Quantum Technology for Defence

What to Expect for the Air and Space Domains

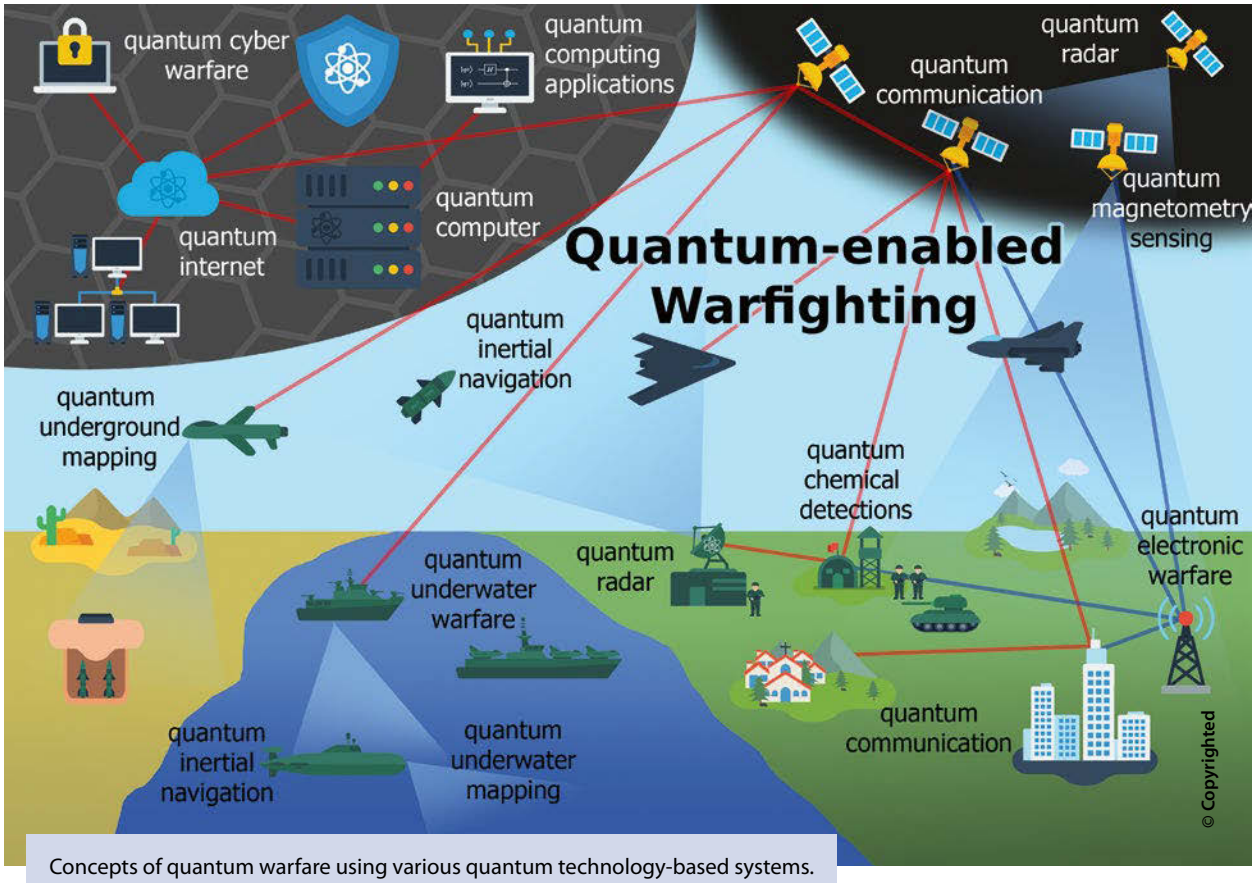
By Dr Michal Krelina, Czech Technical University in Prague
By Lieutenant Colonel Denis Dúbřavčík, CZ Air Force, JAPCC

Introduction

Quantum Technology (QT) has its foundation in quantum mechanics, a discipline more than one hundred years old. The first applications of quantum mechanics, known as Quantum Revolution 1.0, include nuclear fission, lasers, semiconductors, etc., where the statistical aspects of quantum behaviour are exploited. The first quantum revolution had and still has a profound impact on all aspects of society, from the military and international security to the development of atomic weapons, chips, computers, and precise navigation.

