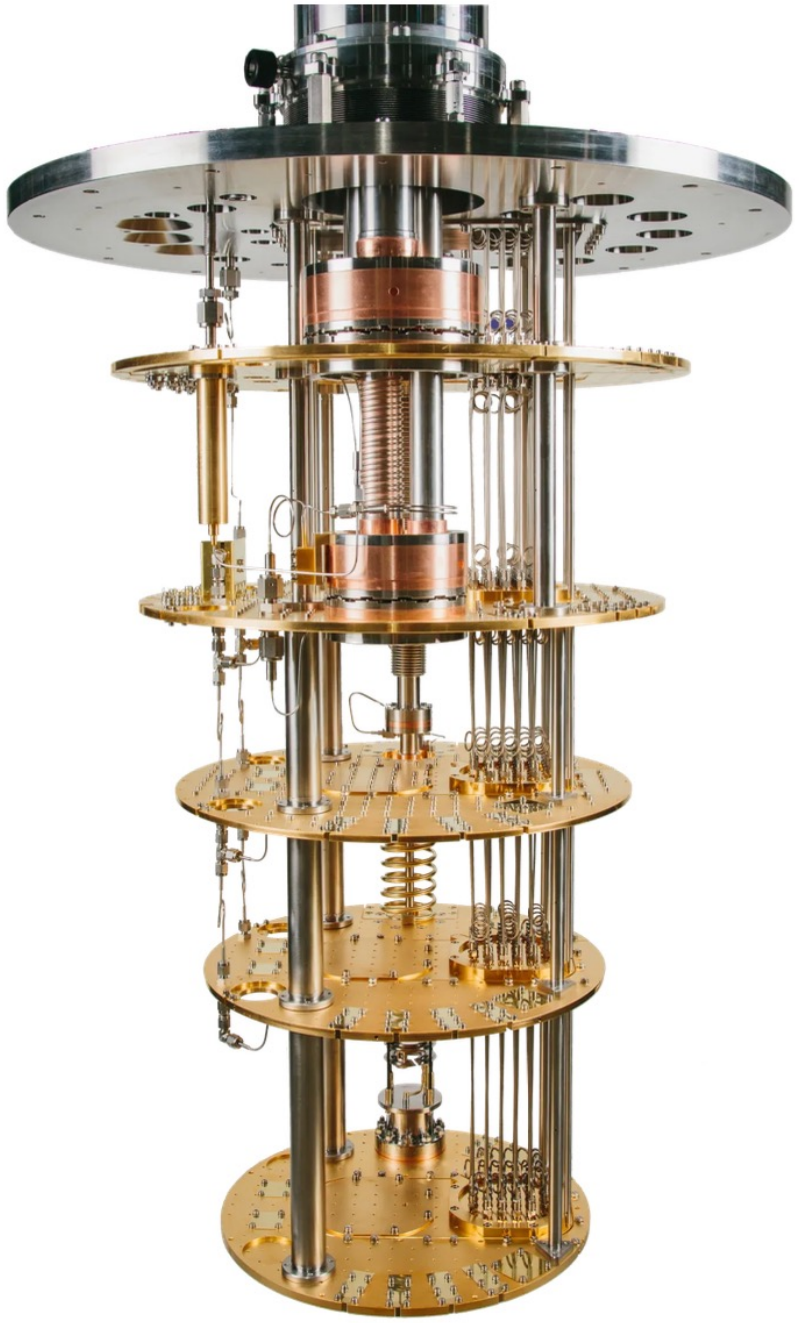
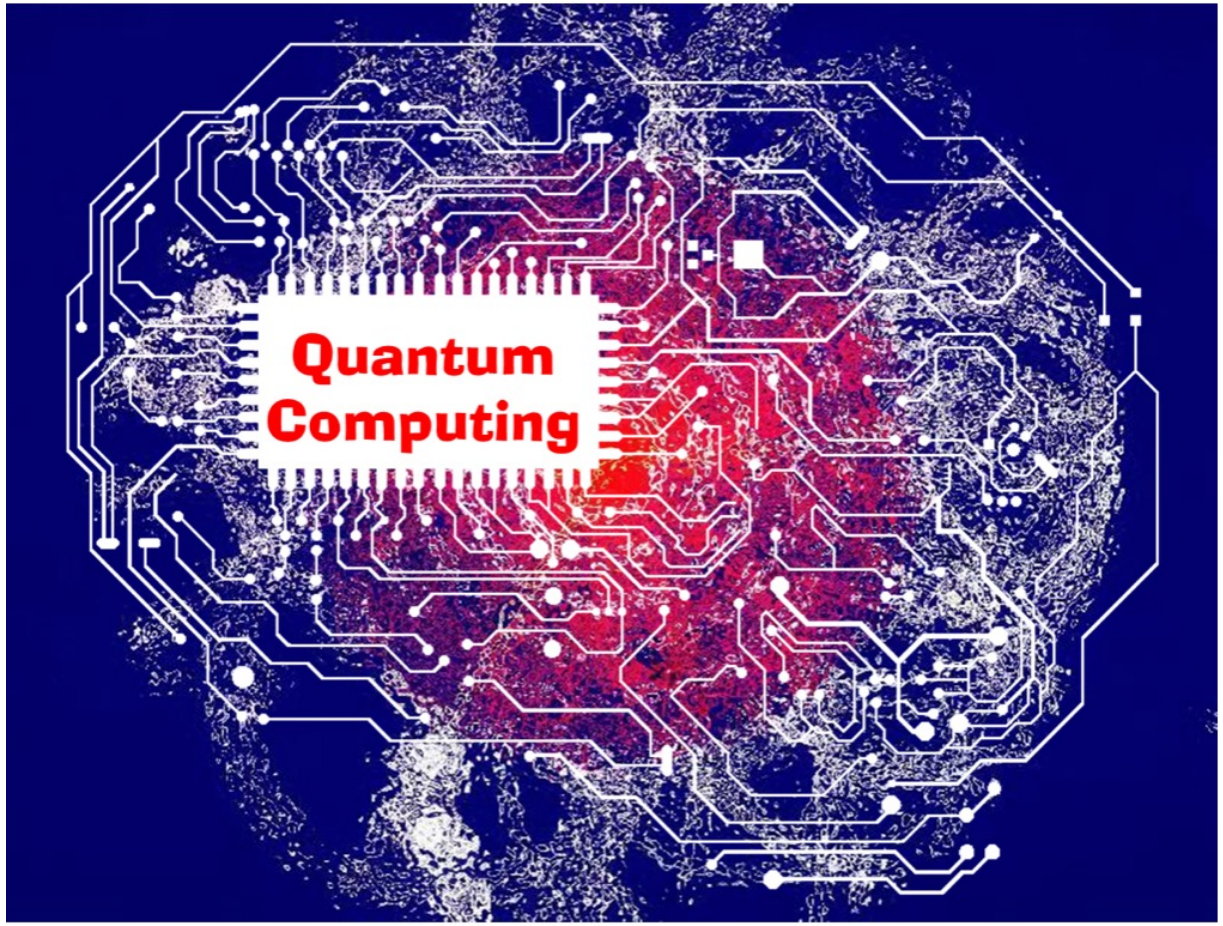


