National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE FUTURE OF ARTIFICIAL INTELLIGENCE AND QUANTUM COMPUTING CAPABILITY

Major Benjamin T. Hendrickson, United States Air Force

JCSP 45

Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 45

Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
2018 – 2020

SOLO FLIGHT

The Future of Artificial Intelligence and Quantum Computing Capability

Major Benjamin T. Hendrickson, United States Air Force

THE FUTURE OF ARTIFICIAL INTELLIGENCE AND QUANTUM COMPUTING CAPABILITY

"*Everything we call real is made of things that cannot be regarded as real. If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet."*

–Niels Bohr, Danish Physicist and Philosopher

INTRODUCTION

Advanced capabilities in Artificial Intelligence technologies have increased the need to develop Cybersecurity strategy worthy of safeguarding critical infrastructure. Current day cybersecurity capabilities are bound by their own limitations, which will ultimately be exposed through advances in quantum computing. Personal information, national security data, critical infrastructure, and our electronic footprint at large are all protected by a relatively complex set of encryption, essentially a hand shake between the information requestor and receiver. Cracking this code with our current technology would take many years. Enter the world of quantum computing. This technology has the capability of performing tasks in a fraction of a second. Fortunately, the science involved within the quantum computing world is still in its infancy. Despite all of the calls for alarm, this technology is still many years away, but within reach. This technology is advancing quickly and will likely not have an advance warning when it does arrive. The problem is simple, any data currently protected by modern encryption techniques will be vulnerable if cybersecurity encryption capabilities do not advance to meet this new threat. As the great power competition evolves any potential vulnerabilities will need to be properly defended. This paper will explore the advancement of quantum computing, the capability it provides for artificial intelligence and how this power would threaten the ability to protect the national security, local infrastructure and personal safety.

While it is important to understand the differences of quantum and conventional computing, it is equally important to know that research into quantum computing capabilities are still exploring the baseline of complex computing systems[1]. Quantum computing is not a universal solution or replacement for modern computing systems, but rather an added capacity for machine learning technologies. An in-depth explanation of quantum mechanics is far beyond the scope of this paper, but certain aspects will provide context and highlight security concerns behind artificial intelligence capabilities.

QUANTUM THEORY

It is not the intent of this paper to prove colossal theories in physics or solve complex equations, but it is interesting to understand why quantum is so strange and why the problems are challenging. First, the theory of relativity as posed by Albert Einstein presents the idea that time is a form of classical mechanics adherent specifically to the observer. His theory identifies and specifically describes the location in time and space, which fits perfectly into the classical mechanics envelope. Objects must have a reason for moving in a particular direction and relativity would describe how and even when it will arrive. While the ideas are complex, they are described and even proven through mathematics. This theory works very well for relatively larger objects, but becomes much more complicated at the atomic level, which was exposed in the study of light. A 42 year old physicist Max Planck's research identified a phenomena called light quanta, or the behavior of particles which would lead to the wave mechanics[2]. Einstein would later present work declaring light behaved both as waves and particles, but more

[1] Warner A. Miller and Rainer Steinwandt, Quantum Technology, High Speed Encryption and Global Analysis of Networks. (Florida: Florida Atlantic University, 2018), 22-23.

[2] Scott Bembenek. Einstein and The Quantum (Scientific American Blog Network, 2018).

importantly light had a ‘strange’ behavior not easily explained[3]. Figure 1 shows the difference between the classical and quantum concepts, essentially highlighting the ability of quantum to behave outside of a classical mechanics picture.

