Global Information Assurance Certification Paper

Straddling the Next Frontier Part 1: Quantum Computing Primer.

GIAC (GCIA) Gold Certification

Author: Eric Jodoin, ejodoin@hotmail.com
Advisor: Stephen Northcutt

Accepted: June 4 2014

"The irony of quantum computing is that if you can imagine someone building a quantum computer that can break encryption a few decades into the future, then you need to be worried right now"

Dr. Daniel Amihud Lidar - Director and co-founder of the USC Center for Quantum Information Science & Technology(CQIST)

Abstract

Theoretical designs of Quantum Computing are progressively transmuting into practical applications. But, how soon will such applications of quantum physics phenomena become available? How will they impact the Cyber Security landscape? As cyber security professionals, what must we know and what must we start doing today to be ready? This paper postulates that quantum technologies have already begun impacting the cyber security landscape through current and nascent practical applications. We already have one proverbial foot over the quantum computing fence. But, to truly appreciate the opportunities and threats it represents to the cyber environment, we must first develop a basic appreciation of quantum theories. Part one of this research project introduces the reader to basic quantum physics principles and how they can be applied to computing. It also sheds light on the current progress and worldwide efforts on research and development of quantum computing technologies.

1. Introduction

Theoretical designs of Quantum Computing are progressively transmuting into practical applications. News articles announcing breakthroughs are appearing in main stream media just about every month. Hacking and cyber security conferences have begun offering presentations on the subject. In fact, it is a lecture by Blake Cornell at Hackfest (Quebec City) in November 2013 which stirred my curiosity. It set me on the path to researching what was quantum computing and how it will impact the cyber security landscape. Then in December 2013, a posting in the SANS GIAC Advisory Board Discussion mailing list regarding Quantum Computing research done by the NSA resulted in over 20 responses. Most of which highlighted the absence of consolidated information available to cyber security professionals regarding the subject. This is when it became obvious there was an informational need regarding the impact of quantum computing on the cyber security landscape and Gold Papers could help fill that need.

As esoteric as the terms Quantum Physics and Quantum Computing may sound, one does not need to be a mathematician or physicist to understand the underlying principles. This paper will only quickly touch the aspects of quantum physics necessary to understand its application in quantum computing. The following books are recommended for readers interested in further broadening their understanding of quantum physics:

- 101 Quantum Questions by Kenneth W. Ford. (2011)
- A Shortcut Through Time: The Path to the Quantum Computer by George Johnson. (2003)
- The Bit and the Pendulum: From Quantum Computing to M Theory--The New Physics of Information by Tom Siegfried (2000)

Research in quantum computing has been progressing steadily over the last few decades. What could only be imagined through science fiction or thoughts experiments only a few years ago is quickly morphing into practical experiments. There remains little

Eric Jodoin, ejodoin@hotmail.com

doubt that quantum computing technologies are poised to undergo an explosive growth in the near future. Therefore, the questions we now must seek to answer are:

1. How soon will practical applications of quantum computing become available?
2. How exactly will they impact the cyber security landscape?
3. What must we know and what must we start doing today to be ready?

The inner workings of quantum computers are strikingly different from computers in use everywhere else. Since today's computers rely on classical physics to operate, they will be referenced throughout this paper as classical computers. It is unclear who coined the term classical computer. However, it is the term used throughout research papers and other literature on quantum computing when comparing quantum computers with computers not using quantum physics in their inner workings.

The advent of quantum computing will be no less revolutionary than classical computing turned out to be. It will also have a profound impact on cyber security professionals from the analyst investigating an incident to the CISO considering mitigation measures in response to a Threat Risk Assessment. In fact, some of the changes are so profound and revolutionary; it behooves cyber security professionals to take them into consideration today. Especially when considering that some of the threats and benefits emanating from quantum physics in general and quantum computing in particular have already begun to materialize.

This gold paper is part one of a two part research project to assess the impact of quantum computing on cyber security. To truly appreciate the opportunities and threats quantum computing represents to the cyber environment, it is essential to develop a basic appreciation of quantum physics principles and understand the progresses made in developing quantum technologies. Part one of this research project presents the following:

1. Basic quantum physics principles and how they can be applied to computing;
2. Timeline and current state of quantum computing research; and,

3. The worldwide race and intensity of efforts focused on research and development of quantum computing technologies.

2. Quantum Computing Primer

Quantum Computing is expected to revolutionize many aspects of society. Some of the physical limitations constraining classical computers today may soon be overcome by quantum computing technologies. Biology, chemistry, meteorology and many other fields of research will benefit, even quantum physics research itself is expected to significantly advance thanks to quantum computers. But, to understand potential applications in any field of expertise, including cyber security, some understanding of the underlying science is necessary. By understanding the basic concepts and recent advances in quantum physics, it becomes easier to appreciate how much the world has progressed toward harnessing the power of quantum computing. Grounded in this knowledge, cyber security professionals can then begin to assess the impact various quantum computing technologies have begun to exert on cyber security. And finally, begin to devise ways to leverage quantum physics and quantum computing for their benefit while preventing others from using that same technology back against their enterprise.

