Conf42 | Quantum Computing

Advancements in Quantum Warfare

- Komal Pandya

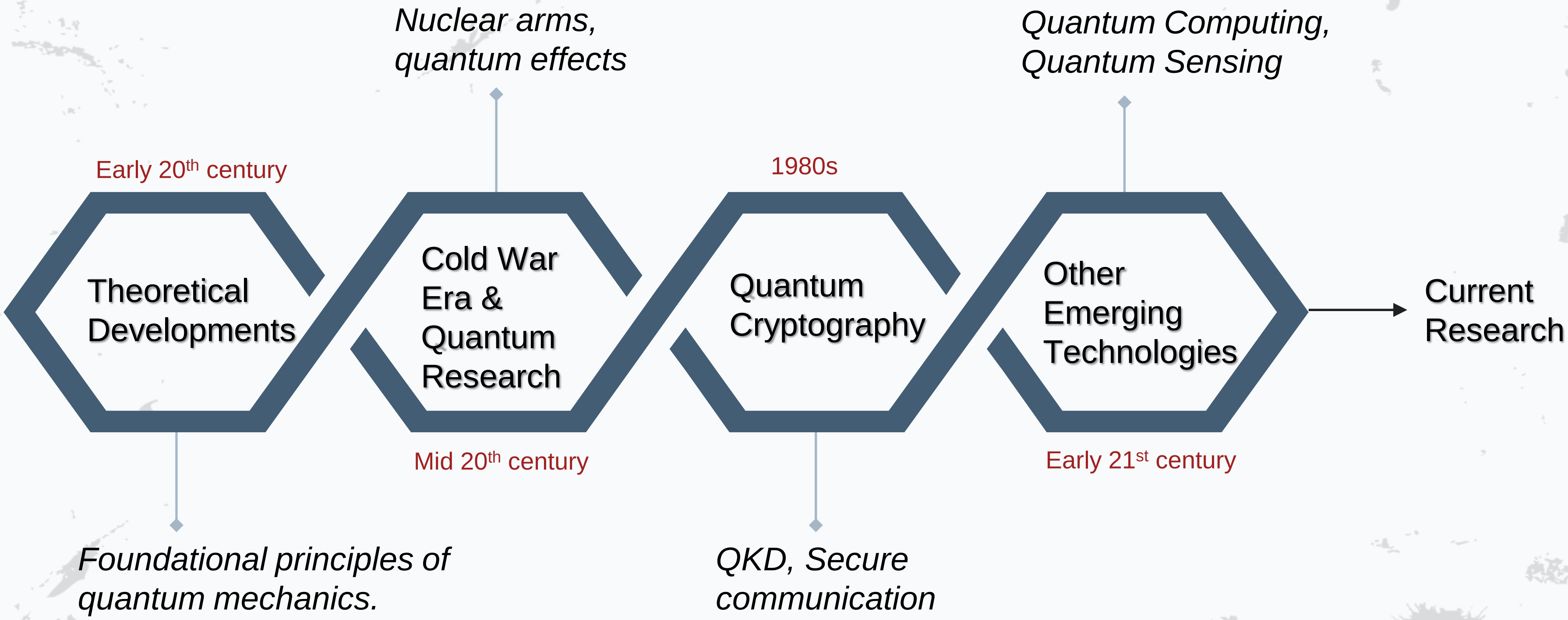
Table of contents

01

Introduction

Quantum Warfare

- Leveraging quantum technologies to enhance military strategies, operations and weapons.
- Offer capabilities that surpass classical methods in encryption, data processing, and sensing.
- Can optimize logistics, enhance decision-making processes, and improve the performance of autonomous systems.