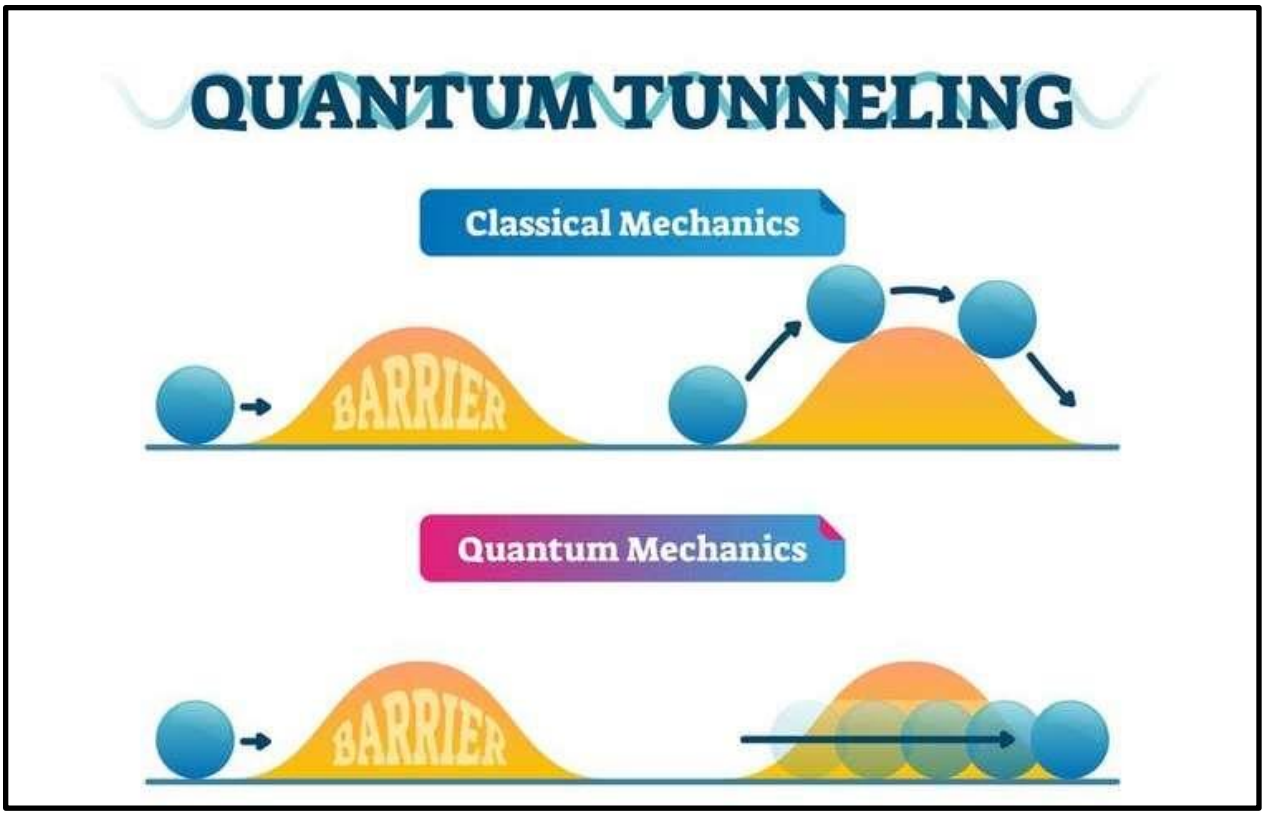

Figure 1 -- Classical Mechanics vs Quantum Mechanics

Source: Satya Sainadh, “We did a breakthrough 'speed test' in quantum tunneling, and here's why that's exciting” (Phys.org, March 19, 2019). https://phys.org/news/2019-03-breakthrough-quantum-tunnelling.html

Many contradictory theories and events occurred as a result of these areas of research, but the important outcome for the purpose of this paper is the spontaneous emission of photons. These photons reactions spawned the invention of laser light and eventual ability to harness this

[3] Ibid.

in the form of transistors, primarily used operate computers today[4]. But there was something strange with the random emission of photons that suggest a significant element of probability was responsible for this behavior. The famous Schrodinger's cat experiment and other such as the double slit experiment would confirmed the discovery surrounding probability, more specifically the behavior of these particles are only known at the time of observation. It is this unique characteristic of light that allows quantum computing to operate outside of a simple 'on' or 'off', 1 or 0 stream of binary information. Quantum theory allowed this form of light to be a range of possible outcomes, all at once. The tricky part, and the focus on quantum computing research to this day surrounds the capability of controlling a quantum state and ultimately developing a capability to calculate multiple outcomes all at once, prior to observation[5]. Artificial intelligence capabilities would benefit through increased computing power and enhance the ability to develop machine learning techniques with exponentially more processing power than though current methods, but the physical limitations keep the technology from its full potential.

QUANTUM COMPUTING

Classical computing techniques operate through observed, physical known binary code is stored in classical computers using one of two positions, on or off[6]. Binary values are simply, 1 or 0 and essentially make up long strings of information that we see as a word document, iTunes songs or movies[7]. These binary numbers and more specifically each digit is considered a bit, which is combined in sequence to equal a logical expression. Quantum computing takes this

[4] Scott Bembenek. Einstein and The Quantum (Scientific American Blog Network, 2018).
[5] Martin Giles, Explainer: What is a Quantum Computer? How it works, why it's so powerful, and where it's likely to be the most useful first (January 29, 2019).
[6] *Ibid.*
[7] Martin Giles, Explainer: What is a Quantum Computer? How it works, why it's so powerful, and where it's likely to be the most useful first (January 29, 2019).

capability and exploits the properties of the quantum world through multi-positioning and an even stranger concept that mirrors the behavior at a distance.