2.1. A Very Brief History of Quantum Physics

Isaac Newton's law of motion and James Clerk Maxwell's theory of electromagnetic fields are prime example of classical physic (McEvoy & Zarate, 2007). Most readers will be somewhat familiar with these principles having studied them at some point in their academic upbringing. Early work in classical physics can be traced back to Galileo in the sixteenth century with the majority of advancements having been made in the seventeenth, eighteenth, and nineteenth centuries (Ford, 2011).

By the middle of the nineteenth century, the broader scientific community felt quite confident that any phenomenon could be explained by classical physic. But, as scientific discoveries fueled new technologies, scientists were able to study increasingly smaller systems. By the late nineteenth century, scientists were beginning to study atoms and molecules. They quickly realized that the laws of classical physics inherited from

Newton, Maxwell and the likes failed when dealing with the infinitely small. Although perfectly adequate at explaining larger systems, classical physics was unable to explain how atoms behaved or why radiation came out of hot objects (Laflamme, 2013).

The term "quantum" and its plural form "quanta" was coined by Max Planck in 1900. Having exhausted all classical theories while trying to explain a phenomenon known as cavity radiation, he performed what he himself called "an act of desperation". He deviated from classical Physics dogma and postulated that cavity radiation was emitted only in bundles he called quanta (Ford, 2011). Without going into mathematical details, it suffices to say that Planck introduced a formula that ushered a new, if revolutionary, idea in physics. The world around us was not smooth and continuous as imagined in classical physics but rather, it came in distinct, equal pieces.

Kenneth W. Ford explains it best in his book, 101 Quantum Questions:

"A quantum is a lump, a bundle. There are lots of things that come in lumps of certain sizes such as loaves of bread. But there is no law of nature saying how big the loaf of bread has to be. The baker could add or subtract a slice or even a crumb, making it a little heavier or lighter. Not so in the small-scale world where quantum rules govern what happens" ... "A Hydrogen atom has a certain diameter. It can't be made any smaller than that. Associated with that size is a certain energy called ground state energy. Every hydrogen atoms in its ground state is exactly the same. The hydrogen atom can be made larger and more energetic but only in quantum increments"..."An electric charge cannot be trimmed finer than the amount carried by one proton. Nor can there be 3.7 quantum units of charge. Every charge in the universe is a whole-number multiple of the proton or electron charge"

Quantum physics also teaches us that even light comes in quantum increment commonly called photons. Thankfully, our eyes require half a dozen quanta before they fire a signal to our brain. Should they be able to fire a signal for every light quantum they receive, every source of light would look like a stroboscope.

Planck's work ushered a quarter century of intense debate and experimentation by leading physicists that included the likes of Albert Einstein and Erwin Schrödinger. Most of the work, including Planck's own work, was aimed at disproving the quantum

mechanics model in favor of classical physics. In a bizarre twist of faith, all of the research turned out to strengthen Planck's original idea instead of disproving it (McEvoy & Zarate, 2007). Thus Quantum Physics was born. Debate on some aspects of quantum physics still rages today. But, the basic principles have been proven in practical experiments and some unique characteristics of quantum Physics are particularly well suited to the fields of computing and communications.

2.2. Principles of Quantum Physics

Principles of classical Physics such as electromagnetism are widely used today in computing and communication. Although a deep knowledge of electromagnetism is not required, some appreciation of where and how it is employed can help cyber security professionals. For example, understanding that a Wifi signal can travel beyond a controlled space and be eavesdropped may prompt a cyber security professional from taking additional defensive measure such as reducing the power of the transmitter, encrypting the signal, using directional antennas, and/or establishing an inspectable zone outside a building.

The same can be said of quantum physics. A basic understanding of the principles will help the cyber security professional assess potential defensive and offensive applications. Not all quantum physics principles are covered in this paper. Only the ones most applicable and only in so far as needed to appreciate their potential application to computing in general and cyber security in particular.

2.2.1. Quantum Superposition & Qubits

Defying common sense and everything we know from classical physic, the quantum superposition principle stipulates that a single particle can be in multiple states at once. For example, an electron can be thought of as spinning clock-wise and counter-clockwise simultaneously. As the human brain is simply not equipped to intuitively understand subatomic particles, explaining how this can be possible is well beyond the scope of this paper. Suffice to say that in the decades since quantum Physics has been discovered, physicists and philosophers have not stopped arguing over what it means (Johnson, 2003). Readers interested in better understanding quantum Physics phenomena introduced in this paper are encouraged to read the additional material proposed in the

introduction. Regardless of how and why this particular characteristic happens to be, its potential is nothing short of remarkable.

In classical computing, a single bit of information can only be in either of two states: 0 or 1. But at the quantum level, a single bit, which is called a quantum bit or qubit, can be both 0 and 1 simultaneously. Arrange two qubits together and they can simultaneously represent four distinct combinations (00,10,01,11). In essence, two qubits can be compared to four distinct instructions or parcels of data being processed simultaneously in parallel. In fact, the number of simultaneous combination equals 2^x where x is the number of qubits. Three qubits can simultaneously represent height combinations, four cubits can represent sixteen, twenty-two cubits can represent over four million combinations, etc…

Size is also a significant factor. Because we are talking about bits subject to the laws of quantum physics, qubits will be made of a single atom. Considering that a single grain of sand holds approximately 2.2×10^{19} atoms (Wittich, 2008), the processing capacity of that single grain of sand could theoretically far exceed the capacity of any existing supercomputer.