Potential Implications of Quantum Computing to ecryption

Jennifer Arnold
Counterterrorism and Public Policy Fellow at Duke's Sanford School of Public Policy

Agenda

- Title
- Quantum race
- Global investment
- Why is this important
- Classical versus quantum computer
- Thesis
- Methodology
- Issues/concerns
- Findings
- Recommendations
- Other areas to explore
- Conclusion

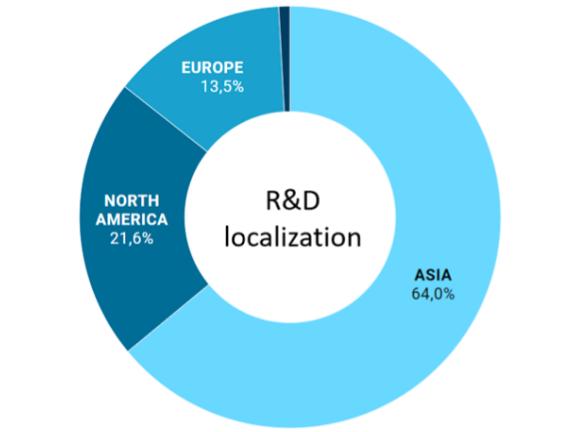


Quantum Race

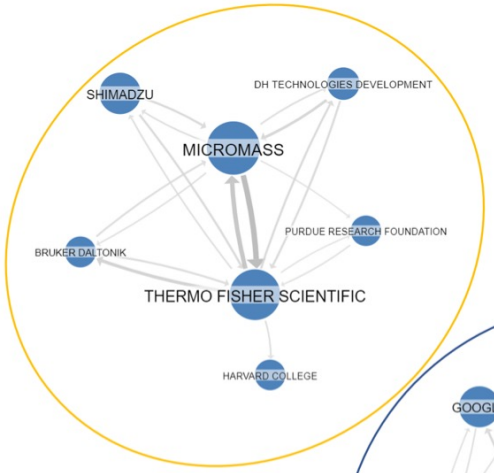
China recently announced a 5-year plan of innovation and technology to parallel the US and aims to focus its development on massive enterprises such as artificial intelligence and quantum computing.

