlighted quantum radar as the “nemesis” of today’s stealth fighter planes that will have “remarkable potential” on the future battlefield.[58] Additionally, other, more theoretical descriptions of quantum radar suggest that it would be able to defeat radar jamming techniques such as digital radio frequency memory (DRFM) jammers which spoof a radar’s broadcasted signal to conceal an aircraft’s true location. However, it remains difficult to evaluate the timeframe within which quantum sensing will become a reality beyond the laboratory in a military context or whether that would be made known in open sources.

Part V. Conclusion and Final Thoughts:

The United States cannot allow itself to fall behind in these critical emerging technologies. Simply to stay competitive, the United States needs to keep ahead or apace of Chinese efforts for scientific, academic, commercial, and military applications. Due to the pace of innovation and economy, the first-to-market advantage here is exponential and will yield near intractable market dominance. The United States is already challenged by the industrial might and growing human resource base of China’s emergence on the world stage. Some of the few, though critical, advantages the United States possesses is dominance in emerging technologies, world-class academic and research institutions, and a central position in information and Internet technologies. If continued Chinese investment in these areas are not met with an appropriate U.S. response, these factors will shift, likely at the expense of the United States, and the strategic balance of power will continue to tilt in China’s favor.

This is not a call for the U.S. to deny Chinese researchers access or to take punitive action against Chinese firms. Rather, it’s a clarion call that the United States should leverage its advantages to restore itself as the innovation powerhouse in this area as it has in many other areas in the past. The shift towards China for quantum information science isn’t the end result of intellectual property theft, espionage, or mergers and acquisition; rather, it largely reflects the high-level support from government, high and consistent levels of funding, and a corresponding

---

[58] “Quantum Radar: “Clairvoyant” with Insight into the Future Battlefield” [量子雷达：洞察未来战场“千里眼”].

lack of these forces in Western countries, including the United States. If these systemic factors are corrected, the U.S. may restore its traditional leadership in this critical technological domain.

To remain dominant in the current information age and coming machine age of warfare, the U.S. military will need to find ways to integrate these technologies where appropriate and establish new technological and operating paradigms to adapt to the potential disruptive changes they bring. This requires staying ahead of foreign efforts, monitoring their progress, and ensuring procurement, acquisition, and planning are properly preparing for contingencies where these technologies are use.

Finally, it is apparent that the golden age of intelligence is likely over. Quantum encryption is just one example of many that show the growing lockdown and securitization of information flows that U.S. national security community and military have taken for granted and leveraged to great effect. Quantum sensing, in its way, also accelerates this trend further. The United States will need to adapt to an information-denied environment both in peace and conflict, one that with lowered quantity, quality, granularity, and actionability of information. This puts a premium on processing power and analysis, highlighting why the United States needs to maintain its dominance in quantum computing, artificial intelligence, and machine learning - all of which are critical technologies for this capability.

Part VI. Recommendations:

Technological innovation is at the center of military strength, economic competitiveness, industrial might in the calculus of national power, as evident in the case of quantum technologies. U.S. Congress should first seek to understand the disruptive effects of these technologies and where the U.S. progress stands in comparison to its most important strategic competitors, such as China and Russia. Where possible, the United States should seek to encourage public private partnerships, strategically apportion state-level R&D funding in pursuit of strategic goals, and enable a regulatory environment that guides and supports rather than quashes innovation. The overall intent of this should be to restore and ensure the U.S. lead in technological innovation and military capability.

My recommendations are as follows:

(1) U.S. Congress should leverage tools already available to it to better understand emerging technologies in general, and quantum in particular. Congress should direct the Government Accountability Office (GAO) to prepare a comprehensive technology assessment to study the

impact of quantum information science, current areas of federal R&D funding, potential commercial applications, ability for U.S. to maintain its technological edge, and potential legislative and policy options. In the military realm, Congress should direct the Department of Defense's (DoD) Office of Net Assessment (ONA) to conduct a study on strategic implications of widespread adoption of quantum technologies on the part of potential adversaries, including China. In the long term, it may be worth directing the DoD to prepare a yearly report to Congress on status of emerging and disruptive technologies like quantum and artificial intelligence and their potential impact on U.S. operational capabilities.

(2) Congress should consider funding more public-sector research that can shed light into China's development of emerging technologies in the disciplines of cybersecurity, quantum information science, machine learning, and artificial intelligence, for both commercial and military use. Currently, there does not exist a public-interest think-tank on the scale of China Maritime Studies Institute (CMSI) or China Aerospace Studies Institute (CASI) that conducts and publishes public research focused on these information and intelligence aspects of China's rise. For an issue that has received so much attention and stands at the center of U.S. and China strategic balance, policy and public debate should not be so limited by a dearth of information. Congress should direct the Department of Defense or the U.S.-China Economic and Security Review Commission to partially or fully-fund a think-tank by which to study these issues more comprehensively both for the U.S. government as well as the public interest.

(3) Congress should consider restoring funding to the Office of Technology Assessment (OTA), which between 1972 and 1995 assisted Congress by providing in-depth assessments of emerging technologies and relevant, comprehensive legislative and policy options for lawmakers. Current congressional support agencies like the GAO and the Congressional Research Service (CRS) have not been able to fully fill the void in technical expertise left by OTA. Think-tanks, private institutions, and lobbyists offset this lack of expertise to some degree, but are unable to provide the same level of peer-reviewed assessment with the comprehensiveness, timeliness, and depth that OTA once provided. It should be noted that while Congress has reduced this role, other nations, including China, have promoted the role and influence of parliamentary science and technology advisory bodies. For China at least, this approach has has paid considerable dividends in apportioning state funds towards R&D efforts in support of long term economic and military objectives.

(4) U.S. Congress should direct the Federal Government to establish an interagency Commission for Investment in Strategic Emerging Technologies (CISET) that will be better able to appropriately assess U.S. R&D funding efforts, deliver recommendations to Congress, and

coordinate amongst relevant federal agencies in investment into strategic technologies. The White House has previously acknowledged that U.S. progress in quantum information science is limited due in part to institutional boundaries as well as an inconsistency in funding and opportunities for research in this field, largely stemming from poor interagency coordination and lack of unitary direction. Formalizing interagency working groups and giving them the oversight and support of Congress would allow for greater synergy in budgeting for and achieving long-term strategic technological goals and ensuring continued U.S. dominance in these fields. More importantly, it would restore consistency in funding and employ a "whole of government" planning, nullifying advantages of the Chinese approach.

Challenges in tech transfer, recruiting top talent overseas, and workforce and education programs have also been cited as systemic issues that are holding back U.S. efforts in quantum information science. These components strike at the heart of U.S. technological and strategic dominance and are dependent on a complex array of social, financial, and political factors. This reality makes policy recommendations particularly difficult. As such, these issues warrant further study before any sort of concrete recommendations can be proposed to address them in the context of bridging gaps in U.S. development of quantum information science.