National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

QUANTUM COMPUTERS – IS THE CANADIAN ARMY READY TO FACE THIS THREAT?

Major D.Y. Begin

JCSP 45

Service Paper

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

Étude militaire

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

14 Octobre 2018

DS 545 Component Capabilities

QUANTUM COMPUTERS – IS THE CANADIAN ARMY READY TO FACE THIS THREAT?

By Major D.Y. Begin

Word Count: 2545

Nombre de mots : 2545

QUANTUM COMPUTERS – IS THE CANADIAN ARMY READY TO FACE THIS THREAT?

AIM

1. The aim of this service paper is to inform the Canadian Army (CA) Chief Of Staff Strategy of the threat associated with the rise of Quantum Computing (QC) and the impact on the encryption of CA classified Information Systems (IS). This paper will first define quantum computing as a threat and then discuss the actions currently undertaken by the Canadian Armed Forces (CAF) to protect all IS. Following, quantum computing security risks will be evaluated against the tactical, operational and strategic domains of the CA to outline some areas of concerns and to propose ideas.

2. This paper only looks at the QC threat and impacts at the unclassified level, but additional discussion at the classified level is required to better understand the ramifications and mitigations associated with QC threat.

INTRODUCTION

3. Unlike regular computers which use bits as a measure of data, QC uses the quantum mechanics properties of physical quantum bits, or qubits, as a measure of data. QC possesses exponentially more processing power than traditional computers and will be capable of solving current impossible mathematical equations in seconds.[1] A computer with just a few hundred qubits would be capable of performing more calculations simultaneously than there are atoms in the known universe[2]. Major advancements are expected to be observed in medical cancer

---

[1] Director Cyber Force Development (D Cyber FD), Quantum computing primer, *"Quantum Computing Advantages"*, September 2017.

[2] MIT Technology Review, "Serious quantum computers are finally here. What are we going to do with them?*"* last accessed 10 October 2018, https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/.

treatments, artificial intelligence development, weather forecasting and climate change predictions.[3]

4. QC is expected to mature within the next 10 to 20 years[4]. China has dedicated $15 billion over the next five years pursuing QC research. Also, China is the first known state who deployed a satellite capable of quantum key distribution encryption[5]. In contrast, the U.S Department of Defence announced a $200 million yearly budget on quantum research[6], and Department of National Defence (DND) recently announced $2.7 million to use QC to study surveillance challenges in the Arctic[7]. Companies, like IBM and Google are leading the development of QC. In March 2018, Google unveiled a new QC chip capable of almost achieving quantum supremacy, the point where calculations can be done faster than today's fastest supercomputer.[8]

5. The large processing power of QC also brings the capacity to rapidly break encryption algorithms that were once thought unbreakable.[9] Medical records, legal proceedings, financial records and state secrets are at risks. Given that the CA heavily relies on the stealth provided by cryptography to achieve operational advantages, this threat must be taken seriously today. Land

---

[3] Forbes, "6 Practical Examples Of How Quantum Computing Will Change Our World**,"** last modified 10 July 2017, https://www.forbes.com/sites/bernardmarr/2017/07/10/6-practical-examples-of-how-quantum-computing-will-change-our-world/#50b8a48780c1.

[4] Communication Security Establishment, "Quantum Computing Security Issues For Public Key Cryptography," last modified May 2017, https://www.cse-cst.gc.ca/en/node/2088/html/27673.

[5] Spacenews, "Pentagon sees quantum computing as key weapon for war in space," last modified 15 July 2018, https://spacenews.com/pentagon-sees-quantum-computing-as-key-weapon-for-war-in-space/.

[6] Meritalk, "Can DoD Take the Point on Quantum Computing?" Last modified 13 June 2018, https://www.meritalk.com/articles/can-dod-take-the-point-on-quantum-computing/.

[7] University of Waterloo - Institute for Quantum Computing, "Government of Canada announces contract award to the University of Waterloo for research and development in support of Arctic surveillance," Last modified 12 April 2018, *https://uwaterloo.ca/institute-for-quantum-computing/news/government-canada-announces-contract-award-university.*

[8]MIT Technology Review, "Google thinks it's close to "quantum supremacy," Here's what that really means," last modified 9 March 2018, https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/.

[9]Andy Majot and Roman Yampolskiy, *Global catastrophic risk and security implications of quantum computers* (Elsevier Ltd, 2015), 1.