Imagine a system capable of being in the same or multiple positions at once. A binary bit can only be in single state of 1 or 0, while if you imagine a three dimensional sphere, a quantum computer can encodes information within any state on this sphere. This is the basic concept of quantum computing, in the form of a qubit and is shown in figure 2.

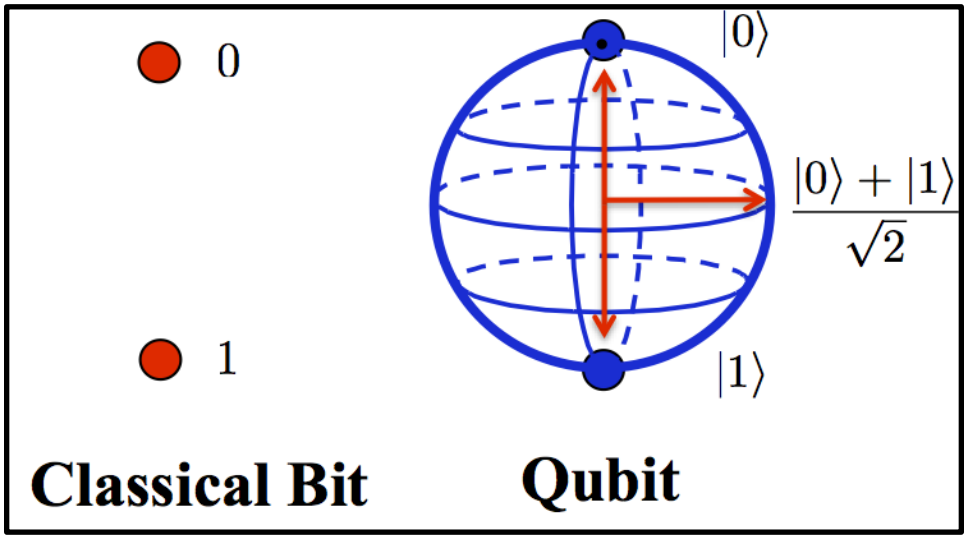

Figure 2 -- Classic Bit vs Qubit

Source: Sam Sattel, The Future of Computing – Quantum and Qubits (EAGLE, 2016).

Qubits or quantum bits are used to compute quantum systems and are achieved through superposition and entanglement properties. Superposition defines the ability of qubits to represent numerous possible combinations of positions simultaneously and allow each of them to perform multiple computations at once[8]. Entanglement describes the ability of qubits to exist in a single quantum state and provide one of the strangest capabilities in the quantum field by

[8] Martin Giles, Explainer: What is a Quantum Computer? How it works, why it's so powerful, and where it's likely to be the most useful first (January 29, 2019).

reacting identical to its counterpart, even at large distances[9]. This stumped Einstein to the point that he famously referred to this phenomenon as "spooky action at a distance" and it haunted his research until he died[10]. It's this level of strange science that produce science fiction type fantasies such as teleporting. In reality, the ability to perform multiple computations at the same time single handily changes the scope of artificial intelligence possibilities and raises the stakes for gaining an edge on this technology.

While quantum computing capabilities are noteworthy and the potential is promising, there are many challenges. In fact, to understand the scale of this potential, a quantum computer with only 300 quantum bits could theoretically compute more calculations than there are atoms in the universe[11]. Qubits have the ability to hold 1 billion more 'bits' of information than a binary bit, however this complexity comes at a price[12]. Quantum information is vulnerable to environmental conditions and ultimately require equipment that make these computers significantly larger and fragile than a modern laptop or handheld device. Subatomic quantum particles easily become unstable and lose the ability to benefit from the superposition and entangled qualities, essentially rendering them useless. Experts in the quantum field believe we are getting closer to a working quantum computer, but we are still many years or possibly decades away from truly effective quantum technology that do not require vacuums and temperatures near absolute zero[13].