To put this processing potential into perspective, take the most advanced supercomputer in operation today (Top 500 Supercomputer Sites, 2013). Named Tianhe-2 (MilkyWay-2), it is operated by China's National University of Defense Technology (NUDT) in Guangzhou. Consuming as much power as a small city, it can process over 3 million calculations simultaneously thanks to its 3.12 million cores working in parallel. In comparison, a quantum computer with only 22 qubits would be able to simultaneously evaluate $2^{22} = 4{,}194{,}304$ probabilities, outperforming Tianhe-2. Such is the power of quantum computing (Johnson, 2003).

Using qubits instead of classical bits is still easier said than done. With one limited exception discussed latter in section 2.3.3, qubits are still confined to laboratories because of the equipment and conditions necessary for their manipulation. But, the potential of qubits opens up a world of new possibilities to solve problems that explode exponentially on classical computers. Factoring very large numbers used to secure public

key cryptography immediately comes to mind and will be covered in the next half of this research project.

2.2.2. Probability Waves and Quantum Indeterminacy

At first glance, it would seem that qubits can hold exponentially more information than classical bits. However, that is not quite accurate. In reality, it is only a probabilistic superposition generally referred to as a probability wave. For as long as qubits remain undisturbed, they can be thought of as holding all probable values. This is known as quantum indeterminacy (Johnson, 2003). But, the instant a qubit is measured, the probability waves collapse into a single outcome. Absent any kind of manipulation, an observer is equally likely to be seeing a 0 or 1. The trick to quantum computing is to manipulate the qubits in such a way that it will collapse into the desired outcome.

Again, the details behind these principles are well beyond the scope of this paper. But, there are a few key points that are important. First of all, quantum particles can be a source of true randomness thanks to quantum indeterminacy. The mere fact of observing a quantum particle forces it into a single state (Johnson, 2003). Repeated measurements are equally likely to turn up a 0 or 1. Repeat the measurement 4096 times absent any other outside manipulation or interference and you have a truly random 4-kbit key.

Second, because merely observing a quantum particle forces it into a particular state, this property can be used to detect surveillance or manipulation attempts. This is particularly significant when trying to protect a communication from eavesdropping. It also provides a mean of detecting a Man-in-the-Middle attack which could not be accomplished without attempting to measure the particle and forcing it into a single state.

Finally, probability waves can be used to manipulate qubits for computational purposes. Imagine a single drop of water creating small waves in a pond. Next, imagine several water droplets hitting the pond following a programmed sequence. An observer would be able to see the waves interacting with each other. Some waves would cancel each other out while some others would merge and become bigger. Now, replace the water droplets with laser beams firing quantum photons at qubits and imagine the probability waves of qubit particles interacting with each other the same way as waves in a pond. By selecting which photon hits which qubit in a specific sequence, some

probability waves will cancel each other out and ultimately, a single wave will prevail. This process is the quantum equivalent of a running program and its output would be the observable outcome the qubits particles would collapse onto during the measurement.

2.2.3. Quantum Entanglement

In 1935, Einstein and two young colleagues (Podolsky and Rosen) tried to prove that the theory of quantum mechanics was flawed in what became known as the EPR argument. The intent was to demonstrate how the idea of superposition was absurd. To do so, they asked physicist to consider a particle that decayed to produce two photons flying off in opposite directions. Assuming the particle had a spin of 0, the two photons it produced would each be spinning in opposite directions, for a net effect equal to the decaying particle's spin of 0. Therefore, one photon would be spinning clockwise while the other would inevitably have to be spinning counter clockwise.

But, if superposition was true, both photons would be simultaneously spinning clockwise and counter clockwise. The EPR argument proposed that this would lead to a contradiction. If at some point in time after the particle decayed one of the photon was measured, it would have to randomly snap into a clockwise or counterclockwise spin. Then the other photon must immediately snap into the opposite spin. But, since the 1st photon randomly selected which way it spun at the exact moment it was measured. And since no time had passed in which any kind of detectable signal could be sent from the 1st photon to the 2nd to tell it which way to spin, there had to be something missing in quantum physics theory.

Although this is inconceivable in our classical view of the world, numerous experiments have demonstrated that this is exactly what happens at the quantum level. Furthermore, there are no limits as to how far the entangled particles can be. It is almost as though the two particles were not separate entities but two faces of some larger thing (Johnson, 2003).

Quantum entanglement can have interesting practical applications in cyber security. First of all, entanglement helps bridging the quantum world to the physical world. With its deterministic property which forces an entangled particle into particular state, it can be used to simulate other deterministic contraptions such as a classical

computer (Johnson, 2003). In essence, it provides a medium for the transfer of data from the quantum realm where it was computed into the physical realm where it can be interpreted by classical computers.

But more astonishing, imagine numerous pairs of entangled particles. A single particle from each pairs would be kept by the sender while the others would be given to a receiver. The sender could manipulate the particles as described in the last paragraph of section 2.2.2 and then measure them. At the other end, the receiver would be able to immediately observe the other half of the entangled particles forced into the opposite state. Just like that, a message was communicated over some great distance without the messages having travelled in between the two locations.

