EPJ Quantum Technology
a SpringerOpen Journal

REVIEW Open Access

Quantum technology for military applications

Michal Krelina[1,2*]

*Correspondence:
michal.krelina@cvut.cz
[1]Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague, Brehova 7, Prague, Czech Republic
[2]Quantum Phi s.r.o., Bryksova 944, Prague, Czech Republic

Abstract

Quantum technology is an emergent and potentially disruptive discipline, with the ability to affect many human activities. Quantum technologies are dual-use technologies, and as such are of interest to the defence and security industry and military and governmental actors. This report reviews and maps the possible quantum technology military applications, serving as an entry point for international peace and security assessment, ethics research, military and governmental policy, strategy and decision making. Quantum technologies for military applications introduce new capabilities, improving effectiveness and increasing precision, thus leading to 'quantum warfare', wherein new military strategies, doctrines, policies and ethics should be established. This report provides a basic overview of quantum technologies under development, also estimating the expected time scale of delivery or the utilisation impact. Particular military applications of quantum technology are described for various warfare domains (e.g. land, air, space, electronic, cyber and underwater warfare and ISTAR—intelligence, surveillance, target acquisition and reconnaissance), and related issues and challenges are articulated.

Keywords: Quantum warfare; Quantum technology; Quantum computing; Quantum sensing; Quantum network; Quantum radar; Quantum imaging; Military applications; Quantum security; Dual-use technology

1 Introduction

Although fourth generation modern warfare is characterised by decentralisation and the loss of states' monopoly on war [1, 2], armies of advanced countries characteristically have access to state-of-the-art military technologies. This includes the appearance of quantum technologies on the horizon.

The term quantum technology (QT) means the technology mostly arising out of the so-called second quantum revolution. Earlier, the first quantum revolution brought technologies that are familiar to us today, such as nuclear power, semiconductors, lasers, magnetic resonance imaging, modern communication technologies or digital cameras and other imaging devices. The first quantum technology resulted in nuclear weapons and energy; then, the classical computer gained a significant role. Presently, laser weapons are being implemented and tested [3].

The second quantum revolution [4] is characterised by manipulating and controlling individual quantum systems (such as atoms, ions, electrons, photons, molecules or various quasiparticles), allowing to reach the standard quantum limit; that is, the limit to measurement accuracy at quantum scales. In this report, the term quantum technology refers to the technology from the second quantum revolution. Quantum technology does not bring fundamentally new weapons or standalone military systems, but rather significantly enhances measurement capability, sensing, precision and computation power and efficiency of the current and future military technology. Most of the quantum technologies typically are technologies of dual use. Consequently, there is tremendous potential for military applications of quantum technology. Various studies and recommendations are emerging, signalling the increasing likelihood of such technology being realised; see, for example, [5–8].

This report provides a more in-depth context in which to understand the term 'quantum warfare', discussing the possibility of its affecting the intelligence, security and defence sectors, and describing new possible capabilities or improvements. The goal is not to provide a precise forecast of quantum-based technologies, but rather to show possible directions and trends in implementation and applications. Quantum technologies in general are considered emerging technologies, with the potential to change the conduct of warfare and the outcomes of battles [8]. Although the current quantum technologies mostly have low Technology Readiness Levels (TRL), they are believed to have disruptive potential [9]. The mapping of quantum technologies' conceivable military applications is also important for the further assessment of threats to global peace and in the discussion of ethics policies or quantum-based preventive arms control.

This report comprises eight sections. In Sect. 2, the terms 'quantum technology' and 'quantum warfare' are defined, with the quantum technology taxonomy and quantum technologies being introduced. Section 3 provides the basic quantum technology overview that is the foundation for a particular application, including the expected time of deployment and utilisation impact. Section 4 presents the general considerations and expectations regarding quantum technology development and deployment in the military domain. In Sect. 5, the applications of individual quantum technologies in the military are presented for various domains (e.g. cyber, underwater, space and electronic warfare). Section 6 identifies and discusses the quantum hype as well as the realistic possibilities. Section 7 contains the initial discussion on related military, peace and ethical aspects as well as the technical consequences and challenges. Section 8 concludes the paper.

Sections 5 and 4 concern national security and defence issues. Although Sect. 3 is based on state-of-the-art research and provides related references, Sect. 5 is based more on various military or government reports, policy briefs and international security analyses such as [5–8, 10–13]. Here, the reader should be wary of the hype surrounding quantum technology and avoid exaggerated expectations; this aspect is addressed in Sect. 6 and by [14]. For many of the presented quantum technology military applications, it is uncertain whether all challenges connected with the demands of high-end military technologies will be resolved, or even that the technology will actually be deployed.

2 Definitions

The term quantum technology is defined as follows:

> *Quantum technology* (QT) is an emerging field of physics and engineering based on quantum-mechanical properties—especially quantum entanglement, quantum superposition and quantum tunnelling—applied to individual quantum systems, and their utilisation for practical applications.

As follows from the definition, quantum technology describes the various physical principles of quantum-mechanical systems, with numerous applications; for instance, the technique of trapped ions can serve as a quantum bit for quantum computers and as a quantum sensor for magnetic fields or quantum clocks.

> *Dual-use technology* refers to fields of research and development with potential application in both defence and commercial production [15].

Quantum technology is a typical dual-use technology which has been of considerable interest not only for military but also for governmental actors [16] and peacekeeping organisations.

> *Quantum warfare* (QW) is warfare that uses quantum technologies for military applications that affect intelligence, security and defence capabilities of all warfare domains, and it ushers in new military strategies, doctrines, scenarios and peace as well as ethics issues.

There have been attempts also to define the *quantum domain* [17] as a new domain for warfare. However, in this text, we will consider quantum technology as a factor that improves all currently defined domains, rather than as a standalone warfare domain.

Subsequently, it is helpful to define the term *quantum attack*, which refers to using quantum technologies to break, disrupt or eavesdrop on either classical or quantum security systems. Typical examples are eavesdropping using quantum key distribution or quantum computers breaking the Rivest–Shamir–Adleman (RSA) encryption scheme.

Although there is plenty of QT literature, there is no explicit agreement on quantum technology taxonomy. We will use the following taxonomy:

- *Quantum Computing and Simulations*
  - Quantum Computers (digital and analogue quantum computers and their applications, such as quantum system simulation, quantum optimisation, …)
  - Quantum Simulators (non-programmable quantum circuits)
- *Quantum Communication and Cryptography*
  - Quantum Network and Communication (quantum network elements, quantum key distribution, quantum communication)
  - Post-Quantum Cryptography (quantum-resilient algorithms, quantum random number generator)
- *Quantum Sensing and Metrology*
  - Quantum Sensing (quantum magnetometers, gravimeters, …)
  - Quantum Timing (precise time measurement and distribution)
  - Quantum Imaging (quantum radar, low-SNR imaging, …)

Aside from the general quantum technology taxonomy presented above, we introduce a new division of quantum technologies according to their benefits and utilisation. The following classification can be generalised; however, we place more emphasis on military applications. The quantum technology utilisation impact classification is as follows:

- *Must have*: quantum technology that has to be implemented to protect against future quantum attacks (e.g. post-quantum cryptography);
- *Effectiveness*: quantum technologies that increase the effectiveness of the current technology and methods (e.g. quantum optimisations, quantum machine learning or artificial intelligence);
- *Precision*: quantum technologies that increase the precision of the current measurement technology (e.g. quantum magnetometry, quantum gravimetry, quantum inertial navigation, timing);
- *New capabilities*: quantum technologies offering new capabilities that were beyond the scope of the present technology (e.g. quantum radar, quantum simulation for chemistry, quantum cryptoanalysis, quantum key distribution).

Note that this classification is not mutually exclusive.

3 Quantum technology overview

This section provides a basic description of quantum technologies, with related references. For each quantum technology, the current development status is presented, the utilisation impact determined, expected time to deployment estimated,[1] and the main challenges are sketched. For quantum computing application, the approximate number of required logical qubits is provided.

Different quantum technologies and their applications are at different TRLs[2] from TRL 1 (e.g., some types of qubits) to TRL 8 (e.g., quantum key distribution).

We are not aiming for completeness here, nor do we present any theoretical background, but just introduce the basics, the effects and the current state of development, as needed to follow the discussed military applications.

3.1 Quantum information science

Quantum information science (QIS) is an information science related to quantum physics, and deals with quantum information. In classical information science, the elementary carrier of information is a bit that can be only 0 or 1. The quantum information elementary carrier of information is the quantum bit, qubit in short. A qubit can be $|0\rangle$ or $|1\rangle$, or an arbitrary complex linear combination of states $|0\rangle$ and $|1\rangle$ called the quantum superposition.

The other crucial property is the quantum entanglement. Quantum entanglement refers to a strong correlation between two or more qubits (or two or more quantum systems in general) with no classical analogue. Quantum entanglement is responsible for many quantum surprises. Another feature is the no-cloning theorem [18], which says that quantum information (qubit) cannot be copied. This theorem has profound consequences for qubit error correction as well as for quantum communication security.

Quantum information science describes the quantum information flow in quantum computing and quantum communications, although in a broader sense it can be applied in quantum sensing and metrology, see [19, 20].

[1] Short-term: 0–5 years, Mid-term: 6–10 years, Long term: 10–20 years.

[2] See Technology Readiness Levels according to EU, https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

There is considerable academic interest, and several quantum algorithms have been created [21]. However, only a few are expected to be valuable for defence and security applications.

3.2 Quantum computing

- *Status*: commercially available with very limited number of physical qubits
- *Utilisation impact*: new capability, effectiveness, precision
- *Timeline expectation*: one million physical qubits in ten years
- *Main challenges*: improving the quality of qubits (coherence, error resistance, gate fidelity), upscaling the number of qubits, logical qubits

Quantum computing refers to the utilisation of quantum information science to perform computations. Such a machine can be called a quantum computer. The classification of quantum computers can be very complex. For the purposes of this report, we simplify the classification as follows:

- *Digital quantum computer* (also called a gate-level quantum computer) is universal, programmable and should perform all possible quantum algorithms and have numerous applications described below. Classical computers can fully simulate the gate-level based quantum computer. The difference is in resources and speed. For instance, the simulation of fully entangled qubits increases the requirement of classical resources exponentially. This means that the simulation of $\gtrsim 45$ qubits is practically impossible on the classical (super)computers.
- *Analogue quantum computer* (also called Hamiltonian computation) is usually realised using quantum annealing (as the noise version of the adiabatic quantum computing). Quantum annealer differs from the digital quantum computer by the limited connectivity of qubits and different principles. Therefore, the utilisation of analogue quantum computers is more constrained but is still suitable for tasks such as quantum optimisations or Hamiltonian-based simulations.
- *Quantum simulator* is used for the study and simulation of other quantum systems that generally are less accessible and is usually built as a single-purpose machine. In comparison with a quantum computer, the quantum simulator can be imagined as a non-programmable quantum circuit.

In general, quantum computing will not replace classical computation. Quantum computers will be practical and useful for a limited type of problems only, typically problems with high complexity. The actual deployment of quantum computing applications depends on the quality (coherence, error resistance, gate fidelity) and the number of qubits. Some of the essential parameters to follow are: the number of qubits, qubit coherence time, quantum-gate fidelity and qubit inter-connectivity. The set of quantum instructions applying quantum gates on individual qubits is called a quantum circuit. A quantum circuit is a practical realisation of the quantum algorithm.

Following [7], quantum computers can be classified into three evolutionary stages: Component quantum computation (CQC), Noisy intermediate-scale quantum (NISQ) computing and Fault-tolerant quantum computing (FTQC). The CQC stage covers quantum computing demonstrators and maturing the basic elements. CQC has a very limited computational capability that is sufficient for demonstration of some proofs of principle. The NISQ stage quantum computer should have a sufficient number of qubits to demonstrate the advantages of quantum computing. Continuous research should lead to increasing

the number and quality of qubits. The FTQC stage starts when a perfect logical qubit is reached (for an explanation, see below).

Physical qubits can be realised by numerous quantum systems. The most recent advanced are quantum computer based on superconducting qubits and the trapped-ion qubits that are in or close to the NISQ stage. All other technologies, such as cold atoms, topological, electron spin, photonic or NV centre-based qubits, are still in CQC stage or theory only. The individual quantum computers and their performance differ significantly (in, e.g. speed, coherence time, the possibility to entangle all qubits, gate fidelity). Various metrics and benchmarks, such as Quantum Volume metric [22], have been developed for their comparison.

The problem, common to all types of qubits, is their quality. A qubit is very fragile and has a limited coherence time (a time scale during which it will not lose the quantum information). Every operation performed on a qubit has limited fidelity. Researchers accordingly need to employ the error correction codes. The error correction for qubits is much more complicated than error correction of classical bits, because qubits cannot be copied, as the no-cloning theorem explains. Two types of qubits are distinguished: the physical qubit realised by a physical quantum system and the logical qubit consisting of several physical qubits and error correction codes. A logical qubit is a perfect or near-perfect qubit with very long-to-infinity coherence time, very high fidelity and higher environment resistivity. For example, based on surface error correction protocol, for one logical qubit, depending on the algorithm, up to 10,000 physical qubits [23] will be needed. For a recent overview of quantum computing, see, for example, [24].

Examples of leading-edge quantum computers are the quantum computer with 53 physical superconducting qubits, manufactured by Google (which claimed quantum supremacy in 2019 [25]), and the one by IBM. The best trapped-ion quantum computers are of 32 qubits by IonQ or six qubits by Honeywell. In the case of photonic qubits, there is a 24-qubit quantum computer by Xanadu. The anticipated timelines as imagined by the quantum computing roadmap by IBM and Google are the following: IBM plans a 433-qubit quantum processor in 2022 and 1121 qubits by 2023 [26]. Google has announced a plan to reach a quantum module of 10,000 qubits. All other quantum processors would consist of such modules up to 1 million qubits in 2029 [27]. Based on a survey among leaders in key relevant areas of quantum science and technology, it is likely that quantum computers will start to become powerful enough to pose a threat to most of the public key encryption schemes (for more details, see Sect. 3.2.2) in about two decades [28]. Examples of analogue quantum computers are the quantum annealer by D-Wave Systems with over 5000 qubits and the coherent Ising machine by Toshiba.

The difference between analogue and digital quantum computers lies in their different physical principles and their limitations. The digital quantum computer is limited by resources and not by noise (noise can be corrected using more resources). In contrast, the analogue quantum computer is limited by noise which is difficult to understand, control and characterise (especially for a quantum annealer). Therefore, analogue quantum computers' applicability is limited [24].

In reality, the tasks accomplished by quantum computers will be mostly only subprograms or subroutines of the classical computer programs. The classical program will not only control quantum computers but will also provide a lot of computation that it would be impractical to carry out on a quantum computer. This includes the recent applications

of quantum simulation in chemistry using, for example, the Variational quantum eigensolver (VQE) [29], which is a hybrid combination of classical and quantum computing. Also, quantum computers are large machines, many of which require cryogenics. It is unlikely therefore that in the decades to come most customers will acquire a personal quantum computer, but rather they will access these as a service in the cloud. The cloud-based models of quantum computing (often called Quantum Computing-as-a-Service – QCaaS) are commercially available nowadays, even for free, and they allow access to anyone interested in quantum computing. The cloud access to quantum computers is offered by individual quantum hardware manufacturers. Some platforms, such as Microsoft Azure Quantum or Amazon Braket, offer access to quantum computers of various manufacturers within one ecosystem.

It is also helpful to clarify the terms of quantum supremacy, advantage and practicality. *Quantum supremacy* is a case where a particular problem is solved by a quantum computer significantly faster than by a classical computer. However, the problem is likely to be theoretical rather than practical. *Quantum advantage* refers to a case when a quantum computer is able to solve real-world problems that classical computers cannot. *Quantum practicality* is similar to quantum advantage, with the only difference being that the quantum computer solves real-world problems faster than the classical computer.

We provide below a basic overview of possible quantum computer applications. The reader should keep in mind that quantum computing is a fast developing sector, and new revolutionary quantum algorithms are still waiting to be discovered. Note that, in the context of quantum computing applications, the term 'qubit' implies a logical qubit. However, small quantum circuits can be run with only physical qubits, with reasonable precision.

3.2.1 Quantum simulations

- *Status*: algorithms in development, small-scale applications
- *Utilisation impact*: new capability (e.g. quantum chemistry computation)
- *Timeline expectation*: short-term, usability scales up with the number of qubits
- *Qubits requirement*: $\sim$ 200 (e.g. for nitrogen fixation problem)
- *Main challenges*: number of logical qubits

Long before the first quantum computer was created, the main task for the quantum computer was considered the simulation of other quantum systems [30]. Molecules are such a quantum system. Despite advancement of extant computing power, the full simulation of only simpler molecules can be performed using present computational chemistry, or of larger molecules for the price of many approximations and simplifications. For example, for a system with n electrons, the classical computer would need 2^n bits to describe the state of electrons, whereas the quantum computer needs only n qubits. Therefore, quantum simulations are the first and still perhaps the most promising application for quantum computers.

The most dominant approaches are two: quantum-phase estimation [31] and quantum variational techniques (VQE) [32, 33]. The latter approach in particular has the highest likelihood of success on NISQ computers; for example, in 2020, Google performed the biggest quantum chemical simulation up to date (of H_{12} molecule using the VQE) [34].

Algorithms for quantum chemistry simulations are being developed. They can be applied to more complex simulations, hand in hand with the number of qubits. Therefore, even at this early stage of quantum computing, there is significant interest from the chemical and pharmaceutical industries. In general, such simulations allow the discovery and

design of new drugs, chemicals and materials. Recently considered topics, for instance, are high-temperature superconducting, better batteries, protein folding, nitrogen fixation and peptides research.

3.2.2 Quantum cryptoanalysis

- *Status*: algorithms ready
- *Utilisation impact*: new capability (e.g. public-key cryptography schemes breaking)
- *Timeline expectation*: mid- to long-term
- *Qubits requirement*: ∼ 6200 for 2048 bit RSA factorisation [35], ∼ 2900 for 256 bit ECDLP-based[3] encryption [36]
- *Main challenges*: number of logical qubits

One of the most well-known quantum computer applications is the factorisation of large prime numbers by exponential speedup described by Shor's algorithm [37]. This is a threat for public-key cryptography schemes, such as RSA, DH and ECC,[4] based on the large prime number multiplications, the discrete logarithm problem or the elliptic-curve discrete logarithm problem-based schema that are considered computationally intractable or very hard for classical computers.

Although the resources of existing NISQ quantum computers are far from what is needed for RSA breaking, the threat is quite real. An adversary or foreign intelligence could intercept and store encrypted traffic until the quantum cryptoanalysis becomes available. Because the time of declassification of many secrets is far beyond the expected timelines for powerful quantum computer delivery, such a threat can be considered genuine, nowadays.

Quantum cryptoanalysis also offers improved tools for a brute-force attack on the symmetric encryption schemes. For example, the well-known Grover's searching algorithm [38] reduces the key security by half against a brute-force attack; a 256-bit AES[5] key could be resolved by brute force in roughly 2^{128} quantum operations. Despite the huge resource requirements of quantum computers, doubling the symmetric key length [39]is recommended, nevertheless. Moreover, Simon's algorithm and superposition queries [40] can completely break most message authentication code (MAC), and authenticated encryption with associated data (AEAD), such as HMAC-CBC and AES-GCM[6] [41, 42].

Further, there is active research on cryptoanalytic attacks upon symmetric key systems based on the structure present in symmetric cryptosystems, which can offer up to superpolynomial speedup [43]. However, these algorithms suffer from excessive resource requirements on the quantum computer.

3.2.3 Quantum searching and quantum walks

- *Status*: algorithms under development
- *Utilisation impact*: effectiveness (e.g. faster searching)
- *Timeline expectation*: short- to mid-term
- *Qubits requirement*: ∼ 100, depends on the searched system size

[3] Cryptography based on Elliptic Curve Discrete Logarithm Problem.

[4] cryptography schemes named after Rivest–Shamir–Adleman, Diffie–Hellman, Elliptic Curve Cryptography

[5] Advanced Encryption Standard

[6] Hash-based Message Authentication Code-Cipher Block Bhaining, AES with Galois/Counter Mode

- *Main challenges*: number of logical qubits

One of the most famous searching quantum algorithms is the Grover's algorithm [38], which offers quadratic speedup in database searching, or generally in inverting a function. For an unsorted list or database, the classical searching algorithms are about complexity $\mathcal{O}(N)$ (meaning proportional to the number of N entities), although Grover's algorithm is about $\mathcal{O}(\sqrt{N})$.

Quantum searching algorithms are an important topic for the so-called Big Data (unstructured data) analysis. Working on a large amount of data requires a large quantum memory. However, there is no reliable quantum memory that would keep the quantum information for an arbitrarily long time and in large amounts. Second, the transformation of classical data to the quantum form is time-consuming and ineffective. Therefore, only the searching on data generated algorithmically is considered practical at the moment.

The other approach to searching can be based on the quantum random walk mechanism [44], which offers similar speedup as Grover's algorithm.

