A nation’s success in military operations often rises and falls on the basis of how well it communicates. When a nation does not secure its communications effectively, its enemies intercept and read its communications and win thereby military and diplomatic advantages.¹

Vice Admiral Noel Gayler, former director of the National Security Agency, once wrote, “Important as it is in peacetime, communications security becomes even more important in wartime.”² For a few decades, nations have been relying on encryption systems to protect a wide variety of computerized transmissions ranging from commerce to government to mil-
itary communications. While today’s encryption systems are considered reasonably secure, the possibilities of quantum cryptography and quantum computing offer a whole new dimension and threat to computerized secrecy.

China is among a growing number of countries seeking to unlock the science of quantum cryptography and computing, which many experts believe will one day revolutionize computerized security. With China’s ongoing push to modernize its military and advancing to become a global innovative force, success in this area could materialize into an enormous economic and military advantage.

This article examines the significance of these technologies, China’s progress in quantum communication and quantum computing, and the consequences for the United States and other nations should the Middle Kingdom acquire a real capability in this science. It is an area that U.S. analysts will need to follow closely in the coming months and years.

China’s Leap
The world is currently in the midst of a second quantum revolution. The first quantum revolution began in 1900 when the new rules governing physical science were discovered. Today, in the second quantum revolution, these rules are being used to develop new revolutionary technologies. Two such possible technologies are quantum computing and quantum cryptography, the latter falling within the area of quantum communications. While they each rely on the properties of quantum physics, their end goals differ. Theoretically, a quantum computer would be able to break current encryption systems, but quantum cryptography is arguably unbreakable even by a quantum computer.

The Quantum Computer: Code Breaker or Problem Solver? The idea of creating a quantum computer has been around since the 1970s. These computers would be extremely powerful since they can harness quantum properties. Unlike an ordinary computer, which uses binary numbers (1s or 0s) to represent data, a quantum computer would use quantum bits (qubits), which can simultaneously have the value of 0, 1, or any “superposition” of the two. The quantum phenomenon becomes even more bizarre when considering the concept of “entanglement.” Entanglement links the properties of two or more qubits together. These qubits, even when separated, remain strongly correlated or interconnected in a manner much stronger than any classical relationship. This is what famed physicist Albert Einstein called “spooky action at a distance.”

A quantum computer using entangled qubits would therefore be vastly faster than the average computer, which uses simple binary numbers. Theoretically, once a quantum computer comes online, it would be able to break current encryption systems such as Rivest, Shamir, and Adleman (RSA), a commonly used computer encryption and authentication system that uses a complex algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. These encryption systems are needed to protect information such as financial transactions as well as military and government communications.

In 2001, Guo Guangcan, an academician of the Chinese Academy of Sciences, established the Key Laboratory of Quantum Information at the University of Science and Technology of China (USTC) in Hefei. The laboratory became “the most important research center of quantum information in the country.” In January 2006, while the field of quantum technology was still considered in its infancy in China, Guo predicted that the first quantum computer would likely be developed in the next 15 to 20 years. In 2007, Dr. Pan Jianwei, director of the Division of Quantum Physics and Quantum Information at Hefei’s National Laboratory for Physical Sciences at the Microscale, USTC, optimistically predicted that the country might be the first to develop a quantum computer. More recently, however, Pan seems to have shifted his focus. A 2010 article quoted him as saying that quantum communication is “more important for China because it is already closer to application” than developing a quantum computer, although the latter is still “very attractive to me.” If Pan really did shift his focus, it could be that the reality of the challenges involved with building a quantum computer had indeed set in.