Global Investment in Quantum

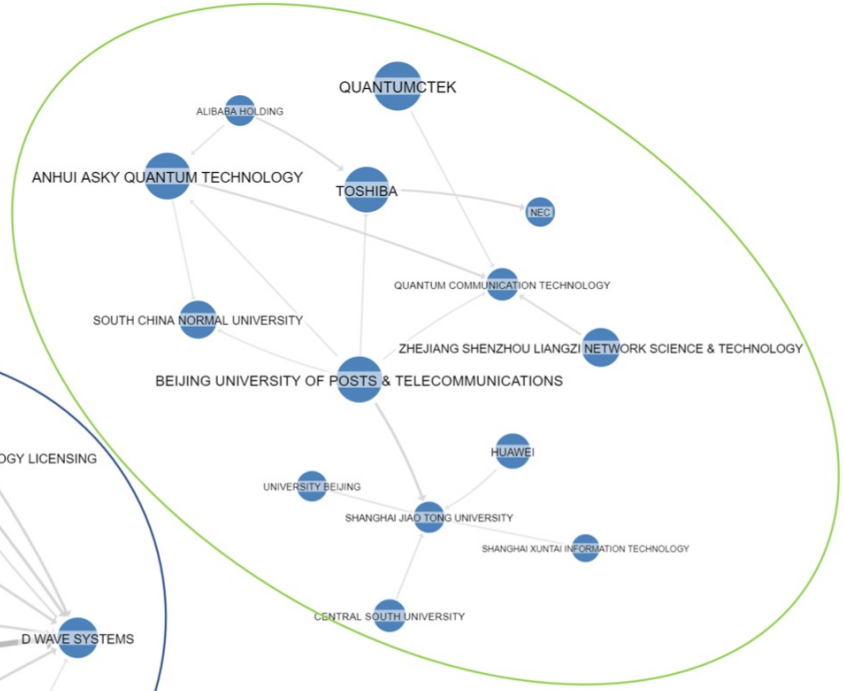
- ✓ 9,905 Patents
- ✓ 50 Inventors (R&D) countries
- ✓ 31 Priority countries



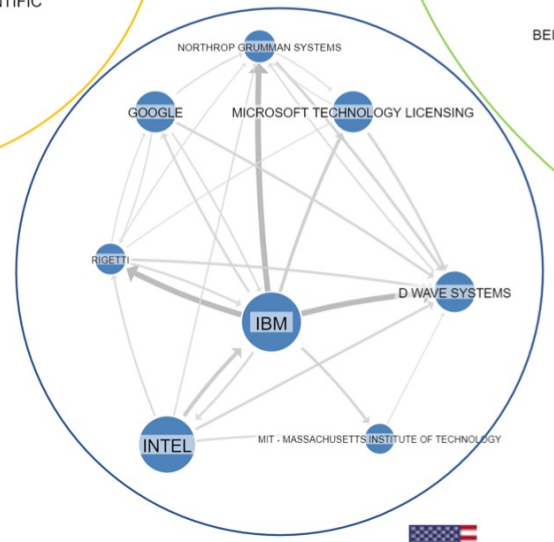
Metrology, Sensing



Patent families by Assignee citations



Quantum Communication China



Computing USA

Why is This Important

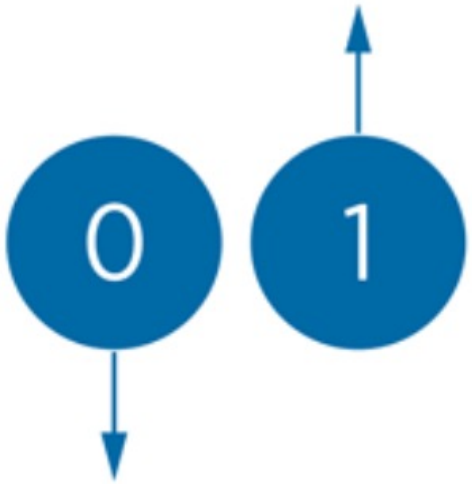
- US could lose its competitive advantage
- Knowledge of military locations and capabilities
- Access to encrypted communications
- Access to sensitive activities planning
- Access to advanced weapons systems
- Access to critical infrastructure
- Internet control