2.3. Advances in Quantum Computing

Recognizing the theoretical potential of quantum particles for computing and communication is something. But translating this potential into practical applications is an order of magnitude more difficult, requiring significant investments in research and development (R&D). It is nothing short of reinventing how computers function at their core.

In the classical sense, computers are composed of very small physical objects that can be in two distinct states, 1 or 0. Since the early days of computing, computer circuitry has been using principles anchored in classical physics. First built using large electrical relays and mechanical switches, computer circuits have significantly shrunk to a point where millions of microscopic switches are packed in today's CPUs. Despite all that miniaturization, each individual switch remains so big that its operation is still governed by the laws of classical physics (Johnson, 2003).

2.3.1. The Origins of Quantum Computing

For years, scientists and engineers believed that as computer circuitry shrunk in size, they would eventually reach a threshold where quantum effects would interfere with the storage and manipulation of the data, making it impossible to shrink circuitry any

further. Then in 1982, Richard P. Feynman[1] and Paul Benioff[2] both published separate research papers which introduced mutually supporting ideas for harnessing the attributes of quantum physics as an alternative to solve computationally demanding problems (West, 2003).

In very broad terms, Feynman and Benioff proposed that instead of trying to counteract the effects of quantum physics in computer circuitry, the circuits could be shrunk small enough that quantum physics would take over from classical physics. Then, instead of employing the attributes of classical physics to compute data, quantum Physics attributes would be used. Thus the idea of a Quantum Computer was born. This ushered a new era of research and technological breakthrough that has seen significant progress toward the ultimate goal of building a useable quantum computer.

2.3.2. Recent Developments

Quantum computing technology has progressed a great deal since Feynman and Benioff. At first, mathematicians and physicist worked at demonstrating practical uses. The idea of Quantum Key Distribution (QKD) was introduced in 1984 (Bennett & Brassard, 1984). Then in 1991 Peter Shor published an algorithm that would allow a Quantum Computer to factor large integers and solve discrete log problems (Johnson, 2003). In 1995, Peter Shor proposed the first Quantum Error Correction scheme, soon followed by others. Then in 1996, Lov Grover introduced a quantum algorithm for game tree which promised to significantly improve database search and automated source code review (Johnson, 2003).

As humanity neared the 21st century, numerous technological advancements refined our ability to observe and manipulate quantum sized particles. The first experiments with 2-qubits took place at Oxford University in 1998, quickly followed by a 3-qubit system. By 2000, Los Alamos National Laboratory was able to demonstrate a 7-qubit "computer". Then in 2006, theorists and experimentalists at the Institute for Quantum Computing (IQC) in Waterloo, along with MIT in Cambridge, had extended

[1] *Simulating Physics with Computers.* International Journal of Theoretical Physics, Vol 21, Nos. 6/7, 1982

[2] *Quantum mechanical hamiltonian models of turing machines.* Journal of Statistical Physics, Volume 29, Issue 3, pp.515-546 11/1982

their experiments up to 12 qubits (Perimeter Institute for Theoretical Physics, 2006). It is important to note that all of these quantum computing devices were not full-fledged computers. But with some coaxing, scientists were able to run Shor's quantum algorithm on these systems to factor 15 into 3 and 5. Although a simple task to accomplish, it succeeded in extrapolating the usefulness of quantum computers when considering much larger numbers.

Over the last five years, new discoveries have multiplied at an exponential rate. A quick google search of the term "Quantum Computing" reveals new discoveries announced on an almost weekly basis. This effervescent research environment stimulates breakthroughs often believed to be still years away. For example, in November 2013 the Canadian Broadcast Corporation (CBC) news website, announced that Canadian researchers succeeded in keeping qubits at room temperatures for 39 minutes (Chung, 2013). The previous record was 25 seconds. Such astounding leaps in research makes it virtually impossible to predict how soon quantum computers will become a reality. But, in the absence of a hard timeline, it would be prudent for cyber security professionals to assume the arrival of quantum computers able to run Shor's and Grover's algorithms within the next decade and perhaps even sooner.

2.3.3. Current State of Quantum Computers

In 2007, a previously little known company by the name of D-Wave rocked the scientific and business world by demonstrating a working quantum computer at the Computer History Museum in Mountain View, California (Jones, 2013). The news was met with much skepticism from the scientific community. D-Wave was the first to admit that its design was not built to run advanced quantum algorithms such as Shor's or Gorver's. Rather than trying to take on these difficult problems, D-Wave simply aimed to solve adiabatic equations more efficiently than possible on a classical computer. Adiabatic equations are used to solve optimization problems such as pattern matching or face recognition where there may be multiple solutions but only one is optimum. This is notoriously slow on classical computers where each solution must be evaluated and compared sequentially (Johnson, 2003). Subsequently, Google developed a D-Wave quantum algorithm that leveraged adiabatic equations for a binary image classifier that

could be used to tell whether a medical image showed a tumor (Jones, 2013). Still, the scientific community questioned the benefit of an adiabatic quantum computer and was wondering if D-Wave's device was not simply a classical computer disguised as a quantum one.

