UNIDIR

# Quantum Technology, Peace and Security

## A Primer

ZHANNA L. MALEKOS SMITH • GIACOMO PERSI PAOLI

## Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This publication was funded by the European Union as part of UNIDIR's Security and Technology Programme, which is also supported by the Governments of Czechia, France, Germany, Italy, the Netherlands, Norway and Switzerland, and by Microsoft.

Special thanks are due to Dr. Irving Lachow and Professor Andrew Reddie of University of California, Berkeley, as well to the diligent team of research assistants at West Point, the United States Military Academy: First Lieutenant Christina Huynh and Cadets Jason Ingersoll, Christopher T. Konin, Conner R. Leggett and Riley Hoyes.

## About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

## Notes

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual author. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, or the European Union, nor their staff members or sponsors.

## Citation

Malekos Smith, Zhanna L., and Persi Paoli, Giacomo. "Quantum technology, peace and security: a primer". Geneva, Switzerland: UNIDIR, 2024.

# About the Authors

## Zhanna L. Malekos Smith

Fellow, Security and Technology

Zhanna L. Malekos Smith JD is a non-resident fellow with UNIDIR and a professor of international law with the United Nations Institute for Training and Research (UNITAR). Additionally, she is a senior associate with the Aerospace Security Project and Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, DC, a visiting fellow with the Carnegie Council for Ethics in International Affairs, and a fellow with the Army Cyber Institute at the US Military Academy at West Point. Previously, Malekos Smith was an assistant professor in the Systems Engineering Department at West Point and a professor of cyberwarfare studies with the US Air War College. A former captain and attorney in the US Air Force's Judge Advocate General's Corps, she received her commission from the Reserve Officers' Training Corps (ROTC) programme at the Massachusetts Institute of Technology. The opinions expressed here are solely those of the author and not those of the United Nations, the US government or the US Department of Defense.

## Dr. Giacomo Persi Paoli

Head of Programme, Security and Technology

Dr. Giacomo Persi Paoli is Head of the UNIDIR Security and Technology Programme. His expertise spans the science and technology domain with emphasis on the implications of emerging technologies for security and defence. Before joining UNIDIR, Giacomo was Associate Director at RAND Europe, where he led the defence and security science, technology and innovation portfolio as well as RAND's Centre for Futures and Foresight Studies. He holds a PhD in Economics from the University of Rome, Italy, and a master's degree in political science from the University of Pisa, Italy.

# Acronyms & Abbreviations

| | |
|---|---|
| **AI** | Artificial intelligence |
| **AWS** | Autonomous weapon system |
| **DSS** | Decision-support system |
| **GNSS** | Global navigation satellite system |
| **ICT** | Information and communications technology |
| **ISR** | Intelligence, surveillance and reconnaissance |
| **OEWG** | Open-ended Working Group |
| **PQC** | Post-quantum cryptography |
| **QKD** | Quantum key distribution |
| **SQUID** | Superconducting Quantum Interference Device |

# Table of Contents


**Executive Summary** **6**

**1. Introduction: The Rise of Quantum Technology** **7**

**2. Fundamental Concepts of Quantum Mechanics** **9**

**3. Exploring the Military Applications of Quantum Technology** **10**

3.1 Quantum Sensing 10
3.2 Quantum Imaging 11
3.3 Quantum Radar Systems 11
3.4 Quantum Communications 12
3.5 Quantum Key Distribution 12
3.6 Quantum Computing 13

**4. International Security Implications of Quantum Technology** **14**

4.1 Global ICT Security 14
4.2 Quantum-Enabled Intelligence, Surveillance and Reconnaissance 14
4.3 Decision-Support Systems and Autonomous Systems 15
4.4 Monitoring and Verification 15

**5. Examples of National and Regional Initiatives on Quantum** **17**

**6. Conclusion** **19**

# Executive Summary

This primer provides policymakers and diplomats with an overview of quantum technology and its anticipated impact on international security, focusing on both its potential benefits and its risks, across military and civilian domains. Quantum advancements promise transformative changes in sensing, computing, communication and cryptography, and they offer enhanced capabilities for intelligence, surveillance and reconnaissance (ISR) as well as critical advancements in information security and cryptographic resilience. However, these same technologies also introduce challenges that could destabilize the security frameworks that underpin global peace.

Quantum sensing, for instance, represents a significant leap in precision measurement, with applications that extend from military operations to disarmament verification. This capability could vastly improve monitoring techniques essential to arms control, allowing for highly sensitive detection of nuclear materials and other critical environmental markers. Quantum sensors also hold promise in the maritime domain, where they could potentially expose previously undetectable underwater assets such as submarines, posing a strategic challenge to traditional naval stealth technologies.

Quantum computing, while still developing, is anticipated to revolutionize fields requiring advanced data processing, such as cryptography, complex simulations and artificial intelligence-driven automation. As this technology matures, it could compromise existing cryptographic systems that secure critical infrastructure and sensitive communications. This underscores the urgency for transitioning to post-quantum cryptographic standards in order to secure government, military and civilian data against future cyberthreats.