3.2.4 Quantum optimisations

- *Status*: algorithms in development
- *Utilisation impact*: effectiveness (e.g. faster solution of NP problems)
- *Timeline expectation*: short- to mid-term
- *Qubits requirement*: $\sim$ 100, depends on the problem complexity
- *Main challenges*: number of logical qubits

Quantum optimisation is a very actively explored topic, given the possibility of solving NP-level[7] complex problems. An example of such an NP problem is the travelling salesman problem. Here, given a list of places and the distances between them, the goal is to find the shortest (and optimal) route. Naively, one can try all possibilities, but such an approach has severe disadvantages, and may even become impossible, with increasing complexity. Therefore, the most common solutions are based on heuristic algorithms that are not necessarily guaranteed to find the best solution but at least one close to it.

Quantum computing introduces a new perspective on the issue and offers different approaches and techniques. The most dominant methods are currently based on a variational approach, such as the Quantum approximate optimisation algorithm (QAOA) [45]. Part of QAOA is the sub-technique called Quadratic unconstrained binary optimisation (QUBO) [46], which is also suitable for analogue quantum computers. Other methods are, for example, the quantum analogy of the least-squares fit [47] or semidefinite programming [48].

So far, it is not clear whether the quantum optimisation will offer some speedup against the classical heuristic methods. However, there is consensus that if at all some speedup is achievable, it will not be more than polynomial [48]. A new paradigm introduced by quantum computing leads to new quantum-inspired classical algorithms, such as in the case of QAOA [49] that delete the quantum speedup. On the other hand, we can speak about quantum-inspired algorithms as of the first quantum computing practical result.

There have been many demonstrations, use cases and proofs of concept for quantum optimisations, especially in connection with analogue quantum computing that currently

[7] NP is a complexity class characterised by the fact that it cannot be solved in polynomial time but can be verified in polynomial time. Specifically, the NP-hard problems are not only hard to solve but are difficult to verify as well. Examples of NP-hard problems are the Travelling Salesman Problem and Graph Colouring problems.

offers the most quantum computing resources for such applications. The typical demonstrations were optimisations for traffic, logistics or the financial sector.[8]

3.2.5 Quantum linear algebra

- *Status*: algorithms in development
- *Utilisation*: effectiveness (e.g. faster linear equation solving)
- *Timeline expectation*: short- to mid-term
- *Qubits requirement*: depends on the solved system size
- *Main challenges*: number of logical qubits

It has been shown that quantum computers can reach super-polynomial speedup for solving linear equations also. Such a speedup was estimated especially for the HHL (Harrow-Hassidim-Lloyd) [50] algorithm for sparse matrices. However, the estimated speedup depends on the size of the problem (matrix). There are also large resource requirements, which for some problems can be considered too impractical [51]. On the other hand, for the system of linear equations of 10,000 parameters, for instance, 10,000 steps are needed to solve it, whereas the HHL can provide an approximate solution after 13 steps.

At present, many numerical simulations in planning, engineering, construction and weather forecasting simplify complex problems as a large set of linear equations. For many of them, being statistical in nature, the approximated solution could be sufficient.

Note that the HHL algorithm was shown as universal for quantum computing and was demonstrated for various applications such as k-mean clustering, support vector machines, data fitting, etc. For more details, see [52].

One of the major caveats of quantum algorithms working with a large amount of input data is data loading. Classical data, especially binary data or bits, need to be transferred into quantum states for follow-on processing by efficient quantum algorithms. This process is slow, and the classical data loading itself can take longer than the coherence time. The solution is a quantum memory or quantum RAM [52, 53].

3.2.6 Quantum machine learning and AI

- *Status*: algorithms in development
- *Utilisation impact*: effectiveness (e.g. better machine learning optimisations)
- *Timeline expectation*: short- to mid-term
- *Qubits requirement*: $\sim$ 100, depends on the problem complexity
- *Main challenges*: number of logical qubits

Due to the hype around classical machine learning and artificial intelligence (ML/AI), it can be expected that there will be quantum research on this topic also. First, note that one cannot expect full quantum ML/AI, considering the very low efficiency of working with classical data [54], all the more so if the missing quantum memory and very slow loading and coding of classical data (e.g. data of picture) into quantum information format are considered. It is simply not practical. Another situation will emerge when ML/AI is applied to quantum data; for instance, from quantum sensors or imaging [55].

Nevertheless, quantum-enhanced ML/AI [56, 57] can be introduced, where quantum computing can improve some machine learning tasks such as quantum sampling, linear

[8] For examples of developed quantum optimisation applications at D-Wave's quantum annealer, see https://www.dwavesys.com/applications.

algebra (where machine learning is about the processing of complex vectors in a high-dimensional linear space) or quantum neural networks [54]. One example is the quantum support vector machine [58].

In fact, the ML/AI topic covers various techniques and approaches, and it is no different in connection with quantum computing. Quantum ML/AI or quantum-enhanced ML/AI is the subject of many research works nowadays. For a survey of quantum ML/AI algorithms and their possible speedup, see [59].

3.3 Quantum communication and cryptography

Quantum communication refers to a quantum information exchange via a quantum network that uses optical fibre or free-space channels. In most cases, quantum communication is realised using a photon as the quantum information carrier. However, due to the limitations of photons, such as losses at large distances, the quantum network contains other elements such as a quantum repeater or quantum switch.

The goal of quantum cryptography is to replace conventional (mainly asymmetric) encryption schemes with quantum-resistant algorithms with the quantum key distribution. The typical quantum features used for quantum communication are the following: quantum entanglement, quantum uncertainty, and the no-cloning theory which states that quantum information cannot be copied [18, 60].

3.3.1 Quantum network

- *Status*: in research (commercially available for QKD with trusted nodes only)
- *Utilisation impact*: new capability, effectiveness (e.g. ultra secure communication, quantum-resilient cryptography)
- *Timeline expectation*: mid-term
- *Main challenges*: quantum repeater and switch (quantum memory)

The aim of the quantum network (sometimes called quantum internet [61] or quantum information network (QIN)) is to transmit quantum information via numerous technologies across various channels. The quantum information (qubit) is usually carried by individual photons, and as such the quantum information transmission is fragile. Moreover, many quantum network applications rely on quantum entanglement.

The usual channels for quantum information transmission are specialised low-loss optic fibres or the current telecommunication optic fibre infrastructures with higher loss. The case of two communicating endpoints close to each other is as simple as using one optical fibre. The complexity of the network increases with more end nodes or large distances, where components such as a quantum repeater or quantum switch are required. Note that very modest (one qubit) quantum processors are sufficient for most quantum network applications.

The free-space quantum channel is more challenging. Optical or near-optical photons are of limited utility in the atmosphere due to the strong atmospheric attenuation. Therefore, the most commonly considered and realised quantum network scenario is using quantum satellites [62, 63]. The advantage of satellites is the possibility of utilising optical-photon communication for transmission of the quantum information, where the losses in the satellite–ground link are lower than the loss between two ground nodes far apart. Nevertheless, the optical photons' communication in the free-space channel for short distances can be realised using, for instance, drones [64]. The best way would be to use the

microwave spectrum as employed by classical wireless communication. However, communication that uses the microwave spectrum at the level of individual photons is even more challenging [65]. Microwave single-photon technology involves greater difficulty in generating and detecting individual photons. Another problem is a noisy environment in microwave bands.

Quantum communication at long distances requires quantum repeaters due to photon loss and decoherence. A quantum repeater is an intermediate node that works similarly to the amplifier in classical optical networks but needs to obey the no-cloning theorem. In fact, the quantum repeater allows entangling qubits of end nodes. When two end nodes are entangled, the effect of quantum teleportation [66] can be exploited. This means that the quantum information can be teleported without a physically sent photon; just a classical communication is required. Utilising quantum entanglement, the quantum information can then flow through a quantum network or part of it, which can even be under eavesdropper control without any chance of revealing the transmitted quantum information. For correct functioning of the quantum repeater, quantum memory is required. However, no reliable and practical quantum memory is available yet.

As an intermediate step, a trusted repeater can be used. The trusted repeater will not entangle end nodes and is used for the quantum key distribution (QKD, see the next section, 3.3.2) only. To imagine how it works, let us consider two parties A and B and a trusted repeater R. Then the key k_{AB} is encrypted with key k_{AR}. The trusted repeater R decrypts k_{AR} to get k_{AB}. At this point, the trusted repeater R knows the key k_{AB}, and A and B have to trust that the key is safe and not under the control of the eavesdropper. Finally, R re-encrypts k_{AB} using the k_{RB} key and sends it to B. This is a technique used in present QKD networks.

The next step, currently tested in experiments, is the measurement device-independent QKD (MDI-QKD) [67, 68]. It is a quantum protocol that not only replaces trusted repeaters (still not quantum, no support of entanglement) with secure repeaters, but also serves as a switch. That means the usual star network topology and infrastructure can start to be built. Note that in the MDI-QKD network, attacks on the central node physically cannot reveal the key nor reveal sensitive information. Later, the central nodes will be replaced by the quantum switch and repeater, and the fully functional quantum information network will be achieved.

Quantum networks will work in parallel with the classical networks, since not all transmitted information needs to be encoded in quantum information. In fact, parallel classical network is required, for instance, for quantum teleportation. Quantum networks can be used for the following applications:

- *Quantum key distribution (QKD)*, a secure transmission of cryptographic key (see Sect. 3.3.2);
- *Quantum information transmission* between quantum computers or quantum computing clusters at large distances or for sharing of remote quantum capabilities;
- *Blind quantum computing* [69, 70] allowing to transmit a quantum algorithm to quantum computer, perform computations and retrieve results without the owner or eavesdropper knowing what the algorithm or result was;
- *Network clock synchronisation* [71], see Sect. 3.4.2;
- *Secure identification* [72] allowing identification without revealing authentication credentials;

- *Quantum position verification* [73] allowing to verify the position of the other party;
- *Distributed quantum computing* [74, 75] for several quantum computers, allowing to compute tasks as one quantum computer;
- *Consensus and agreement tasks* refering to the so-called Byzantine Agreement (problem of decision of group on one output despite the intervention of an adversary). The quantum version [76] can reach agreement in $\mathcal{O}(1)$ complexity in comparison with classical complexity $\mathcal{O}\sqrt{n/\log n}$.
- *Entangled sensor network* [77, 78] allowing improvement in the sensitivity of the sensors and reduction of errors, and evaluating global properties rather than gathering data about specific parts of a system.

A quantum network allows direct secure quantum communication between quantum computers, where quantum data can be directly exchanged. This can be useful for effective redistribution of computing tasks according to individual quantum computer performance, mainly when an enormous task can be divided into smaller tasks. Another case is the quantum cloud, where quantum data can be shared between several quantum computers. Moreover, it is questionable whether it will be possible to build one standalone high-performance quantum computer. The realisation will be more likely via distributed quantum computing [74, 75], where many quantum computers will be connected via the quantum network.

3.3.2 Quantum key distribution

- *Status*: commercially available (with trusted repeaters)
- *Utilisation*: new capability
- *Timeline expectation*: short-term
- *Main challenges*: secure quantum repeater (quantum memory), security certification of the physical hardware

Quantum key distribution (QKD) is the most mature application of quantum communication. The goal is to distribute a secret key between two or more parties for encrypted data distributed via classical channels. Due to the no-cloning theorem, any eavesdropper has to perform a measurement that is detectable by communicating parties.

The dominant classes of protocols are two: one based on BB84 (Bennett-Brassard 1984) protocol [79] and the other the E91 (Ekert 1991) protocol [80]. The dominant BB84 protocol is technically simpler but requires a quantum random number generation (see Sect. 3.3.4), and the providing party has to prepare a key before the distribution. Protocol E91 utilises quantum entanglement that generates the key during the process of distribution, and all parties know the key simultaneously. In this protocol, the quantum random number generator is not required. However, the technical solution with quantum entanglement is more challenging. Both classes of protocols are information-theoretically secure.

Theoretically, the QKD is impenetrable during the transmission. However, the typical vector of attack can focus on the final (receiver/transmitter) or intermediate nodes where the hardware of the software layer can contain vulnerabilities such as bugs in control software, an imperfect single-photon source, parties verification problem, etc. This is an area of very active research. For example, the imperfect physical hardware can be abused by the so-called photon-number-splitting [81], or Trojan-horse [82] attacks. Here, security certification of the hardware and software is necessary and will take time.

Apart from trusted repeaters, the other weak point is the qubit transfer rate, which is too slow to distribute long keys. A new high transfer rate of single-photon sources can resolve the issue.

At present, QKD technology is commercially available as a point-point connection at short distances or by using trusted repeaters at large distances. The trusted repeater can be a space satellite, as was demonstrated by China [62, 63].

3.3.3 Post-quantum cryptography

- *Status*: algorithms ready
- *Utilisation impact*: must have
- *Timeline expectation*: short-term
- *Main challenges*: standardisation, implementation

Post-quantum cryptography (sometimes referred to as quantum-proof, quantum-safe or quantum-resistant cryptography) represents an area of encryption techniques that should resist future quantum computer attacks. Presently, this is not true for most of the asymmetric encryption that uses public-key technology. On the other hand, most of the symmetric cryptographic algorithms and hash functions are considered relatively secure against attacks by quantum computers [83]. Nevertheless, doubling the symmetric key length is recommended [39].

Now, several approaches are considered as quantum-resistant. For example, lattice-based cryptography [84], supersingular elliptic curve isogeny cryptography [85], hash-based [86] cryptography, multivariate-based [87] cryptography, code-based cryptography [88] and symmetric key quantum resistance.

Unlike QKD, all these algorithms are not provably secure from a mathematical perspective. Therefore, within the process of standardisation, all these algorithms are rigorously tested and analysed, including the implementation. There is no worst case where a quantum-resistant algorithm with bugs in implementation could be cracked by a classical computer [89]. The most followed standardisation process is the one by the U.S. National Institute of Standards and Technology (NIST). The standardisation process is in the third round [90], with three finalists (algorithms based on the lattice, code-based and multivariate) and several alternate candidates. The NIST standardisation process is expected to conclude in 2023-24. Regardless, more and more commercial vendors are offering new quantum-resistant encryption solutions now.

3.3.4 Quantum random number generator

- *Status*: commercially available
- *Utilisation impact*: new capability (truly random number generation)
- *Timeline expectation*: short-term
- *Main challenges*: increasing bit rate

Random number generators (RNG) are essential for many applications such as Monte Carlo simulations and integration, crypto operations, statistics and computer games. Nevertheless, the RNG in a classical computer, since it acts deterministically, is not truly random, and is called pseudo-random number generation. However, for many applications, the pseudo-RNG is sufficient.

On the other hand, generating strong keys is the cornerstone of security, which can be achieved only by truly random RNG. One solution is a quantum random number gener-

ator (QRNG) that is hardware-based. Moreover, QRNG is a crucial part of BB84-based QKD protocols, to be provably secure.

QRNG can be used for any cryptography and makes all cryptography better. One of the advantages of QRNG is that it can be verified and certificated [91], unlike any other RNG.

3.4 Quantum sensing and metrology

Quantum sensing and metrology is the most mature quantum technology area, which improves timing, sensing or imaging. For example, atomic clocks from the first quantum revolution have been part of the Global Positioning System (GPS) for almost half a century. The current quantum clocks are coming up with much higher time measurement precision.

Quantum sensing stands for all quantum technologies that measure various physical variables such as external magnetic or electric fields, gravity gradient, acceleration and rotation. Quantum sensors can produce very precise information about an electric signal, magnetic anomalies and for inertial navigation.

Quantum imaging is a subfield of quantum optics exploiting photon correlations, allowing suppression of noise and increasing the resolution of the imagined object. Quantum imaging protocols are considered for quantum radar, detecting objects in the optically impermeable environment, and in medical imaging.

Quantum sensing and metrology technology relies on one or more of the following features: quantum energy levels, quantum coherence and quantum entanglement [92]. Individual quantum sensors have various metrics that vary with the application. The common metrics are: sensitivity (a signal that gives unity signal-to-noise ratio after 1 second of integration time), dynamic range (minimal and maximal detectable signal), sampling rate (how often the signal is sampled), operating temperature, etc. Derived key metrics include, for example, spatial resolution at a certain distance and the time required to achieve a specified sensitivity. The typical measure quantities are magnetic and electric fields, rotation, times, force, temperature and photon counting.

3.4.1 Quantum electric, magnetic and inertial forces sensing

- *Status*: laboratory prototypes
- *Utilisation impact*: precision, new capability
- *Timeline expectation*: short- to long-term
- *Main challenges*: miniaturisation, cooling

Many sensing quantum technologies are universal and can measure various physical quantities. A detailed description of each technology is outside the scope of this report; however, a basic overview is provided. Many applications include various quantum technologies. For example, quantum inertial navigation consists of three types of sensing: acceleration, rotation and time. In general, precise quantum-based timing is required for many applications, not only for quantum technologies. For quantum timing, see Sect. 3.4.2. The most promising technologies are: atomic vapour, cold-atom interferometry, nitrogen-vacancy centres, superconducting circuits and trapped ions.

Cold-atom interferometry (measured quantities: magnetic field, inertial forces, time). Atoms cooled at very low temperatures exhibit wave-like behaviour and are sensitive to all forces that interact with their mass. The changes are observed in the interference pattern [5, 92, 93]. The particular realisation can be in the form of Raman atom interferom-

etry, atom Bloch oscillation or others [94–96]. For example, in gravimetry, the quantum-based gravimeter has the potential to reach about several orders of magnitude higher precision [5] than the best classical counterparts. Such a precise gravimeter allows very detailed mapping of the Earth's surface and underground with a resolution at the centimetre level. Regarding inertial navigation, the shaken lattice interferometry has the potential to overcome shortcomings of the state-of-the-art atom interferometry techniques and can work as accelerometer and gyroscope at once [97]. Several challenges remain. Some of the biggest challenges are the integration of the quantum sensor into one quantum inertial measurement unit, miniaturisation of laser cooling apparatus used for cooling down atoms and simultaneously maintaining the coherency (suppression of the interaction with the noisy environment), or the dynamic range of the cold atom sensor outside the laboratory. However, significant advances also can be found in this area, e.g. [98]. For a review see [99].

Trapped ions (measured quantities: electric and magnetic field, inertial forces, time). Trapped ions are one of the most universal sensing platforms [100–102]. Well-controlled trapped ions form a crystal with quantised modes of motion. Any disturbance can be measured through the transition between these modes. A single trapped ion can serve as a precise measurement of time or as a qubit in a quantum computer. For inertial navigation, the optical lattice technology of trapped cold atoms in 1, 2 and 3-dimensional arrays potentially offers a sub-cm level in size. Besides allowing measurement of gravitational and inertial parameters, it can measure Casimir or van der Waals forces. More recently, using quantum-entangled trapped ions, measurement of electric fields has reached a sensitivity of ~ 240 nV/ms^{-1} [103], which is several orders of magnitude better than the classical counterpart.

Nitrogen-vacancy (NV) centres (measured quantities: electric and magnetic field, rotation, temperature, pressure). Nitrogen-vacancy centre in a diamond crystal works as an electron spin qubit that couples with external magnetic fields. In addition, negatively charged NV centres using Berry's phase can measure rotation. In general, NV centre-based sensors offer high sensitivity, cheap production and operation in a wide range of conditions [92, 104, 105]. In particular, NV centre-based technology can also work at room temperature and higher. A novel proposed 3D design allows to sense all three components of magnetism, acceleration, velocity, rotation or gravitation simultaneously [106]. The strengths of NV centres in diamond-based sensing are spatial resolution and sensitivity. On the other hand, the challenge is choosing, implementing and manufacturing individual NV centres or their ensembles. In the case of electric field sensing, it is challenging to define a sensitivity [107].

Superconducting circuits (measured quantities: electric and magnetic field). The technology of superconducting circuits based on the Josephson effect describes the quantum tunnelling effect between two superconductors [92]. This technology allows manufacturing a quantum system at the macroscopic scale and can be controlled effectively with microwave signals. The superconducting quantum interference device (SQUID) is one of the best magnetometric sensors. However, the disadvantage is the requirement of cryogenics. Note that for the measurement of magnetic-field variations smaller than the geomagnetic noise, the preferred design is based on an array of sensors to cancel the spatial-correlation with applications, such as in medical and biomedical applications (e.g. MRI or molecule

tagging). The recent development shows that the superconducting qubits used in quantum computers can be used to measure electric and magnetic fields [92] as well.

Atomic vapour (measured quantities: magnetic field, rotation, time). Spin-polarised high-density atomic vapour undergoes state transition under external magnetic field which can be measured optically [92, 108, 109]. An advantage is a deployment at room temperature. The atomic vapour is suitable for rotation sensing, known as the Atomic Spin Gyroscopes (AGS). AGS can be chip-scale [5]. For comparison, the best classical rotation sensors are very precise (e.g. ring laser gyroscope). The expected quantum sensor will be about twice as precise. However, the mentioned best classical gyroscope has a size of 4×4 m, which is impractical [110]. Atomic vapour cell magnetometers based on atomic ensembles have the potential to outperform SQUID magnetometers and work at room temperature [92].

