Technology Platform

Quantum Computer Applications

Yehoshua Kalisky, Ruth Poplavsky[1] | November 17, 2026

Summary

Quantum computing is regarded as one of the most important technological revolutions of the 21st century, promising a dramatic breakthrough in areas where the digital computing familiar to us has nearly reached its physical limits. While conventional computers operate using "bits" (electrical switches that can only exist in one of two states: 0 or 1), a quantum computer utilizes units of information known as qubits, which can exist in both states simultaneously. This capability, combined with a property termed "quantum entanglement" which allows particles to instantaneously affect one another at any distance in the universe, gives the computer immense computational power, enabling it to execute millions of operations in parallel. For the fields of national security and weapons technologies, this represents a game changer: the ability to decipher encrypted communications, crack today's standard codes, break RSA encryption within seconds, locate numerical codes concealed among millions in a short timeframe, run simulations, and optimize processes. Consequently, the race to achieve quantum supremacy has becomes a leading strategic objective for the major world powers, as well as for the State of Israel.

Defining the Concept

In the classical computing familiar to us, the fundamental unit of information is the bit, which acts as an electrical switch that, at any given moment, can only be in one of two states: 0 or 1 namely, off and on, respectively. In contrast, in a quantum computer, the basic unit of information is the qubit—a unit based on atomic or subatomic components (such as electrons or photons) that harness the principle of superposition. This property allows the qubit to exist in multiple states simultaneously. In a binary system, a quantum particle can exist in both states (0 and 1) at the same time with varying statistical probabilities, much like an electron, which is commonly likened to a spinning top rotating in both directions at once. This capability breaks the linearity of digital computing, enabling the system to perform an immense number of computational operations in parallel, rather than sequentially.

Another property that gives the quantum computer its unique power is quantum entanglement. This refers to a property in which particles become "linked" to each other, such that a change in the state of one particle immediately affects the state of the other, regardless of the distance between them. The combination of superposition and entanglement makes it possible to create "logic quantum gates" and complex computational circuits that efficiently perform operations on many entangled qubits

[1] Specialist in technology and security affairs.

simultaneously. Consequently, computational power grows exponentially with each qubit added to the system. Through the use of unique algorithms, a quantum computer can thus solve intricate mathematical problems within seconds—tasks that would take a conventional computer thousands of years to complete.

The strategic need to transition to quantum computing stems from the fact that classical digital computing has nearly reached its physical and technological limits. The processing power of a digital computer depends on the density of chips per unit area, but efforts to continue miniaturizing them are encountering physical barriers that make performance improvements particularly difficult and costly. At such minuscule scales, the laws of classic physics cease to apply, and systems become governed by the laws of quantum mechanics. This creates a widening gap between complex computing needs and the capabilities of existing computers.

Quantum computing is not a disruptive technology but a technological revolution that changes the rules of the game by making it possible to perform an enormous number of computational operations in parallel. This reduces computing times from thousands of years to a few seconds and creates a paradigm shift in many fields, both civilian and related to national security and military strategy. This capability makes the technology a top strategic priority, since it offers a decisive advantage in cracking encryption, orchestrating complex logistics, and simulating future battlefield scenarios—challenges that current computing can no longer handle efficiently.

The Global Race

The chart below illustrates global investment in quantum technology, in billions of dollars:



Source: *Quantum Initiatives Worldwide, June 2026*

A recent report by QURECA estimates global investment in quantum technologies in 2026 at approximately $65.9 billion. The race to achieve quantum supremacy has become a strategic priority for the major powers, who identify this technology as a key to military and security superiority on the future battlefield.

The global quantum computing market was estimated at approximately $1.3 billion in 2024 and is projected to reach around $5.3 billion by 2029. Another report puts the average compound annual growth rate at 18.3 percent between 2026 and 2032. In 2025, the fastest-growing regional market share was North America's, at 38.5 percent, of which 21.4 percent was in the United States; the leading market segment was hardware development, at 45.7 percent. A more recent projection asserts that the quantum computing market will reach $40.45 billion in 2035, representing a compound annual growth rate of 36 percent over the 2026–2035 period.

A detailed report by Bain & Company states that growth in the quantum computing market will significantly expand other industries that use, among other things, quantum computing methods, including simulations for materials and drug design, process optimization, machine learning, and encryption. As the technology matures in terms of qubit stability and error correction, the quantum computing market, together with industries that use quantum computing, is expected to reach approximately $100–250 billion by 2035.