Command Support System (LCSS) and Combat Net Radio (CNR) are potentially at risk of being partially and maybe completely exposed in future conflicts. Critical sensitive information could be read by adversaries the same way the Allied forces did with the solving of the German Enigma code.[10]

DISCUSSION

Threat

6. QC will facilitate electronic *back-traffic* attacks and *man-in-the-middle* attacks for cyber and signal intelligence forces. For *back-traffic* attacks, assuming that security agencies around the world are already intercepting and storing encrypted traffic, QC will provide them the ability to decrypt it while it is still considered classified. Canadian Security Establishment (CSE), the leader for cryptography in Canada, advised that sensitive information with lifespan of 10 years or more is already at risk.[11] At the same time, *man-in-the-middle* attacks could temper with classified IS information affecting the integrity and authenticity of transmitted.[12] Command and Control (C2) systems could be deceived and influenced with altered information in real time.

Vulnerabilities with today's encryption

7. The emergence of the QC threat has created significant vulnerabilities with current cryptographic algorithms and their respective keys. While these algorithms will be the main target for adversaries, the entire crypto chain can be thought of the armor surrounding these algorithms. If not secured, management of key generation and distribution, storage and fill

[10] Wired, "Quantum computing is the next big security risk," last accessed 10 Octobre 2018, https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/.
[11] Communication Security Establishment, "Quantum Computing Security Issues For Public Key Cryptography," last modified May 2017, https://www.cse-cst.gc.ca/en/node/2088/html/27673.
[12]Neil B. Barnas, "Blockchains in National Defense: Trustworthy systems in a trustless world," (U.S.A: Blue Horizons Fellowship Air University, 2016), http://www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/barnas_n.pdf?ver=2017-12-29-142140-393, 11.

devices, End Cryptographic Units (ECU) and radio systems with embedded crypto are all vulnerable targets.

8. Asymmetric encryption[13] algorithms are the backbone of the internet, financial and government networks. In the CA, asymmetric encryption is used to achieve important enabling tasks, such as disk encryption for confidentiality, digital integrity verifications and most importantly, symmetric algorithm key exchange. Shor's quantum algorithm, developed by Dr. Peter Shor, will render most of today's asymmetric encryption algorithms, including the main one such as the Rivest, Shamir, Adleman (RSA) and the Elliptic Curve Cryptography (ECC) algorithms, obsolete[14]. As a temporary solution to this threat, National Security Agency (NSA) urged the global security community to upgrade algorithm key sizes. However permanent mitigation of the threat posed by Shor's algorithm is unknown at this time[15].

9. Symmetric encryption[16] algorithms are also at the risk of being exposed by the QC threat. Grover's quantum algorithm will exponentially reduce the computational hardness of symmetric encryption, making most commercial algorithms vulnerable[17]. The CA heavily relies on symmetric encryption to deploy classified networks. Fortunately, for the majority of its networks, the CA is privileged to use NSA certified Type 1, non-commercial, cryptographic products which are more resistant to QC than commercial products, but nevertheless not immune

---

[13] Asymmetric Encryption or Public Key Encryption is a cryptosystem where the encrypting and the decrypting keys are different and it is computationally infeasible with conventional computers to calculate one from the other, given the encrypting algorithm, In public key cryptography, the encrypting key is made public but the decrypting key is kept secret - Certified Information System Security CBK, fourth edition, (ISC)2.

[14] Andy Majot and Roman Yampolskiy, *Global catastrophic risk and security implications of quantum computers* (Elsevier Ltd, 2015), 1.

[15] Key size refers to the sequence of bits that are used as instructions that govern the act of cryptographic functions within an algorithm. The larger the key size, the harder it is for a computer to find the solutions. In cryptography, algorithms are often public and known to all while the key is kept secret - - Certified Information System Security CBK, fourth edition, (ISC)2.

[16] Symmetric algorithms is an encryption method where the sender and the receiver use an instance of the same key for encryption and decryption purpose - Certified Information System Security CBK, fourth edition, (ISC)2.

[17] Ibid, Director Cyber Force Development (D Cyber FD), 2017.

in the future. For the remainder, the CA uses commercial encryption. The NSA urged - as a minimum - to upgrade to Advanced Encryption System 256 bits for national security system up to Top Secret– currently understood as quantum resistant[18]. For example, the CA's new Integrated Soldier System uses that encryption.