Beyond the field of information and communication security, quantum sensors and quantum computing have the potential to impact international peace and security more broadly, in both a positive and negative way. For example, quantum technology could support more accurate verification techniques, bolster non-proliferation efforts and offer remote-monitoring capabilities that are sensitive enough to detect nuclear activity from space, further extending the surveillance reach available to the international community.

There is widespread interest among states in advancing quantum capabilities, spurred by the potential for both competitive advantage and security enhancement. Some states have incorporated quantum development into their national security strategies, often forming public–private partnerships that accelerate research and bridge the gap between scientific innovation and practical application. These initiatives underline the need for multilateral collaboration to address growing asymmetries in quantum capabilities, which could exacerbate existing digital divides between states taking the lead in quantum technology and developing countries.

Moving forwards, there is a need for robust governance frameworks, cross-sector partnerships and a focus on capacity-building to support a quantum-ready workforce. Multilateral cooperation will be essential to establishing norms around the responsible use of quantum technology, promoting stability rather than competition and ensuring that quantum advancements benefit all. A holistic approach to quantum technology – one that addresses its full life cycle – will help states to anticipate and mitigate both its opportunities and its challenges for international peace and security.

# 1. Introduction: The Rise of Quantum Technology

The rise of research, innovation and investment in quantum technology is becoming a global phenomenon.[1] As a technology, it holds much promise for enabling significant breakthroughs in support of many sustainable development goals.[2]

Despite the alluring benefits of quantum technology, there is also apprehension about the risks it could bring to international peace and security. The United Nations Secretary-General cautioned the General Assembly in 2022 that quantum computers could potentially "destroy cybersecurity and increase the risk of malfunctions to complex systems. We don't have the beginnings of a global architecture to deal with any of this."[3]

To be sure, the extent to which quantum-based technologies may shape the future character of warfare, or of security more generally, remains highly uncertain, especially given the fragile and nascent state of quantum systems.[4] Despite this ambiguity, from a global security perspective, because quantum science and technology could revolutionize the field of computing so profoundly, it is important to invest in early education and knowledge-building.

States are showing heightened interest in this technology, as shown by increasing investments in quantum technology research[5] and through the high number of references to quantum made by Member States during the official sessions of the United Nations Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies. [6]

In the approach to 2025, which has been designated by the United Nations as the International Year of Quantum Science and Technology, this primer aims to elevate awareness about the potential implications of quantum technology on international security. It is designed to equip policymakers and diplomats with a frame of reference for considering the risk ecosystem surrounding quantum science and technology.

To help the reader navigate the complexity of the subject, after this introduction, Section 2 provides an overview of selected national and regional initiatives on quantum. Next, Section 3 outlines several foundational concepts in quantum mechanics. Section 4 introduces the military applications of quantum technology. Section 5 then provides a first overview of the possible implications of quantum technology for the international security landscape before the conclusions presented in Section 6.

---

1 Alina Clasen, "Germany Strives to Catch Up with US, China in Quantum Tech Race", Euractiv,12 May 2023, https://www.euractiv.com/section/digital/news/germany-strives-catch-up-with-us-china-in-quantum-tech-race/.

2 Open Quantum Institute, *Progress Report 2024: Quantum for All Initiative* (Geneva: Gesda, October 2024), https://gesda.global/wp-content/uploads/2024/10/GESDA-Quantum-For-All-Progress-Report-2024_Final.pdf.

3 United Nations, "'Our World Is in Big Trouble', Secretary-General Warns General Assembly, Urging Member States to Work as One United Nations", Press Release SG/SM/21466, 20 September 2022, https://press.un.org/en/2022/sgsm21466.doc.htm.

4 Lauren Biron, "Five Ways QSA Is Advancing Quantum Computing", Berkeley Lab News Center, 10 April 2023, https://newscenter.lbl.gov/2023/04/10/five-ways-qsa-is-advancing-quantum-computing/.

5 Indra, "ADEQUADE: Advanced, Disruptive and Emerging QUAntum Technologies for Defence", 2022, https://www.indracompany.com/en/indra/adequade-advanced-disruptive-emerging-quantum-technologies-defence.

6 United Nations, Office for Disarmament Affairs, "Open-ended Working Group on Security of and in the Use of Information and Communications Technologies", https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