One of the largest public offerings in 2026, totaling $1.68 billion, was conducted by Quantinuum—a company formed through the merger of Honeywell Quantum Solutions and the British startup Cambridge Quantum. It develops trapped-ion quantum computers.

China is investing enormous sums, estimated at approximately $15 billion, in its national programs. It has gained an advantage in quantum encryption and satellite communications, including the establishment of a 1,250-mile eavesdropping-resistant communications network between Beijing and Shanghai. Chinese scientists have also unveiled a photonic quantum computer that performs calculations billions of times faster than classical computers.

The United States defines its competition with China as a top national priority, channeling billions of dollars into research, development, and the training of a dedicated workforce. Its main advantage lies in close cooperation between the Pentagon and agencies such as DARPA, alongside tech giants like Google and IBM. It was recently reported that IBM intends to invest $10 billion through 2029 in developing an error-resistant quantum computer. In addition, the company and the Department of Commerce will each invest $2 billion to establish an independent quantum facility, Anderon. IBM is strengthening its hardware capabilities with the aim of building hardware, software, and development tools around its quantum operations, much like NVIDIA built an entire ecosystem around its processors. Google recently reported, in October 2026, a significant breakthrough in preparing quantum states and logic gates on its Willow processor, with early detection and a 40-fold error reduction compared to operating without the newly developed method. Ultimately, the U.S. administration is moving vigorously to renew quantum initiatives and ensure its strategic competitiveness with China and Russia.

Russia is also investing substantial resources, estimated at $1.45 billion, aimed at developing independent quantum computing capabilities to serve its military needs. The Russian effort centers on ensuring the resilience of its national encryption systems and preventing its rivals from gaining a decisive technological edge. Moscow views this technology as an integral component of modern warfare and an essential tool for real-time strategic planning and intelligence.

Overall Progress in the Middle East

The Middle East is in the early stages of developing a quantum ecosystem, with key efforts focused on building research infrastructure and training a skilled workforce. Countries such as the United Arab Emirates and Qatar are working to position themselves as key regional players by establishing international partnerships and bridging academia with industry. These initiatives aim to create

technology incubators that encourage the development of innovative solutions while advancing the industrialization of quantum technology across the region.

In the **United Arab Emirates,** a new quantum laboratory at Abu Dhabi University marked a breakthrough. The project was carried out in partnership with the Vernewell Group. The laboratory was designed to serve as a collaboration hub for students, researchers, and experts in the field, as well as a technology incubator to encourage the development of innovative solutions. One of its main objectives is to advance theoretical research while developing industrial processes for applying quantum technologies in the country.

In **Qatar**, strategic efforts focus on building a broad knowledge base and training a "Quantum-ready Workforce." To this end, Hamad Bin Khalifa University (HBKU) signed a partnership agreement with Canadian company Xanadu, which specializes in photonic technology. This is the Qatar Center for Quantum Computing's (QC2) first international collaboration since its establishment in 2022, and it reflects the country's commitment to becoming an indispensable player in the field through investment in education and professional training. Qatar's strategic effort in quantum technologies was further advanced by an agreement signed in May 2025 between Quantinuum and the Qatari investment agency, Invest Qatar. The agreement aims to develop advanced quantum capabilities and technological cooperation between the two parties, and to strengthen Qatar's quantum ecosystem.

Iran has established its standing as a leading player in the Middle East and among Muslim countries in the field of quantum science and technology. It is currently ranked first across all areas of quantum technology in the region. The country operates in accordance with the "National Document on Quantum Science and Technology," enacted in July 2025 by President Masoud Pezeshkian. The document sets strategic goals, evaluation metrics, and a development roadmap for the research and commercialization of quantum computing, communications and sensing technologies. Iran's notable achievements include the establishment in Tehran, in 2025, of the first Quantum Key Distribution (QKD) network, by researchers from Sharif University of Technology. The network facilitates secure communications for the governmental and banking sectors. Moreover, in 2019, the Atomic Energy Organization of Iran (AEOI) launched a dedicated quantum physics research laboratory as part of a broader effort that also includes exploring military applications in quantum radar and quantum warfare.

Iran ranks 16th worldwide in scientific publications in the field and has recorded particularly notable achievements in remote quantum sensing (8th worldwide), quantum clocks (12th), and quantum radar (15th). In June 2023, however, Iran was forced to retract its announcement that it had developed a quantum processor after the product it presented was identified as a standard ARM-based development board available for purchase online.

