AIR WAR COLLEGE

AIR UNIVERSITY

TAKING A QUANTUM LEAP IN CYBER-DETERRENCE

By

James G. Sturgeon, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Biography

Lt Col Sturgeon is a 1989 graduate of the United States Air Force Academy. Following his commission, he attended UPT. He has over 3000 hours flying the F-16A, F-16C, T-37, T-38, and AT-38B aircraft. He has over 100 combat hours from OPERATION SOUTHERN WATCH and served as the PACAF F-16 Demonstration Pilot. Lt Col Sturgeon completed two staff tours, one in the Korean Air Operations Center and one in Checkmate at Headquarters Air Force. Most recently, he served as the squadron commander of the 21st Fighter Squadron at Luke AFB, AZ. Lt Col Sturgeon holds a Masters degree in Educational Administration from Mississippi State University and a Masters of Military Arts and Science from the Army Command and Staff College, Fort Leavenworth, Kansas.

Abstract

There has been much speculation in Defense and Homeland Security circles about what a so called cyber-9/11 would look like. Decisions made by United States today could prevent or invite such a scenario in the next 25 years. Cyberspace research and development will significantly impact the increasingly interconnected environment that will describe the world in 2035 creating opportunities and danger. Opportunities lead to cyber omniscience[1] while dangers warn of less privacy, compromised sensitive data, and more vulnerable networks. Quantum computing will be the key to this future.

Protecting information and networks in an increasingly connected world has grown exponentially more difficult. Less than a decade ago, defense officials theorized about the cyber crime and data exploitation we see today.[2] As such, information is increasingly protected by encryption methods. Quantum computing enables more secure encryption, permitting the use of larger keys without increasing decipher time. Quantum theory provides new options for secure communications. Quantum computing paradoxically renders data and networks less secure. A quantum computer could break the encryption it enables leading to increased espionage, attacks on financial institutions and critical infrastructure. Anyone with quantum computing muscle gains power and groups (criminal and terrorist) have more to gain. Therefore nation-states must learn how to deter Non-State Actors (NSAs) from illicitly using this technology.

As computing technology evolves and quantum computers become readily available will the United States be able to deter violent NSAs from using quantum computer technology to launch potentially devastating attacks in or from cyber space? Conversely, does quantum information technology provide the United States new cyberspace deterrence options? This research will strive to answer these questions.

[1] Cyber omniscience is the ability to know when an individual has entered or is using cyberspace as well as track that person's movement and actions in physical space and cyberspace. It is dependent upon the inclusion of all networks and equipment into the cloud. (See Flash for his definition).

[2] Irving Lachow, "Cyber Terrorism: Menace or Myth,"In *Cyberpower and National Security*, by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz. (Dulles, Virginia: National Defense University Press & Potomac Books, Inc., 2009), 441.

Introduction

Tampa Bay, Florida, January 21, 2035: The Indianapolis Colts and the New Orleans Saints are ready to kickoff Super Bowl LXVII. The traditional flyby is planned to be a demonstration of the newest aircraft in the inventory. The Air Force, Navy, and Marine Corp will each fly a four-ship of the Joint Unmanned Combat Air Vehicle (UCAV). The new Tampa Bay stadium is sold out to its capacity of 100,000 fans. As the formation approaches from the East, the lead element begins a shallow dive toward the west end zone. Instead of flying over the stadium, the formation flies into the stadium. The lead element impacts the west end in perfect formation. The next element hits the north side of the arena while the last element turns and crashes into the east side. Fire and fuel fill the arena causing it to collapse in less than an hour. In the end, thousands of Americans lose their lives while more than half in attendance are injured. A cyber attack has produced an even darker day of infamy than America has ever experienced.

There has been much speculation in Defense and Homeland Security circles about what a so called cyber-9/11 would look like. Decisions made by United States today could prevent or invite such a scenario in the next 25 years. Cyberspace research and development will significantly impact the increasingly interconnected environment that will describe the world in 2035 creating opportunities and danger. Opportunities lead to cyber omniscience while dangers warn of less privacy, compromised sensitive data, and more vulnerable networks. Quantum computing will be the key to this future.

Physicists, mathematicians, and computer scientists have referred to the quantum computer as the "holy grail" of computing and the logical extension of Moore's law.[3] As transistors continue to shrink they approach the physical limit of performance.[4] To continue to improve speed and power, processors must be built at the subatomic level where quantum mechanics govern the environment. Physicists and mathematicians around the world are harnessing the unique properties of quantum mechanics as they design the first usable quantum computer. If successful, this ‘quantum leap’ represents tremendous promise.

In theory, a quantum computer computes billions of times faster than today’s personal computer and places more computing power in the hands of users than today’s supercomputers.[5] Computers modeling complex biological structures could lead to breakthroughs in vaccines and other critical medicines. Scientific and engineering problems could be modeled and simulated on a desktop computer prior to actual experiments, saving research money. It also holds promise for protecting networks and sensitive data.

Protecting information and networks in an increasingly connected world has grown exponentially more difficult. Less than a decade ago, defense officials theorized about the cyber crime and data exploitation we see today.[6] As such, information is increasingly protected by encryption methods. Quantum computing enables more secure encryption, permitting the use of larger keys without increasing decipher time. Quantum theory provides new options for secure communications. But in that lies a double edged sword.

Quantum computing paradoxically renders data and networks less secure. A quantum computer could break the encryption it enables leading to increased espionage, attacks on financial institutions and critical infrastructure. Anyone with quantum computing muscle gains power and groups (criminal and terrorist) have more to gain. Therefore nation-states must learn how to deter Non-State Actors (NSAs) from illicitly using this technology.

Deterrence simply is preventing “someone from doing something that he or she would otherwise like to do.”[7] Classical deterrence theory relies upon the assumption that all players are rational actors able to calculate the cost and benefit of their proposed actions.[8] It also assumes that deterrence is a nation-state activity involving an intense rivalry.[9] This theory of deterrence was shaped by the nuclear rivalry between the United States and the Soviet Union and, based on the assumptions, does not ably apply to NSAs. Therefore, states need new deterrence frameworks to help them understand an increasingly complex security environment and develop policy options for deterring NSAs in both the physical and cyber realms.

As computing technology evolves and quantum computers become readily available will the United States be able to deter violent NSAs from using quantum computer technology to launch potentially devastating attacks in or from cyber space? Conversely, does quantum information technology provide the United States new cyberspace deterrence options? This research will strive to answer these questions.

This paper is divided into four distinct sections. The first section explains the science behind the quantum computer, its capabilities, and establishes its reality in 2035. The next section describes technological and strategic trends in today's global security environment and extrapolates those in order to address the global setting in 2035. The third section examines current thoughts on deterrence and establishes a framework for deterring NSAs. Finally, this paper will explore possible deterrence options and provide specific technological and policy recommendations for deterring the hostile use of quantum computing by violent NSAs in cyberspace against the United States.

[3] Karlin Lillington, "Quantum Leap," *The Irish Times*, February 2, 2009, 41.

[4] George Johnson, *Shortcut Through Time: The Path to the Quantum Computer* (New York: Alfred A. Knopf, 2003), 52. Physical limits refer to the heat generated by microprocessors due to the irreversible computing taking place and the size of the microprocessors themselves. Reversible computing is able to use the remaining bits at the end of a logic gate rather than discarding those bits' energy as heat.

[5] SC Magazine, "Quantum Computing," *Secure Computing (SC) Magazine*. 1 July 2008, 8.

[6] Lachow, "Cyber Terrorism: Menace or Myth,"441.

[7] Janice Gross Stein, “Rational Deterrence Against ‘Irrational’ Adversaries? No Common Knowledge.” In *Complex Deterrence: Strategy in the Global Age*, by T V Paul, Patrick M. Morgan and James J. Wirtz, 58-82. (Chicago: The University of Chicago Press, 2009), 61.

[8] T V. Paul, “Complex Deterrence: An Introduction.” In *Complex Deterrence: Strategy in the Global Age*, by T V Paul, Patrick M Morgan and James J Wirtz, (Chicago: The University of Chicago Press, 2009), 4.

[9] Ibid., 5.

Quantum Computing

I do not think there is any thrill that can go through the human heart like that felt by the inventor as he sees some creation of the brain unfolding to success.

