Analysis of the Necessity of Quantum Computing Capacity Development for National Defense and Homeland Security

Dominic Rosch-Grace
Department of Computer Science
North Dakota State University
Fargo, North Dakota, USA
dominic.rosch@ndsu.edu

Jeremy Straub
Institute for Cyber Security Education and Research
North Dakota State University
Fargo, North Dakota, USA
jeremy.straub@ndsu.edu

***Abstract*—Prior work has discussed the significant benefits of the use of quantum computing systems in an array of different fields. These systems have already demonstrated the potential to expedite processing in key areas, such as factoring large integers, as compared to their classical counterparts. The specific value of quantum factoring has been demonstrated for cryptography. It will render one of the most prevalent encryption techniques, RSA encryption – which is dependent on computational systems being incapable of determining the prime factors of large integers, effectively obsolete. However, defeating encryption is not the only prospective use or value of quantum computing for national defense and homeland security purposes. This paper analyzes the need to invest resources in quantum systems and quantum computing technology development due to the potential threats they pose and the benefits that technological innovation in this area is poised to provide. The benefits of quantum computing in a variety of national defense and homeland security application areas are discussed and the implications of investment – as well as failure to invest – in this technology are considered.**

Keywords—quantum computing, homeland security, cybersecurity, encryption, investment, technology development

I. INTRODUCTION

Quantum computers harness the benefits of quantum mechanics to perform calculations. Phenomena such as quantum superposition and entanglement provide significant benefits beyond classical computing. While classical computers are limited to binary mechanics in processing information, where their operations are based on a single state of either 1 or 0, quantum computers make use of qubits, whose state is probabilistically defined until observed. These differences allow quantum computers to perform a selection of complex calculations simultaneously.

Superposition is the quantum mechanical phenomenon that allows a particle to be, with a certain level of probability, in all possible states concurrently. It is one of the keys to the dramatic speed enhancement, for some tasks [1], provided by quantum computing. However, it is not without cost. Quantum superposition requires the capability to measure and not interfere with, prior to measurement, phenomena such as the spin of an electron or the polarization of a photon. Quantum computing error correction is a considerable area of research within the quantum technology research community, where decoherence of qubits is one of, if not, the biggest obstacle in recognizing large-scale quantum computer usage.

Making use of these capabilities, in 1994 mathematician Peter Shor derived an algorithm for factoring large prime numbers, given an ideal quantum computer with enough qubits [2]. This capability threatens many modern implementations of public key encryption by facilitating private key determination in a much more rapid manner than was previously possible. It is also a key demonstration of the benefit and threat posed by quantum computing. Using this and other algorithms, a future quantum computer could break different encryption methodologies allowing any third-party with such quantum hardware to seize control over computational assets and sensitive data stored on a network. This represents a significant national security benefit to those nations which possess the capability and a demonstrable threat to those who do not. It is a clear indication as to why research in quantum computing is needed for national security.

However, this is not the only prospective security benefit that quantum computing is poised to provide. Recent work in quantum computing technology has been focused on the development of large-scale, sustainable quantum computing hardware and services for a multitude of different areas of interest. This capability is projected to facilitate improvements in areas with computational tasks that enjoy a quantum advantage (i.e., the problems that, if given to a quantum computer, can be processed more efficiently than classical computers).

Quantum computing research has shifted from speculation to application over the past two decades. In the future, it is expected that many applications will combine both quantum and traditional hardware to maximize efficiency. Future quantum computing is also poised to change society. This paper discusses several areas of consideration of quantum computing from a defense and homeland security perspective. It continues with a discussion of the threat posed by foreign adversaries equipped with quantum computing capabilities. Then, the benefits of possessing domestic quantum computing capabilities are discussed. Finally, key areas of quantum computing development are reviewed before concluding.

II. Foreign Adversary Quantum Computing Threat

Zhang, et al.'s [3] study showed that multiple nation states are researching how to develop, apply, and improve upon existing quantum computing hardware. Much like nuclear weapons, quantum computing proliferation seems all but inevitable due to the risks posed [4] by asymmetric capabilities. The risks associated with falling behind an opposing nation state in quantum computing capability development must be considered, as neglecting developments in quantum computing technology may result in a variety of different risk factors, as well as a lack of tools for expediting advancement in various fields of research.