Dr. Ivan Deutsch, professor and Regents’ Lecturer at the University of New Mexico, explained the difficulty in achieving a quantum computer. In quantum cryptography, which is explained more in depth below, the goal is to distribute two shared secret keys. Basically, the secret keys are created using the properties of quantum randomness. It works on a particle-by-particle basis. In other words, in quantum encryption one photon can be sent at a time. It is simple to control a single particle. Quantum computing, on the other hand, is much more complex because it deals with computation as opposed to the transmission of single photons. Computations require logic, and logic requires the use of many 1s and 0s that cannot be sent individually since each one is interdependent. Furthermore, each qubit needs to be in an entangled state simultaneously. Due to this added degree of complexity, quantum computing is much further away from realization than quantum cryptography.

Despite this apparent shift in interest from quantum computing to quantum cryptography, in February 2013, a Chinese report emerged touting a breakthrough in trying to achieve the quantum computer: “The solid-state quantum research crew from the University of Science and Technology of China succeeded in performing the quantum logic gate operation on one single electron at 10 picoseconds, renewing the previous world records by nearly 100 times.” Prior to China’s achievement, “U.S. and Japanese research institutes achieved the electrically controlled semiconductor logic gate at 1,000 picoseconds.”

China’s achievement, however, increased the operational speed by nearly 100 times to 10 picoseconds. According to Guo Guoping, director of the research project:
footstool in the global competition in the next-generation computer chips. . . . The quantum chip. . . . will make the quantum computer characterized by exponentially increased operational speed and greatly improved data processing capabilities.12

The ability to break current encryption systems makes modern day information vulnerable. Furthermore, an inherent risk to national security should a quantum computer come online would be its ability to access archived information previously protected by systems such as today’s RSA encryption. Dr. Jonathan Dowling, a professor and Hearne Chair of Theoretical Physics at Louisiana State University, explained that information encrypted using RSA could be intercepted and archived today in its encrypted format. Once a quantum computer is online, it could be used to break older archived encrypted data, possibly still classified.13

Carl Williams, chief of the Quantum Measurement Division of the National Institute of Standards and Technology, agrees that there are certain risks to quantum computers, but he adds that there are benefits as well, pointing out they could eventually solve problems of profound scientific and technical benefit. “If you ask me 100 years from now what the benefit of this technology is, I would probably say it is a societal benefit,” stated Williams.14

Quantum Communication: The Pursuit of the Perfect Encryption System. Encryption methods have evolved over time, becoming increasingly complex and difficult for an adversary to break. The trend in cryptography has evolved from traditional manual enciphered and deciphered codes to mechanical encryptions and computerized cryptography. Today’s top cryptography systems such as RSA and Pretty Good Privacy are considered highly secure. Breaking messages has become nearly impossible with the growing sophistication of today’s cryptography. However, experts believe it is only a matter of time before existing encryption systems are broken.

Currently there are projects in place to try to counter the threat of a future quantum computer. Post-quantum cryptography is a relatively new field in which research is conducted on public-key encryption systems, which are not breakable using quantum computers. Quantum cryptography (distinct from post-quantum cryptography) offers another way to try to counter the risks of a quantum computer coming online. This newest form of cryptography is based on quantum theory and is proving to be unbreakable.

Quantum key distribution (QKD), a process within the context of quantum cryptography, generates a random encryption key shared by the sender and recipient. The biggest advantage of QKD is that if a third party attempts to intercept it, the party will be detected and the secret message will not be sent. QKD deals with photon states and works as follows: Alice, Bob, and Eve are three fictional characters. In quantum cryptography, Alice wants to send a secret message to Bob. She has to first send him the key through the process known as QKD. This means she is sending him a series of photons in random quantum states. If Eve tries to intercept the message, it changes the quantum states of the photons.

QKD is already a reality, although limited in capability. A small number of commercial companies have offered quantum encryption systems. For example, the U.S.-based technology company MagiQ sold a system in 2003 called the Q-Box. The Q-Box is a single-photon-based system developed for further research related to QKD. These systems, however, are far from perfect and have had a limited distribution. Moreover, QKD can be sent either via fiber optic or through free space. Going through fiber optic cables, it generally cannot travel more than 50 kilometers (km) without a quantum repeater, which has not yet been developed.