-Nikola Tesla, 1896, Inventor of Alternating Current

Quantum computing begins with classical computing logic and becomes magic when explored through the lens of quantum theory. Starting with the concept of the simplest computer, the Turing machine, and adding the foundation of quantum theory results in an extremely powerful computing device. The reality of this mystical machine is that it opens doors for applications rooted in mathematics. Factoring large numbers and creating complex search algorithms take advantage of the massive amount of parallel computation afforded by the quantum computer. As long as mathematicians develop algorithms to solve math intensive problems, the quantum computer will have an unfair advantage over the silicon computers and change how Moore's Law is conceived today.

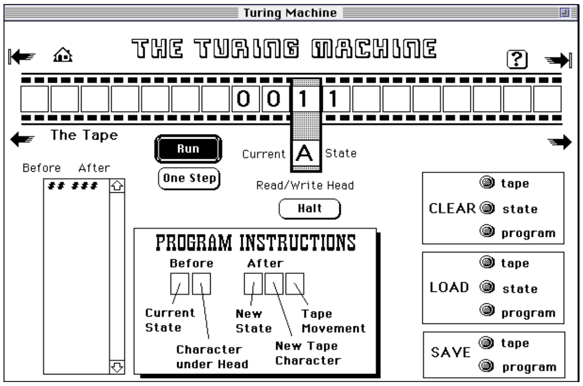

Figure 1: Turing Machine (courtesy of Virginia Institute of Technology)

The most primitive computers were nothing more than Boolean logic machines.[10] British mathematician Alan Turing used Boolean logic as instructions for a problem solving tool that became the theoretical foundation for today's computers. The Turing machine (Figure 1) was "an imaginary device with just two parts: a clocklike dial with a pointer and a scanning head that can move alongside a lengthy paper tape examining, one by one, the marks it finds."[11] The pointer started in a specific position and then moved up and down the paper in accordance with a simple set of logic instructions (today's computer program), and produced the desired result. With the right set of instructions any number of problems could be solved.[12] The pervasive thought in computer science is that nothing is more powerful than a Turing machine.[13] That is until the quantum computer.

Quantum theory began in 1900 when German Physicist Max Planck discovered that light seemed to possess two sets of properties, that of a wave and a particle. He said that light is emitted in tiny packets, and Einstein built upon this concept to explain the photoelectric effect and said, “Think of light as infinitesimal identical ‘packets’ of energy, called photons.” [14] These photons exhibit themselves every day. Looking through a window at the landscape outside, it is possible to see a faint image of oneself in front of the window. The image is formed by photons bouncing back off the window. The majority of the particles travel through the window, making it possible to see outside. So what caused the other photons to bounce back?

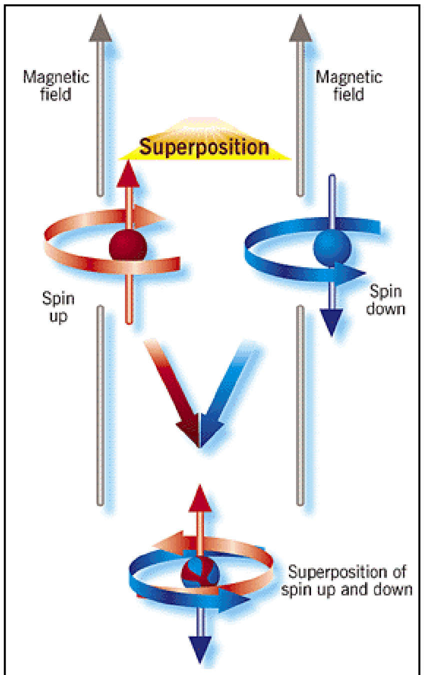

Figure 2: Quantum Superposition

According to Einstein, each individual packet of light is identical. Therefore, the when particles reach the window they randomly bounce back, pass through, or bounce off.[15] All of the possible outcomes occur simultaneously. This state is called quantum superposition (see Figure 2). [16] The *magic* of quantum computing is in quantum superposition. [17]

Particle states in quantum superposition are described by a probability wave; that is the sum of probabilities that the particle is in any one state.[18] Particles can be measured by physical properties like velocity or spin. When a particle is observed or disturbed by the outside world, the probability wave collapses randomly to an actuality. From the example above, when the light particle hits the glass, it randomly through the glass or in a direction that produces an image in the window. Scientists, including Einstein, doubted the indeterminacy of quantum mechanics. He set out to disprove it.

In an attempt to challenge quantum mechanics, Einstein and two colleagues, Boris Podolsky and Nathan Rosen, conducted a thought experiment.[19] They imagined a particle that decayed to produce two photons in opposite directions. One quality of photons, called spin, is seen as clockwise or counter-clockwise. The decaying particle had zero spin, so the photons had to be spinning in the opposite direction, for a net effect of zero.[20]

Quantum mechanics states that these two photons, until measured, exist in a superposition of spin--that is the photons are spinning clockwise and counter clockwise simultaneously. When a measurement of one of the photons is taken to determine spin, the other photon must then snap into an equal and opposite spin for the net spin to be zero. Therefore, these photons must be synchronized because no time has passed that would allow for them to "communicate". Scientists say that they are "entangled" in such a way that they seem to defy the concept that something cannot be in two places at one time.[21] Experiments have since proven this effect.

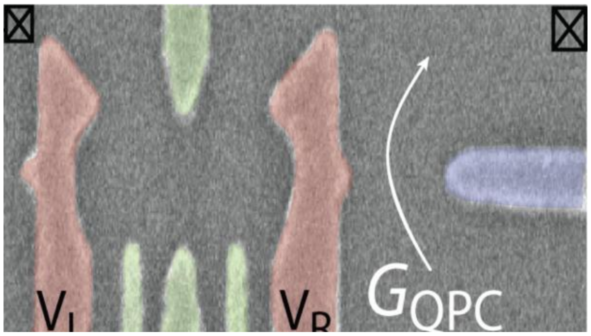

Figure 3: Quantum bits

Manipulation of voltages on the metallic gates (in red) allows formation of two single-electron spin qubits, which can be made to interact by changing the potential on the plunger gates (in green). Qubit states in the nearby quantum dot can be detected by quantum point contact (blue).

The significance of this is twofold. One – it means particles can spin clockwise or counter-clockwise at the same time. This concept led to the suggestion by American Physicist Richard Feynman in 1982 that a computer working quantum mechanically would have switches that could be expressed as a 1 or a 0 or both at the same time. In the classical computer, switches expressed as either 1 or 0 are called bits. In the quantum computer, these switches are called quantum bits, or qubits (Figure 3).[22] Two – entangled particles that seemingly communicate simultaneously could form the foundation of a new way of communicating and in fact some research has been done in this field. These information bits (a combination of qubits and bits), are referred to as ebits[23], but qubits represent the building blocks of the quantum computer.

The power of qubits is exponential. The number of possible combinations of three bits is 2^x where x is the number of bits. Because each qubit can be 1, 0, or both 1 and 0 (represented by ɸ), all possible combinations are accounted for in three qubits. Suppose the right hand qubit is set to ɸ, then 000, and 001 can be represented simultaneously. The same is true for the remaining qubits until all eight patterns are accounted for at once (Figure 4). So the concept of superposition allows us to use x qubits to store 2^x bit strings allowing exponentially large amounts data to be stored and processed concurrently.[24]

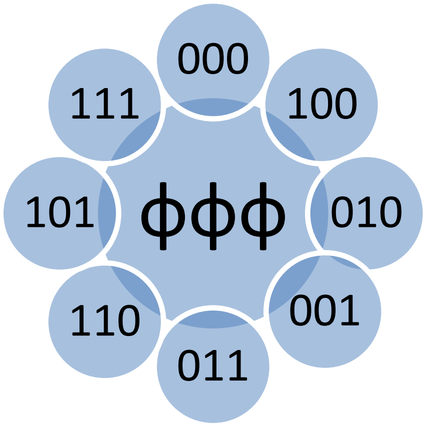

Figure 4: Exponential power of qubits

A Turing machine whose tape is marked with ɸ instead of 1s and 0s operates in parallel producing an advantage over the classical computer in factoring large numbers. A classical computer operates in sequence so that the larger the number, the longer it takes to find the prime factors (Figure 5). A calculation time that scales by 3^x nanoseconds means that a three digit number would take nine nanoseconds. Using that same scale, a 20 digit number would take 3.5 seconds, but a 30 digit number would take nearly 60 hours, and a 50 digit number would take 23 million years to factor.[25] This 'exponential explosion' occurs in classical computing because the bit string representing a large number is extremely long and the machine operates in sequence. A quantum computer finds solutions in parallel and therefore solves these factoring problems in a matter of seconds. The possibilities of storing and processing huge amounts of bit strings simultaneously urged mathematicians write algorithms taking advantage this capability.