Significant benefit may accrue to nation states who have reliable and robust quantum computing capabilities first. This will be particularly true if their adversaries have not taken actions to prepare for quantum computing threats. For example, polynomial-time integer factorization capabilities being possessed by foreign entities, absent significant preparation, represents a key threat to national security. Integer factorization being difficult and computationally expensive is the basis of common encryption techniques (e.g., RSA encryption [5]). Quantum computers have previously demonstrated the capability to factor large integers significantly faster than their classical counterparts.

With sufficient quantum computing capabilities, currently indecipherable encryption implementations will become readily decryptable [6], [7]. Sensitive data presently protected by traditional cryptography may potentially be accessed by an adversary. Cyber-physical systems whose command capabilities are similarly protected may be compromised and remotely controlled or reconfigured. This generates a variety of potential risks for a nation state in possession of cyber-physical assets built with classical encryption methodologies. Previously, the sheer magnitude of time required for this made it impractical: a conventional computer would take, on average, 300 trillion years to crack a 2,048-bit digital key [8]. However, this is no longer the case with quantum computing, as a quantum computer with 4,099 qubits would need only need, on average, 10 seconds to crack this same key [8]. This represents a threat to numerous key assets such as autonomous aircraft [9], satellites, public and private communications traffic [10], reconnaissance capabilities [11], other warfighting craft and equipment [12], and global positioning system components [13]. Not only would this usage impact the efficacy of these cyber-physical systems, but an adversary may choose to seize control over them to be used against the nation that originally possessed them.

Perhaps most problematically, key infrastructure such as satellites, power plants, water treatment plants and military craft can take years to develop and remain in service for decades. Thus, preparations for an adversary's future quantum capabilities must start years before they possess them, to be effective. Shankland [8] notes another similar area of concern: nations may choose to record network data, store it, and use quantum computation to crack it when this is viable. Any confidential information contained in these communications – including the identification of undercover operatives, key credentials, battle plans, system designs or embarrassing commentary on foreign nations – would then become available for use, analysis and public dissemination by the state possessor.

Given the rapid, albeit uncertain, pace of quantum computing advancement, it is possible that these preparation activities may have needed to have started months or years ago. In the immediate future, it is imperative that technological development considers the potential for technologies to need to operate in a future environment with adversaries (both state actors and others) possessing significant quantum computing assets. Unlike with nuclear weapons, where the impact of damage and retaliation has resulted in a stability born from a fear of mutual assured destruction, there is little reason to believe that quantum computing offensive capabilities will not be deployed [14]. Ideally, a diplomatic approach could be used to prevent adversaries from using quantum computing capability maliciously; however, this may be ineffective.

Longer-term planning should also consider the potential consequences of falling behind adversaries in terms of quantum computing development – both to attempt to ensure that this doesn't eventuate and to develop contingency plans for implementation, should it occur. Remaining conscious of international innovation and activities in quantum computing is essential. Adversaries with asymmetric access to quantum computing systems is an imminent threat and potentially dangerous to the national cyber defense. National realization of quantum computing capability is key to safeguarding a nation's computational infrastructure, as well as any cyber-physical systems dependent on it.

III. Quantum Computing Benefits

The use of quantum computing provides benefit in a number of areas ranging from cybersecurity applications to facilitating activities that promote national scientific progress and, thereby, enhance national security. One of the most identifiable differences between quantum and classical systems is that quantum computers can generate truly random numbers [15]. While classical computers generate pseudorandom values, using mathematically complex algorithms, quantum randomization is key to several future cryptographic techniques [2] as it makes third party identification of keys impractical. Random number generation is also useful for simulation.

This section discusses military and other offensive quantum computing benefits. Then, the use of simulation for providing general societal benefits is discussed. Finally, the benefits of quantum grid computing are discussed.