10. For communications security (COMSEC) in the CA, the challenge is to securely distribute keys across the battlefield. "*In information security often the weakest link is not the transmission of encrypted data, but rather security breaches at the end points where the data is no longer encrypted.*"[19] To protect the confidentiality and integrity of these keys, COMSEC relies on robust equipment and rigid chain of custody procedures. Facing a QC threat, COMSEC must be properly safeguarded. At the center of it, key management and distribution centers must be able to process approved algorithms and produce sufficient key lengths, and must be updated with appropriate secure connections to exchange keys. Consequently, portable crypto storage and fill devices must be digitized and upgraded to process larger encryption keys. ECUs and communications with embedded crypto modules, such as tactical radios, must also be upgraded to the newer validated products. Upgrades of this magnitude represent significant efforts and resources and address so much more than simply complying with new algorithms.

Current Solution: the Defence Cryptography Modernization Project (DCMP)

11. The DCMP omnibus was created in 2005 to replace the CAF aging secure communication systems and to maintain connectivity with our coalition partners. It is scheduled

[18] Information Assurance Directorate National Security Agency, "Commercial National Security Algorithm Suite and Quantum Computing FAQ", last modified 15 January 2018, https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

[19] Nature Communications, "Quantum computing on encrypted data," last modified 21 January 2014, https://www.nature.com/articles/ncomms4074.

for final delivery in 2022.[20] Containing several sub-projects, DCMP is championed by CSE and most importantly synchronized with the U.S.A. NSA equivalent project. The following are the key deliveries programmed under DCMP.

12. First, the CAF key management and distribution system will be upgraded. All Land Force Crypto Distribution Authority (LFCDA) within the CA with be automated with reliable key management systems.[21] Fill and storage devices will also be replaced.[22]

Second, ECUs will also be upgraded under the Advanced Crypto Capability Project which will implement U.S directed software upgrades to address quantum threat vulnerabilities, to minimize in-service support, and to maintain interoperability with allies.[23] Third, radios with embedded crypto will be upgraded. The Secure Radio Modernization (SRM) project is replacing legacy radios with the CNR Enhanced radio, the 117G manpack and the 152A handheld radio.[24] In addition, the Secure Command and Control Mobile Device project will replace the secure Iridiums and the Sectera satellite phones.

13. Overall, DMCP currently impacts the CA with the replacement of tactical radios, ECU, and changes to the key distribution systems. Without a doubt, longer algorithm key lengths and upgraded crypto equipment will better position the CA to counter these emerging threats. The CA should continue to embrace DCMP changes - the only current solution vector in motion within the CAF.

---

[20] Government of Canada, "Defence Cryptographic Modernization Project (DCPM) - Omnibus," last modified 30 May 2018, http://dgpaapp.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=1704, and National Defence, *National Defence Departmental Performance Report*, 31 March 2005, 83.

[21] Government of Canada, "Canadian Cryptographic Modernization Program (CCMP) Classified Security Management Infrastructure (CSMI)", last modified 30 May 2018, http://dgpaapp.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=1742.

[22] Business Case Analysis Brief, *Advanced Cryptographic Capabilities Project Increment 1* (Ottawa: Director Cyber Force Development, 2017)

[23] *Ibid*.

[24] Synopsis Sheet to Deputy Commander Canadian Army Update, *Cryptographic Capability Program, Presentation to Programme Management Board (*Ottawa: DLCI, 2018), 1.

14. Post-quantum algorithms are by design completely resistant to QC threat and compatible with current asymmetric cryptosystems. Some scientists argue that upgrading the key size of current algorithms is perhaps less urgent than transitioning from current existing cryptosystems to post-quantum cryptosystems[25]. However, post-quantum algorithms are in early development phase and the National Institute of Standard Technology recommends more research is needed before they could be recommended for use today.[26]

Strategic, Operational and Tactical considerations in light of the QC threat

15. For the CA, DCMP addresses the technological changes necessary to protect IS against early iterations of the QC threat. However, as new algorithms are created and QC improves, the CAF will be required to adjust its posture by updating algorithms and equipment within the crypto chain. While these are necessary, they are driven by other departments, such as CSE, and the CA will be somewhat reactionary these changes. However, organizational and procedural changes within the CA could create a better posture to face this threat.

