# Quantum Computing: Applications in the Defense Sector

Gautam Bhatia
gbhatia@umd.edu

Robert H. Smith School of Business, University of Maryland
College Park, MD 20742, USA

**Keywords**

Quantum Computing; Quantum Simulation; Quantum Cryptography; Quantum Optimization; Quantum Communication Network; Quantum Key Distribution (QKD); Post-Quantum Cryptography; Defense Applications

## Table of Contents

## 1 Introduction

Quantum technology is an emergent and potentially disruptive field poised to revolutionize various aspects of human activity, including defense and security. By leveraging the fundamental principles of quantum mechanics—particularly quantum entanglement, superposition, and tunneling—quantum technology offers unprecedented precision and capabilities across a wide array of applications. These include quantum computing, sensing, communication, and cryptography, each with significant implications for military and defense operations.

The second quantum revolution [1], characterized by the ability to manipulate and control individual quantum systems, has opened new avenues for technological advancements. Quantum computing, a central component of this revolution, holds the potential to perform complex calculations at speeds unattainable by classical computers, thereby enhancing strategic decision-making, cryptographic security, and operational efficiency in the defense sector.

This report provides an in-depth analysis of quantum computing and its applications within the defense sector. It covers the current state of quantum computing technology, its integration with other quantum technologies, and its potential to address critical defense challenges. The report also explores the expected timelines for the deployment of various quantum technologies and outlines strategic recommendations for leveraging these advancements to maintain a competitive edge in military operations.

By understanding the transformative potential of quantum computing and related technologies, defense organizations can develop comprehensive strategies to harness these innovations effectively. This includes fostering collaboration between academia, industry, and government, investing in research and development, and preparing for the integration of quantum technologies into existing defense systems and protocols.

The subsequent sections of this report will delve into the specific aspects of quantum computing, including its types, key concepts, and applications, followed by an exploration of quantum communication, cryptography, sensing, and metrology. Each section will highlight the current status, challenges, and future prospects of these technologies, providing a detailed overview of how quantum advancements are shaping the future of defense.

## 2 Quantum Information Science

Quantum information science deals with the flow of quantum information in computing and communications. Key concepts include:

- ***Qubits****:* The fundamental unit of quantum information, which can be in a state of 0, 1, or both simultaneously due to superposition.
- ***Quantum Entanglement****:* A phenomenon where qubits become intertwined, such that the state of one qubit instantly influences the state of another, regardless of distance.
- ***No-Cloning Theorem****:* A principle stating that it is impossible to create an identical copy of an unknown quantum state, ensuring the security of quantum information. [2]

## 3 Quantum Computing and Simulations

Quantum computing refers to the utilization of quantum information science to perform computations. Such a machine can be called a quantum computer.

### 3.1 Quantum Computers

Quantum computers utilize qubits, which can exist in multiple states simultaneously, unlike classical bits that are either 0 or 1. This property enables quantum computers to process complex calculations at unprecedented speeds. There are several types of quantum computers, each with unique characteristics:

1. ***Digital Quantum Computers**:* Universal and programmable, these computers can perform a wide range of quantum algorithms. They are based on quantum gates and circuits, allowing them to execute complex computations that are infeasible for classical computers.
2. ***Analog Quantum Computers**:* These computers are limited to specific types of calculations, such as optimization problems, using quantum annealing. They are not universal but are highly efficient for particular tasks like finding the ground state of a system.
3. ***Quantum Simulators**:* Designed to simulate specific quantum systems, these simulators are useful for studying materials and chemical reactions. They are not programmable like digital quantum computers but can model complex quantum interactions effectively.

### 3.2 Leading-Edge Quantum Computers and Their Development Timelines

Examples of state-of-the-art quantum computers include Google's 53-qubit superconducting quantum computer, which claimed quantum supremacy in 2019 [3], and IBM's quantum computer. Among trapped-ion quantum computers, IonQ's 32-qubit system and Honeywell's six-qubit system are notable. In the realm of photonic qubits, Xanadu has developed a 24-qubit quantum computer. According to the quantum computing roadmaps of IBM and Google, IBM aims to produce a 433-qubit quantum processor in 2022 and reach 1,121 qubits by 2023 [4]. Google plans to develop a 10,000-qubit quantum module, with a goal of integrating such modules into a system with up to 1 million qubits by 2029 [5].

A survey of experts in quantum science and technology suggests that within two decades, quantum computers will likely become powerful enough to threaten most public key encryption schemes [6]. Examples of analogue quantum computers include D-Wave Systems' quantum annealer with over 5,000 qubits and Toshiba's coherent Ising machine.

The primary difference between analogue and digital quantum computers lies in their physical principles and limitations. Digital quantum computers are constrained by resources rather than noise, as noise can be corrected with additional resources. In contrast, analogue quantum computers are significantly affected by noise, which is difficult to manage and characterize, especially in quantum annealers, thus limiting their applicability. [7]

In practice, the tasks performed by quantum computers will primarily serve as subprograms or subroutines within classical computer programs. Classical computers will not only control quantum computers but also handle many computations that are impractical for quantum computers. Given the large size and cryogenic requirements of many quantum computers, it is unlikely that personal quantum computers will become common in the near future. Instead, most users will access quantum computing via cloud-based services. Quantum Computing-as-a-Service (QCaaS) is currently available and allows users to access quantum computers through platforms such as Microsoft Azure Quantum and Amazon Braket, which offer quantum computing resources from various manufacturers.

Understanding the terms "quantum supremacy," "quantum advantage," and "quantum practicality" is also important. Quantum supremacy occurs when a quantum computer solves a problem significantly faster than a classical computer, typically a theoretical problem. Quantum advantage refers to a quantum computer's ability to solve practical, real-world problems that classical computers cannot. Quantum practicality is similar to quantum advantage but emphasizes solving real-world problems faster than classical computers.

## 4 Quantum Computing Applications

### 4.1 Quantum Simulations

*Status:* Algorithms are in development, with small-scale applications currently being explored
*Timeline Expectation:* In 0-5 years, usability scales up with the number of qubits available
*Qubits Requirement:* Approximately 200 qubits are needed for specific problems, such as the nitrogen fixation problem
*Main Challenges:* Increasing the number of logical qubits to perform more complex simulations

**Current State and Significance**:

Long before the first quantum computer was created, its primary anticipated application was the simulation of other quantum systems, such as molecules [8]. Despite advancements in computational power, fully simulating complex molecules using classical computational chemistry is challenging and often requires many approximations and simplifications. For instance, simulating a system with n electrons on a classical computer requires $n^2$ bits to describe the electron states, whereas a quantum computer only needs n qubits. This makes quantum simulations particularly promising and feasible as one of the first major applications for quantum computers.