China has touted a number of significant experiments in the area of quantum communication. For example, in 2004 the Key Laboratory of Quantum Information reportedly completed a 125-km fiber point-to-point QKD experiment. This experiment, according to Chinese reports, “solved the problem of stability in quantum cryptography systems.”15 These results are questionable, but not impossible. According to Carl Williams, “If I wait long enough and my fiber is perfectly dark and still, I can probably get a photon through at a longer distance than 50 kilometers.”

In a November 2005 article, China claimed to lead the United States, France, and Austria in quantum entanglement research when it provided an “experimental demonstration of five-photon entanglement and open-destination teleportation.”16 The more photons that can be successfully entangled, the higher the accuracy of the transmission.17

In 2006, China reported having fulfilled quantum teleportation of a two-particle system. Voting results at the Chinese Academy of Sciences showed that 565 academics chose it as the ninth most significant development that year in the country’s science-technology sector.18

In 2007, a report stated that China had created a quantum router, which they claimed was the first in the world. The router was said to have succeeded in encrypting data flowing between four computers on a commercial communications system. The router is different from point-to-point transmissions conducted in other parts of the world because it makes a quantum network possible.19

Then, in May 2009, a report emerged in the Chinese press claiming that the country had built the world’s first quantum encrypted government network and that its trial operation in Wuhu City, Anhui Province, served eight government departments in Wuhu.20

Scientists in China in 2012 reportedly teleported multiple photons 97 km across a lake within the country.21 This significant experiment puts China one step closer to achieving global transmission of quantum communications. Scientists would eventually like to use satellites to achieve global transmission of quantum communications. The distance that a quantum key can be sent through free space depends on which direction it is traveling. Traveling straight up toward space, it can go farther due to the integrated air mass (that is, the air becomes less dense). China recognizes that “by
using satellites, ultra-long-distance quantum communication and tests of quantum foundations could be achieved on a global scale.”

By 2016, China plans to launch the first “Chinese Quantum Science Satellite,” a satellite dedicated to quantum experiments, which according to China Daily would put the country ahead of both the United States and Europe. According to Pan, “The satellite will provide scientific answers to the feasibility of intercontinental quantum teleportation—to make it simple, whether I can talk to my friend in Vienna from Beijing on a quantum phone.”

Matthew Luce, a researcher with Defense Group Inc.’s Center for Intelligence Research and Analysis, thinks that because of important applications for satellites as well as the security level:

quantum communication technology figures centrally in the objectives of the Chinese military to upgrade their growing command and control capabilities. A functional satellite-based quantum communication system would give the Chinese military the ability to operate further afield without fear of message interception.

Furthermore, Luce points out that China’s research in quantum applications could help the country expose weaknesses in a network should the United States or another nation win the race in achieving the same technology.

A Military Perspective on Quantum Power

While the possibility of cracking quantum technology is often viewed by scientists in academia as a personal challenge—presenting a potential opportunity to receive a Nobel Prize or a patent—it is also viewed by militaries and governments as having great security potential and significant implications. In November 2012, for example, the U.S. Army News Service reported that scientists at the U.S. Army Research Laboratory were conducting research and development on data teleportation to one day achieve secure, tamper resistant security. According to Ronald Meyers, who is leading an Army project in collaboration with the Joint Quantum Institute at the University of Maryland at College Park, “The greatest potential that a quantum communications network holds for the Army is secure communications.” Meyers also contends, “Quantum computers will be able to easily decrypt communications that are currently secure. . . . That’s one reason why it’s vital for us to explore quantum encryption.” Meyers envisions a future in which there will be “very powerful quantum computers with a lot of intelligence. They’ll be able to work over long distances without being intercepted. It’s going to change the world.”