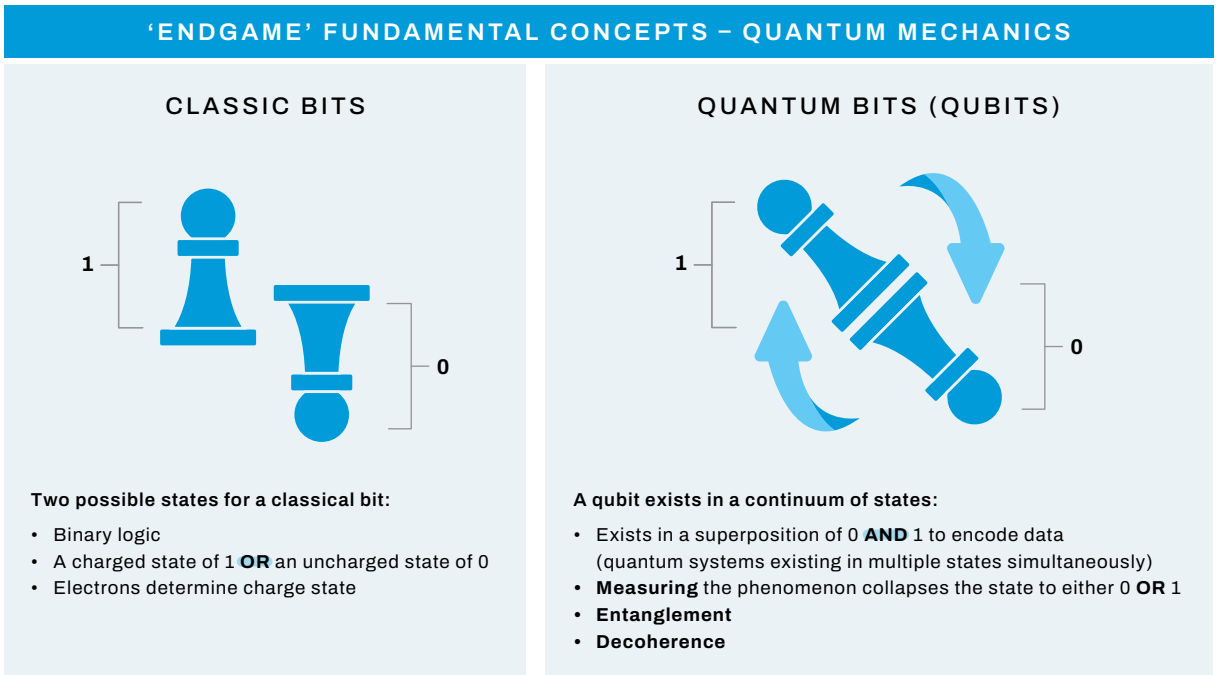
# 2. Fundamental Concepts of Quantum Mechanics

Quantum mechanics studies the behaviour of atoms and particles. Atoms consist of a nucleus, made up of protons and neutrons, that is orbited by electrons. Electrons travel in discrete quanta (i.e., the very smallest unit of energy) and can also move in a continuous wave, like a stream of water from a kitchen sink. Electrons can occupy multiple states simultaneously, in what is called superposition.[7] This phenomenon means that quantum mechanics has been labelled "bizarre" by some physicists.[8]

At the quantum level, events are not simply determined. For example, rather than two discrete states of charge, uncharged (denoted 0) and charged (denoted 1), both can apply simultaneously, and at random too. The famous double-slit experiment demonstrates these unique properties of quantum phenomena. Briefly summarized, scientists observed that, when electron waves passed through two slits, they produced smaller waves, which amplified and negated one another until they collided with the back wall of the testing area. This interference pattern occurred because "electrons seem to act like waves until the point at which they are observed, or measured, when they revert to being particles again".[9]

FIGURE 1.

**A visual representation of classical bits and quantum bits**




7 Ibid.

8 Michio Kaku, *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100* (New York: Anchor, 2012).

9 Amit Katwala, *Quantum Computing: How It Works and How It Could Change the World* (London: Random House Business Books, 2021), p. 16.

Superposition can be explained further using the image of the pawn chess pieces in Figure 1. Imagine that the pawn can either be positioned standing up (indicating a charged stated of 1) or rotated upside down (indicating an uncharged state of 0). This binary logic is how modern digital computers operate. A classical bit (the basic unit of information) – or the classical pawn in this example – can either represent a 0 or a 1. In contrast, quantum computers are more complex systems that operate using different units of information, called **quantum bits** or **qubits**, which exists in a superposition of 0 and 1 to encode data.[10] The quantum pawn in Figure 1 can exist in a continuum of states as it rotates – an atom can thus "contain much more information than a 0 or 1", explains theoretical physicist Michio Kaku.[11] When viewed under a specialized microscope, qubits resemble "silvery plus signs".[12] They enable quantum computers to perform complex modelling tasks and solve multivariable problems more efficiently than digital computers.[13]

Further, qubits can also interact with other qubits in a phenomenon called entanglement. Entanglement is a condition in which "two or more objects in a quantum system can be intrinsically linked to one another, such that measurement of one object dictates the possible measurement outcomes for another, irrespective of how far apart the objects are".[14] This property enables quantum systems to perform multiple calculations at once.[15] However, quantum states are highly sensitive to environmental disturbances, such as sound, movement and changes in temperature.

Scientists are exploring how to leverage superposition to enhance the computational power and speed of quantum computers. Among the many challenges of developing and deploying quantum technology is how to ensure that the highly sensitive quanta are not influenced by decoherence or uncertainty in frequency measurement.[16] The reason for this is that even the act of measuring quantum systems could alter the integrity of the result, collapsing it into a binary form of 0 or 1.[17] These environmental disturbances lead to atrophy (i.e., decoherence), which make it difficult for quantum systems to sustain superposition and entanglement for longer periods of time for experimentation.

---

10 IBM, "IBM Quantum Learning", n.d., https://learning.quantum.ibm.com/.

11 Kaku, *Physics of the Future*.

12 Katwala, *Quantum Computing*, p. 45.

13 Lily Chen et al., *Report on Post-Quantum Cryptography* (Washington, DC: National Institute of Standards and Technology, April 2016), https://doi.org/10.6028/nist.ir.8105.

