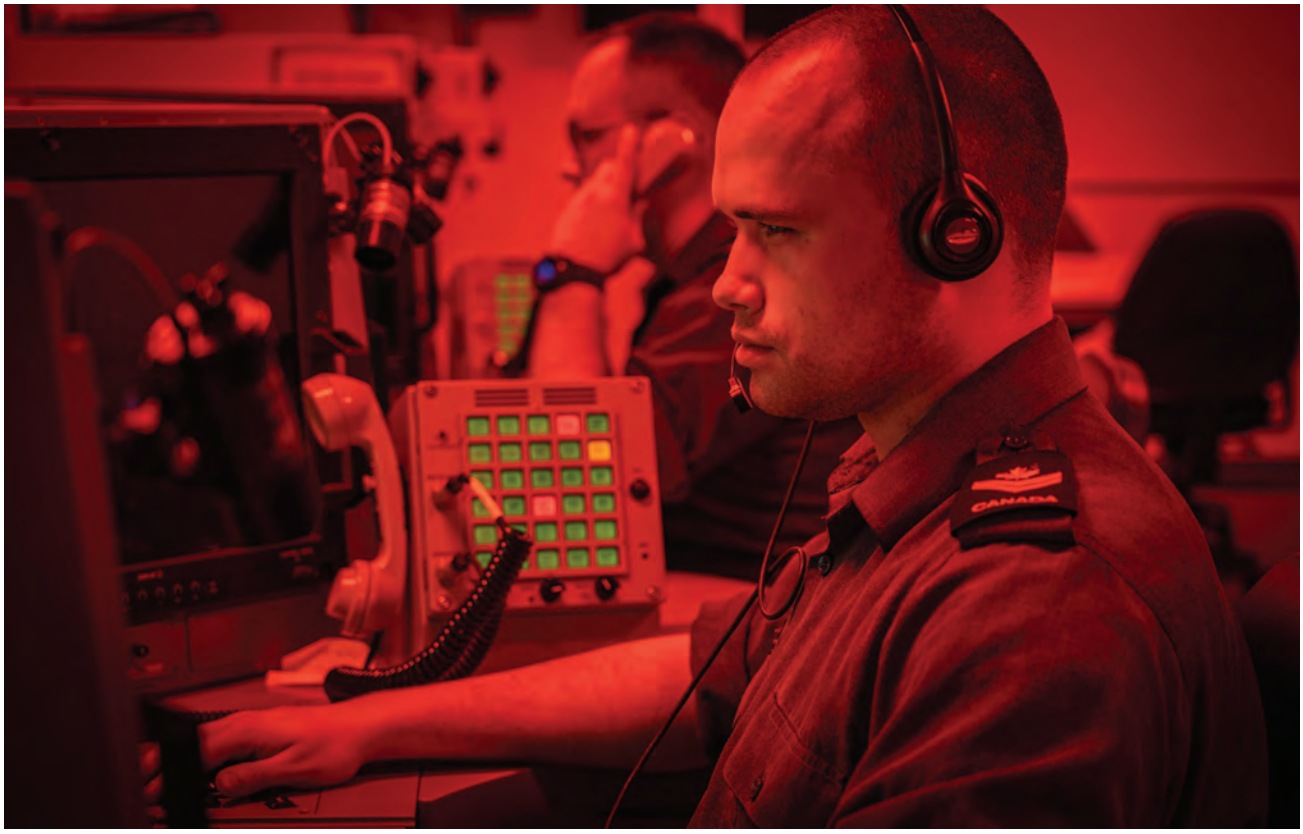

This photo has been digitally altered due to operational security. A sailor monitors their computer as HMCS HARRY DEWOLF sails the Atlantic Ocean during Operation CARIBBE on April 14, 2022.

Photo: Canadian Armed Forces photo

Quantum Technologies in Defence and Intelligence Security

BESSMA MOMANI AND MICHELE MOSCA

Bessma Momani is Associate Vice-President, International and Full Professor in the Department of Political Science at the University of Waterloo. She is also a senior fellow at the Centre for International Governance Innovation and a Fulbright Scholar. She is a Governor on the board of the International Development Research Centre.

Michele Mosca is co-founder of the Institute for Quantum Computing at the University of Waterloo, a Professor in the Department of Combinatorics & Optimization of the Faculty of Mathematics, and a founding member of Waterloo's Perimeter Institute for Theoretical Physics. He was the founding Director of CryptoWorks21, a training program in quantum-safe cryptography. He co-founded evolutionQ Inc. to support organizations as they evolve their quantum-vulnerable systems to quantum-safe ones and softwareQ Inc. to provide quantum software tools and services.

