BIPSS Commentary
www.bipss.org.bd
April -2025
BIPSS
Towards a Secure World

Quantum Computing and the Future of Global Deterrence

Tasmia Binte Hossain[1]

Introduction

The emergence of quantum computing represents one of the most significant technological inflection points of the 21st century, with profound implications for global security architecture and deterrence frameworks. As nations race to achieve quantum supremacy, the traditional paradigms of deterrence built upon conventional and nuclear capabilities, cyber dominance, and intelligence supremacy face unprecedented disruption. This commentary examines how quantum computing technologies will reshape the landscape of global deterrence, creating new vulnerabilities while simultaneously opening avenues for enhanced security measures.

The stakes could not be higher. Quantum computers harness the peculiar properties of quantum mechanics - superposition, entanglement, and interference - to perform calculations at speeds unattainable by classical computers. For certain problems, quantum computers offer exponential advantages over their classical counterparts. This computational leap forward threatens to undermine existing cryptographic systems, enhance artificial intelligence capabilities, and revolutionize sensor technologies, all critical components of modern deterrence strategies.

As we stand at this technological crossroads, policymakers and security professionals must understand not only the technical capabilities of quantum systems but also their strategic implications. The nation that achieves decisive quantum advantages first may fundamentally alter global power balances in ways more subtle but potentially more far-reaching than the advent of nuclear weapons.

[1] Tasmia Binte Hossain is a Research Intern at Bangladesh Institute of Peace and Security Studies (BIPSS). She has completed her BSS & MSS in Development Studies from the Bangladesh University of Professionals (BUP).

The Quantum Computing Revolution: Technical Foundations

Before analyzing deterrence implications, we must understand the fundamental differences between classical and quantum computing paradigms. Classical computers process information in binary digits (bits), which exist in one of two states: 0 or 1. Quantum computers, however, leverage quantum bits or "qubits" that can exist in multiple states simultaneously through the principle of superposition. This enables quantum systems to explore multiple computational paths concurrently, offering exponential acceleration for specific computational problems.

Quantum entanglement, Einstein's "spooky action at a distance", allows qubits to become correlated in ways that have no classical analog. This property enables quantum computers to execute complex algorithms that would require billions of years on classical systems, potentially solving them in minutes or seconds.

Several quantum computing architectures are under development globally, including:

- Superconducting circuits (pursued by IBM, Google, and Amazon)
- Trapped ions (developed by IonQ, Honeywell)
- Photonic systems (Xanadu, PsiQuantum)
- Topological qubits (Microsoft)
- Silicon spin qubits (Intel, various research institutions)

Each architecture offers distinct advantages and faces unique engineering challenges, but all share the potential to dramatically alter the security landscape through three primary mechanisms: cryptographic disruption, enhanced sensing capabilities, and advanced artificial intelligence.

The race toward practical quantum computers has accelerated dramatically. In 2019, Google claimed to have achieved "quantum supremacy" when its 53-qubit Sycamore processor completed a specific calculation in 200 seconds that would reportedly take the world's most powerful supercomputer 10,000 years.[2] While this claim has been disputed and the calculation held little practical value, it marked an important symbolic milestone in quantum development.

[2] Brumfiel, Geoff. "Google Claims Quantum Supremacy, But IBM Disagrees." NPR, October 23, 2019. https://www.npr.org/2019/10/23/772580902/google-claims-quantum-supremacy-but-ibm-disagrees.

Cryptographic Vulnerabilities and the "Harvest Now, Decrypt Later" Threat

Perhaps the most immediate and concerning implication of quantum computing for global deterrence is its potential to compromise existing public-key cryptographic systems. Many of today's most widely used encryption protocols including RSA, DSA, and elliptic curve cryptography derive their security from mathematical problems that are computationally intensive for classical computers but vulnerable to quantum algorithms.

Peter Shor's eponymous algorithm, developed in 1994, demonstrated that a sufficiently powerful quantum computer could efficiently factor large numbers, breaking RSA encryption.[3] Similarly, Lov Grover's search algorithm can quadratically accelerate brute-force attacks against symmetric cryptographic systems, effectively halving their security strength.

