CYBERSECURITY RISKS AND OPPORTUNITIES IN THE QUANTUM COMPUTING AGE: A STUDY

VANCE, A. S.

Department of Quantum Computing, Capitol Technology University, Washington DC, United States of America.
e-mail: asvance[at]captechu.edu

(Received 23rd April 2024; revised 15th July 2024; accepted 25th July 2024)

Abstract. The 21st century is confronting profound transformations driven by emerging technologies, notably quantum computing, which promises opportunities and risks. As industries and governments invest heavily in quantum capabilities, the looming threat of quantum computers compromising current encryption schemes has prompted the exploration of postquantum systems. This research surveys quantum technologies and reviews existing and proposed quantum policies, particularly cybersecurity, to address critical policy challenges encompassing full-spectrum quantum computing development. Our retrospective literature review and prospective analysis reveal that the research and innovation trajectory involving quantum computing technologies will mature within the next decade. With geopolitical actors gaining access to cloud-based quantum computers, more stakeholders will engage with these nascent technologies, presenting new opportunities and risks. We argue that misaligned proposals, not sufficiently aligned with strategic policy, could hinder the adoption of emerging technologies and undermine national security. This thesis analyzes and addresses these issues and provides recommendations to enhance quantum computing security analysis and reshape geopolitical policies to effectively counter the imminent threats to national security.
Keywords: *cybersecurity, quantum computing, quantum standards and policy, warfare*

Introduction

Quantum computing is an emerging technology being researched and developed by scientists, researchers, entrepreneurs, and nation-states seeking commercialization and operationalization of its capacity-amplifying capabilities (Khan and La Torre, 2021). Theoretically, quantum computing could revolutionize data processing, enabling artificial intelligence and blockchain to operate exponentially faster than classical computing. Speculatively, this increase in data processing could bolster cybersecurity, as quantum computing has the potential to generate true randomness, enhancing cryptography (Jacak et al., 2021). Emerging technologies, pivotal in the transformative changes of the Fourth Industrial Revolution, are anticipated to impact current and post-quantum cybersecurity, both positively and negatively. Despite its potential, the opportunities and consequences of quantum computing are still not fully understood. This research aims to synthesize findings from prior research, which delineated its focus into three phases. Through retrospective analysis, we identify gaps in research focus and propose standards and frameworks to strengthen the connection between scientific inquiry and policymaking. The synthesis of these topics highlights critical themes linking nation-state conflicts and cyberwarfare concerns, underscoring the need for a more comprehensive approach to quantum computing and cyberwarfare/cybersecurity. The first phase analyzed the current consensus of quantum research, which began with an industry and scientific focus (analogous to the "race to the moon" problem). The second phase evaluated and emphasized more the identified gaps in research, which evolved towards a nation-state cybersecurity focus (analogous to the "nuclear arms race" problem). The third phase evaluated the gaps more thoroughly and considered

solutions and further research, which became more cyberwar. Further research is warranted to address the evolving geopolitical landscape and its implications for cybersecurity policy development in the quantum computing age.

Problem statement

An arms race among nations and industries to advance quantum computing, particularly among the United States, European Union, and China, has raised significant national security concerns. A significant risk factor of cyberwarfare is technological evolution. Quantum computing is a particular emerging technology that is predicted to disrupt the balance of nation-state power. In the 1960s, the National Security Agency (NSA) developed the Verona project to harvest encrypted communication to be deciphered when technological capabilities allowed (Vance, 2023). Quantum computing research has reignited this effort. Since 2014, the NSA has been refocused on quantum computers to defeat encryption. Since 2018, the Central Intelligence Agency (CIA) had 137 projects involving other emerging technologies, such as artificial intelligence, to increase intelligence community capabilities (Harvard Science Review, 2020). Despite acknowledging the need for more research to understand the cybersecurity implications of quantum computing, there is a significant disconnect between quantum computing research and accompanying cybersecurity solutions (Wallden and Kashefi, 2019). While it may be unlikely for hacktivists and cybercriminals to access quantum computers in the foreseeable future, nation-states currently have access. "Harvesting attacks," where nation-state-funded hackers steal encrypted data for decryption once quantum computers are available, are already occurring. The nexus of quantum cybersecurity and quantum-enabled cyberwarfare is disturbingly predictable. Research results implicate that the nation winning the quantum arms race will be able to secure its secrets with higher security levels than other nations while potentially gaining unrestricted access to other nations' secrets. Quantum computing cybersecurity research is limited, primarily focusing on cryptography, with insufficient emphasis on broader opportunities and risks. While quantum computing has the potential to advance cybersecurity capabilities, such research is not as prevalent as classical computing cybersecurity research.