3.4.2 Quantum clocks

- *Status*: laboratory prototypes
- *Utilisation impact*: precision
- *Timeline expectation*: short- to mid-term
- *Main challenges*: miniaturisation

Atomic clocks have been with us for several decades; for example, as part of GPS satellites. The current atomic clocks are based on atomic physics, where the electromagnetic emissions from electrons when changing energy level utilise a 'tick'. As such, the atomic clock is a very mature technology. Today, the atomic clocks based on atomic fountain or thermal atomic beam and magnetic state selection principles can reach a relative uncertainty $\sim 10^{-15} - 10^{-16}$ [111], or state-of-the-art chip-size atomic clocks have uncertainty 2×10^{-12} [5].

The second quantum revolution comes with new principles for atomic or quantum clocks. Quantum logic clock is based on single-ion, a technology related to trapped-ion qubit for quantum computing [101]. Quantum logic clock was the first with clock uncertainty below 10^{-18} [112]. Quantum clocks can also benefit from quantum entanglement [113].

Later, the quantum logic clock was superseded by experimental optical lattice clocks. Note that the current atomic clocks work with microwave frequencies, i.e. the transition between energy levels emits a microwave photon. The measurement of level transition with the emitted photon in optical frequencies is harder to achieve, although it offers better performance. Optical clocks are still in development, with systems being based on: single ions isolated in an ion trap, neutral atoms trapped in an optical lattice and atoms packed in a 3D quantum gas optical lattice. The 3D quantum gas optical lattice clocks in particular have demonstrated frequency precision 2.5×10^{-19} [114]. Recently, it was demonstrated that quantum entanglement could enhance the clock stability [115].

Another research focuses on vapour-cell (or gas-cell) atomic clock that provides chip-size realisation [116]; solid-state (for instance, the NV centre in diamond) clock [117]; or nuclear clock with a similar principle as microwave or optical atomic clock, except that it uses nuclear transition instead of electron transition in an atom's shell [118], with the potential for unprecedented performance, outstripping atomic optical clocks [119].

Various clock technologies have their own challenges, such as precise frequency comb, laser system for control and cooling down and black body radiation shift (in the case of op-

tical clocks). Also, miniaturisation usually comes at the cost of lower frequency precision. Another common type of challenge is the synchronisation of those clocks.

Precise timing is essential for many technologies, such as satellite navigation, space systems, precise measurement, telecommunication, defence, network synchronisation, finance industry, energy grid control, and in almost all industrial control systems. However, very precise timing is crucial for quantum technologies, especially for quantum sensing and imaging. For instance, a very high precision clock allows new measurements, such as gravity potential measurement down to the centimetre level at the Earth's surface or searching for new physics.

3.4.3 Quantum RF antenna

- *Status*: laboratory prototypes
- *Utilisation*: effectiveness
- *Timeline expectation*: short- to mid-term
- *Main challenges*: miniaturisation, cooling

Radio frequency (RF) antennas serve as receivers or transmitters of various signals. They can be simple dipole antennas to complex AESA[9] modules. Their size limitation is bounded by the wavelength of the produced or received signal. For example, a 3 GHz signal has a wavelength of ~ 10 cm and the size of the antenna should be no less than approximately 1/3 of this wavelength. This is called the Chu–Harrington limit [120, 121].

Rydberg atoms' technology allows breaking this limit and having an antenna of the size of a few micrometres independently on the receiving signal wavelength. Rydberg atoms are highly excited atoms with a correspondingly large electric dipole moment, and therefore high sensitivity to external electric field [122, 123]. Note that Rydberg atoms-based antenna can only receive a signal.

The recent prototypes of Rydberg atoms-based analyser were demonstrated for frequencies 0 to 20 GHz for AM or FM radio, WiFi and Bluetooth signals [124]. The combination of more antennas can detect the angle-of-arrival of the signal [125]. At the laboratory level, Rydberg atoms technology is available commercially.

Quantum RF receiver as a single cell (for targeted frequency, narrow bandwidth) or arrayed sensor (broad frequency span) can find its applications in navigation, active imaging (radar), telecommunications, media receiver or passive THz imaging.

3.4.4 Quantum imaging systems

- *Status*: laboratory prototypes and proof-of-concept verifications
- *Utilisation*: new capability
- *Timeline expectation*: short- to long term
- *Main challenges*: improving resolution, high rate single-photon sources

Quantum imaging systems are a wide area covering 3D quantum cameras, behind-the-corner cameras, low brightness imaging and quantum radar or lidar (for quantum radar, see Sect. 3.4.5).

SPAD (Single Photon Avalanche Detectors) Array is a very sensitive single-photon detector connected with a pulsed illumination source that can measure the time-of-flight

[9] AESA (active electronically scanned array) module consists of an array of small transmitters and receivers that are controlled by a computer. Simply put, each cell of AESA can behave as an independent radar module.

from source to an object and hence the range of the object. Then, putting SPAD into an array can work as a 3D camera. SPAD works with the optical spectrum with extension developed to the near-infrared spectrum.

SPAD array can be used to detect objects out of the line of sight, too (e.g. hidden behind the corner of a wall). The idea is based on laser and camera cooperation, where the laser sends a pulse in front (e.g. a spot on the floor) of the SPAD camera. From the spot, the laser pulse will scatter in all directions, including behind the corner, where the photons can be reflected to the spot in front of the SPAD camera and then to the camera. SPAD is sensitive enough to detect such a three-scattered signal [126].

Quantum ghost imaging [127–129], also known as coincidence imaging or two-photon imaging, is a technique that allows imaging an object that is out of the line of sight of the camera. In the source, two entangled photons are created, each of a different frequency. The one in the optical frequency is recorded directly by a high-resolution photon-counting camera. The second photon having a different frequency (e.g. the infrared) is sent toward the object. The reflected photon is detected by a single-photon detector (the so-called 'bucket' detector). The image is then created from the correlations between both photons. The ghost imaging protocol was demonstrated without quantum entanglement, too (using classical correlation), although with worse resolution.

Such a schema allows imaging an object at extremely low light levels. Also, infrared light can better penetrate some environments with a better signal-to-noise ratio (SNR) [130]. Ghost imaging experiments that use x-ray or ultra-relativistic electrons were demonstrated recently [131, 132].

Sub-shot-noise imaging [133] is another quantum optics schema allowing detection of a weak absorption object with a signal below the shot noise. Shot noise is the result of fluctuations in the detected number of photons. For example, the shot noise is the limit for lasers. This limit can be overcome using correlated photons. The detection of one 'herald' or 'ancilla' photon signifies the presence of the correlated photon that probes the object or environment.

Quantum Illumination (QI) [134] is a quantum protocol to detect a target using two correlated (entangled) photons. One photon, called the 'idler', is kept. The other, called the 'signal' photon, is sent toward the target and reflected, and both photons are measured. The advantage of this protocol remains even when the entanglement is destroyed by a lossy and noisy environment. QI protocol is one of those mainly adapted for the quantum radar, but it can also be applied to medical imaging or quantum communication.

3.4.5 Quantum radar technology

- *Status*: laboratory prototypes and proof-of-concept verification
- *Utilisation*: new capability
- *Timeline expectation*: long-term and more
- *Main challenges*: high rate single-photon source, quantum microwave technology

Quantum radar, in principle, works similarly to classical radar, in the sense that a signal has to be sent toward the target, and the radar system needs to wait for the reflected signal. Nevertheless, theoretically improved precision and new capabilities can be achieved by quantum mechanical approaching.

There are several protocols considered for quantum radar, such as interferometric quantum radar [135], quantum illumination (QI) [134], hybrid quantum radar [136, 137] or

Maccone-Ren quantum radar [138]. None of the mentioned protocols is perfect. Interferometric quantum radar, for example, is too sensitive to noise and requires quantum entanglement preservation. QI is an ideal protocol for a noisy environment and is even laboratory-verified for microwave spectrum [139], but it requires knowledge of the distance to the target, and such as it has no ranging function. Nevertheless, the QI-based approach to quantum target ranging is under development [140]. This ranging problem is also solved by the hybrid quantum radar, but at the expense of sensitivity. The Maccone-Ren protocol has QI properties and ranging function, but it is only a theoretical concept so far.

The biggest challenge common to all protocols is the high rate of generation of entangled photons in (not only) a microwave regime. The quantum version of the radar equation [141] still holds the dominant term $1/R^4$, where R is the radar–target distance. As a result, the number of demanded entangled photons (modes) is several orders of magnitude higher than is available currently [142]. In a sense, quantum radar is similar to noise radars and shares many properties such as the probability of interception, low probability of detection, efficient spectrum sharing, etc., see [137] and references therein.

Another related challenge is target finding. Theoretical work [143] shows that quantum entanglement can outperform any classical strategy in finding the unknown position of the target. Moreover, the presented method can work as a quantum-enhanced frequency scanner for the fixed target range.

3.4.6 Other sensors and technology

- *Status*: laboratory prototypes
- *Utilisation*: new capability (e.g. chemical and precise acoustic detection)
- *Timeline expectation*: short- to medium term
- *Main challenges*: improving resolution

Quantum technologies can be used for ultra-precise sound sensing up to the level of a phonon, a quasiparticle quantising sound waves in solid matter [144, 145], using photoacoustic detection. Precise detection of acoustic waves is essential for many applications, including medical diagnostics, sonar, navigation, trace gas sensing and industrial processes [146, 147].

Photoacoustic detection can be combined with quantum cascade laser and used for gas or general chemical detection. Quantum cascade laser (QCL) is yet a mature technology [148]. QCL is a semiconductor laser that emits in the mid- and long-wave IR bands and, as with many other quantum technologies, requires cooling far below –70°C. However, recent development allows chip-level implementation working at around –23°C, which can be achieved by a portable cooling system [149].

4 Quantum technology in defence

Military technologies have more demanding requirements than industrial or public applications. This requires greater caution, considering possible deployment on the battlefield. Section 5 presents various possible military applications with different TRLs, time expectations and with multiple risks of realisation.

It will be simpler and less risky for technologies that are easily implemented and fit into current technologies, such as quantum sensors where, simply put, we can replace a classical sensor with a quantum sensor.

On the contrary, QKD is an example of a technology that is already commercially available but is challenging to deploy. A lot of new hardware, systems and interoperability with current communication systems are needed. Thus, this technology carries more significant risks in terms of military deployment.

We can expect an advantage in lowering SWaP and scaling up quantum computers and quantum networks in the long term. That will make the deployment easier and probably necessary if the nation/army wants to compete with other nations/armies with edge (quantum) technologies.

4.1 Quantum strategy

The future users of military quantum technologies will have to think carefully about whether, where and when to invest time and resources. The goal of the defence forces is not to develop military technology but usually only to specify requirements and their acquisition. However, they can participate significantly in development, especially if they are the end user.

As a foundation, it is ideal to have a national quantum ecosystem in place composed of industry and academic institutions. Such an ecosystem should be supported generally at the government level, i.e. having a national quantum plan, but should also be motivated to develop technologies for the defence sector. This can be achieved through appropriate grant funding and even various thematic challenges, in which individuals and startups can participate and perhaps bring new disruptive ideas and solutions. This will naturally lead to closer cooperation with industry and academia. The quantum industry is quite interesting, where there is a great deal of cooperation between academia and industry.

The first step is to establish a quantum technology roadmap or quantum strategy. The roadmap/strategy should specify all the next steps, from identifying disruptive quantum solutions, market survey, technology and risk assessment and development itself to prototype testing and eventually solution deployment. The roadmap or quantum strategy can consist of three parts:

1. Identification,
2. Development,
3. Implementation and deployment.

The most critical part is the identification of the most advantageous and disruptive quantum technologies for the considered warfare domains. This step also includes the technological and scientific assessment to balance technological risk (limited deployability, performance below expectations, or impossibility of transfer from the laboratory to the battlefield) versus the potential advantage of individual quantum technologies. This process of identification should be repeated in cycles in order to react relatively quickly to new discoveries and disruptive solutions. It is important to remember that many applications are yet to be identified or discovered.

The next step is the usual process of research and development (R&D). The R&D should be sufficiently supported financially, but also with minimal bureaucratic obstacles. It should involve fast development cycles with close interaction with the end user of the military technology (specifications and performance consultations, prototype testing, preparing for certifications, ...). At the end of this phase, the new system at the initial operating capability should be ready.

The last step is to reach full operational capability, including modification or creation of new military doctrines, preparing new military scenarios, strategies and tactics fully exploiting the quantum advantage.

The final note pertains to the Identification phase. Here, the decision maker needs to also assume the long-term perspective. So far, many quantum technologies have been considered individually: sensors, QKD, quantum computing, etc. However, the long-term vision considers the interconnection of quantum sensors and quantum computing via the quantum network. Here, the theoretical and experimental works demonstrate additional quantum advantage exploiting quantum entangled sensors and computers [77, 78]. More similar applications may yet be discovered or invented. This is important to consider when the optical-fibre/quantum networks are being built. Later, the current elements such as trusted repeater can be replaced by fully quantum repeaters and switches, allowing to reach the full potential of the quantum network.

4.2 TRL and time horizon

As has been mentioned several times, various quantum technologies are at different TRL, varying from 1 to 8. The TRL variation and time horizon expectations are even more complex when considering various applications and deployment platforms, especially for military purposes. Some TRL and time horizon estimates were provided in [150]. However, some estimations, such as quantum precision navigation at TRL 6, seem too optimistic based on what is described in this report.

Here, we provide our own TRL and expected time horizon in Table 1, which correspond to the findings of this work.

The reader can compare these with other timelines in [11, 150].

The actual military deployment can take some time to overcome all technological obstacles and meet military requirements. Take, for example, the quantum gravimeter for undeground scanning. The first generation will likely be deployed as a static sensor placed on a truck, and the range/spatial resolution will be rather low. In time, the next generation will improve sensitivity and spatial resolution. Along with reduction of SWaP, the sensor will be capable of being placed aboard an aircraft, and later on a drone and maybe on an LEO satellite. However, it is also possible that the sensor's limits will be reached earlier, resulting in deployment becoming impossible, e.g. on a drone or LEO satellite.

Table 1 TRL and time horizon expectations. These expectation reflect general TRL rather than just military TRL. Note that various quantum technologies are at different TRL within the same application

Technology	TRL	Horizon
Quantum computer (annealer)	4-5 (5-6)	2030
QKD (satellite)	7-8 (6-7)	2025 (2030)
Post-quantum cryptography	7-8	2025
Quantum communication network	1-3	2030-2035
Quantum inertial navigation	4-5	2025-2030
Quantum clocks	4-6	2030
Quantum radar	1-2	none
Quantum RF antenna	4	2025-2030
Quantum magnetic and gravity sensing	5-6	2025
Quantum imaging	5	2025-2030

4.3 Quantum technology countermeasures

A standalone section on quantum technology countermeasures is warranted, although this topic will be touched upon, e.g. in Sect. 5.6 about the quantum analogy of the classical electronic warfare. This topic is less studied, and few texts deal with this subject; besides, a detailed description is beyond the scope of this report.

Briefly, this topic refers to the methods and techniques of spoofing, disabling or destroying quantum technologies, whether it is quantum computers, quantum networks or quantum sensors and imaging systems. Quantum technologies exploit the quantum-physical properties of individual quanta. As such, they are very susceptible to interference and noise from the environment, and so can potentially be spoofed or paralysed. Especially in relation to quantum networks and in particular to QKD, we speak about quantum hacking [151–155], which has developed hand in hand with QKD itself.

Authors and decision makers on quantum strategy should keep in mind that when quantum technologies are deployed in the military field, various countermeasures will very likely emerge sooner or later. What is currently unknown is the possible effectiveness of quantum technology countermeasures and their impact.

5 Quantum technology military applications

Quantum technologies have the potential to significantly affect many areas of human activity. This is especially true for the defence sector. Quantum technologies can impact all the domains of modern warfare. The second quantum revolution will improve sensitivity and efficiency, and introduce new capabilities and sharpen modern warfare techniques rather than lead to new types of weapons.

The following text maps the conceivable quantum technology applications for military, security, space and intelligence in different aspects of modern warfare, as sketched in Fig. 1. It also mentions the industrial applications which may suggest quantum technolo-

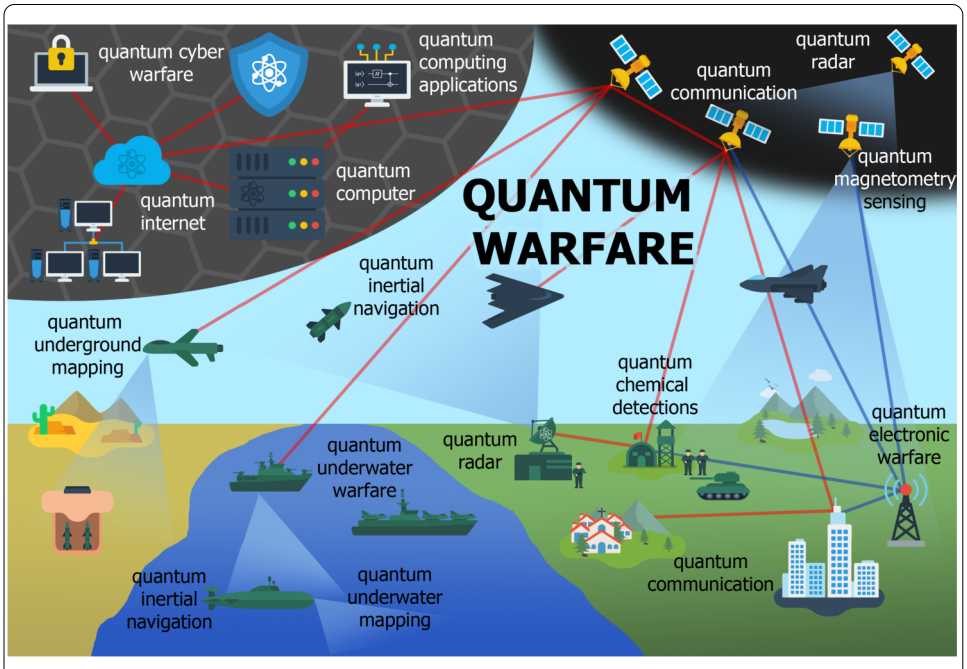

Figure 1 Sketch of quantum warfare utilising various quantum technology systems

gies' capabilities and performances, especially when no public information on military applications is available.

It is important to notice that many applications are still more theoretical than realistic. The significant quantum advancement achieved in the laboratory does not always result in similar progress outside the laboratory. The transfer from laboratory to practical deployment involves other aspects too, such as portability, sensitivity, resolution, speed, robustness, low SWaP (size, weight and power) and cost, apart from a working laboratory prototype. The practicality and cost-effectiveness of quantum technologies will determine whether particular quantum technologies are manufactured and deployed.

The integration of quantum technology into a military platform is even more challenging. Apart from quantum computers that will mostly be located at data centres similarly as for civil use, the integration and deployment of quantum sensing, imaging and networks faces several challenges posed by the increased demands of military use (in comparison with civil/industry or scientific requirements). For example, the military level requirement of precise navigation necessitates fast measurement rates that can be quite limiting for the current quantum inertial sensors. There are more examples, and probably more are yet to come.

Moreover, this area is still very young, and new technological surprises, both in a bad and a good sense, could impose other quantum advantages or disadvantages.

5.1 Quantum cybersecurity

Key points:

- Necessity of quantum crypto-agility implementation.
- Operations that want to take advantage of Shor's algorithm should start to collect the data of interest before the quantum-safe encryption is deployed.
- The implementation of QKD needs to be carefully considered.
- In QKD, the endpoints will be the weakest part of the system.

Quantum advantage in cyber warfare can provide new, but on the one hand very effective (with exponential speedup), vectors of attack on the current asymmetric encryptions (based on integer factorisation, the discrete logarithm or the elliptic-curve discrete logarithm problem) and, theoretically, on symmetric encryption [90, 156]. On the other side are new quantum-resilient encryption algorithms and approaches, as well as quantum key distribution. For an overview, see, for example, [157–160].

The current trend also is the development and employment of machine learning or artificial intelligence for cyber warfare [161]. For more details on the quantum opportunities, see Sect. 5.2.

5.1.1 Quantum defence capabilities

The post-quantum cryptography implementation is the 'must-have' technology that should be carried out as soon as possible. The risk that hostile intelligence is gathering encrypted data with the expectation of future decryption using the power of quantum computers is real, high and present [162]. This applies to military, intelligence and government sectors as well as to industry or academia where secrets and confidential data are exchanged or stored. The current trend is to start preparing the infrastructure for implementing quantum crypto-agility when the certified (standardised) post-quantum cryptography becomes ready to deploy [90, 156].

New quantum-resilient algorithms can offer not only a new mathematical approach difficult enough even for quantum computers, but also a new paradigm of working with encrypted data. For instance, fully homomorphic encryption (FHE) allows the data to never get decrypted—even if they are being processed [163]. Although the security applications, such as for genomic data, medical records or financial information, are the most mentioned, applications for intelligence, military or government are evident, too. As such, FHE is a good candidate for cloud-based quantum computing to ensure secure cloud quantum computation [164].

Note that post-quantum cryptography should be implemented in the Internet of Things (IoT), or the Internet of Military Things (IoMT) [165], as a rapidly growing sector with many potential security breaches. For an overview of post-quantum cryptography for IoT, see [166].