Now, we are entering Quantum Revolution 2.0, or QT, where we are exploiting the full spectrum of quantum physics' so-called 'strange' laws at the limits of known physics. In Quantum Revolution 2.0 we exploit the behaviour of individual quantum systems such as the electron, atom, nucleus, molecule, quasiparticles, etc. QTs will not introduce fundamentally new weapons, as happened with nuclear and laser weapons, but rather improve and sharpen present sensing, communication, and computing capabilities. Although most QT's aspects are still in the form of fundamental rather than applied research, we can foresee several highly relevant applications for defence.

QTs are at the forefront of advanced nations' long-term defence planning, including the United States, China, the United Kingdom, Australia, India, Russia, Canada, etc. In February 2021, NATO Defence Ministers endorsed the Emerging and Disruptive Technologies



Concepts of quantum warfare using various quantum technology-based systems.

(EDT) Strategy to promote a coherent approach to developing and adopting dual-use technologies, with quantum-enabled technology being one of the nine technology areas promoted in this strategy.[1]

Other international actors are aggressively pursuing QTs. For example, the Chinese People's Liberation Army has recognized the strategic value and potential decisive advantage of QT,[2] while the European Union has marked QT as an 'emerging technology of global strategic importance' and noted that it will be used 'for sensitive applications in the area of security, and in dual-use applications'.[3] As such, it is clear that QTs are set to play a major role in the defence strategies of nations across the world.

NATO organizations, bodies, and member states are actively studying QTs, both theoretically and experimentally, to cope with the inherent critical technological challenges.[4, 5] At the 2021 NATO Summit, Allied leaders launched the Defence Innovation Accelerator for the North Atlantic (DIANA), with a branch dedicated to QTs.[6] Importantly, QT are a subject of interest in NATO ACT studies.[7] Moreover, the NATO Science and Technology Organization study 'Science & Technology Trends 2020-2040' examined the basis and expectations for QT in NATO while the NATO Conference of National Armaments Directors discussed the implementation plan for QT.[8]

It is important to stress here that most QTs are currently at low Technology Readiness Levels (TRL) and, thus, difficult to accurately predict the actual performance, capability, all possible applications, and timelines. This is known as the Collingridge dilemma that applies when 'a) impacts cannot be easily predicted until the technology is extensively developed and widely used; b) control or change is difficult when the technology has become entrenched'.[9] In this paper, we aim to build awareness of QT by briefly introducing the QT's key elements, their basic applications, the potential utility in the air and space domains, and set realistic expectation for fielded QT.

Key Elements

Why are the QTs so interesting and important? Using fundamental quantum physics' principles can, in theory, lead to exponential speed-up in computation,

impressive increase of sensor sensitivity, and unprecedented secure communications. Overall, these areas are covered by the quantum information science discipline. Before we consider individual QTs, we must understand a few fundamentals. The features critical for the QT revolution which we will further examine are the quantum bit, quantum superposition, quantum entanglement, no-cloning theorem, and quantum tunnelling.

The quantum bit, or qubit, is the quantum analogy of the classical information bit. Whereas the classical bit can have only the values of 0 or 1, the qubit is described by a quantum state. The quantum superposition means that a qubit can represent two states simultaneously. Such behaviour has important implications for computational power enhancement. With N qubits, we can represent 2N states (i.e. the number of represented states grows exponentially with the number of qubits). Note that when the quantum measurement is applied at the end of a quantum algorithm the whole superposition collapses into one state only. Therefore, we must run one algorithm several times and draw conclusions based on the statistical distribution of individual states. With multiple repetitions, we can reach exponential speeds. However, such an increase in computational capacity requires the development of new quantum algorithms and departure from conventional computing.[10] There are also many technical complications that challenge our ability to accomplish quantum computing at scale.