[9] Scott Bembenek. Einstein and The Quantum (Scientific American Blog Network, 2018).
[10] *Ibid.*
[11] Dr. Arthur Herman and Idalia Friedson, Quantum Computing: How to Address the National Security Risk (Washington D.C., August 2018), 3.
[12] Jonathan Hui, QC – What is a quantum Computer? (Medium: Science, Nov 5, 2018).
[13] Jonathan Hui, QC – What is a quantum Computer? (Medium: Science, Nov 5, 2018).

ARTIFICIAL INTELLIGENCE

So what does all of this mean for Artificial Intelligence? First and probably the most impressive, the ability to factor large numbers, which is key to modern encryption techniques[14]. Quantum computing will provide the ability to not only factor large numbers, but do so randomly and much more efficiently. Imagine searching for an answer to a problem and simultaneously searching thorough every book at the library to produce not only a single answer, but thousands of answers close to the actual solution. For example, an image is broken into thousands of pieces and sorted through a multi-layered network, each analyzing individual pixels and producing a result. In the case provided in image 3 we find the output is a dog, but what if we want to know what kind of dog? The amount of possibilities require a complex set of matrices, which happens to be ideal for quantum computing since it has the ability to handle random patterns and identify anomalies[15].

[14] Dr. Arthur Herman and Idalia Friedson, Quantum Computing: How to Address the National Security Risk (Washington D.C., August 2018), 5.
[15] Ibid, 7-8.

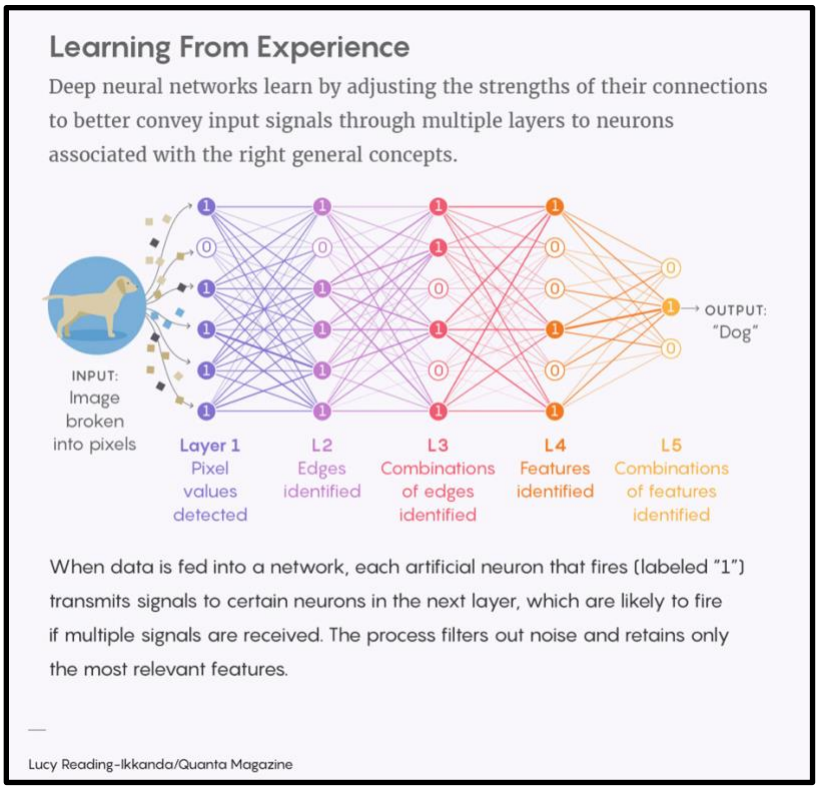

Figure 3 --Artificial Intelligence example: Illustrates the ability of artificial intelligence to identify incorrect data points and collectively determine an object.

Source: Natalie Wolchover, New Theory Cracks Open the Black Box of Deep Learning (Quanta Magazine, September 21, 2017). https://www.quantamagazine.org/new-theory-cracks-open-the-black-box-of-deep-learning-20170921/

A small Canadian company, BlueDot was one of the first to break the news of a potential serious medical outbreak using an artificial intelligence driven algorithm[16]. The algorithm was designed by engineers, geographers, ecologists and medical experts in the respective fields over the span of a year to detect over 150 pathogens and track potential contagions through cell phone, GPS and flight manifest data[17]. Timing is critical in these kind of situations as it allows doctors, frontline workers and citizens to take extra precautions and reduce the spread. Artificial

[16] Bill Whitaker, The Computer Algorithm that was Among the First to Detect the Coronavirus Outbreak (60 Minutes, April 27, 2020). https://www.cbsnews.com/news/coronavirus-outbreak-computer-algorithm-artificial-intelligence/
[17] *Ibid.*

intelligence algorithms like the one BlueDot created could change the way governments plan for future pandemics. It's been obvious to many that nobody expected this level of outbreak and it's more concerning to think without this kind of technology the impact of the virus could have been much worse. Artificial intelligence is far from perfect, but the potential shown by BlueDot has exposed a whole new level of capability.

