National Intelligence University

MST 684
Cyber Threat
Professor Feehan

An Examination of Quantum Use Cases and Threats

Submitted by

Alejandro F. Sosa

I verify that this submission is my own original work.
03 November 2023

An examination of Quantum Threats

In the past 30 years, the world has changed dramatically. Before the information age, most knowledge was retained in printed form in books, magazines, and encyclopedias. This limited access to information to those who could access a library or were relatively wealthy. Access to niche or esoteric information meant seeking out larger or specialized libraries. Most financial transactions were either conducted with cash or checks. Credit Cards and bank cards had not been widely adopted. It is taken for granted that transactions will be conducted in a way that ensures confidentiality, integrity, and availability. That is to say that when a transaction is made, it is only visible to those authorized to view that transaction, none of the details of the transaction can be changed once agreed upon, and no outside entity can change them, and finally, that authorized entities have unimpeded access to the data when required. These three attributes ensure that someone can view their mortgage balance whenever they want.[1] Specialized and valuable information has migrated from physical libraries to digital information systems where they can fuel collaborative projects in a secure environment. Encryption across platforms is a significant factor in ensuring the security of all of these transactions as well as private and valuable communication.

If a hostile nation were to develop effective quantum computing, it could easily break the encryption standards used across the world to secure information systems. That entity would be able to destabilize modern society without firing a single shot. However, quantum-based computing exponentially increases the computing power available to previously unimaginable levels. This paper will explore the current quantum development ecosystem, specific use cases for quantum computing, and how an adversary may utilize those use cases against the United

[1] "Election Security Spotlight – CIA Triad," *CIS*, accessed October 15, 2023, https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/.

States and its interests. This paper will not explore the specific challenges facing the development of quantum computing except for how those challenges impact the operationalization of quantum use cases.

Quantum Computing; Use Cases and Associated Risks

Quantum computing utilizes physical states to compute instead of utilizing an energy state or integrated circuits to make calculations through binary digits or bits. So rather than two bits, quantum computers, by using the relative position of physical elements, can represent both the one and zero of a binary state simultaneously in polynomial time; this is also referred to as a superposition or coherence.[2] Computing via physical states does more than just provide additional computing power or more speed; it allows for an entirely different of problem-solving outside of traditional computations. There are other challenges due to the physical properties of quantum systems, meaning there is still a lot to learn, discover, and overcome before quantum computing can become practical or broadly implemented.

Currently, due to the extremely niche parts and complexity of the systems, there are only a few dozen quantum computers in the world. As of 2022, there were 20 countries with publicly available numbers on the amount of funding directed toward quantum computing.[3] The top six best publicly funded programs in order belong to China, the European Union, Germany, The United States, The United Kingdom, and India.[4] Top six because Germany also contributes about half of the funding to the EU's program. Public funding is only a portion of the quantum

---

[2] Kyrylo Petrenko, Atefeh Mashatan, and Farid Shirazi, "Assessing the Quantum-Resistant Cryptographic Agility of Routing and Switching IT Network Infrastructure in a Large-Size Financial Organization," *Journal of Information Security and Applications* 46 (June 1, 2019): 151–63, https://doi.org/10.1016/j.jisa.2019.03.007.

[3] Emily Grumbling and Mark Horowitz, eds., *Quantum Computing: Progress and Prospects* (Washington, D.C.: National Academies Press, 2019), https://doi.org/10.17226/25196.

[4] Mohr, Niko; Pflanzer, Anika; Soller, Henning, "The Quantum Technology Monitor, Facts and Figures" (McKinsey & Company, December 2020), https://www.mckinsey.com/~/media/mckinsey/featured%20insights/the%20rise%20of%20quantum%20computing/quantum%20technology%20monitor/2020/mckinsey-quantum-technology-monitor-202012.pdf.

ecosystem because there are significant private interests and start-ups that also operate in the same space since there are massive investment opportunities with quantum use cases. For example, in 2020, the EU had 51 quantum computing start-ups compared to 9 in 2015; the United States had 36 in 2020 compared to 12 in 2015, and Canada had 20 in 2020 compared to 6 in 2015. Unfortunately, there is no good data for Chinese start-ups because most Chinese players are government-owned/funded.[5]