Early 20th century
Theoretical Developments
Foundational principles of quantum mechanics.
Mid 20th century
Cold War Era & Quantum Research
Nuclear arms, quantum effects
1980s
Quantum Cryptography
QKD, Secure communication
Early 21st century
Other Emerging Technologies
Quantum Computing, Quantum Sensing
Current Research

02

Components

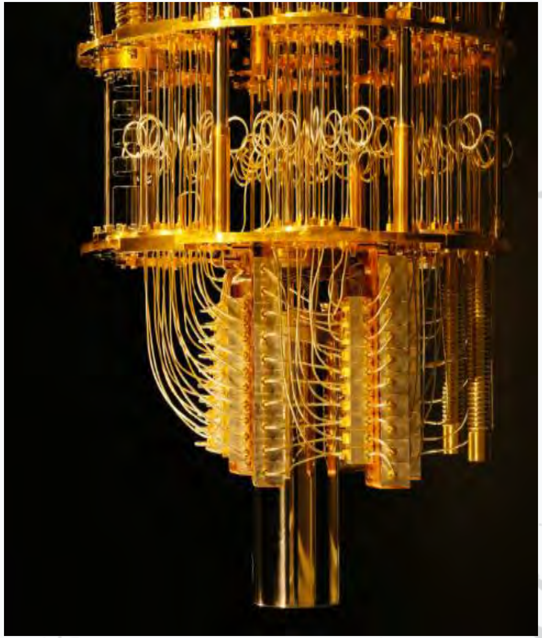
Main Components

Components

1. Quantum Computing
2. Quantum Communication
3. Quantum Sensing

01 Quantum Computing

- Utilizing quantum mechanics principles to perform computation and process information.
- Superconducting, trapped ions, photonic, annealing-based, etc.
- Useful for solving complex problems, usually through subroutines and hybrid computation.
- The quantum computers can be availed through cloud services.



Quantum ML & AI

- The properties like superposition and parallelism have garnered significant interest, prompting efforts to adapt classical ML algorithms for quantum computing in the NISQ era.

- Promise advancements in semi-supervised approaches, such as reinforcement learning and Bayesian networks.

- Quantum-enhanced ML/AI enhance specific machine learning tasks like quantum sampling, linear algebra operations, and quantum neural networks.

Status : Research in progress

Role

- Intelligence/Threat Analysis and Classification using Pattern Recognition.
- Big data processing.
- Automated defense mechanisms.
- Combat simulations.

Major Challenges

- Error correction.
- Developing quantum algorithms.
- Processing classical data.
- Quantum memory.

Quantum Optimization

- Explores solving complex NP problems using optimization procedures like QAOA and QUBO.
- Quantum Approximate Optimization Algorithm (QAOA) finds approximate solutions to optimization problems.
- Quadratic Unconstrained Binary Optimization (QUBO) transforms an optimization problem into a form that can be tackled by quantum annealers.
- Quantum-inspired classical algorithms may provide performance improvements.

Status : Various proof-of –concept demonstrated

Role

- Mission planning and scheduling.
- Resource allocation strategies.
- Efficient decision-making.
- Logistics and supply chain management.

Major Challenges

- Mapping the problems.
- Developing hybrid systems.
- Scalability.

Other Quantum Algorithms

- Quantum searching algorithms and quantum random walk mechanisms, offer significant speedup for unstructured data analysis.

- The HHL algorithm shows potential for super-polynomial speedup in solving linear equations.

- Quantum-phase estimation and variational techniques (like VQE) are dominant approaches for quantum simulations.

Status : Demonstrated effectiveness, other algorithms in progress.

Timeline

Next 5 Years

- Improvements in quantum error correction and qubit coherence times.

- Increasingly used for specialized applications such as optimization problems, complex simulations, and machine learning

5-10 Years

- Quantum computers with hundreds to thousands of qubits could emerge.

- More robust error-corrected quantum computers that can outperform classical systems.

10-20 Years

- Fully fault-tolerant quantum computers could become a reality.

- Practical, large-scale quantum computers with thousands of qubits.

02 Quantum Communication

- Transmitting quantum information using fibres or free-space channels with quantum communication protocols.
- Enable the exchange of cryptographic keys to provide theoretically secure communication channels.
- Developing quantum-safe cryptographic algorithms to secure data against potential threats from quantum computers.

Quantum Key Distribution

- Designed to securely distribute a secret key between parties for encrypting data over classical channels.

- It leverages the no-cloning theorem to ensure that any eavesdropper is detectable.

- Two main protocols - BB84, E91.

Status: Commercially available, further experiments ongoing.

Role

- Enhanced cybersecurity.
- Secure satellite-based communications.
- Protection of defense networks and command and control systems.