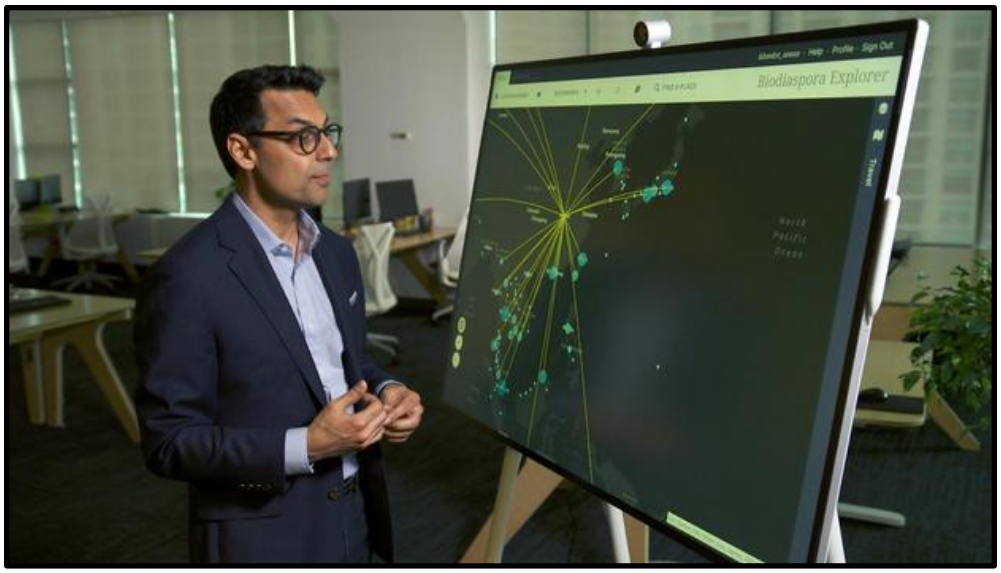

Figure 4 -- Dr. Kamran Khan describes how the BlueDot algorithm traced the origin of Coronavirus and identified population centers that would be effected through flight travel.

Source: Bill Whitaker, The Computer Algorithm that was Among the First to Detect the Coronavirus Outbreak (60 Minutes, April 27, 2020). https://www.cbsnews.com/news/coronavirus-outbreak-computer-algorithm-artificial-intelligence/

Another advantage of quantum computing and potential for artificial intelligence capabilities is the ability to build more complex models. Information and hybrid warfare techniques would absolutely thrive with advances in this area. These data sets would feed machine learning algorithms and ultimately provide an ability to produce quick answers to decision makers or commanders in the field. Artificial intelligence could theoretically identify the enemy, execute information operations, control critical resources and launch kinetic attacks

with precision, all with minimal human interaction. Data built in models, analyzed through complex matrices and executed through a series of predetermined thresholds.

Machine learning techniques have already been successful in identifying embedded code intended to attack vulnerable systems. Data bases have been compiled in order to train machine learning algorithms to spot variants of existing malware hidden within useless code a hacking group in Vietnam attempted to launch[18]. The ability to manipulate security software is specific strength of Artificial Intelligence and the power of quantum technology, but it is also a strength of cybersecurity through an impressive ability to identify anomalies and react appropriately. Machine learning techniques could potentially allow malicious attacks to essentially take on a life of their own and it will be up to the strength of our cybersecurity to use self-learning as an advantage to seek out negative behaviors[19]. It is important to note that the human element will not be replaced, but rather artificial intelligence capacities will enhance the role of cybersecurity.

The human element thresholds are apparent when considering the exploitation of strategic threats on the battlefield, but could not be possible without the assistance of artificial intelligence. Terabytes of data are collected daily across the intelligence community for example, making it impossible for an analyst, or even a group of analysts to accurately sort through and make accurate assessments. Artificial intelligence makes it possible to perform data mining functions and reduce the possibility of missing important pieces of information. Additionally, this information can be used to develop a larger dataset that would provide a means of fine tuning algorithms, essentially increasing the intelligence of the machine.

