Quantum Computing

A Technology Primer

BY KELLY SWANSON

TYPE	CHARACTERISTICS	RISK FACTORS
Cyber	Detectability, Speed	Vulnerable, Predictive, Action-enabling

DOMAIN	COUNTRY
Cyber	United States, China

- Quantum computers have capabilities that exceed those of classical computers, processing information in a fundamentally different way by taking advantage of physics that occurs only on the quantum level.
- Quantum computers have yet to demonstrate supremacy over traditional computers, but due to their potential significant advantages in computing, many countries are investing in this emerging technology.
- Quantum computers will have implications for situation awareness as a result of their significant increase in processing power. Quantum computers have the capability to break many of the existing encryption algorithms used to protect online data and communications, permitting a significant advantage in intelligence gathering.

Introduction

Quantum computers have capabilities that exceed those of classical computers, processing information in a fundamentally different way by taking advantage of physics that occurs only on the quantum level. Classical computers use bits, strings of 0s and 1s, to encode information, and they process each bit one at a time. Quantum computers, however, use quantum bits, or qubits, which can be simultaneously 0 and 1. When created, qubits are correlated and not treated independently, as in the case of classical bits. These properties allow qubits to be operated on in parallel, increasing information capacity and processing power.

With these characteristics, quantum computers can solve problems that are not feasible on a classical computer. For example, quantum computers can efficiently factor large numbers, breaking various cryptographic protocols that are used to authenticate and secure communications and transactions.[1] Similarly, machine learning algorithms could also benefit from the improved processing power of quantum computers, allowing large data sets to be analyzed using a small number of qubits, thus providing more efficient pattern recognition.

[1] RSA is one widely-employed algorithm used to encrypt and decrypt messages. It relies on the difficultly for conventional computers to find the factors of large numbers.

These technological advances can enhance situational awareness capabilities through improved intelligence gathering, faster data analysis, and advanced autonomous detection techniques—in combination with sensor networks and other persistent observation modalities. Arguably the most disruptive implication of quantum computing is the effect it will have on the cyber domain. Quantum computers have superior hacking and decrypting capabilities as well as increased encryption protection against other quantum computing attacks.

State of Play

Quantum computers have yet to demonstrate supremacy[2] over traditional computers, but because of their potential significant advantages in computing, many countries—including the United States, Russia, and China—and corporations—such as Google, IBM, Intel, and Microsoft—are investing in this emerging technology.[3] IBM, for example, recently released a 50-qubit chip; Google is testing its 72-qubit chip; and the start-up Rigetti Computing is developing a 128-qubit processor. These quantum computers are approaching the capabilities of some of the most powerful conventional supercomputers.[4]

In quantum computing research, the United States and China currently are vying for dominance. The United States funds research through agencies such as the Department of Defense, the Department of Energy, and the National Security Agency but relies heavily on cooperative industry investments.[5] China, in contrast, has developed an ambitious investment strategy for quantum encryption and communication systems in response to fears of cyber espionage by the United States.[6] China has committed to building the world's largest quantum research facility, the National Laboratory for Quantum Information Science, and in 2017 became the first country to launch a quantum-communications satellite.[7] China has also developed the world's largest quantum key distribution network for secure, land-based communications between Shanghai and Beijing.[8]

"While quantum computing is still highly developmental, great strides are rapidly being made which could lead to the exceeding of more conservative expectations."

There remain several fundamental challenges that must be addressed before a fully functioning quantum computer is viable. Qubits operate in very isolated environments since disturbances to the system will destroy their quantum nature and convert them to conventional bits. To prevent these disturbances from destroying the qubit, qubits must be fault-tolerant and error-correcting. In addition, because quantum computers operate differently from classical computers, they require specifically designed algorithms and architectures. Solutions to these problems require continued investment in research institutions and close collaboration with industry. Because of these complications, the National Academies of Sciences, Engineering, and Medicine

---

[2] The level at which quantum computers become more powerful than classical ones.

[3] Katia Moskvitch, "Inside the High-Stakes Race to Make Quantum Computers Work," *Wired*, March 8, 2019, https://www.wired.com/story/inside-the-high-stakes-race-to-make-quantum-computers-work/.

[4] Tom Simonite, "The Wired Guide to Quantum Computing," *Wired*, October 30, 2018, https://www.wired.com/story/wired-guide-to-quantum-computing/.