The no-cloning theorem states that the quantum data of a qubit (or of an arbitrary quantum state in general) cannot be copied or cloned. On one side, this has significant consequences for increasing the complexity of quantum computers due to the need for more sophisticated quantum error corrections. The quantum errors are corrected indirectly because, as described above, a measurement of an actual state will lead to its destruction. On the other side, it provides unprecedented applications for security that cannot be eavesdropped on. The intruder's interference would require quantum measurement, which would lead to the quantum collapse to one state. Such a situation can be easily discovered by comparing the measurements of the sender and receiver.

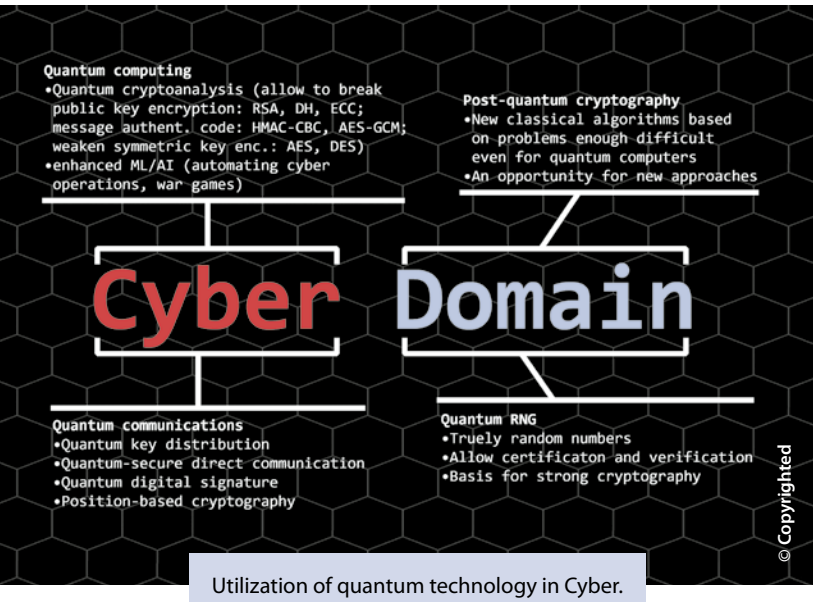
Quantum entanglement is another key concept that refers to the strong correlation between two or more qubits, a link with no classical analogy. In short, any quantum manipulation with one of the entangled qubits will have an instant effect on the other linked qubits, irrespective of the distance or obstacles between them. As such, quantum entanglement is an essential feature for most QTs, allowing them to reach the fundamental limits of present physics defined by the Heisenberg uncertainty principle, and a key element for many quantum algorithms.

In general, qubits and quantum sensing systems can be realized using different quantum-physical properties such as electric current flow in superconducting electronics, polarization or the number of photons, or the spin or energy state of electrons, nuclei, or molecules. All these quantum systems are extremely fragile, and many can be manipulated only at temperatures close to absolute zero (about -273 °C). As such, the above-described quantum properties cannot be applied directly in weapons since even the slightest disturbance leads to the loss of quantum information or sensitivity in quantum sensors. With this basic appreciation of the underlying science, let us consider potential applications.

Basic Applications

To properly understand the potential benefits, we will divide QTs into three categories: quantum computing, quantum networks and communications, and quantum sensing and imaging.