Despite the controversy, D-Wave attracted interest from buyers. In 2011, Lockheed-Martin acquired a 128-qubits computer appropriately named D-Wave One (Merali, 2011). In 2013, Google in partnership with NASA procured a 512-qubits computer, named D-Wave Two, with the intent of upgrading it to 2,048-qubits once the technology becomes available sometime in 2015 (Hardy, 2013).

Today, criticisms toward D-Wave's quantum computers have been quieted to some degree. But, they have been replaced by subtler questions (Jones, 2013):

1. Even if D-Wave computers are harnessing quantum powers, is it really faster or better than conventional computers?
2. Will they eventually crack problems deemed intractable by classical computers like factoring large numbers or will it hit some developmental wall?

Only the future will tell but one thing is certain, the early successes of D-Wave and the names of clients in its order book is sure to attract new venture capitalists and engender other start-ups that will undoubtedly spur innovations. Not to mention giants of the industry such as IBM, who have been actively researching quantum computing for decades and have been making breakthroughs of their own (Mearian, 2012).

At the moment, D-Wave remains the only known commercial venture that offers quantum computing technology for sale. According to D-Wave's terms and conditions, its products and services are controlled by Canadian and US Export Laws. This is not surprising given the potential applications such as code breaking. This effectively restrains the dissemination of D-Wave quantum computing technology to entities and territories approved by the Canadian and US governments.

But, there is little doubt that governments and enterprises inside and outside of Canada and the US are actively funding research and development of quantum technology.

Eric Jodoin, ejodoin@hotmail.com

Given the breath of publically available research data on quantum technologies, it is possible that quantum computers closely matching D-Wave capabilities, or trying to solve other quantum algorithm, may be close to completion or even already in operations elsewhere.

2.4. Quantum Computing R&D Funding

With so many academic disciplines poised to significantly benefit from the power of quantum computing, quantum technologies in general and quantum computing research in particular are receiving substantial international attention and financial backing. Research Institutes and Centers of Excellence funded by a mix of public and private investment sources have been created in a dozen countries in the last decade alone. Although some investment and funding figures are made public, more is being kept secret for national security and competitive reasons by governments and private enterprises. While exact figures are hard to come by, a tally of publically announced funding in quantum information and quantum computing research over the last decade totals over one billion dollar worldwide when counting research grants and investments in research infrastructures.

2.4.1. Australia

According to the Australian Research Council Website[3], Australia committed over $74 million AUD for their Centre of Excellence for Quantum Computation & Communication Technology (CQC^2T) since 2002. An additional $46 million AUD was also injected through collaboration with the private sector and international partnerships. The CQC^2T has published 49 notable research papers since 2011 touching various aspects of quantum computing.

2.4.2. Canada

Canada has built a strong reputation in the quantum computing field and is home of the Institute for Quantum Computing (IQC) at the University of Waterloo. It has received over $100 million dollars in private and governmental funding since it was founded in 2002. Soon, IQC will have a complement of 30 faculty members, 50 postdoctoral fellows and 125 students (The Institute for Quantum Computing (IQC), 2014). Other Canadian Universities also devote time and money to research such as the

[3] http://www.arc.gov.au/ncgp/ce/ce_outcomes.htm

Institute for Quantum Science and Technology (IQST) at U of Calgary, and Dalhousie University which is credited for having developed the first high-level quantum programming language (Williams, 2013).

Canada is also the home of D-Wave. Founded in 1999, D-Wave Systems is the first commercial quantum computer manufacturer. Privately held, it has offices in Vancouver, Canada, Palo Alto, California and Washington, DC (D-Wave Systems, 2014). Amazon.com founder Jeff Beznos and In-Q-Tel, a known supplier to the US Intelligence community, reportedly invested $30 million into D-Wave in 2012 alone (Knapp, 2012). News media also reported that D-Wave One was sold for $10 million USD while D-Wave Two sold for $15 million.

2.4.3. China

Information on China's efforts to developing quantum computing technologies is scarce. But, a recent article in the South China Morning Post provides a rare insight. The article states that the National Natural Science Foundation of China funded 90 quantum related projects in 2013 alone. The article also quoted Professor Wang Haohua, a physicist at Zhejiang University who is reportedly trying to build a quantum computer with superconducting materials. He was quoted saying: "the central government is so eager - even desperate - to have quantum computers, that scientists have been told to ignore non-technical constraints such as cost and size". Then, he re-emphasized his comment by saying: "The value of the quantum computer to the military and government is so great, its cost has never been considered" (Chen, 2014).

The Chinese School of Physical Sciences employs 245 faculty staff and an undisclosed number of students. One of its four key laboratories has been doing research on quantum information since 2001 (Shcool of Physical Sciences, USTC, 2014). The Hefei Institutes of Physical Science employs 1,600 researchers and technicians alongside 1,200 students. One of its six research divisions has been working since 2008 on high magnetic fields that have applications in quantum computing (Hefei Institutes of Physical Science, 2014). Although there are no published figures indicating how much China actually spends on quantum computing research, at the very least it probably matches the US's funding.