The impact of quantum technology on intelligence gathering for defence and security operations may become significant, but it is imperative to be prepared and not reactionary. As a dual-use technology, quantum technologies can be used for both good and harm and for civilian and military uses. We take an agnostic view of this technology while arguing that we may be at the cusp of a technological breakthrough that will expose tour vulnerabilities in protecting sensitive information and grant adversary's new military capabilities. Moreover, this could apply to

adversaries that are both states and, eventually, when the technology is more diffused and commercialized by non-state actors, including criminal and political terrorist groups. The latter threat will come in the long term since the quantum capability is still relatively expensive to acquire and concentrate in state institutions and select multinational commercial entities. One partial exception is quantum computation, where access to the device (versus possession) suffices for threat actors so that the time lag may be much less. That said, policymakers must invest in this critical area to proactively address disruptive shifts resulting from quantum's transformative capabilities. This article explains quantum technology's potential defence and security implications while emphasizing the policy imperative of investing in and supporting this Canadian industry. Canada's National Quantum Strategy is a positive step, and its full implementation is necessary to see this strategy come to fruition and benefit a burgeoning industry that can have a positive spillover to Canadians' overall wealth and prosperity.

The quantum threat to our digital systems is impending and requires urgent policy attention. While the timeline of the threat is unknown, key milestones continue to be achieved, and policymakers must invest in research, development, and deployment to ensure we keep our comparative advantage in this space and thwart and/or mitigate quantum-related attacks. Although many quantum technology applications have lower Technology Readiness Levels or Solutions Readiness Levels, the scientific knowledge and direction of these applications are becoming more transparent and more diffuse, and there is a national security and national prosperity imperative to have Canada remain a strong player in the global quantum race, which is intensifying.

Throughout this article, we review open-source documents and studies on the potential application of quantum technologies to national defence and security, focusing on intelligence gathering. Each author has expertise in quantum science, cryptography, international affairs, cybersecurity, geopolitics, and defence and security studies. Where possible, we have embedded links to related academic and news items.

This article discusses the application of quantum computing, quantum communication/networks, and quantum sensing to intelligence gathering, analysis and dissemination. These three areas of quantum science are the most salient to our discussion of applying quantum technologies to the defence and security space. In layperson's terms, the latest evolution in quantum technologie—often called the second quantum revolution or Quantum 2.0—will enhance many aspects of the digital world, making processes faster, measurements more precise, and data processing more potent than current technologies and previous generations of quantum technologies. Importantly, this second wave of the quantum revolution will not necessarily bring new types of instruments or weapons, but it will significantly enhance existing ones, enhancing overall capabilities[1]

Within Canada, Vancouver, Calgary, Sherbrooke, Toronto and the region of Waterloo are home to a critical mass of Canada's intellectual power and start-ups behind quantum technology.[2] Yet, we are losing ground to competitors in countries like China and the United States, who outspend, out-invest, and outsmart Canada in quantum technology's research, application, and commercialization.[3] This article reviews the technological landscape and its application to defence and security, focusing on intelligence gathering and analysis. However, the rapid pace of technological change cannot be overstated. The National Quantum Strategy to help Canada compete offers a promising initiative to advance the country's quantum capabilities, but its full implementation requires considerably more investments in research, talent development, and industry commercialization to help Canada be globally competitive in this critical sector.[4]

In the final section of this article, we aim to provide some policy rather than technical recommendations on how Canada can better navigate and address the challenges and opportunities arising from emerging quantum technologies. There is still time to maintain our important place in this field, particularly in the areas where Canada has had a global lead for some time, such as quantum computer algorithms and applications, quantum-safe cybersecurity, and certain types of quantum sensing.[5]

1. What is Quantum?

This section begins with a fundamental review of what quantum is before delving into its application to intelligence gathering, analysis and dissemination, and its risks and benefits. We first give an overview of how quantum impacts three main areas of technology, and in the next section, we elaborate on the defence and security implications. To begin with, quantum mechanics is a fundamental theory that has enabled physicists to resolve challenging problems and paradoxes in understanding various physical phenomena. Quantum technologies are the realization of applications that depend on quantum effects. Built upon quantum mechanics, quantum information theory provides the basis for quantum computing and other quantum information processing technologies. A key feature of this framework is the ability to describe a physical system's state as occupying two or more distinguishable configurations "simultaneously," also known as superposition. For example, a single electron may occupy multiple energy levels of an atom at once, and a single photon may simultaneously traverse multiple paths.

Quantum rules are a fundamental theory of physics that impacts what is possible. For example, quantum rules determine

whether codes are breakable and how precisely we can measure an object.

One implication of quantum is for computation. Computers store information in physical bits with two distinguishable states labelled 0 and 1. Quantum physics implies that a complete description of a single bit of information requires two complex numbers to represent the amplitudes of 0 and 1 states, whereas describing n qubits requires representing 2^n complex numbers representing the amplitudes of all 2^n possible configurations. The only known method for a classical computer to simulate n quantum bits is to track these 2^n amplitudes. For even a few hundred qubits, the storage demands would exceed all the matter in the known universe. This observation highlights the potential of quantum computers to solve problems that would take exponentially more classical resources.