Israel, alongside the major powers, ranks highly in terms of investment in the field as a share of GDP. It sees quantum technology as an engine of growth and a critical component of its national resilience and the protection of its vital infrastructure. As discussed below, Israel ranks second in the world, after China, in quantum investment as a share of GDP, at approximately 0.082 percent. The race as a whole is driving a paradigm shift that will give rise to quantum warfare, in which technological superiority will determine the outcome of a campaign.

Current Uses of Quantum Technology

Applications in Security and Technology

- **General**: As discussed below, quantum computing is revolutionizing intelligence in the areas of sensing and detection, as well as the development of advanced weapons systems. A quantum computer will be able to crack RSA encryptions (the most widely used encryption method today) within seconds, rendering the current digital warfare domain breached and vulnerable. Its immense computing power also enables complex simulations of chemical and biological processes for the development of new materials or defense measures against biological warfare, as well as real-time optimization of multidimensional battlefield scenarios, such as the efficient operation of drone swarms via eavesdropping-resistant communication channels.
- **Sensing and Detection (Quantum Sensing):** One of the central and most dramatic uses of quantum technology today is in atomic clocks for highly precise time measurement or detection and sensing technologies, which provide a strategic advantage against stealth weapons systems. Quantum sensing relies on the ability of quantum systems to detect various objects by measuring minute changes in different physical parameters, as detailed below. Quantum radar can expose stealth aircraft and missiles designed to absorb or deflect the radio waves used by conventional radar. It does so by using pairs of entangled photons that make it possible to distinguish between the object and background noise or electronic interference. In addition, exceptionally sensitive quantum sensors are used to detect submarines and underwater mines by measuring minute changes in magnetic and electric fields. This capability is changing the face of naval warfare and making the underwater environment much more transparent for the defender.
- **Quantum radar:** As noted above, quantum radar is designed to detect stealth aircraft and missiles by using entangled photons. The system works by sending one photon toward the target while keeping the second photon at the transmission station. When the signal returns, the system checks its quantum entanglement "signature," allowing it to distinguish the object from heavy background noise or electronic interference designed to deceive conventional radar. This capability enables the radar to detect objects designed to absorb or deflect radio waves without their operators knowing they have been detected. The technology is still in the development stages. Researchers at the University of Waterloo (Canada) are working to develop the system to overcome background noise and severe weather conditions, but sources have not yet described it as an operational system deployed in the field.
- **Underwater detection**: Quantum sensors use the principles of quantum mechanics to detect minute changes in physical parameters, such as magnetic fields and electric fields. This makes them ideal for locating enemy submarines and detecting underwater mines, as they are capable of picking up the unique magnetic signature of these vessels even in a noisy marine environment. The use of these sensors is changing the face of underwater warfare and making the environment “transparent” to the defending force. This technology exists and is already in use. Such sensors are increasingly being used to calculate military data and detect enemy submarines. This is one of the areas in which quantum technology is already having a significant impact on military operations.

Information Warfare and Encryption

- **Breaking Encryption**: A quantum computer can factor large numbers hundreds of digits long at tremendous speed using Shor's algorithm. A conventional computer would need thousands of years to crack the widely used RSA encryption method, which is based on mathematical operations involving the product of two large prime numbers. A quantum computer, by contrast, could do so in just seconds. This capability would leave current communications, command and control systems entirely vulnerable and change the nature of warfare in the digital domain. The technology is under development and has significant future potential. Although the algorithm exists, current quantum computers are still experimental and have a limited number of qubits; at this stage, they cannot crack complex RSA encryption. (Note: Post-Quantum Cryptography (PQC) Computing is a new generation of cryptographic algorithms designed to protect information against cracking it by both conventional computers and powerful quantum computers).

- **Eavesdropping-Resistant Communication (QKD)** based on the Bennett-Brassard protocol (BB84): This method is based on Quantum Key Distribution and utilizes the principles of quantum mechanics to securely exchange encryption keys between two parties. This can be done over fiber-optic cables or through open-air channels, known professionally as free-space communication. Because measuring a quantum particle causes its state to collapse, any attempt by an outside listener to intercept or copy the information immediately causes disturbances, exposing the eavesdropping attempt. This technology makes it possible to establish communications channels that are entirely resistant to eavesdropping or decryption by a third party. It exists and is commercially available. QKD is considered the most mature application of quantum communications, and China has already completed an underground quantum network spanning approximately 1,250 miles between Beijing and Shanghai.