China developed the world's first quantum satellite. Photo: Chinese Academy of Science

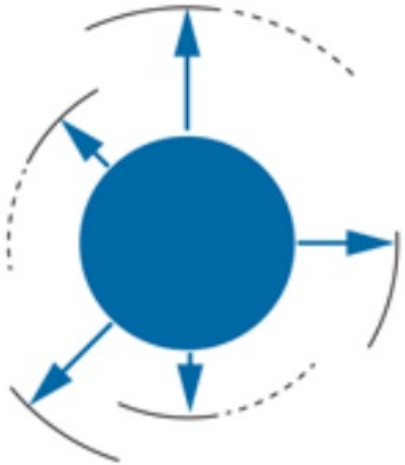
United States could be beholden to a malicious actor

Classical and Quantum Computers

CONVENTIONAL COMPUTERS:
Store and use information as individual bits encoded in one of two states, either 0 or 1.



QUANTUM COMPUTERS:
Encode information in "qubits," which can simultaneously contain an infinite and continuously changing number of states (including negative values). This is called "superposition."



qubit = Increased computational ability

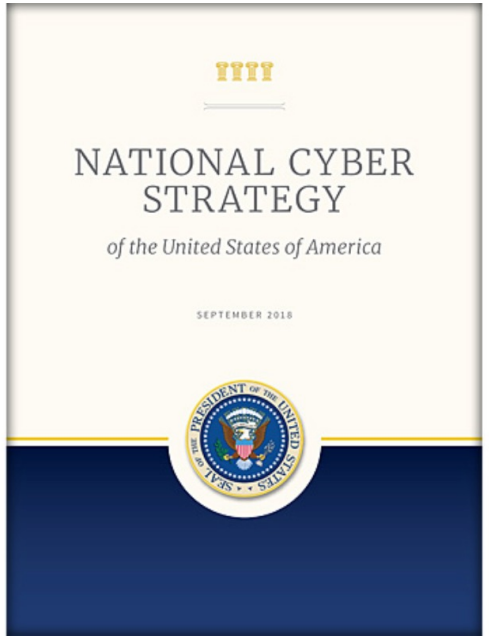
Thesis Statement

While quantum computing is still in the nascent stages, the United States must invest heavily in quantum computing research in order to capitalize on potential strategic opportunities and take steps to defend its critical infrastructure.

Quantum computers' ability to crack encrypted data is precisely what makes them so dangerous, if in the wrong hands.

Methodology

- Analysis of 2018 National Cyber Strategy and 2020 Cyberspace Solarium Commission
- Literature Review
- Interviews UK/US Experts from public and private sector
  - National Security Agency (NSA), former National Institute of Standards and Technology (NIST) employee, cybersecurity experts, venture capitalist, Solarium contributor, cryptology researcher, former policy advisor for the office of Science and Technology Policy (OSTP)



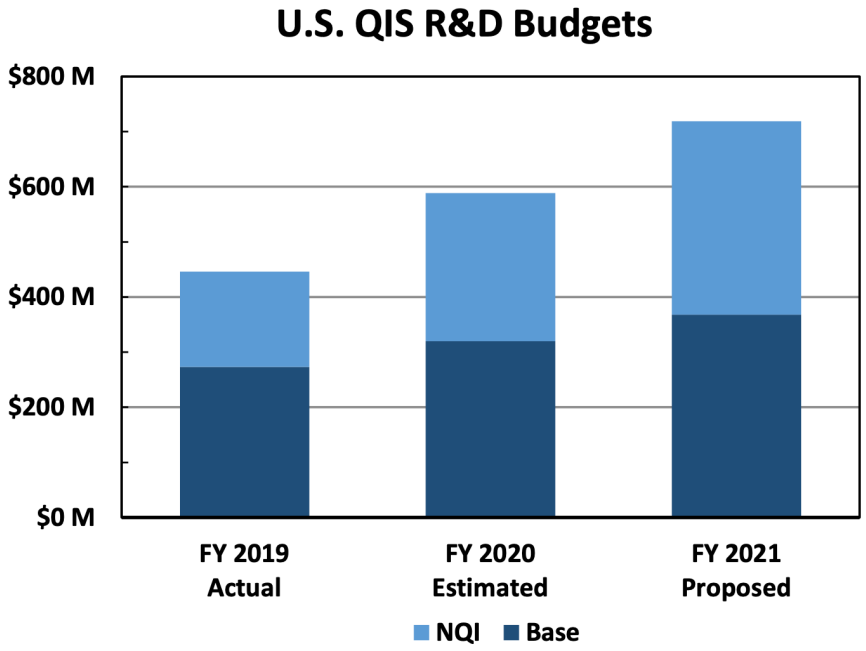
Issues/Concerns

- Shor's Algorithm could crack public Key encryption with a quantum computer
- QC infrastructure is a challenge
- Waiting for a encryption solution that is QC resistant
- Need public policy prioritization