Materials and Methods

Our research is intentionally inclusive of our previous research, which qualitatively and quantitatively examined data generated from a retrospective review of published research, policy, and standards from authoritative resources. Our scope was constrained to multi-disciplinary legislation analysis from authoritative sources; Global Cyberlaw Tracker from United Nations Conference on Trade and Development Cybercrime Legislation World-wide; Asian School of Cyber Law Global Cyber Law Database; NYU Cybersecurity Center International Law Repository, U.S. Federal Archives, IEEE Xplore, Science Direct, Google Scholar, Scopus, Academia, ResearchGate, and resources.data.gov. These were analyzed to develop the main principles for a global policy framework in cyberspace. Governance and regulations not reviewed that do not directly address the national security of the 16 Homeland Security-identified critical infrastructures. Examples of policies not reviewed are the Federal Privacy Act of 1974 (FPA), Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), EU-US Privacy Shield. This research is not an exhaustive list

of all quantum research nor an introduction to the field. This research does not review the conceptions or misconceptions of quantum computing's computational power, particularly compared to classical computing. We focused on identifying influential impacts from nation-states and multinational collaborative bodies and providing solutions to address legislative and policy gaps. This involved understanding the current focus of quantum research, the breadth of research and solutions involving cybersecurity, broader emerging technology implications, identifying policy gaps, and a lack of emphasis on enabling wider adoption of related emerging technologies. The culmination of this work is an analysis of the impact on national security and the resulting recommendations for solving the problem.

Results and Discussion

Among the current practical challenges is protracted controversy involving what scientists and engineers consider a "real" quantum computer. Gartner Research Group contends that 'quantum computing is heavily hyped' (Smith III, 2020). Contributing to the hype are industry announcements for increasing qubit computation by stabilizing quantum computing qubits (Seffers, 2024). A qubit loses its superposition and destabilizes to either 0 or 1 once a qubit measurement is performed. The instability of qubits is due to decoherence (the phenomenon that qubits lose their state when observed due to interference from the 'outside'), which is a problem many researchers are trying to overcome. However, recent research reveals qubit stabilization is being achieved ahead of predictions (Bakker and Budde, 2012) and that it is no longer a question of whether quantum computing is "hype" but simply 'when' quantum computers will be fully operationalized. The global quantum technology market is projected to reach $42.4 billion by 2027 (You et al., 2024). In 2020, the White House stated that it intends to double funding towards overall quantum research to $1.2 billion by 2022 (*Figure 1*).

Figure 1. *Quantum spending.*

Despite the hype and challenges surrounding quantum computing, cybersecurity researchers predict that it will shape nation-states' physical and cyberwar doctrines. The United States has a program for intercepting and storing encrypted information for later cryptanalysis called the Venona Project, where a quantum computer can break classical

encryption schemes in the future, which researchers call “harvest and decrypt”. While there are aspects of cybersecurity incorporated across multiple quantum computing funding areas, research lacks a cybersecurity focus. Quantum computing security research emphasis has accounted for only 1% of total research up until 2018, when it began increasing to 4% (*Figure 2*). Within the 4%, 96% of security research focused on cryptography and key distribution (*Figure 3*).