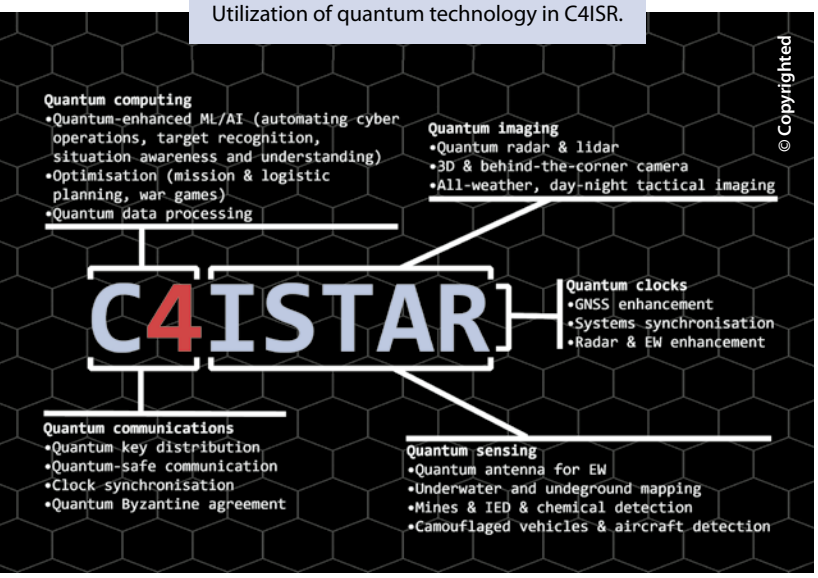
Quantum computing represents universal programmable quantum computers, quantum annealers (an imperfect adiabatic computation), and quantum simulators which can provide considerable computational advantage over classical computers. However, despite the common misconception that the exponential increase in processing speed will affect and take over all the classical computers' tasks and applications, quantum computers will only be efficient in certain highly complex and challenging computational problems. Examples of such problems are quantum simulations (molecule simulation



Utilization of quantum technology in Cyber.

for chemical and pharmaceutical research, new material development, etc.), quantum cryptoanalyses (breaking of most asymmetric encryption schemes commonly used to encrypt emails, voice and video calls, data transfers, and remote access to intranets), faster searching, faster solving of linear or differential equations, quantum optimizations (e.g. supply chains optimizations, logistics, investment portfolios, or customized medications), and quantum-enhanced machine learning. At the moment, quantum computing for practical deployment is at least ten years away and will not replace classical computers.

Utilization of quantum technology in C4ISR.



Quantum networks and communications aim to transmit quantum information (qubits) across various channels, such as fibre optic lines or free-space communication. The only practical use in first-generation quantum networks is Quantum Key Distribution (QKD). A significant advantage of QKD over conventional asymmetric encryption (also called public-key cryptography) is that any interception or eavesdropping attempt would be noticed immediately. QKD is commercially available for use with optical fibres, and many commercial free-space QKD services are to be launched in the next two to five years. Note that QKD is often described as unhackable. However, this is only true for properly implemented quantum information transmissions; the endpoints, controlled by classical computers, will remain targets for offensive cyber operations.

The next-generation quantum network, called Quantum Information Network (QIN) or quantum internet, differs in its ability to distribute entangled qubits.[11] QIN will offer more services related to security, such as secure identification, position verification, and distributed quantum computing. Significant technical applications will also lead to high-precision clock synchronization and networked quantum sensors. The biggest obstacle to QIN implementation is the need for reliable quantum memory to store quantum information for synchronization and distribution across a network with many intermediate nodes. The QIN could be expected in 2030+.

Quantum sensing aims for more precise measurements of various physical variables such as magnetic or electric fields, gravity gradients, acceleration rotations, and time. Improved time measurements can be used for more precise clocks (used by many current technologies), quantum inertial navigation, underground and undersea exploration, more effective radio frequency communication, etc. Quantum sensing is the most developed QT (highest TRL in average), but the effectiveness of deployed sensors is still very uncertain. However, military

applications require a portable or mobile solution with low SWaP (size, weight, and power). At the same time, the spatial resolution of quantum sensors needs to improve, as it is often inversely correlated with sensitivity. For example, detecting a submarine from space may be possible, but using a quantum sensor with a useful degree of precision is unlikely since sufficient spatial resolution will lead to insufficient sensitivity. On the other hand, some quantum sensors, such as those in quantum navigation, are expected to be tested in the relevant field environments within the next five years.