2.4.4. The European Union

The European Union (EU) has invested over 23 million EUR in quantum computing Research since 2009 as part of its Quantum Information Foundations and Technology Initiative (CORDIS, 2013). In addition, The EU boasts four major research facilities that regularly make major contributions to quantum computing research. The Institute of Photonic Sciences (ICFO) was founded in 2002. The Austrian Institute for Quantum Optics and Quantum Information (IQOQI) was founded in 2003. Both located in Germany, the Max Planck Institute for the Science of Light (MPL) was founded in 2009 while the Max-Planck-Institute of Quantum Optics (MPQ) was founded in 1981. Together, these institutions employ several hundred researchers with a combined annual budget in the tens of million euros.

The EU, is also the home of ID Quantique (IDQ) which is headquartered in Switzerland. Although not strictly in the quantum computing business, it manufactures and sells security appliances that leverage attributes of quantum physics. Some of which will be presented in the second half of this research project. On October 2013, IDQ received 5.6 million in investments from QWave Capital, a venture capital firm focused on seeking out early stage private companies with breakthrough quantum technology (IDQ Press Release, 2013).

2.4.5. Russia

The Russian Quantum Center (RQC) was founded on December 14, 2010. A late comer in the quantum computing research industry, the RQC aims to make up grounds and turn Russia into a world leader in the field of quantum technology. According to an English presentation[4] given by one of RQC's group leader, Alexander Lvovsky, at the 2012 RU SCI Tech Forum, the RQC aims to become one of the world's top 5 quantum research institute with 100 to 200 scientists in 10 to 20 groups. The RQC appears to be funded by a mix of grants from Russian government agencies and Russian industries.

2.4.6. Singapore

Singapore founded its own Centre for Quantum Technologies (CQT) in 2007 to the tune of $100 million USD over 10 years with a particular focus on the Quantum

[4] http://www.ru-scitech-forum.org/wp-content/uploads/AlexanderLvovsky.pdf

Cryptography niche. The project was jointly funded by the Education Ministry and the National Research Council (Tan, 2007). According to its website[5], the CQT currently employs over 100 researchers. The CQT can boast of having made significant breakthroughs in both theoretical and applied research in various areas of studies such as Quantum Key Distribution.

2.4.7. The United States

In 2008, The United States Executive Office of the President National Science and Technology Council (NSTC) published a Federal Vision for Quantum Information Science[6]. This document recognized the transformational effect quantum computing will have on society. It also called for a coordinated approach between government agencies and national laboratories to prioritize research efforts nationwide. This document listed several organizations involved in quantum computing research:

a. The National Institute of Standards and Technology (NIST);
b. The National Security Agency (NSA);
c. The National Science Foundation (NSF);
d. The Intelligence Advanced Research Projects Activity (IARPA);
e. The Defense Advanced Research Projects Agency (DARPA);
f. The Department of Energy (DOE);
g. The Army Research Laboratory (ARL);
h. The Air Force Research Laboratory (AFRL); and,
i. The Naval Research Laboratory (NRL).

NIST was a pioneer in quantum computing research. In 1995, its Ion Storage Group demonstrated the first quantum-logic gate (NIST, 2012). With five distinct research groups involved in quantum computing work, it has made significant contributions to the field. In January 2014, the Washington Post revealed that the NSA had invested 79.7 million USD in the development of a quantum computer. NSA's other

[5] http://www.quantumlah.org/main/aboutus.php
[6] http://www.nist.gov/pml/div684/upload/FederalVisionQIS.pdf

investments in quantum computing research remain shrouded in secrecy but in 2006, NIST revealed that it had partnered with NSA and the University of Maryland to create the Joint Quantum Institute (JQI) to advance quantum physics research (NIST Press Release, 2006). Its initial annual budget was originally set at 6 million USD but it has likely grown in light of the 10.3 million allocated by NIST in 2010 to build the Laboratory for Advanced Quantum Science at the JQI.

Then there is the NSF with an annual budget of $7.2 billion. Each year, the NSF receives about 50,000 competitive requests for funding, and makes about 11,500 new funding awards. Obviously the NSF serves many disciplines but, it regularly grants funding in both theoretical and applied quantum research. A quick search for the word "quantum" on the NSF website[7] reveals hundreds of grants awarded, each worth several hundreds of thousand dollars. Although not all search results are related to quantum computing technologies, titles like "Exploring a Robust Quantum Cryptography Protocol for Securing Optical Burst Switching Networks" and "Entanglement and Coherence Decay in Nanosystems and Applications to Quantum Information Systems" have unmistakable applications in quantum computing.

On the Department of Defense side, IARPA funded three programs, two of which are still ongoing. The US ARL is also funding quantum information research programs in collaborations with the private and public sectors (U.S. Army Research Laboratory, 2013). Figures indicating the amount of funding have not been made public. However, in February 2012, IBM claimed major advances in quantum computing device performance that may accelerate the realization of practical, full-scale quantum computers (IBM Press Release, 2012). At the very end of the press release, IBM acknowledged support from IARPA through the Army Research Office (ARO) contract W911NF-10-1-0324. A Google search for this contract revealed pass-thru funding to Princeton University totaling 1.1 million USD between 2011 and 2013[8]. IBM Patented its findings in January 2012 and acknowledged having received federal governments support. This gives the federal government a claim on the patent should IBM decides to abandon it. But more

[7] http://www.nsf.gov/awardsearch/

[8] https://finance.princeton.edu/princeton-financial-overv/financial-facts/A-133AuditReportFY2010-2011.pdf
https://finance.princeton.edu/princeton-financial-overv/financial-facts/Princeton-A-133-Report-2013.pdf
https://finance.princeton.edu/princeton-financial-overv/financial-facts/A-133AuditReportFY2011-2012.pdf

importantly, it suggests that IBM invested a significant amount of its own funds into this research. The ARL also awarded 2.25 million in funding to researchers from the University of Wisconsin, and the University of the Saarland in Germany (Scalese, 2014).