China has also recognized the potential power of quantum communications, and there is evidence indicating it is researching the possibilities at a higher level. Reports reveal that the National University of Defense Technology has been conducting quantum information technology research since the 1990s. The People’s Liberation Army (PLA) has clearly taken an interest in quantum communications because other institutions are also studying the topic. For example, the PLA’s University of Science and Technology (PLAUST) reportedly opened 11 new research directions in 2011, to include quantum communication technology. Some researchers believe that quantum communications, along with cloud computing, intelligence optic networks, and high-speed satellite communications, provide asymmetric operational superiority for military forces and generate new types of combat power.

PLAUST has worked with both military and nonmilitary research institutes, achieving major successes in key technologies. The university conducts strategic cooperative research with civilian institutes to establish joint laboratories, which have...
reportedly resulted in over 90 percent of their achievements being applied to the armed forces’ needs. Quantum communications research is just one area, with information grid networking and electromagnetic camouflage and protection also being researched. The China Academy of Space Technology has done preparatory work to establish the country’s first quantum remote-sensing laboratory. The aerospace community believes that remote sensing is an important area for the application of quantum information technology. It is hoped the laboratory will allow Institute 508 to apply for funding from the national 863 and 973 programs. Such a funding request appears appropriate because, in 2012, quantum information technology was designated as one of the four key areas of scientific research in the next 15 years.

More recently, quantum communication received recognition as a key technology by the Chinese Academy of Sciences (CAS) after the university’s president, Bai Chunli, announced plans to establish five innovation centers that would unite the country’s leading scientists and experts in advanced science and technology. The fields of study were quantum information and technology, Tibet plateau and Earth system science, particle physics, brain science, and thorium molten salt reactors. As a result, on January 15, 2014, China established the CAS Center for Excellence Quantum Information and Quantum Physics in Hefei. This new center is recognized as a model for the other four centers.

Research, Academics, China’s Education Dilemma, and Economic Impact

China considers itself second in the world in terms of research and development spending, and it has conducted original research in quantum communications that has had an international impact. Former President Hu Jintao stated in a speech that quantum communications had exerted great influence on China’s economic and social development. Premier Wen Jiabao noted, “Quantum theory and the theory of relativity stimulated the development of semiconductors and microelectronic integrated circuit technology, information technology, laser technology, nuclear energy, and related technologies.” In 2011, Liu Yandong, state councilor and Communist Party of China Central Committee Political Bureau member, noted that quantum communications have made “fresh contributions to scientific development.” She stated in 2012 that quantum communication technology has important strategic significance in ensuring the safety of state information. More important, she made these remarks...
While attending a ceremony to launch the financial information quantum communication verification network, it is not surprising that China’s rapid science and technology development has been tied to quantum information. As an example of the use of quantum information, in 2011 CAS reported on cooperation between the Institute of Modern Physics and the International Atomic Energy Agency. The physics research team “reportedly made significant progress in the research on the quantum state of ion-atom collisions, contributing to the better understanding of plasma evolution and plasma state diagnosis.” Such discoveries are ongoing and expanding.

China has been on a path to expand its overall technological capabilities. One approach has been to overhaul the country’s education system. During China’s Ninth Five-Year Plan (1996–2000), the government began to initiate actions to strengthen a number of higher learning and key disciplinary areas. The goal was to upgrade 100 institutions to greatly improve their quality of education, scientific research, management, and institutional efficiency. The select 100 institutions were expected to, through their own merit, easily “exert significant impact on the country’s social and economic development, scientific and technological advancement, and the national defense.”

The availability of funding in China for basic research has also been increasing steadily. In 1986 the investment in basic research was only 80 million yuan (approximately $9 to $10 million). By 2012, according to Chen Yiyu, director of the National Natural Science Foundation of China (NSFC), the Chinese government allocated more than 15 billion yuan ($2.38 billion) from the central budget to the NSFC. While only a portion of the money goes toward researching quantum information, the NSFC is a key source of funding for China’s research and development on quantum properties and applications.