Quantum imaging is a subfield of quantum optics that is active (i.e. some signal is emitted and its reflection needs to be detected) compared to quantum sensors (that measure some external quantity). For any sensor, the Signal-to-Noise Ratio (SNR) represents the fundamental limit of its sensitivity. However, a significantly higher SNR can be reached using quantum entanglement, as the signal itself may be unrecognizable in the background noise without additional knowledge of entanglement. Quantum imaging can improve the existing technology, such as quantum radars, three-dimensional cameras, around-the-corner cameras, gas leakage cameras, and low-visibility vision devices.

Lastly, Post-Quantum Cryptography (PQC), also known as quantum-resistant cryptography, is nothing quantum at all but an evolution of the present asymmetric cryptography. PQC relies on more advanced mathematics that is more difficult to compute, even for quantum computers. As such, PQC can be imagined simply as software/hardware updates to existing systems, although they are usually more computationally demanding. In principle, it can never be proven that PQC is completely secure as new classical or quantum crypto-analytical attacks may occur. Still, PQC will be available soon and resilient against quantum attacks for the foreseeable future. For example, based on the NSA recommendation, the White House published in 2022 a memorandum providing directions for agencies to start the migration to PQC with full implementation by 2035.[12] However, the US Department of Homeland Security is aiming to migrate its systems by 2030.

QT in Air and Space

As in the past with other technologies, defence applications are again the primary drivers of research and development in the field of QT, particularly in the United States and China. While much of this research is often classified, there are several overviews and roadmaps available that outline potential use cases and ideas for the air and space domains.[13] These documents provide a glimpse into the exciting possibilities of QT and its potential to revolutionize the defence industry.

Even though QT has promising potential with real transformational aspirations, due to its complexity it is still poorly understood by non-specialists and its importance is often exaggerated and hyped. At present, being mostly at the laboratory stage with low TRLs complicates realistic estimates of future utility, capabilities, or the role it will play in the future.

Here, we will present the most discussed ideas and possible use cases for the Air and Space domains.

Quantum radar is a quantum imaging system that works similarly to classical radar but at the level of individual photons. Theoretically, it offers various advantages such as higher noise resistance, stealthiness (extremely low intensity and, therefore, low probability of detection), and possible target identification. The principles of quantum LIDAR (light detection and ranging) or RADAR were already demonstrated successfully in laboratories. However, the microwave regime, which is crucial for many types of ground-based radars, presently seems unfeasible.[14] Nevertheless, space-based quantum LIDAR applications in the optical regime remain viable in the medium-to-long term. Conversely, more precise quantum or optical atomic clocks can improve the performance of current radars and electronic warfare systems.

Free-space quantum communication will be an important channel for future quantum internet and will lead to a higher presence of quantum communication assets in air and space. In the next five years, free-space quantum communication is unlikely to

be part of military or governmental satellite communication services because its implementation requires new infrastructure and more investments. Moreover, the present performance is too low for practical use and the quantum network's low density makes it very vulnerable. However, quantum communication will be present in the air and space domains mainly for research and development, proof-of-concept demonstrations, and experimental, mainly commercial, applications.

The situation will change with the arrival of reliable quantum memory and high-rate quantum optics. Then, quantum internet with significant space presence may start to build up after 2030. In the future, there is an opportunity to implement quantum communication with laser communication where significant technological overlap exists. Laser communication would offer high-speed data transfer secured by quantum communication. Quantum cryptography is presently considered a secondary developmental effort to PQC. PQC is the preferred solution today since it could be just a software update, has a shorter deployment timescale, and can use the current classical networks or internet infrastructure.