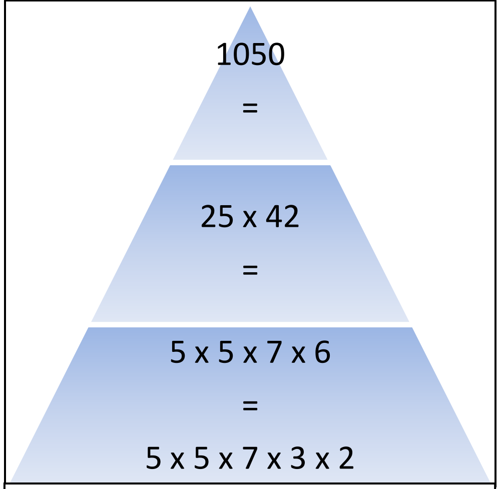

Figure 5: Prime Factoring

In 1994, Bell Laboratory scientist Pete Shor[26] developed an algorithm that took advantage of performing a large number of calculations in quantum superposition. He created a quantum waveform representing every possible factor and then collapsed it to produce the answer.[27] This meant that a quantum computer can practically factor every number imaginable. Recently, MIT researchers presented a new algorithm that could bring the same kind of efficiency to linear equations. Solving these equations is critical to image processing, video and signal processing, and robotic control among other things.[28] University of London researchers developed a new quantum algorithm for solving differential equations.[29] A vast number of engineering and physics problems could be solved with this kind of power. With algorithms developed to use quantum computing, the computer must be built.

To build a quantum computer, logic gates must be created and currently there are many different methods for manipulating particles to build logic gates. The trick is to perform the calculations before the particle superpositions collapse. Maintaining particle superpositions represents the most recent obstacle for quantum computing technology to overcome[30] and great strides are being made each day.

In June of 2009, a team of Yale University researchers produced the first solid state quantum processor.[31] The two qubit chip constructed from a billion aluminum atoms acting like a single particle occupying two different energy states was able to run simple quantum algorithms that previously had only been demonstrated in the lab using single nuclei, atoms and photons.[32] The scientists preserved the qubits superpositions for a microsecond, long enough to do required algorithms.[33] This breakthrough moves the technology closer to realizing the first practical quantum computer, advancing computing well beyond Moore's Law.

Moore's Law has described the pace of computing advancement for the last forty years. Gordon Moore, co-founder of Intel Corporation, observed in 1965 that the number of microcircuits on a silicon chip will double approximately every two years[34]. This doubling effect has increased computing speed and power due to the reduced physical size. Today, microcircuit spacing is measured in nanometers and is reaching a perceived limit.

The most limiting factor is the heat generated by the microchips themselves. When computing, microcircuits discard intermediate results which then must be erased. Physicist Rolf Landauer showed that when a bit is erased, heat is dissipated.[35] This heat must be carried away so the microchip does not malfunction. Therefore cooling becomes a problem.[36] In the mean time, engineers are finding other ways to increase computing power.

The latest computer chips, referred to as *dual* or *quad core*, represents doubling or quadrupling the size of a silicon chip to accommodate two or four parallel processors. The result is a bigger chip (requiring more cooling) capable of parallel processing, a method used by supercomputers on a much larger scale. Based on a recent breakthrough in material technology, scientists surmise five more iterations of Moore's Law remain before reaching the limits of the silicon microchip's power and speed. Parallel processing could extend this limit by another ten years. This would extend silicon based processor technology twenty years total. This coincides with futurist Ray Kurzwiel's prediction in 2005 that there is perhaps fifteen to twenty more years of doubling before reaching physical limits.[37] By then, it is likely that Moore's Law will evolve.

Current technology allows logic gates 50 nanometers wide.[38] To extrapolate Moore's law out for the next twenty years, the size of transistors would be at the atomic level.[39] Although quantum computing is quite different than today's silicon-based chips, it is one way Moore's law could outlive the projected twenty year life span.[40] By then it is possible that Moore's law will be discussed in terms of computing power rather than numbers of circuits or speed.

Floating-point Operations per Second (FLOPS) is a measure of computing performance. As of November 2009, the fastest computer is the Cray XT5, known as the Jaguar, performs at 1.75 PetaFLOPS, or 1.75×10^{15} FLOPS. The fastest PC processor as of 2008 was Intel's Core i7 965XE performing just over 70 GigaFLOPS ($70 \times 10^{9)}$. If the quantum computer operates a billion times faster, then it will operate in the range of one ExaFLOPS (1.0×10^{18}) to one YottaFLOPS to (1.0×10^{24}). Adding qubits to a quantum computer increases its computing power and writing new algorithms to solve complex mathematical equations makes it useful for more than just factoring. As the business case improves for quantum computers, eventually QCs will replace the PC.

Harnessing the power of quantum physics and applying it to the most basic concept of computing captures a shift in today's computing paradigm. Having already produced a two qubit computer, the foundation has been laid for more powerful quantum computers. The development of algorithms that take advantage of the parallel processing of a quantum computer makes this technology all the more usable. The quantum computer will make 2035 an exciting and dangerous time.

[10] Stanley Schmidt, *The Coming Convergence: Surprising Ways Diverse Technologies Interact to Shape Our World and Change the Future.* (New York, New York: Prometheus Books, 2008) George Boole developed a way of symbolically representing logical premises, relationships (like IF, AND, and OR), and conclusions in a way resembling the symbology of algebra. These symbols could be manipulated according to specified rules and give logically meaningful results. Boolean algebra would later become the basis of computer switching procedures.

[11] Johnson, *Shortcut Through Time*, 53.

[12] Ibid., 54.

[13] Ibid., 55.

[14] Gerard J Milburn, *Feynman Processor: Quantum Entanglement and the Computing Revolution.* (Reading: Perseus Books, 1998), 3.

[15] Johnson, *Shortcut Through Time*, 36.

[16] University of Oregon, "Quantum Superposition Spin."http://abyss.uoregon.edu/~js/images/spin.gif.

[17] Johnson, *Shortcut Through Time*, 38.

[18] Milburn, *Feynman Processor*, 200.

[19] Ibid., 47.

[20] Johnson, *Shortcut Through Time*, 43.

[21] Ibid, 44.

[22] Craig Collins, "Quantum Information Science: DARPA'S New Frontier." In *50 Years of Bridging the Gap*, by DARPA, (Washinington DC: Defense University Press, 2009),102.

[23] Ibid., 102.

[24] Lillington, "Quantum Leap," 41.

[25] Johnson, *Shortcut Through Time*, 44.

[26] Collins, "Quantum Information Science," 105.

[27] Johnson, *Shortcut Through Time*, 75.

[28] Larry Hardesty, "Quantum Computing May Actually Be Useful." *web.mit.edu.* http://web.mit.edu/newsoffice/2009/quantum-algorithm.html

[29] Ibid,.

[30] Johnson, *Shortcut Through Time*, 75. Decoherence occurs when the superposition breaks down into an observable physical characteristic such as spin or position.

[31] Yale University, "First Electronic Quantum Processor Created." *www.sciencedaily.com.* June 29, 2009. http://www.sciencedaily.com/releases/2009/06/090628171949.htm

[32] Ibid.

[33] Ibid.

[34] Lloyd's List, "Quantum Mechanics Makes More of Moore; Quantum Computing May Facilitate New Types of Applications and Enable Us to Escape the Limitations of Moore's Law." *Lloyd's List*, January 11, 2008: 7. It was first stated that the number of individual microprocessors will double every eighteen months and then adjusted to two years.

[35] Johnson, *Shortcut Through Time, 77.*

[36] Ibid., 77. For this reason, researchers are experimenting with energy efficient reversible computing where every step of the computation is preserved. The only problem with reversible computing right now is the fact that the circuitry is extremely complex, slowing the speed of the micro circuit. It is possible that reversible and traditional computer chips will exist in a single computer to help reduce overall heat dissipated.

[37] Ray Kurzweil, *Singularity is Near: When Humans Transcend Biology.* (New York, New York: Penguin Books, 2005), 112.

[38] Ibid.

[39] Collins, "Quantum Information Science," 103.