Quantum key distribution (QKD) [160, 167, 168] is another new capability that allows safe encryption key exchange where the security is mathematically proven. Although it is impossible to eavesdrop on the quantum carrier of the quantum data (key), the weaknesses can be found at the end nodes and trusted repeaters, due to imperfect hardware or software implementation. Another question is the cost, considering the quantum data throughput, security and non-quantum alternatives independently if the solution is optical fibre-based or utilising quantum satellites. The QKD solution seems to be preferred in EU [169], while the post-quantum encryption solution finds favour in US [170].

The last note refers to quantum random number generators. QRNG increases security [171] and denies attacks on pseudorandom number generators [172].

5.1.2 Quantum attack capabilities

With Shor's algorithm-based quantum cryptoanalysis of Public key encryption (PKE)—for instance, RSA, DH, ECC—the attacker can decrypt the encrypted data collected earlier. There is no precise forecast when the so-called 'Q-Day', the day when a quantum computer breaks the 2048-bit RSA encryption, will happen. However, the general opinion is it will take about 10–15 years (based on a survey in 2017) [173]. A similar threat applies to most message authentication codes (MAC) and authenticated encryption with associated data (AEAD), such as HMAC-CBC and AES-GCM, because of Simon's algorithm and superposition queries.

One has to assume that such offensive operations already exist or that intense research is being done. In 10 years, most sensitive communication or subjects of interest will be using the post-quantum cryptography or QKD implemented in the next six years. That means by the time a quantum computer able to crack PKE becomes available, most of the security-sensitive data will be using a quantum-safe solution.

In theory, Grover's algorithm weakens the symmetric key encryption algorithms; for example, DES and AES. However, the quantum computing, and in particular quantum memory, requirements are so huge that it seems to be unfeasible in the next few decades [174].

Another vector of attack uses the classical hacking methods of classical computers that will remain behind quantum technologies. In general, quantum technology is a technologically young sector where plenty of new quantum system control software is being developed. The new software and the hardware tend to have more bugs and security breaches. For example, the current QKD quantum satellites working as trusted repeaters

controlled by a classical computer can be an ideal target for a cyber attack. Moreover, specific physical-based vectors of attack against quantum networks (e.g. QKD) are the subject of active research [175], such as photon-number-splitting [81] or the Trojan-horse attack [82], and future surprises cannot be excluded. For an overview of quantum hacking, see, e.g. [157].

5.2 Quantum computing capabilities

Key points:

- Quantum computing capabilities will increase with the number of logical qubits.
- Most likely, quantum computing will be used as part of a hybrid cloud.
- Small, embedded quantum computing systems are desirable for direct quantum data processing.
- General use for quantum optimisations, ML/AI enhancements and faster numerical simulations.

Quantum computing will introduce new capabilities to the current classical computing services, helping with computational problems of high complexity. Further, besides the quantum simulations described above, quantum computing covers quantum optimisations, machine learning and artificial intelligence (ML/AI) improvement, quantum data analysis, and faster numerical modelling [11, 24]. The military problems that could be solved with near-term quantum computers were presented in [10]. They are: Battlefield or war simulations; Analysis of radio frequency spectrum; Logistics management; Supply chain optimisation; Energy management; and Predictive maintenance.

To get the most effective results, future quantum computing implementation will be in computing farms along with classical computers, which will create a hybrid system. A hybrid quantum-classical operating system will analyse the tasks to be computed using ML/AI, and split individual computations into resources such as CPU, GPU, FPGA,[10] or quantum processor (QPU), where the best and fastest result can be obtained.

A small, embedded quantum computer that could be placed, for example, in an autonomous vehicle or mobile command centre is questionable. The current most advanced qubit designs need cryogenic cooling. Therefore, more efforts should be focused on the other qubit designs as photonic, spin or NV centres that can work at room temperature. The embedded quantum chip could perform simple analytical tasks or serve for simple operations related to quantum network applications where a straightforward quantum data process is desired. Nevertheless, the machine learning and model optimisation of autonomous systems and robotics can also benefit from 'large' quantum computers.

Quantum computing is likely to be efficient in optimisation problems [10, 176, 177]. In the military sector, examples of quantum optimisations could be logistics for overseas operations and deployment, mission planning, war games, systems validation and verification, new vehicles' design and their attributes such as stealth or agility. At the top will be an application for enhanced decision making, supporting military operations and functions through quantum information science, including predictive analytics and ML/AI [178]. Specifically, quantum annealers have proven themselves in verifying and validating complex systems' software code [179, 180].

[10] Central Processing Unit; Graphics Processing Unit; Field-Programmable Gate Array

Quantum computers are expected to play a significant role in Command and Control (C2) systems. The role of C2 systems is to analyse and present situational awareness or assist with planning and monitoring, including simulation of various possible scenarios to provide the best conditions for the best decision. Quantum computers can improve and speed up the scenario simulations or process and analyse the Big Data from ISR (Intelligence, Surveillance and Reconnaissance) for enhanced situational awareness. This also includes the involvement of quantum-enhanced machine learning and quantum sensors and imaging.

Quantum information processing will probably be essential for Intelligence, Surveillance, and Reconnaissance (ISR) or situational awareness. ISR will benefit from quantum computing, which offers a considerable boost to the ability to filter, decode, correlate and identify features in signals and images captured by ISR. Quantum image processing in particular is an area of extensive interest and development. It is expected that in the near term situational awareness and understanding can benefit from quantum image analysis and pattern detection utilising neural networks [13].

Quantum computing will enhance classical machine learning and artificial intelligence [54], including for defence applications [178]. Here, quantum computing will surely not be practical to carry out the complete machine learning process. Nevertheless, quantum computing can improve ML/AI machinery (e.g. quantum sampling, linear algebra, quantum neural networks). A recent study [181] shows that quantum ML provides an advantage just for some kernels fitting particular problems. Quantum computing can possibly enhance, in principle, most classical ML/AI applications in defence; for example, automating cyber operations, algorithmic targeting, situation awareness and understanding and automated mission planning [182, 183]. The most immediate application of quantum ML/AI is probably quantum data; for instance, data produced by quantum sensing or measuring apparatus [55]. Actual applicability will grow with quantum computer resources, and in eight years, quantum ML/AI can be one of the important quantum computing applications [184]. Such applicability can be accelerated by hybrid classical-quantum machine learning where tensor network models could be implemented on small near-term quantum devices [185].

Quantum computers, through quantum neural networks, can be expected to provide superior pattern recognition and higher speed. This may be essential, for instance, in biomimetic cyber defence systems that protect networks, analogously to the immune systems of biological organisms [13].

Besides, through faster linear algebra (see 3.2.5), quantum computing has the potential to improve the current numerical linear equation-based numerical modelling in the defence sector, such as war games simulations, radar cross section calculations, stealth design modelling, etc.

In the long term, the quantum systems can enable Network Quantum Enabled Capability (NQEC) [13]. NQEC is a futuristic system that allows communication and sharing information across the network between individual units and the commander to respond quickly to battlefield developments and for coordination. Quantum enhancement can bring secured communication, enhanced situational awareness and understanding, remote quantum sensor output fusing and processing, and improved C2.

5.3 Quantum communication network

Key points:

- Various security applications (e.g. QKD, identification and authentication, digital signatures).
- The adoption of security applications will happen as quickly as all new technology security aspects are explored, carefully.
- Quantum clock synchronisation allows utilising higher precision quantum clocks.
- Quantum internet is the most effective way of communication between quantum computers and/or quantum clouds.

Quantum internet stands for a quantum network with various services [186] which have significant, and not only security, implications. However, many progressive quantum communication network applications require quantum entanglement; that is, they require quantum repeater and quantum switch. Recall that the trusted repeaters can be used for QKD only (see Sect. 3.3.1). Future combinations of optical fibre and free-space channels will interconnect various end nodes such as drones, planes, ships, vehicles, soldiers, command centres, etc.

5.3.1 Security applications

Quantum key distribution is one of the most matured quantum network applications. This technology is going to be interesting for the defence sector later, when long-distance communication using MDI-QKD or quantum repeaters becomes possible. Currently, basic commercial technology that uses trusted repeaters is available. These pioneers can serve as a model of how quantum technologies can be employed. Here, QKD companies promote the technology as the most secure, and more and more use cases appear, especially in the financial and healthcare sectors. On the other hand, the numerous recommendation reports and authorities are more circumspect; for example, the UK National Cyber Security Centre [187] that does not endorse QKD for any government or military applications in its current state.

Apart from QKD, which distributes the key only, the quantum network could be used for quantum-secure direct communication (QSDC) [188–191] between space, special forces, air, navy and land assets. Here, the direct messages encrypted in quantum data take advantage of security similar to QKD. One obstacle could be a low qubit rate, which will only allow sending simple messages and not audiovisual and complex telemetry data. In that case, the network switch to the QKD protocol for distributing the key and the encrypted data will be distributed over classical channels. Other protocols such as quantum dialogue [192] and quantum direct secret sharing [193] aim to use the quantum network for provable secure communications as QSDC. Note that QKD and QSDC are considered to be a native part of 6G wireless communication networks and discussed accordingly in [194].

Another significant contribution of the quantum approach to security is the quantum digital signature (QDS) [195]. It is the quantum mechanical equivalent of a classical digital signature. QDS provides security against tampering of a message after a sender has signed the message.

Next, quantum secure identification exploits quantum features allowing identification without revealing authentication credentials [72]. Non-quantum identification is based on the exchange of login and password or cryptographic keys, which allows intruders to at least guess who has tried to authenticate.

The other application is position-based quantum cryptography [196, 197]. Position-based quantum cryptography can offer more secure communication, where the accessed

information will be available only from a particular geographical position, such as communication with military satellites only from particular military bases. Position-based quantum cryptography can also provide secure communication when the geographical position of a party is its only credential.

5.3.2 Technical applications

Quantum network will perform network clock synchronisation [71, 198] that is already a major topic in classical digital networks. Clock synchronisation aims to coordinate otherwise independent clocks, especially atomic clocks (e.g. in GPS) and local digital clocks (e.g. in digital computers). A quantum network that uses quantum entanglement will reach even more accurate synchronisation, especially when quantum clocks come to be deployed (for Time standards and frequency transfer see Sect. 5.4). Otherwise, the high precision of quantum clocks would be utilised locally only. Precise clock synchronisation is essential for the cooperation of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems for accurate synchronisation of various data and actions across radar, electronic warfare, command centres, weapon systems, etc.

A short note is dedicated to blind quantum computing [69, 70]. This class of quantum protocols allows for a quantum program to run on a remote quantum computer or quantum computing cloud and retrieve results without the owner knowing what the algorithm or result was. This is valuable when secret computation is needed (e.g. military operation planning or new weapon technology design) and no own quantum computer capability is available.

Distributed quantum computing via the quantum network—see Sect. 3.3.1—will be important for the military and governmental actors owning quantum computers, to build high-performance quantum computing services or quantum cloud.

A quantum network capable of distributing entanglement can integrate and entangle quantum sensors [77] for the purpose of improving the sensitivity of the sensors, reducing errors, and most importantly to perform a global measurement. That provides an advantage in cases where the parameters of interest are global properties of the entire network; for example, when a signal's angle of arrival needs measurement from three sensors, where each measures a signal with a certain amplitude and phase. Afterwards, each sensor's output can be used to estimate the angle of arrival of the signal. Quantum entangle sensors can evaluate this globally. This process can then be improved by machine learning [78].

Quantum protocols for distributed computing agreement [76] can have advantageous military application for a swarm of drones, or in general for a herd of autonomous vehicles (AVs). Here, quantum protocols can help achieve agreement between all AVs at the same time scale, independent of their quantity. Nevertheless, open space quantum communication between all rapidly moving AVs will be a challenge that has to be solved first. Note that the first experiment of quantum entanglement distribution from a drone was successfully carried out, recently [64].

5.4 Quantum PNT

Key points:

- All quantum PNT technologies have in common the demand for a highly accurate quantum clock.

- Quantum inertial navigation could bring few orders of magnitudes higher precision than its classical counterpart.
- Quantum inertial navigation can be extended by the quantum augmented navigation using quantum magnetic or gravity mapping.
- Promising quantum navigation based on Earth's magnetic anomalies.

Quantum technologies are expected to significantly improve positioning, navigation and timing (PNT) systems, especially inertial navigation. Time standards and frequency transfer (TFT) is a fundamental service that provides precise timing for communication, metrology, but also global navigation satellite system (GNSS). Although present TFT systems are well established, the performance of optical atomic or quantum clocks in combination with TFT utilizing quantum networks [199, 200] will keep pace with the increasing demands of the present applications (communication, GNSS, financial sector, radars, electronic warfare systems) and enables new applications (quantum sensing and imaging).

New quantum-based technologies and approaches support the development of sensitive precision instruments for PNT. The quantum advantage will be manifested for GPS denied or challenging operational environments, enabling precise operations. Examples of such environments are underwater and underground, or environments under GPS jamming.

Current GNSS (GPS, GLONASS, Galileo, BeiDou, …) rely on precise timing provided through multiple atomic clocks in individual satellites that are corrected by the more stable atomic clocks on the ground. The higher precision of the quantum clock will increase the accuracy of positioning and navigation as well. Over the long term, the GNSS satellites should be connected to the quantum internet for timing distribution and clock synchronisation. Chip-size precise mobile clocks could help discover GNSS deception and spoofing [201].

Some quantum GNSS (not only quantum clock) have been considered and investigated; for instance, interferometric quantum positioned system (QPS) [199, 202, 203]. One of the schemes of QPS [202, 203] has a structure similar to the traditional GNSS where there are three baselines, each consisting of two low-orbiting satellites, with the baselines are perpendicular to each other. However, although theoretically the accuracy of positioning is astonishing, significant engineering must be done to design a realistic QPS.

Most of the current navigation relies on GPS, or in general GNSS, which is the most precise available technology for navigation. GNSS technology is prone to jamming, deception, spoofing or GPS-deprived environments such as densely populated areas with high electromagnetic spectrum use. Moreover, for underground or underwater environments, GNSS technology is not available at all. The solution is inertial navigation. The problem with classical inertial navigation is its drifting, a loss of precision over time. For example, the marine-grade inertial navigation (for ships, submarines and spacecraft) has a drift 1.8 km/day and navigation grade (for military aircraft) has a drift 1.5 km/hour [204]. In 2014, DARPA started a MTO-PTN project with a goal to reach drift 20 m and 1 ms/hour [205]. Even so, some expectations are very high, that quantum inertial navigation will offer error of only approximately hundreds of meters per month [5, 206].

The full quantum inertial navigation system consists of a quantum gyroscope, accelerometer and atomic/quantum clocks. Although the individual sensors required for quantum inertial navigation are tested out of laboratories, it is still challenging to create a complete quantum inertial measurement unit. For navigation for highly mobile platforms, sensors need fast measurement rates of several 100 Hz, or to improve the measurement

bandwidth of quantum sensors [204, 207]. The key component that needs the most improvement is the low-drift rotation sensor. The classical inertial sensors are based on various principles [208]. One common chip-size technology is the MEMS (Micro Electro Mechanical Systems) technology, where MEMS gyroscopes have demonstrated instabilities at level $\sim 10^{-7}$ rad $\cdot$ s^{-1} that is suitable for military applications [99]. The instability limit for the best current cold-atom gyroscopes is about $\sim 10^{-9} - 10^{-10}$ rad $\cdot$ s^{-1} (at integration time 1000 s) [209]. The uncertainty is in the precision of the in field-deployable quantum sensors in comparison to the presented laboratory experiments' precision. The intermediate step between classical and quantum inertial navigation can be a hybrid system fusing the outputs of classical and quantum accelerometers [210]. With the size of the quantum inertial navigation device decreasing to chip size, its deployment can be expected on smaller vehicles, especially unmanned autonomous vehicles or missiles. However, the miniaturisation we can reach is unknown. There are many doubts about chip-sized quantum inertial navigation. It is certainly a next-generation technology, although a very big challenge.

Currently, the individual elements, such as gyroscope or accelerometer, are also tested on various platforms; for instance, on board an aircraft [211], or more recently a [212].

For many years, the US National Oceanic and Atmospheric Administration (NOAA) were mapping the Earth's magnetic anomaly and creating a magnetic anomalies map. Using sensitive quantum magnetometers in combination with Earth's magnetic anomaly map is another way to realise quantum non-GNSS navigation [213, 214].

Gravitational map matching [215] works on a similar principle, and one can expect improved performance using the quantum gravimeter. Together, quantum gravimeter and magnetometer could be a basis for a submarine quantum augmented navigation, especially in undersea canyons, wrinkled seabeds, or littoral environments.

In general, quantum inertial navigation or augmented navigation has vast potential, since there is no need for GPS, infra or radar navigation and it is not susceptible to jamming, or in general to electronic warfare attacks. However, the claim of 'no need for GPS' is not quite accurate. These systems will always need some external input on their initial position, most probably from GNSS.

5.5 Quantum ISTAR

Key points:

- Intense involvement of quantum computing to gather and process information.
- Desired deployment on low-orbit satellites, but the resolution is questionable.
- Vast applications for undersea operations.
- Expected advanced underground surveillance with uncertain resolution.
- New type of 3D, low-light or low-SNR quantum vision devices.

ISTAR (intelligence, surveillance, target acquisition and reconnaissance) is a crucial capability of a modern army for precise operations. Quantum technologies have the potential to dramatically improve situational awareness of multi-domain battlefields.

In general, a large impact can be expected from quantum computing that will help with acquiring new intelligence data, processing Big Data from surveillance and reconnaissance and identifying targets using quantum ML/AI [178, 183].

Apart from the processing part of ISTAR, dramatic advancement can be expected from quantum sensing placed on individual land/sea/aerial vehicles and low-orbit satellites.

Quantum gravimeters and gravitational gradiometers promise high accuracy that can improve or introduce new applications: geophysics study, seismology, archaeology, minerals (fissile material or precious metals) and oil detection, underground scanning and precise georeferencing and topographical mappings (e.g. of the seabed for underwater navigation) [7].

Another significant type of sensing is quantum magnetometry. The applications of quantum magnetometry are partially overlapped by applications for quantum gravimetry, thus introducing new applications: Earth's magnetic field including magnetic anomalies, local magnetic anomalies due to the presence, such as metallic objects (submarines, mines, etc.), or weak biological magnetic signals (applications mainly for medical purposes) [7].

The third field interesting for ISTAR is quantum imaging. Quantum imaging offers plenty of diverse applications; for example, quantum radar (see Sect. 5.7), imaging devices for medicine, 3D camera, stealth rangefinder, etc.

The potential quantum computing applications in ISR and situational awareness are described in Sect. 5.2.

5.5.1 Quantum Earth's surface and underground surveillance

Quantum sensing based on magnetometry, gravimetry and gravity gradiometry at the first level helps with the study of continents and sea surface, including underground changes of natural origin. Both magnetic anomaly and gravity-based sensing provide a different picture of the Earth's surface. The Earth is very inhomogeneous (ocean, rocks, caves, metallic minerals, ...), including the massive constructions or vehicles made by people which generate a unique gravitational (depending on the mass) and magnetic (depending on metallic composition) footprint.

The discussed quantum sensing technologies—magnetometry, gravimetry and gravity gradiometry—can reach very high precision, at least in the laboratory. For example, the precision of absolute gravimetry out of the laboratory is about 1 μGal (10 nm $\cdot$ s^{-2}) [216]. Note that the sensitivity of 3.1 μGal corresponds to a sensitivity per centimetre of height above the Earth's surface. However, the problem is the spatial resolution that usually is anti-correlated with the sensitivity (higher sensitivity is at the cost of lower spatial resolution and vice versa). Spatial resolution and sensitivity are the critical attributes that define what you will recognise (large-scale natural changes or small underground structures) and from what distance (from the ground, drone or satellite-based measurement). Examples of the current spatial resolution are about 100 km [217] for satellite-borne gravity gradiometer or 16 km [218] additional width using radar satellite altimetry (for sea areas), or 5 km [219] for airborne gravimetry. For more information, see e.g. [5].

For many quantum sensing applications, it would be essential to place sensors on low Earth orbit (LEO) satellites [220]. However, the current sensitivity and spatial resolution allow only the applications for Earth monitoring (mapping resources such as water or oil, earthquake or tsunami detection).

Apart from low-orbit satellites, the mentioned quantum sensors are considered for deployment on airborne, sea or ground vehicle platforms. Nowadays, quantum sensing experiments are performed outside the laboratory environment, such as in a truck [221], on drones and aeroplanes [222, 223] or aboard ships [217]. For example, the quantum gravimeter could be mounted on drones to search for human-made structures such as tunnels used to smuggle drugs [223]. Placing quantum sensing devices on a drone (this

may be an unmanned aerial vehicle (UAV), Unmanned Surface Vessel (USV), Remotely Operated Vehicle (ROV) or unmanned underwater vessel (UUV)) needs more engineering to reach the best sensitivity, resolution and operability simultaneously.

Low-resolution quantum sensing could be used for precise georeferencing and topographical mappings to help with underwater navigation or mission planning in rugged terrain. Also, the detection of new minerals and oil fields can become a new centre of interest, especially under the seabed [224]. This can be a source of international friction, despite the fact that borders are clear in most cases.