There is such diverse interest in quantum computing because it has the potential to revolutionize certain industries. Among scholarly articles and industry reports on the potential use cases, there are often four primary use cases that can have a broad array of impacts depending on the perspective of analysis. The four most well-developed cases for quantum computing are quantum simulation, quantum linear algebra, quantum optimization, and quantum factorization. Each of these use cases has both private and public uses; although quantum computing is being developed by government-funded research facilities, industry giants like IBM and Google and start-ups, depending on who leads in what area, can have huge downstream effects. In the near term, the one thing that most quantum scientists agree upon is that it is unlikely that major threats will appear within the next 5-10 years,[6] although some who work in the space, such as IBM, suggest that some of the use cases for quantum could be operationalized within five years.[7]

Quantum simulation also refers to a specific type of quantum computer, a quantum simulator or emulator. Currently, these types of quantum computers utilize ions trapped by a field

[5] Mohr, Niko; Pflanzer, Anika; Soller, Henning.
[6] "2022 Quantum Threat Timeline Report," *Global Risk Institute* (blog), accessed November 4, 2023, https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.
[7] Arthur Herman and Idalia Friedson, "Quantum Computing: How to Address the National Security Risk," n.d.

of lasers and electrodes in a vacuum.[8] This makes them significantly more coherent than other types of qubits, which rely upon extremely cold environments but also tend to be the slowest quantum computers.[9] These types of quantum computers can be used to model and simulate complex physical properties. This is one of the leading areas of quantum computing because it could revolutionize the industries of material science, pharmaceuticals, and chemistry because they can model and simulate complex interactions at the molecular level.[10] These could be used to map enzymes, conduct gene editing, and create advanced synthetic materials. This could be used by an adversary to become the first nation to develop a cure for a pandemic and develop lighter and stronger or more volatile materials.

Quantum linear algebra is the application of quantum computing to traditional computation. This can be achieved by the use of a second kind of quantum computer called a quantum annealer, which utilizes the random nature of a large pool of qubits and their entanglement principles to conduct computation rather than trying to physically manipulate the qubits.[11] This can be applied toward developing artificial intelligence by emulating and training complex quantum neural networks. Artificial intelligence developed through this process could be used to write additional advanced quantum algorithms. This application is also a leading candidate for a financial services role that could advise investors on portfolio management.[12] A malicious actor could use quantum-trained AI for a myriad of attacks, including developing

[8] "Quantum Simulators Wield Control over More than 50 Qubits," November 29, 2017, https://jqi.umd.edu/news/quantum-simulators-wield-control-over-more-50-qubits.
[9] Herman and Friedson, "Quantum Computing: How to Address the National Security Risk."
[10] "Exploring Quantum Computing Use Cases for Electronics," n.d.
[11] Andrea Morello, "Double or Nothing: Could Quantum Computing Replace Moore's Law?," The Conversation, June 2, 2011, http://theconversation.com/double-or-nothing-could-quantum-computing-replace-moores-law-362.
[12] "Quantum Computing Use Cases—What You Need to Know | McKinsey," accessed November 4, 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know.

malware, manipulating markets, or for use in advanced conventional weapons for autonomous targeting.

Quantum optimization could also be achieved by utilizing a quantum annealer. It would essentially develop algorithms that test the efficiency of certain layouts and functions in order to determine the best use of resources. Quantum optimization could help to develop a truly universal quantum computer. The primary financial case for quantum optimization would be in executing Monte Carlo simulations to enable faster trading.[13] An adversary could utilize quantum optimization in order to determine the ideal placement of strategic and tactical military resources, dramatically cutting down on the planning timeline.

Finally, the clearest and most well-researched area of threat for quantum computing applications is quantum factorization. Quantum factorization refers to the ability of a quantum computer to determine the prime factors of any given number. Factorization is a principle that underpins all modern cryptography, which essentially multiplies massive prime numbers to generate a number so large that its factors would take billions of years to break.[14]

The vast majority of information technology services currently use the internet, public critical infrastructure, e-mail, a virtual public network, or an intranet[15]. Each of these instances utilizes different encryption forms to ensure security. The internet has different ways of authenticating users between the different transfer and communication protocols it employs. Throughout all of the various levels and forms of private and public services, just as everything relies upon information technology, that information technology relies upon secure encryption.