[40] Lloyd's List, "Quantum Mechanics Makes More of Moore," 7. Kurtzweil, *Singularity is Near*, Chapter 3. Kurtzweil covers biological, DNA, light, spin, 3D, self assembly and molecular, as well as quantum computing, but believes that nanotubes are the best bet for continuing Moore's law in terms of speed and power of computing.

Trends Toward Transparency and the Dangerous World of 2035

We are certain that we shall—with the grace of Allah—prevail over the Americans. . . If the present injustice continues. . . , it will inevitably move the battle to American soil

-Osama bin Laden, 1993 interview with PBS

The further backward you look, the further forward you can see.

-Winston Churchill

While computing speed and power has evolved at a relatively predictable pace, the interconnectivity of the world has grown exponentially. Social and economic interactions made possible by the internet are beginning to dominate western society. Facebook, Twitter, Second Life, and My Space have changed the way new generations interact. Ebay, Amazon.com, and other on-line markets challenged the traditional market place such that most businesses now have online shops to compliment traditional storefronts. Increasingly, business is conducted in cyberspace while governments and industry move toward a paperless, wireless, transparent society, capturing the power of networking by interacting in an information "cloud".

The benefits of increasing connectivity in cyberspace have been informally captured in Metcalfe's Law. Robert Metcalfe, one of the inventors of Ethernet technology, stated that the value of telecommunications is proportional to the square of the number of users.[41] David P. Reed, a computer scientist from Massachusetts Institute of Technology and one of the developers of internet protocol, took this even further to say that the utility of large networks, especially social networks, can scale exponentially. Metcalfe's and Reed's Laws (Figure 6) are difficult to quantify, but they do explain that networks grow at a rate greater than standard linear growth.[42]

One reason for this growth is the proliferation of broadband. The internet backbone is built upon large numbers of fiber optic cables installed in the 1990's during the dot-com boom. When the boom ended, the price of fiber fell making it extremely cheap to buy. [43] Currently, the technology for propagating signals along fiber cables is rapidly improving and carrying more information to new users each day. The proliferation of PCs and this increased cyber connectivity throughout the world and has given rise to social networking and cloud computing.

Social networking via the internet began in the early 1980s. What began as a gaming service called Quantum Computer Services, America On Line (AOL) provided individuals electronic mail as early as 1989. By 1986 subscribers could chat live with friends on-line. Business models changed and Yahoo! began offering free email services in 1997[44] gaining market share and users. To expand services, and markets, Web service companies began constructing "server farms." By 2007, Google had as many as a half a million computer servers[45] to accommodate the new concept of cloud computing and the data on these servers grows several terabytes each day.[46]

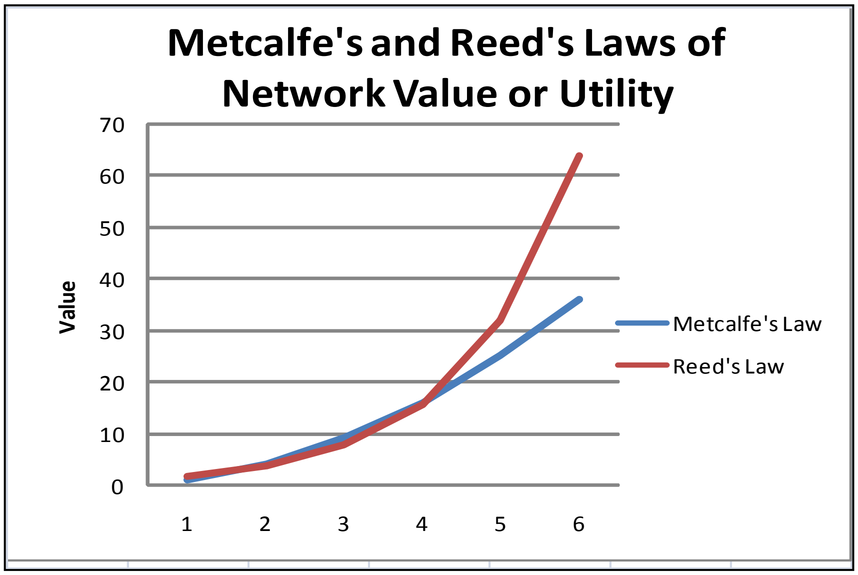

Figure 6: Metcalfe's and Reed's Laws

Cloud computing is a system where a user can have all their computing needs met without having to buy expensive software or hardware packages because all of the required computing power is in the cloud.[47] The cloud is enabled by networking computers to provide application software and data storage. Users log-on to the cloud from computers or network devices and access word processing, presentation, database, financial software, email, pictures, and personal information stored within the cloud. A user can also participate in social networks through Facebook or Myspace, or live life as an avatar in a virtual world such as Second Life. Access has become more mobile as wireless communication becomes more available.

Wireless technology has also increased the connectivity of the world. Cities, hotels, doughnut shops, coffee shops, and bookstores often provide free Wifi.[48] Advancements in data transmission technology continue to increase the speed and distance of wireless connectivity. According to Metcalfe, cities are providing public Wifi so more people can connect making the network increasingly valuable.[49] Cell phones with computer processors as powerful as five year old desktops coupled with access to the cloud nearly everywhere in the globalized world produces what Thomas Friedman calls an increasingly small, flat, and connected planet[50] moving toward more transparency.

Increasing connectivity, whether by fiber optic cable or Wifi, leads to the merging of all networks, computers, and computing devices into a single cloud. By 2035 data will be ubiquitous via the cloud and sensitive information will be protected behind encryption. Regardless of position on the planet, individuals will have access to the cloud. However, the cost of access to this plethora of information is the loss of anonymity. The world is becoming more transparent.

To date, individuals who interact with the World Wide Web (WWW) are identified by an Internet Protocol (IP) address which can be traced to a specific computer. In 2035 a person who accesses the cloud via a small computer or hand held device would be readily identified by their IP address and their position could be easily determined by triangulating signal reception. Once the position is determined, they could be visually identified by local surveillance cameras connected to the cloud or even by the camera on their own cloud computing device. Many in the

United States would object to this type of intrusion under the premise that it is a violation of an individual’s privacy rights.

In spite of objections, younger generations are growing accustomed to this kind of transparent society, largely due to the advent of social networking sites such as My Space and Facebook. These social networks represent a voluntary sacrifice of privacy while the above “cyber omniscience” scenario might only be accepted if focused on those engaging in illicit activities via the cloud. Correlating events in cyberspace to individuals or groups requires extremely powerful computing and search algorithms, such as that provided by quantum computing. Likewise, protection of networks and information in the cloud requires powerful encryption.

Public Key Encryption (PKE) began in the 1970s and is still widely used in Secure Sockets Layer (SSL) and Secure Shell.[51] Both SSL and Secure Shell are network protocols that allow secure messages to pass over an insecure network. The Rivest, Shamir, & Adleman algorithm (RSA) built upon PKE and now enables the use of digital certificates to authenticate the sender of encrypted text.[52] RSA cryptography is based on the assumption that factoring large numbers is computationally infeasible using current microchips embedded with transistors and their associated computational algorithms. However, as noted in the above section, a quantum computer easily factors large numbers and therefore quickly breaks this type of encryption.[53] Knowing RSA is vulnerable will require effective counters to quantum cryptography.

Scientists and engineers are examining quantum ‘resistant’ cryptography such as lattice-based ciphers which do not rely on prime number factoring as their strength.[54] However, changing encryption methods and standards across networks takes a great amount of work and investment in cyber infrastructure. This new investment is unlikely in the near term because the threat is not recognized by most. The power of quantum computing will enable cyber omniscience with power to break encryption, quickly search, and correlate actions in cyberspace making attribution possible. Therefore 2035 will be a paradoxical world of cyber omniscience and vulnerability and it will intersect with a volatile security environment.

The security environment of the 21st century has been shaped by three very important events – the end of the Cold War, Globalization, and the September 11th, 2001 terrorist attacks on the United States. The end of the Cold War heralded the demise of the Soviet Union and the rise of the United States as the sole hegemonic power. This added impetus to the already powerful force of globalization and opened new markets.[55] Ironically, it also spurred groups like Aum Shinrikyo in Japan, and Shining Path in Peru, to attack with the intent to halt globalization, protect cultures, and to overthrow the existing power structure.   The United States' failure to define and deal with this new security environment after the Cold War created a vulnerability exploited by Osama bin Laden and al Qaeda on 9/11.