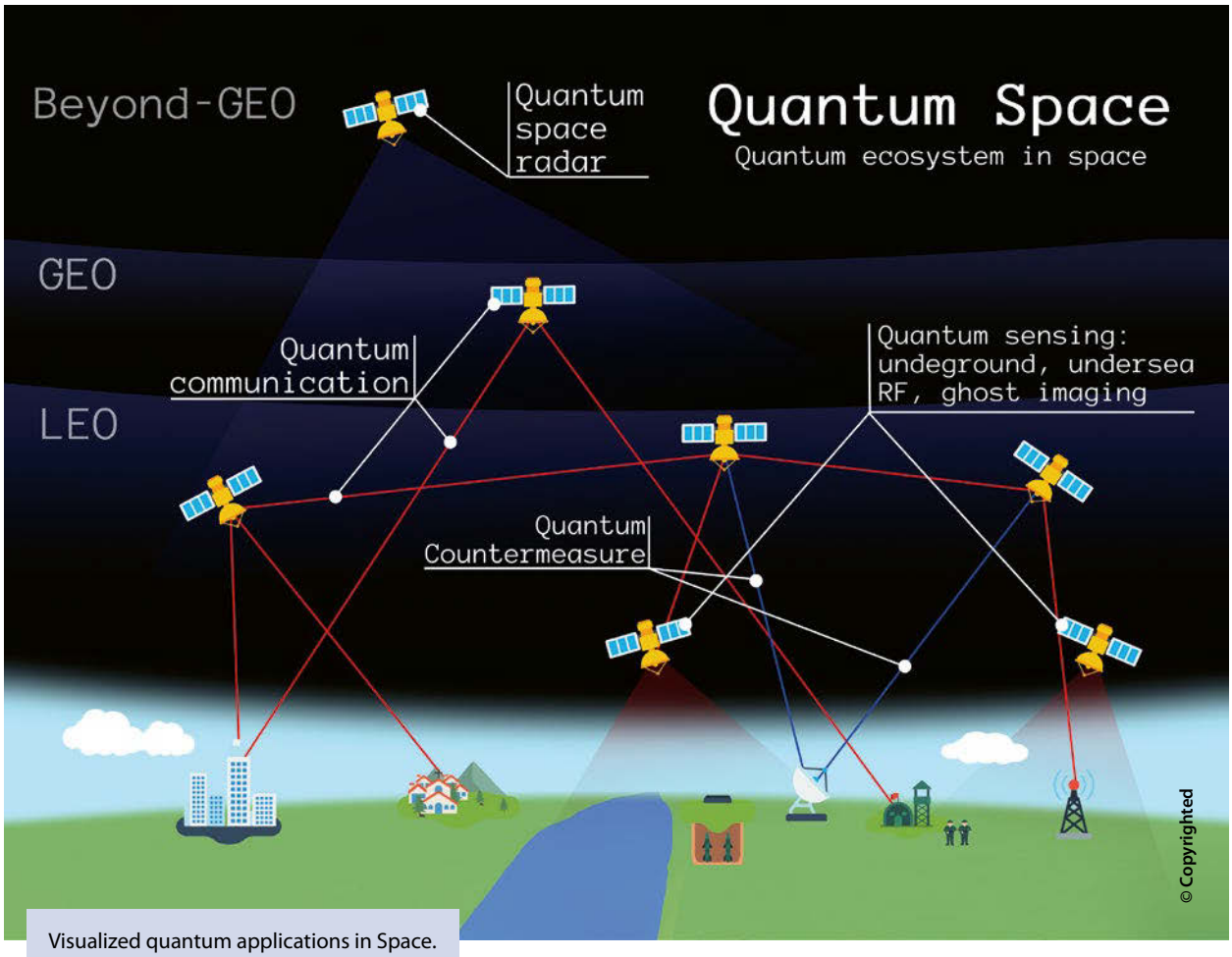
One of the most interesting applications for QT is Intelligence, Surveillance, and Reconnaissance (ISR). Individual QTs offer various sensing and imaging systems that significantly improve the extant ISR systems. Furthermore, fusing quantum ISR capabilities with conventional capabilities may lead to a new epoch in ISR by leveraging the strengths and offsetting the weaknesses of both. However, fully realizing these possibilities will depend upon quantum computing and communications.