This vulnerability creates a distressing scenario: the "harvest now, decrypt later" threat. Adversaries are already collecting and archiving encrypted communications with the expectation that future quantum computers will render them readable. This threatens the confidentiality of sensitive diplomatic communications, military command and control systems, and critical infrastructure.

Real-world example: In January 2023, researchers at the University of Science and Technology of China demonstrated a 66-qubit quantum computer solving a specific computational problem 100 trillion times faster than classical supercomputers.[4] While still far from breaking modern encryption, this achievement underscores the accelerating pace of quantum development. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has already issued directives urging federal agencies to inventory cryptographic systems vulnerable to quantum attacks and develop migration plans toward quantum-resistant algorithms.

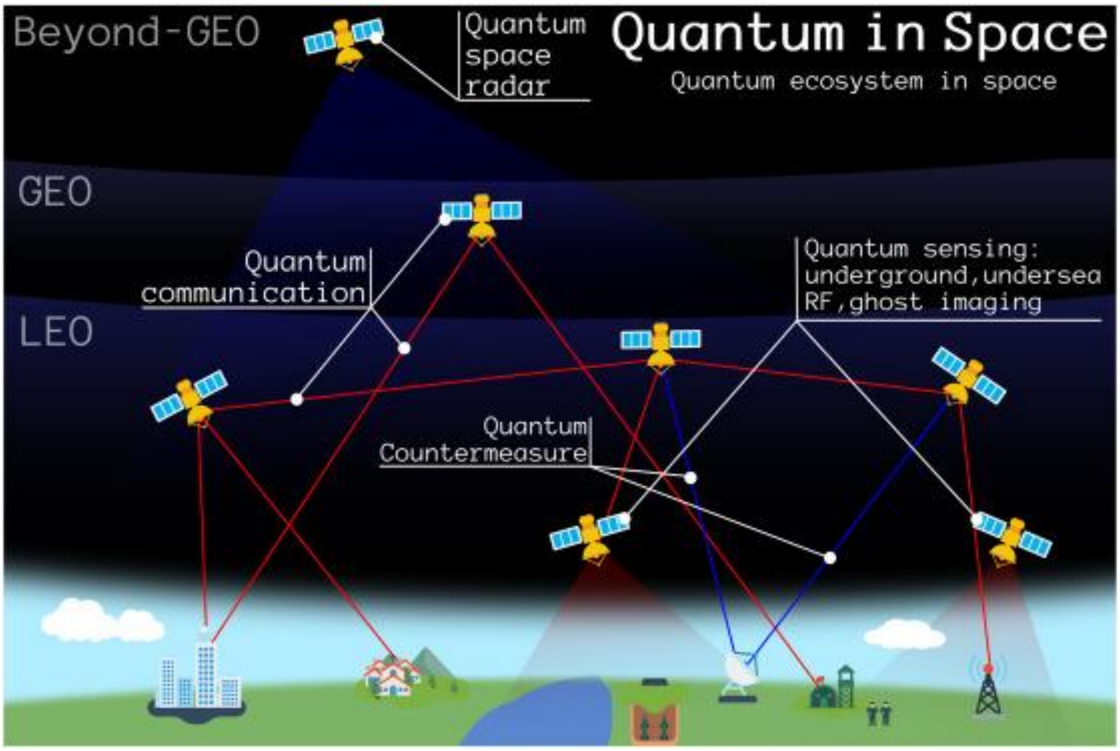
The implications for deterrence are profound. Nations with advanced quantum computing capabilities may gain unprecedented intelligence advantages, potentially undermining the strategic calculations that underpin deterrence frameworks. If a nation believes its secure

---

[3] Perrig, Adrian, Pawel Szalachowski, and Anupam Joshi. "Quantum-Safe Cryptography: Challenges and Solutions." IEEE Security & Privacy 18, no. 5 (2020): 43-50.
[4] Pan, Jian-Wei, Xiang-Bin Wang, Yang Liu, Cheng-Zhi Peng, and Zeng-Bing Chen. "Quantum Science and Technology in China: Progress and Global Impact." Nature Reviews Physics 4, no. 1 (2022): 20-30.

communications have been compromised, it may alter its behavior, potentially leading to more aggressive postures or dangerous misperceptions during crises.