**Dominant Approaches**:

1. ***Quantum-Phase Estimation (QPE)****:* This approach is used to estimate the eigenvalues of a unitary operator and is vital for quantum simulations. It is highly accurate but also resource-intensive, requiring a significant number of qubits and quantum gates [9].
2. ***Quantum Variational Techniques (VQE)****:* The Variational Quantum Eigensolver (VQE) is particularly promising for near-term intermediate-scale quantum (NISQ) computers. VQE combines quantum and classical computing to optimize parameters and find the ground state energy of a quantum system [10]. In 2020, Google performed the largest quantum chemical simulation to date using VQE to simulate the H12 molecule, demonstrating the potential of this approach [11].

The ability to perform quantum simulations effectively depends on the development of algorithms and the scaling up of qubit numbers. Despite these challenges, the potential benefits make quantum simulations a focal point of interest for advancing quantum computing capabilities in defense sectors.

### 4.2 Quantum Cryptoanalysis

*Status:* Algorithms are ready
*Timeline Expectation*: 6-20 years
*Qubits Requirement:* Approximately 6,200 qubits are needed for 2048-bit RSA factorization, and around 2,900 qubits are required for 256-bit Elliptic Curve Discrete Logarithm Problem (ECDLP)-based encryption
*Main Challenges:* Increasing the number of logical qubits

**Current State and Significance**:

One of the most well-known applications of quantum computers is the factorization of large prime numbers with exponential speedup using Shor's algorithm. This poses a significant threat to public-key cryptography schemes, such as Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC), which rely on the difficulty of these mathematical problems for security.
Although current NISQ (Noisy Intermediate-Scale Quantum) computers do not yet have the resources needed to break RSA encryption, the threat is real and imminent. Adversaries or foreign intelligence agencies could intercept, and store encrypted communications today, with the intention of decrypting them once quantum cryptoanalysis becomes feasible. Given that the declassification period for many secrets extends well beyond the expected timeline for the development of powerful quantum computers, this threat needs to be addressed now.

**Quantum Algorithms for Cryptoanalysis**:

1. ***Shor's Algorithm****:* This algorithm allows for the factorization of large prime numbers exponentially faster than classical algorithms, threatening the security of RSA, DH, and ECC-based cryptosystems. For instance, breaking a 2048-bit RSA encryption key requires around 6,200 qubits [12].
2. ***Grover's Algorithm****:* This algorithm provides a quadratic speedup for brute-force attacks on symmetric encryption schemes. It effectively reduces the security of a 256-bit AES key to 128-bit security, making it vulnerable to brute-force attacks with approximately $2^{218}$ quantum operations [13].
3. ***Simon's Algorithm****:* This algorithm, along with superposition queries, can completely break most message authentication codes (MAC) and authenticated encryption with associated data (AEAD) schemes, such as HMAC-CBC and AES-GCM [14].
4. ***Structural Attacks on Symmetric Key Systems****:* Ongoing research explores crypto analytic attacks on symmetric key systems by exploiting the structure inherent in these cryptosystems. These attacks can offer up to super-polynomial speedup, although they currently require excessive quantum resources [15].

### 4.3 Quantum Searching and Quantum Walks

*Status:* Algorithms are under development
*Timeline Expectation:* 0-10 years
*Qubits Requirement:* Approximately 100 qubits, depending on the size of the searched system
*Main Challenges:* Increasing the number of logical qubits

**Current State and Significance**:

One of the most famous quantum searching algorithms is Grover's algorithm [13], which offers a quadratic speedup in database searching or inverting a function. For an unsorted list or database, classical searching algorithms have a complexity of O(N) meaning the search time is proportional to the number of N entities. In contrast, Grover's algorithm has a complexity of O(√N) offering a significant speedup for large datasets.

Quantum searching algorithms are particularly important for analyzing large volumes of unstructured data, often referred to as Big Data. However, practical implementation faces several challenges, such as the need for a large quantum memory to store vast amounts of data. Currently, there is no reliable quantum memory that can preserve quantum information for long periods and in large quantities. Additionally, transforming classical data into a quantum format is time-consuming and inefficient. Thus, the most practical applications of quantum searching algorithms involve data that is generated algorithmically.
Another approach to quantum searching is based on the quantum random walk mechanism [16], which offers similar speedup advantages as Grover's algorithm. Quantum random walks can enhance search efficiency and are an area of active research.

### 4.4 Quantum Optimizations

*Status:* Algorithms are in development
*Timeline Expectation:* 0-10 Years
*Qubits Requirement:* Approximately 100 qubits, depending on the problem's complexity
*Main Challenges:* Increasing the number of logical qubits

**Current State and Significance**:

Quantum optimization is a highly active area of research due to its potential to solve NP-hard problems, which are known for their computational complexity. An example of such a problem is the traveling salesman problem, where the objective is to find the shortest possible route that visits a set of locations and returns to the origin. Classical approaches to solving NP-hard problems, like brute force, become impractical as the problem size increases, often requiring heuristic algorithms that provide approximate solutions.
Quantum computing introduces new methods for optimization, leveraging quantum principles to explore vast solution spaces more efficiently than classical algorithms. The most prominent method currently being explored is the Quantum Approximate Optimization Algorithm (QAOA), which includes techniques like Quadratic Unconstrained Binary Optimization (QUBO). These methods are suitable for both digital and analog quantum computers.

**Dominant Methods**:

1. ***Quantum Approximate Optimization Algorithm (QAOA)****:* QAOA is a variational algorithm that optimizes a problem by iteratively adjusting parameters to minimize or maximize a given objective function. It is particularly effective for discrete optimization problems [17].
2. ***Quadratic Unconstrained Binary Optimization (QUBO)****:* This technique is used to solve optimization problems by representing them as binary variables and optimizing a quadratic objective function. QUBO is well-suited for analog quantum computers like quantum annealers [18].
3. ***Least-Squares Fit and Semidefinite Programming****:* These are other quantum-inspired methods that offer potential advantages for specific optimization problems [19].