A. Military, Offensive and Defensive Benefits

Quantum computing capability has the potential to be leveraged as a tool for offensive and defensive endeavors. For example, the encryption-breaking capability projected in future versions of quantum computing systems [6] may be utilized as a powerful tool for accessing sensitive data protected by outdated forms of encryption, enabling a nation state with quantum capability access to this information, as well as any cyber-physical systems secured by similar forms of encryption. Alternatively, quantum cryptography is a prominent area of research [16] that focuses on the development of quantum cryptographic frameworks, considering the key-finding capability of quantum computers and the resultant risk to

modern encryption techniques based on classical computing. These new quantum cryptographic encryption methodologies are meant be computationally expensive for even quantum computers. Proper development and implementation of these quantum encryption techniques has the potential to safeguard information traffic, as well as any cyber-physical assets dependent on encryption techniques being computationally expensive/impractical to break [17].

B. Simulation

Quantum computers can also potentially be used for simulation [18]. Simulation facilitates experimentation under a multitude of scenarios using computational resources instead of real-world ones. It is used in a wide variety of fields to understand the implications of scientific principles or to assess the performance of a design and design optimizations. Applicable areas where quantum computing simulation may contribute to defense and homeland security include atomics, materials science [18], aerospace [19] and vehicle design, and cloud computing system research [20]. Quantum computers are well-suited to solving simulation and optimization problems, due to their random number generation and other capabilities. Quantum computing has also been projected to enhance the performance of some machine learning techniques [21] which could be used for everything from network intrusion detection to facilitating technological advancement in numerous areas.

In the initial use of quantum computers for certain tasks, they were identified as a powerful tool in the understanding of quantum mechanics. As quantum mechanics is the basis for powerful, yet accurate quantum computers, quantum simulation could be utilized to improve quantum computing technology. An example of this would be a quantum computer designing new variants of qubits [22].

The use of quantum computing has also been proposed to enhance nanoscale simulation [23] which can lead to advances in nuclear technologies. As the behaviors of matter at the atomic scale is better understood through quantum computing [24], these principles could potentially be applied to areas such as nuclear weapon innovation and nuclear power.

Research in pharmaceuticals is another prospective area of quantum application [25]. Chemical processes can be accurately simulated to a degree that is currently intractable. This is poised to accelerate research in this field by allowing some types of experimentation to be done on a computer, as opposed to in a laboratory. Computational simulation can decrease the time spent on drug research and remove the potential for errors and other safety considerations that would exist in a laboratory setting.

Quantum computing simulations are also well-suited for research in particle, atomic, and quantum physics [26]. Work in these areas could provide a foundation for the innovation in technologies such as ion thrusters [27] and nuclear fusion [28].

Quantum computing could also be used at nanoscale to analyze the behavior of a virus to better understand both its intrinsic properties and factors regarding transmission [29]. Machine learning could be implemented to understand the geographical transmission of the virus according to multiple factors, such as population density and climate, which would prospectively allow governments and other organizations to plan using this information [30]. Likewise, this could operate in tandem with the drug discovery capabilities of quantum computing simulation, effectively reinforcing how a nation state solves the problem of spontaneous, fast-spreading illnesses.

The improved processing and optimized simulation capabilities provided by quantum computing systems may have the potential to accelerate modern research endeavors, resulting in significant advancements in modern technologies. This will inherently benefit any nation that possesses quantum computing technology. Quantum computing possessing nations will benefit both through general technological and scientific advancement and via homeland security and defense-specific studies and development. Conversely, opposing nation states with better quantum computing capability could also experience this array of technological advancements, highlighting consequential risks to any nation that is not on par. This suggests that each nation should ensure that their quantum technology is equal to, if not, greater than the opposing nations.

C. Quantum Grid Computing

Grid computing, for classical computers, provides efficiencies in data storage and processing power [31]. A quantum grid environment could enable quantum computer users by providing a mechanism to support simulation, machine learning and other types of research. The multi-computer, multi-processor nature of a computing grid, as a virtual collection of devices connected over a network, has the potential to facilitate wide access to quantum computing hardware. It can also manage jobs to ensure that only tasks that will benefit significantly from quantum computing hardware are assigned to it (the rest would be assigned to conventional hardware to maximize the value of the quantum computing system). Scheduling systems in a computational grid environment act as the moderators for assigning tasks to available, suitable processors. A framework for a quantum grid scheduling algorithm would take into consideration whether a task is meant for classical or quantum systems, data marshalling costs, as well as appropriate task preemption when fed a high priority computing task.