Post-Quantum Cryptography: A New Deterrence Imperative



Source: ScienceDirect.com

Recognizing the existential threat to cryptographic systems, nations and organizations have accelerated the development of post-quantum cryptography (PQC) algorithms resistant to both classical and quantum attacks.[5] The U.S. National Institute of Standards and Technology (NIST) has led a multi-year standardization process to identify viable PQC candidates, with final standards expected to be fully implemented by 2030.

Leading candidates include:

- Lattice-based cryptography
- Hash-based cryptography
- Code-based cryptography
- Multivariate polynomial cryptography

---

[5] Khan, Zeba, Neetesh Saxena, and Prashant Pillai. "Post-Quantum Cryptography and Its Implementation Challenges." IEEE Access 9 (2021): 24475-24508.

- Isogeny-based cryptography

The transition to quantum-resistant algorithms represents a massive global undertaking with significant deterrence implications. Nations that successfully implement robust PQC across government, military, and critical infrastructure systems will establish new strategic advantages. Those that lag behind may find themselves vulnerable to intelligence exploitation and strategic coercion.

Real-world example: In 2022, the Biden administration issued National Security Memorandum 10, directing all federal agencies to begin transitioning to quantum-resistant cryptographic standards by 2035.[6] Similarly, China's 14th Five-Year Plan explicitly prioritizes quantum-resistant cryptography development, allocating substantial resources to the effort. This has created a new dimension in the U.S.-China strategic competition, where cryptographic resilience becomes a crucial element of national security.[7]

The transition to post-quantum cryptography also introduces new verification challenges. Unlike physical weapons systems that can be counted and monitored through traditional arms control verification measures, cryptographic implementations are inherently difficult to verify externally. This creates potential trust deficits that could undermine strategic stability.

Quantum Sensing and the Erosion of Strategic Stealth

Beyond cryptography, quantum sensing technologies threaten to erode strategic capabilities that rely on concealment and stealth fundamental aspects of nuclear deterrence strategies. Quantum sensing leverages quantum entanglement, superposition, and squeezing to detect minute variations in gravity, magnetic fields, and other physical phenomena with unprecedented precision.

These capabilities could potentially:

- Detect previously undetectable submarines, undermining sea-based nuclear deterrents

---

[6] The White House. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." May 4, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[7] Kania, Elsa B., and John K. Costello. "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership." Center for a New American Security, September 12, 2018. https://www.cnas.org/publications/reports/quantum-hegemony.

- Identify underground military facilities, including hardened missile silos
- Enhance surveillance capabilities across electromagnetic spectrums
- Provide countermeasures against existing stealth technologies