**Current Demonstrations and Use Cases**:

There have been numerous demonstrations and proof-of-concept applications of quantum optimization, particularly with analog quantum computers like those from D-Wave [20]. Examples include:

- ***Traffic Optimization****:* Quantum optimization algorithms have been used to optimize traffic flow in urban areas, reducing congestion and improving mobility.
- ***Logistics Planning****:* Quantum algorithms have been employed to optimize supply chain logistics, ensuring efficient distribution of goods and resources.
- ***Financial Sector****:* Quantum optimization has shown potential in portfolio optimization and risk management, which can be adapted for defense-related financial planning and resource allocation.

### 4.5 Quantum Linear Algebra

*Status:* Algorithms are in development
*Timeline Expectation:* 6-20 Years
*Qubits Requirement:* Depends on the size of the system being solved
*Main Challenges:* Increasing the number of logical qubits

**Current State and Significance**:

Quantum computers have demonstrated the potential for super-polynomial speedup in solving linear equations, particularly through the Harrow-Hassidim-Lloyd (HHL) algorithm [21] for sparse matrices. The estimated speedup varies depending on the problem size (matrix), but the resource requirements for some problems may be considered impractical. For example, solving a system of linear equations with 10,000 parameters would typically require 10,000 steps on a classical computer, whereas the HHL algorithm can provide an approximate solution in just 13 steps.

Many numerical simulations in planning, engineering, construction, and weather forecasting simplify complex problems into large sets of linear equations. In many cases, these problems are statistical in nature, and an approximate solution provided by quantum algorithms can be sufficient. The HHL algorithm has shown its versatility in various applications, such as k-mean clustering, support vector machines, and data fitting.

**Challenges and Considerations**:

One of the significant challenges with quantum algorithms that work with large amounts of input data is the data loading process. Classical data, especially binary data or bits must be transferred into quantum states for processing by efficient quantum algorithms. This data loading process is slow, and it can take longer than the coherence time of the quantum system. Quantum memory or quantum RAM is being explored as a solution to this problem, enabling faster data loading and processing [22].

**Current Demonstrations and Use Cases**:

Several demonstrations and proof-of-concept applications of quantum linear algebra have been conducted, particularly with the HHL algorithm [23]. Examples include:

- ***K-Mean Clustering****:* Using quantum algorithms to perform k-mean clustering for data analysis and pattern recognition, applicable in intelligence gathering and threat assessment.
- ***Support Vector Machines (SVM)****:* Enhancing machine learning techniques like SVM for classifying and analyzing large datasets, which can be used in cybersecurity and signal processing.
- ***Data Fitting****:* Applying quantum algorithms for data fitting in engineering and scientific research, improving the accuracy and efficiency of simulations.

### 4.6 Quantum Machine Learning and AI

*Status:* Algorithms are in development
*Timeline Expectation:* 0-10 Years
*Qubits Requirement:* Approximately 100 qubits, depending on the problem's complexity
*Main Challenges:* Increasing the number of logical qubits

**Current State and Significance**:

Quantum machine learning and AI are emerging fields expected to build upon the advancements of classical ML/AI. While full quantum ML/AI systems may not be practical due to the challenges associated with working with classical data—such as slow data loading and encoding into quantum formats—the application of ML/AI to quantum data (e.g., data from quantum sensors or imaging) presents a viable alternative. Quantum-enhanced ML/AI can leverage quantum computing to improve specific machine learning tasks, such as quantum sampling, linear algebra, and quantum neural networks.

**Challenges and Considerations**:

One of the main challenges with quantum ML/AI is the inefficiency of processing classical data using quantum computers. Without quantum memory and with the slow process of loading classical data into quantum states, practical applications remain limited. However, quantum-enhanced ML/AI, which uses quantum computing to augment classical ML techniques, offers significant potential. Examples include the quantum support vector machine and quantum neural networks.

**Current Demonstrations and Use Cases**:

Several demonstrations and proof-of-concept applications of quantum ML/AI have been conducted [24, 25]. Examples include:

- ***Quantum Support Vector Machines (SVM)****:* Enhancing machine learning techniques like SVM for classifying and analyzing large datasets, which can be used in cybersecurity and signal processing.
- ***Quantum Neural Networks****:* Developing quantum versions of neural networks to improve data processing capabilities and optimize complex decision-making processes.
- ***Quantum Sampling****:* Using quantum algorithms to perform sampling tasks more efficiently, which is critical for various ML applications, including data analysis and pattern recognition.

### 4.7 Quantum Communication and Cryptography

Quantum communication and cryptography leverage the principles of quantum mechanics to provide enhanced security and efficiency in information exchange. These technologies use quantum entanglement, quantum uncertainty, and the no-cloning theorem to ensure secure communication and cryptographic operations.

#### 4.7.1 Quantum Network

*Status:* In research (commercially available for QKD with trusted nodes only)
*Timeline Expectation:* 6-10 Years
*Main Challenges:* Developing reliable quantum repeaters and switches (quantum memory)

**Current State and Significance**:

A quantum network, also known as the quantum internet [26] or quantum information network (QIN), aims to transmit quantum information through various technologies across different channels. Quantum information, typically carried by photons, is extremely fragile and susceptible to loss and decoherence. Quantum networks require components like quantum repeaters and switches to maintain the integrity of the transmitted information over long distances.

Quantum networks use low-loss optical fibers or existing telecommunication infrastructures for ground-based communication. For longer distances, free-space quantum channels, such as satellite-based quantum communication, are being developed. These satellites can utilize optical-photon communication to reduce losses compared to ground-based nodes [27, 28].

**Challenges and Considerations**:

Quantum repeaters, essential for long-distance quantum communication, face significant challenges due to the no-cloning theorem, which prohibits copying quantum information. Quantum repeaters must entangle qubits at the end nodes, enabling quantum teleportation and ensuring secure transmission without physically sending photons. Reliable and practical quantum memory is still under development, posing a challenge to building fully functional quantum networks.

**Current Demonstrations and Use Cases**:

Several demonstrations and proof-of-concept applications of quantum networks have been conducted. For example, China has demonstrated satellite-based QKD using trusted repeaters, showcasing the potential for secure long-distance quantum communication.

Quantum networks can be used for the following applications:

- Quantum key distribution (QKD), a secure transmission of cryptographic keys.
- Quantum information transmission between quantum computers or computing clusters at large distances or for sharing remote quantum capabilities.
- Blind quantum computing allows the transmission of a quantum algorithm to a quantum computer, performing computations, and retrieving results without the owner or eavesdropper knowing what the algorithm or result was.
- Network clock synchronization, improving the synchronization of clocks in communication and sensor networks.
- Secure identification, providing secure methods for identification and verification without revealing sensitive authentication credentials.
- Quantum position verification, allowing the verification of the position of the other party.
- Distributed quantum computing, connecting multiple quantum computers to work on a single computational task.
- Consensus and agreement tasks using quantum versions of consensus algorithms, offering faster and more secure agreement protocols.
- Entangled sensor networks, enhancing the sensitivity and accuracy of sensor networks by leveraging quantum entanglement.