High-resolution quantum magnetic and gravity sensing [217, 225–227] is considered in numerous reports and articles [7, 225, 228–231] to be able to: detect camouflaged vehicles or aircraft; effectively search for a fleet of ships or individual ships from LEO; detect underground structures such as caves, tunnels, underground bunkers, research facilities and missile silos; localise buried unexploded objects (landmines, underwater mines and improvised explosive devices); achieve through-wall detection of rotating machinery.

However, note again that it is highly uncertain where the technical limits are and whether the mentioned quantum gravimetry and magnetometry applications will reach such sensitivity and resolution (especially for using from LEO) as to realise all the aforementioned ideas. Quantum sensors will be delivered to the market in many generations, each with better sensitivity and resolution and lower SWaP, allowing more extensive deployment and application.

5.5.2 Quantum imaging systems

Besides quantum radar and lidar (see Sect. 5.7), there are other military-related applications of quantum imaging. In general, all-weather, day-night tactical sensing for ISTAR for long/short-range, active/passive regime, invisible/stealth using EO/IR/THz/RF frequencies features and advantages are considered. Quantum imaging systems can use various techniques and quantum protocols; for example, SPAD, quantum ghost imaging, sub-shot-noise imaging, or quantum illumination as was described in Sect. 3.4.4. In general, it is not a problem to construct quantum imaging systems of small sizes. The critical parameters are the flux of the single-photon/entangled photon emitter or the single-photon detection resolution and sensitivity. Moreover, a large-scale deployment of a quantum imaging system with high photon flux will require powerful processing that can limit the system deployability and performance.

Quantum 3D cameras exploiting quantum entanglement and photon-number correlations will introduce fast 3D imaging with unprecedented depth of focus with low noise aiming at sub-shot noise or long-range performance. This capability can be used to inspect and detect deviation or structural cracks on jets, satellites and other sensitive military technology. Long-range 3D imaging from UAV can be used for reconnaissance and to explore mission destination or hostile facilities and equipment.

Another commercially available technology is quantum gas sensors [232]. Technically it is a single-photon quantum lidar calibrated to detect methane leakage. The next prepared product is a multiple gas detector able to also detect carbon dioxide (CO_2). With proper improvement and calibration, it could serve for human presence detection, too.

A specific feature at short range is the possibility of behind-the-corner or out of the line-of-sight visibility, [126]. These methods can help to locate and recover trapped people, people in hostage situations or to improve automated driving by detecting incoming vehicles from around a corner.

Quantum imaging can serve as a low-light or low-SNR vision device; for example, in an environment such as cloudy water, fog, dust, smoke, jungle foliage or in the night-time, leading to an advantage. Low-SNR quantum imaging could help in target detection, classification and identification with low signal-to-noise ratios or concealed visible signatures and potentially counter adversaries' camouflage or other target-deception techniques. Quantum imaging will be very useful for helicopter pilots when landing in dusty, foggy or smoky environments [9].

One significant product will be a quantum rangefinder [233, 234]. Conventional rangefinders use a bright laser and can be easily detected by the target. A quantum rangefinder will be indistinguishable from the background both temporally and spectrally when viewed from the target. In other words, the quantum rangefinder will be invisible and stealthy, including at night time, whereas the classical rangefinder can be visible to the target or others.

Under some circumstances, quantum ghost imaging can play the role of quantum lidar [235], especially when the target does not move or moves very slowly and infinite depth of focus is required for 3D imaging.

5.6 Quantum electronic warfare

Key points:

- Enhancement of current EW by smaller universal quantum antennas, precise timing and advanced RF spectrum analysers.
- The problem with detection of quantum channels.
- When the quantum channel is localised, several types of attacks are considered and developed.

Quantum electronic warfare (EW) can be divided into quantum-enhanced classical EW and quantum EW focusing on countermeasures, counter-countermeasure and support against quantum channels. By a quantum channel is meant any transfer of photons carrying quantum information for quantum internet, quantum radar or another quantum system that uses the free-space or optical fibres channel.

Classical EW systems for electronic support measures can benefit from the quantum antenna. Quantum antenna based on Rydberg atoms can offer a small size independent of the measured signal wavelength (frequency) [122, 123]. This means that even for low-frequency (MHz to kHz [124, 236]) signal interception a few-micrometres of quantum antenna is sufficient. There can be an array of quantum antennas for multi-frequency measurement for different bandwidths or one antenna dynamically changing bandwidth according to the interest. Moreover, Rydberg atoms-based antennas can measure both AM and FM signals, offer self-calibration, and measure both weak and very strong fields and detect the angle-of-arrival [125]. 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. The weakest aspect of such antennas is the cryogenics required for cooling Rydberg atoms that need to be scaled down to an acceptable size. In general, quantum RF sensors are a key enabler for advanced (LPD/LPI[11]) communications, over-horizon directional RF, resistance to RF interference and jamming, RF direction finding, or RF-THz imaging. As

[11] Low Probability of Intercept/Low Probability of Detection (LPI/LPD)

an example, an arrayed quantum RF sensor is developed as a potential upgrade for fighter F-35 [237].

Classical EW can also benefit from quantum computing, offering improved RF spectrum analysers for electronic warfare where quantum optimisations and quantum ML/AI techniques can be applied. Higher effectiveness can be reached by the processing and analysing directly of quantum data [55] from RF quantum sensors (Rydberg atoms, NV centres), where the impact of a quantum computer can be more significant. Moreover, other quantum-based solutions and approaches are under development, such as NV centre based RF spectrum analysis or SHB based rainbow analyser [238].

The current EW systems will also benefit from quantum timing. Quantum timing can enhance capabilities such as signals intelligence, counter-DRFM (digital radio frequency memory) and other EW systems that require precise timing; for instance, counter-radar jamming capabilities.

The other area of quantum EW will be signals intelligence (SIGINT) and communications intelligence (COMINT) (detecting, intercepting, identifying, locating) and quantum electronic attack (jamming, deception, use of direct energy weapons). Quantum channels (for quantum communication or quantum imaging) have specific characteristics. First, the simple signal interception is problematic because the quantum data are carried by individual quanta, and their interception can be easily detected. Second, typical quantum imaging technologies use a low signal-to-noise ratio, which means that it is challenging to recognise signal and noise without extra knowledge. Third, coherent photons, usually used as a signal, behave like a laser that is very focused. Finding such a quantum signal without knowing the position of at least one party is very challenging. These characteristics make the classical EW obsolete and blind against quantum channels.

The situation is difficult even for potential quantum electronic warfare systems, since it is open to question whether it will be possible to detect the presence of a quantum (free-space) channel. This will require the development of quantum analogy of laser warning receivers [239]. For quantum EW, it will be critical to get intel on the position of one or both parties using the quantum channel.

Classical EW would intercept and eavesdrop on the free-space classical channel. However, this is not possible for the quantum channel where it would be detected promptly. One possible attack is a man-in-the-middle type attack [240, 241], since the early quantum network parties can have a problem with authentication or trusted repeaters. Other types of attacks are considered at the quantum physics level; for example, a photon number splitting attack relies on utilising coherent laser pulses for the quantum channel [81] or the Trojan-horse attacks [82], or the collecting of scattered light and its detection [242]. However, these types of attacks are very sophisticated, and their practicability, for example in space, is uncertain.

It is more probable that the quantum EW attack will be just a type of denial of service, where the quantum channel is intercepted, leading to stoppage of use of the channel. Another possibility is the sophisticated jamming of the receivers on one or both sides, leading to enormous noise. When the position of the receiver or transmitter is known, another countermeasure of the classical EW is to make use of directed energy weapons such as laser, leading to damage or destruction of sensors. Such an attack also could help eavesdroppers [155].

In general, new approaches and methods will need to be developed to realise the capabilities of quantum electronic warfare and address the corresponding requirements.

5.7 Quantum radar and lidar

Key points:

- Long-range surveillance quantum radar is unlikely with existing quantum microwave technology.
- Possible applications in the optical regime - quantum lidar.
- Quantum radar could be used for space warfare.

The perception of the quantum radar topic [141, 243, 244] is affected by the hype in the media claiming quantum radar development in China [245, 246] or by optimistic laboratory experiments. Indeed, the theoretical advantages and features of quantum radar are significant (some of them depend on individual quantum protocols):

- Higher resistance to noise—that is, better SNR (signal-to-noise ratio)—higher resistance to jamming and other electronic warfare countermeasures;
- Based on individual photons; that is, the output signal power is so low that it will be invisible to electronic warfare measures;
- Target illumination; that is, a radar allowing identification of the target.

Based on the list of unique quantum radar features, it could be a powerfully disruptive technology that could change the rules of modern warfare. Therefore, attention is being paid to this topic internationally, despite the immaturity of the technology, and the many doubts about whether the quantum radar could work as the standard primary surveillance radar.

Moreover, many people immediately imagine quantum radar as a long-range surveillance radar with a range of hundreds of kilometres, whereas such an application of quantum radar seems unlikely [247, 248]. Such an optimal, long-term surveillance quantum radar would be extremely expensive (many orders of magnitude higher than the classical radar cost for any range) [247], and it would still not fulfil all the advantages and features listed above.

Briefly, the practical problems are the following [247]. Quantum radar too is subject to the radar equation, where the received power is lost with the distance's fourth power. In parallel, to keep the quantum advantage, it is desirable to have one or fewer photons per mode. In summary, the relatively high power made of low-photon modes in the microwave regime is needed to be generated. This requires a lot of quantum signal generators, cryogenics, large antenna sizes, etc. All this leads to extremely high cost, and impractical design [137, 247]. Scientists need to come up with more practical quantum microwave technology to overcome these difficulties.

Apart from the high price, scepticism also remains about the detection of stealthy targets or jamming resistance. Quantum radar can be advantageous against a barrage jammer, but not necessarily against a DRFM or other smart jammer [247]. In summary, the long-range surveillance quantum radar is unlikely to be achieved even as a long-term prospect. For its realisation, one would need to evolve new technology allowing smaller cryogenics, RF quantum emitter working at a higher temperature or more efficient cryogenics cooling, and a more powerful emitter (high rate of low photon pulses). Note that even if the room-temperature superconducting materials were developed, it would not help in the Josephson parametric amplifier (JPA) method of entangled microwave photon generation

[249]. Nevertheless, JPA is not the only method to obtain entangled microwave photons [137]. It is not entirely impossible that a new theory and designs of quantum radar will be discovered in the future. The long-range surveillance quantum radar described above would suffer from large size, weight and power consumption, and it is questionable if such a radar would be stealthy [247].

Another problem is the ranging in the case of quantum illumination (QI) protocol. QI protocol requires knowledge of the target in advance, and therefore it requires some extension for ranging, whether classical or quantum [6].

For several years, it was believed that the quantum radar cross section (RCS) is higher than the RCS of classical radars [250, 251]. A new precise study of quantum RCS [252] shows that the previously claimed advantage of quantum RCS over the classical RCS results from erroneous approximation. Quantum and classical RCS seem to be equal, at the moment.

Another approach can be the quantum-enhanced noise radar [137, 253, 254]. Noise radar uses noise waveform as a transmission signal, and detection is based on the correlation between the transmitted signal and the received noise waveform radar returns. The advantage is the low probability of interception (LPI), being nearly undetectable by today's intercept receivers. The quantum noise radar design needs more study to see practical applicability. However, a potential use here is especially for the microwave regime.

Still, the current theory and research have applications in the radar sector, especially that which uses the optical or near-optical photons; that is, quantum lidar. Here, a short-range quantum lidar could be used for target illumination at short distances. Experiments with single-photon imaging were demonstrated from 10 [255] to 45 km [256]. In this range, quantum lidar could operate as an anti-drone surveillance radar or as part of a SHORAD (Short Range Air Defense) complex.

Space can be another example of an advantageous environment for quantum radar/lidar [257] which is low noise for the optical regime, and it even almost eliminates the decoherence problem in the case of entangled photons. For example, Raytheon performs simulations of the quantum radar in the optical regime for space domain [258, 259]. The idea is to place a quantum radar on a satellite and detect small satellites that are difficult to detect because of their small cross-sectional area, reflectivity, and environmental lighting conditions. The deployment of quantum radar/lidar for the space environment can provide almost all the advantages listed above.

A small note is dedicated here to quantum-enhanced radar. Classical radar can be equipped with an atomic or quantum clock. Such quantum-enhanced radars show high precision and reduced noise, and thus demonstrate an advantage in detecting small, slow-moving objects such as drones [260].

5.8 Quantum underwater warfare

Key points:

- Submarines can be one of the first adopters of quantum inertial navigation.
- Quantum magnetometers as the main tool for detection of submarines or underwater mines.

Quantum technologies can significantly interfere in underwater warfare, with enhanced magnetic detection of a submarine or underwater mines, novel inertial submarine navigation and quantum-enhanced precise sonars. In general, in the maritime environment,

sensing based on quantum photo-detectors, radar, lidar, magnetometers, or gravimeters can be applied [257]. For a general overview of the implications of quantum technology for nuclear weapon submarines' near invulnerability, see [261].

Submarines and other underwater vehicles will benefit from quantum inertial navigation described in Sect. 5.4 about PNT. Large submarines can probably be one of the first adopters of quantum inertial navigation because they can afford to install larger quantum devices, including cryogenics cooling. Moreover, sensitive quantum magnetometers and gravimeters can help map surroundings such as an undersea canyon, icebergs and a wrinkled sea bottom without using sonar that can be easily detected. An example of another type of inertial navigation especially suitable for underwater arctic navigation is based on quantum imaging [262].

The basic tool for anti-submarine warfare could be the quantum magnetometer. Researchers anticipate that the SQUID magnetometers in particular could detect a submarine from 6 kilometres away, with still improving noise suppression [263, 264]. Note that the current classical magnetic anomaly detectors, usually mounted on a helicopter or a plane, have a range of only hundreds of meters. An array of quantum magnetometers, such as along the coast, could cover significant areas, leading to denial area for submarines. Moreover, an array of quantum magnetometers seems to work better with more suppressed noise.

Quantum magnetometers can also be used to detect underwater mines using, for instance, an unmanned underwater vessel [230].

However, the main discussion is about the detection range, sensitivity, etc., as in Sect. 5.5.1. Even other underwater domain technology such as sonar offers longer detection range [229]. It was also pointed out in [261] that quantum technologies will have little impact on SSBN (ballistic missile submarines). It is possible that quantum magnetometers could work with other sensors to aid in detection, identification and classification of targets [229].

5.9 Quantum space warfare

Key points:

- Important for long-distance quantum communication.
- Low Earth orbit will be important for the future deployment of quantum sensing and imaging technologies.
- Space warfare will lead to new quantum radar/lidar and quantum electronic warfare technologies for deployment in space.

The space domain is gaining in importance and will be an important battlefield used by advanced countries. Space used to be a place mainly for satellites for navigation, mapping, communication and surveillance, often for military purposes. Nowadays, space is becoming more weaponised [265]; for example, satellites with laser weapons or 'kamikaze' satellites are placed in Earth orbit, and anti-satellite warfare is growing in parallel. Another surging problem is the amount of space garbage, with the number of satellites estimated at 2,200 and several more planned to be released [266].

Space also will be key for placing quantum sensing and communication technology in satellites [267–271], as well as for space countermeasures.

For many quantum technology applications described in previous sections, it would be desirable to place quantum sensing technology such as quantum gravimeter, gravity gradiometer or magnetometer on satellites in Earth orbit, especially the low one (LEO). Such

applications are in development; for example, a low-power quantum gravity sensing device that can be deployed in space on board a small satellite for accurately mapping resources or to aid in assessing the impact of natural disasters [272]. However, such an application does not require too high spatial resolution. See Sect. 5.5.1 for a detailed discussion. The same applies to satellite-based quantum imaging. For example, China claimed the development of a spy satellite that uses ghost imaging technology [273]. However, what spatial resolution it has is uncertain. Nevertheless, quantum ghost imaging would have the advantage of being usable in cloudy, foggy weather or at night as well.

On the other hand, utilisation of satellites for quantum communication has already been demonstrated [62, 274]. Satellite-based quantum communication will be essential for the near-term integrated quantum network at long distances [275]. The present quantum communication satellites suffer from the same problems as trusted repeaters for optic fibre channel. In fact, present quantum satellites are trusted repeaters. The issue with trusted repeaters is that they keep the doors open to possible cyber attacks on the satellite control system. A better security situation is with the presently demonstrated MDI-QKD protocol [276], where the central point works as a repeater or switch, but in a safe regime, and later with quantum repeaters. For a space quantum communication overview, see [270, 271].

A new required military capability will be technology to detect other satellites, space-borne objects, space garbage and track them. classical radars are used for this purpose; for instance, the Space Fence project as part of the US Space Surveillance Network [277]. However, most of these space surveillance radars have problems with objects with a size of about 10 cm and smaller [266] (in the case of Space Fence, the minimal size is about 5 cm), and another problem is the capacity, as to how many objects they can track. This is the case with most of the space garbage that is only a few centimetres in size. Instead of classical radar, quantum radar or lidar is considered [6, 257, 259] as an alternative. Specifically for the space environment, the quantum radar in optical regime is considered [259], since the optical photons do not suffer from losses such as in the atmosphere. Space quantum radar can offer most of the advantages of quantum radar as described in Sect. 5.7, including stealth. According to simulations [259], quantum radar in space can offer at least one order of magnitude higher detection sensitivity and object tracking sensitivity in space in comparison with GEODSS (Ground-based Electro-Optical Deep Space Surveillance). Space quantum radar would be very useful for tracking small, dark and fast objects, such as satellites, space garbage or meteoroids.

The increasing presence of quantum sensing and communication devices in space will lead to increased interest in quantum electronic warfare as described in Sect. 5.6.

5.10 Chemical and biological simulations and detection

Key points:

- $\sim$ 200 qubits are sufficient to carry out chemical quantum simulation research.
- The capability of achieving more complex simulations increases with the number of logical qubits.
- Chemical detection in the air or in samples.
- Suitable for detecting explosives and chemical warfare agents.

The defence-related chemical and biological simulations are primarily interesting for the military and national laboratories, the chemical defence industry or CBRN (Chemical, Biological, Radiological and Nuclear) defence forces. Research on new drugs and chemical

substances based on quantum simulations will require an advanced quantum computer, classical computing facility and quantum-chemical experts. The quantum simulations for chemical and biological chemical warfare agents, in principle, have the same requirements as civil research, such as the already ongoing protein folding, nitrogen fixation and peptides research.

The number of required qubits depends on the number of spatial basis functions (various basis sets exist, e.g., STO-3G, 6-31G or cc-pVTZ); for example, using the 6-31G basis, the Benzene and Caffeine molecules can be simulated by approx. 140 and 340 qubits, respectively [278]. Then, the Sarin molecule simulation, for instance, requires about 250 qubits. Based on quantum computer roadmaps [27, 279] and logical qubit requirements, one can come to 100 logical qubits in 10 years, but probably earlier with more effective error corrections and error-resisting qubits. This is sufficient for medium-sized molecule simulations.

The threat could be the design and precise simulation of structures and the chemical properties of new small- to medium-sized molecules that could play the role of chemical warfare agents similar to, for example, Cyanogen, Phosgene, Cyanogen chloride, Sarin or Yperit. On the other hand, in general the same knowledge can also be used for CBRN countermeasures and new detection technique development.

The research on protein folding, DNA and RNA exploration, such as motifs identification, Genome-wide association studies and De novo structure prediction [280] could impact the research on biological agents as well [281]. However, more detailed studies are needed to assess the real threat from quantum simulations.

Photoacoustic detection with quantum cascade laser will be effective as a chemical detector. For example, quantum chemical detectors can detect TNT and triacetone triperoxide elements used in improvised explosive devices (IED) that are a common weapon used in asymmetric conflicts. The same system for detecting Acetone can be used to discover baggage and passengers with explosives boarding aircraft. In general, quantum chemical detection can be used against chemical warfare agents or toxic industrial chemicals [282, 283].

In the mid- to long term, such detectors can be placed on autonomous drones or ground vehicles that are inspecting an area [284].

5.11 New material design

Key points:

- General research impacts; for example, room-temperature superconducting allowing the highly precise SQUID magnetometers to operate without cooling can have a remarkable impact on military quantum technology applications.
- Defence industry research on camouflage, stealth, ultra-hard armour or high-temperature tolerance material.

Modern science is developing new materials, metamaterials, sometimes called quantum material, by exploiting the quantum mechanical properties (e.g. graphene, topological insulator). Material as a quantum system can be simulated by a quantum computer; for example, the electronic structure of the material. The considered applications can be, for instance, the room-temperature superconductor, better batteries and improvement of specific material features.

To explain in greater detail, the room-temperature superconductivity material, for example, exploits superconductivity at high temperatures [285]. That would allow building

Josephson junctions, usually used as the building blocks of SQUIDs or superconducting qubits. So far, cooling near absolute zero is required. It is expected that a quantum computer with about 70 logical qubits [286] could be sufficient for the basic research on high-temperature superconductors.