---

[13] Vikas Hassija et al., "Forthcoming Applications of Quantum Computing: Peeking into the Future," *IET Quantum Communication* 1, no. 2 (2020): 35–41, https://doi.org/10.1049/iet-qtc.2020.0026.
[14] Herman and Friedson, "Quantum Computing: How to Address the National Security Risk."
[15] "Post-Quantum Cryptography Initiative | CISA," accessed October 14, 2023, https://www.cisa.gov/quantum.

Many websites utilize public key infrastructure in order to ensure that users are safely interacting with the correct website and not a fake website with a similar address meant to fool the user into giving up their personal data. This form of authentication occurs in the background and requires little or no user input. Certificate Authorities monitor, issue, and revoke certificates as a means of removing malicious websites. This security mechanism relies on public key cryptography. There are many kinds of cryptography, each of which has different benefits and drawbacks. The most commonly adopted form of cryptography (Integer Factorization Based Cryptography) is transparent to the end user and multiplies two extremely high prime numbers to compute a result. Once that number has been generated, the potential number of solutions to arrive at that result increases exponentially; it is challenging to determine which two prime numbers were used to arrive at an answer when one is using binary math.[16]

Despite its relative infancy, quantum algorithms such as Shor's algorithm have already been formulated, which are already capable of breaking two broadly implemented widely utilized types of encryption once quantum systems of sufficient capacity have been built. Estimates vary on when quantum computing will have matured enough to truly disrupt the current technological ecosystem, but on average, estimates suggest about ten years, depending on the level of funding and support, which has grown significantly in the past five years.[17] The Department of Homeland Security is working on a roadmap to identify critical areas of vulnerability and is working with the National Institute of Standards and Technology (NIST) to begin developing a standard for post-quantum cryptography.[18] NIST is currently working with government and private industry partners to develop a standard that neither interrupts commerce

[16] John Mulholland, Michele Mosca, and Johannes Braun, "The Day the Cryptography Dies," *IEEE Security & Privacy* 15, no. 4 (2017): 14–21, https://doi.org/10.1109/MSP.2017.3151325.
[17] Grumbling and Horowitz, *Quantum Computing*.
[18] "Post-Quantum Cryptography Initiative | CISA."

nor demands an excessive cost. NIST's initial recommendations are projected for 2024.[19] Timelines will become increasingly crucial as capable quantum computers begin to come online because it took over 20 years to deploy and adapt modern cryptographic standards.[20] There are other options that exist both within the government and within the private sector to help mitigate some of these risks within the financial services sector.

The push towards distributed accounting and blockchain ledgers could also make it more difficult for any malicious actor to make a change that goes unnoticed. However, these are still relatively new technologies with limited applications. Additionally, there are many people who assume that these technologies are impervious to tampering, but in many cases, it is not the encryption of these technologies that makes them theoretically safer; it is their distributed nature that makes them difficult to modify because there so many entities within the ecosystem that would have to be altered nearly simultaneously. The blockchain encryption methods by the two most heavily utilized blockchains, Bitcoin and Ethereum, both use the same encryption techniques as many modern information systems, namely the Elliptical Curve Digital Signature Algorithm. This type of encryption has been shown theoretically to be vulnerable to sufficiently sized quantum computers[21].

Known Encryption Attack Profiles

The two most famous instances of utilizing and breaking codes come from World War II, where the code talkers were used to ensure that allied messages were secure due to the esoteric nature of the language used to transmit and decode them. There is also the breaking of the enigma machine. When the enigma was broken, the Allied forces tried deliberately to ensure that

---

[19] William Barker, "MIGRATION TO POST-QUANTUM CRYPTOGRAPHY," n.d.
[20] Petrenko, Mashatan, and Shirazi, "Assessing the Quantum-Resistant Cryptographic Agility of Routing and Switching IT Network Infrastructure in a Large-Size Financial Organization."
[21] Robert Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," *The Journal of the British Blockchain Association* 2, no. 1 (October 4, 2019): 1–8.