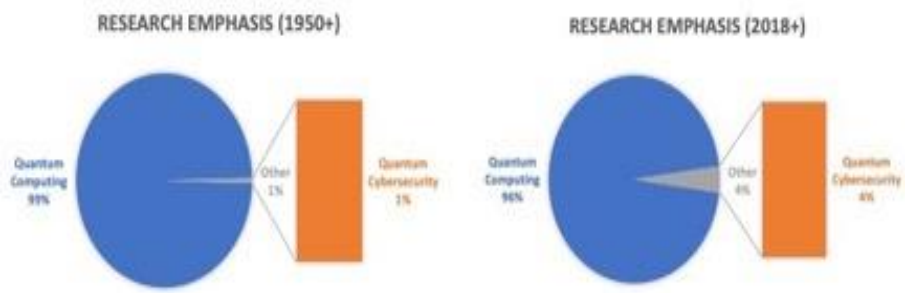

Figure 2. *Research emphasis.*

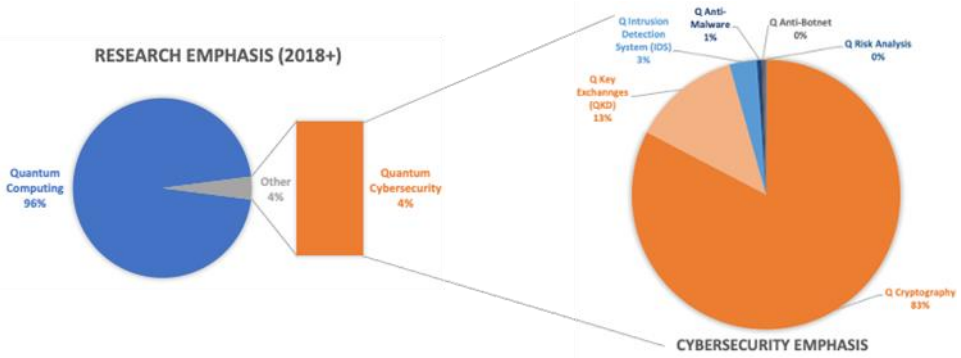

Figure 3. *Cybersecurity emphasis.*

Quantum computing could also be exploited to crack encryption and passwords much faster than classical computing. Advancing practical security solutions involving emerging technologies like virtual reality, blockchain, and artificial intelligence is imperative, necessitating additional academic attention and innovative approaches. Quantum computing risks to encryption are not the only concern. Chinese research scientists claim to have developed a quantum-based radar capable of detecting “invisible” targets 100km away (Report Linker, 2022). This technology would make stealth submarines completely obsolete or expose clandestine aircraft, making the F-35 strike fighter and B-2 bomber ineffective. There are risks to long-term intelligence and national security. Risks about misuse or unintended implications reflected in government policies correlate to a need for expanded quantum security policy and programs. Quantum computing’s prospective power could facilitate the broader adoption of emerging technologies like blockchain and artificial intelligence, enhancing cybersecurity capabilities through unbreakable key generation and quantum key distribution (Moret-Bonillo, 2015). Quantum computing’s impact on existing quantum computing security compared to classical computing security.

Establishing a national quantum research task force and a National Quantum Research Cloud could accelerate research and innovation in quantum computing, allowing for greater emphasis on quantum computing cybersecurity in national security

policies. A consensus among research information and reliable media sources suggests that quantum computing's computational advantage holds promise in solving complex and computationally intractable problems across various domains, including data science, energy, finance, industrial development, secure communications, and quantum security. Emerging technologies may also enhance the cyberwarfare capabilities of nation-states. Weaponized quantum computing may begin supplanting nuclear and high-end conventional weapons, where a quantum-based nation-state disrupts the balance of power (Garisto, 2021). A cyber-attack on national command, control, and communication systems, whether by a state or a nonstate actor, could be perceived as an attempt to disable that nation's nuclear capability and prompt a nuclear first-strike response.