For the defence industry, opportunities for research on new materials such as better camouflage, stealth (electromagnetic absorption), ultra-hard armour or high-temperature tolerance material design are considered without any details being revealed.[12]

5.12 Brain imaging and human-machine interfacing

Key points:

- Quantum enabled magneto-encephalography
- Enhanced human-machine interfacing

MEG (magneto-encephalography) scanner is a medical imaging system that visualises what the brain is doing by measuring the magnetic fields generated by current flowing through neuronal assemblies. Quantum magnetometers—based, for instance, on optically pumped magnetometers [287]—can enable high-resolution magnetoencephalography for real-time brain activity imaging. This technology is safe and non-invasive, and is already laboratory tested. The technology itself is small, and wearable [287].

In the near term, quantum MEG could be a part of a soldier's helmet for continuous and remote medical monitoring and diagnosis in case of injury. The long-term expectations include enhanced human–machine interfacing, i.e. practical non-invasive cognitive communication with machines and autonomous systems [11].

6 Optimism versus pessimism

Many of the quantum technology military applications mentioned above sound very optimistic and can drive exaggerated expectations. Some applications are taken from various reports and newspapers or magazine articles, wherein the author could have overestimated the quantum technology transfer from the laboratory to the battlefield or been influenced by general quantum technology hype [288]. It is especially important to avoid exaggerated expectations when the topic concerns national security or defence. This issue has been described in [14].

Quantum technology military applications described above are based on public-domain, state-of-the-art research supplemented by various reports and newspaper or magazine articles about defence applications. Critical remarks on their feasibility are not given for several technologies, since there is no public information on the same. In these cases, the reader should be more careful and critical until more detailed studies are available.

On the other hand, it is known that big defence corporations and national defence laboratories have had quantum research and development programmes for several years. However, only some detailed information is publicly communicated. The opposite extreme seems to include announcements, such as from China [245, 246, 263, 273], where it is difficult to disentangle the real research advancement from the state's strategic propaganda [289].

[12] Usually mentioned in public news articles or interviews but without details or references.

For many of the mentioned quantum technologies, only a laboratory proof of concept has been provided so far. The decisive factors determining whether the quantum technologies will be applied outside the laboratory to general use are component miniaturisation and susceptibility to interference. These improvements must not be made at the expense of sensitivity, resolution and functionality. Another decisive factor in real deployment is the price of the technology.

In conclusion, considering the advancements in quantum technology research and in supportive systems, such as laser and cryogenic cooling miniaturisation in the last few years, it is reasonable to be optimistic rather than pessimistic about the future quantum technology military applications (from the perspective of military or governmental actors). One needs to be careful about the real capabilities in operational deployment, to see whether they fulfil the requirements and if the price-performance ratio justifies acquisition and deployment.

7 Quantum warfare consequences and challenges

The development, acquisition and deployment of quantum technologies for military application will raise new, related challenges. The concept of quantum warfare will impose new demands on military strategy, tactics and doctrines, on ethics and disarmament activities and on technical realisation and deployment. Studies should be conducted to understand the issues, implications, threats and choices that arise from the development of quantum technologies, and not only for military application.

7.1 Military consequences and challenges

Quantum technologies in military applications have the potential to sharpen the present capabilities, such as by providing more precise navigation, ultra-secure communication or advanced ISTAR and computing capabilities. In general, quantum warfare will require an update, modification or creation of new military doctrines, military scenarios and plans to develop and acquire new techniques and weapons for the quantum age.

Before this, the development of technology policies and strategies is needed to respond to the strategic ambitions of individual actors [290]. National technology policies and strategies should include, for example, the research of national quantum technology resources (universities, laboratories and corporations) and markets, the state of development and feasibility studies and the military and security threat and potential assessments, such as [261].

The monitoring of quantum technology evolution and adaptation is essential to avoid technological surprises due to neighbouring or potentially hostile countries. Quantum warfare monitoring is essential even if the quantum technology is beyond their financial, research or technological capabilities for some countries. Therefore, all modern armies should be interested in the possible impacts of quantum warfare.

The national trade and export policies are also important. For example, the European Union has declared quantum computing as an emerging technology of global strategic importance and is considering more restricted access to the research programme named Horizon Europe [291]. Further, China has prohibited the export of cryptography technology, including quantum cryptography [292].

Another topic is the careful communication of significant quantum advantages along with allies, especially in the quantum ISTAR and quantum cyber capabilities, which can

reveal military secrets, such as classified files, nuclear submarines' positions or underground facilities. A significant disruption of the balance of power could upset allies as well as neutral or hostile players [9].

7.2 Peace and ethics consequences and challenges

To date, the military applications of quantum technologies mapped in Sect. 5 do not introduce new weapons even as they sharpen the existing military technology; for instance, by developing more precise sensing and navigation, new computing capabilities and stronger information security. Nevertheless, the question if quantum technologies, especially for military applications, will be good or bad for world peace is relevant.

Already various calls for ethical guidelines for quantum computing [293–295] have appeared, wherein ethical concerns, such as human DNA manipulation, creation of new materials for war and intrusive AI are mentioned [294].

Despite the fact that quantum technologies do not generate new weapons, their improvement of present military technology will sharpen such capabilities, shortening the time for an attack, warning and decision making. Consequently, quantum technologies can make the use of force more likely even while reducing individual risk [296], and thus make war more probable [297, 298].

The preventive arms control of generic dual-use technologies such as quantum technologies will be more difficult because they can be used for civilian applications too, such as in quantum sensing for medicine. An analogy with nanotechnologies has been made [299]. Export controls to prevent or slow down proliferation and military use by other countries or non-state groups are the most likely way to attempt to reduce any threat posed by quantum technologies [298].

Specifically, quantum computing research and development is very expensive. However, the goal is to develop a technology that allows simple and reliable qubit production. This can lead to cheaper, more widely distributed and accessible technology for actors with fewer skills, which is a trait of upcoming problematic military technology [298].

7.3 Technical consequences and challenges

The transfer of successful laboratory proofs of concept to real 'outside' application faces many technical and technological challenges, such as miniaturisation and operability that is not at the expense of laboratory-achieved sensitivity and resolution. Further, there are other related technical challenges.

A significant problem could be the quantum workforce. The quantum workforce does not need to comprise physicists or scientists with a doctorate. However, they should be quantum engineers with knowledge of quantum information science and a quantum technology overview who can understand and be able to process and evaluate the outgoing data from quantum sensors, computers and communications. Presently, an existing quantum ecosystem is growing continuously, and this ecosystem will require an increasingly larger quantum workforce [300]. This requires training and educating new quantum engineers and experts; that is, more universities offering quantum programmes and more students taking them. Besides, it can be even more difficult to get these people to work in the army. Therefore, the basic principles of quantum information and quantum technology should also appear as part of the curriculum at military colleges of modern armies, where quantum technologies are or will be deployed.

Another technical challenge will be the enormous amount of data. Quantum technologies, through all quantum sensors, quantum imaging, quantum communication and computing, will produce a lot of classical and quantum data that will increase requirements for data transmission, processing and evaluation. These requirements should be considered during the planning of C4ISR and quantum infrastructure.

The final challenge will be standardisation. The standardisation process is important for the interoperability of devices manufactured by different producers. Apart from the unification interface and communication protocols, the standardisation process can also include security verification, such as in the post-quantum cryptography standardisation process [90]. Various connected devices in particular (such as nodes, repeaters, switches, fibre channels and open-space channels) can be expected in the case of a quantum network, and it is important to develop and implement some standards that will allow the successful transmission of quantum information.

8 Conclusion

Quantum technology is an emerging area of technologies that utilise the manipulation and control of individual quanta for multiple applications with the potential to be disruptive. Many of these applications are dual-use or are directly used for military purposes. However, individual quantum technologies are at TRLs for military use, from TRL 1 (basic principles observed) to TRL 6 (technology demonstrated in relevant environment).

Quantum technology for military applications will not only offer improvements and new capabilities but will also require the development of new strategies, tactics and policies, assessment of threats to global peace and security and identification of ethics issues. All this is covered by the term 'quantum warfare'.

In this report, various quantum technologies at different TRL have been described, focusing on possible utilisation or deployment in the defence sector. A precise forecast of quantum technology deployment is not possible, since the transition from the laboratory to real-world applications has not been implemented or is in progress. This raises questions such as whether we will be able to reach a resolution providing a real quantum advantage over the classical systems that are usually significantly cheaper and often in action already. Despite the fact that the description of the possible military application of quantum technologies sounds very optimistic, one should be wary of the quantum hype and draw attention to the challenges that lie ahead of the real deployment of quantum technologies for military applications.

Quantum technologies can be expected to have strategic and long-term impacts. Nevertheless, the probability of technological surprises affecting military and defence forces is rather low. The best ways to avoid surprises are cultivating quantum technology knowledge and monitoring quantum technology development and employment. Treating quantum technology with care will play the role of quantum insurance.

Acknowledgements

The author is very grateful for several comments and feedback on the draft, especially by Dr Katarzyna Kubiak, Dr Jürgen Altmann and others. The author is also grateful for the minor comments to the first preprint and valuable suggestions and journal reviewers' comments.

Availability of data and materials

The datasets used and analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests
The author declares that he has no competing interests.

Authors' contributions
As the sole author of the manuscript, MK conceived, designed and performed the analysis and review, and wrote the paper. The author read and approved the final manuscript.

Publisher's Note

Received: 6 April 2021 Accepted: 25 October 2021 Published online: 06 November 2021

References

1. Lind W et al. The changing face of war: into the fourth generation. In: Marine corps gazette. 1989.
2. Lind WS. Understanding fourth generation war. Mil Rev. 2004;84:12.
3. Affan Ahmed S, Mohsin M, Muhammad Zubair Ali S. Survey and technological analysis of laser and its defense applications. Defence Technology (2020). ISSN 2214-9147. https://doi.org/10.1016/j.dt.2020.02.012.
4. Dowling JP, Milburn GJ. Quantum technology: the second quantum revolution. Philos Trans R Soc, Math Phys Eng Sci. 2003;361(1809):1655–74. https://doi.org/10.1098/rsta.2003.1227.
5. Till S, Pritchard J. UK quantum technology landscape 2016. DSTL/PUB098369, UK National Quantum Technologies Programme. 2016.
6. Davies A, Kennedy P. Special report - from little things: quantum technologies and their application to defence. ASPI (Australian Strategic Policy Institute); 2017.
7. Wolf SA et al. Overview of the status of quantum science and technology and recommendations for the DoD. Institute for defense analyses; 2019.
8. Andas H. Emerging technology trends for defence and security. FFI-RAPPORT. Apr. 2020.
9. Inglesant P, Jirotka M, Hartswood M. Responsible Innovation in Quantum Technologies applied to Defence and National Security. NQIT (Networked Quantum Information Technologies); 2018.
10. ATARC Quantum Working Group. Applied quantum computing for today's military. White paper. May 2021.
11. Australian Army. Army Quantum Technology Roadmap. Apr. 2021.
12. Sayler KM. Defense primer: quantum technology. IF11836. June 2021.
13. Middleton A, Till S, Steele M. Quantum Information Processing Landscape 2020: Prospects for UK Defence and Security. DSTL/TR121783. June 2020.
14. Biercuk MJ. Read before pontificating on quantum technology. War on the Rock. 2020. URL: https://warontherocks.com/2020/07/read-before-pontificating-on-quantum-technology/ (visited on 02/27/2021).
15. Perani G. Military technologies and commercial applications: public policies in NATO countries. July 1997.
16. Nouwens M, Legarda H. China's pursuit of advanced dual-use technologies. IISS. Dec. 2018. URL: https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance (visited on 09/30/2010).
17. Davidson A. A new dimension of war: the quantum domain. Canadian Forces College. 2020.
18. Park JL. The concept of transition in quantum mechanics. In: Foundations of physics. 1970. p. 23–33. https://doi.org/10.1007/bf00708652.
19. Nielsen MA, Chuang IL. Quantum computation and quantum information: 10th anniversary edition. Cambridge: Cambridge University Press; 2010. ISBN 9781139495486.
20. Mermin ND. Quantum computer science: an introduction. Cambridge: Cambridge University Press; 2007. ISBN 9781139466806.
21. Jordan S. Quantum Algorithm Zoo. URL: https://quantumalgorithmzoo.org/ (visited on 09/13/2021).
22. Cross AW, et al. Validating quantum computers using randomized model circuits. Physical Review A. 2019;100(3). https://doi.org/10.1103/physreva.100.032328.
23. Fowler AG, et al. Surface codes: towards practical large-scale quantum computation. Physical Review A. 2012;86(3). https://doi.org/10.1103/physreva.86.032324.
24. National Academies of Sciences, Engineering, and Medicine et al. Quantum Computing: Progress and Prospects. National Academies Press, 2019. ISBN 9780309479721. https://doi.org/10.17226/25196.
25. Arute F et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019;574(7779):505–10. https://doi.org/10.1038/s41586-019-1666-5.
26. Gambetta J. IBM's Roadmap For Scaling Quantum Technology. IBM. 2020. URL: https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/ (visited on 10/07/2020).
27. Finke D. Google Goal: Build an Error Corrected Computer with 1 Million Physical Qubits by the End of the Decade. Quantum Computing report. 2020. URL: https://quantumcomputingreport.com/google-goal-error-corrected-computer-with-1-million-physical-qubits-by-the-end-of-the-decade/ (visited on 10/07/2020).
28. Mosca M, Piani M. Quantum threat timeline. Global Risk Institute; 2019.
29. Simulating Molecules using VQE. Qiskit Textbook. URL: https://qiskit.org/textbook/ch-applications/vqe-molecules.html (visited on 01/25/2021).
30. Feynman RP. Simulating physics with computers. Int J Theor Phys. 1982;21(6):467–88. https://doi.org/10.1007/BF02650179.
31. Reiher M et al. Elucidating reaction mechanisms on quantum computers. In: Proceedings of the national academy of sciences. vol. 114. 2017. p. 7555–60. https://doi.org/10.1073/pnas.1619152114.
32. Peruzzo A, et al. A variational eigenvalue solver on a photonic quantum processor. Nature Communications. 2014;5(1). https://doi.org/10.1038/ncomms5213.

33. McClean JR et al. The theory of variational hybrid quantum-classical algorithms. New J Phys. 2016;18(2):023023. https://doi.org/10.1088/1367-2630/18/2/023023.
34. Arute F et al. Hartree-Fock on a superconducting qubit quantum computer. Science. 2020;369(6507):1084–9. https://doi.org/10.1126/science.abb9811.
35. Gidney C, Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum. 2021;5:433. https://doi.org/10.22331/q-2021-04-15-433.
36. Häner T et al. Improved quantum circuits for elliptic curve discrete logarithms. In: Post-quantum cryptography. Berlin: Springer; 2020. p. 425–44. https://doi.org/10.1007/978-3-030-44223-1_23. 2001.09580 [quant-ph].
37. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. Los Alamitos: IEEE Comput. Soc.; 1994. https://doi.org/10.1109/sfcs.1994.365700.
38. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing - STOC '96. New York: ACM; 1996. https://doi.org/10.1145/237814.237866.
39. Bernstein DJ. Grover vs. McEliece. In: Post-quantum cryptography. Berlin: Springer; 2010. p. 73–80. https://doi.org/10.1007/978-3-642-12929-2_6.
40. Simon DR. On the power of quantum computation. In: Proceedings 35th annual symposium on foundations of computer science. Los Alamitos: IEEE Comput. Soc.; 2002. https://doi.org/10.1109/sfcs.1994.365701.
41. Kaplan M, et al. Breaking Symmetric Cryptosystems using Quantum Period Finding. 2016. 1602.05973 [quant-ph].
42. Bonnetain X, Jaques S. Quantum Period Finding against Symmetric Primitives in Practice. 2020. 2011.07022 [quant-ph].
43. Kaplan M et al. Breaking symmetric cryptosystems using quantum period finding. In: Advances in cryptology - CRYPTO 2016. Berlin: Springer; 2016. p. 207–37. https://doi.org/10.1007/978-3-662-53008-5_8.
44. Shenvi N, Kempe J, Whaley KB. Quantum random-walk search algorithm. Physical Review A. 2003;67(5). https://doi.org/10.1103/physreva.67.052307.
45. Farhi E, Goldstone J, Gutmann S. A quantum approximate optimization algorithm. 2014. 1411.4028 [quant-ph].
46. Glover F, Kochenberger G, Du Y. A Tutorial on Formulating and Using QUBO Models. 2019. 1811.11538 [cs.DS].
47. Wiebe N, Braun D, Lloyd S. Quantum Algorithm for Data Fitting. Physical Review Letters. 2012;109(5). https://doi.org/10.1103/physrevlett.109.050505.
48. Brandao FGSL, Svore K. Quantum Speed-ups for Semidefinite Programming, 2017. 1609.05537 [quant-ph].
49. Barak B, et al. Beating the random assignment on constraint satisfaction problems of bounded degree. 2015. 1505.03424 [cs.CC].
50. Harrow AW, Hassidim A, Lloyd S. Quantum Algorithm for Linear Systems of Equations. Physical Review Letters. 2009;103(15). https://doi.org/10.1103/physrevlett.103.150502.
51. Scherer A, et al. Concrete resource analysis of the quantum linear-system algorithm used to compute the electromagnetic scattering cross section of a 2D target. Quantum Information Processing. 2017;16(3). https://doi.org/10.1007/s11128-016-1495-5.
52. Aaronson S. Read the fine print. Nat Phys. 2015;11(4):291–3. https://doi.org/10.1038/nphys3272.
53. Blencowe M. Quantum RAM. Nature. 2010;468(7320):44–5. https://doi.org/10.1038/468044a.
54. Biamonte J et al. Quantum machine learning. Nature. 2017;549(7671):195202. https://doi.org/10.1038/nature23474.
55. Dunjko V, Taylor JM, Briegel HJ. Quantum-Enhanced Machine Learning. Physical Review Letters. 2016;117(13). https://doi.org/10.1103/physrevlett.117.130501.
56. Wittek P. Quantum machine learning: what quantum computing means to data mining. Amsterdam: Elsevier; 2016. ISBN 9780128100400.
57. Dunjko V, Wittek P. A non-review of quantum machine learning: trends and explorations. Quantum Views. 2020;4:32. https://doi.org/10.22331/qv-2020-03-17-32.
58. Havlicek V et al. Supervised learning with quantum-enhanced feature spaces. Nature. 2019;567(7747):209–12. https://doi.org/10.1038/s41586-019-0980-2.
59. Bakhtiari Ramezani S et al. Machine learning algorithms in quantum computing: a survey. In: 2020 international joint conference on neural networks (IJCNN). New York: IEEE; 2020. https://doi.org/10.1109/ijcnn48605.2020.9207714.
60. Gisin N, Thew R. Quantum communication. Nat Photonics. 2007;1(3):165–71. https://doi.org/10.1038/nphoton.2007.22.
61. Wehner S, Elkouss D, Hanson R. Quantum Internet: a vision for the road ahead. Science. 2018;362(6412):eaam9288. https://doi.org/10.1126/science.aam9288.
62. Yin J et al. Satellite-based entanglement distribution over 1200 kilometers. Science. 2017;356(6343):1140–4. https://doi.org/10.1126/science.aan3211.
63. Yin J, et al. Satellite-to-Ground Entanglement-Based Quantum Key Distribution. Physical Review Letters. 2017;119(20). https://doi.org/10.1103/physrevlett.119.200501.
64. Liu H-Y, et al. Optical-Relayed Entanglement Distribution Using Drones as Mobile Nodes. Physical Review Letters. 2021;126(2). https://doi.org/10.1103/physrevlett.126.020503.
65. Pogorzalek S, et al. Secure quantum remote state preparation of squeezed microwave states. Nature Communications. 2019;10(1). https://doi.org/10.1038/s41467-019-10727-7.
66. Bouwmeester D et al. Experimental quantum teleportation. Nature. 1997;390(6660):575–9. https://doi.org/10.1038/37539.
67. Braunstein SL, Pirandola S. Side-Channel-Free Quantum Key Distribution. Physical Review Letters. 2012;108(13). https://doi.org/10.1103/physrevlett.108.130502.
68. Lo H-K, Curty M, Qi B. Measurement-Device-Independent Quantum Key Distribution. Physical Review Letters. 2012;108(13). https://doi.org/10.1103/physrevlett.108.130503.
69. Broadbent A, Fitzsimons J, Kashefi E. Universal blind quantum computation. In: 2009 50th annual IEEE symposium on foundations of computer science. New York: IEEE; 2009. https://doi.org/10.1109/focs.2009.36.
70. Fitzsimons JF. Private quantum computation: an introduction to blind quantum computing and related protocols. npj Quantum Information. 2017;3(1). https://doi.org/10.1038/s41534-017-0025-3.
71. Chuang IL. Quantum algorithm for distributed clock synchronization. Phys Rev Lett. 2000;85(9):2006–9. https://doi.org/10.1103/physrevlett.85.2006.