they did not tip their hand by utilizing the information from the broken cipher too often. Allied forces often employed feints or cover stories to obfuscate the source of their successes. It is likely that this type of obfuscation would also occur if a great power were to develop a quantum computer capable of breaking modern encryption standards. It would likely be used to steal valuable intellectual property and take it to market first, effectively waging economic espionage.[22] It would likely also be used for a host of forms of attacks and breaches. The breaking of cryptography could also go entirely unnoticed. There are malicious actors who have been stealing vast troves of encrypted data with the intent of decrypting it once quantum computing finally realizes that capability. In that scenario, any information previously collected would be at risk of exposure.[23]

The cybersecurity community has long sought to ensure that encryption practices are well tested often by offering bounties for those who are able to break encryptions. To date, one of the most famous instances of breaking encryption is the cracking of DES in 1997.[24] The cracking DES led many cyber to realize that encryption needed to be much more resilient than the current day's technology due to the rapid pace of technological innovation and computing power.[25] The current cryptographic standards vary based on function, but the current standard to which quantum factorization is compared is RSA-2048, which is a semiprime (a number composed of two large prime numbers) with 617 digits or 2048 bits; it is often estimated that a classical computer would take 300 trillion years to factor such a number[26]. The current standard challenge

---

[22] Catherine Lotrionte, "Countering State-Sponsored Cyber Economic Espionage under International Law," *North Carolina Journal of International Law and Commercial Regulation* 40, no. 2 (2015 2014): 443–542.
[23] Michele Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," 2015, Cryptology ePrint Archive, https://eprint.iacr.org/2015/1075.
[24] "A Brief History of Cryptography," accessed November 4, 2023, https://www.redhat.com/en/blog/brief-history-cryptography.
[25] Mulholland, Mosca, and Braun, "The Day the Cryptography Dies."
[26] Valerio Scarani and Christian Kurtsiefer, "The Black Paper of Quantum Cryptography: Real Implementation Problems," *Theoretical Computer Science*, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, 560 (December 4, 2014): 27–32, https://doi.org/10.1016/j.tcs.2014.09.015.

for quantum computers to break RSA-2048 often refers to breaking the encryption within 24 hours, although it has yet to be broken[27].

Recommendations and Conclusion

As of right now, quantum computing is still assessed to be in its infancy, and there are still many hurdles to clear before it can become an effective form of computation capable of outperforming modern binary technology. Assessments suggest that there is currently a ten-year window in which to develop, test, and deploy effective post-quantum cryptography against an increasingly diverse field of organizations, technology, and financial products[28]. Due to the extreme cost and complexity associated with quantum computing, including the hazardous materials often required to generate the frigid environments required for quantum computing, it is likely that the first actor to develop an effective quantum computer would be either a nation or a multinational company such as IBM or Google which would have dramatically different outcomes for the United States government, global economy, and world order.

It is critical that the United States Intelligence Community remain aware of the changes and developments occurring within the quantum computing industry. The knowledge of the risk of broken modern cryptography could lead to better cyber security practices or more stringent practices in the most critical areas of research and development. It becomes critical to begin implementing post-quantum cryptography in areas where the intelligence community is either working to develop advanced capabilities that may be stolen or where there are sensitive, clandestine, or covert operations being conducted in order to protect those involved. Arguably, one of the greatest areas of risk for the military and the intelligence community is its partnerships with academia, which often do not require security clearances or the same standards of

[27] Herman and Friedson, "Quantum Computing: How to Address the National Security Risk."
[28] Marco Piani, "QUANTUM THREAT TIMELINE REPORT 2022," 2022.

protection for government-owned and operated information systems. Finally, areas of critical infrastructure must also be brought into focus because ownership of critical infrastructure such as water, electricity, internet, and sewage are constantly being upgraded in order to make servicing them more cost-efficient. Often, good security practices are merely considered another cost, as indicated by the Colonial Pipeline ransomware, which stopped the flow of petroleum and gasoline products on the East Coast of the United States for several days.[29]

At the end of the day, the best solution is one where the government can develop a standard and then mandate that the standard be applied across the information technology sector so that the many different critical infrastructures, industries, and government and military capabilities that rely upon it will be safeguarded. It is still in the best interest of leaders to remain aware of the advancements in quantum computing and the potential threats posed to their industries.