China’s growing economy and increasing wealth make it easier than most other countries to sink money into research and development programs. During the U.S. Naval Research Laboratory’s second annual Karles Invitational Conference, Zachary J. Lemnios, Assistant Secretary of Defense for Research and Engineering, pointed out that:

“Nations with strong GDP growth—think China, Russia, South Korea—are using their increasing wealth to bolster investments in basic science, applied research, and advanced technology development, and these investments are increasingly focused. For example, the Chinese National Medium- to Long-Term Plan for the Development of Science and Technology (2005–2020), aims to make China an “indigenous innovator” by 2020, and to do this they are investing in 16 goal-oriented basic research “megaprojects,” one of which is quantum research.”

Basic research is essential for innovation. While the United States spends more money overall in basic research than any other country, Chinese investments are rising at a faster rate. According to Dowling, “One of the things that concerns me in the United States right now is that we are falling behind in our investments, particularly in basic science research. . . . We are getting to the point where we are no longer even in the top ten in terms of per capita investment in basic research anymore.”

Despite its economic wealth, however, China still has a number of hurdles to overcome before it can become a global innovative force. Pan attributes some of China’s lack of creativity to the high amount of pressure placed on students. Students devote years to intensive studying. However, according to Pan, they “are often incapable of developing independent solutions” due to a lack of creativity. There has been talk of changing the education system, but this has not yet happened. As Pan pointed out, there are simply too many students.

China’s academic and scientific efforts point to the country’s desire to achieve global technical superiority. Williams, who recognizes that quantum technologies will likely one day offer tremendous benefits to society, also sees the importance of maintaining a competitive edge in research and development to maintain both innovative and economic superiority. According to Williams, “While quantum technologies clearly create a direct risk to national security, the bigger risk is the threat to economic security since a strong economy is required to drive a strong military and innovation and quantum technologies are likely to be an innovation driver for the 21st century.”

Physicist Paul Davies once wrote, “The nineteenth century was known as the machine age, the twentieth century will go down in history as the information age. I believe the twenty-first century will be the quantum age.” Quantum technology is still in its infancy. The first organization or government to achieve quantum communication or quantum computing will control the technology, giving that country an advantage in every respect.

Conclusion

According to a 2010 article published by Time, “China is now at the cutting-edge of military communications, transforming the field of cryptography and spotlighting a growing communications arms race.” China, intent on becoming a global technology innovative force, has been making huge strides in research and development in many areas including quantum communication. There is a major push in the country to become the frontrunner in breakthroughs that will one day lead to the first quantum computer and the perfect quantum communication network. Should China eventually win the race in achieving certain quantum-based technologies, it could have a significant impact on national security and China’s role as an emerging superpower.

Quantum technologies have the potential to revolutionize secure communications for military and intelligence organizations. A quantum computer might one day be able to access information that had been archived but not yet declassified. Quantum technologies could also lead to revolutionary applications that might help propel a nation to economic superiority.
While China still lags behind developed nations in many ways, as its academic programs and research methodology continue to evolve, the country could eventually gain a lead in the research and development of quantum information. It is impossible to predict who will win the race for this revolutionary technology. However, one thing is certain: The force behind China’s research and development programs is growing.

Notes


2. Ibid.


5. Key Laboratory of Quantum Information, *School of Physical Sciences, University of Science and Technology of China* Web site, available at <en.physics.ustc.edu.cn/research_9/Quantum/201107/t20110728_116550.html>.


7. Huang.


11. Ibid.; one picosecond is the equivalent of one trillionth (10^-12) of a second.

12. Ibid.


17. Williams.


25. Ibid.

26. Discussions in this section developed in concert with Timothy Thomas.


39. Discussions developed in concert with Timothy Thomas.


42. Discussions in the first two paragraphs of this section developed in concert with Timothy Thomas.


44. Currency exchange rates for 1987 are not available. Calculation done based on 2002 rates. See “Central Gov’t to Pour 2.4 Billion U.S. Dollars Into Sciences,” *Xinhua,* March 27, 2012.


46. Dowling.

47. Schramm.

48. Williams.