### 4.7.2 Quantum Key Distribution (QKD)

*Status:* Commercially available (with trusted repeaters)
*Timeline Expectation:* 0-5 Years
*Main Challenges:* Developing secure quantum repeaters (quantum memory) and achieving security certification for physical hardware

**Current State and Significance**:

Quantum Key Distribution (QKD) is the most mature application of quantum communication. QKD enables the secure distribution of cryptographic keys between parties, ensuring that any eavesdropping attempts are detectable due to the no-cloning theorem. The two dominant classes of protocols for QKD are the BB84 (Bennett-Brassard 1984) protocol and the E91 (Ekert 1991) protocol [29, 33].

**Challenges and Considerations**:

While QKD theoretically offers impenetrable security during transmission, practical implementation faces challenges such as vulnerabilities in hardware and software, including imperfect single-photon sources and control software bugs. Security certification of hardware and software is necessary to address these issues. Additionally, the qubit transfer rate needs improvement to distribute long keys efficiently.

**Current Demonstrations and Use Cases**:

Currently, QKD technology is commercially available as a point-to-point connection for short distances or using trusted repeaters for long distances. For example, China has demonstrated satellite-based QKD using trusted repeaters, showcasing the potential for secure long-distance quantum communication [27, 28].

### 4.7.3 Post-Quantum Cryptography

*Status:* Algorithms ready
*Timeline Expectation:* 0-5 Years
*Main Challenges:* Standardization and implementation

**Current State and Significance**:

Post-quantum cryptography refers to encryption techniques designed to resist future quantum computer attacks. While many current asymmetric encryption schemes are vulnerable to quantum attacks, most symmetric cryptographic algorithms and hash functions are considered relatively secure. Nevertheless, doubling the symmetric key length is recommended for enhanced security.

Several approaches to post-quantum cryptography are being developed, including lattice-based, hash-based, multivariate-based, and code-based cryptographic algorithms. These algorithms are undergoing rigorous testing and standardization processes to ensure their security and effectiveness.

**Challenges and Considerations**:

The main challenges in post-quantum cryptography involve the standardization and implementation of new algorithms. These algorithms must be thoroughly tested and analyzed to ensure they are secure against both quantum and classical attacks. The U.S. National Institute of Standards and Technology (NIST) is leading the standardization process [30], with several finalist algorithms expected to be standardized by 2023-24.

**Current Demonstrations and Use Cases**:

Many commercial vendors are already offering quantum-resistant encryption solutions. As quantum computing technology advances, the adoption of post-quantum cryptographic algorithms will become essential to ensure the security of sensitive information.

### 4.7.4 Quantum Random Number Generator (QRNG)

*Status:* Commercially available
*Timeline Expectation:* 0-5 Years
*Main Challenges:* Increasing the bit rate

**Current State and Significance**:

Random number generators (RNG) are crucial for various applications, including Monte Carlo simulations, cryptographic operations, statistics, and computer games. Classical RNGs are deterministic and known as pseudo-random number generators. However, truly random number generation is essential for generating strong cryptographic keys.

Quantum random number generators (QRNG) utilize quantum phenomena to produce truly random numbers, providing superior randomness compared to classical RNGs. QRNGs are a crucial component of BB84-based QKD protocols, ensuring provable security [33].

**Challenges and Considerations**:

The main challenge for QRNGs is increasing the bit rate to generate random numbers more efficiently. Security certification of QRNG hardware is also necessary to ensure their reliability and effectiveness in cryptographic applications.

**Current Demonstrations and Use Cases**:

QRNGs are commercially available and can be used for any cryptographic application, enhancing the security of cryptographic operations by providing truly random numbers. They are essential for implementing secure QKD protocols and improving overall cryptographic security. The advantage of QRNG is that it can be verified and certificated [31], unlike any other RNG.

## 5 Technology Readiness Level (TRL) and Time Horizon for Quantum Computing

Various quantum technologies are at different Technology Readiness Levels (TRLs), ranging from 1 to 8. The TRL variation and time horizon expectations are complex, especially for military purposes. Here, we summarize TRL and expected time horizons for key quantum computing technologies based on reports and findings [32, 33]:

| Technology | TRL | Horizon |
|---|---|---|
| Quantum Computer (Annealer) | 4-5 | 2030 |
| Post-Quantum Cryptography | 7-8 | 2025 |
| Quantum Communication Network | 1-3 | 2030-2035 |

The actual military deployment can take time to overcome all technological obstacles and meet military requirements. For example, quantum simulations may first be applied to specific defense-related problems, such as chemical simulations for warfare agents, before being adapted for broader use.