Globalization is the integration of nations throughout the world into an increasingly interrelated economic relationship. Thomas L. Friedman argues that we are in the third great era of globalization and it is shrinking and flattening the world.[56] Proliferation of fiber optic cable, personal computers (PCs), cell phones, and the internet riding on all this technology resulted in Globalization 3.0, as Friedman calls the period from 2000 to today, and brought the world closer together. For some countries such as India, which is peacefully integrating into what Barnett calls the Functioning Core[57], this is a good thing. But civilizations that are home to extremely conservative religious groups, Globalization 3.0 is viewed as an evil.

In 1965 Sayyid Qutb, the leading intellectual of the Egyptian Brotherhood whose writings inspired Osama bin Laden, stated:

> Humanity today is living in a large brothel! One has only to glance at its press, films, fashion shows, beauty contests, ballrooms, wine bars and broadcasting stations! Or observe its mad lust for naked flesh, provocative pictures, and sick, suggestive statements in literature, the art, and mass media! And add to all this the system of usury which fuels man's voracity for money and engenders vile methods for its accumulation and investment, in addition to fraud, trickery, and blackmail dressed up in the garb of law.[58]

His obvious hatred for the fruits of globalization in 1965 led him to radicalize his faith and eventually his followers would use his words to justify a war against whomever they view as the source of this debauchery; for Al Qaeda, the United States of America is the source.

In the aftermath of Operation Desert Storm, the United States Military found itself increasingly deployed in the Middle East. This perceived impingement on their culture provided radicalized Arab Muslims the motivation to attack. Sulaiman Abu Ghaith, a former Kuwaiti religions teacher and Al Qaeda operative, appeared on Al-Jazeera to explain why they struck America on 9/11, "America, with the collaboration of the Jews, is the leader of corruption and the breakdown [of values], whether moral, ideological, political, or economic corruption. It disseminates abomination and licentiousness among the people via the cheap media and the vile curricula."[59] The 9/11 attacks demonstrated to the United States the unintended consequences of globalization. Ironically, the proliferation of advanced technology through globalization gave them the capability to act.

According to Gabriel Weimann, a professor of communications at Haifa University and former senior fellow at the United States Institute of Peace, the internet played a key role in Al Qaeda's ability to collect information, communicate between cells, and coordinate attacks including 9/11.[60] As demonstrated by the arrest of five American students in Pakistan seeking terrorist training, [61] radical Islamic extremist groups, such as the Taliban and Al Qaeda, are using the internet to recruit and communicate. Al Qaeda is constantly recruiting computer experts and scientists to help them forge electronic documents, encode and decode messages, defeat encryption techniques, and encrypt their own networks.[62] As they seek to protect their own networks it is not impossible to imagine the exploitation of networks to their advantage, even military networks.

Today, networks permeate the battlefield. Link 16 dominates air battle space management systems. Encrypted data is passed from platform to platform providing critical situational awareness. Recently, insurgents in Iraq intercepted and hacked the network video link from Predator drones providing them critical situational awareness.[63] If a group could intercept and decrypt the flight control signal, they could hijack a UAV and use it against American troops. As networks become increasingly connected, they become open to new avenues of attack. Critical infrastructure is also rendered more vulnerable.

Irving Lachow, a Senior Research Professor at the Information Resources Management College at the National Defense University, argues that in spite of the advertised vulnerability of the Supervisory Control and Data Acquisition (SCADA)[64] systems in the United States critical infrastructure, there has not been a large-scale systematic attack against it.[65] Such an attack would require a highly coordinated, sophisticated, and technologically well equipped team to pull off. Yet the United States' President only four months after taking office recognized, "We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness."[66] In order to perpetrate an attack like this, groups require sufficient resources.

Violent NSAs have learned how to use the internet to finance their operations by stealing credit card information, identities, and bank accounts. In December 2009, a Russian cyber gang hacked into Citibank and made off with tens of millions of dollars.[67] Violent NSAs have been known to copy what they see criminal groups do in cyberspace and the leader of the 2002 Bali disco bombing wrote a primer on the use of the internet for funding operations.[68] These groups will continue to use and grow their capability in cyberspace because it gives them access to resources they need and in the future that key resource will be quantum computers.

The quantum computer gives groups the resource they need to execute their operations. It enables them to fly through firewalls protecting sensitive data that can be used to generate or acquire more resources. It gives them the ability to create more robust encryption for their own systems and networks. It also gives them the ability to strike at the West in new and possibly devastating ways as described above. Today, NSAs use cyberspace because it gives them anonymity,[69] but in the future, this will not necessarily be the case.

If 2035 is characterized by cyber omniscience, state agencies will know who is conducting suspicious actions in the cloud at any time. However, this assumes that the proper infrastructure is in place everywhere in the world. In 2035, there will still be places that will be difficult to physically find due to limited access for political or geographical reasons. The United States has looked for Osama bin Laden eight and a half years now and has not found the cave in which he is hiding. The good news is that these areas of limited access will continue to shrink as globalization grows infrastructure and technology improves. But the result is that NSAs willing to live in the ungoverned regions of the world will enjoy some freedom of action.

The cloud presents opportunity and danger for NSAs. Opportunities include communication with operating cells around the world, recruiting, training, and resources (money, information, and more computers-even quantum computers). The danger is being discovered. Therefore it is critically important for them to operate in ungoverned spaces and be able to recruit new operatives that appear to be law abiding citizens until it is time to attack.

Umar Farouk Abdulmutallab certainly appeared to be a normal student at the University of London and would not have been on a watch list had it not been for his father's actions to tip off Nigerian and United States officials.[70] Groups may seek and find scientists and engineers sympathetic to their cause and use them to develop the necessary technology to avoid detection in the cloud.[71] This would provide them more freedom of action to plan, finance, and execute attacks in the physical and cyberspace.

Al Qaeda has demonstrated the capability and unwavering intent to strike at the American homeland. Unless that group or successor groups are completely destroyed, it is likely that this threat will exist even in 2035. Quantum computing potentially gives them great freedom to operate within the cloud. It also provides them the capability to intercept and decrypt wireless combat networks. But it also makes them vulnerable to detection and capture. They will actively seek out ways to remain hidden while interacting with the cloud so they can continue to finance, communicate and execute their operations. While there are a plethora of scenarios for another 9/11, the scope of this paper does not allow for an exhaustive list. Instead, the dangerous scenarios discussed represent what is not only possible, but also plausible. Al Qaeda and other similar groups have proven their resourcefulness not only within the United States but against its interests abroad, and against its allies and friends. Exponential technological change in cyberspace will, by 2035, present enormous challenges.

41. Edward Skoudis, "Evolutionary Trends in Cyberspace" In *Cyberpower and National Security*, by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Dulles: Potomac Books, Inc., 2009), 148.
42. Ibid., 148.
43. Thomas L Friedman, *World is Flat: A Brief history of the Twenty-First Century*. (New York: Farrar, Straus, Giroux, 2005), 115.
44. Yahoo! "Yahoo! Expands Community Services with Free E-mail." *Yahoo docs.* October 8, 1997. http://docs.yahoo.com/docs/pr/release124.html
45. George Gilder, "Information Factories," *Wired.com.* October 14, 2006. http://www.wired.com/wired/archive/14.10/cloudware.html 1.
46. Ibid., 1.