14 National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Washington, DC: National Academies Press, 2019), https://doi.org/10.17226/25196, p. 26.

15 Alexandre Menard et al., "A Game Plan for Quantum Computing", McKinsey & Company, 6 February 2020, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing.

16 Adrian Cho, "A Quantum Sense for Dark Matter", *Science*, 28 April 2022, https://www.science.org/content/article/crack-mystery-dark-matter-physicists-turn-super-sensitive-quantum-sensors.

17 Ibid.

# 3. Exploring the Military Applications of Quantum Technology

The fundamental properties of quantum mechanics described in Section 2 enable the exploration of multiple military or security applications. In fact, quantum technologies have the potential to offer capabilities in computing, communications and situational awareness that are unparalleled to technology currently available.[18]

This section provides an introductory overview of those applications most commonly referred to in the academic and wider literature: quantum sensing, quantum imaging, quantum radar systems, quantum communications, quantum key distribution (QKD) and quantum computing.

## 3.1 Quantum Sensing

Fundamentally, quantum sensors are measurement tools. While the physics principles and materials for building quantum sensors are the same as conventional sensors, the former are ultra-sensitive. For instance, they are capable of sensing the slightest of environmental disturbances in electric and magnetic fields and the presence of radiation. The major difference between quantum sensors and conventional sensors, however, is that quantum sensors possess remarkable precision capabilities that allow them to detect the smallest unit of energy or measurement, called quanta.[19]

Given quantum sensors' precision capabilities in detecting such infinitesimal changes in time and gravity, scientists are exploring ways in which this technology could be applied to provide an advantage to current military sensing capabilities, for both defensive and offensive purposes. For example, quantum sensors could offer militaries the ability to maintain timing and positioning accuracy in environments where the global navigation satellite system (GNSS) is challenged by electronic interference in the form of signal jamming and spoofing.[20]

In 2017, the Chinese Academy of Sciences announced that it had developed a sensor, called a Superconducting Quantum Interference Device (SQUID), which relies on quantum sensors to detect ultra-sensitive environmental changes (e.g., faint magnetic fields in brain activity). The SQUID is so ultra-sensitive that it can register remote activity in outer space (e.g., solar flares). In addition, the SQUID can detect aircraft as part of national defence and can also support anti-submarine aircraft with enhanced magnetic anomaly detection. Chinese researchers are also developing various types of magnetic detectors, some of which could be mounted on satellites.[21] that could be operated on aircraft to precisely locate minerals beneath the earth's surface.[22]

---

18 North Atlantic Treaty Organization (NATO), "Summary of NATO's Quantum Technologies Strategy", 17 January 2024, https://www.nato.int/cps/en/natohq/official_texts_221777.htm.

19 David Chandler, "Quantum Sensor Can Detect Electromagnetic Signals of Any Frequency", MIT News, Massachusetts Institute of Technology, 21 June 2022, https://news.mit.edu/2022/quantum-sensor-frequency-0621.

20 US Department of Defense, Defense Science Board (DSB), "DSB Reports", n.d., https://dsb.cto.mil/reports/.

21 Henk H.F. Smid, "An Analysis of Chinese Remote Sensing Satellites", *Space Review*, 26 September 2022, https://www.thespacereview.com/article/4453/1.

22 Stephen Chen, "Has China Developed the World's Most Powerful Submarine Detector?", *South China Morning Post*, 24 June 2017, https://www.scmp.com/news/china/society/article/2099640/has-china-developed-worlds-most-powerful-submarine-detector.

In addition, quantum sensors are emerging as a promising technology for enhancing capabilities for detecting submarines underwater. Whether satellite-based systems, fixed underwater systems, or aircraft- or ship-mounted systems, future quantum sensors could have a disruptive impact on the stealth of submarine operations, including for nuclear-powered ballistic missile submarines (SSBNs), which are a crucial asset for nuclear deterrence. In particular:

- **Quantum magnometers** could be used to detect minute changes in magnetic fields caused by a submarine's metal hull or propulsion system. This would vastly expand the detection range for submerged submarines.
- **Quantum gravimeters** could be to measure the smallest variations in gravitational pull, potentially revealing the presence of a submarine's mass. Quantum gravimeters could potentially detect submarines without any method for the submarines to shield themselves.[23]

## 3.2 Quantum Imaging

Quantum imaging is a specialized imaging method that enables scientists to capture advanced quality optical images of an object.[24] This method utilizes entangled light particles to create detailed images of otherwise highly sensitive and unobservable wavelengths.[25] Through manipulating photon pairs, scientists can capture higher quality image resolution, beyond that of traditional methods.[26]

For military operations, advanced infrared imaging capabilities could potentially be developed to augment intelligence, surveillance, and reconnaissance (ISR) capabilities. For example, quantum imaging systems could be applied to sense the presence of harmful noxious gasses in battlefield environments and assist with forensic analysis of chemical weapons and the composition of plastics.[27] In addition, quantum technology could enable so-called ghost imaging, a technique that uses quantum correlations between photons to create images of objects without directly "seeing" them, potentially allowing targets to be imaged through such obscurants as clouds, fog or smoke. This would be valuable for military reconnaissance and targeting.[28] A similar concept would enable a significant improvement in extreme low-light conditions, another scenario of primary importance for successful ISR operations.[29]

## 3.3 Quantum Radar Systems

Conventional radar systems are subject to radar-jamming devices and noise interference from natural phenomena. In contrast, a resilient quantum-enabled radar system could

---

23 Rudy Ruitenberg, "Armed with Quantum Sensors, France Eyes Leaps in Electronic Warfare", *Defense News*, 25 June 2024, https://www.defensenews.com/global/europe/2024/06/25/armed-with-quantum-sensors-france-eyes-leaps-in-electronic-warfare/.