Quantum magnetometers and gravimeters are two examples. Quantum magnetometers detect magnetic fields, such as local magnetic anomalies or weak biological magnetic signals. Quantum magnetic sensors are under development for detecting metallic objects generating local magnetic anomalies, such as mines, improvised explosive devices, submarines, camouflaged vehicles, and rotating machinery through walls. They can also serve as an alternate method of underwater navigation. Quantum gravimeters are under development for underground surveillance systems and are tested for detecting underground structures such as caves, tunnels, bunkers, research facilities, or missile silos. Both sensors could be deployed on airborne systems or space assets in low Earth orbit.

The closest QT to real deployment is the quantum radio-frequency (RF) receiver. A quantum RF receiver has improved features such as a wider band, better SNR, smaller size, better angle-of-arrival detection, self-calibration, no metallic parts to generate additional noise, output in optical regime allowing faster signal processing, and measurement of both weak and very strong fields. In the defence context, quantum RF receivers could enable reception of advanced Low Probability of Intercept/Low Probability of Detection (LPI/LPD) communications and over-the-horizon RF signals, resistance to RF interference and jamming, RF direction finding, and terahertz frequency imaging. In the future, quantum RF receivers can become the standard RF receiver for multiple systems, e.g. for 5G and the Internet of Things. Quantum RF receivers are expected to be equally helpful to expanding our communications, improving the detection of adversary signals, and calibrating the existing RF devices.

Quantum imaging systems could further serve in Intelligence, Surveillance, Target Acquisition, and Reconnaissance roles. These include all-weather, day-night tactical sensing in long/short-range, active/passive regimes, and stealth detection modes. They can work as low-light or low-SNR vision devices in environments with clouds, fog, dust, smoke, and jungle foliage or at night; for example, to assist helicopter pilots to land in dusty, foggy, or smoky environments.

Quantum inertial navigation is another relevant technology for the air domain and is analogous to classical inertial navigation but using quantum sensors. Individual parts are being tested in laboratories and relevant environments with stabilities sufficient for military use. However, creating a complete quantum inertial measurement unit is still challenging. General expectations are that quantum inertial



Visualized quantum applications in Space.

navigation will attain drift rates of only a few hundred metres per month compared to current marine-grade inertial navigation (for military ships and submarines) with a drift of 1.8 km/day.[15] The first users will probably be submarines with the least restrictive SWaP parameters. In time, we can expect more miniaturization and deployment in planes, drones, and missiles.

Quantum computing has great potential in many applications, such as improved machine learning and artificial intelligence, better aerodynamic designs, faster simulations, etc. All are expected to bring significant improvements in areas such as ISR processing and command and control. However, quantum computing is not expected to be operational for 10–20+ years, compared to 5–10+ years for quantum communication or 3+ years for quantum sensing.[16]

Conclusions

Quantum technologies hold great promise in the long term for a broad spectrum of applications, from sensing to communications to computing, but should not be assumed to revolutionize defence applications in the foreseeable future.

Even though principles were proven successful in laboratories, the transition from laboratory to real-world applications is still in progress. Requirements, such as low SWaP, mobility, and cost, still represent significant limiting factors.

For a good reason, QTs have captured our attention and imagination. Based on theoretical and laboratory work, we have an appreciation of the technology and its possible uses in real-world applications. Towards

that end, NATO's role is to set goals and standards to encourage development and ensure interoperability. Meanwhile, Allied nations must invest in the necessary research and look for dual-use opportunities to speed development and reduce cost. With this understanding, we can pursue the great promise of QT with a realistic understanding of the timeline and effort involved. ●