47. Michaael Miller, *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online.* (Indianapolis: Que Publishing, 2009), 145.
48. Wikipedia, "Wi-Fi. " http://en.wikipedia.org/wiki/Wi-Fi. "A Wi-Fi enabled device such as a personal computer, video game console, mobile phone, MP3 player or personal digital assistant can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more interconnected access points — called a hotspot — can comprise an area as small as a few rooms or as large as many square miles covered by a group of access points with overlapping coverage. Wi-Fi technology has been used in wireless mesh networks, for example, in London.
In addition to private use in homes and offices, Wi-Fi can provide public access at Wi-Fi hotspots provided either free of charge or to subscribers to various commercial services. Organizations and businesses such as airports, hotels and restaurants often provide free hotspots to attract or assist clients. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. As of 2008 there are more than 300 metropolitan-wide Wi-Fi (Muni-Fi) projects in progress. There were 879 Wi-Fi based Wireless Internet service providers in the Czech Republic as of May 2008."
49. Skoudis, "Evolutionary Trends in Cyberspace", 150.
50. Friedman, *World is Flat*, 130.
51. Mark Mayne, "Encryption – Past, Present and Future", *SC Magazine*, September 9, 2009, 32. Each Secure Socket Layer (SSL) Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a Secure Sockets Layer handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key and secure transmission can begin. VeriSign, "Secure Sockets Layer: How It Works." Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. Wikipedia, "Secure Shell."
52. Mayne, "Encryption – Past, Present and Future", 32.
53. SC Magazine, "Quantum Computing," 8.
54. Mayne, "Encryption – Past, Present and Future," 32.
55. Barnett, *Pentagon's New Map*, 20.
56. Friedman, *World is* Flat, 128. Friedman explains that the first era was the period "from 1492 – when Christopher Columbus set sail, opening trade between the Old World and the New World – until around 1800." This shrank the world from large to medium size. The second period of globalization was "from 1800 to 2000, interrupted by the Great Depression, World Wars I and II." This reduced the world from medium size to small size. He refers to these eras as Globalization 1.0 and 2.0 respectively.
57. Thomas P.M. Barnett, *Pentagon's New Map: War and Peace in the Twenty-First Century.* (New York: G.P. Putman's Sons, 2004), 25. The Functional Core is the civilizations already firmly established in Globalization 3.0 and taking advantage of it economically and for security. Thomas Barnett, a senior strategic researcher and professor at the U.S. Naval War College, argues that after the Berlin Wall fell in 1989, the U.S. had a sense that a new world order was in the making, but never described exactly what that meant. The old security rule sets did not apply and the United States did not define new ones. As a result, there was no foundation or principle to guide choices and the United States found itself engaged around the world in crisis action mode. Interestingly enough the United States engaged in countries and regions Barnett refers to as the Non-Integrating gap, those civilizations that globalization either clashed with or left behind, such as some North African and Middle Eastern Countries.
58. Paul L. Williams, *Al Qaeda Connection: International Terrorism, Organized Crime and the Coming Apocalypse.* (Amherst: Prometheus Books, 2005), 52.
59. Ibid., 58.
60. Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenge.* (Washington D.C.: United States Institute of Peace, 2006), *169.*
61. Abbas Majeed Khan Marwat, *Interrogation Report*, Police Report, (Sargodha: Sargodha Police, 2009), 1. "Recently, five American students were apprehended in Pakistan seeking training as terrorists after having watched YouTube videos of soldiers being killed in Afghanistan and making connections with terrorists on Facebook and communicating through Yahoo! mail.
62. Weimann, *Terror on the Internet*, 170.
63. Siobhan Gorman, Yochi J. Dreazen and August Cole. "Insurgents Hack U.S. Drones." *Wall Street Journal.* December 17, 2009. http://online.wsj.com
64. SCADA is the hardware and software used to control some of the nation's vital infrastructure. The most common system that uses SCADA is the power grid. New generation power generators are increasingly controlled

by computer software. The vulnerability lies in controlling the load on the generator which, if not controlled, could cause it to fail.

65. Lachow, "Cyber Terrorism: Menace or Myth?" 440.

66. CBS News, "Cyber War: Sabotaging the System,"*cbsnews.com.* November 8, 2009. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml 1.

64. Siobhan Gorman and Evan Perez, "FBI Probes Hack at Citibank: Russian Cyber Gang Suspected of Stealing Tens of Millions; Bank Denies Breach." *Wall Street Journal*, December 22, 2009. http://online.wsj.com

68. Louis I. Shelley, et al., *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism.* Government, (Washington D.C.: U.S. Department of Justice, 2004), 8-49.

69. Ibid., 49.

70. Nick Bunckley and Liz Robbins, "Nigerian Arraigned in Bomb Attempt," *The New York Times*, January 9, 2010, A9.

71. According to Paul L. Williams' book, *The Al Qaeda Connection*, Osama bin Laden has acquired tactical nukes from Chechnya and the scientists required to maintain them. I think it is plausible that they would pursue or hire experts in the field for cyberspace if it meant they could possibly strike the U.S.

A Quantum Leap in Cyber Deterrence

For much of the last century, America's defense relied on the Cold War doctrines of deterrence and containment. In some cases, those strategies still apply. But new threats also require new thinking. Deterrence, the promise of massive retaliation against nations, means nothing against shadowy terrorist networks with no nation or citizens to defend.

President George W. Bush, Graduation Address at West Point, 1 June 2002

Deterrence simply is preventing "someone from doing something that he or she would otherwise like to do."[72] Prevention is achieved through a credible threat of violence against the one being deterred or by denial of objectives. Deterrence theory came to the fore during the nuclear age seeking to prevent one nation from launching nuclear weapons against the other. The theory hung on key assumptions that do not completely encompass current security challenges. Today, deterrence is made more complex with the rise of NSAs that can threaten large powerful nations while benefiting from either action or inaction by the state. This environment requires a new paradigm that addresses how to approach deterrence across the spectrum of actors, actions and domains.

Classic deterrence theory, whether conventional or nuclear, relies on three assumptions. First, the decision makers are rational and possess the capability to develop a decision calculus that weighs the cost and benefit of an action.[73] According to John Mearsheimer, that decision calculus is "a function of the costs and risks associated with military action."[74] He goes on to say, "Specifically, deterrence . . . is most likely to obtain when an attacker believes that his probability of success is low and that the attendant costs will be high."[75] The final two assumptions are that the actors are nation states and there is an intense rivalry between parties. This model worked well in the Cold War bipolar world where the threat was major theater war between NATO and the Soviet bloc or a nuclear holocaust. However, as noted by President

Bush in his graduation address at West Point in 2002, in many cases this no longer applies and deterrence "requires new thinking."[76]

The first issue to think through is the concept of rationality. Rationality is still a pivotal assumption for deterrence in that the actor who is being deterred must make a decision about whether or not to initiate action. Without a rational adversary, deterrence is hopeless.[77] It is generally assumed that violent NSAs are not rational, but even ideologically or religiously motivated terrorists have objectives that may warrant restraint.[78] Janice Gross Stein, director of the Munk Centre for International Studies at the University of Toronto, argues that when assessing rationality, context matters. Cognitive style, history, and culture combine to frame an adversary's rationale and decision calculus.[79] Understanding a group's rationale helps frame a strategy for deterrence.

Emanuel Adler, Chair of Israeli studies in the department of political science at the University of Toronto, suggests that the success or failure relies on a deterrence social structure.[80] The first of three tiers is the deterrence collective or background knowledge comprised of deterrence culture and common knowledge. The United States and Soviet Union shared a symmetric deterrence collective knowledge.[81] They understood deterrence, its rules, and objectives in the same way. Asymmetry defines the deterrence collective between Al Qaeda and the United States because they view deterrence as a tool to leverage against America.[82] Adler adds that when deterrence culture in this context is driven by religious and ethnic-nationalist beliefs there is little chance for developing common knowledge. If there is no shared knowledge, signals between the two are misinterpreted and deterrence fails. So if NSAs are to be deterred one must consider them rational and develop common understanding.

Violent NSAs have objectives that they desire to achieve. Given the fact that their actions are guided by goals and objectives gives clues to the fact that they are not irrational. The 9/11 attacks were planned well over a year prior to execution. The difficulty is in communicating intentions and whether or not those intentions are interpreted correctly or not seen as a credible threat. This comes down to the actors and their perceived power.

The second tier in Adler's model is the number of actors involved while the third tier focuses on the power relationship between the actors. Power is measured by material, technology, and social power.[83] Social power is determined by the ability of an actor to construct social reality and is related to actors' authority and legitimacy.[84] This is why terrorists often use the West's concept of deterrence against itself. A terrorist group commits an act of terror and the state retaliates. After the retaliatory strike, the group prepares the sight to show innocent civilians casualties to the media demonstrating the heavy handed nature of the state and the wanton disregard for human life.

This was a common sight during the most recent conflict between Israel and Hezbollah. Through media and image manipulation after Israeli aircraft bombed the terrorist organization, Hezbollah was able to produce horrific images that swayed local Lebanese, Arab, Muslim, and global public opinion.[85] These performances are an example of the deterrence trap into which NSAs will attempt to draw stronger states. Governments lose social power as a result of their action but also lose power when they do nothing, conveying the message that they are not able to protect the people. According to Alder, the only way out of this deterrence trap is to delegitimize terrorists. [86] This means defeating attacks and providing credible counter messages to discredit the terrorists. A strategy like this must limit punishment options that produce collateral damage and focus defensive measures.