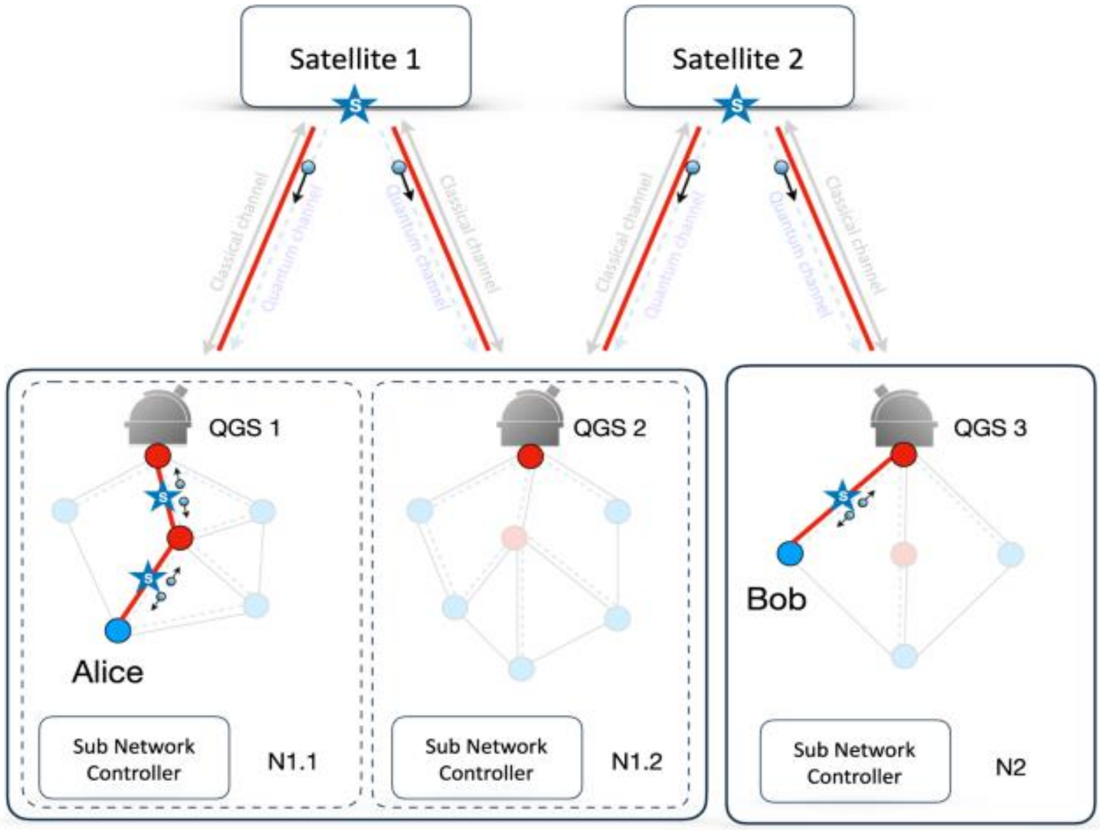
The erosion of strategic stealth could fundamentally destabilize the nuclear balance of power by undermining second-strike capabilities, the cornerstone of nuclear deterrence since the Cold War.

Real-world example: In 2021, researchers at MIT and DARPA demonstrated quantum accelerometers capable of detecting minute gravitational changes without external references.[8] Scaled and refined, such technologies could eventually detect large, dense objects underwater like nuclear submarines from aircraft or satellite platforms. The Chinese Academy of Sciences has reportedly achieved significant breakthroughs in quantum magnetometers that could similarly detect submarine magnetic signatures at greater ranges than current technologies allow.

This potential capability shift raises profound questions for strategic stability. If sea-based nuclear deterrents become vulnerable to detection and tracking, nuclear powers may pursue alternative deployment strategies or technologies, potentially including more destabilizing options. Similarly, if hardened missile silos can be precisely located through quantum gravimetry, nations may reconsider fixed land-based systems in favor of mobile platforms.

[8] Zeng, Bei, and Xianfeng Xu. "Quantum Sensing: Precision Measurement and Applications." National Science Review 8, no. 10 (2021): nwab121.

Quantum Communication Networks and Strategic Stability



Source: Nature

While quantum computing introduces new vulnerabilities, quantum communication networks particularly those utilizing quantum key distribution (QKD) offer unprecedented security guarantees.[9] QKD leverages the fundamental properties of quantum mechanics to create theoretically unhackable communication channels. Any eavesdropping attempt necessarily disturbs the quantum states being transmitted, alerting the communicating parties to intrusion.

Nations leading in quantum communication infrastructure development may establish new strategic advantages in secure command and control systems particularly for nuclear forces potentially altering deterrence calculations.