Another implication of quantum is for sensing. The quantum framework implies that an outcome detectable with probability p exists with quantum probability amplitude proportional to $\sqrt{p}$, which is greater than p if p is less than one (with 0 = 0% and 1 = 100%). Quantum sensors manipulate objects at the quantum level, allowing for detection with a sample of size N instead of size N^2, or with N probe signals instead of N^2 probe signals. Furthermore, some advanced instruments developed for quantum technologies can also enhance classical sensing and measurement applications.

The third family of applications impacted by quantum is communication. Quantum technology is transforming communication networks and the digital security landscape. For example, the additional complexity intrinsic to quantum bits implies that any eavesdropping, that is, any extraction of information about the quantum bits, leads to a measurable disturbance proportionate to the amount of information extracted. This foundational quantum property opens the door to new tools for protecting information, including quantum key distribution (which we elaborate on later).

Quantum communication networks can enable distributed quantum computations, sometimes with much less communication between the different computers in the network. Quantum linking of quantum computers enables enhanced quantum computing power. They also enable quantumly correlated quantum sensing, combining information from different sensors in different locations to reconstruct potentially better images. Quantumly correlated quantum sensors, using a quantum network, can similarly enable a sensing or measurement capability beyond what would be possible with only classical communication networks connecting the sensors.

The timing and impact of the potential of quantum technologies depend on several factors. These factors include, for example, achieving technological advances that enable less noisy and faster fundamental operations, such as the conversion of quantum information between photons, which are effective for moving information, and other qubits, which are more effective for multi-qubit operations or storage, and on the development of improved methods for leveraging imperfect quantum operations. Lastly, the timing and impact will also depend on the amount of effort and focus dedicated to the different challenges and opportunities.

2. Quantum Applications

We have noted three areas of application of quantum technology that are likely to interest the defence and security community: quantum communication/networks, quantum computing, and quantum sensing. In this section, we also discuss the implications of quantum technology for the work of defence and security policymakers, practitioners, and military personnel.

a. Quantum Communication/Networks

Modern communication networks are essential to global society. Quantum technology will enhance and revolutionize communication channels and networks that underpin our interconnected devices. As devices become more digitally enabled and interconnected, they become highly reliant on safe and secure forms of communication.

Emerging quantum technologies will impact the intercommunication of planes, ships, vehicles, personnel, and command centres in defence and security. While there is enthusiasm about improving these networks, the risk of adversaries intercepting communications and deciphering them with new quantum capabilities increases. Secure and reliable communications are vital for military operations and intelligence sharing and could be compromised if not quantum-proofed with new cryptography designed to thwart quantum-enabled attacks.

Quantum computation can expose intelligence and data currently encrypted on classical computers and digital infrastructure. Conventional secure communication networks will become more vulnerable to quantum technology, but advancements in cryptography and quantum networks offer opportunities to bolster communication networks' security and privacy. Secure communication systems are essential for a robust economy. Quantum-safe cryptograph, designed to counter quantum-enabled attacks, includes classical algorithms (called post-quantum cryptography).[6] In addition, quantum key exchange/distribution (QKD) is a type of cryptography that can protect digital communications and is not susceptible to quantum or classical code-breaking. QKD technology has been commercially available for years and used by some governments and private entities. Ongoing standardization, certification, performance improvements, and more extensive network deployments will facilitate broader deployment.

It is still premature to suggest that this communication technology is the precursor to a quantum internet. Still, with advancements in satellite communication and the communication of quantum nodes, which are evolving rapidly, there is optimism that these scientific discoveries could move us closer

to achieving the various capabilities that reliable long-distance networks would enable.

b. Quantum computing

Quantum computers will be able to solve specific problems with astronomically fewer steps and thus be much faster than classical computers. For example, breaking today's public-key cryptography using classical computers requires exponentially more time compared to quantum computers. In 2020, Chinese researchers used the Jiuzhang quantum computer to solve a mathematical problem in under 5 minutes, a task that would take a classical computer 2.5 billion years.[7] Notably, this followed Google's 2019 claim of quantum supremacy with its Sycamore processor. While Noisy Intermediate Scale Quantum (NISQ) devices don't fully leverage quantum mechanics' computational power, these experiments validated that sufficiently large and well-controlled quantum computing systems cannot be practically simulated by classical computing platforms using the best-known algorithms. Researchers are exploring practical applications of NISQ computers by examining real-world computational challenges through NISQ computing capabilities. The only known way to capture all the computational capabilities of quantum computers is by using fault-tolerant quantum error correction, which minimizes errors and noise, similar to classical error correcting codes used in classical computing and communication systems to enable reliable communication and computation in the presence of errors.