[5] National Science and Technology Council, *National Strategic Overview for Quantum Information Science*, (Washington, D.C.: Executive Office of the President, Sept 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf, 14-15.

[6] Elsa Kania, "China's Challenge to US Quantum Competitiveness," *Hill*, June 30, 2018, https://thehill.com/opinion/technology/394894-the-chinese-challenge-to-us-quantum-competitiveness.

[7] Stephen Chen, "China Building World's Biggest Quantum Research Facility," *South China Morning Post*, July 20, 2018, https://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility.

[8] CORDUS, "China to Launch World's First Quantum Communication Network," Phys.org, August 4, 2017, https://phys.org/news/2017-08-china-world-quantum-network.html.

(NASEM) issued a report titled *Quantum Computing: Progress and Prospects*, which concluded that it is too early to predict a timeline for the development of a practical quantum computer. Many scientists agree with the report that one is unlikely to be built in the next decade.[9]

Despite these challenges, others have declared that quantum computers may begin solving real-world problems in the near future. In 2017, the Canadian company D-Wave Systems, Inc. sold the world's first quantum annealing computer D-Wave 2000Q for $15 million.[10] Intel Labs believes it will be five to seven years before industry can start using quantum computers to solve engineering-scale problems.[11] The European Quantum Technologies Roadmap, Europe's response to the United States' and China's investment in quantum computing, sees large-scale quantum processing in five to 10 years.[12] Google believes quantum supremacy might even be achievable within the next year.[13] Therefore, although quantum computing is still highly developmental, great strides are rapidly being made, which could lead to the exceeding of more conservative expectations.

Effects on Situational Awareness

Quantum computers will have implications for situational awareness as a result of their significant increase in processing power. In the near future, their ability to obtain information that is not currently accessible given today's encryption techniques (*vantage*) can make military, commercial, and government systems vulnerable. Quantum computers have the capability to break many of the existing encryption algorithms used to protect online data and communications, permitting a significant advantage in intelligence gathering.[14] Quantum computers can hack into non-quantum-resistant forms of encryptions on enemy servers, obtaining previously inaccessible information and potentially controlling their systems.[15] This process can take exponentially less time than with classical computers, increasing the *speed* with which information can be gathered and enabling faster decisionmaking.

Even before quantum computers become fully functional, encrypted data are vulnerable to a harvest and decrypt scheme, where hackers scrape encrypted data and hold them until quantum computers become mature enough to be used for decryption.[16] Although some government secrets may be obsolete by that time, other information, such as Social Security numbers, healthcare data, and financial transactions can be useful many years after its initial collection. Evidence already exists of government security services harvesting and storing

---

[9] Peter Gwynne, "Practical Quantum Computers Remain at Least a Decade Away," Quantum, December 12, 2018, https://physicsworld.com/a/practical-quantum-computers-remain-at-least-a-decade-away/.

[10] The fastest supercomputer, the Chinese Sunway TaihuLight, costs $273 million; James Temperton, "Got a Spare $15 Million? Why Not Buy Your Very Own D-Wave Quantum Computer," *Wired*, January 26, 2017, https://www.wired.co.uk/article/d-wave-2000q-quantum-computer.

[11] "2018 CES: Intel Advances Quantum and Neuromorphic Computing Research" [Press Release], Intel, January 8, 2018, https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/.

[12] Antonio Acin, Immanuel Bloch, Harry Buhrman, Tommaso Calarco, Christopher Eichler, Jens Eisert, Daniel Esteve, Nicolas Gisin, Steffen J Glaser, Fedor Jeletzko, et al., "The European Quantum Technologies Roadmap." arXiv preprint arXiv:1712.03773, December 12, 2017.

[13] Julian Kelly, "A Preview of Bristlecone, Google's New Quantum Processor," Google AI Blog, March 5, 2018, https://research.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

[14] *The Economist*, "Quantum Computers Will Break the Encryption That Protects the Internet," October 20, 2018, https://www.economist.com/science-and-technology/2018/10/20/quantum-computers-will-break-the-encryption-that-protects-the-internet.

[15] David Cardinal, "Quantum Cryptography Demystified: How It Works in Plain Language," ExtremeTech, March 11, 2019, https://www.extremetech.com/extreme/287094-quantum-cryptography.