---

[18] Danny Palmer, AI is changing Everything about Cybersecurity for the better and for worse. Here's what you need to know (ZDNet, March 2, 2020). https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/

[19] Zachary S. Davis, Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise (Center for Global Security Research Lawrence Livermore National Laboratory, March 2019)

QUANTUM COMPUTING

Quantum computing will absolutely enhance artificial intelligence and if armed with the appropriate technology will pose a significant threat to national security since critical infrastructure and information rely on asymmetric encryption. Asymmetric or Public-key encryption is secure because the solution involves finding the semi-prime solution to two very large numbers and matching it with a privately held key, a task that would take modern computers years to complete[20]. Passwords and two factor identification are other methods of safeguarding data, but as we know there are limitations to these preventive steps, especially since data breaches exposed 4.1 billion records in the first half of 2019[21]. The cost of cybercrime globally is estimated to exceed $6 trillion USD by 2021[22].

There is a good chance that if you had an email account, stayed in a hotel, shopped at a retail store, rode in an uber or simply used your credit card, your information is being shared on the dark web. This is our reality now. Imagine what would happen if hackers had the ability to breach any current public-key encryption technology in seconds? In a 2018 Hudson Institute paper, Dr. Arthur Herman and Idalia Friedson called quantum computer capability equivalent to a 'quantum Pearl Harbor,' referencing the ability to access a large portion of public infrastructure to include; electrical grids, water purifications, transportation systems, traffic lights, railroad,

[20] Dr. Arthur Herman and Idalia Friedson, Quantum Computing: How to Address the National Security Risk (Washington D.C., August 2018), 6-7.
[21] Rob Sobers, 110 Must-Know Cybersecurity Statistics for 2020 (Varonis, April 15, 2020). https://www.varonis.com/blog/cybersecurity-statistics/
[22] Kenneth Coats, The Cyber Threats Every Company Should Know About (August 16, 2019). https://www.forbes.com/sites/forbestechcouncil/2019/08/16/the-cyber-threats-every-company-should-know-about/#7bd0f1ac10c2

nuclear power plants, etc[23]. It is imperative that regardless of the anticipated timeline of a launch of quantum computing we leverage our existing knowledge and artificial intelligence capabilities to develop appropriate cybersecurity defense.

The addition of quantum computing will provide is a serious threat to national security by itself, however the data being collected now will also be at risk once there is a solution. For this reason, it is critical that quantum cybersecurity aspects are implemented now. Fortunately, cybersecurity is evolving in this direction through quantum random-number generators, which can be used for quantum or current cryptography[24]. Quantum keys are used in place of public-key encryption to produce a software solution and are currently being used in banks, governments and private cloud carriers but are not a universal solution, quantum cryptography will still need to be enhanced once the physical quantum technology arrives[25]. While it is hard to predict when the quantum capabilities will arrive, post quantum cryptography methods are at least ten years away. The race is on for quantum 'supremacy.'

GREAT POWER COMPETITION

As the great power competition continues, each country strives to find an edge and quantum computing technology may be the answer. China has pledged to become the world leader in a $150 Billion (USD) artificial intelligence technology industry by 2030[26]. In 2017 Vladimir Putin announced that whoever leads Artificial Intelligence in 2030 will dominate global

[23] Dr. Arthur Herman and Idalia Friedson, Quantum Computing: How to Address the National Security Risk (Washington D.C., August 2018), 10.
[24] Danny Palmer, AI is changing Everything about Cybersecurity for the better and for worse. Here's what you need to know (ZDNet, March 2, 2020). https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/
[25] *Ibid.*
[26] Paul Mozur, Beijing Wants A.I. to be Made in China by 2030 (The New York Times, July 20, 2017). https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html

power, which was catalyst of the 2019 national artificial intelligence strategy[27]. President Trump also announced in 2019 that the U.S. government has established an artificial intelligence initiative focused on providing a whole-of-government approach to research and development in the field[28]. In all of these cases, quantum computing would provide an upgrade they are seeking. The real question is, when will this be possible? If it is possible at all. While quantum computing is impressive, there have been decades of research with minimal practical results to show[29].