Quantum computers' computational power threatens current public-key cryptography, potentially exposing encrypted intelligence data if access to the encryption keys is protected by public-key cryptography. This risk is heightened for data communicated today or in the past using public-key cryptography for session keys. It is worth emphasizing that malicious actors may have already intercepted and stored encrypted data, where the keys were shared with public-key cryptography, awaiting computing abilities to decrypt it.

Today's threat models may underestimate the risk of data encrypted with public-key cryptography, as it is viewed as inaccessible without quantum computing or irrelevant until advanced AI reveals new patterns. However, adversaries may have already conducted such offensive hacking operations, and security breaches may not be exposed in the future. Therefore, it's crucial to quantum-proof sensitive and classified information today, as data protected by Suite B or similar algorithms may have already been siphoned off to be unlocked by future quantum cryptanalysis.

Protecting intelligence gathered and state secrets will take years to prepare, and quantum-proofing intelligence data is imperative to national security and defence. The Department of National Defence should inventory sensitive data, assess risk tolerance, and develop a strategy for moving to quantum-safe cryptography through its technology lifecycle management processes. In support of this migration, quantum communication

"In 2020, Chinese researchers used the Jiuzhang quantum computer to solve a mathematical problem in under 5 minutes, a task that would take a classical computer 2.5 billion years."

enables a key exchange that is not susceptible to algorithmic cryptanalysis (quantum key distribution, QKD). QKD can be integrated into the suite of solutions, including pre-shared keys, to provide resilience against unexpected cryptanalytic advances.

Beyond breaking codes faster than any known classical method, quantum computing could more efficiently address other computational challenges, making possible improved predictive analytics with machine learning and artificial intelligence. This capability may enable pre-emptive actions by anticipating adversaries' moves based on previous battlefield plans, improving target accuracy, and limiting collateral damage.

Among the more futuristic predictions is the issue of cognitive warfare powered by quantum computing as society expands its digital footprint and puts more information about its thought processes and decision-making on digital devices. Quantum computing advancements may facilitate the manipulation of leaders and societies by identifying behaviour patterns through advanced machine learning and artificial intelligence. Indeed, social media is an integral part of this mass societal digital footprint collection; hence, we already see significant commercial interest in understanding human behaviour. This will only accelerate with advances in quantum computing. Moreover, as open and Western societies with increased public expectations for government transparency, we contribute to our adversaries' increased understanding of our societies. The same cannot be said for them, as their digital authoritarian tendencies have meant less contribution to the virtual public space. Moreover, polarization within Western democracies exposes internal weaknesses, providing opportunities for adversaries to find fault lines to disturb cognitive warfare.[8] Calls to improve our awareness of the risks of Cognitive Warfare need to be heeded.[9]

c. Quantum Sensing

Quantum sensing and metrology will also transform the collection and analysis of intelligence. Quantum sensing may enhance our ability to measure temperature, acceleration, time, and gravity. It could improve instruments used to detect and measure objects and movement, potentially enabling precise mapping and situational awareness in positioning and navigation. Quantum

sensors may be used to improve intelligence gathering and surveillance on the movement of individuals, camouflaged vehicles, and objects behind walls and around corners. It may also detect movement in bunkers, tunnels, or caves below the Earth's surface. However, some potential applications are speculative and still face challenges like high sensitivity and data processing issues in unclear environments.

Quantum sensors will also significantly advance the application of quantum metrology to low-brightness or night-time situations, enhancing military intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) capabilities on a multi-domain battlefield. Advancements in quantum sensing are already in use and commercially available in atomic clocks and gravimeters. However, some challenges remain, requiring extensive global research to overcome these limitations.[10]

Quantum sensors used for Position, Navigation, and Timing (PNT) may supplement or replace GPS, particularly where signals and reception fail. For example, significant excitement surrounds the potential of quantum sensing used in ocean depths as an odometer. Advances in quantum sensing could expose submarines and torpedoes previously undetectable at specific depths, potentially disrupting the balance of power and complicating detection.[11] Moreover, new territorial claims could accelerate with the application of quantum sensors and impact a race for claims to newfound territory. The South and North poles are areas to watch for new territorial claims partly attributable to multiple scientific advancements such as quantum sensing.

Increased underwater warfare may be observed with increased use of quantum sensors. Quantum magnetometers, such as those based on a superconducting quantum interference device (SQUID), could revolutionize the detection of materials and magnetic fields. Current dependence on sonar to detect submarines may give way to increased use of SQUID-based technology. Scientists have used an airborne device of multiple SQUIDs to identify buried metal balls.[12] Scientists have also referenced the possibility of using this to detect submarines several kilometres away, but this remains a speculative and potentially distant realization of this technology. The data analysis of the study is ongoing, and there are likely many difficulties in applying this in the field, let alone in a militarized setting. These instruments require significant cooling and miniaturization to be helpful in most moving platforms, for example, on an unmanned vehicle's reconnaissance mission. The short battery life of these drones continues to be a significant challenge in making them operable. These challenges have dampened expectations that SQUID-based magnetometers will be used in anti-submarine warfare.[13] Similar challenges exist with gravity gradiometers.