The dominant perception posits that quantum computing is universally superior to classical computing across all domains. However, empirical investigations suggest that quantum computers are anticipated to demonstrate superiority primarily in delineated realms, notably optimization. Consequently, it is pertinent to reconceptualize quantum computing as a technological innovation optimized for executing highly precise, specialized functions rather than serving as wholesale substitutes for classical computational frameworks. Despite initial anecdotal research indicating that when quantum computing reaches quantum supremacy, classical computing will be obsolete, the trajectory (*Figure 4*) of applied quantum solutions indicates a synergistic coexistence of both within computing architectures as part of a classical-quantum hybrid system (Rajan and Visser, 2019). While quantum computing may indeed surpass classical counterparts in select functional areas, classical computing infrastructure is poised to persist as robust and indispensable. The synergistic coexistence of quantum computing means that it will serve as an accelerator and enabler of future capabilities across various domains. Its impact may will reshape perceptions of risk and deterrence; however, research dissemination remains fragmented across disciplinary silos.

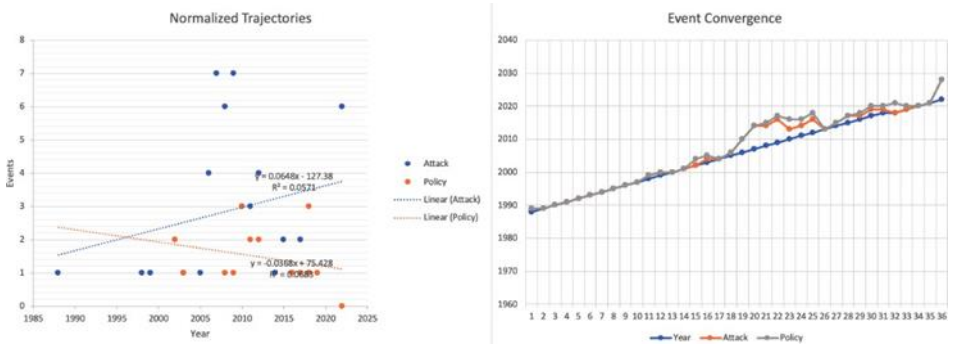

Figure 4. *Research trajectories.*

Our initial research results revealed the fundamental aspects of quantum computing and its potential applications in solving complex problems. Quantum supremacy, where quantum computers outperform classical ones, presents both opportunities and challenges, particularly in national security and related emerging technologies like AI and blockchain (Schwab, 2016). Extended research revealed the geopolitical implications of quantum computing, framing it as a critical factor in the Fourth Industrial Revolution. Consistent with historical precedent, numerous technologies initially developed for civilian purposes exhibit distinct potential for military application (Rao, 2024). These technologies encompass diverse domains such as artificial

intelligence, autonomous systems, biotechnology, and quantum computing (Lonergan and Montgomery, 2024). Therefore, within the sphere of conflict, technology maintains a critical role, with emerging innovations poised to reshape the landscape of warfare and the outcomes of engagements. The arms race among nations and corporations to develop quantum computers intensifies international tensions, with quantum technologies poised to redefine global power dynamics. Expanded and culminating research revealed the transformative potential of quantum computing in enabling wider adoption of emerging technologies. Quantum-enabled cyberwarfare represents a significant evolution in warfare, necessitating new strategies, tactics, and policies to address global security threats and ethical considerations. As quantum computing advances, its intersection with AI holds immense promise and poses significant national security challenges, necessitating robust research and policy frameworks to mitigate risks and maximize benefits. Quantum computing advances will drive progress in quantum research and benefit emerging technologies like AI, blockchain, and IoT, enhancing critical infrastructure. Geopolitical cyber decision-making often reacts to cyber-attack events, but there is a need for proactive global guidelines to manage the opportunities and risks of quantum computing. The U.S. views quantum computing and AI as transformative technologies impacting national security, driving research funding alignment, and raising significant security concerns globally.

