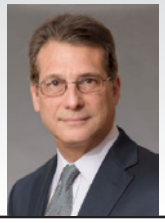
feature

Roy Altman, Peopleserv



The Quantum Apocalypse is Coming! Is HR Ready?

Quantum computing, an esoteric branch of computer science, holds promises of vast computing power once it becomes viable. One use case is that it will render all current encryption schemes vulnerable. Thus, all information on the web will become immediately hackable, which would mean that the internet, as we know it, will be fundamentally changed, and unless we adapt, we risk a chaotic outcome.

Quantum computing is still in the theoretical stage. A stable, functional machine is still a few breakthroughs away. Such breakthroughs may not arrive for decades or never occur, or they could be just a couple of years away. Regardless, we have no plan to protect the data on the web, and may be caught unprepared if those breakthroughs come early. Harkening to Y2K, the term Y2Q stands for "years to quantum." However, with Y2K we knew exactly the deadline to fix the problem, and what that fix was. In the case of Y2Q, we know neither. Quantum computers can create an encryption scheme that is not vulnerable, but you need quantum computers to enact it – the same computers that could be used to break encryption!

Human Resources is not prepared! This article will explain quantum computing and the nature of the encryption issue, in layman's terms, and propose a roadmap to keep our data protected. We must raise awareness of this issue and find a way to address it.

What is Quantum Computing?

Albert Einstein once said: "If you can't explain it simply, you don't understand it well enough." Well, here goes: Quantum mechanics theorizes that an object can be in two states simultaneously, and only resolves into one of those states when it is observed. The classic example is the thought experiment known as Schrödinger's cat. In it, a cat, a flask of poison, and a radioactive source are placed in a box. If a Geiger counter detects radiation, then the flask is shattered and the cat killed. The cat is thought to be both alive and dead simultaneously until someone looks in the box – then the cat is observed as either alive or dead (most cats I know would decline to participate in a demonstration of the experiment). As odd as this sounds, it is the way the universe works, and has practical implications in computing. In traditional computing, each bit has two states: on or off (1 or 0). Bits combine with millions of others to form the information that we access over the web, or are used by systems to perform the tasks that we automate. In a quantum computer, however, each bit, called a qubit (or sometimes, a qbit), can have many states: on, off or some combination. The combination is called *quantum superimposition*. Since qubits have many possible states instead of two, they have access to vastly more information in the same amount of time as a conventional computer.

Quantum mechanics also has a property called entanglement, which Einstein described as "spooky." With entanglement, when a particle is observed and resolves into a state, another particle *entangled* with it will resolve into the same state. These particles will react this way even when the particles are a vast distance from each other! Spooky, indeed!

Uses of Quantum Computing

Having a computer that can process information much faster than conventional computers has many applications, such as complex decision-making or optimization, but the most significant one is its application to the field of cryptography.

Cryptography is the process of encoding information to keep it private, even when it is being transported over a public medium, such as the internet. Strong cryptography involves factoring two very large numbers, and the key to decode the information can be any one of the results of the factorization. Conventional computers, even the fastest supercomputers in the world, would take hundreds of years to try every combination. Strong encryption is

defined as anything over 256 bits. With current technology, it would take $3x10^{51}$ years to try every combination. These days, the highest encryption algorithm uses 4096 bits! Thus our information is safe from prying eyes.

President Bill Clinton legalized strong cryptography for export by executive order in 1996, in part because the banking industry wanted to conduct online banking. This spawned the e-commerce era, so information can be sold over the web and the sensitive details behind each transaction are private. Opponents of the export of strong technology argued that terrorists would use encryption to plot attack, which of course has occurred.

Before the web, companies kept their information private by owning the computers it resides on and the physical wires connecting the computers along private networks. The World Wide Web, invented by Tim Berners-Lee in 1989, connected us all over the internet using protocols that all computers can understand. The addition of strong encryption turned the web into a place where financial transactions, application software and messages are kept private even though they are being conducted on a public network.

Because quantum computers are orders of magnitude faster than conventional computers, they can try every combination and find the key in a matter of minutes rather than hundreds of years, exposing all private information on the web.

Quantum computers can enact a form of encryption that is safe from other quantum computers. The algorithm relies on the property of entanglement to inform the data owner that the message is being tampered with. However, it's a chicken and egg scenario in that the technology to safeguard data in the future is the same technology that can hack messages currently.

State of the Technology

The issue with quantum computing is that the qbits are unstable – too unstable to be reliable. We need reliability to be .999999 (or six nines). Creating enough stable qubits to do meaningful work is not here yet. Part of the problem is engineering, whereby we can expect steady, incremental progress, and the other part will rely on breakthroughs in materials science which are yet to occur, and we don't know when, *or if*, those breakthroughs will occur. Major technology companies and governments are working on quantum computing. This past October, Google claimed a breakthrough that was a proof of concept of quantum computing's potential.[1] Although experts disagree about the impact of Google's accomplishment, it underscores the urgency about planning for a future where current encryption schemes are laid bare. IBM has seen exponential progress in quantum computing power in the years since 2017.[2]

While companies such as Google and IBM are investing huge sums of money in quantum computing, so are governments such as China.[3] [4] Who knows who will develop these machines with nefarious intent?

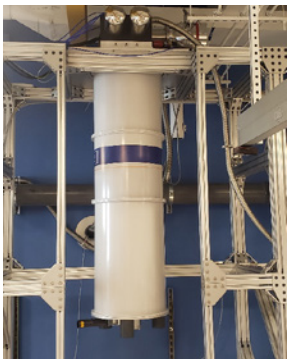
The creation of quantum computers requires the commitments of governments, academia or large technology companies. It's akin to the development of the first computer, the ENIAC, in the late 1950s – a post-WW II, cold war, arms race effort.