Major Challenges

- Scalability issues.
- Integration with current systems.
- Lack of specialized hardware.
- Limited range.
- Vulnerable to attack.

Quantum Network

- Designed to transmit qubits between spatially separated quantum processors.
- The structure of quantum networks comprise end nodes (quantum processors), communication lines, optical switches, and quantum repeaters.
- Enable secure direct communication and efficient redistribution of tasks based on individual quantum computer performance.
- Data sharing across networked quantum computers facilitates scalable quantum computing via distributed systems.

Status: Research in progress

Role

- Position verification techniques.
- Distributed yet powerful computing network.
- Resilient and Tamper-proof networks.

Major Challenges

- Development and maintenance of components.
- Enhancing quantum processors.

Post – Quantum Cryptography

- Encompasses encryption techniques designed to withstand future quantum computer attacks.
- Most current symmetric cryptographic algorithms and hash functions are still secure against quantum attacks.
- New algorithms are being created in anticipation of Q-Day, when current cryptographic methods will become vulnerable to quantum computing.
- Can safeguard the integrity and authenticity of military data.

Status: Different approaches developed, Testing for implementation

Timeline

Next 5 Years

- Expansion of QKD networks in urban and metropolitan areas.

- Continued development of satellite-based quantum communication.

5-10 Years

- Integration of quantum communication protocols with classical internet infrastructure.

- Development of quantum repeaters.

10-20 Years

- Realization of a global quantum internet.

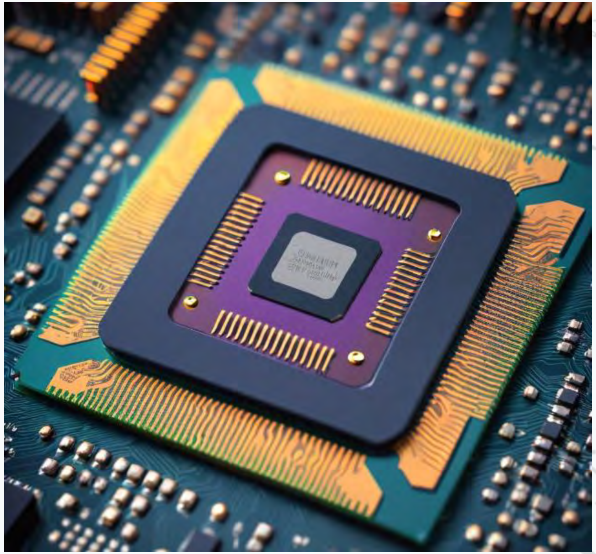
- Robust quantum repeaters and satellite constellations to maintain quantum entanglement.

03 Quantum Sensing/ Metrology

- Using quantum phenomena for measuring physical quantities like magnetic/electric fields, temperature, pressure, etc.

- Exploits the inherent weakness of quantum technology – strong sensitivity to external disturbances.

- Offer sensitivity and precision in measuring, providing long-term stability and accuracy compared to conventional sensors.



Quantum Clocks

- Highly precise timekeeping devices, uses laser-cooled single ions in an electromagnetic trap.
- State-of-the-art chip-sized atomic clocks achieve an uncertainty of 2×10^{-12}, while quantum logic single-ion clocks have uncertainties as low as $\sim 9 \times 10^{-18}$.
- The higher precision of quantum clocks enables new types of measurements, can measure the difference in height between arbitrary points on Earth at an accuracy of one centimeter.

Status: Lab prototypes, Miniaturization in progress

Role

- Precise positioning and navigation.
- Advancing missile guidance systems.
- Synchronizing multi-phase ops and attacks.
- Co-ordinating complex military manoeuvres.

.

Major Challenges

- Ensuring reliability and longevity.
- Making energy-efficient models.
- Addressing technical complexities.
- Miniaturization.

Quantum Radar

- Utilizes quantum features in both the radiation source and output detection to outperform classical radar systems.

- Counteract conventional radar jamming techniques.

- Properties with noise radars - probability of detection and efficient spectrum sharing.

- Several protocols proposed, each having its own requirements, strength and limitation.

Status: Proof-of-concept, Preliminary experimental prototype.