2.4.8. India, Iran, France, Japan and others

Several other countries have invested resources and energy toward quantum computing research. India setup the Centre for Quantum Information and Quantum Computation (CQIQC) in 2010 as a 5-year Research Project[9]. Iran has held five International Conferences on Quantum Information since 2007[10]. France and Japan have banded together and formed the "Japanese French Laboratory for Informatics | quantum computing Research Team"[11]. Others invest in more fundamental research with practical application in quantum computing. For example, Israel's Weizmann Institute of Science continues to make discoveries in Quantum Physics that are directly applicable to quantum computing (Weizmann Institute of Science, 2008).

2.4.9. Private Enterprises

Several enterprises worldwide, big and small, are actively conducting research on quantum computing. Hewlett Packard (HP) has stood up the Quantum Information Processing (QIP) Group in Bristol, UK. Its areas of interest include Quantum Computation, Quantum Cryptography, and Quantum Communications (hp.com, 2014). MagiQ Technologies, QuintessenceLabs, and SeQureNet all currently sell technology based on quantum Physics. Like D-Wave and ID Quantique, these companies have recognized the potential windfall that would come with securing some portion of the emerging quantum technologies market.

3. Conclusion

Terms like quantum superposition, qubits, probability waves, quantum indeterminacy, and quantum entanglement are becoming ever more present in the communication and the computer sciences vocabulary. As a result, a basic

[9] http://cts.iisc.ernet.in/CQIQC.html
[10] http://iicqi.sharif.edu/
[11] http://www.qis.ex.nii.ac.jp/jfli_qc/

comprehension of these quantum physics principles is becoming increasingly unavoidable for anyone involved in cyber security. It is particularly important for anyone searching for emerging threats as well as opportunities to strengthen their organization's cyber security posture. By utilizing attributes of quantum physics, quantum technologies have already begun transforming computing technologies. Some quantum technologies like quantum key distribution can already help enhance communication security. Other technologies such as Shor's factoring algorithm, are already driving change in cyber security practices.

Existing and emergent quantum computing technology providers, such as ID Quantique and D-Wave, will continue to deliver evermore improved quantum technologies that fill niches meant to address specific needs. With quantum research funding estimated in the billions of US dollars and given the progress made in the last decade alone, there is little doubt that more advanced quantum computers will make their entry within this next decade. Initially, quantum computers will be for the exclusive use of select governments and large enterprises. Their existence creates both opportunities and threats to cyber security professionals.

Understanding basic principles of quantum physics applicable to computing in general and cyber security in particular is the first step in developing an adequate cyber security posture. Realizing the progress made thus far and being aware of the amount of investment supporting quantum technologies research and development helps us appreciate how far quantum technologies have progressed. One thing that will help cyber security professionals prepare and posture their resources to counter threats and take advantages of new opportunities is a look at quantum applications already in use or in latter stages of development. That is a research topic deserving to become a separate gold paper and the abstract has already been accepted by GIAC.

4. References

Bennett, C., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing.* Bangalore, India. Retrieved from http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf

Eric Jodoin, ejodoin@hotmail.com

Chen, S. (2014, January 10). *China in race to build first code-breaking quantum supercomputer*. Retrieved from South China Morning Post Online Edition: http://www.scmp.com/lifestyle/technology/article/1401755/china-race-create-first-quantum-code-breaking-supercomputer

Chung, E. (2013, November 14). *Qubit record moves quantum computing forward*. Retrieved from CBC News: http://www.cbc.ca/news/technology/qubit-record-moves-quantum-computing-forward-1.2426986

CORDIS. (2013, December 18). *FP7: FET Proactive Intiative: Quantum Information Foundations and Technologies(QI-FT)*. Retrieved from EU Community Research and Development Information Service (CORDIS): http://cordis.europa.eu/fp7/ict/fet-proactive/qift_en.html

D-Wave Systems. (2014, April 28). *Meet D-Wave*. Retrieved from www.dwavesys.com: http://www.dwavesys.com/our-company/meet-d-wave

Ford, K. W. (2011). *101 quantum questions: what you need to know about the world you can't see.* Cambridge, Mass.: Harvard University Press.