There is currently no framework to manage weaponized quantum computing escalations. Emerging technologies may also enhance the cyberwarfare capabilities of nation-states. Weaponized quantum computing may begin supplanting nuclear and high-end conventional weapons, where a quantum-based nation-state disrupts the balance of power. A cyber-attack on national command, control, and communication systems, whether by a state or a non-state actor, could be perceived as an attempt to disable that nation's nuclear capability and prompt a nuclear first-strike response. The nuclear decision-making model could provide a basis for an asymmetric Emerging and Disruptive Technologies (EDT) response (*Figure 5*). Nationally and Internationally, there is a lack of uniform standards. Existing instruments for innovation integration and interoperability should be used to ensure wider adoption of collateral emerging technologies. Industry and academia should co-develop quantum-enabled or quantum-capable innovations. Public-private partnerships could encourage and facilitate consensus, monitor frameworks and standards evolution, and curate them through peer-reviewed conferences, journal issues, and public policy advisement. NIST and IEEE should serve as the nexus to support standards and policy activities. While cyber regulation and legislation grow, cyber policy is still reactive. The United States has led efforts to establish cyberwar norms but failed to achieve international consensus. Since 2011 and again in 2020, the United States has asserted that any state-sponsored cyber-attack can be constituted as an act of war that could escalate to a cyber or physical response (Molini, 2023). Since 2013, NATO has affirmed this position. No international treaty consistently defines cyber warfare norms at the United Nations level or otherwise.

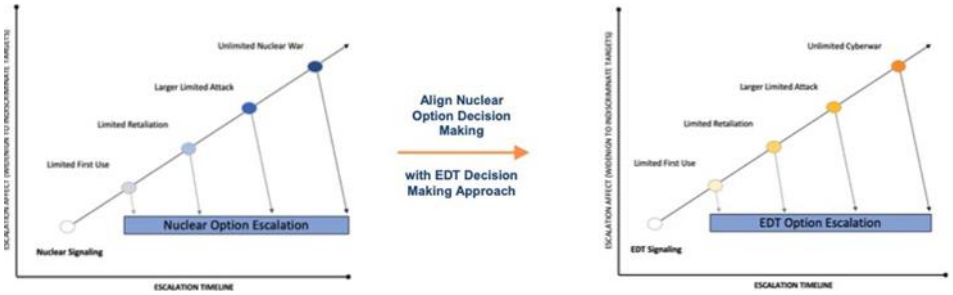

Figure 5. *Emerging and disruptive technologies.*

Domestically, there is no quantum research task force like the one established in the National AI Research Resource Task Force Act of 2020. The National Quantum Initiative is the closest model to the AI task force. Formulating a National Quantum Computing Research Resource Task Force Act that provides a quantum computing research cloud will expand research on threats and drive innovation in solutions and policy. If a Quantum Task Force Act is unviable, an alternative is to amend the National Quantum Initiative Act. Internationally, there is no weaponized quantum policy. Research indicates a viable approach would be to Amend the Council of Europe's Budapest Convention Treaty 185. While some Asian states are participants, China is not a signatory. Treaty 185 has limited Asian nation-state participants; currently, just Japan and the Philippines. Collaborating with China through existing international instruments attempting to establish cybersecurity norms would leverage the existing dialogue and trust to accelerate the adoption of new norms involving emerging technologies. Utilizing an existing treaty with 66 signatories would ensure more globally acceptable norms and enforcement. There is a need to collaborate with United Nations government experts and Asian nations.

Conclusion

Emerging technologies, particularly in quantum computing, are increasingly intertwined with defense considerations, posing regulatory challenges. Quantum cyber warfare is becoming a reality, and achieving quantum supremacy is imminent. There's a pressing need to address the impact of quantum computing on cybersecurity and develop comprehensive policies to safeguard national interests. Despite advances in quantum-proof encryption, there are alarming quantum cybersecurity gaps in research and policy for quantum-enhanced cyber solutions, highlighting the need for more comprehensive approaches to cybersecurity. Historical cyberattacks like the 2007 assault on Estonia underscore the potential devastation of cyber warfare. Quantum computing could exacerbate such attacks, demanding proactive policy development to mitigate risks to national security. Quantum-resistant technologies could defend developed nations, but global cooperation is needed to address cyber threats, particularly in the emerging field of quantum warfare. While cryptography research is substantial, there's a lack of emphasis on broader quantum-enhanced cybersecurity solutions and policies, with most efforts centered on encryption. Quantum-enabled security has the potential to ensure accuracy, reliability, and privacy in emerging technologies. Quantum computing can serve as a force multiplier for existing technologies, offering unprecedented advancements and capabilities.