72. Damgård I et al. Secure identification and QKD in the bounded-quantum-storage model. Theor Comput Sci. 2014;560:12–26. https://doi.org/10.1016/j.tcs.2014.09.014.
73. Unruh D. Quantum position verification in the random oracle model. In: Advances in cryptology - CRYPTO 2014. Berlin: Springer; 2014. p. 1–18. https://doi.org/10.1007/978-3-662-44381-1_1.
74. Crépeau C, Gottesman D, Smith A. Secure multi-party quantum computation. In: Proceedings of the thiry-fourth annual ACM symposium on theory of computing - STOC '02. New York: ACM; 2002. https://doi.org/10.1145/509907.510000.
75. Cuomo D, Caleffi M, Cacciapuoti AS. Towards a distributed quantum computing ecosystem. IET Quantum Communication. 2020;1(1):3–8. https://doi.org/10.1049/iet-qtc.2020.0002.
76. Ben-Or M, Hassidim A. Fast quantum byzantine agreement. In: Proceedings of the thirty-seventh annual ACM symposium on theory of computing - STOC 05. New York: ACM; 2005. https://doi.org/10.1145/1060590.1060662.
77. Proctor TJ, Knott PA, Dunningham JA. Multiparameter Estimation in Networked Quantum Sensors. Physical Review Letters. 2018;120(8). https://doi.org/10.1103/physrevlett.120.080501.
78. Xia Y, et al. Quantum-Enhanced Data Classification with a Variational Entangled Sensor Network. Physical Review X. 2021;11(2). https://doi.org/10.1103/physrevx.11.021047.
79. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems and signal processing. vol. 175. New York: IEEE; 1984.
80. Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett. 1991;67(6):661–3. https://doi.org/10.1103/physrevlett.67.661.
81. Brassard G et al. Limitations on practical quantum cryptography. Phys Rev Lett. 2000;85(6):1330–3. https://doi.org/10.1103/physrevlett.85.1330.
82. Jain N et al. Trojan-horse attacks threaten the security of practical quantum cryptography. New J Phys. 2014;16(12):123030. https://doi.org/10.1088/1367-2630/16/12/123030.
83. Bernstein DJ. Introduction to post-quantum cryptography. In: Post-quantum cryptography. Berlin: Springer; 2009. p. 1–14. https://doi.org/10.1007/978-3-540-88702-7_1.
84. Hoffstein J, Pipher J, Silverman JH. NTRU: a ring-based public key cryptosystem. In: Lecture notes in computer science. Berlin: Springer; 1998. p. 267–88. https://doi.org/10.1007/bfb0054868.
85. De Feo L, Jao D, Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology. 2014;8(3). https://doi.org/10.1515/jmc-2012-0015.
86. Merkle RC. A certified digital signature. In: Advances in cryptology — CRYPTO' 89 proceedings. New York: Springer; 2001. p. 218–38. https://doi.org/10.1007/0-387-34805-0_21.
87. Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature- verification and message-encryption. In: Lecture notes in computer science. Berlin: Springer; 1988. p. 419–53. https://doi.org/10.1007/3-540-45961-8_39.
88. McEliece RJ. A public-key cryptosystem based on algebraic coding theory. In: Deep space network progress report. vol. 44. 1978. p. 114–6.
89. In: Wall Street Journal (Mar. 2021). ISSN: 0099-9660. URL: https://www.wsj.com/articles/encryption-isnt-main-data-security-threat-11615577004 (visited on 03/15/2021).
90. Alagic G, et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309, NSIT; 2020. https://doi.org/10.6028/nist.ir.8309.
91. Abbott AA, Calude CS, Svozil K. A quantum random number generator certified by value indefiniteness. Math Struct Comput Sci. 2014;24(3). https://doi.org/10.1017/s0960129512000692.
92. Degen CL, Reinhard F, Cappellaro P. Quantum sensing. Rev Mod Phys. 2017;89(3). https://doi.org/10.1103/revmodphys.89.035002.
93. Barrett B, Bertoldi A, Bouyer P. Inertial quantum sensors using light and matter. Phys Scr. 2016;91(5):053006. https://doi.org/10.1088/0031-8949/91/5/053006.
94. Kasevich M, Chu S. Atomic interferometry using stimulated Raman transitions. Phys Rev Lett. 1991;67:181–4. https://doi.org/10.1103/PhysRevLett.67.181.
95. Rasel EM et al. Atom wave interferometry with diffraction gratings of light. Phys Rev Lett. 1995;75:2633–7. https://doi.org/10.1103/PhysRevLett.75.2633.
96. Young B et al. Atom optic inertial and gravitational sensors. In: Frontiers in optics 2007/laser science XXIII/organic materials and devices for displays and energy conversion. OSA. 2007. https://doi.org/10.1364/ls.2007.ltuh1.
97. Weidner CA, Anderson DZ. Experimental Demonstration of Shaken-Lattice Interferometry. Physical Review Letters. 2018;120(26). https://doi.org/10.1103/physrevlett.120.263201.
98. Zhu L et al. A dielectric metasurface optical chip for the generation of cold atoms. Sci Adv. 2020;6(31):eabb6667. https://doi.org/10.1126/sciadv.abb6667.
99. Geiger R et al. High-accuracy inertial measurements with cold-atom sensors. AVS Quantum Science. 2020;2(2):024702. https://doi.org/10.1116/5.0009093.
100. Biercuk MJ et al. Ultrasensitive detection of force and displacement using trapped ions. Nat Nanotechnol. 2010;5(9):646–50. https://doi.org/10.1038/nnano.2010.165.
101. Diddams SA. An optical clock based on a single trapped 199Hg+ ion. Science. 2001;293(5531):825–8. https://doi.org/10.1126/science.1061171.
102. Ivanov PA, Vitanov NV, Singer K. High-precision force sensing using a single trapped ion. Scientific Reports. 2016;6(1). https://doi.org/10.1038/srep28078.
103. Gilmore KA et al. Quantum-enhanced sensing of displacements and electric fields with two-dimensional trapped-ion crystals. Science. 2021;373(6555):673–8. https://doi.org/10.1126/science.abi5226.
104. Taylor JM et al. High-sensitivity diamond magnetometer with nanoscale resolution. Nat Phys. 2008;4(10):810–6. https://doi.org/10.1038/nphys1075.
105. Ledbetter MP, et al. Gyroscopes based on nitrogen-vacancy centers in diamond. Physical Review A. 2012;86(5). https://doi.org/10.1103/physreva.86.052116.
106. Baumgratz T, Datta A. Quantum enhanced estimation of a multidimensional field. Phys Rev Lett. 2016;116:030801. https://doi.org/10.1103/PhysRevLett.116.030801.

107. Radtke M et al. Nanoscale sensing based on nitrogen vacancy centers in single crystal diamond and nanodiamonds: achievements and challenges. Nano Futures. 2019;3(4):042004. https://doi.org/10.1088/2399-1984/ab5f9b.
108. Dang HB, Maloof AC, Romalis MV. Ultrahigh sensitivity magnetic field and magnetization measurements with an atomic magnetometer. Appl Phys Lett. 2010;97(15):151110. https://doi.org/10.1063/1.3491215.
109. Wasilewski W et al. Quantum noise limited and entanglement-assisted magnetometry. Phys Rev Lett. 2010;104:133601. https://doi.org/10.1103/PhysRevLett.104.133601.
110. Schreiber KU, Wells J-PR. Invited review article: large ring lasers for rotation sensing. Rev Sci Instrum. 2013;84(4):041101. https://doi.org/10.1063/1.4798216.
111. BIPM Time Department. BIPM Annual Report on Time Activities. May 2020.
112. Brewer SM, et al. Al+27 Quantum-Logic Clock with a Systematic Uncertainty below 10-18. Physical Review Letters. 2019;123(3). https://doi.org/10.1103/physrevlett.123.033201.
113. Hwang WY et al. Entangled quantum clocks for measuring proper-time difference. Eur Phys J D. 2002;19(1):129–32. https://doi.org/10.1140/epjd/e20020065.
114. Marti EG, et al. Imaging Optical Frequencies with 100 Hz Precision and 1.1 m Resolution. Physical Review Letters. 2018;120(10). https://doi.org/10.1103/physrevlett.120.103201.
115. Pedrozo-Peñafiel E et al. Entanglement on an optical atomic-clock transition. Nature. 2020;588(7838):414–8. https://doi.org/10.1038/s41586-020-3006-1.
116. Camparo J. The rubidium atomic clock and basic research. Phys Today. 2007;60(11):33–9. https://doi.org/10.1063/1.2812121.
117. Hodges JS et al. Timekeeping with electron spin states in diamond. Phys Rev A. 2013. https://doi.org/10.1103/physreva.87.032118.
118. von der Wense Lars, Seiferle B. The 229Th isomer: prospects for a nuclear optical clock. The European Physical Journal A. 2020;56(11). https://doi.org/10.1140/epja/s10050-020-00263-0.
119. Campbell CJ, et al. Single-Ion Nuclear Clock for Metrology at the 19th Decimal Place. Physical Review Letters. 2012;**108**(12). https://doi.org/10.1103/physrevlett.108.120802.
120. Chu LJ. Physical limitations of omni-directional antennas. J Appl Phys. 1948;19(12):1163–75. https://doi.org/10.1063/1.1715038.
121. Harrington RF. Effect of antenna size on gain, bandwidth, and efficiency. J Res Natl Bur Stand, D Radio Propag. 1960;64D(1):1. https://doi.org/10.6028/jres.064d.003.
122. Facon A et al. A sensitive electrometer based on a Rydberg atom in a Schrödinger-cat state. Nature. 2016;535(7611):262–5. https://doi.org/10.1038/nature18327.
123. Cox KC, et al. Quantum-Limited Atomic Receiver in the Electrically Small Regime. Physical Review Letters. 2018;121(11). https://doi.org/10.1103/physrevlett.121.110502.
124. Meyer DH, Kunz PD, Cox KC. Waveguide-Coupled Rydberg Spectrum Analyzer from 0 to 20 GHz. Physical Review Applied. 2021;15(1). https://doi.org/10.1103/physrevapplied.15.014053.
125. Robinson AK, et al. Determining the Angle-of-Arrival of an Radio-Frequency Source with a Rydberg Atom-Based Sensor; 2021. 2101.12071 [physics.atom-ph].
126. Gariepy G, et al. Single-photon sensitive light-in-fight imaging. Nature Communications. 2015;6(1). https://doi.org/10.1038/ncomms7021.
127. Aspden RS et al. Photon-sparse microscopy: visible light imaging using infrared illumination. Optica. 2015;2(12):1049. https://doi.org/10.1364/optica.2.001049.
128. Moreau P-A et al. Ghost imaging using optical correlations. Laser Photonics Rev. 2017;12(1):1700143. https://doi.org/10.1002/lpor.201700143.
129. Meyers R, Deacon K. Space-time quantum imaging. Entropy. 2015;17(3):1508–34. https://doi.org/10.3390/e17031508.
130. Walborn SP et al. Spatial correlations in parametric down-conversion. Phys Rep. 2010;495(4–5):87–139. https://doi.org/10.1016/j.physrep.2010.06.003.
131. Pelliccia D, et al. Experimental X-Ray Ghost Imaging. Physical Review Letters. 2016;117(11). https://doi.org/10.1103/physrevlett.117.113902.
132. Li S, et al. Electron Ghost Imaging. Physical Review Letters. 2018;121(11). https://doi.org/10.1103/physrevlett.121.114801.
133. Brida G, et al. Measurement of Sub-Shot-Noise Spatial Correlations without Background Subtraction. Physical Review Letters. 2009;102(21). https://doi.org/10.1103/physrevlett.102.213602.
134. Lloyd S. Enhanced sensitivity of photodetection via quantum illumination. Science. 2008;321(5895):1463–5. https://doi.org/10.1126/science.1160627.
135. Smith III JFS. Quantum entangled radar theory and a correction method for the effects of the atmosphere on entanglement. In: Donkor EJ, Pirich AR, Brandt HE, editors. Quantum information and computation VII. 2009. Bellingham: SPIE. https://doi.org/10.1117/12.819918.
136. Barzanjeh S et al. Microwave quantum illumination using a digital receiver. Sci Adv. 2020;6(19):eabb0451. https://doi.org/10.1126/sciadv.abb0451.
137. Luong D, Rajan S, Balaji B. Entanglement-based quantum radar: from myth to reality. IEEE Aerosp Electron Syst Mag. 2020;35(4):22–35. https://doi.org/10.1109/maes.2020.2970261.
138. Maccone L, Ren C. Quantum Radar. Physical Review Letters. 2020;124(20). https://doi.org/10.1103/physrevlett.124.200503.
139. Barzanjeh S, et al. Microwave Quantum Illumination. Physical Review Letters. 2015;114(8). https://doi.org/10.1103/physrevlett.114.080503.
140. Karsa A, Pirandola S. Energetic Considerations in Quantum Target Ranging; 2021. 2011.03637 [quant-ph].
141. Lanzagorta M. Quantum radar. In: Synthesis digital library of engineering and computer science. San Mateo: Morgan Kaufmann; 2011. ISBN 9781608458264.
142. Pirandola S et al. Advances in photonic quantum sensing. Nat Photonics. 2018;12(12):724–33. https://doi.org/10.1038/s41566-018-0301-6.
143. Zhuang Q, Pirandola S. Entanglement-enhanced testing of multiple quantum hypotheses. Communications Physics. 2020;3(1). https://doi.org/10.1038/s42005-020-0369-4.

144. Chu Y et al. Quantum acoustics with superconducting qubits. Science. 2017;358(6360):199–202. https://doi.org/10.1126/science.aao1511.
145. Satzinger KJ et al. Quantum control of surface acoustic-wave phonons. Nature. 2018;563(7733):661–5. https://doi.org/10.1038/s41586-018-0719-5.
146. Wu H, et al. Beat frequency quartz-enhanced photoacoustic spectroscopy for fast and calibration-free continuous trace-gas monitoring. Nature Communications. 2017;8(1). https://doi.org/10.1038/ncomms15331.
147. Fischer B. Optical microphone hears ultrasound. Nat Photonics. 2016;10(6):356–8. https://doi.org/10.1038/nphoton.2016.95.
148. Faist J et al. Quantum cascade laser. Science. 1994;264(5158):553–6. https://doi.org/10.1126/science.264.5158.553.
149. Khalatpour A et al. High-power portable terahertz laser systems. Nat Photonics. 2020. https://doi.org/10.1038/s41566-020-00707-5.
150. Reding DF, Eaton J. Science & technology trends 2020-2040. NATO science & technology organization. 2020.
151. Makarov V, Hjelme DR. Faked states attack on quantum cryptosystems. J Mod Opt. 2005;52(5):691–705. https://doi.org/10.1080/09500340410001730986.
152. Zhao Y, et al. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Physical Review A. 2008;78(4). https://doi.org/10.1103/physreva.78.042333.
153. Lydersen L et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat Photonics. 2010;4(10):686–9. https://doi.org/10.1038/nphoton.2010.214.
154. Gerhardt I, et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications. 2011;2(1). https://doi.org/10.1038/ncomms1348.
155. Bugge AN, et al. Laser Damage Helps the Eavesdropper in Quantum Cryptography. Physical Review Letters. 2014;112(7). https://doi.org/10.1103/physrevlett.112.070503.
156. Vermeer MJD, Peet ED. Securing communications in the quantum computing age: managing the risks to encryption. Santa Monica: RAND Corporation; 2020. https://doi.org/10.7249/RR3102.
157. Pirandola S et al. Advances in quantum cryptography. In: Advances in optics and photonics. 2020. p. 1012. https://doi.org/10.1364/aop.361502.
158. Lindsay JR. Demystifying the quantum threat: infrastructure, institutions, and intelligence advantage. Secur Stud. 2020;29(2):335–61. https://doi.org/10.1080/09636412.2020.1722853.
159. Herman A, Friedson I. Quantum computing: how to address the national security risk. Hudson Institute; 2018.
160. European Commission. Joint Research Centre. The impact of quantum technologies on the EU's future policies. Part 2, Quantum communications: from science to policies. Publications Office; 2018. ISBN: 978-92-79-77314-3. https://doi.org/10.2760/881896.
161. Kline K, Salvo M, Johnson D. How artificial intelligence and quantum computing are evolving cyber warfare. Cyber intelligence initiative, The Institute of World Politics. 2019. https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/ (visited on 02/24/2021).
162. Wolf SA et al. The changing face of data security: 2020 Thales data threat report. Thales. 2020.
163. Gil D. How to Preserve the Privacy of Your Genomic Data. Scientific American. Nov. 2020. URL: https://www.scientificamerican.com/article/how-to-preserve-the-privacy-of-your-genomic-data/ (visited on 11/11/2020).
164. Huang H-L, et al. Homomorphic encryption experiments on IBM's cloud quantum computing platform. Front Phys. 2016;12(1). https://doi.org/10.1007/s11467-016-0643-9.
165. Cameron L. Internet of Things Meets the Military and Battlefield. IEEE Computer Society. URL: https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt (visited on 03/29/2021).
166. Fernandez-Carames TM. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of things. IEEE Int Things J. 2020;7(7):6457–80. https://doi.org/10.1109/jiot.2019.2958788.
167. Moskovich D. An Overview of the State of the Art for Practical Quantum Key Distribution. 2015. 1504.05471 [quant-ph].
168. Lucamarini M, et al. Implementation Security of Quantum Cryptography. 2018. ETSI White Paper No. 27.
169. European Commission. The European Quantum Communication Infrastructure (EuroQCI) Initiative. Oct. 26, 2020. URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (visited on 09/08/2021).
170. National Security Agency (NSA). NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography. Oct. 2020;26. https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2394053/nsa-cybersecurity-perspectives-on-quantum-key-distribution-and-quantum-cryptogr/ (visited on 09/08/2021).
171. Abellan C, Pruneri V. The future of cybersecurity is quantum. IEEE Spectr. 2018;55(7):30–5. https://doi.org/10.1109/mspec.2018.8389185.
172. Kelsey J et al. Cryptanalytic attacks on pseudorandom number generators. In: Vaudenay S, editor. Fast software encryption. Berlin: Springer. 1998. p. 168–88. ISBN 978-3-540-69710-7.
173. Mosca M, Mulholland J. A methodology for quantum risk assessment. GRI (Global Risk Institute); 2017.
174. Bogomolec X, Underhill JG, Kovac SA. Towards Post-Quantum Secure Symmetric Cryptography: a Mathematical Perspective. Cryptology. ePrint Archive, Report 2019/1208. 2019.
175. Satoh T et al. Attacking the quantum Internet. 2020. 2005.04617 [quant-ph].
176. Lavoix H. Quantum Optimization and the Future of Government. The Red Team Analysis Society. Oct. 2019. URL: https://www.redanalysis.org/2019/10/28/optimisation-quantique-et-futur-gouvernements/ (visited on 11/17/2020).
177. Uppal R. Military decision support require efficient optimization algorithms. International Defense Security & Technology. Oct. 2019. URL: https://idstch.com/technology/ict/military-decision-support-require-efficient-optimization-algorithms/ (visited on 01/27/2021).