## 6 Quantum Computing in Defense

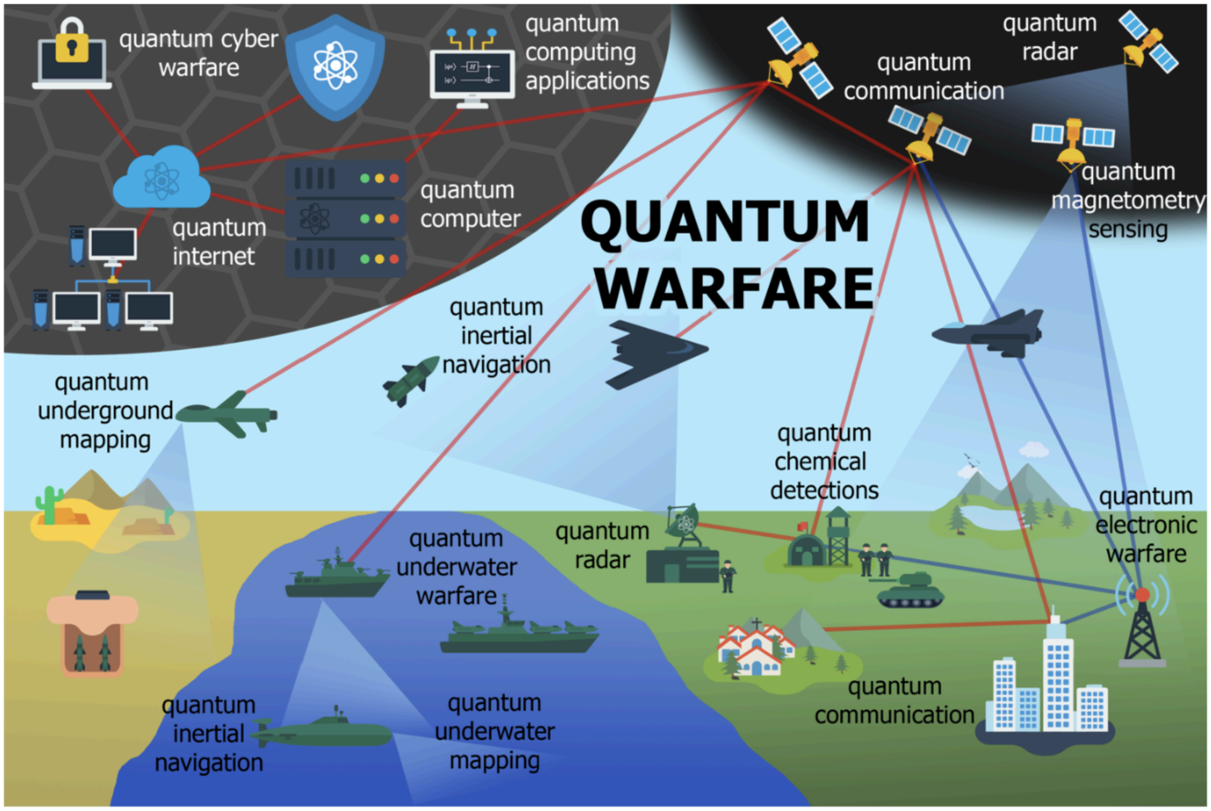
quantum cyber warfare
quantum computing applications
quantum radar
quantum communication
quantum computer
quantum internet
quantum magnetometry sensing
QUANTUM WARFARE
quantum inertial navigation
quantum underground mapping
quantum chemical detections
quantum electronic warfare
quantum underwater warfare
quantum radar
quantum communication
quantum inertial navigation
quantum underwater mapping

**Figure 1** Sketch of quantum warfare utilising various quantum technology systems

Quantum technologies have the potential to significantly impact many areas of human activity, especially in the defense sector. These technologies can enhance all domains of modern warfare, improving sensitivity, efficiency, and introducing new capabilities that sharpen existing techniques rather than leading to entirely new types of weapons. The second quantum revolution is set to bring transformative changes in military, security, space, and intelligence applications.

This section explores the potential applications of quantum computing in defense, mapping out how these advanced technologies could be integrated into various military operations and strategies. It is important to note that while significant advancements have been made in laboratory settings, the transition to practical deployment involves additional challenges such as portability, sensitivity, resolution, speed, robustness, low SWaP (size, weight, and power), and cost. The effectiveness and cost-efficiency of quantum technologies will determine their feasibility for manufacturing and deployment in military contexts.

Integrating quantum computing into military platforms presents particular challenges. While quantum computers are likely to be housed in data centers similar to those used for civilian purposes, their application in military operations requires overcoming increased demands for precision, speed, and robustness. Despite these challenges, the potential benefits of quantum computing in defense make it a critical area of research and development.

## 6.1 Quantum Cybersecurity

Quantum advancements in cyber warfare can provide highly effective ways to attack current encryption methods and introduce new, resilient encryption algorithms and approaches, such as quantum key distribution (QKD) [33].

### 6.1.1 Quantum Defense Capabilities

Implementing post-quantum cryptography is crucial. The risk of hostile intelligence gathering encrypted data to decrypt later with quantum computers is real and pressing. This applies to military, intelligence, government, industry, and academia. The current trend is to prepare the infrastructure for quantum crypto-agility to deploy standardized post-quantum cryptography.

New quantum-resilient algorithms can offer a new mathematical approach difficult for quantum computers to break and a new way of working with encrypted data, such as fully homomorphic encryption (FHE). FHE allows data to remain encrypted even while being processed, making it suitable for cloud-based quantum computing.

Post-quantum cryptography should also be implemented in the Internet of Things (IoT) and the Internet of Military Things (IoMT), which have many potential security breaches.

Quantum key distribution (QKD) allows safe encryption key exchange with proven security. However, weaknesses can be found at end nodes and trusted repeaters due to imperfect hardware or software. The cost and effectiveness of QKD, whether optical fibre-based or using quantum satellites, is a consideration. The EU prefers QKD, while the US favors post-quantum encryption solutions.

Quantum random number generators (QRNG) increase security by preventing attacks on pseudorandom number generators.

### 6.1.2 Quantum Attack Capabilities

Shor’s algorithm allows quantum computers to break current public key encryption methods, like RSA, DH, and ECC. The timeline for when this will be possible is uncertain, but it is estimated to be around 10–15 years. This threat also applies to most message authentication codes (MAC) and authenticated encryption with associated data (AEAD).

Offensive operations using these capabilities likely already exist or are in development. In the next decade, sensitive communications will need to use post-quantum cryptography or QKD to be secure against quantum attacks.

Grover’s algorithm can weaken symmetric key encryption algorithms like DES and AES, but the resource requirements for this are currently unfeasible.

Classical hacking methods will continue to target vulnerabilities in quantum systems, which are still developing and likely to have many bugs and security breaches. Current QKD quantum satellites, controlled by classical computers, are potential targets for cyberattacks. Research is ongoing into specific physical-based attacks on quantum networks, like photon-number-splitting and Trojan-horse attacks.

### 6.2 Quantum Computing

Quantum computing will introduce new capabilities to classical computing services, aiding in solving highly complex computational problems [33]. Quantum computing covers quantum optimizations, machine learning and artificial intelligence (ML/AI) improvements, quantum data analysis, and faster numerical modeling. Military applications that could benefit from near-term quantum computers include battlefield simulations, radio frequency spectrum analysis, logistics management, supply chain optimization, energy management, and predictive maintenance.

Future quantum computing implementations will likely be in computing farms along with classical computers, creating hybrid systems. These hybrid systems will use ML/AI to analyze tasks and allocate them to the appropriate resources, such as CPUs, GPUs, FPGAs, or quantum processors (QPUs), for the best and fastest results.

While small, embedded quantum computers for direct quantum data processing in autonomous vehicles or mobile command centers are currently challenging due to the need for cryogenic cooling, ongoing research focuses on other qubit designs that can operate at room temperature. Embedded quantum chips could perform simple analytical tasks or straightforward quantum data processes related to quantum network applications. Larger quantum computers will benefit machine learning and model optimization in autonomous systems and robotics.