Quantum sensors can detect electromagnetic emissions, enhance military capabilities in locating adversarial forces, and improve electronic warfare. At the same time, military detection of electromagnetic emissions using quantum sensors could help thwart electronic warfare. Quantum antennas will also enhance electronic warfare systems to intercept low-frequency signals. In areas like signals and communications intelligence and counter-radar jamming, quantum technology may enhance intelligence collection, interception, and object identification. Additionally, quantum networks can better detect potential eavesdropping, especially in low-frequency ranges and dynamically switching bandwidths. As Krelina notes, "In the future, quantum antennas could look like an array (matrix) of Rydberg atom cells. Different cells can measure different signals, and in the joint measurement of two or more cells, the angle-of-arrival of the signal could be determined."[14] However, the same author notes that the cooling of these atoms poses challenges. Hence, the U.S. Defence Science Board has expressed skepticism about quantum radars significantly enhancing the Pentagon's radar capabilities in the near future.[15] In particular, ovenized crystal oscillators (OCXO), which maintain temperature and synchronize with GPS, are already incredibly accurate, small, and inexpensive, improving precision in location applications.

Turning to a quantum radar technique called quantum illumination, we may see more advanced detection of light that could lead to deciphering more delicate details of an identified object and could improve targeting on the battlefield. Quantum radars could improve detection and accuracy in harsh conditions such as space, fog, smoke, clouds, low light, night, and high temperatures, like wildfires.[16] Conventional radars are also more sensitive to geomagnetic storms and solar flares, which is particularly relevant for Canadian operations in the Arctic. Quantum radars could improve search and rescue missions and operations in difficult environments by emitting much less energy and offering 'stealth detection' where a target is much less likely to know it is being detected. That said, this use of quantum radar technique is still underdeveloped. There are many challenges with "…obstruction, cancellation calculations, and factual examination of unused space."[17] bistatic quantum radar cross-sections often exhibit sidelobe quantum effect, posing a persistent challenge in the scattering field.[18] This is a nascent development. Some argue a 'futuristic' view of potential applications of quantum radars that still needs significant research to find practical purposes.[19]

Hence, quantum radars are in the very early stages of application, mainly in laboratories with the lowest TRL. There have been some debated[20] and exaggerated claims of quantum radar usage and its application to the battlefield.[21] Austrian researchers in 2019 briefly claimed "quantum supremacy" in a laboratory demonstration of quantum radar, but the claim was quickly removed from the arXiv pre-print server after significant criticism. Engineers have debunked[22] claims that quantum radars can detect stealth aircraft.[23] Moreover, other researchers have posited that quantum radars only outperform conventional radars where signals are weak or background noise conditions are strong, limiting their application on the battlefield for the time being.[24]

Nonetheless, there is considerable interest in developing quantum radars for stealth aircraft detection and

low-probability-of-intercept applications, which could revolutionize battlefield dynamics. Great powers and the military industry are in a global race to produce this capability. Certainly, NORAD modernization and updating Canada's radar system are pressing procurement issues. For now, the readiness of this quantum radar technology in any update of the NORAD system is likely limited by engineering considerations.

3. Emerging Global Trends

This section examines recent developments in quantum capabilities globally, focusing on the competition among the global players in the quantum race, such as the US, China, the UK, Canada, and Europe.[25] Many of these global players have identified a national strategy on quantum to focus on research and development, building commercial ecosystems, advancing workforce talent, and technological independence.[26] As noted earlier, state-led investment in research and development and the military-industrial sector has led the way, except in Canada, where private-sector in quantum technology exceeds government investment.[27]

China has made significant investments and, therefore, has a likely lead in quantum communication. According to a CNAS paper, the Micius satellite's launch marked a significant milestone, leading to numerous 'megaprojects' in quantum communications.[28] Using their national civil-military integration strategy with great determination to be a science and technological superpower, China has invested heavily in its scientists and researchers, reducing dependence on foreign technology transfers—a shift partly driven by the Snowden revelations of the US spying on Chinese systems. The Chinese state has invested in quantum communication and computing, hoping that these advancements would protect them against foreign espionage and data mining on their systems.[29] Moreover, China's 2008 'Thousand Talents Plan' seeks to repatriate ethnic Chinese scientists working abroad, with nearly 60,000 professionals recruited so far, often through support to scientists' commercialization efforts, as noted by a US Senate report.[30]

Recognizing the international race for quantum supremacy and hence the potential foreign interference in Canadian researchers' capacity to advance quantum research and development, one can appreciate the existing Canadian government's concerns about advancing research and development in the quantum domain. Indeed, government research funding in this area now undergoes significant national security oversight, including added screening of funding applications. However, excessive national security controls could disincentivize international collaboration, particularly with leading Chinese researchers, potentially hindering Canada's progress in quantum technology. China is more assertive in acquiring foreign talent and intellectual property, including from Canada, with partial taxpayer subsidies, which invariably raises national security concerns.