178. Wilson JR. The future of artificial intelligence and quantum computing. Military & Aerospace Electronics. Aug. 2020. URL: https://www.militaryaerospace.com/computers/article/14182330/future-of-artificial-intelligence-and-quantum-computing (visited on 01/27/2021).
179. Allen EH, Tallant GS, Elliot MA. Computer systems and methods for quantum verification and validation. US patent US8832165B2. 2010.
180. Quantum Computing: Spot-Checking Millions of Lines of Code. Lockheed Martin; 2017. URL: https://www.lockheedmartin.com/en-us/news/features/2017/quantum-computing-spot-checking-millions-lines-code.html (visited on 11/17/2020).
181. Huang H-Y et al. Power of data in quantum machine learning. Nat Commun. 2021. https://doi.org/10.1038/s41467-021-22539-9.
182. Artificial Intelligence and Machine Learning in Defense Applications et al., eds. Artificial Intelligence and Machine Learning in Defense Applications: 10-12 September 2019, Strasbourg, France. English. OCLC: 1130085146. 2019. ISBN: 9781510630413.
183. De Spiegeleire S, Maas M, Sweijs T. Artificial intelligence and the future of defense: strategic implications for small- and medium-sized force providers. The Hague Centre for Strategic Studies (HCSS); 2017.
184. Chancé A. Quantum machine learning is going to be the biggest application of quantum computing in the next ten years. http://quantumwa.org/wp-content/uploads/2018/09/Peter-Wittek-Quantum-machine-learning-is-going-to-be-the-biggest-application-of-quantum-computing-in-the-next-ten-years.pdf.pdf. Interview with Prof. Peter Wittek. 2018.
185. Huggins W et al. Towards quantum machine learning with tensor networks. Quantum Sci Technol. 2019;4(2):024001. https://doi.org/10.1088/2058-9565/aaea94.
186. Neumann NMP, van Heesch MPP, de Graaf P. Quantum Communication for Military Applications. 2020. 2011.04989 [quant-ph].
187. Quantum security technologies. NCSC (white paper). Mar. 2020. URL: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies (visited on 11/25/2020).
188. Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A. 2002;65(3). https://doi.org/10.1103/physreva.65.032302.
189. Boström K, Felbinger T. Deterministic Secure Direct Communication Using Entanglement. Physical Review Letters. 2002;89(18). https://doi.org/10.1103/physrevlett.89.187902.
190. Zhang W et al. Quantum Secure Direct Communication with Quantum Memory. Physical Review Letters. 2017;118(22). https://doi.org/10.1103/physrevlett.118.220501.
191. Qi R, et al. Implementation and security analysis of practical quantum secure direct communication. Light Sci Appl. 2019;8(1). https://doi.org/10.1038/s41377-019-0132-3.
192. Gao G. Two quantum dialogue protocols without information leakage. Opt Commun. 2010;283(10):2288–93. https://doi.org/10.1016/j.optcom.2010.01.022.
193. Han L-F et al. Multiparty quantum secret sharing of secure direct communication using single photons. Opt Commun. 2008;281(9):2690–4. https://doi.org/10.1016/j.optcom.2007.12.045.
194. You X, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci. 2020;64(1). https://doi.org/10.1007/s11432-020-2955-6.
195. Gottesman D, Chuang I. Quantum digital signatures. arXiv e-prints. May 2001. quant-ph/0105032 [quant-ph].
196. Malaney RA. Quantum location verification in noisy channels. In: 2010 IEEE global telecommunications conference GLOBECOM 2010. New York: IEEE; 2010. https://doi.org/10.1109/glocom.2010.5684009.
197. Chakraborty K, Leverrier A. Practical position-based quantum cryptography. Physical Review A. 2015;92(5). https://doi.org/10.1103/physreva.92.052304.
198. Kómár P et al. A quantum network of clocks. Nat Phys. 2014;10(8):582–7. https://doi.org/10.1038/nphys3000.
199. Giovannetti V, Lloyd S, Maccone L. Quantum-enhanced positioning and clock synchronization. Nature. 2001;412(6845):417–9. https://doi.org/10.1038/35086525.
200. Jozsa R et al. Quantum clock synchronization based on shared prior entanglement. Phys Rev Lett. 2000;85(9):2010–3. https://doi.org/10.1103/physrevlett.85.2010.
201. Krawinkel T, Schön S. Benefits of Chip Scale Atomic Clocks in GNSS Applications. 2015. p. 2867–2874.
202. Bahder TB. Quantum positioning system; 2004. quant-ph/0406126.
203. Yang C, Wu D, Yu Y. The integration of GPS and interferometric quantum position system for high dynamic precise positioning. In: The 2010 IEEE international conference on information and automation. New York: IEEE; 2010. https://doi.org/10.1109/icinfa.2010.5512389.
204. Travagnin M. Cold atom interferometry for inertial navigation sensors: technology assessment: space and defence applications. EUR 30492 EN, JRC122785. Publications Office of the European Union; 2020. ISBN 978-92-76-27076-8. https://doi.org/10.2760/237221.
205. Lutwak R. Micro-Technology for Positioning, Navigation, and Timing Towards PNT Everywhere and Always. DARPA Dec. 2014;10. https://www.gps.gov/governance/advisory/meetings/2014-12/lutwak.pdf (visited on 09/10/2021).
206. Lewis A, et al. Quantum Technologies: implications for European Policy. 2016. EUR 28103 EN, EU JRC Science Hub.
207. Bongs K et al. Taking atom interferometric quantum sensors from the laboratory to real-world applications. Nat Rev Phys. 2019;1(12):731–9. https://doi.org/10.1038/s42254-019-0117-4.
208. El-Sheimy N, Youssef A. Inertial sensors technologies for navigation applications: state of the art and future trends. Satell Navig. 2020;1(1). https://doi.org/10.1186/s43020-019-0001-5.
209. Savoie D et al. Interleaved atom interferometry for high-sensitivity inertial measurements. Sci Adv. 2018;4(12):eaau7948. https://doi.org/10.1126/sciadv.aau7948.
210. Wang X, et al. Enhancing Inertial Navigation Performance via Fusion of Classical and Quantum Accelerometers. 2103.09378 [quant-ph].
211. Battelier B et al. Development of compact cold-atom sensors for inertial navigation. In: Stuhler J, Shields AJ, editors. Quantum optics. 2016. Bellingham: SPIE. https://doi.org/10.1117/12.2228351.
212. ColdQuanta. High-BIAS2 Accelerates Quantum Sensing Into Commercialization With New Milestones For Quantum Positioning System. Press release. Apr. 2021. URL: https://www.prnewswire.co.uk/news-releases/high-bias2-accelerates-quantum-sensing-into-commercialization-with-new-milestones-for-quantum-positioning-system-859771353.html (visited on 09/08/2021).

213. Canciani A, Raquet J. Airborne magnetic anomaly navigation. IEEE Trans Aerosp Electron Syst. 2017;53(1):67–80. https://doi.org/10.1109/taes.2017.2649238.
214. Quantum Physicists Found a New, Safer Way to Navigate. Wired. Jan. 2018. URL: https://www.wired.com/story/quantum-physicists-found-a-new-safer-way-to-navigate/?from=article_link (visited on 12/17/2020).
215. Moryl J, Rice H, Shinners S. The universal gravity module for enhanced submarine navigation. In: IEEE 1998 position location and navigation symposium (Cat. No. 98CH36153). New York: IEEE; 1998. https://doi.org/10.1109/plans.1998.670124.
216. Ménoret V, et al. Gravity measurements below 10-9 g with a transportable absolute quantum gravimeter. Scientific Reports. 2018;8(1). https://doi.org/10.1038/s41598-018-30608-1.
217. Bidel Y, et al. Absolute marine gravimetry with matter-wave interferometry. Nature Communications. 2018;9(1). https://doi.org/10.1038/s41467-018-03040-2.
218. Sandwell DT et al. New global marine gravity model from CryoSat-2 and Jason-1 reveals buried tectonic structure. Science. 2014;346(6205):65–7. https://doi.org/10.1126/science.1258213.
219. Bidel Y, et al. Absolute airborne gravimetry with a cold atom sensor. Journal of Geodesy. 2020;94(2). https://doi.org/10.1007/s00190-020-01350-2.
220. Travagnin M. Cold atom interferometry for earth observation: perspectives for satellite based quantum gravimetry. European Commission. Joint Research Centre. Publications Office; 2020. https://doi.org/10.2760/225071.
221. Mahadeswaraswamy C. Atom interferometric gravity gradiometer: disturbance compensation and mobile gradiometry. PhD thesis. Stanford University; 2009.
222. Geiger R, et al. Detecting inertial effects with airborne matter-wave interferometry. Nature Communications. 2011;2(1). https://doi.org/10.1038/ncomms1479.
223. Perkins S. Tiny gravity sensor could detect drug tunnels, mineral deposits. Science. 2016. https://doi.org/10.1126/science.aaf9852.
224. Guo R. Cross-border resource management: theory and practice. Developments in environmental science 4. OCLC: 255072969. 1st ed. Amsterdam: Elsevier; 2005. ISBN 9780444519153.
225. Battersby S. The quantum age: technological opportunities. UK Government Office for Science; 2016.
226. Gravity sensors see underground. Gravity Pioneer project, UK National Quantum Technologies Programme; 2019.
227. Marmugi L et al. Remote detection of rotating machinery with a portable atomic magnetometer. Appl Opt. 2017;56(3):743. https://doi.org/10.1364/ao.56.000743.
228. Hussain SY. Application of quantum magnetometers to security and defence screening. London: University College London; 2018.
229. Bond A, Brown L. The Suitability of Quantum Magnetometers for Defence Applications. Thales, UDT; 2019.
230. Kumar S et al. Real-time tracking magnetic gradiometer for underwater mine detection. In: Oceans'04 MTS/IEEE Techno-Ocean'04 (IEEE Cat. No. 04CH37600). New York: IEEE; 2004. https://doi.org/10.1109/oceans.2004.1405583.
231. Streland AH. A system concept for detecting deeply buried facilities from space. Fort Belvoir: Defense Technical Information Center; 2003. https://doi.org/10.21236/ADA424602. (Visited on 02/26/2021).
232. QLM Technology Ltd. Quantum Gas Cameras for Continuous Industrial Methane Monitoring. Product Brochure; 2021.
233. Cohen L, et al. Thresholded Quantum LIDAR: Exploiting Photon-Number-Resolving Detection. Physical Review Letters. 2019;123(20). https://doi.org/10.1103/physrevlett.123.203601.
234. Frick S, McMillan A, Rarity J. Quantum rangefinding. Opt Express. 2020;28(25):37118. https://doi.org/10.1364/oe.399902.
235. Hardy ND, Shapiro JH. Computational ghost imaging versus imaging laser radar for three-dimensional imaging. Physical Review A. 2013;87(2). https://doi.org/10.1103/physreva.87.023820.
236. Meyer DH et al. Assessment of Rydberg atoms for wideband electric field sensing. J Phys B, At Mol Opt Phys. 2020;53(3):034001. https://doi.org/10.1088/1361-6455/ab6051.
237. ColdQuanta. QRF - Technology Deep Dive. 2021. URL: https://cdn.sanity.io/files/sbcw1clc/production/7bd897d88fc744d0ef0ae7725ceff5475699eb33.pdf.
238. Baili G et al. Quantum-based metrology for timing, navigation and RF spectrum analysis. In: Quantum technologies in optronics. European Defence Agency; 2019. https://doi.org/10.2836/848731.
239. Pietrzak J. Laser warning receivers. In: Wolinski WL, Jankiewicz Z, Romaniuk R, editors. Laser technology VII: applications of lasers. Bellingham: SPIE; 2003. https://doi.org/10.1117/12.520769.
240. Fei Y-Y, et al. Quantum man-in-the-middle attack on the calibration process of quantum key distribution. Scientific Reports. 2018;8(1). https://doi.org/10.1038/s41598-018-22700-3.
241. Vergoossen T et al. Satellite quantum communications when man-in-the-middle attacks are excluded. Entropy. 2019;21(4):387. https://doi.org/10.3390/e21040387.
242. Lee MS et al. Quantum hacking on a free-space quantum key distribution system without measuring quantum signals. J Opt Soc Am B. 2019;36(3):B77. https://doi.org/10.1364/josab.36.000b77.
243. Gallego Torromé R, Ben Bekhti-Winkel N, Knott P. Introduction to quantum radar. 2021. 2006.14238 [quant-ph].
244. Shapiro JH. The quantum illumination story. IEEE Aerosp Electron Syst Mag. 2020;35(4):8–20. https://doi.org/10.1109/maes.2019.2957870.
245. China's quantum radar was successfully developed. [in Chinese]. Phoenix News. Sept. 2016. URL: http://news.ifeng.com/a/20160907/49929146_0.shtml (visited on 10/06/2020).
246. China Shows Off First Quantum Radar Prototype. Aviation Week. Nov. 2018. URL: https://aviationweek.com/defense-space/china-shows-first-quantum-radar-prototype (visited on 10/06/2020).
247. Daum F. Quantum radar cost and practical issues. IEEE Aerosp Electron Syst Mag. 2020;35(11):8–20. https://doi.org/10.1109/maes.2020.2982755.
248. Karsa A, et al. Quantum illumination with a generic Gaussian source. Physical Review Research. 2020;2(2). https://doi.org/10.1103/physrevresearch.2.023414.
249. Luong D et al. Receiver operating characteristics for a prototype quantum two-mode squeezing radar. IEEE Trans Aerosp Electron Syst. 2020;56(3):2041–60. https://doi.org/10.1109/taes.2019.2951213.

250. Lanzagorta M. Quantum radar cross sections. In: Zadkov VN, Durt T, editors. Quantum optics. 2010. Bellingham: SPIE. https://doi.org/10.1117/12.854935.
251. Brandsema MJ, Narayanan RM, Lanzagorta M. Theoretical and computational analysis of the quantum radar cross section for simple geometrical targets. Quantum Information Processing. 2016;16(1). https://doi.org/10.1007/s11128-016-1494-6.
252. Brandsema MJ, Lanzagorta M, Narayanan RM. Equivalence of classical and quantum electromagnetic scattering in the far-field regime. IEEE Aerosp Electron Syst Mag. 2020;35(4):58–73. https://doi.org/10.1109/maes.2020.2970264.
253. Sandbo Chang CW et al. Quantum-enhanced noise radar. Appl Phys Lett. 2019;114(11):112601. https://doi.org/10.1063/1.5085002.
254. Lukin K. Evolution of quantum radar concept to noise radar concept. IEEE Aerosp Electron Syst Mag. 2020;35(11):30–6. https://doi.org/10.1109/maes.2020.3004015.
255. Pawlikowska AM et al. Single-photon three-dimensional imaging at up to 10 kilometers range. Opt Express. 2017;25(10):11919. https://doi.org/10.1364/oe.25.011919.
256. Li Z-P et al. Single-photon computational 3D imaging at 45 km. Photon Res. 2020;8(9):1532. https://doi.org/10.1364/prj.390091.
257. Lanzagorta M, Uhlmann J. Space-based quantum sensing for low-power detection of small targets. In: Ranney KI et al., editors. Radar sensor technology XIX and active and passive signatures VI. 2015. Bellingham: SPIE. https://doi.org/10.1117/12.2183326.
258. Koblick DC, Wilkinson S. Space-based spooky radar orbit determination benefits at Earth-Moon Lagrange points. In: AMOS 2020, 2020. p. 13.
259. Future space domain awareness. Raytheon Intelligence and space. Sept. 2020. URL: https://www.raytheonintelligenceandspace.com/news/feature/future-space-domain-awareness (visited on 01/21/2021).
260. Transforming detection with quantum-enabled radar. University of Birmingham, 2020. URL: https://www.birmingham.ac.uk/news/latest/2020/12/transforming-detection-with-quantum-enabled-radar.aspx (visited on 02/02/2021).
261. Kubiak K. Quantum technology and submarine near-invulnerability. Global security policy brief, European leadership network. 2020.
262. Lanzagorta M. Quantum imaging for underwater Arctic navigation. In: Ranney KI, Doerry A, editors. Radar sensor technology XXI. 2017. Bellingham: SPIE. https://doi.org/10.1117/12.2262654.
263. Hambling D. China's quantum submarine detector could seal South China Sea. New Scientist. Aug. 2017. URL: https://www.newscientist.com/article/2144721-chinas-quantum-submarine-detector-could-seal-south-china-sea/ (visited on 03/01/2021).
264. Roblin S. No More 'Stealth' Submarines: Could Quantum 'Radar' Make Submarines Easy to Track (And Kill)? The National Interest. Apr. 2019. URL: https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547 (visited on 10/14/2020).
265. Al-Rodhan N. Weaponization and Outer Space Security. Global Policy Journal. 2020. URL: https://www.globalpolicyjournal.com/blog/12/03/2018/weaponization-and-outer-space-security (visited on 02/27/2021).
266. Harris M. Why satellite mega-constellations are a threat to the future of space. MIT Technology Review. 2019. URL: https://www.technologyreview.com/2019/03/29/136268/why-satellite-mega-constellations-are-a-massive-threat-to-safety-in-space/ (visited on 01/29/2021).
267. Quantum Technologies in Space - Intermediate Strategic Report for ESA and national space agencies. QTSpace. 2017.
268. Jia B et al. Quantum technology for aerospace applications. In: Pham KD, Cox JL, editors. Sensors and systems for space applications VII. 2014. Bellingham: SPIE. https://doi.org/10.1117/12.2050032.
269. Oi DKL et al. CubeSat quantum communications mission. EPJ Quantum Technol. 2017;4(1). https://doi.org/10.1140/epjqt/s40507-017-0060-1.
270. Sidhu JS et al. Advances in Space Quantum Communications. 2021. 2103.12749 [quant-ph].
271. Pirandola S. Satellite Quantum Communications: Fundamental Bounds and Practical Security. 2021. 2012.01725 [quant-ph].
272. Hautaluoma G. NASA Awards Prizes to Six Startup Companies in Entrepreneur's Challenge. NASA. Dec. 2020. URL: https://www.nasa.gov/press-release/nasa-awards-prizes-to-six-startup-companies-in-entrepreneur-s-challenge (visited on 12/19/2020).
273. South China Morning Post. Could ghost imaging spy satellite be a game changer for Chinese military? IBM. 2017. URL: https://www.scmp.com/news/china/society/article/2121479/could-ghost-imaging-spy-satellite-be-game-changer-chinese (visited on 03/01/2021).
274. Liao S-K et al. Satellite-to-ground quantum key distribution. Nature. 2017;549(7670):43–7. https://doi.org/10.1038/nature23655.
275. Chen Y-A et al. An integrated space-to-ground quantum communication network over 4, 600 kilometres. Nature. 2021;589(7841):214–9. https://doi.org/10.1038/s41586-020-03093-8.
276. Cao Y, et al. Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution. Physical Review Letters. 2020;125(26). https://doi.org/10.1103/physrevlett.125.260503.
277. Erwin S. Space Fence surveillance radar site declared operational. Space News. 2019. URL: https://spacenews.com/space-fence-surveillance-radar-site-declared-operational/ (visited on 01/29/2021).
278. Aspuru-Guzik A. Simulated quantum computation of molecular energies. Science. 2005;309(5741):1704–7. https://doi.org/10.1126/science.1113479.
279. Chinese team lead by Pan Jianwei is expected to realize a 60-bit quantum computer this year. Quantum Hermit. Sept. 2020. URL: http://quantumhermit.com/chinese-team-lead-by-pan-jianwei-is-expected-to-realize-a-60-bit-quantum-computer-this-year/ (visited on 11/10/2020).
280. Emani PS et al. Quantum computing at the frontiers of biological sciences. 2019. 1911.07127 [quant-ph].

281. Wheelis M, Dando M. New technology and future developments in biological warfare. In: Vignard K, editor. Biological weapons: from the BWC to biotech. 2000. p. 43–53. Disarmament Forum 4. UNIDIR.
282. Kumar C, Patel N. Quantum cascade laser based techniques for the detection of explosives, chemical warfare agents and toxic industrial chemicals. In: 2007 international workshop on physics of semiconductor devices. New York: IEEE; 2007. https://doi.org/10.1109/iwpsd.2007.4472446.
283. Li JS et al. Contributed review: quantum cascade laser based photoacoustic detection of explosives. Rev Sci Instrum. 2015;86(3):031501. https://doi.org/10.1063/1.4916105.
284. Burkhart F. Airborne sensors: challenges and opportunities. SPIE. Apr. 2017. URL: https://optics.org/news/8/4/26 (visited on 12/21/2010).
285. Cirac JI, Zoller P. Goals and opportunities in quantum simulation. Nat Phys. 2012;8(4):264–6. https://doi.org/10.1038/nphys2275.
286. Kessler E. Introduction to Quantum Computing on AWS. AWS Online Tech Talks. August 24, 2020.
287. Tierney TM et al. Optically pumped magnetometers: from quantum origins to multi-channel magnetoencephalography. NeuroImage. 2019;199:598–608. https://doi.org/10.1016/j.neuroimage.2019.05.063.
288. Biercuk MJ. Hype and cash are muddying public understanding of quantum computing. The Conversation. 2017. URL: https://theconversation.com/hype-and-cash-are-muddying-public-understanding-of-quantum-computing-82647 (visited on 02/27/2021).
289. Kania EB, Costello J. Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership. Center for a New American Security. Sept. 2018.
290. Defence Technology Framework: Defence Science and Technology. UK MoD Defence Science and Technology. 2019.
291. Work Programme 2021-2022 - 7. Digital, Industry and Space. Horizon Europe. 2021.
292. Announcement No. 63 (2020) of the Ministry of Commerce, the State Encryption Administration, and the General Administration of Customs, Announcement on Issuing the List of Commercial Encryption Import Licenses, Export Control Lists, and Related Management Measures. Ministry of Commerce of the People's Republic of China. Dec. 2020. URL. http://www.mofcom.gov.cn/article/zwgk/zcfb/202012/20201203019733.shtml (visited on 03/01/2021).
293. Castellanos S. Quantum Computing Scientists Call for Ethical Guidelines. Wall Street Journal. (Feb. 2021). ISSN: 0099-9660. URL: https://www.wsj.com/articles/quantum-computing-scientists-call-for-ethical-guidelines-11612155660 (visited on 03/01/2021).
294. Khan I. Will Quantum Computers Truly Serve Humanity? Feb. 2021. URL: https://www.scientificamerican.com/article/will-quantum-computers-truly-serve-humanity/ (visited on 03/01/2021).
295. Quantum Computing Ethics. URL: https://www.weforum.org/projects/quantum-computing-ethics/ (visited on 03/01/2021).
296. Pfaff CA. The ethics of acquiring disruptive military technologies. Texas National Security Review. 2020;3(1):34–61.
297. Altmann J. Technology, Arms Control and World Order: Fundamental Change Needed. Toda Peace Institute, Policy Brief No. 89. Sept. 2020, p. 16.
298. Altmann J. New military technologies: dangers for international security and peace. Sicherheit & Frieden. 2020;38(1):36–42. https://doi.org/10.5771/0175-274X-2020-1-36. ISSN: 0175-274X.
299. Altmann J. Nanotechnology and preventive arms control. Deutsche stiftung friedens-forschung DSF. 2005.
300. Venegas-Gomez A. The quantum ecosystem and its future workforce. PhotonicsViews. 2020;17(6):34–8. https://doi.org/10.1002/phvs.202000044.