According to Javad Shabani, assistant professor of Quantum Computing at New York University, "The problem is that the qbits are unstable: how stable they are and how stable they need to be. If I could get to 51 qbits within 1 to 10^6 reliability, I could do anything I want." He predicts that we will reach that point within 5 to 10 years. Although all quantum computing scientists agree that encrypted data will be vulnerable with the advent of viable quantum computers, cybersecurity experts seem unfazed. When I mention the impending threat of quantum computing to cybersecurity, those experts tend to say "I'll be retired by then, so someone else will have to worry about it." Yet, 5 to 10 years may be well within their career spans.

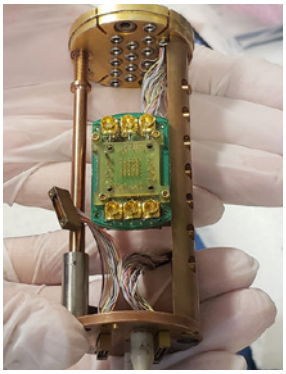
Quantum chips are very volatile and need to be kept at just a few degrees Kelvin above absolute zero. At NYU, they manufacture their own qbit chips, using cryogenic tanks that are able to achieve temperatures that low. Dr. Shabani says the effort involves a collaboration of computer science, materials science, physics, electrical engineering and radio frequency engineering companies.

What Should We do About it?

Before the internet, data and systems were secured physically as on-premise systems. If companies wanted to send data to a remote user, they did so over a network that was



Cryogenic tank at the NYU Quantum Computing lab, used to manufacture qbit chips.



Qbit chip manufactured for the cryogenic tank.

Graduate Research Assistant Joseph Yuan (L) and Professor Javad Shabani of NYU
(See bio on next page)

owned and secured by the company. It was expensive and of limited utility to have private networks, but it was the only way of ensuring that data would remain private, because strong encryption wasn't widespread.

In a quantum computing future, we may have to go back to private systems and networks. However, that, in itself, doesn't solve the problem. Encrypted messages can be captured and stored today, and decrypted once quantum computers are available.

I can foresee a "Mad Max-like" future, where bandits look for encrypted data on the public internet that they can exploit, and companies scramble to stuff their data onto fortified computers unconnected to the web. Transmitting data along private wires will be akin to navigating an oil tanker through the Strait of Hormuz, trying to avoid Somali pirates.

Companies need to begin to plan for a future where their data may not be safe. It is not too early to begin to think about a strategy. It will not happen overnight – breakthroughs may accelerate over time, but it's unlikely that a major breakthrough will occur without some notice that we are close.

1. **Anticipate risks and devise a plan** – We are no longer in the realm of *if* quantum computing will become viable. Our concern now is when. Of course, the breakthroughs needed may never occur, but it's unlikely, and foolhardy not to plan. Once we are about two to three years from a viable quantum computer, the plan needs to be invoked. Here are some steps that should be taken:
   - **Make your data private** – Begin migrating sensitive information from the web to private storage. This will mean giving up e-commerce revenue, but it would be negligent to allow information to continue to be exposed. Work with your cloud vendors to see if they have a plan to deal with this situation. Devise a backup plan for your mission-critical applications. Contact your cloud vendors and ensure that *they* have a plan.
   - **Construct private networks** – Begin creating physical private networks (as we had in the mainframe days), with limited access points. Commerce can continue, but from fewer locations. Data security will be more about physical security rather than the encryption/hacking arms race we have now.
   - **Implement quantum cryptography** – Begin laying the groundwork for the future by using quantum encryption. Gradually reintroduce quantum encrypted data back onto the publicinternet.

Quantum computing has much promise to take computing to a new level, and solve many vexing problems that will help humanity. However, all online computing, or life as we know it, will be irrevocably changed once it is viable. We need to make these issues part of our discourse and planning if we are to avoid catastrophe. The time to begin planning is *now!*

Endnotes

[1] https://www.nytimes.com/2019/10/23/technology/quantum-computing- google.html?searchResultPosition=3

[2] https://www.ibm.com/blogs/research/2020/01/quantum-volume-32/

[3] https://www.washingtonpost.com/technology/2019/12/26/chinas-top-quantum-scientist-has-ties-countrys-defense-companies/

[4] https://www.technologyreview.com/s/614776/how-suspicions-of-spying-threaten-cross-border-science/

About the Author

Roy Altman is an adjunct professor of NYU's new MS in Human Capital Analytics and Technology program. He is also the founder/CEO of Peopleserv, a software/services company. Over a multifaceted career, he has a history of delivering ROI to well-known companies in several industry sectors and is the creator of multiple commercial software products. He has co-authored six books on Business Process Management (BPM), and has published articles in IHRIM Workforce Solutions Review and The Saturday Evening Post. Altman has presented at several HR and BPM industry and academic conferences. He currently serves as co-managing editor of Workforce Solutions Review magazine and on the board of IHRIM. He can be reached at ***roy@peopleserv.com.***

Javad Shabani is an assistant professor of Physics at New York University and a member of the Center for Quantum Phenomena. He received his Ph.D. from Princeton University and conducted post-doctoral research at Harvard University and University of California, Santa Barbara. His research is primarily focused on quantum computing, topological superconductivity and developing novel superconducting devices. Shabani is an expert in epitaxial growth of quantum materials and developing hybrid solutions for computation technologies. He is the recipient of the U.S. Army and U.S. Air Force early career awards. He can be reached at ***jshabani@nyu.edu***.