Hardy, Q. (2013, May 16). *Google Buys a Quantum Computer*. Retrieved 04 14, 2014, from Bits (New York Times Blog): http://bits.blogs.nytimes.com/2013/05/16/google-buys-a-quantum-computer/?_php=true&_type=blogs&_r=0#postComment

Hefei Institutes of Physical Science. (2014, April 30). *Introduction for High Magnetic Field Laboratory*. Retrieved from Hefei Institutes of Physical Science: http://english.hf.cas.cn/r/ResearchDivisions/HFML/

hp.com. (2014, April 30). *Quantum Information Processing*. Retrieved from hp.com: http://www.hpl.hp.com/research/qip/

IBM Press Release. (2012, February 28). *IBM Research Advances Device Performance for Quantum Computing*. Retrieved from IBM: http://www-03.ibm.com/press/us/en/pressrelease/36901.wss

IDQ Press Release. (2013, October 15). *Qwave capital invests $5.6 million in id quantique to drive the future of secure, encrypted communications*. Retrieved from idquantique.com: http://www.idquantique.com/press-releases/qwave-investment.html

Johnson, G. (2003). *A Shortcut Through Time: The path to the Quantum Computer.* New York: Alfred A. Knopf.

Jones, N. (2013, June 19). *Computing: The quantum company*. Retrieved from nature.com: http://www.nature.com/news/computing-the-quantum-company-1.13212

Knapp, A. (2012, May 10). *Jeff Bezos And The CIA Invest In D-Wave's Quantum Computer*. Retrieved from Forbes.com:

Eric Jodoin, ejodoin@hotmail.com

http://www.forbes.com/sites/alexknapp/2012/10/05/jeff-bezos-and-the-cia-invest-in-d-waves-quantum-computer/

Laflamme, R. (2013, Oct 1). From Wonder To Wow: Why The Quantum Age Is Closer Than You Think. Waterloo, On. Retrieved from http://perimeterinstitute.ca/videos/wonder-wow-why-quantum-age-closer-you-think

McEvoy, J., & Zarate, O. (2007). *Introducing quantum theory.* London: Icon Books.

Mearian, L. (2012, February 28). *IBM touts quantum computing breakthrough*. Retrieved April 21, 2014, from Computerworld.com: http://www.computerworld.com/s/article/9224670/IBM_touts_quantum_computing_breakthrough

Merali, Z. (2011, May 31). *First sale for quantum computing*. Retrieved April 14, 2014, from Nature.com: http://www.nature.com/news/2011/110531/full/474018a.html

NIST. (2012, May 30). *The Beginning of Quantum Information at NIST*. Retrieved from NIST Physical Measurment laboratory: http://www.nist.gov/pml/div684/qip.cfm

NIST Press Release. (2006, September 11). *Joint Quantum Institute Created by University of Maryland, NIST and NSA*. Retrieved from Nist.gov: http://www.nist.gov/public_affairs/releases/joint_quantum_institute.cfm

Perimeter Institute for Theoretical Physics. (2006, May 8). *12-qubits Reached In Quantum Information Quest*. Retrieved 04 27, 2014, from ScienceBaily.com: http://www.sciencedaily.com/releases/2006/05/060508164700.htm

Scalese, S. (2014, February 10). *Physicist's Proposal in Quantum Computing Receives $2.25 Million in Funding*. Retrieved from Syracuse University News: http://news.syr.edu/physicists-proposal-in-quantum-computing-receives-2-25-million-in-funding-66048/

Shcool of Physical Sciences, USTC. (2014, April 30). *Key Laboratory of Quantum Information*. Retrieved from Shcool of Physical Sciences, USTC: http://en.physics.ustc.edu.cn/research_9/Quantum/201107/t20110728_116550.html

Tan, V. (2007, May 2). *Singapore sets up S$150m research centre for quantum*. Retrieved April 28, 2014, from Channel NewsAsia: 2014http://www.physics.nus.edu.sg/QIT.pdf

The Institute for Quantum Computing (IQC). (2014, April 28). *About Institute for Quantum Computing*. Retrieved from uwaterloo.ca: https://uwaterloo.ca/institute-for-quantum-computing/about

Top 500 Supercomputer Sites. (2013, November 18). *China's Tianhe-2 Supercomputer Maintains Top Spot on 42nd TOP500 List* . Retrieved from Top

500 Supercomputer Sites: http://www.top500.org/blog/lists/2013/11/press-release/

U.S. Army Research Laboratory. (2013, March). *2012 Annual Review.* Retrieved from U.S. Army Research Laboratory: http://www.arl.army.mil/www/pages/172/docs/2012_annual_review.pdf

Weizmann Institute of Science. (2008, June 02). *Scientists find new 'quasiparticles'*. Retrieved April 29, 2014, from Phys.org: http://phys.org/news131631206.html

West, J. (2003, July). The Quantum Computer. *Xootic Magazine*, pp. 5-10.

Williams, A. (2013, July 8). *Science: Quipper brings high-level programming to quantum computing - See more at: http://www.electronicsweekly.com/news/research/science-quipper-brings-high-level-programming-to-quantum-computing-2013-07/#sthash.ru1zm6Rh.dpuf*. Retrieved from Electronics Weekly: http://www.electronicsweekly.com/news/research/science-quipper-brings-high-level-programming-to-quantum-computing-2013-07/

Wittich, P. (2008, January 23). *Archives of Ask A Scientist! How many atoms are in a grain of sand?* Retrieved from Cornel Center for Material Research (CCMR): http://www.ccmr.cornell.edu/education/ask/?quid=1268

Eric Jodoin, ejodoin@hotmail.com