16. At the strategic level, the CA could benefit from a centralized COMSEC office. The CA is responsible for the key management, distribution, and the overall compliance to current cryptographic standards for CA systems. Current management is the responsibility of the Formation COMSEC Authority (FCA) within Army G6. However, future operations and plans relating to cryptography, such as DCMP implementation or assessments of new capabilities, are not formalized and often handled by a mixture of organizations, like FCA, CA IS Security Officer, Director of Land Requirements or Capability Development. No one within the CA is officially responsible for these incoming issues. This is mainly due to cryptographic authorities

[25] National Institute of Standards and Technology, "Report on Post-Quantum Cryptography," last modified April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf,6.
[26] *Ibid*.

residing outside of the CA, and the fact that the CA has operated in a cryptographically uncontested environments in the last decades. However, the argument can be made that in the face of such a paradigm shift, the CA must become attentive to the evolution of the QC threat, the safeguards and the risks associated with our vulnerabilities. An office with these responsibilities would be beneficial within the CA.

17. However, changes to the current policy within the CA would not be recommended. CA crypto policy heavily relies on National rules and leaves little flexibility for the distribution, use and destruction of crypto material. The COMSEC chain of custody is separate from the chain of command, and is subject to inspections without notice. Although confining, the current policy ensures compliance with NSA standards which in turn allows NSA products to be available to the CA. Changes to the current crypto policy would not be recommended as it provides the necessary robustness required to face QC threats.

18. For the operational level, there are three important considerations: (1) Interoperability with Five Eyes (FVEY) partners; (2) interoperability with non-FVEYs, and (3) large extended networks for classified systems. First, the CA must remain interoperable with its FVEYs allies when it comes to network and systems compatibility. The use of approved algorithms and certified equipment will allow the CA classified systems to remain interoperable.[27] Second, key distribution with non-FVEY partners will become increasingly difficult as disparity between cryptographic products will prevent sharing of information. Many non-FVEY partners adopted low assurance crypto systems, such as type-2 commercial, as opposed to the more controlled and often restricted high assurance NSA certified type-1 crypto solutions. As a result, deployed lead nations will be unable to distribute high assurance crypto across their entire task force, and will

[27] Synopsis Sheet to CA COS Strat, *Advanced Cryptographic Capabilities Project (*Ottawa: DLCI, 2017), 1.

be forced to use less desirable technological information gateway solutions to achieve interoperability. Lastly, the use of large extended networks for operational systems has increased significantly. While they offer connectivity from strategic to tactical, they could easily be intercepted along the way by adversaries, stored for later decryption. Therefore, the CA should enhance monitoring of these systems and maximize the use of its integral links as both attack vectors, previously discussed, are likely to occur on these large scale systems.

19. At the tactical level, the upgrades to current algorithms and arrival of equipment will have minimal impact. On the one hand, more frequent updates to equipment are expected as QC safeguards become known. Power consumption and bandwidth requirement will slightly increase to adjust for the processing required for larger keys.[28] On the other hand, size and weight will not be affected by radios and ECU updates. Key distribution in the battlefield will be streamlined as electronic transfers are going to be favored vice manual transfers.

20. The probability of signal interception at the tactical level is higher due to radio communications and the proximity to the enemy. Fortunately, tactical information typically has a shorter intelligence lifespan. Efforts and time required to decrypt such signals will be greater than the amount of time the information remains relevant, making back-traffic attacks less probable, but man in the middle attack would still be possible. For example, the new Integrated Soldier System could be in similar situations. In addition, the tactical domain connects with the operational domain on LCSS. Critical information with longer intelligence lifespan, such as operational, targeting or intelligence plans, are available and run the risk of being intercepted. Secret information at the tactical and operational level have different lifespans, and therefore

[28]National Institute of Standards and Technology, "Report on Post-Quantum Cryptography," last modified April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf,4.

should be protected differently. Procedural gateways and greater awareness at the staff level are possible solutions for this problem and should be investigated further.

21. Lastly, tactical forces should train to better react to facing QC threats. The CA will arguably face more cryptographically contested environments in future conflicts with the rise of QC and the emergence of the cyber domain. CA Force Generation activities recently adopted *communication denied* scenarios where forces must rely on secure secondary and contingency communication means. *Crypto contested or denied* environment scenarios would pressure tactical forces to increase the use of voice procedure as a mean to protect confidentiality, to enhance electronic protection against information integrity breach and other innovative solutions.

CONCLUSION

22. QC technology will bring many positive developments in science and governments. However, their computational power will render important portions of current military encryption obsolete, and methods to exploit it, such as back-traffic and man-in-the-middle, already exists. DCMP will bring many changes needed to the CA to survive first contacts with QC enabled state actors. Nevertheless, DCMP is not the final solution to counter this threat, but more of a first line of defence. As the search for post quantum algorithm continues, the CA must embrace these changes and become a proactive member able to swiftly react to this threat.