Quantum computing is expected to be highly efficient in optimization problems. In the military sector, quantum optimizations could include logistics for overseas operations, mission planning, war games, system validation and verification, new vehicle designs, and attributes such as stealth or agility. Enhanced decision-making supported by quantum information science, including predictive analytics and ML/AI, will be critical.

Quantum computers will play a significant role in Command and Control (C2) systems by improving and speeding up scenario simulations and processing and analyzing Big Data from Intelligence, Surveillance, and Reconnaissance (ISR) for enhanced situational awareness. Quantum-enhanced machine learning and quantum sensors and imaging will be integral parts of these systems.

Quantum computing will enhance classical machine learning and artificial intelligence, including defense applications. While not practical for the entire machine learning process, quantum computing can improve ML/AI machinery, such as quantum sampling, linear algebra, and quantum neural networks. Quantum ML provides advantages for specific problems, and hybrid classical-quantum machine learning models can be implemented on small near-term quantum devices.

Quantum computers, through quantum neural networks, can offer superior pattern recognition and higher speeds, essential for biomimetic cyber defense systems that protect networks similarly to biological immune systems. Quantum computing can also improve numerical modeling in the defense sector, such as war games simulations, radar cross-section calculations, and stealth design modeling.

In the long term, quantum systems can enable Network Quantum Enabled Capability (NQEC), a futuristic system allowing secure communication, enhanced situational awareness and understanding, remote quantum sensor output fusion and processing, and improved C2.

**Current Application:**

Recently, D-Wave Quantum Inc., in partnership with Davidson Technologies, announced the placement of the second US-based D-Wave Advantage quantum computer at Davidson's new global headquarters in Huntsville, AL. Davidson Technologies, a technology services company, provides innovative engineering, technical, and management solutions for the U.S. Department of Defense, aerospace, and commercial customers. The quantum computer will be used to run sensitive applications using quantum computing technology. Initially accessible via D-Wave's Leap™ real-time quantum cloud service, the system will eventually be dedicated to developing and operating sensitive national security applications. This placement marks a significant advancement in leveraging quantum computing for national defense and security [34].

### 6.3 Quantum Communication Network

Quantum internet stands for a quantum network with various services, which have significant security implications. Many advanced quantum communication network applications require quantum entanglement, necessitating quantum repeaters and quantum switches. Future combinations of optical fiber and free-space channels will interconnect various end nodes such as drones, planes, ships, vehicles, soldiers, and command centers [33].

#### 6.3.1 Security Applications

Quantum key distribution (QKD) is one of the most mature quantum network applications. This technology will be particularly interesting for the defense sector once long-distance communication using MDI-QKD or quantum repeaters becomes feasible. Currently, basic commercial technology using trusted repeaters is available. QKD companies promote the technology as the most secure, with increasing use cases, especially in the financial and healthcare sectors. However, numerous recommendation reports and authorities, such as the UK National Cyber Security Centre, do not endorse QKD for any government or military applications in its current state.

Apart from QKD, which only distributes keys, the quantum network could be used for quantum-secure direct communication (QSDC) between space, special forces, air, navy, and land assets. Here, direct messages encrypted in quantum data take advantage of security similar to

QKD. However, a low qubit rate might limit the communication to simple messages, not audiovisual or complex telemetry data. In such cases, the network may switch to the QKD protocol for distributing keys, with encrypted data distributed over classical channels. Other protocols such as quantum dialogue and quantum direct secret sharing aim to use the quantum network for provably secure communications.

Another significant contribution to security is the quantum digital signature (QDS), which provides security against tampering with a message after a sender has signed it. Quantum secure identification allows identification without revealing authentication credentials, enhancing security.

Position-based quantum cryptography can offer more secure communication, accessible only from specific geographical positions, such as communication with military satellites only from particular military bases.

### 6.3.2 Technical Applications

Quantum networks will perform network clock synchronization, already a major topic in classical digital networks. Clock synchronization 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 using quantum entanglement will achieve more accurate synchronization, especially when quantum clocks are deployed. Precise clock synchronization is essential for the cooperation of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) systems, ensuring accurate synchronization of various data and actions.

Blind quantum computing allows a quantum program to run on a remote quantum computer or quantum computing cloud and retrieve results without the owner knowing the algorithm or result, valuable for secret computation needs.

Distributed quantum computing via the quantum network will be important for military and governmental actors to build high-performance quantum computing services or quantum clouds.

A quantum network capable of distributing entanglement can integrate and entangle quantum sensors to improve sensor sensitivity, reduce errors, and perform global measurements. This is advantageous when measuring global properties of the entire network.

Quantum protocols for distributed computing agreement can have advantageous military applications for a swarm of drones or a herd of autonomous vehicles (AVs), helping achieve agreement between all AVs at the same time scale, regardless of their quantity.

## 6.4 Quantum ISTAR

Quantum technologies can dramatically improve ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance) capabilities, providing a significant edge in situational awareness on multi-domain battlefields.

Quantum computing will enhance the ability to acquire and process new intelligence data, filter, decode, correlate, and identify features in signals and images captured by ISR (Intelligence, Surveillance, and Reconnaissance) systems. Quantum image processing is expected to offer significant advancements in situational awareness and understanding, benefiting from quantum image analysis and pattern detection utilizing neural networks [33].

### 6.4.1 Quantum Earth's Surface and Underground Surveillance

Quantum sensing based on magnetometry, gravimetry, and gravity gradiometry provides detailed information about the Earth's surface and underground changes, both of natural and human-made origins. These sensors can reach very high precision, especially in laboratory settings, offering detailed mapping of the Earth’s surface and underground structures.

Deploying quantum sensors on low Earth orbit (LEO) satellites could enhance applications such as Earth monitoring, mapping resources, earthquake and tsunami detection, and precise georeferencing and topographical mappings. However, the sensitivity and spatial resolution are crucial factors determining the effectiveness of these applications.

Quantum sensing devices on airborne, sea, or ground vehicle platforms can improve applications like searching for underground tunnels, caves, or bunkers. Low-resolution quantum sensing could assist with precise georeferencing and topographical mappings, aiding in underwater navigation or mission planning in rugged terrain.

### 6.4.2 Quantum Imaging Systems

Quantum imaging systems, including quantum radar and lidar, offer significant advancements in all-weather, day-night tactical sensing for ISTAR. Techniques such as SPAD (Single Photon Avalanche Detectors), quantum ghost imaging, sub-shot-noise imaging, and quantum illumination provide various military applications.