An Australian think tank has been tracking Chinese universities engaged in military research to assist international universities in identifying partner institutions that could facilitate potential technology and research leakage to the Chinese state.[31] This has generated considerable unease in many universities and the Canadian government, fearing a leaky pipeline of talent and scientific knowledge to the advantage of China. That said, academic communities are considerably uneasy about excessive national security attention to universities and research when many scientists publish their research findings for the broader benefit of the quantum scientific community. Canada's tri-council funding agency and some provinces have grown more aware of this potential leakage, mandating a security review of grant applications. Ironically, researchers are concerned that these tri-council security reviews are pushing them to seek out more industry funding instead, which might lead to further leakage to countries like the US and parts of Europe. Moreover, researchers at RAND noted that as TRL of quantum computing and communications remains low, export controls might further slow scientific research and technological advancements.[32]

Both the US and the UK were viewed as leaders in quantum sensing. Significant DARPA investment in quantum technology is driving scientific progress in the US. US academic research has expanded with significant government investment, mainly through the National Quantum Initiative, which spent $710M in research and development in 2021 alone, increasing by 20% annually in recent years. According to RAND researchers, the US focuses on quantum computing and sensing, while China prioritizes quantum communication with quantum computing closely following.[33] The US' AUKUS agreement with Australia and the UK to advance military technologies has raised speculation that the US was outfitting Australian submarines with quantum sensing technology and advancing innovation in this technological area that might exclude Canada.[34]

4. Policy Recommendations

We outline recommended measures to prepare for and address challenges and opportunities arising from emerging quantum technologies while noting that DRDC has developed a quantum strategy for DND/CAF.[35] ISED has undertaken a consultative process to formulate an integrated National Quantum Strategy (NQS).[36] Quantum research is evolving rapidly, and Canada's DND/CAF must continue to involve the academic sector to overcome the many scientific challenges, many of which are engineering considerations that will turn the research into a deployable reality.[37] Budget allocation in 2021 to $360M over 7 years to a National Quantum Strategy is insufficient to keep existing quantum dominance and to catch up to peer competitors.

International collaboration with NATO allies on commercialization, research, and development is crucial for collective success and interoperability. That said, China is successfully attracting

A CAF member monitors the progress of firefighters during a fire exercise aboard HMCS HALIFAX during Operation REASSURANCE on January 14, 2021.

Photo: Sailor First Class Bryan Underwood, Canadian Armed Forces photo

and funding global researchers. The dual-use nature of quantum technology will naturally lead to commercial advances in quantum technology that DND/CAF can utilize. Continued investment by DND/CAF in researching quantum sensing and radars, particularly for submarine and stealth aircraft detection, is imperative for our national defence and Arctic surveillance.

Leveraging Canada's academic and SME strengths is vital to address scientific challenges. Given the competitive talent pool, this integrated approach across sectors is needed to maximize Canada's quantum technological developments. Therefore, we must develop a coherent program exploring quantum sensing, computing, and communications/networking for national defence and intelligence. This could imply we take inspiration from a DARPA/IARPA type model where the ultimate mission is to prevent strategy surprise, where IP ownership remains with researchers to foster commercial activity and support the Canadian quantum ecosystem, including projects of varying TRL. Part of the program can include education/training for DND/CAF personnel via secondments at universities and in industry while noting that this would also support SMEs that dominate this ecosystem.

We need to remember that the impact of quantum technology is more likely to be exponential and not linear; hence, we need an urgent investment. Canada cannot afford a "wait-and-see" approach, particularly in securing national intelligence. The impact of this technology can leap from "no known impact" to "transformative impact," as seen with public key cryptography between 1993 and 1994. Quantum computers did not even exist at the time. Once quantum computers appear, there will be no "time-out" to prepare for the security implications. Once the IP, in the form of knowledge and products, is in the hands of adversaries, we will not have an easy path to accessing the transformative quantum capabilities. We have to proactively bring the owners of the challenging problems together with the world-class experts in Canadian academia and industry to discover and develop the potential application areas of quantum technology.

In many cases, the conclusion will be that there is no known quantum advantage. This is not a failure but rather part of the scientific discovery process. It steers us away from less promising applications and toward more promising applications while advancing the expertise needed. Successes can be further developed in higher TRL projects.