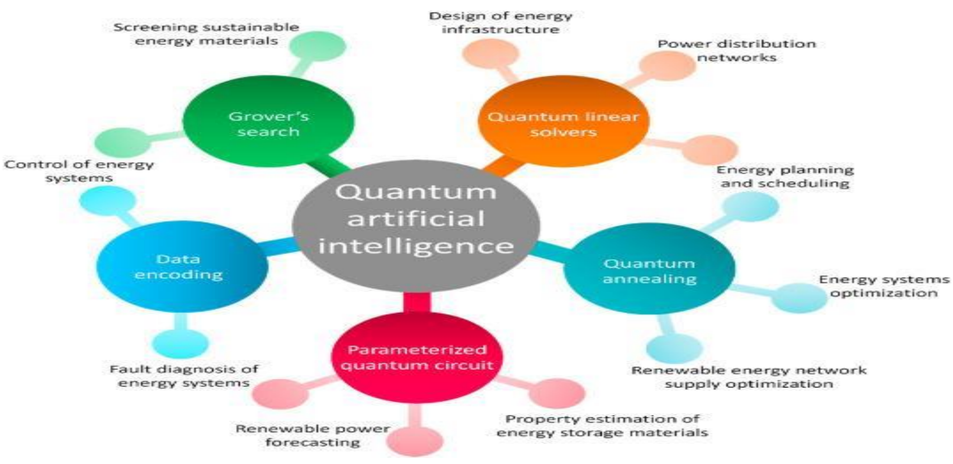
[9] Yang, Yuan-Yuan, Michael Brodsky, and Carl Williams. "Quantum Communications and Quantum Networks: A Quantum Information Perspective." Journal of Lightwave Technology 38, no. 4 (2020): 811-824.

Real-world example: China has invested heavily in quantum communication networks, completing a 2,000-kilometer quantum link between Beijing and Shanghai in 2017 and launching the world's first quantum communication satellite, Micius. In 2020, Chinese researchers reported successful quantum key distribution between space and ground stations over distances exceeding 1,200 kilometers. Similarly, in 2022, the European Quantum Communication Infrastructure initiative announced plans for a continent-wide quantum network by 2027.[10]

These developments suggest a future where quantum-secured communication networks could enhance strategic stability by providing high-confidence command and control channels resistant to disruption or interception. However, asymmetric deployment of such technologies could create destabilizing advantages or perceptions of vulnerability among nations lacking similar capabilities.

Of particular significance is the potential application of quantum communication technologies to nuclear command and control systems. Nations with quantum-secured nuclear command channels may operate with greater confidence in their ability to maintain positive control over nuclear forces even during complex crisis scenarios or under cyber attack.

Quantum Computing and Artificial Intelligence: Force Multipliers for Deterrence



Source: ScienceDirect.com

---

[10] Pan, Jian-Wei, Xiang-Bin Wang, Yang Liu, Cheng-Zhi Peng, and Zeng-Bing Chen. "Quantum Science and Technology in China: Progress and Global Impact." Nature Reviews Physics 4, no. 1 (2022): 20-30.

The intersection of quantum computing and artificial intelligence represents another critical dimension in future deterrence frameworks. Quantum computers offer potential advantages for specific AI tasks, including:

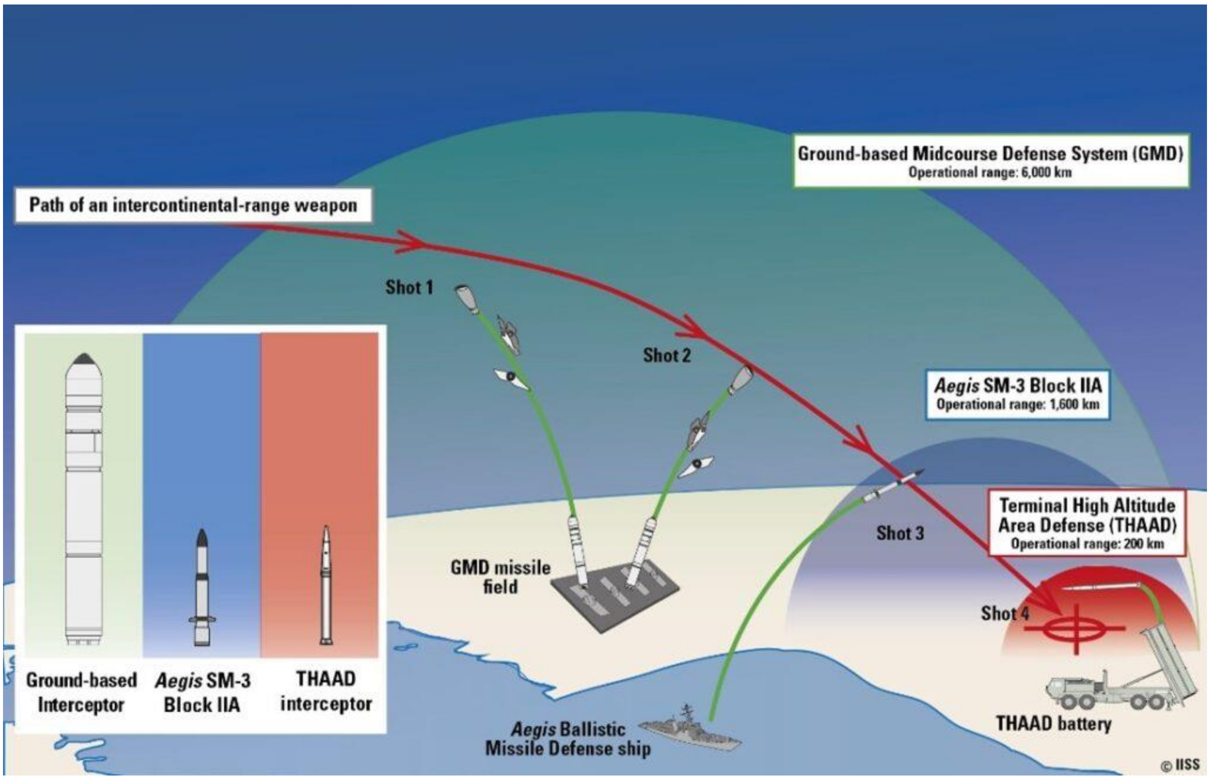
- Enhanced machine learning through quantum algorithms
- Accelerated optimization problems critical for military planning
- Improved pattern recognition for intelligence analysis
- More efficient simulation of complex systems for wargaming and scenario planning

The nation that first successfully integrates quantum computing with advanced AI systems may achieve decision-making advantages that fundamentally alter deterrence calculations. While classical AI systems have already demonstrated superhuman capabilities in specific domains, quantum-enhanced AI could potentially process vastly more complex scenarios with greater speed.

Real-world example: In 2023, researchers at the Defense Advanced Research Projects Agency (DARPA) demonstrated a quantum-classical hybrid system that achieved a 20x performance improvement for specific machine learning tasks related to satellite imagery analysis.[11] While still experimental, this proof-of-concept illustrates the potential for quantum technologies to enhance military intelligence capabilities.

[11] Department of Defense. "DOD Adopts First Department-wide Policy for Responsible Artificial Intelligence." Press Release, February 16, 2023. https://www.defense.gov/News/Releases/Release/Article/3301547/dod-adopts-first-department-wide-policy-for-responsible-artificial-intelligence/.

The Quantum Arms Race and New Deterrence Frameworks



Source: Atlantic Council

The global competition to achieve quantum advantages has accelerated dramatically, with significant implications for strategic stability.[12] Major powers are pursuing distinct quantum strategies:

- The United States has adopted a primarily private-sector-driven approach, leveraging companies like IBM, Google, and Microsoft, with government support through DARPA, NSF, and DOE initiatives.
- China has implemented a state-directed strategy with massive centralized investments, establishing the world's largest quantum research facility in Hefei.
- The European Union pursues a collaborative approach through the Quantum Flagship program, emphasizing cross-border research networks.
- Russia, India, Japan, South Korea, and others have established national quantum initiatives with varying levels of funding and focus areas.