Role

- Stealth Detection.
- Electronic Warfare.
- Maritime Security.
- Space Situational Awareness.

.

Major Challenges

- Limited range and power.
- Dependence on other quantum services.
- Sensitivity to noise.

Quantum Imaging

- Enhance imaging capabilities beyond the limits of classical systems.

- Techniques in quantum imaging include quantum ghost imaging, SPAD arrays, quantum illumination, and sub-shot-noise imaging, etc.

- Can perform tasks such as behind-the-corner imaging, low-light level detection, and high-resolution 3D mapping.

Status: Prototypes, Testing for future use-cases

Role

- Non-Line-of-Sight Imaging.
- High-resolution images with minimal light.
- Improved Signal-to-Noise Ratio for monitoring.
- 3D imaging for better mapping of terrains and structures.

Major Challenges

- Development costs.
- Environmental sensitivity.
- Real-time data processing.
- Security and reliability.

Timeline

Next 5 Years

- Prototyping and testing quantum sensors in various environments.

- Deployments for precision navigation and resource exploration are anticipated.

5-10 Years

- Can enter the commercial market.

- More extensive use of quantum sensors in military applications.

10-20 Years

- Can become affordable , standard equipment.

- Integration into space-based/naval platforms with long-range capabilities.

03

Mechanisms

Mechanisms

Attacking

- **Shor's Algorithm** - Threatens public key encryptions.
- **Grover's Algorithm** - Weakens symmetric key encryption.
- **Simon's Algorithm** - Pose risks to MAC and AEAD algorithms.
- **Classical hacking/Physical attack** - Can target classical components.

Mechanisms

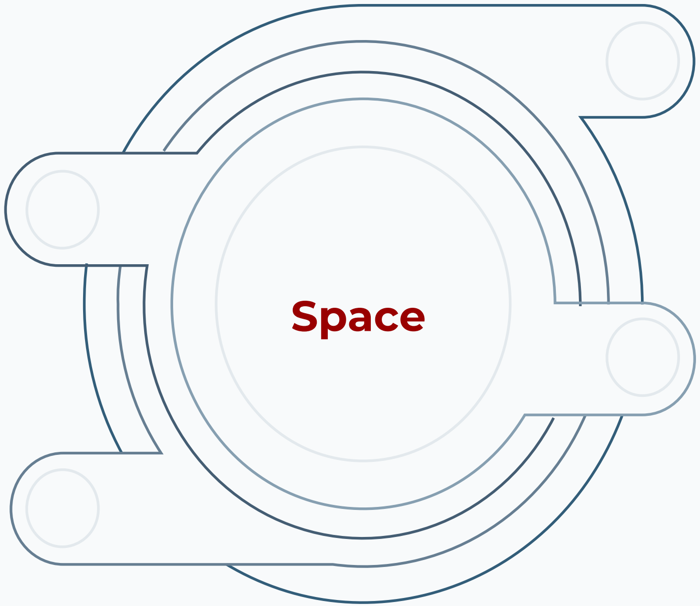
Defensive

- **Secure QKD** – A secure method for encryption key exchange.
- **PQC** – Can counter the risk of future decryption by quantum computer.
- **QCA** – Preparing existing infrastructure for quantum crypto-agility.
- **QRA** – Developing quantum-resilient algorithms.