Collaboration across public and private sectors will be required to identify nation-state-sensitive aspects of developed technology. Congress should create a National Quantum Research Task Force comprising academia, government, and industry to develop a roadmap for establishing a national quantum computing cloud, providing affordable access to quantum resources and expertise. Then, the export of critical computing knowledge should be controlled to prevent the weaponization of quantum computing, aligning with existing classification and export control mechanisms while promoting economic opportunities and national security interests. Ultimately, ubiquitous international cooperation through existing treaties like the Budapest Convention on Cybercrime can serve as effective instruments to advance consensus and cooperation on quantum computing-related cybersecurity, fostering collective identification of strengths, gaps, and opportunities

Future research should focus on assessing the risk quantum computers pose to classical computers with post-quantum defenses and rapidly developing defense systems against cyber and quantum weapons. Further exploration of international norms and increasing education in quantum computing workforce skills are essential for effective policy creation and technology development. Access to quantum resources and education must be made accessible to all researchers, spanning students, industry, and diverse socio-economic communities, to ensure cohesive policy alignment and effectiveness. These recommendations aim to address the challenges posed by quantum computing's rapid advancement, ensuring that national security interests are protected while fostering innovation and collaboration in this transformative field.

Acknowledgement

This research is self-funded.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

[1] Bakker, S., Budde, B. (2012): Technological hype and disappointment: lessons from the hydrogen and fuel cell case. – Technology Analysis & Strategic Management 24(6): 549-563.
[2] Garisto, D. (2021): China is pulling ahead in global quantum race, New studies suggest. – Scientific American 9p.
[3] Harvard Science Review (2020): The race to quantum supremacy. – Harvard Science Review Web Portal 13p.
[4] Jacak, M.M., Jóźwiak, P., Niemczuk, J., Jacak, J.E. (2021): Quantum generators of random numbers. – Scientific Reports 11(1): 21p.
[5] Khan, F.S., La Torre, D. (2021): Quantum information technology and innovation: A brief history, current state and future perspectives for business and management. – Technology Analysis & Strategic Management 33(11): 1281-1289.
[6] Lonergan, E., Montgomery, M. (2024): United States Cyber Force: A Defense Imperative. – Foundation for Defense Democracies Web Portal 22p.

[7] Molini, G. (2023): The Evolving Cyber-Based Threat: The Need for International Regulations to Avoid 'Accidental' Conflicts. – Center for Arms Control and Non-Proliferation 6p.
[8] Moret-Bonillo, V. (2015): Can artificial intelligence benefit from quantum computing? – Progress in Artificial Intelligence 3: 89-105.
[9] Rajan, D., Visser, M. (2019): Quantum blockchain using entanglement in time. – Quantum Reports 1(1): 3-11.
[10] Rao, R. (2024): Quantum Computers Can Now Run Powerful AI That Works like the Brain: The influential AI design that makes chatbots tick now runs on quantum computers. – Scientific American 8p.
[11] Report Linker (2022): Quantum Computing: Technologies and Global Markets to 2026. – GlobeNewswire Web Portal 5p.
[12] Schwab, K. (2016): The Fourth Industrial Revolution. – Melbourne Law School 172p.
[13] Seffers, G.I. (2024): DARPA Hopes To Help Settle Quantum Computing Wild West. – The CyberEdge Web Portal 10p.
[14] Smith III, F.L. (2020): Quantum technology hype and national security. – Security Dialogue 51(5): 499-516.
[15] Vance, T.R. (2023): Artificial Intelligence in Cybersecurity: A Survey of National Research, Investment and Policy Implementation. – International Journal of Computer Science and Information Technology Research 11(2): 18-25.
[16] Wallden, P., Kashefi, E. (2019): Cyber security in the quantum era. – Communications of the ACM 62(4): 120-120.
[17] You, X., Huang, Z., Alyanak, U., Romanenko, A., Grassellino, A., Zhu, S. (2022): Stabilizing and improving qubit coherence by engineering the noise spectrum of two-level systems. – Physical Review Applied 18(4): 14p.