As many machine learning techniques are dependent on large sets of data, a grid environment's data management capabilities may be key to enabling quantum machine learning [32]. Quantum computing machine learning algorithms have, in some cases, demonstrated increased efficiency [33] enabling faster discoveries. Quantum computing capabilities will likely also facilitate the development and use of specialized quantum machine learning algorithms that cannot run on classical computers. These information storage and processing capabilities are also well-suited for supporting simulations [34]. Prior work has demonstrated the efficacy of grid computing in materials science [35] and the simulation of air pollution [36]. Feynman suggests that simulation of these types of physical systems is best performed on quantum computers [26]. A quantum grid computing environment would, thus, be well suited to research in these and other related areas.

IV. Capability Development Required

To support the attainment of the benefits described in the previous section, several technical and capability development activities are required. The future of effective cyber defense and the attainment of a multitude of benefits in other areas ranging from materials science to drug discovery is dependent on research development in a number of different areas.

A. Quantum Software Engineering Best Practices

Numerous theoretical quantum algorithms have been derived [37] and some are now being put into practice. Existing quantum algorithms need to be validated and efforts are required to make quantum computing development more accessible to those with classical computer software development skills. Understanding how to most effectively use quantum hardware, from a software design perspective, is also an area of current work [38]. There is, similarly, a need for many foundational developments in quantum computer science and quantum software engineering.

At present, modern software development methodologies based on classical systems are well understood and battle-tested. Thought must be given to how quantum software development is to be managed in the future. Key questions regarding topics such as similarities between existing software development lifecycle frameworks for classical and quantum computing, education regarding quantum computing technology, and providing access to quantum resources to facilitate exposure to the technology must also be addressed.

Increased availability of quantum computing resources for research may contribute to the efficiency of quantum computing development over time, as nationwide exposure to the concepts and resources will facilitate research and experimentation endeavors. An example of this would be a cybersecurity organization having access to quantum computing resources and using them to experiment with new quantum cryptographic algorithms. Similarly, this same principle can be applied to areas of research such as machine learning and autonomous vehicles.