Space Warfare

Quantum-Enhanced Satellite Detection

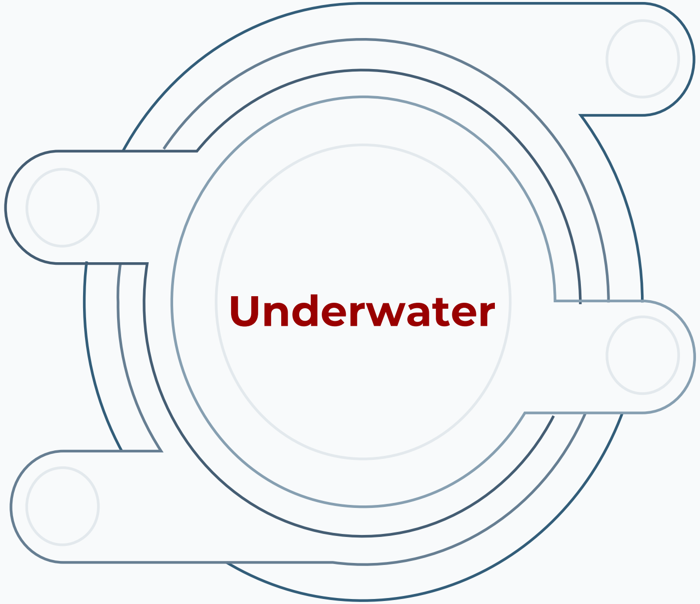
Satellite-Based Quantum Communication



Anti-Satellite Warfare and Space Weaponization

Quantum Ghost Imaging for Surveillance

Underwater Warfare



Quantum Inertial Navigation and Magnetic Detection

Underwater Mapping with Quantum Magnetometers and Gravimeters

Anti-Submarine Warfare Capabilities

Quantum-Enhanced Sonar

Other Warfare Capabilities

Quantum PNT

Terrestrial and Underground Surveillance

Other Electronic Warfare

Quantum ISTAR

04

Progress

Global Players

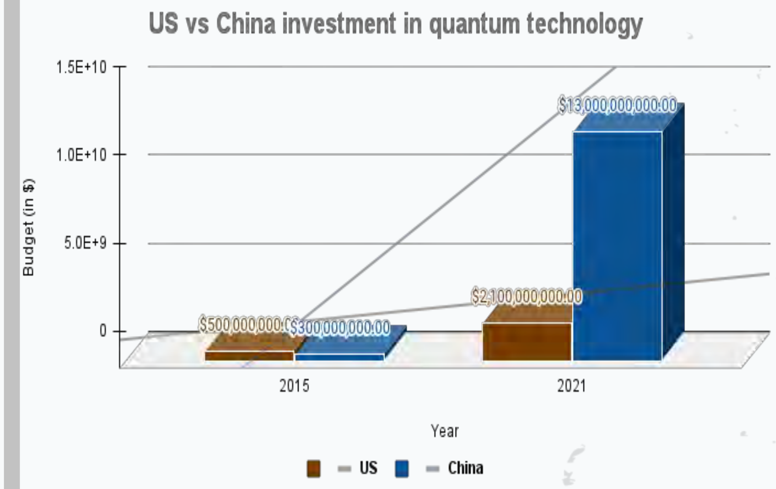
US and China : Frontrunners

US

- Three pillars model.
- Active research on quantum teleportation.
- Alliances with NATO, AUKUS.
- Led in quantum computing.

China

- PLA, defense companies.
- Demonstrated satellite-based QKD.
- Collaborating with Russia and other institutes.
- Ahead in quantum communication.



Global Quantum Warfare Market

2022 ~ USD 134.66 million

2031 ~ USD 540.91 million

CAGR : 16.8%

05

Challenges

Challenges

01

Technical

- Practical Implementation
- Integration
- Testing and Validation
- Data Handling

02

Policy-Making

- Ethical Boundaries
- Legal Consequences
- Global Security

03

Standardization

- Interoperability
- Verification Protocols
- Unification

Challenges

04

Manpower

- Training
- Dedicated curriculum
- Interdisciplinary expertise

05

Economical

- Financial Impact
- Sustainable development
- Resource Allocation

06

Conclusion

Conclusion

- Transformative shift in military capabilities.
- Currently, many quantum technologies are still in the experimental or developmental stages.
- Some areas have shown excellence, some others are promising, while some may raise doubts.
- The next few decades will be critical !!

References

- *Quantum Warfare: Definitions, Overview and Challenges:* https://indianstrategicknowledgeonline.com/web/2103.12548.pdf

- *The US and China are in a quantum arms race that will transform warfare:* https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/

- *The Weaponization of Quantum Mechanics: Quantum Technology in Future Warfare:* https://apps.dtic.mil/sti/pdfs/AD1083173.pdf

- *Quantum Warfare Market:* https://www.insightaceanalytic.com/report/quantum-warfare-market/2053

Thank You!

Komal Pandya

Research Scholar,
Department of Computer Science and Engineering,
Indian Institute of Technology Patna, India

komalsp98@gmail.com

https://www.linkedin.com/in/komal-pandya/