Currently, China lags behind the United States and the United Kingdom in Artificial Intelligence hardware since the United States companies lead the industry in semiconductor chips, but they expect to make major advances in the Artificial Intelligence field in the next 5-10 years[30]. The majority of China's efforts have been concentrated on research so as this research progresses it is reasonable to believe they will achieve their 2030 artificial intelligence leader goal. They have the ability to test features such as the highly controversial face reconditioning software, which through artificial intelligence algorithms identify a person from a data base of at least 2 billion people in a matter of seconds[31]. China has used this technology to augment law-enforcement and control society through a social credit system designed to blacklist those violating laws and reward those who obey. The idea is terrifying to those with any value in personal privacy, but President Xi Jingping's ambition is to create a 'completely transparent

[27] Indermit Gill, Whoever leads in artificial intelligence in 2030 will rule the world until 2100 (Brookings, January 17, 2020).
[28] Select Committee on Artificial Intelligence, The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update (National Science & Technology Council, June 2019). 1-3.
[29] Mikhail Dyakonov, The Case Against Quantum Computing (IEEE Spectrum, November 15, 2018).
[30] Sarah O'Meara, Will China Overtake the U.S. in Artificial Intelligence Research? (Scientific American, August 24, 2019).
[31] Amanda Lantino, This Chinese facial recognition start-up can identify a person in seconds (CNBC, May 17, 2019).

society'[32]. While these advances in artificial intelligence are concerning, it speaks to the commitment China has in the global power competition. The strength in artificial intelligence will only be enhanced with the origin of quantum computing and will ultimately change the strategic policies of the United States and its allies.

Russia has similar ambitions in the global power competition despite having an economy eight times smaller than China[33]. The money that they do have has been focused on modernization efforts to the navy and cyber warfare, both provide capabilities aimed at achieving the maximum level of influence and information operations. Russia recognizes the potential for economic and strategic significance in the Northern Sea Route and initiated a significant polar region military buildup. Advances in artificial intelligence will only benefit Russia's ability to achieve President Putin's goals without the use of conventional warfare. According to the U.S. Geological Survey, there are an estimated 412 billion barrels of oil, roughly 22% of global undiscovered reserves in the Arctic, which highlights the importance of developing an effective defense against Russian aggression in the region[34]. Information operations leverage political differences between the United States and Canada to gain influence in the region and pursue control of northern trade routes as artic regions adjust to global temperature changes. Increased artificial intelligence capabilities would create a means for Russia to expedite these efforts and challenge the balance of power in the great power competition.

---

[32] Christina Zhou and Bang Xiao, China's Social Credit System is pegged to be fully operational by 2020 – but what will it look like (January 1, 2020). https://www.abc.net.au/news/2020-01-02/china-social-credit-system-operational-by-2020/11764740

[33] Ron R. Wallace. The Arctic is Warming and Turning Red: Implications for Canada and Russia in an Evolving Polar Region (Canadian Global Affairs Institute, January 2019). https://www.cgai.ca/the_arctic_is_warming_and_turning_red_implications_for_canada_and_russia_in_an_evolving_polar_region#Canadian

[34] *Ibid.*

CONCLUSION

The quantum field of study has promising capabilities and is definitely something we cannot ignore regardless of the challenges. The possibilities are endless, especially when integrated with artificial intelligence. The ability to detect anomalies within large datasets at lighting quick speeds have a boundless potential for safeguarding against fraud, protecting critical infrastructure, exploring medical mysteries, and connecting pharmaceutical responses in a fraction of the time as modern techniques. The latter may be critical in the event of a medical emergency or bio-weapon scenario, much like the reality we have found ourselves in today with Covid-19. Artificial intelligence and machine learning technology will exponentially improve capabilities with quantum computing techniques. While this capability may be years way from it's full potential. The artificial intelligence community as a whole is learning techniques from quantum computing that will advance modern computing despite computing limitations. However, planning for the day quantum computing arrives will be critical, especially our cybersecurity defense and encryption methods. While Niles Boyd was correct in stating the ultimate complexity of the quantum world, he also stated "every great and deep difficulty bears in itself its own solution. It forces us to change our thinking in order to find it.[35]"

[35] Elizabeth Palermo, Niels Bohr: Biography & Atomic Theory. (LiveScience, Aug 29, 2017). https://www.livescience.com/32016-niels-bohr-atomic-theory.html

BIBLIOGRAPHY

Bembenek, Scott, "Einstein and The Quantum" *Scientific American Blog Network*, Last Modified March 27, 2018. Https://blogs.scientificamerican.com/observations/einstein and-the-quantum.