We must also enhance the national defence and intelligence community's capacity to advance their understanding of potential quantum threats and opportunities through continuous training and education from academia and industry. The knowledge base on this technology is rather thin and relatively young. To ensure a continuous talent pool, Canada needs to nurture the young professionals working in this space, and provide a vibrant ecosystem in Canada that enables them to create value for Canada. Graduate student and post-doctoral funding are lacking in Canada, and many opt to leave to study elsewhere. Apart from competitive salaries, researchers require opportunities to work on impactful cutting-edge projects. Moreover, outside their labs and academic environments, graduate students, post-doctoral fellows, and early career researchers would also benefit from opportunities to network, share information, and collaborate with the defence and security policy community to solve some of the pressing national defence challenges discussed in this article.

Conclusion

Quantum information science and technology is a vast field with different elements at various stages of maturity and many pockets of expertise worldwide. The global players in the quantum race, primarily the United States, China, the United Kingdom, Canada, and Germany, have identified a national quantum strategy focussing on research and development, building commercial ecosystems, advancing workforce talent, and technological independence. Overall, the broadly held view is that North America is the overall leader in quantum computing technology (followed by China and then Europe), China is the overall leader in quantum communications (including its Micius satellite), and there is a strong concentration of leadership in quantum sensing (which is a much broader field) in the UK and North America.

Geopolitical tensions and concerns about potential scientific leakage to China are increasing pressure for export and other controls around quantum technologies. This is more relevant considering that state-led investment in research and development and the military-industrial sector have led the way. In protecting our scientific knowledge and technological capabilities, quantum poses some unique challenges. It is difficult to control a technology still in development whose implications are still being discovered, developed, and assessed. Premature or misdirected attempts at controlling will slow down and potentially undermine the developments. Yet, the implications of not having adequate controls may be unexpected and potentially exponential. Navigating these uncertain waters requires significant policy attention, funding, and commitment.

Notes

1 Krelina, M. Quantum technology for military applications. *EPJ Quantum Technol*. 8, 24 (2021). https://doi.org/10.1140/epjqt/s40507-021-00113-y

2 Government of Canada, Canadian Institute for Advanced Research, Natural Sciences and Engineering Research Council of Canada. "Seizing Canada's Quantum Opportunity: Report on the Quantum Canada Symposium and Workshop" April 11-12, 2017. :NR16-151/2017E-PDF - Government of Canada Publications - Publications.gc.ca, 2017. https://publications.gc.ca/site/eng/9.858243/publication.html.

3 Gaida, Jamie. "ASPI's Critical Technology Tracker." Aspi.org.au, 2023. https://www.aspi.org.au/report/critical-technology-tracker

4 Valigra, Lori. "Canada Lays the Groundwork to Become a Powerhouse in Quantum Technology." Science Business, June 23, 2022. https://sciencebusiness.net/news/quantum-computing/canada-lays-groundwork-become-powerhouse-quantum-technology.

5 Sussman, Ben, Paul Corkum, Alexandre Blais, David Cory, and Andrea Damascelli. "Quantum Canada." *Quantum Science and Technology* 4, no. 2 (February 22, 2019): 020503. https://doi.org/10.1088/2058-9565/ab029d.

6 Chen, Lily, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. "Report on Post-Quantum Cryptography." *Report on Post-Quantum Cryptography*, April 2016. https://doi.org/10.6028/nist.ir.8105.

7 Zhong, Han-Sen, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, et al. "Quantum Computational Advantage Using Photons." *Science* 370, no. 6523 (December 18, 2020): 1460–63. https://doi.org/10.1126/science.abe8770.

8 Orinx, Kimberly, and Tanguy. "China and Cognitive Warfare: Why Is the West Losing?" *Hal.science*, 2022, 8, 1–6. https://hal.science/hal-03635930.

9 Bernal, A., C. Carter, I. Singh, K. Cao, and O. Madreperla. "Fall 2020 Cognitive Warfare. An Attack on Truth and Thought." (2021). https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf

10 Geiger, Remi, Arnaud Landragin, Sébastien Merlet, and Franck Pereira Dos Santos. "High-accuracy inertial measurements with cold-atom sensors." *AVS Quantum Science 2*, no. 2 (2020). https://arxiv.org/pdf/2003.12516#page25

11 Congressional Research Service, *Defense Primer: Quantum Technology*, November 4, 2024, https://crsreports.congress.gov/product/pdf/IF/IF11836

12 Hambling, David. "China's Quantum Submarine Detector Could Seal South China Sea." New Scientist, August 22, 2017. https://www.newscientist.com/article/2144721-chinas-quantum-submarine-detector-could-seal-south-china-sea/.

13 Kubiak, Katarzyna. "Quantum Technology and Submarine Near-Invulnerability," European Leadership Network (ELN) *Global Security Policy Brief.* December (2020) https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/12/Quantum-report.pdf.