24 "Quantum Imaging", *Nature*, n.d., https://www.nature.com/collections/gehjgebjcc.

25 Fraunhofer-Gesellschaft, "Quantum Imaging: Pushing the Boundaries of Optics", Phys.org, 3 January 2022, https://phys.org/news/2022-01-quantum-imaging-boundaries-optics.html.

26 Ibid.

27 Ibid.

28 Rajesh Uppal, "Quantum Imaging Technique Can Have Military Applications, US and China Racing to Deploy Quantum Ghost Imaging in Satellites for Stealth Plane Tracking", IDST, 26 June 2022, https://idstch.com/technology/photonics/revolutionary-new-quantum-imaging-technique-can-have-military-applications/.

29 National Security Technology Accelerator (NSTXL), "Quantum Technology in the Military", 1 February 2023, https://nstxl.org/quantum-technology-in-the-military/.

detect stealth aircraft with greater accuracy by utilizing a more sophisticated photon-relay system.[30]

Some scholars posit that the potential impact of quantum radar in military operations should not be in question because, once the technology reaches the implementation phase, it will signal the "end of the stealth era".[31] Conversely, according to other experts, there are "still big engineering challenges" surrounding quantum radar, ranging from constructing sensitive detectors to finding a means of stabilizing streams of entangled photons.[32] Overall, there is vigorous debate among theoreticians about the value added by quantum radar technology in military operations.

With regard to space operations, some scholars hypothesize that quantum radar could be used in outer space to detect stealth spacecraft, to track the movement of miniscule yet harmful orbital debris, as well as to monitor ballistic missiles.[33] Others remain sceptical as to the extent of the upgrade in object-detection capability.[34]

Collectively, quantum sensing, imaging and radar technology offer the potential to provide enhanced situational awareness capabilities to militaries, while also potentially threatening to reduce military stealth capabilities in certain contexts.[35]

## 3.4 Quantum Communications

Of all the categories of quantum technology presented in this primer, quantum communications is the least developed for military application at this time. Quantum communications utilizes entanglement – the process by which qubits can communicate with one another simultaneously – to transfer data across transmission channels and locations.[36]

While quantum communication is in its infancy, the subfield of QKD is slightly more developed for military applications.

## 3.5 Quantum Key Distribution

In the military context, communication security is of paramount importance to ensure the ability to exercise effective command and control and achieve mission success. In this regard, encryption of data and information has always played an important role in the military domain. Quantum key distribution utilizes the principles of quantum mechanics to encrypt data. In the physical world, a key is used to both lock and unlock systems. In computing, a key can signify a string of 1s and 0s that can be used to encrypt and decrypt information.

China successfully conducted the first-ever intercontinental ground-to-satellite and satellite-to-ground QKD communications network

---

30 Martin Giles, "The US and China Are in a Quantum Arms Race That Will Transform Warfare", *MIT Technology Review*, 3 January 2019, https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/.

31 See, for example, Professor Seth Lloyd of the Massachusetts Institute of Technology, cited in ibid.

32 See, for example, Professor Jonathan Baugh of the University of Waterloo, cited in ibid.

33 Chris Jay Hoofnagle and Simson Garfinkel, "Quantum Sensors—Unlike Quantum Computers—Are Already Here", Defense One, 27 June 2022, https://www.defenseone.com/ideas/2022/06/quantum-sensorsunlike-quantum-computersare-already-here/368634/.

34 US Department of Defense, Defense Science Board (DSB), "DSB Reports".

35 Hoofnagle and Garfinkel, "Quantum Sensors—Unlike Quantum Computers—Are Already Here".

36 US National Science Foundation (NSF), "NSF and White House Office of Science and Technology Policy Initiate Collaborative Effort to Develop Critical Resources for Quantum Education", 18 May 2020, https://www.nsf.gov/news/special_reports/announcements/051820.jsp.

between the quantum satellite Micius and a quantum communications ground station in Hebei Province in 2017.[37] According to the system commander of Micius, this quantum communications network is "the most secured method of communication because any eavesdropper will disrupt the entanglement and be detected".[38] This test was significant because it demonstrated that quantum-enabled secure communications in space is possible. Further, an article in the *NATO Review* posits that QKD could potentially be leveraged to enable "'ultra-secure' data communication, potentially even completely unhackable" in military defence communications.[39]