Simulations and the Development of Materials and Weapons

Quantum simulation is regarded as the most promising practical application in the near term, particularly for multi-particle physical processes—an inherent advantage when simulating complex molecular structures and chemical processes. As is well known, Nobel laureate Richard Feynman stated that "nature isn't classical"; only a quantum system can simulate quantum processes that occur in nature, such as chemical synthesis. By contrast, processes occurring at the quantum scale demand immense memory resources from classical computers to successfully emulate the quantum process. A quantum computer's processing capabilities make it possible to develop new chemical materials efficiently and rapidly, including new explosives, corrosion-resistant materials, and advanced defenses against chemical and biological warfare, by simulating molecular biological mechanisms. These simulations save an enormous amount of laboratory time, particularly because the synthesis of chemical materials often involves trial and error, and make it possible to develop weapons covertly and efficiently. This application exists and is being used in advanced research. Companies such as Rolls-Royce are already partnering with quantum centers to develop computational tools for simulating complex materials comprising large numbers of molecules, or simulations of complex biological structures. For instance, it was recently reported that an IBM quantum computer simulated the structure of a protein containing 12,000 atoms. In addition, quantum sensors could help identify the locations of missile launches or detect the signature of weapons of mass destruction.

Battlefield Optimization

- **Drone Swarms:** Quantum computing offers unprecedented capabilities for solving multivariable optimization problems, which pose a major challenge for classical computers given the dynamics of the modern battlefield. The technology can calculate an enormous number of routes and coupled system states simultaneously, identifying the optimal solution in which the system is at its lowest energy level. This capability is essential for controlling drone swarms, as it enables the precise synchronization of numerous autonomous vehicles operating as a single unit in complex and extreme scenarios.

  In addition to route calculation, combining quantum computing with artificial intelligence (quantum machine learning) can create systems that respond to changes in real time and provide multidimensional responses to drone swarm attacks. Using eavesdropping-resistant quantum communication channels makes it possible to operate these attack swarms without fear that the enemy will disrupt control or intercept operational commands. These capabilities are expected to give the side that possesses the technology a decisive tactical advantage in executing operations based on speed and precision.

- **Logistics and Strategic Planning:** Logistics and supply are considered among the most promising near-term applications for quantum optimization, particularly for solving complex problems involving the routing and transportation of resources. Quantum computers can analyze geopolitical, economic, and social variables simultaneously to predict areas of conflict and plan force deployments accordingly. This capability can dramatically improve the planning of supply routes, helping ensure that equipment and resources are positioned in the most suitable locations at critical times, even amid shifting threats.

  Beyond routine planning, the technology makes it possible to simulate numerous wartime scenarios simultaneously, helping assess new strategies and predict enemy movements. Its rapid processing capabilities make strategic planning dynamic, enabling commanders to make data-driven decisions in real time based on analysis of operational patterns. This optimization of supply chains and strategic planning not only conserves resources but also strengthens national resilience and helps ensure military superiority in prolonged campaigns.

National Investments: The Israeli Effort

Israel views quantum technology as a critical component of its national resilience and security. It therefore launched the National Quantum Science and Technology Program in 2020. The program has a budget of NIS 1.5 billion and is led through cooperation among the Israel Innovation Authority, the Directorate of Defense Research and Development (DDR&D, known by its Hebrew acronym MAFAT) at the Ministry of Defense, the Planning and Budgeting Committee (PBC), and other government ministries. This effort aims to ensure that Israel remains at the technological forefront and can develop independent capabilities in quantum hardware and software.

Israeli investments focus on building a broad infrastructure, including the development of an Israeli-made quantum computer. In 2022, the Innovation Authority and DDR&D allocated NIS 200 million to build a quantum computer, with the participation of Israeli and international companies and academia. A budget of NIS 115 million was also approved for a consortium working to develop quantum computing technologies. In total, between 2018 and 2023, Israel invested approximately $480 million in the field, in addition to venture capital investments totaling $650 million, as of June 2025. Total investment in Israeli

quantum companies as of mid-2026 are estimated at approximately $800 million, with the potential for a further $200–$300 million in investment by the end of 2026.