Punishment strategies in cyberspace require accurate attribution. With today's technology, that is difficult at best. Although computers have a signature Internet Protocol (IP) address, attackers use botnets[87] to perpetrate an attack which leads to identifying computers that were unknowingly hijacked by hackers. Rouge packets can be bounced from computer to computer on their way to the target, hiding the origin of the attack.[88] Without attribution, retaliation in cyberspace will produce the equivalent of collateral damage in the physical domain. Unless something of value can be attacked, punishment will not work and defensive denial is the only remaining option.

Mearsheimer's decision calculus described above indicates that if the cost of an attack is high, or the probability of success is low, deterrence is effective.[89] Thus the more difficult it is to attack, the more it costs the attacker, the lower the value of success. Mathematically it looks like this: $D = \big(P(s)x\ V(s)\big) - \big(P(f)x\ V(f)\big)$ where $D = \text{Deterrence}, \mathrm{P(s)} = \text{Probability of Success}, \mathrm{V(s)} = \text{Value of Success}, \mathrm{P(f)} = \text{Probability of Failure},$ and $\mathrm{V(f)} = \text{Value of Failure.}$[90] $\big(P(s)x\ V(s)\big)$ represents the payoff for success while $\big(P(f)x\ V(f)\big)$ represents the cost. If D is less than zero, deterrence works. Cyberspace omniscience would eliminate an actor's anonymity, accurately attribute attacks, and increase the cost associated with attack via a precise retaliation. The world is becoming more interconnected and transparent, and cyber omniscience requires transparency.

The Quantum computer's ability to quickly break encryption codes, search data at extremely high speeds, and compute with greater power than today's supercomputers can break down barriers to cyber transparency. With appropriate software, it is possible for a quantum computer or a set of them to build a graphic depiction of what is happening in cyberspace in real time (this where the ability to quickly search data and solve differential equations becomes useful). That graphical depiction could be the cyber common operating picture (COP). A cyber COP gives situational awareness in cyberspace leading to cyber omniscience and attribution.

Disabling the offending computer or network with a computer network attack may develop future deterrence if the retaliatory strike conveys a clear signal to the offender. This is where the common deterrence knowledge could be built as long as the NSA understands who attacked them and there is no collateral demonstrable damage that can be exploited in a deterrence trap. Cyber omniscience gives actors the ability to attribute attack and counter with precision, but denial based strategies should still be explored.

Defensive denial comes in two forms. Denying capability requires physically controlling the distribution of quantum computers such that only the best and fastest remain with responsible governments. That requires treating quantum computers as controlled items such as nuclear material. Tight control of quantum computers would be tough, but ensuring the state had the latest and most up to date quantum computers would be easier. In this case, denial becomes a race to produce the most powerful quantum computers for the government and controlling their public release. An easier denial strategy involves denying NSAs their objectives.

Quantum computing and quantum communication enables denial strategies by protecting networks and information and therefore preventing NSAs from achieving their objectives. Quantum communication uses quantum super-position to enable secure communication through Quantum Key Distribution (QKD). Using photons, information is passed between two parties to establish a key for encryption of data over a classic network protocol. If the transmission of the key information is intercepted, the message decoheres and cannot be read, therefore the key is not compromised.[91] As long as that key is larger than the capabilities of the best quantum computer on the market then the data stays relatively safe behind classic RSA encryption.

Networks riding on quantum informatics, using entangled particles as described in the chapter three, could not be compromised because the message would decohere and become unreadable when attacked. Entire networks could be developed using quantum entanglement preventing any attempt to eavesdrop on the network or break-in. This would keep the network safe and deny the attacker any objectives. Thus deterrence is achieved.

Deterrence of NSAs requires a comprehensive approach that takes into consideration the context of the deterrence challenge as well as viable offensive, and defensive strategies. Those options are represented in figure below (Figure 7). Strictly speaking about operations in cyberspace in 25 years, the quantum computer provides solutions for both offensive and defensive options. First, using quantum computing to develop a cyber-COP moves the world toward cyber omniscience. Total omniscience in cyberspace solves attribution problems and makes punishment a credible option. Meanwhile, quantum informatics and computing provide good tools for defending information and networks, denying NSAs their objectives in cyberspace. With a good offensive and defensive strategy, deterrence of NSAs is possible.

Deterrence Option	**Equation component effected**	**Probability of Deterrence Success**
Cyber omniscience	Increases probability of failure	Increases
Punishment through CAN	Increases cost of failure	Increases
Denial of capability	Decreases probability of success	Increases
Deny objective	Decreases probability of success	Increases

Figure 7: Deterrence Options and Effects

[72] Stein, "Rational Deterrence Against 'Irrational' Adversaries?" 60.
[73] Paul, "Complex Deterrence: An Introduction," 5.
[74] John J Mearsheimer, *Conventional Deterrence*, (Ithaca: Cornell University Press, 1983), 23.
[75] Ibid., 23.
[76] George W. Bush, "Bush Delivers Graduation Speech at West Point." *White House.gov.* June 01, 2002. http://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html
[77] Stein, "Rational Deterrence Against 'Irrational' Adversaries?" 58.

78. James H. Lebovic, *Deterring International Terrorism and Rogue States: US National Security Policy after 9/11.* (New York: Routledge, 2007), 19-20.

79. Stein, "Rational Deterrence Against 'Irrational' Adversaries?" 74.

80. Emanuel Alder, "Complex Deterrence in the Asymmetric-Warfare Era," In *Complex Deterrence: Strategy in the Global Age*, by Patrick M. Morgan, James J. Wirtz and T. V. Paul (Chicago: The University of Chicago Press, 2009), 90.

81. Ibid., 94-95.

82. Ibid., 95.

83. Ibid., 91.

84. Ibid., 91.

85. Ibid., 98.

86. Ibid., 100.

87. Botnets are computers remotely networked together and used by a third party either for computing power our to conduct denial of service attacks on networks and websites.

88. Martin C. Libicki, *Cyberdeterrence and Cyberwar,* (Santa Monica: Rand Corporation, 2009),44.

89. Mearsheimer, *Conventional Deterrence*, 24.

90. Ibid., 23.

91. Collins, "Quantum Information Science," 103.

The **W**ay **F**orward

The world today is more interconnected than ever before and will only get smaller and flatter, as Friedman would say, as we move into the future. Technology and globalization potentially will make the world of 2035 more dangerous. Globalization offers prosperity while causing a backlash by violent fundamentalists who view it only as an evil thrust upon them by "the West," which they equate to the United States. Ironically, the very technology brought to them by globalization may be the very technology that the United States may have to defend against. The quantum computer is one such piece of technology.

Quantum information science is a field that is rapidly developing. To date, QKD is in production for secure key encryption and a two bit quantum computer has been realized by researchers at Yale. Moving forward, quantum entanglement and quantum superposition, the science behind the quantum computer, may be used to even further secure communications such that eavesdropping will become physically impossible. As these concepts are developed into reality, mathematicians have been hard at work on the algorithms that will move the quantum computer beyond encryption and cryptanalysis. Complex database searches, image processing, simulation, and modeling are just some of the potential uses for a desktop device with more power than a supercomputer. In the wrong hands, this technology becomes a threat.

The quantum computer will threaten the security of networks and critical information by quickly and easily breaking encryption schemes. In the hands of violent NSAs, it poses a serious security threat. Deterring its use is vital to the security of the United States. With this powerful technology, offensive and defensive cyber deterrent strategies are possible.

Using the quantum computer to enable cyber omniscience increases the probability of failure as well as the cost of failure for would be attackers. The power of a quantum computer may be used to model the entirety of cyberspace. Identifying those who enter and exit cyberspace and recognizing suspicious behavior puts would be attackers at risk of retaliation due to accurate attribution. If the chance of punishment is not deterrent enough, denial strategies are available using the quantum computer.

Denying complete access to quantum computing will be difficult, but denying access to the most powerful quantum computers and allowing states to use them to secure data and networks is possible. Using either QDK or quantum communication, networks become virtually impenetrable. But it requires continuous improvement and evolution of encryption keys and schemes to stay ahead of any would be attackers.