## 3.6 Quantum Computing

Quantum computing is an advanced form of computing that uses the principles of quantum physics to process information. This has the potential to solve problems that would take regular computers thousands of years. As such, quantum computing is an enabling technology that holds much promise in all sectors of society, including the military domain. Key military applications include:[40]

- **Cryptography and cybersecurity**, including both code-breaking and quantum-resistant encryption (see Section 4)
- **Artificial intelligence (AI) and machine learning**, supporting both superior decision-support systems (DSSs) and a new generation of autonomous systems
- **Logistics and complex optimization problems**, such as supply chain management and mission planning
- **Simulation and modelling**, providing more accurate and complex simulations of battlefield conditions for military training
- **Materials sciences**, accelerating the discovery and development of new materials for military applications, such as stronger and lighter armour

37 "China Achieves a Quantum Jump", *China Daily*, 18 June 2017, http://en.people.cn/n3/2017/0618/c90000-9229972.html.

38 Ibid.

39 Michiel van Amerongen, "Quantum Technologies in Defence & Security", *NATO Review*, 3 June 2021, https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html.

40 National Security Technology Accelerator (NSTXL), "Quantum Technology in the Military".

# 4. International Security Implications of Quantum Technology

After providing a brief overview of quantum technology and its potential military uses in previous sections, this section provides a first high-level overview of possible international security implications in four key areas: global ICT security, ISR, DSSs and AWS, and monitoring and verification.

## 4.1 Global ICT Security

As mentioned in the introduction, an increasing number of Member States participating in the OEWG on ICT security have highlighted the potential threats posed by quantum technology. How can these threats manifest themselves in practice?

For example, quantum computers could break many current encryption methods, including widely used public-key cryptography systems (e.g., RSA and ECC). This would threaten the security of sensitive government, military and intelligence communications both domestically and between states. This capability would also enable malicious actors to decrypt previously intercepted and stored encrypted communications. In this type of malicious ICT act – referred to as harvest now, decrypt later (HNDL) – encrypted data is exfiltrated and stored today, to then be decrypted in the future using PQC algorithms.[41] This is alarming because these security protocols secure day-to-day Internet-based communications and operations, including those of critical services such as finance and healthcare.[42] Although no quantum computer is presently equipped with enough qubits to quickly calculate the prime factors needed to decrypt sensitive communications,[43] that should not lull policymakers into a state of complacency in considering this growing cybersecurity risk.[44]

States should begin planning how to update sensitive systems to PQC algorithms in order to better protect them against the PQC risk environment. However, transitioning critical infrastructure to PQC standards is a complex challenge that would require time, investment and well-structured cooperation between the public and private sectors. As an initial planning framework, policymakers should focus on addressing these considerations and engage with stakeholders to build trust around upgrading vulnerable systems and infrastructure.

## 4.2 Quantum-Enabled Intelligence, Surveillance and Reconnaissance

Quantum sensors are developing at a fast pace. Some technologists think that they will transition from the laboratory to an operational context more rapidly than quantum computing.[45]

---

41 US National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division, "Post-Quantum Cryptography", n.d., https://csrc.nist.gov/projects/post-quantum-cryptography.

42 Ibid.

43 QuTech Academy, "Shor's Algorithm", n.d., https://www.qutube.nl/quantum-algorithms/shors-algorithm.

44 Menard et al., "A Game Plan for Quantum Computing".

45 Marco Lanzagorta and Jeffrey Uhlmann, "Opportunities and Challenges of Quantum Radar", *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 11 (1 November 2020): 38–56, https://doi.org/10.1109/maes.2020.3004053.

Quantum sensors would first need to be scaled up before being deployed in military operating environments.[46] Quantum sensors could augment ISR capabilities (as explained in Section 3.1), in particular to redefine the concept of stealth operations across all environments. At least at the theoretical level, this could have cascading impacts on international security and stability given the potential ability of quantum sensors to revolutionize the planning and conduct of military operations as well as nuclear deterrence (e.g. through its impact on submarine detection as explained in Section 3.1).

## 4.3 Decision-Support Systems and Autonomous Systems

Quantum systems also have the potential to accelerate research in advanced AI and machine learning capabilities that can unlock a new generation of complex AI systems to support both more advanced DSSs and a new generation of autonomous systems, including AWS. For example, enhanced computational power and the ability to run AI models with quantum algorithms would enable better and faster real-time decision-making (made by humans or autonomous systems) and allow the tackling of intricate optimization problems that are often intractable for classical computers.

To provide some perspective on the magnitude of this innovation, already in 2019 Google's quantum computer was able to complete a task in just 200 seconds that would take a classical computer 10,000 years.[47] This capability is essential for military operations that involve numerous variables and potential outcomes. In addition to providing increased capability for real-time data processing, the integration of quantum computing with AI will allow military planners to simulate various scenarios and outcomes much more efficiently, leading to better-informed decision-making.

