Counterintelligence and the Quantum Computing Race Short

Student Guide

June 2026

Center for Development of Security Excellence

Contents

Introduction

News Reporter: In today's news, we'll discuss the failing financial markets, reports of bank accounts being wiped out as a result of a data breach, and the critical compromise of our naval warships' communications and positioning systems. Are these events connected to emerging technologies? We'll discuss this and more in today's segment…

Narrator: Although these stories aren't headlines in today's news, they could be soon. Technological progress drives many of today's most significant achievements, but like many advancements, it is a double-edged sword. Quantum technologies will define the next era of progress, but this will benefit only those equipped with the most powerful and effective systems. For those who do not have the quantum technology advantage, there could be catastrophic outcomes. Should adversaries attain relevant quantum technologies before the U.S., they could exploit technological capabilities in areas of logistics, optimization, machine learning, and materials discovery, leading to compromised national security and jeopardizing vital data and communications across all sectors. This Short will help you recognize the impacts of quantum computing, both positive and negative, and the implications for counterintelligence (CI).

Quantum Computing Definition and Timeline

Quantum computers are the pinnacle of quantum technology; they are emerging computational devices that exploit the phenomena of quantum mechanics to enhance computation. Whereas classical computers encode information in binary states represented by a "1" or a "0" —called bits— quantum computers can encode a "0", "1", or a combination of "0" and "1" at the same time—called quantum bits, or qubits—thus increasing the power of the quantum computer exponentially with the addition of each qubit. The potential of quantum computers first became apparent over 30 years ago with the discovery that a quantum computer could break asymmetric cryptographic protocols such as Rivest-Shamir-Adleman (RSA), a public key cryptosystem that enables any user to encode data in such a way that it can be read only by those who know a private key.

As this technology advances over the next decade, quantum computers are expected to break some encryption methods that are widely used to protect customer data, complete business transactions, and secure communications. Some analysts believe that an initial quantum computer prototype capable of breaking current encryption methods could be developed in the 2030 to 2040 timeframe. Analysts estimate that a quantum computer with around 20 million qubits would be required to break current encryption methods; however, the most advanced quantum computers today generally have no more than 1,088 qubits.

Advantages of Quantum Computing

It's only a matter of time until quantum computing is fully developed and it offers tremendous potential for advancement across industries. CI plays a large part in protecting the people, technologies, data, and supply chains that make advantages of quantum computing possible. Advantages of quantum computing include the possibilities for:

- Discovery of new drugs and materials
- New ways to solve optimization problems
- Enhanced artificial intelligence capabilities
- More accurate financial modeling
- Strengthened cryptography
- Improved accuracy in weather forecasting
- Understanding fundamental science
- Improving national security defenses

Drug Discovery and Materials Science

Quantum computers can simulate molecular interactions with unprecedented accuracy, accelerating the discovery of new drugs, therapies, and advanced materials with specific properties, such as superconductors and lightweight alloys.

Solving Optimization Problems

Quantum computers excel at solving complex optimization problems, leading to improvements in logistics, supply chain management, financial modeling, and traffic flow; this could result in significant cost savings and increased efficiency.

Artificial Intelligence (AI)

Quantum machine learning (ML) algorithms could enhance AI capabilities, leading to more powerful and efficient ML models for image recognition, natural language processing, and other AI tasks.

Financial Modeling

Quantum computing can improve financial risk assessment, portfolio optimization, and fraud detection, leading to more stable and efficient financial markets.

Cryptography

While posing a threat to current encryption, quantum computing also enables the development of quantum-resistant cryptography, securing future communications and data; quantum key distribution offers fundamentally secure communication channels.

Weather Forecasting and Climate Modeling

Improved accuracy in weather forecasting and climate modeling can help us better prepare for natural disasters.

Fundamental Science

Quantum computing can advance our understanding of fundamental physics, chemistry, and biology by simulating complex quantum systems that are impossible to model with classical computers.

National Security

While it could pose a threat in the wrong hands, quantum computing can also be used defensively to enhance cryptography and protect our nation's infrastructure.

The Race for Advanced Quantum Computing

The race for quantum supremacy is a complex and rapidly evolving field, with the United States, China, and Russia all making significant investments and strides. Currently, the United States holds an edge in high-performance quantum computing, but China has established a dominant position in the more mature field of quantum communications. China leads in developing a countermeasure known as quantum key distribution (QKD) and is also outspending the rest of the world in an effort to harvest information and resources now and decrypt later, once they obtain a capable quantum computer. Like China, Russia is actively pursuing quantum technologies and has unveiled new, higher performance quantum computers. Russia is also continuing to expand quantum communications networks but still lags behind both the U.S. and China. Even if the U.S. wins the race and becomes the first country to attain useful quantum computers, it won't be long before others, including adversaries, will achieve this too, and that could put the U.S. at a severe disadvantage.

Disadvantages of Quantum Computing

As discussed earlier, quantum computing is a double-edged sword; the same advantages of quantum computing can become disadvantages for those who do not win the quantum computing race. Quantum computers threaten to decrypt classified or controlled unclassified information (CUI), intellectual property, and other sensitive data

stored on encrypted media that is protected by our current encryption methods. This would allow adversaries to gain access to sensitive information in both private and public sectors. Although some analysts note that significant advances in quantum computing would likely be required to break current encryption methods, the potential inability to protect advancements and intelligence is a future threat that can only be addressed proactively.