IBM computer with sheathing

Findings

- China is our major competitor - stated purpose of establishing “quantum supremacy” 10 Billion in investment
- US proposed investment 600 Million
- Lack of understanding of the problem set
- Implementation of new cryptology solution is a big challenge
- Private Sector key players: Google, IBM, Amazon
- Public Sector key players: NSA, NIST, DoE, NSF, DoC, DHS/CISA



Good News

- The National Quantum Initiative Act (NQI) 2018
- National Institute of Standards and Technology (NIST) managing a post-quantum cryptography standardization project.
- NSA responsible for national security systems and is actively working with NIST to find an adoptable solution

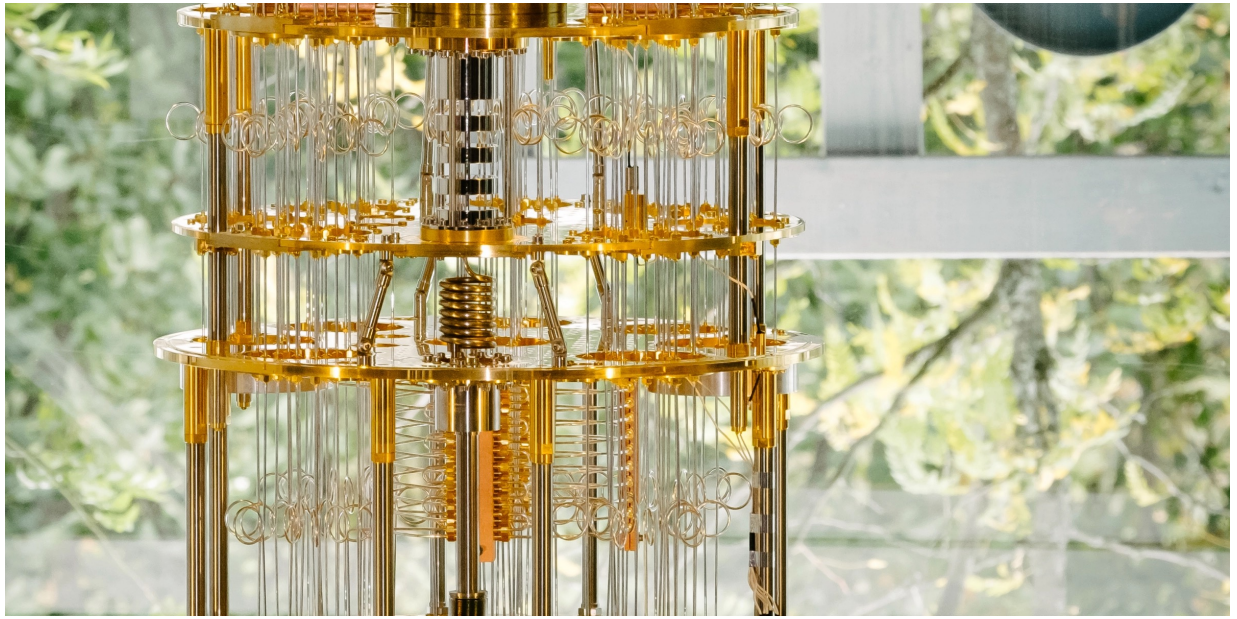
Recommendations

- Need a baseline level of understanding
- Inventory of current critical networks
- Prioritize critical infrastructure upgrades
- Development an implementation plan
- Education funding and incentives-need skilled workers
- Increased research and development investment
- Key Partnerships: Allied partners/private sector

"It is critical to begin planning for the replacement of hardware, software and services that use public-key algorithms now, so that the information is protected from future attacks," NIST urges.

Areas to Further Explore

- Post Quantum encryption: The US government needs to maintain the competitive advantage and develop ways to crack quantum encryption.
- Artificial Intelligence meets QC: What sort of policies can we put in place to ensure moral and ethical lines are not crossed.



Conclusion

- The risk of inaction is too great
- US is headed in the right direction
- US must increase its investment in research and development
- Must development an implementation plan to upgrade encrypted communications systems
- Must increase partnerships with private sector and our allies
- Need to invest in education to develop and keep skilled workers