[16] Meredith Rutland Bauer, "Quantum Computing is Coming for Your Data," *Wired*, July 19, 2017,

https://www.wired.com/story/quantum-computing-is-coming-for-your-data/.

internet traffic. The British Government Communications Headquarters and the United States National Security Agency, in an operation codenamed Tempora, collected and stored data transmitted through fiber-optic cables for approximately 18 months, searching for hints of criminal and terrorist activity.[17] Such schemes would be capable of holding encrypted information until a quantum computer became viable.

Network security might be ensured using quantum cryptography, but until such a technique is developed and installed, existing systems will remain vulnerable to decryption or harvesting. Decryption by a quantum computer, without specific quantum-based security protocols in place, could be *undetectable*, and data can be continuously collected until such quantum-secure countermeasures are established (*persistence).*[18] However, the *reliability* and *precision* of the information depend on whether the adversary believes its networks are secure. If the target is concerned that its data are compromised, false information or other spoofing measures may be incorporated.

Beyond their decryption capabilities, quantum computers combined with machine learning algorithms may allow for new and more sophisticated ways to analyze large data sets for patterns and relationships. With more data being collected at a faster rate, humans and conventional computers may be unable to keep up with the pace. Quantum computers could allow for a substantial increase in the ability to process large amounts of data utilizing existing open-source information and clandestine intelligence sources (*vantage)*. Patterns which may otherwise be buried in noise (*precision)* can be identified, even with incomplete and chaotic information. During rapidly changing situations, faster processing can lead to increased reaction times.

However, as with conventional computers, artificial intelligence (AI) and quantum computers are programmed and trained to carry out particular tasks. If the situation changes too rapidly and is far from the original scope, the system may be unable to shift focus. To combat this fault, multiple systems could jointly operate, providing a level of *resilience* to changing circumstances. However, if the data used to train the AI systems are corrupt, the AI can incorrectly classify data and become susceptible to false positives.[19] This vulnerability will decrease the *reliability* of the systems.

Risk Factors for Strategic Stability

Data interception by a quantum computer may be undetectable even when the system under attack is itself quantum. Whereas traditional systems are not capable of detecting eavesdroppers, quantum systems were thought to provide secure data transmissions. However, recent research has demonstrated successful cloning of qubits, allowing for undetectable*, non-destructive, non-intrusive* hacking of both traditional and quantum systems.[20]

The information obtained can be used to help *predict* adversary actions assuming the data haven't been compromised. With faster data processing and better pattern recognition, quantum computers can, for example, increase awareness of hard to detect military units, such as submerged enemy submarines. Data gathered from multiple platforms can be integrated into a single set of conclusions for a more comprehensive view of the environment, potentially finding useful information that could not be identified by a single platform. Analysis of

---

[17] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications," *Guardian,* June 21, 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[18] Arthur Herman, "The Executive's Guide to Quantum Computing and Quantum-Secure Cybersecurity," Hudson Institute, March 2019, https://www.hudson.org/research/14930-the-executive-s-guide-to-quantum-computing-and-quantum-secure-cybersecurity.

[19] Anh Nguyen, Jason Yosinki and Jeff Clune, "Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images." *Computer Vision and Pattern Recognition,* IEEE, April 2, 2015.

[20] Frederic Bouchard, Robert Fickler, Robert W. Boyd and Ebrahim Karimi, "High-dimensional Quantum Cloning and Applications to Quantum Hacking," *Science Advances,* February 3, 2017, DOI: 10.1126/sciadv.1601915.

these large data sets can lead to predictive models.[21] For example, data gathered about past enemy operations can lead to predictions of future behavior.

Using such models, attacks can be prevented, and responses can be improved. Quantum computers are superior to conventional computers at optimization problems, which can aid in logistical planning. By identifying the quickest and/or easiest strategy to manage materials, personnel, and the increasing number of unmanned robotic systems, quantum computers can increase the speed and efficiency of operations through improved resource allocation. Faster, potentially real-time responses could allow for the *preemption* of enemy attacks and provide new military options *(action-enabling)*. Drone footage, which generates more data than humans can review, can be more efficiently analyzed to identify hostile targets, and improved pattern recognition applied to satellite images can search for movement of military forces.