In sectors such as healthcare, water management and food security, quantum technology is already showing promising results in terms of efficiency, productivity, accuracy and speed. It is thus important that discussions on the responsible development, deployment and use of AI in the military domain also take into account the potential impact of quantum technology.[48]

## 4.4 Monitoring and Verification

A final, but important, field of application for quantum technology in international security would be monitoring and verification in support of non-proliferation and safeguards. These are critical components in ensuring the peaceful use of nuclear technology and preventing the spread of nuclear weapons. Quantum sensors are emerging as promising tools to enhance these efforts in different ways:

- **Enhanced detection capabilities:** Quantum sensors offer significant improvements in detecting nuclear materials and activities. In particular they improve the

---

46 Marcus Doherty, "Quantum Technology: The Defence Imperative", Australian Army Research Centre, 5 May 2020, https://researchcentre.army.gov.au/library/land-power-forum/quantum-technology-defence-imperative.

47 Cameron Wood and Alex Krijger, "The Convergence of Artificial Intelligence and Quantum Computing: Unravelling the Complex Geopolitical Nexus", Transformation Forums, 18 June 2023, https://www.transformationforums.com/the-convergence-of-artificial-intelligence-and-quantum-computing-unravelling-the-complex-geopolitical-nexus/.

48 Open Quantum Institute, *Intelligence Report on Quantum Diplomacy for the Sustainable Development Goals (SDGs)* (Geneva: Gesda, October 2024), https://open-quantum-institute.cern/wp-content/uploads/2024/10/GESDA_OQI_Intelligence-Report-2024_Final.pdf.

sensitivity and range of radiation detection.[49] They consequently enable more effective monitoring of nuclear facilities and borders to prevent trafficking of nuclear materials.

- **Enhanced environmental sampling:** Quantum sensing technologies could enhance the analysis of environmental samples collected for safeguards purposes. This offers potential to detect trace amounts of nuclear materials with greater precision.[50]
- **Improved verification techniques:** Advanced quantum sensing techniques may allow for more accurate non-destructive measurement of quantities and compositions of nuclear materials. Such measurement is crucial for verifying declarations and detecting diversion.[51] **Enhanced remote monitoring capabilities:** Future quantum sensors deployed on satellites could potentially detect nuclear activities from space with unprecedented sensitivity, enhancing global monitoring capabilities.

---

49 Samanvya Hooda, "Quantum Sensors and Submarine Invulnerability", 16 October 2023, https://www.9dashline.com/article/quantum-sensors-and-submarine-invulnerability.

50 Henning Soller and Niko Mohr, "Quantum Sensing's Untapped Potential: Insights for Leaders", 17 September 2024, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-sensings-untapped-potential-insights-for-leaders.

51 Ibid.

# 5. Examples of National and Regional Initiatives on Quantum

Some states have been investing, or have announced investments, in quantum technology. Many have also leveraged structured public–private partnerships with private-sector actors, from start-ups to major technology companies.[52]

Germany, for example, aspires to lead the global quantum innovation race according to its 2023 Quantum Technologies Conceptual Framework Programme.[53] This document sets forth Germany's strategic framework and it plan to invest €3 billion to develop a universal quantum computer by 2026. Canada also envisions taking centre stage based on its 2023 National Quantum Strategy, having allocated CA$360 million to advancing quantum research, innovation and commercialization.[54]

In 2023, the Australian Government published a National Quantum Strategy and pledged AUS$1 billion towards accelerating quantum innovation.[55] China, by some estimates, is investing $15 billion in quantum technology, and could potentially outspend the rest of the world's investments combined.[56] In contrast with this figure, the European Union is planning to invest $7.2 billion (€6.8 billion) in quantum computing projects by 2025[57] and the United States pledged to spend $1.9 billion up to 2025.[58] Additionally, the Russian Federation pledged to invest $800 million in developing quantum technology up to 2025, and it has adopted a five-year Russian Quantum Technology road map.[59]

In Europe, the European High-Performance Computing Joint Undertaking (EuroHPC JU) has announced plans to invest €100 million in constructing six sites for European quantum computers, in Czechia, Germany, Spain, France, Italy and Poland.[60] As another example, the European Commission's Advanced, Disruptive and Emerging QUAntum technologies for DEfence (ADEQUADE) project, which has over 30 partners in 8 European states, seeks to leverage quantum sensing technology to augment warfighting capabilities.[61]

---

52 See, for example, IBM, "IBM and Government of Quebec Launch Groundbreaking Partnership to Accelerate Discovery with First IBM System in Canada", 3 February 2022, https://newsroom.ibm.com/2022-02-03-IBM-and-Government-of-Quebec-Launch-Groundbreaking-Partnership-to-Accelerate-Discovery-with-First-IBM-Quantum-System-in-Canada.

53 Federal Ministry of Education and Research, "Quantum Technologies Conceptual Framework Programme of the Federal Government", April 2023, https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Quantum-Technologies-Conceptual-Framework-2023_english_bf_C1.pdf.

54 Government of Canada, "Overview of Canada's National Quantum Strategy", 31 July 2023, https://ised-isde.canada.ca/site/national-quantum-strategy/en.

55 Government of Australia, "National Quantum Strategy", 3 May 2023, https://www.industry.gov.au/publications/national-quantum-strategy.

56 Mateusz Masiowski et al., "Quantum Computing Funding Remains Strong, But Talent Gap Raises Concern", McKinsey, 15 June 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern.