Coats, Kenneth, "The Cyber Threats Every Company Should Know About, " Last modified August 16, 2019, https://www.forbes.com/sites/forbestechcouncil/2019/08/16/the-cyber threats-every\company-should know-about/#7bd0f1ac10c2

Davis, Zachary S. "Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise", *Center for Global Security Research Lawrence Livermore National Laboratory,* (March 2019).

Dyakonov, Mikhail "The Case Against Quantum Computing" IEEE Spectrum, Last modified November 15, 2018. https://spectrum.ieee.org/computing/hardware/the-case-against quantum-computing.

Giles, Martin, "What is a Quantum Computer? How it works, why it's so powerful, and where it's likely to be the most useful first," MIT Technology Review, Last Modified January 29, 2019. https://www.technologyreview.com/2019/01/29/66141/what-is quantumcomputing/

Gill, Indermit, "Whoever leads in artificial intelligence in 2030 will rule the world until 2100," Brookings, Last Modified January 17, 2020. https://www.brookings.edu/blog/future development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the world-until-2100/

Herman, Arthur and Friedson, Idelia, "Quantum Computing: How to Address the National Security Risk" (Washington D.C., August 2018), 3. https://www.brookings.edu/ blog/future-development/2020/01/17/whoever-leads-in artificial-intelligence-in-2030 will-rule-the-world-until-2100/

Hui, Jonathan, "QC – What is a quantum Computer?" *Medium: Science* (Nov 5, 2018).

Miller, Warner A., and Rainer Steinwandt, "Quantum Technology, High Speed Encryption and Global Analysis of Networks." Florida: Florida Atlantic University, (2018), 22-23.

Mozur, Paul, "Beijing Wants A.I. to be Made in China by 2030" The New York Times, Last Modified July 20, 2017. https://www.nytimes.com/2017/07/20/business/china-artificial intelligence.html

Lantino, Amanda, "This Chinese facial recognition start-up can identify a person in seconds" *CNBC,* Last Modified May 17, 2019. https://www.cnbc.com/2019/05/16/this-chinese facial-recognition-start-up-can-id-a-person-in-seconds.html

O'Meara, Sarah, "Will China Overtake the U.S. in Artificial Intelligence Research?" *Scientific American*, (August 24, 2019).

Palermo, Elizabeth, "Niels Bohr: Biography & Atomic Theory," LiveScience, Last Modified August 29, 2017. https://www.livescience.com/32016-niels-bohr-atomic-theory.html

Palmer, Danny, "AI is changing Everything about Cybersecurity for the better and for worse. Here's what you need to know," *ZDNet*, Last Modified March 2, 2020. https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better and-for-worse-heres-what-you-need-to-know/

Sainadh, Satya, "We did a breakthrough 'speed test' in quantum tunneling, and here's why that's exciting," *Phys.org*, Last Modified March 19, 2019. https://phys.org/news/2019-03 breakthrough-quantum-tunnelling.html.

Sattel, Sam, "The Future of Computing – Quantum and Qubits," *EAGLE*, (2016).

Sobers, Rob, "110 Must-Know Cybersecurity Statistics for 2020," Varonis, Last Modified April 15, 2020. https://www.varonis.com/blog/cybersecurity-statistics/

United States, "Select Committee on Artificial Intelligence, The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update," *National Science & Technology Council*, (June 2019). 1-3.

Wallace, Ron R. "The Arctic is Warming and Turning Red: Implications for Canada and Russia in an Evolving Polar Region," *Canadian Global Affairs Institute*, Last Modified January 2019. https://www.cgai.ca/the_arctic_is_warming_and_turning_red_implications _for_canada_and_russia_in_an_evolving_polar_region#Canadian

Whitaker, Bill. "The Computer Algorithm that was Among the First to Detect the Coronavirus Outbreak," *60 Minutes*, Last Modified April 27, 2020. https://www.cbsnews.com/news/ coronavirus-outbreak-computer-algorithm-artificial-intelligence/

Wolchover, Natalie. "New Theory Cracks Open the Black Box of Deep Learning," *Quanta Magazine*, Last Modified September 21, 2017. https://www.quantamagazine.org/new theory-cracks-open-the-black-box-of-deep-learning-20170921/

Zhou, Christina and Bang Xiao, "China's Social Credit System is pegged to be fully operational by 2020 – but what will it look like," ABC News, Last Modified January 1, 2020. https://www.abc.net.au/news/2020-01-02/china-social-credit-system-operational-by-2020/11764740