Policy Option	Equation Component Effected	Probability of Deterrence Success
Lead pursuit of quantum computer technology	Cyber omniscience Increase Cost	Increase
Lead research of quantum encryption and information science	Increase probability of failure	Increase
Delay release of production capability to commercial sector	Increase probability of failure	Increase

Figure 8: Policy Options

From a policy standpoint (Figure 8), it behooves the United States to aggressively continue to pursue quantum computing and information science. It alone can change the paradigm for addressing cybercrime, espionage, and terrorism. This is one area that will become a race between nations to develop the capability first and to remain on top. The United States has already made great strides in the field, but they need to build upon what they have learned and continue to push toward cyber omniscience. Once that is a reality, deterrence becomes easier.

Denial includes safeguarding the technology. The potential harm that a quantum computer could do warrants its gradual release of capabilities, while states maintain an upper hand in order to ensure the security of critical infrastructure, networks, and data. Continued advancement in encryption and cryptanalysis will work in conjunction with the quantum information science to ensure states maintain information security in a more transparent world.

While the focus of this paper was deterrent options in cyberspace, deterrence strategies must also include options across the diplomatic, military, and economic realms. A comprehensive approach creates more options for decision makers when dealing NSAs. Options can then be applied at the appropriate time and place to achieve maximum deterrent effect. Further study should focus on how to deter specific groups based upon their objectives and capability.

Bibliography

Alder, Emanuel. "Complex Deterrence in the Assymetric-Warfare Era." In *Complex Deterrence: Strategy in the Global Age*, by Patrick M. Morgan, James J. Wirtz and T. V. Paul, 345. Chicago: The University of Chicago Press, 2009.

Barnett, Thomas P.M. *The Pentagon's New Map: War and Peace in the Twenty-First Century.* New York: G.P. Putman's Sons, 2004.

Bunckley, Nick, and Liz Robbins. "Nigerian Arraigned in Bomb Attempt." *The New York Times*, January 9, 2010: A9.

Bush, George W. "President Bush Delivers Graduation Speech at West Point." *White House.gov.* June 01, 2002. http://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html.

Cable Network News. "CNN World." *CNN.* December 11, 2009. http://www.cnn.com/2009/WORLD/asiapcf/12/11/pakistan.arrests/index.html.

CBS News. "60 Minutes." Cyber War: Sabotaging the System. *cbsnews.com.* November 8, 2009. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

Collins, Craig. "Quantum Information Science: DARPA'S New Frontier." In *50 Years of Bridging the Gap*, by DARPA, 252. Washinington DC: Defense University Press, 2009.

Friedman, Thomas L. *The World is Flat: A Brief history of the Twenty-First Century.* New York: Farrar, Straus, Giroux, 2005.

Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies--and What It Means to Be Human.* New York: Broadway Books, 2005.

Gilder, George. "The Information Factories." *Wired.com.* October 14, 2006. http://www.wired.com/wired/archive/14.10/cloudware.html.

Gorman, Siobhan. "Utilities, Refineries and Banks Are Victims of Cyber Attacks, Report Says." *Wall Street Journal,* January 29, 2010. http://online.wsj.com.

Gorman, Siobhan, and Evan Perez. "FBI Probes Hack at Citibank: Russian Cyber Gang Suspected of Stealing Tens of Millions; Bank Denies Breach." *Wall Street Journal,* December 22, 2009. http://online.wsj.com.

Gorman, Siobhan, Yochi J. Dreazen, and August Cole. "Insurgents Hack U.S. Drones." *Wall Street Journal,* December 17, 2009. http://online.wsj.com.

Hardesty, Larry. "Quantum Computing May Actually Be Useful." *web.mit.edu.* October 9, 2009. http://web.mit.edu/newsoffice/2009/quantum-algorithm.html.

Johnson, George. *A Shortcut Through Time: The Path to the Quantum Computer.* New York: Alfred A. Knopf, 2003.

Kapur, S. Paul. "Deterring Nuclear Terrorists." In *Complex Deterrence: Strategy in teh Global Age*, by T. V. Paul, Patrick M. Morgan and James J. Wirtz, 345. Chicago: The University of Chicago Press, 2009.

Kurzweil, Ray. *The Singularity is Near: When Humans Transcend Biology.* New York, New York: Penguin Books, 2005.

Lachow, Irving. "Cyber Terrorism: Menace or Myth?" In *Cyberpower and National Security*, by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz. Dulles, Virginia: National Defense University Press & Potomac Books, Inc., 2009.

Lebovic, James H. *Deterring International Terrorism and Rogue States: US National Security Policy after 9/11.* New York: Routledge, 2007.

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica: Rand Corporation, 2009.

Lillington, Karlin. "Quantum Leap." *The Irish Times,* February 2, 2009: 1.

Lloyd's List. "Quantum Mechanics Makes More of Moore; Quantum Computing May Facilitate New Types of Applications and Enable Us to Escape the Limitations of Moore's Law." *Lloyd's List*, January 11, 2008: 7.

Marwat, Abbas Majeed Khan. *Interrogation Report.* Police Report, Sargodha: Sargodha Police, 2009.

Mayne, Mark. "Encryption - Past, Present and Future." *SC Magazine*, September 9, 2009: 32-34.

Mearsheimer, John J. *Conventional Deterence.* Ithaca: Cornell University Press, 1983.

Milburn, Gerard J. *The Feynman Processor: Quantum Entanglement and the Computing Revolution.* Reading: Perseus Books, 1998.

Miller, Michael. *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online.* Indianapolis: Que Publishing, 2009.

Mockenhaupt, Brian. "We've Seen the Future and It's Unmanned." *Esquire Magazine On Line.* October 14, 2009. http://www.esquire.com/print-this/unmanned-aircraft-1109.

Paul, T V. "Complex Deterence: An introduction." In *Complex Deterrence: Strategy in the Global Age*, by T V Paul, Patrick M Morgan and James J Wirtz, 1-27. Chicago: The University of Chicago Press, 2009.

Paul, T. V., Patrick M. Morgan, and James J. Wirtz. *Complex Deterrence: Strategy in the Global Age.* Chicago: University of Chicago Press, 2009.

Schmidt, Stanley. *The Coming Convergence: Surprising Ways Diverse Technologies Interact to Shape Our World and Change the Future.* New York, New York: Prometheus Books, 2008.

Secure Computing (SC) Magazine. "Quantum Computing." *SC Magazine*, July 1, 2008: 8.

Shaud, John A., and Adam Lowther. "Deterring Nonstate Actors." *Air Force Research Institute Research Study.* Maxwell Air Force Base: Air University Press, November 2009.

Shelley, Louis I., et al. *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism.* Government, Washington D.C.: U.S. Department of Justice, 2005.

Silberglitt, Richard, Philip S. Anton, David R. Howell, and Anny Wang. *The Global Technology Revolution 2020: Bio/Nano/Materials/ Information Trends, Drivers, Barriers, and Social Implications.* Santa Monica: Rand Corporation, 2006.

Skoudis, Edward. "Evolutionary Trends in Cyberspace." In *Cyberpower and National Security*, by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 147-170. Dulles: Potomac Books, Inc., 2009.

Stein, Janice Gross. "Rational Deterrence Against "Irrational" Adversaries? No Common Knowledge." In *Complex Deterrence: Strategy in the Global Age*, by T V Paul, Patrick M. Morgan and James J. Wirtz, 58-82. Chicago: The University of Chicago Press, 2009.

University of Oregon. *University of Oregon.* December 2, 2009. http://abyss.uoregon.edu/~js/images/spin.gif.

VeriSign. *Secure Sockets Layer: How It Works.* January 1, 2010. http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/.

Virginia Institute of Technology. *Turing Machine.* December 3, 2001. http://courses.cs.vt.edu/~cs1104/ModelsComp/Working.010.html.

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenge.* Washington D.C.: United States Institute of Peace, 2006.

Wikipedia. *Secure Shell.* February 15, 2010. http://en.wikipedia.org/wiki/Secure_Shell.

"Wi-Fi." *Wikipedia.* 11 02, 2009. http://en.wikipedia.org/wiki/Wi-Fi.

Williams, Paul L. *The Al Qaeda Connection: International Terrorism, Organized Crime and the Coming Apocalypse.* Amherst: Prometheus Books, 2005.

Yahoo! "Yahoo! ExpandsCommunity Services with Free E-mail." *Yahoo docs.* October 8, 1997. http://docs.yahoo.com/docs/pr/release124.html.

Yale University. "First Electronic Quantum Processor Created." *www.sciencedaily.com.* June 29, 2009. http://www.sciencedaily.com/releases/2009/06/090628171949.htm.