The importance of the field to Israel is reflected in its global ranking: approximately 20 out of the world's 270 quantum-related companies operate in Israel; Israel currently ranks fifth worldwide in financial investment in quantum companies, and seventh on the innovation and ecosystem index. In addition, Israel ranks second globally, after China, in quantum investment as a share of GDP, standing at approximately 0.082 percent. This substantial investment, together with a highly skilled workforce and a well-developed academic infrastructure, is intended to ensure Israel's "quantum supremacy" over major powers and regional actors. The following table briefly outlines a number of Israeli companies active in quantum computing software, control systems, and hardware:

Company	Technology	Notes
Quantum Art	Develops ion-based qubits (electrically charged atoms)	Longer information retention and accuracy in computational operations
Quantum Source	Photon-based qubits	Operates at room temperature using individual photons
Quantum Transistors	Uses a defect in a diamond's structure to trap an electron that serves as a qubit	Operates at room temperature; long coherence time
Q-Factor	Develops qubits based on neutral atoms trapped in laser beams	Operates at room temperature, but is relatively slow compared with other systems when performing operations between qubit logic gates
Quantum Machines	Develops control systems for operating qubits	Supplies hardware and software
Israel Quantum Computing Center (IQCC)	National development center for quantum computers using various types of qubits	Currently operates a quantum computer with superconducting qubits and control systems made by Quantum Machines
QuamCore	Develops a unique architecture for connecting superconducting qubits to a single cryostat (refrigerator)	Optimal wiring reduces background noise and errors
QTREX Quantum	Develops sophisticated interconnect infrastructure for data communications in quantum computers	The interconnect infrastructure operates in a cryogenic environment
Quedma	Reduces and corrects errors in quantum computers	Enables the quantum computer to obtain accurate results for complex computations
Classiq[2]	Develops specialized software for quantum computers	Develops purpose-built algorithms and automatically translates code into machine language

Risks and Opportunities: The Qualitative Edge and the Threat

As we have written previously, the transition to the quantum era poses a real threat to the erosion of Israel's qualitative edge. While supercomputers today are the exclusive domain of major powers, quantum technology is expected to be more accessible and easier to operate. Easier access to enormous computing capabilities could allow small countries and, in the longer term, even paramilitary organizations (terrorist groups), to acquire capabilities once reserved for major powers, thereby threatening Israel's technological superiority over its adversaries.

The central risk in the military dimension is the collapse of current encryption systems. The quantum computer's ability to crack RSA encryption within seconds could render the digital dimension of the battlefield entirely breached. This means that all of Israel's communication systems, command and

control, and vital infrastructure could become vulnerable and penetrable, necessitating a major shift in its approach to cyber defense and its doctrine for digital warfare.

Alongside these risks, the technology offers unprecedented strategic opportunities. Achieving quantum supremacy will enable Israel to develop eavesdropping-resistant communication, significantly enhance artificial intelligence capabilities, and run complex simulations to develop new explosives and defenses against chemical and biological warfare. For Israel, leadership in the quantum field is not only a technological goal, but also an engine of growth and an essential component of national deterrence and the ability to respond optimally to extreme scenarios on the battlefield of the future.

Despite its promising potential, the quantum computing technology market faces several challenges. Technical limitations such as instability, error rates, and the loss of information stored in qubits when they cease to be coherent (Qubit Decoherence) remain significant obstacles to developing reliable, scalable quantum computers. The complexity and cost associated with building and maintaining quantum hardware are substantial, limiting access primarily to large corporations and government-funded projects. There is a shortage of professionals skilled in quantum programming and algorithms, hindering the rapid development and commercialization of applications.

Moreover, the lack of universally accepted standards and protocols creates interoperability issues among different quantum platforms and technologies. Market uncertainty, resulting from the evolving nature of the technology, leads to cautious investment and distant return-on-investment horizons. Cybersecurity concerns surrounding the potential of quantum computing to break existing encryption methods necessitate preemptive solutions and add regulatory and compliance challenges. Furthermore, the quantum ecosystem requires stronger development tools, software, and applications to achieve broad-scale deployment. Integration with existing IT infrastructures is also complex, requiring extensive transformation and new approaches. Enterprise quantum computing has the potential to address organizational needs in finance, healthcare, logistics, and process optimization, as well as leveraging quantum computing capabilities to accelerate business development. The market volume in 2033 is projected to reach a value of $3.25 billion, with an average compound annual growth rate of 32.5 percent between 2026 and 2033.