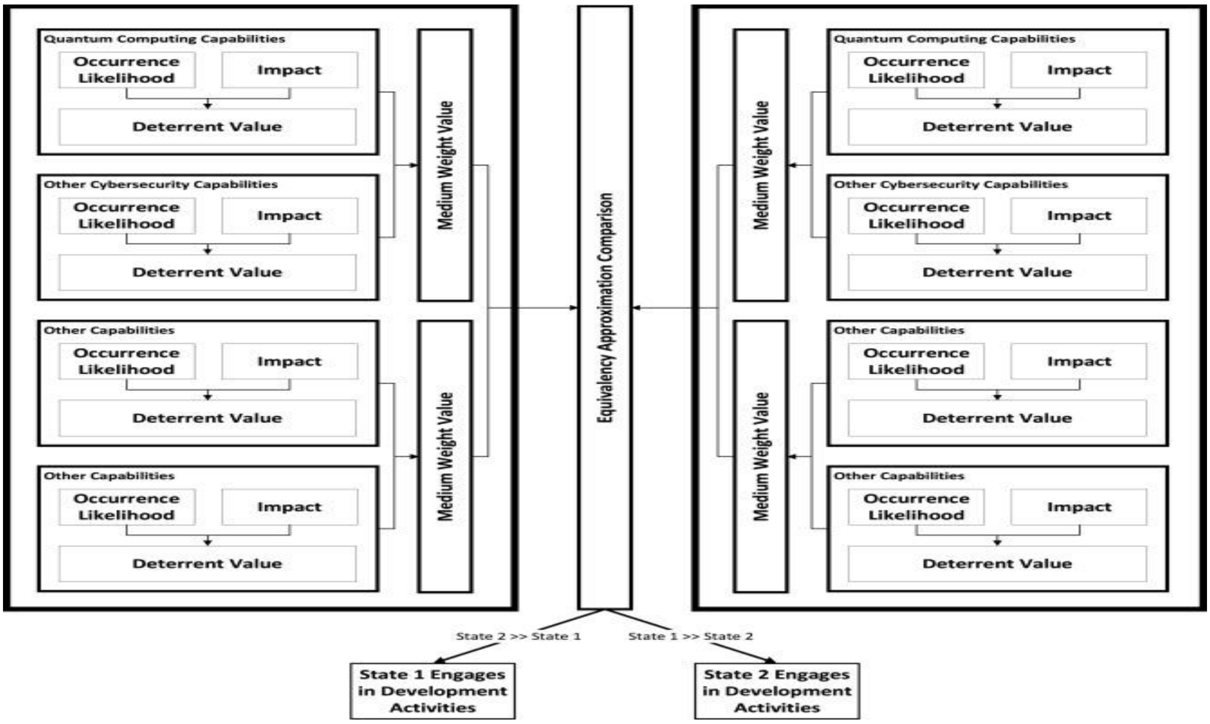
[12] Dellios, Rosita, and Fiona Cunningham. "The New Great Game: Quantum Arms Race and Strategic Stability." Global Policy 13, no. 2 (2022): 245-259.

This quantum arms race introduces several concerns for strategic stability:

- **First-mover advantages**: Nations achieving quantum breakthroughs first may gain temporary but decisive intelligence and military advantages.
- **Transparency challenges**: Quantum capabilities are difficult to verify externally, complicating arms control verification.
- **Dual-use ambiguity**: Most quantum technologies have both civilian and military applications, creating attribution challenges.
- **Proliferation risks**: Unlike nuclear technology, quantum expertise may prove difficult to contain through traditional nonproliferation approaches.

Of particular concern is the development timeline asymmetry between offensive quantum capabilities (breaking encryption) and defensive measures (implementing quantum-resistant systems). If offensive capabilities mature more rapidly, the global system may experience a period of heightened vulnerability and strategic instability.

Toward a Quantum Deterrence Framework



Source: ScienceDirect.com

As quantum technologies mature, nations must develop new deterrence frameworks that account for these transformative capabilities. Several principles should guide this evolution:

1. **Quantum Resilience as Strategic Imperative**

Nations must prioritize quantum-resilient systems across government, military, and critical infrastructure. This includes:

- Implementing post-quantum cryptography before large-scale quantum computers emerge
- Developing quantum-resistant communication networks for nuclear command and control
- Creating heterogeneous security systems that don't rely on single cryptographic approaches
- Establishing cryptographic agility that allows rapid updates as threats evolve

The resilience imperative extends beyond technological solutions to include organizational adaptations, workforce development, and novel strategic concepts. Military and intelligence organizations must develop quantum literacy among key personnel while establishing specialized units focused on quantum applications.