23. At the tactical level, where the CA arguably operates the most, the upgrades to current algorithms and arrival of new technology should be transparent to the user. Equipment characteristics will remain relatively similar to today. In addition, the information intelligence lifespan at the tactical level will minimize the QC threat, but necessary controls need to be established to ensure classified information with longer lifespan is protected. Tactical force

could also benefit from training in cryptographic denied environments. At the operational level, crypto modernization is essential for the maintenance of interoperability, but will create significant challenges with non-FVEY partners. Large extended networks, such as LCSS, should maximize military dedicated links and being constantly monitored. At the strategic level, the CA would benefit from restructuring itself to plan and adapt for the cryptographic problems of tomorrow.

24. Finally, the CA is well supported by DND and the CAF to protect itself against the emerging QC threat. Although this threat is often seen as a future problem, it shows the vulnerability of today's information exchanges with a long intelligence lifespan. Our communications must be safeguarded to the value of the information we place on them. Mitigating measures for the short term will need to be immediately adopted while a refresh of the complete cryptographic suite of equipment becomes a necessity.

BIBLIOGRAPHY

Barnas, Neil. "Blockchains in National Defense: Trustworthy systems in a trustless world." (U.S.A: Blue Horizons Fellowship Air University, 2016), http://www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/barnas_n.pdf ?ver=2017-12-29-142140-393, 11.

Business Case Analysis Brief. *Advanced Cryptographic Capabilities Project Increment 1* (Ottawa: Director Cyber Force Development, 2017)

Communication Security Establishment. "Quantum Computing Security Issues For Public Key Cryptography." Last modified May 2017. https://www.cse-cst.gc.ca/en/node/2088/html/27673.

Director Cyber Force Development (D Cyber FD). *"*Quantum computing primer, Quantum Computing Advantages (Ottawa: Director Cyber Force Development, September 2017).

Forbes. "6 Practical Examples Of How Quantum Computing Will Change Our World." Last modified 10 July 2017. https://www.forbes.com/sites/bernardmarr/2017/07/10/6-practical-examples-of-how-quantum-computing-will-change-our-world/#50b8a48780c1.

Government of Canada. "Defence Cryptographic Modernization Project (DCPM) – Omnibus." Last modified 30 May 2018. http://dgpaapp.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=1704

Government of Canada, "Canadian Cryptographic Modernization Program (CCMP) Classified Security Management Infrastructure (CSMI)." Last modified 30 May 2018. http://dgpaapp.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=1742.

Information Assurance Directorate National Security Agency. "Commercial National Security Algorithm Suite and Quantum Computing FAQ." Last modified 15 January 2018. https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

Meritalk. "Can DoD Take the Point on Quantum Computing?" Last modified 13 June 2018. https://www.meritalk.com/articles/can-dod-take-the-point-on-quantum-computing/.

Majot, Andy. Yampolskiy Roman. "Global catastrophic risk and security implications of quantum computers.*"* (Elsevier Ltd, 2015), 1.

MIT Technology Review. "Serious quantum computers are finally here. What are we going to do with them?" Last accessed 10 Octobre 2018. https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/.

National Defence. *National Defence Departmental Performance Report*. (Ottawa. 31 March 2005), 83.

Nature Communications. “Quantum computing on encrypted data.” Last modified 21 January 2014. https://www.nature.com/articles/ncomms4074.

National Institute of Standards and Technology. “Report on Post-Quantum Cryptography.” Last modified April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf,4.

Spacenews. “Pentagon sees quantum computing as key weapon for war in space.” Last modified 15 July 2018. https://spacenews.com/pentagon-sees-quantum-computing-as-key-weapon-for-war-in-space/.

Synopsis Sheet to Deputy Commander Canadian Army Update, *Cryptographic Capability Program, Presentation to Programme Management Board (*Ottawa: DLCI, 2018), 1.

Synopsis Sheet to Chief of Staff Strategy Canadian Army. *Advanced Cryptographic Capabilities Project (*Ottawa: DLCI, 2017), 1.

University of Waterloo - Institute for Quantum Computing. “Government of Canada announces contract award to the University of Waterloo for research and development in support of Arctic surveillance,” *Last modified 12 April 2018.* https://uwaterloo.ca/institute-for-quantum-computing/news/government-canada-announces-contract-award-university.

Wired. “Quantum computing is the next big security risk.” Last accessed 10 October 2018. https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/.