1. 'Emerging and Disruptive Technologies', NATO, December 2022. https://www.nato.int/cps/en/natohq/topics_184303.htm (accessed 3 January 2023).
2. Kania, E. and Costello, J., 'Quantum Leap (Part 2): The Strategic Implications of Quantum Technologies', The Jamestown Foundation, 21 December 2016. https://jamestown.org/program/quantum-leap-part-2-strategic-implications-quantum-technologies/ (accessed 12 December 2022).
3. 'Horizon Europe - Work Programme 2021–2022 – 7. Digital, Industry and Space', European Commission, 23 August 2021. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-7-digital-industry-and-space_horizon-2021-2022_en.pdf (accessed 12 December 2022).
4. 'Quantum Computing and Artificial Intelligence Expected to Revolutionize ISR', NATO ACT, 30 September 2022. https://act.nato.int/articles/quantum-computing-and-artificial-intelligence-expected-revolutionize-isr (accessed 12 December 2022).
5. 'Using Quantum Technologies to Make Communications Secure', NATO, 27 September 2022. https://www.nato.int/cps/en/natohq/news_207634.htm (accessed 12 December 2022).
6. Naujokaitytė, G. and Burke, F., 'NATO to launch €1B fund for high tech start-ups in dual use technologies', Science|Business, 12 April 2022. https://sciencebusiness.net/news/nato-launch-eu1b-fund-high-tech-start-ups-dual-use-technologies (accessed 12 December 2022).
7. 'NATO Exploring Quantum Technology for Future Challenges', NATO ACT, 14 October 2022. https://www.act.nato.int/articles/nato-exploring-quantum-technology-future-challenges (accessed 12 December 2022).
8. Reding, D. F. and Eaton, J., 'Science & Technology Trends 2020-2040', NATO Science & Technology Organization, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf (accessed 12 December 2022).
9. Roberson, T., 'Talking about responsible quantum: Awareness is the absolute minimum ... that we need to do', arXiv.org. https://doi.org/10.48550/arXiv.2112.01378 (accessed 18 October 2022).
10. Biercuk, M. J. and Fontaine, R., 'The Leap into Quantum Technology: A Primer for National Security Professionals', War on the Rocks, 17 November 2017. https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/ (accessed 12 December 2022).
11. Wehner, S., Elkouss, D. and Hanson, R., 'Quantum Internet: A vision for the road ahead', Science, Vol. 362, no. 6412, 19 October 2018. https://doi.org/10.1126/science.aam9288 (accessed 12 December 2022).
12. Young, S. D., 'Memorandum for the heads of executive departments and agencies – Migrating to Post-Quantum Cryptography', The White House's Office of Management and Budget, 18 November 2022. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf (accessed 23 January 2023).
13. Krelina, M., 'Quantum Technology for Military Applications', EPJ Quantum Technology 8 December 2021. https://doi.org/10.1140/epjqt/s40507-021-00113-y (accessed 18 October 2022).
14. Daum, F., 'Quantum Radar Cost and Practical Issues', IEEE Aerospace and Electronic Systems Magazine, November 2020. https://doi.org/10.1109/MAES.2020.2982755 (accessed 28 October 2022).
15. Travagnin, M., 'Cold Atom Interferometry for Inertial Navigation Sensors', Joint Research Centre, European Commission, 2020. https://data.europa.eu/doi/10.2760/237221 (accessed 28 October 2022).
16. Ibid. 12.

Dr Michal Krelina

is a research scientist at the Czech Technical University in Prague, the Czech Republic, and a quantum security expert in the GOVSATCOM programme at the EUSPA (European Union Agency for the Space Programme). His original background is in high-energy theoretical particle and nuclear physics. Michal is a consultant, analyst, and strategist in quantum technology, emphasizing security and defence applications. His quantum technology research focuses on mapping quantum technology military applications, exploring quantum technology roles in future conflicts, quantum technology risk and threat assessment, and consulting for different departments of NATO and various defence and law enforcement organizations. He has a PhD in experimental nuclear physics.

Lieutenant Colonel Denis Dúbřavčík

was enlisted in the Czech Air Force in 1996. He graduated from the Brno Military Academy with a BSc in Military Rocket and Aircraft Systems and an MSc in Mechanical Engineering. He is a graduate of the Squadron Officers School at Maxwell Airbase, US. He served, among other functions, as a weapons instructor and commander of the 212th Tactical Squadron at Air Force Base Čáslav, the Czech Republic. He is a pilot and instructor on the L-159 ALCA aircraft with more than 1,500 flight hours. He is currently serving in the Assessment, Coordination, and Engagement Branch of the JAPCC as the Plans, Concepts, Development, and Vision Staff Officer.