Another considerable disadvantage is the potential loss of global innovative leadership. With access to sensitive information, the U.S. could be put in a position where we are unable to protect our own advancements and innovations. A loss of the quantum computing race could even jeopardize our ability to protect vital communications, including those leveraged in times of war. From a defensive standpoint, understanding these disadvantages and developing quantum-resistant cryptographic algorithms will be crucial to protecting future data from quantum attacks.

CI Implications

The danger of losing the quantum computing race has significant implications for CI. The U.S. would be at a massive CI disadvantage if adversaries were to gain the technological edge. CI personnel and teams will set an example for the rest of the federal government in how they respond to and proactively approach threats to our quantum computing efforts posed by foreign adversaries. CI efforts can demonstrate the seriousness of a quantum computing threat by acting swiftly and decisively, should a threat arise.

CI also has a vital role in protecting current quantum computing research and development. CI must be applied broadly and deeply in the areas of government, industry, and academia. CI is in a position to protect against foreign adversarial targeting and collection of U.S. quantum computing research and intelligence. All three areas of focus—government, industry, and academia— are integral in researching, developing, and testing, thus all three areas are being targeted aggressively by adversaries and require CI attention.

Finally, CI efforts should include concrete and achievable steps that can be taken now to prepare organizations for the transition to post-quantum cryptography. Adversaries are aware of quantum computing countermeasures and CI efforts should incorporate countermeasure intelligence as part of a proactive strategy. To provide relevant stakeholders with these steps, the Department of Homeland Security (DHS), in partnership with the National Institute of Standards and Technology (NIST), created the Post-Quantum Cryptography Guide.

Post-Quantum Cryptography Guide

When preparing for the transition to post-quantum cryptography, organizations should first take inventory of their current cryptographic systems, and the data being protected, and prioritize their systems for transition. From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum-vulnerable. Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard.

Impact Activity 1

Quantum computing has advantages and disadvantages. Take a moment to test your knowledge.

Which of the following statements does NOT represent the advantages of winning the quantum computing race?

Select the best response. Check your answers in the Answer Key at the end of this Student Guide.

- ○ Quantum computers can simulate chemicals and materials with high accuracy, accelerating drug discovery and advanced material development.
- ○ Once attained, owners of quantum computers are guaranteed an advantage over their adversaries, ensuring they never gain quantum capabilities.
- ○ Quantum machine learning (ML) could dramatically improve AI performance, enabling faster and more accurate intelligence analysis.
- ○ Quantum optimization can enhance logistics, financial modeling, and supply-chain efficiency across national industries.
- ○ Quantum computing can enhance weather forecasting and climate modeling with greater precision.

Impact Activity 2

Now, try this one.

Which of the following statements represents the disadvantages of not winning the quantum computing race?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- ☐ Adversaries could potentially decrypt classified and controlled unclassified information (CUI) protected by today's encryption methods.

- ☐ The U.S. may lose global leadership in innovation if foreign competitors gain quantum superiority.
- ☐ Quantum computing would enable faster and more accurate AI models but would not be applicable for military and intelligence purposes.
- ☐ Critical U.S. wartime and secure communications could become vulnerable to quantum-enabled interception.
- ☐ Adversaries could steal U.S. intellectual property, defense innovations, and sensitive research using quantum-enabled exploitation.

Conclusion

News Reporter: Up next, we're highlighting recent advances in quantum computing as the U.S. experiences strengthened financial markets, more secure critical military communications and accurate GPS locations, and enhanced life-saving weather forecasting capabilities. Officials say the nation's quantum advantage is driving innovation, protecting vital systems, and reinforcing national security. More on this new era of technological leadership is coming up.

Narrator: Quantum computing will transform industries, scientific discovery, and national security—but only for those who lead. By now, you should be able to recognize that losing the race for quantum computing could bring catastrophic consequences to our nation. Counterintelligence plays an essential role in protecting research, defending against emerging threats, and securing the transition to post-quantum cryptography.

Congratulations. You have completed the *CI and the Quantum Computing Race* Short.

Appendix A: Answer Key

Impact Activity 1

Which of the following statements does NOT represent the advantages of winning the quantum computing race?

- ○ Quantum computers can simulate chemicals and materials with high accuracy, accelerating drug discovery and advanced material development.
- ⊙ Once attained, owners of quantum computers are guaranteed an advantage over their adversaries, ensuring they never gain quantum capabilities. (correct response)
- ○ Quantum machine learning (ML) could dramatically improve AI performance, enabling faster and more accurate intelligence analysis.
- ○ Quantum optimization can enhance logistics, financial modeling, and supply-chain efficiency across national industries.
- ○ Quantum computing can enhance weather forecasting and climate modeling with greater precision.

Feedback: *There is no guarantee that owners of quantum computers will have an everlasting advantage over their adversaries or prevent their adversaries from gaining quantum capabilities.*

Impact Activity 2

Which of the following statements represents the disadvantages of not winning the quantum computing race?

- ☑ Adversaries could potentially decrypt classified and controlled unclassified information (CUI) protected by today's encryption methods. (correct answer)
- ☑ The U.S. may lose global leadership in innovation if foreign competitors gain quantum superiority. (correct answer)
- ☐ Quantum computing would enable faster and more accurate AI models but would not be applicable for military and intelligence purposes.
- ☑ Critical U.S. wartime and secure communications could become vulnerable to quantum-enabled interception. (correct answer)
- ☑ Adversaries could steal U.S. intellectual property, defense innovations, and sensitive research using quantum-enabled exploitation. (correct answer)

***Feedback**: Those who do not win the quantum computing race risk the loss of global leadership due to adversaries who may decrypt protected information, hack secure communications, and steal intellectual property or defense innovations.*