Summary, Conclusions, and Recommendations Ahead of the "Quantum Revolution"

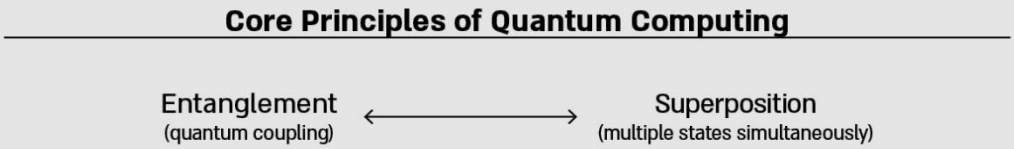
Quantum computing represents a gradual improvement in processing power while also bringing about a profound paradigm shift in science and technology, breaking through the physical limits of classical digital computing. As conventional computing approaches the limits of chip miniaturization, quantum computers offer a revolutionary alternative that can perform millions of operations in parallel, providing an unprecedented strategic advantage in the field of national security.

This revolution will fundamentally change the digital domain on the battlefield: the ability to crack RSA encryption in seconds will make current command and control systems and the internet vulnerable. In effect, this will bring the era of digital warfare as we have known it to an end, or significantly curtail it, and usher in the era of quantum warfare. The following table briefly summarizes the advantages offered by the quantum revolution:

Topic	Advantage	Notes
Quantum Computing (Quantum Supremacy)	Performs complex operations very quickly and solves problems that cannot be solved by a classical digital computer	In this context, this refers to Quantum Supremacy
Quantum Simulation	Simulates quantum processes and systems (atomic or molecular)	Simulates chemical or physical processes that classical computers cannot perform or that require enormous memory resources
Quantum Communication	Transfers sensitive information securely against eavesdropping over all types of communication channels, using photons and their physical properties	An eavesdropping attempt is effectively a measurement that causes the photon's quantum state to collapse, disrupting the communication and exposing the interception attempt
Code Breaking	Quantum computers can crack codes based on operations involving prime numbers	Shor's algorithm is designed for this purpose. It relies on complex mathematical operations performed simultaneously by a quantum computer
Quantum Networks	Connects networks of quantum computers and sensors to transmit information using technology based on quantum principles	This method is used to transmit quantum information across various channels, including satellites, and is also known as the "quantum internet"
Quantum Imaging	Detects and maps objects at high resolution, with a significant improvement over existing sensors	Detects objects or creates three-dimensional maps by measuring minute physical changes by applying the quantum properties of photons or electrons
Quantum Optimization	Finds optimal ways to carry out diverse operations	Analyzes situations, scenarios, and options in different fields quickly and efficiently

The emergence of quantum warfare as part of the quantum revolution necessitates the development of new military strategies, doctrines, and ethics suited to these capabilities, with an emphasis on applying quantum technologies to satellite communications, remote sensing, atomic clocks, and imaging. Quantum technology not only enhances the precision of existing weapons systems but also transforms how battles are conducted — ranging from more accurate prediction of enemy movements to the real-time optimization of responses against attack swarms. This shift requires world powers and states aspiring to technological superiority to rethink fundamental concepts of national security, as future accessibility to this technology could erode the qualitative edge of states vis-à-vis paramilitary organizations.

The following illustrates the core principles of quantum computing as well as a future battlefield managed by quantum systems:





Source: Based on data from Quantum computing in the military.

The key recommendation for decision-makers is to strive for comprehensive quantum readiness, including the acquisition of hardware and software, as well as the development of new encryption protocols for secure communications that prevent eavesdropping. A critical component of this readiness is training a dedicated workforce of quantum technology engineers capable of analyzing and assessing data generated by quantum sensors and computers.

Since recruiting these specialists into the military presents a challenge, it is recommended that the principles of quantum science and technology be incorporated into the curricula of universities and military colleges. This will help ensure that command and technology personnel are prepared to deploy and operate these systems on the battlefield of the future. Finally, military commanders must be aware of emerging and disruptive technologies to keep their forces relevant. Quantum computing is one such technology.

Although quantum computing is still in its early stages and challenges remain in producing reliable qubits, businesses and governments are investing heavily in research and development, and governments around the world are already showing great interest in the subject. This may have tangible ramifications in both civilian and military dimensions.

The authors wish to thank Ms. Hadas Lorber and Dr. Nadav Cohen for their helpful comments.