2. **International Norms and Governance**

The international community should develop norms and governance frameworks specifically addressing quantum technologies in security contexts. Potential approaches include:

- Quantum technology verification regimes
- International standards for quantum-safe systems
- Agreements limiting quantum applications in specific military domains
- Confidence-building measures around quantum capabilities

Real-world example: In 2023, seventeen nations signed the Quantum Security Principles declaration at the Munich Security Conference, committing to responsible quantum technology development, establishment of PQC standards, and protection of critical infrastructure.[13] While non-binding, this represents an initial step toward international quantum governance.

---

[13] Chowdhury, Amlan, Jérôme François, and Olivier Festor. "Quantum Safe Cryptography: A Survey." In 2021 International Conference on Computer Communications and Networks (ICCCN), 1-9. IEEE, 2021.

Unlike nuclear weapons, quantum technologies resist easy categorization and verification, complicating traditional arms control approaches. New verification methodologies will be required, potentially leveraging a combination of technical measures, inspections, and confidence-building mechanisms.

3. Multi-Domain Deterrence Integration

Quantum technologies will not exist in isolation but must be integrated into comprehensive multi-domain deterrence strategies. This requires:

- Incorporating quantum capabilities into conventional, nuclear, and cyber deterrence frameworks
- Developing attribution capabilities for quantum-enabled attacks
- Establishing clear escalation ladders that include quantum dimensions
- Creating credible response options to quantum-enabled aggression

Military planners must consider how quantum advantages might alter traditional deterrence calculations while developing contingency plans for scenarios where quantum capabilities disrupt expected outcomes.[14] This includes reconsidering nuclear command and control systems, strategic communication channels, and intelligence collection methodologies.

4. Reducing Strategic Surprise through Research Transparency

Given the potential for quantum breakthroughs to create strategic surprise, nations should consider selective transparency measures around fundamental quantum research. While classified applications will necessarily remain protected, greater openness in basic research could reduce miscalculation risks and provide early warning of significant capability shifts.

International scientific collaboration on quantum technologies offers a potential vehicle for confidence-building while advancing shared interests in peaceful applications. Collaborative research initiatives could focus on quantum applications for climate modeling, medical research, and other global challenges while establishing communications channels that might reduce tensions during crises.

---

[14] Jervis, Robert. "Deterrence Theory Revisited." World Politics 31, no. 2 (1979): 289-324.

Conclusion

Quantum computing represents both an existential challenge to current deterrence frameworks and an opportunity to build more robust security architectures.[15] The world stands at a technological inflection point comparable to the dawn of nuclear weapons or the emergence of cyberspace, a moment when technological revolution forces fundamental reconsideration of strategic concepts. Nations that successfully integrate quantum technologies into comprehensive deterrence strategies while simultaneously building resilience against quantum-enabled threats will establish significant advantages in the emerging security landscape. Those that fail to adapt risk strategic obsolescence and potential coercion.

The race toward quantum advantages will define international security in the coming decades. Unlike previous technological revolutions, quantum supremacy may be achieved suddenly and without clear external indicators. This places a premium on proactive policy development, international dialogue, and strategic foresight. As quantum technologies continue to advance, policymakers, military strategists, and national security professionals must develop nuanced understandings of these complex technologies and their strategic implications. Only through such understanding can nations navigate the quantum future while maintaining strategic stability and effective deterrence frameworks.

The future of global deterrence will be shaped not only by the quantum capabilities nations develop but by the wisdom with which they integrate these technologies into comprehensive security strategies. The challenge before the international community is to harness quantum innovation while avoiding the destabilizing effects that could undermine decades of carefully constructed deterrence frameworks.

[15] Dellios, Rosita, and Fiona Cunningham. "The New Great Game: Quantum Arms Race and Strategic Stability." Global Policy 13, no. 2 (2022): 245-259.