Quantum 3D cameras exploiting quantum entanglement and photon-number correlations will introduce fast 3D imaging with unprecedented depth of focus and low noise, which can be used to inspect and detect deviations or structural cracks in sensitive military technology.

Quantum imaging systems can also detect objects out of the line of sight, like hidden behind the corner of a wall, and provide low-light or low-SNR vision capabilities in environments like cloudy water, fog, dust, smoke, jungle foliage, or nighttime, countering adversaries' camouflage or target-deception techniques.

Quantum rangefinders will offer stealth capabilities, operating invisibly and undetectably, unlike classical rangefinders. Additionally, quantum ghost imaging can function as a quantum lidar for slow-moving or stationary targets, providing 3D imaging with infinite depth of focus.

## 6.5 Chemical and Biological Simulations and Detection

Defense-related chemical and biological simulations are crucial for military and national laboratories, the chemical defense industry, and CBRN (Chemical, Biological, Radiological, and Nuclear) defense forces. Research on new drugs and chemical substances based on quantum simulations requires advanced quantum computers, classical computing facilities, and quantum-chemical experts. Quantum simulations for chemical and biological warfare agents share requirements with civil research, including protein folding, nitrogen fixation, and peptide research [33].

The number of qubits required depends on the spatial basis functions used. For example, using the 6-31G basis, the Benzene and Caffeine molecules require approximately 140 and 340 qubits, respectively. Simulating a Sarin molecule requires about 250 qubits. Based on quantum computer roadmaps and logical qubit requirements, achieving 100 logical qubits within the next decade is feasible, enabling medium-sized molecule simulations.

Potential threats include the design and precise simulation of new small- to medium-sized molecules as chemical warfare agents. However, this knowledge can also be applied to CBRN countermeasures and developing new detection techniques.

Research on protein folding, DNA, and RNA exploration, such as motifs identification, genome-wide association studies, and de novo structure prediction, can impact the research on biological agents. Detailed studies are required to assess the real threat from quantum simulations.

Photoacoustic detection using quantum cascade lasers can effectively detect chemicals. Quantum chemical detectors can identify TNT and triacetone triperoxide elements used in improvised explosive devices (IEDs), common in asymmetric conflicts. These systems can also detect acetone to identify baggage and passengers with explosives. Quantum chemical detection is useful against chemical warfare agents and toxic industrial chemicals.

In the mid- to long-term, these detectors can be placed on autonomous drones or ground vehicles to inspect areas for chemical threats.

### 6.6 New Material Design

Modern science is developing new materials and metamaterials, often called quantum materials, by exploiting quantum mechanical properties (e.g., graphene, topological insulators). These materials can be simulated by quantum computers to understand their electronic structures. Applications include room-temperature superconductors, better batteries, and improved material features.

For instance, room-temperature superconductivity materials exploit superconductivity at high temperatures, enabling the construction of Josephson junctions, which are the building blocks of SQUIDs or superconducting qubits. Currently, these materials require cooling near absolute zero. A quantum computer with approximately 70 logical qubits could suffice for basic research on high-temperature superconductors.

In the defense industry, research opportunities include developing materials for better camouflage, stealth (electromagnetic absorption), ultra-hard armor, or high-temperature tolerance. These advancements can enhance military equipment and operational capabilities, though specific details are often classified [33].

## 7 Countermeasures to Quantum Computing

As quantum Computing becomes more integrated into military operations, it is essential to develop countermeasures to address potential threats. Quantum hacking, for instance, aims to exploit vulnerabilities in quantum communication and computing systems. Ensuring robust security and developing strategies to mitigate quantum-based attacks are crucial for maintaining a strategic advantage.

## 8 Quantum Computing Geopolitical Landscape

The dangers posed by quantum computing to encryption networks have made it a point of increasing geopolitical sensitivity. This has forced major world players like the US, China, and others to develop national quantum strategies. Leading military bodies such as the Pentagon, the Chinese People's Liberation Army (PLA), and NATO are investing heavily in quantum technology [35].

### 8.1 United States

Close ties to tech giants like Microsoft, IBM, and Intel give the US a key advantage in developing quantum technology for military applications. In 2022, President Biden signed the CHIPS and Science Act, which authorizes new investments in core quantum research programs. The US military announced $3 billion in federal quantum projects, with an additional $1.2 billion from the National Quantum Initiative. While the US may struggle to compete with China's centralized, state-led approach in quantum communication research, the diverse range of hardware research increases the likelihood of major breakthroughs happening in Washington first.

### 8.2 China

China is committing more than $15 billion to quantum computing over the next five years and is drawing expertise from across the country through its $10 billion National Quantum Lab at USTC Hefei. Over the long term, China's autocratic economic model will be an advantage due to less bureaucracy and pushback against quantum investments. The PLA leads in quantum communication through the Micius satellite project and the Beijing–Shanghai Quantum Secure Communication Backbone. Quantum supremacy claims from some of the world's fastest photon-based and supercomputing quantum computers show China's potential.

### 8.3 European Union and NATO

The EU's Quantum Technologies Flagship program will provide $1.2 billion of funding over the next ten years. Individual member states like France and Germany are rolling out various R&D initiatives. Germany announced $3 billion to develop quantum technologies in May 2023. NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) has driven quantum investment, conceptualizing quantum underwater warfare, inertial navigation, and chemical detections.

### 8.4 Russia and India

Both countries established a quantum agenda in 2020, each committing $1 billion. Russia’s National Quantum Laboratory, led by state atomic energy company Rosatom, focuses on applying quantum technologies in the nuclear industry. However, smaller talent pools and loosely built ecosystems mean it will be several years before they are competitive with the US, China, and other established quantum players.

## 9 Conclusion

Quantum computing holds significant promise for transforming various aspects of modern warfare and national security. Advancements in quantum computing, communication networks, ISTAR, chemical and biological simulations, and new material design offer substantial improvements in military capabilities, such as enhanced encryption, superior intelligence and surveillance, optimized logistics, and innovative defense materials.

However, the potential of these technologies must be viewed with caution. Many applications are still in the proof-of-concept stage, and overly optimistic expectations often stem from reports that may overstate the readiness of quantum technologies for battlefield deployment. Critical factors such as miniaturization, susceptibility to interference, sensitivity, resolution, functionality, and cost will determine their practical use.

Global interest in quantum technology is intense, with the US, China, and the EU making substantial investments. The US benefits from its tech giants and federal funding, while China's centralized approach drives rapid advancements. The EU and NATO are also heavily investing, partly to counter other global powers.