These capabilities give quantum computers the potential to undermine strategic stability by increasing one's ability to better target adversarial forces. Information superiority offered by quantum computing gives a significant advantage to the first user. Coupled with better pattern recognition and modeling of an opponent's forces, quantum computers can allow for more credible target identification and destruction of forces in a first strike. At the same time, if it is believed that the opponent might have quantum computing capabilities, and thus critical information about one's forces may be known, the ability to mount a dependable second strike may be compromised, causing escalation risks. For example, AI coupled with quantum computing can better hunt for nuclear submarines, decreasing their perceived survivability and capacity to carry out a second strike.

If the existence of a quantum computer or the specifics of how it was designed is known, protocols to block decryption attempts or purposefully communicate false information could be implemented. As quantum computers improve, quantum-resistant encryption techniques are also being developed to dampen the effects of a quantum computer.[22] Thus, governments and militaries have an interest in keeping their possession of quantum computers secret. However, if quantum capabilities, both quantum computers and quantum cryptography, are kept secret, then both sides may misperceive the capabilities of their adversaries and potentially assume their data has become compromised. This could lead to escalation through miscalculation during a conflict.

Interest in developing a quantum computer is not limited to the military. Because of its potential to exponentially improve processing power, corporations and start-ups are investing heavily in quantum computing research for applications to big data analytics, computational biology and medicine, and machine learning and AI. A quantum computer can speed up drug discoveries, help discover new materials, and validate code needed to test complex systems. As such, quantum computers are inherently *dual-use* in terms of economic applications.

Concluding Remarks: Risks versus Rewards

Quantum computers have not yet reached the stage where they offer advantages over conventional computers, but they have the potential to greatly affect strategic stability in the near future. The ability to break current encryption methods using a quantum computer would give the first user significant offensive advantages, potentially creating a use-it-or-lose it incentive to attack before an adversary can develop its capabilities. However, depending on the specific policy of individual countries, the repercussions of a quantum cyber-attack may or may not greatly affect global instability or supplant nuclear weapons as the indication of national security. Regardless, the threat of a quantum cyberattack can further inflame already tense situations and aggravate relationships between adversaries.

---

[21] Jennifer Ouellette, "How Quantum Computers and Machine Learning Will Revolutionize Big Data," *Wired*, August 14, 2018, https://www.wired.com/2013/10/computers-big-data/.

[22] Lisa O'Connor, Carl Dukatx, Louis DiValentin, and Nahid Farhady, "Cryptography in a Post-Quantum World," Accenture Labs, 2018, https://www.accenture.com/_acnmedia/PDF-87/Accenture-809668-Quantum-Cryptography-Whitepaper-v05.pdf.

Benefits of a quantum attack can be mitigated with post-quantum cryptography. The development of quantum key distribution (QKD), which is a quantum-based encryption scheme hardened to quantum computer hacking, also might lead to a quantum arms race in which QKD offers advantage to the defensive. However, the switch to a fully protected system will be slow and require significant investment. During the upgrade time, transactions and data remain vulnerable. Thus, quantum computers would give a powerful intelligence advantage to whomever develops and employs it first. Quantum cryptography and computing could counterbalance each other if employed equally; however, the United States and China are asymmetrically developing this technology, making global strategic stability dependent on which aspects dominate in the near future.

If quantum encryption reaches maturity faster, giving China a security advantage, the relationship between the United States and China may become unstable. If China protects its systems using theoretically perfectly protected quantum techniques, it could become more secure in its communications and intelligence. Reliable intelligence can lead to increased stability as countries understand each other's motives and capabilities. Thus, if a country could completely protect its information, misunderstandings and misperceptions could lead to instability during a crisis. If, however, a country had complete confidence in the security of its information and communications, it might feel less incentive to escalate first in a crisis.

With the benefits of improved processing power, and the disadvantages of being left behind, quantum computers are a highly desirable emerging technology. The capability to eavesdrop on an adversary's communications, transactions, and data has the potential to significantly enhance strategic situational awareness. In addition, AI-coupled quantum computers can improve the speed of military operations and decisionmaking. Although quantum computing is in the research phase, the disruption of the cyber domain and the advantage of information superiority afforded by this emerging technology have the potential to greatly alter global strategic stability.

ABOUT CSIS