57 Ibid.

58 Ibid.

59 "Russia's Quantum Patent Applications Decline Amid Sanctions", *Moscow Times*, 14 June 2023, https://www.themoscowtimes.com/2023/06/14/russias-quantum-patent-applications-decline-amid-sanctions-a81499.

60 Laura Kabelka, "Commission Announces Six Sites for European Quantum Computers", Euractiv, 5 October 2022, https://www.euractiv.com/section/digital/news/commission-announces-six-sites-for-european-quantum-computers/.

61 Indra, "ADEQUADE: Advanced, Disruptive and Emerging QUAntum Technologies for DEfence".

These range from enhancing position, navigation and timing capabilities to advancing radio frequency sensing and optronics sensing.[62] The governments of France and Denmark are collaborating on testing a quantum sensor for determining the earth's gravitational field and assessing how to navigate using quantum-based systems if global positioning satellite navigation services were disrupted during a crisis.[63] Lastly, with adoption in 2023 of its National Quantum Strategy, the United Kingdom committed to more than doubling the investment into quantum by investing £2.5 billion over the next ten years.[64] The United Kingdom is also developing prototype quantum sensors for compact satellites, called "CubeSats", as part of an initiative to explore the applications of quantum technology from earth to outer space.[65]

Turning to the Indo-Pacific, India's National Security Council Secretariat has established the Quantum Lab at the Military College of Telecommunication Engineering to keep abreast of quantum information threats to military systems, such as post-quantum cryptography (PQC).[66] Japan's Government has also announced that it will produce a domestic quantum computer and establish four quantum research centres.

The past several years have demonstrated how the promise of quantum technology is shaping the formation of bilateral and multilateral quantum partnerships, such as the agreements signed by the United States with Switzerland, Japan and Australia.[67] Partnerships are also a key feature of NATO's Quantum Technologies Strategy that highlights how "A quantum-ready Alliance requires, first and foremost, a closer cooperation among Allies, and a resilient quantum ecosystem that extends beyond availability of appropriate funding".[68]

Some projections anticipate that, by the end of 2027, states and private industry are likely to have invested over $16 billion in quantum computing.[69]

---

62 Ibid.

63 Technical University of Denmark, "Navigation Quantum Sensor Being Tested in Greenland", The Mirage, 12 June 2023, https://miragenews.com/navigation-quantum-sensor-being-tested-in-1024820.

64 United Kingdom Department of Innovations, Science and Technology, "National Quantum Strategy", 15 March 2023, https://www.gov.uk/government/publications/national-quantum-strategy#full-publication-update-history.

65 Alanna Madden, "Researchers to Test Limits of Quantum Technologies with Nanoparticles in Space", Courthouse News Service, 21 June 2023, https://www.courthousenews.com/researchers-to-test-limits-of-quantum-technologies-with-nanoparticles-in-space/.

66 Indian Ministry of Defence, "Indian Army Establishes Quantum Laboratory at MHow (MP)", 29 December 2021, https://pib.gov.in/PressReleasePage.aspx?PRID=1786012.

67 Thomas Wong, "The United States and Switzerland Sign Joint Statement to Strengthen Collaboration on Quantum", National Quantum Initiative, 21 October 2022, https://www.quantum.gov/the-united-states-and-switzerland-sign-joint-statement-to-strengthen-collaboration-on-quantum/; United States Department of State, "Tokyo Statement on Quantum Cooperation", 19 December 2019, https://www.state.gov/tokyo-statement-on-quantum-cooperation/; The White House, "The United States and Australia Partner to Build Quantum Future", 18 November 2021, https://www.whitehouse.gov/ostp/news-updates/2021/11/18/the-united-states-and-australia-partner-to-build-quantum-future/.

68 North Atlantic Treaty Organization (NATO), "Summary of NATO's Quantum Technologies Strategy", 17 January 2024, https://www.nato.int/cps/en/natohq/official_texts_221777.htm.

69 IDC, "IDC Forecasts Worldwide Quantum Computing Market to Grow to $7.6 Billion in 2027", 17 August 2023, https://www.idc.com/getdoc.jsp?containerId=prUS51160823.

# 6. Conclusion

As quantum technology advances, it introduces both transformative potential and complex risks into international security. A holistic approach to quantum innovation – one that considers the full life cycle from development to deployment – is essential to understanding its implications for global stability and arms control. In particular, the potential for quantum computers to compromise today's cryptographic protocols underscores the importance of transitioning to PQC standards. This transition will be vital for securing critical infrastructure, communications and defence systems against emerging cybersecurity threats.

Addressing these challenges requires robust collaboration across governments, industry and academia. Such cross-sector partnerships are essential for cultivating a quantum-ready workforce and mitigating digital divides that could emerge as quantum technology advances. Additionally, developing multilateral governance frameworks, confidence-building measures and capacity-building initiatives will support responsible quantum innovation.

Amara's Law states that "we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run". Bearing this in mind, the future of quantum technology calls for careful and coordinated action.

By fostering global cooperation and preparedness, the international community can responsibly integrate quantum advancements. This can then ensure that they serve as tools for stability and security, rather than sources of conflict and disruption.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais de Nations
1211 Geneva, Switzerland



WWW.UNIDIR.ORG