In conclusion, while optimism about the future of quantum computing in military applications is justified, it must be tempered with realism. The true test will be in the operational deployment of these technologies, ensuring they meet performance and cost-effectiveness criteria. Ongoing research and advancements in supportive systems provide a solid foundation for future developments, but careful and critical assessment is essential to navigate the hype and realize their potential in defense.

## 10 References

1. Williams C. The Second Quantum Revolution. NIST. 2022. https://www.nist.gov/physics/introduction-new-quantum-revolution/second-quantum-revolution

2. Bacon D. The No-Cloning Theorem, Classical Teleportation and Quantum Teleportation, Superdense Coding. Department of Computer Science & Engineering, University of Washington. 2011. https://courses.cs.washington.edu/courses/cse599d/06wi/lecturenotes4.pdf

3.Arute F., Arya K., Babbush R., et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019. https://doi.org/10.1038/s41586-019-1666-5

4. Gambetta J. IBM's Roadmap For Scaling Quantum Technology. IBM. 2020. https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/

5. Finke D. Google Goal: Build an Error Corrected Computer with 1Million Physical Qubits by the End of the Decade. Quantum Computing report by GQI. 2020. https://quantumcomputingreport.com/google-goal-error-corrected-computer-with-1-million-physical-qubits-by-the-end-of-the-decade/

6. Mosca M., Piani M., Quantum threat timeline. Global Risk Institute. 2019. https://globalriskinstitute.org/publication/quantum-threat-timeline/

7. National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

8. Feynman R.P., Simulating physics with computers. Int J Theor Phys. 1982. https://doi.org/10.1007/BF02650179

9. Reiher M et al. Elucidating reaction mechanisms on quantum computers. In: Proceedings of the national academy of sciences. vol. 114. 2017. https://doi.org/10.1073/pnas.1619152114

10. Jarrod R McClean et al. New J. Phys. 2016. https://doi.org/10.1088/1367-2630/18/2/023023

11. Arute Fetal. Hartree - Fock on a superconducting qubit quantum computer. Science. 2020.. https://doi.org/10.1126/science.abb9811

12. Shor, P. W. "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, 1994. https://doi.org/10.1109/sfcs.1994.365700

13. Grover, L. K. "A fast quantum mechanical algorithm for database search." Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing - STOC '96, ACM, 1996. https://doi.org/10.1145/237814.237866

14.Simon, D. R. "On the power of quantum computation." Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, 2002. https://doi.org/10.1109/sfcs.1994.365701

15. Kaplan, M., et al. "Breaking symmetric cryptosystems using quantum period finding." Advances in Cryptology - CRYPTO 2016. Berlin: Springer, 2016, pp. 207–237. https://doi.org/10.1007/978-3-662-53008-5_8

16. Shenvi, N., Kempe, J., Whaley, K. B. "Quantum random-walk search algorithm." Physical Review A, vol. 67, no. 5, 2003. https://doi.org/10.1103/physreva.67.052307

17. Farhi, E., Goldstone, J., Gutmann, S. "A quantum approximate optimization algorithm." 2014. 1411.4028 [quant-ph]

18. Glover, F., Kochenberger, G., Du, Y. "A Tutorial on Formulating and Using QUBO Models." 2019. 1811.11538 [cs.DS]

19. Wiebe, N., Braun, D., Lloyd, S. "Quantum Algorithm for Data Fitting." *Physical Review Letters*, vol. 109, no. 5, 2012. https://doi.org/10.1103/physrevlett.109.050505

20. D-Wave, Hundreds of Quantum Applications https://www.dwavesys.com/applications

21. Harrow, A. W., Hassidim, A., Lloyd, S. "Quantum Algorithm for Linear Systems of Equations." Physical Review Letters, vol. 103, no. 15, 2009. https://doi.org/10.1103/physrevlett.103.150502

22. Blencowe, M. "Quantum RAM." Nature, vol. 468, no. 7320, 2010, pp. 44–45. https://doi.org/10.1038/468044a

23. Aaronson, S. "Read the fine print." Nature Physics, vol. 11, no. 4, 2015, pp. 291–293. https://doi.org/10.1038/nphys3272

24. Biamonte, J., et al. "Quantum machine learning." Nature, vol. 549, no. 7671, 2017, pp. 195–202. https://doi.org/10.1038/nature23474

25. Havlicek, V., et al. "Supervised learning with quantum-enhanced feature spaces." Nature, vol. 567, no. 7747, 2019, pp. 209–212. https://doi.org/10.1038/s41586-019-0980-2

26. Wehner, S., Elkouss, D., Hanson, R. "Quantum Internet: a vision for the road ahead." Science, vol. 362, no. 6412, 2018, eaam9288. https://doi.org/10.1126/science.aam9288

27. Yin, J., et al. "Satellite-based entanglement distribution over 1200 kilometers." Science, vol. 356, no. 6343, 2017, pp. 1140–1144. https://doi.org/10.1126/science.aan3211

28. Yin, J., et al. "Satellite-to-Ground Entanglement-Based Quantum Key Distribution." Physical Review Letters, vol. 119, no. 20, 2017. https://doi.org/10.1103/physrevlett.119.200501

29. Ekert, A. K. "Quantum cryptography based on Bell's theorem." Physical Review Letters, vol. 67, no. 6, 1991, pp. 661–663. https://doi.org/10.1103/physrevlett.67.661

30. Alagic, G., et al. "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process." NISTIR 8309, NIST, 2020. https://doi.org/10.6028/nist.ir.8309

31. Abbott, A. A., Calude, C. S., Svozil, K. "A quantum random number generator certified by value indefiniteness." *Mathematical Structures in Computer Science*, vol. 24, no. 3, 2014. https://doi.org/10.1017/s0960129512000692

32. Reding, D. F., Eaton, J. "Science & technology trends 2020-2040." *NATO Science & Technology Organization*, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

33. Krelina M., Quantum technology for military applications. EPJ Quantum Technology. 2021. https://doi.org/10.1140/epjqt/s40507-021-00113-y

34. Business Wire. D-Wave to Deploy Second US-Based Advantage™ Quantum Computer at New Davidson Technologies Global Headquarters. Morningstar. 2024. https://www.morningstar.com/news/business-wire/20240617689254/d-wave-to-deploy-second-us-based-advantage-quantum-computer-at-new-davidson-technologies-global-headquarters

35. Blair A., How is quantum technology used in the military? Army Technology. 2024. https://www.army-technology.com/news/how-is-quantum-technology-used-in-the-military/?cf-view&cf-closed