14 Krelina, Michal. "Quantum Technology for Military Applications." *EPJ Quantum Technology* 8, no. 1 (November 6, 2021). https://doi.org/10.1140/epjqt/s40507-021-00113-y.

15 Sayler, Kelley M. "Defense Primer: Quantum Technology." *Congressional Research Service (CRS) Reports and Issue Briefs* (2022):Updated November 24 (2024) https://crsreports.congress.gov/product/pdf/IF/IF11836#:~:text=Quantum%20sensors%20could%20also%20enable,electromagnetic%20emissions%2C%20thus%20enhancing%20electronic

16 Hasan Abbas Al-Moahmmed. "Quantum Radar: A Brief Analytical Study" 3 (December 29, 2020): 174–80. https://doi.org/10.1109/icenco49778.2020.9357379.

17 Kumar, Adarsh, Diego Augusto, Keshav Kaushik, and Joel J.P.C Rodrigues. "Futuristic View of the Internet of Quantum Drones: Review, Challenges and Research Agenda." *Vehicular Communications* 36 (May 16, 2022): 100487–87. https://doi.org/10.1016/j.vehcom.2022.100487.

18 *Ibid*.

19 *Ibid*.

20 Hill, Lieutenant-Commander Graham. "Quantum Radar Is Stealth Radar: Examining the Potential Impact on the Defence Team." JCSP 48 Service Paper (2022). https://www.cfc.forces.gc.ca/259/290/24/192/Hill.pdf

21 Mizokami, Kyle. "How Quantum Radar Could Completely Change Warfare." Popular Mechanics, August 26, 2019. https://www.popularmechanics.com/military/a28818232/quantum-radar/.

22 Vella, Heidi. "Could Quantum Radars Expose Stealth Planes?" Engineering and Technology Magazine, April 18, 2019. https://eandt.theiet.org/2019/04/18/could-quantum-radars-expose-stealth-planes.

23 Mizokami, Kyle. "China Claims It Developed 'Quantum' Radar to See Stealth Planes." Popular Mechanics, September 22, 2016. https://www.popularmechanics.com/military/research/a22996/china-quantum-stealth-radar/.

24 Hardy, Nicholas, Ben Dixon, Jeff Shapiro, and Scott Hamilton. "Quantum Illumination Radar Feasibility," 2018. https://apps.dtic.mil/sti/pdfs/AD1132052.pdf.

25 Parker, Edward. "Commercial and Military Applications and Timelines for Quantum Technology Research Report." *Rand Corporation Research Report*, October 28, 2021. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA1482-4/RAND_RRA1482-4.pdf.

26 The Australian Army. "Army Quantum Technology Roadmap." *Quantum Technology Roadmap*, April 2021. https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf.

27 Parker, Edward. "Commercial and Military Applications and Timelines for Quantum Technology Research Report." *Rand Corporation Research Report*, October 28, 2021. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA1482-4/RAND_RRA1482-4.pdf.

28 B. Kania, Elsa , and John Costello. "Quantum Hegemony?" CNAS, 2024. https://www.cnas.org/publications/reports/quantum-hegemony.

29 *Ibid*.

30 Portman, Rob, Tom Carper, and Ranking Member. "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans ." *United States Senate Permanent Subcommittee on Investigations on Homeland Security and Governmental Affairs*. Accessed November 26, 2024. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf.

31 Chinese Defence Universities Tracker. "Home," 2024. https://unitracker.aspi.org.au/.

32 Parker, Edward, Daniel Gonzales, Ajay K Kochhar, Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, et al. *An Assessment of the U.S. And Chinese Industrial Bases in Quantum Technology. Rand.org*. RAND Corporation, 2022. https://www.rand.org/pubs/research_reports/RRA869-1.html.

33 *Ibid*.

34 Bondy, Matthew. "AUKUS Is Not Just about Subs: It's about Advanced Technology." Centre for International Governance Innovation, December 10, 2021. https://www.cigionline.org/articles/aukus-is-not-just-about-subs-its-about-advanced-technology/.

35 Gunther, Aimee, Peter Mason, and Julie Lefebvre. "CAN UNCLASSIFIED DND/CAF Quantum S&T Strategy: Preparing for Disruptions in Future Operating Environments Defence Research and Development Canada CAN UNCLASSIFIED," 2021. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc356/p812809_A1b.pdf.

36 Innovation Science and Economic Development Canada. "What We Heard Report." *ISED*. National Quantum Strategy Consultations. Accessed November 26, 2024. https://ised-isde.canada.ca/site/national-quantum-strategy/sites/default/files/documents/2022-07/1032_06_21_nqs_wwh_report_en_v4.pdf.

37 The Economist. "Here, There and Everywhere," 2019. Originally found at: https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own.