Bibliography

"A Brief History of Cryptography." Accessed November 4, 2023. https://www.redhat.com/en/blog/brief-history-cryptography.

[29] John Keary, "Rebuffing Russian Ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for Ransomware.," n.d.

Barker, William. “MIGRATION TO POST-QUANTUM CRYPTOGRAPHY,” n.d.

Campbell, Robert. “Evaluation of Post-Quantum Distributed Ledger Cryptography.” *The Journal of the British Blockchain Association* 2, no. 1 (May 4, 2019): 1–8. https://doi.org/10.31585/jbba-2-1-(4)2019.

CIS. “Election Security Spotlight – CIA Triad.” Accessed May 15, 2023. https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/.

“Exploring Quantum Computing Use Cases for Electronics,” n.d.

Global Risk Institute. “2022 Quantum Threat Timeline Report.” Accessed November 4, 2023. https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.

Grumbling, Emily, and Mark Horowitz, eds. *Quantum Computing: Progress and Prospects*. Washington, D.C.: National Academies Press, 2019. https://doi.org/10.17226/25196.

Hassija, Vikas, Vinay Chamola, Adit Goyal, Salil S. Kanhere, and Nadra Guizani. “Forthcoming Applications of Quantum Computing: Peeking into the Future.” *IET Quantum Communication* 1, no. 2 (2020): 35–41. https://doi.org/10.1049/iet-qtc.2020.0026.

Herman, Arthur, and Idalia Friedson. “Quantum Computing: How to Address the National Security Risk,” n.d.

Keary, John. “Rebuffing Russian Ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for Ransomware.,” n.d.

Lotrionte, Catherine. “Countering State-Sponsored Cyber Economic Espionage under International Law.” *North Carolina Journal of International Law and Commercial Regulation* 40, no. 2 (2015 2014): 443–542.

Mohr, Niko; Pflanzer, Anika; Soller, Henning. “The Quantum Technology Monitor, Facts and Figures.” McKinsey & Company, December 2020. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/the%20rise%20of%20quantum%20computing/quantum%20technology%20monitor/2020/mckinsey-quantum-technology-monitor-202012.pdf.

Morello, Andrea. “Double or Nothing: Could Quantum Computing Replace Moore’s Law?” The Conversation, June 2, 2011. http://theconversation.com/double-or-nothing-could-quantum-computing-replace-moores-law-362.

Mosca, Michele. “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?,” 2015. Cryptology ePrint Archive. https://eprint.iacr.org/2015/1075.

Mulholland, John, Michele Mosca, and Johannes Braun. “The Day the Cryptography Dies.” *IEEE Security & Privacy* 15, no. 4 (2017): 14–21. https://doi.org/10.1109/MSP.2017.3151325.

Petrenko, Kyrylo, Atefeh Mashatan, and Farid Shirazi. “Assessing the Quantum-Resistant Cryptographic Agility of Routing and Switching IT Network Infrastructure in a Large-Size Financial Organization.” *Journal of Information Security and Applications* 46 (June 1, 2019): 151–63. https://doi.org/10.1016/j.jisa.2019.03.007.

Piani, Marco. “QUANTUM THREAT TIMELINE REPORT 2022,” 2022.

“Post-Quantum Cryptography Initiative | CISA.” Accessed May 14, 2023. https://www.cisa.gov/quantum.

“Quantum Computing Use Cases—What You Need to Know | McKinsey.” Accessed November 4, 2023. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know.

“Quantum Simulators Wield Control over More than 50 Qubits,” November 29, 2017. https://jqi.umd.edu/news/quantum-simulators-wield-control-over-more-50-qubits.

Scarani, Valerio, and Christian Kurtsiefer. “The Black Paper of Quantum Cryptography: Real Implementation Problems.” *Theoretical Computer Science*, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, 560 (December 4, 2014): 27–32. https://doi.org/10.1016/j.tcs.2014.09.015.