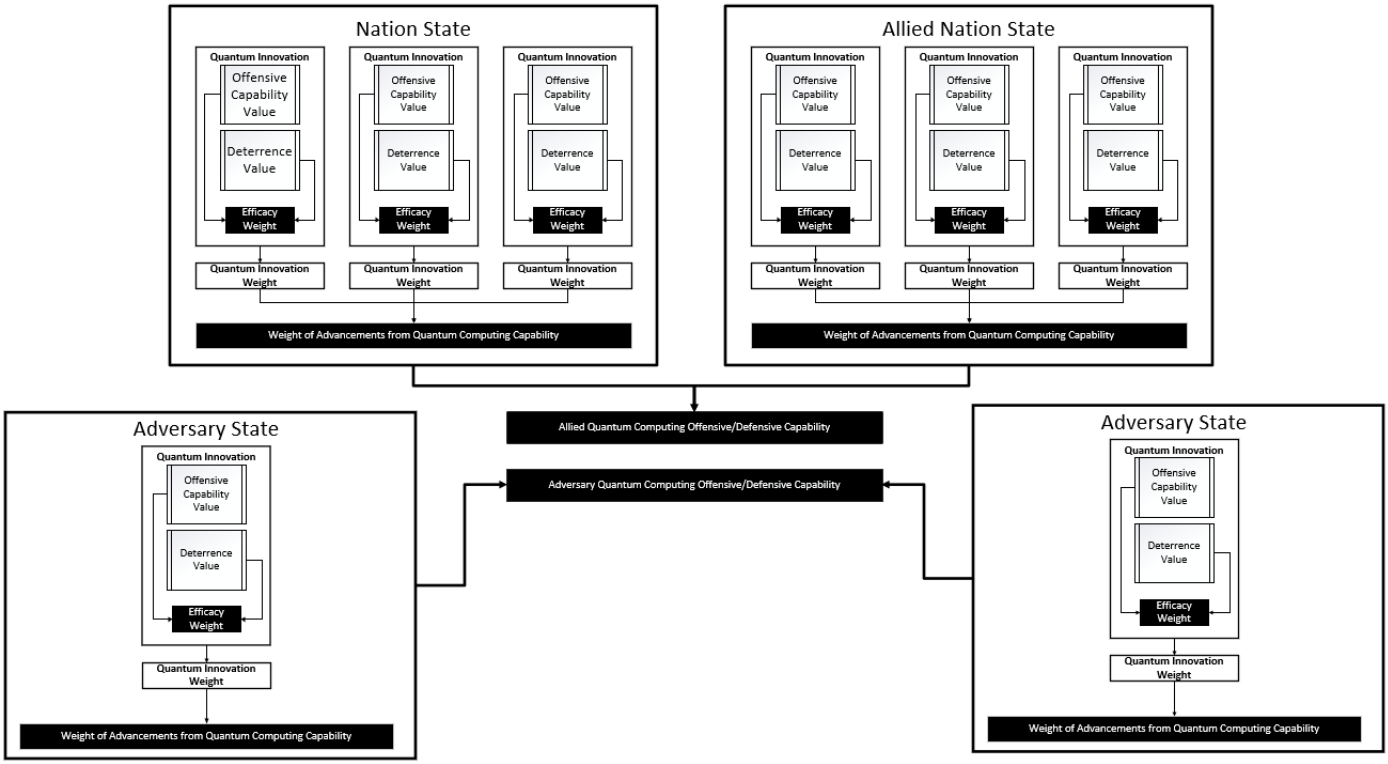


Fig. 1. Comparative impact of state, allies and adversaries possessing quantum computing capabilities.

Much like current classical computers in an academic setting, the availability of quantum computing resources to students is another possible way to generate awareness of quantum computing capability and shepherd prospective computing students towards developing quantum computing applications and implementing new types of quantum cryptography. Students can gain an understanding of the conceptual foundation of cryptography, as well as how quantum cryptographic methods can be implemented in a variety of computing environments. This may ultimately assist in the magnitude of research focus being given to safeguarding a nation's computing assets.

B. Quantum Computing Hardware Development

The quantum computing hardware itself can also be improved upon. Systems with more qubits are required for increased processing capability to support algorithms such as Shor's. Improved algorithms for mitigating the effect of quantum processor noise [39] and hardware developments to

remove it are also needed, as effective suppression or prevention of quantum noise will reduce error rates for computational tasks and may increase throughout. Currently, the decoherence rates of qubits serve as one of the most recognizable obstacles in the realization of quantum computing technology on the national scale [40].

C. Error Correction and Noise

Quantum error correction is a considerable area of research for the large-scale realization of quantum computers, in that certain utilizations by consumers and organizations are dependent on robust, accurate computing resources. Quantum error correction focuses on methodologies for both mitigating and compensating for the error produced by quantum noise in quantum computing calculations. As these improve, more qubits may be added to a single quantum system, allowing the quantum computer to compute more types of problems, as well as maintain stability in calculations over time.

Prior work [41] has demonstrated the utility of using quantum computing noise productively, though, for some applications. The random variation can be used to help facilitate the exploration of a solution space.

D. Improved Operating Conditions Support

Another area of development that could have significant defense and security benefits is work to increase the practicality of quantum hardware. Current hardware requires extreme operating conditions which requires extensive supporting systems (such as cooling) that make small quantum computing facilities impractical. Distributing quantum computing capabilities geographically provides key resiliency benefits, in addition to increasing their accessibility. The development of quantum computers that can operate at room temperature [42] and which are not vibration sensitive would facilitate their use in a larger number of facilities and potentially onboard aircraft carriers and other military vehicles (which could prospectively use quantum computing for rapid decision-making support and cryptographic purposes).

Research is underway regarding making quantum computers viable under a larger set of environment conditions such as in conventional 'room temperature' environments [43]. Miniaturization and greater environmental condition support both will be key to increasing the number and types of locations that quantum computers can be deployed to. Recently, there has been significant research on how quantum computing hardware can be kept sustainable in more realistic environments [44]. As this research progresses, quantum computing capability can be utilized in a wider range of environments for application. SpinQ Gemini [45] is a desktop quantum computer that demonstrates how quantum computing hardware tends towards higher availability over time. Gemini is a quantum computer intended for educating students regarding quantum computing applications. To facilitate quantum computing's increasing availability, more research should be performed regarding keeping qubits stable in room temperature environments, mitigating decoherence rates in these environments, as well as in the presence of more qubits. With this, cyber-physical assets may be able to house quantum computing hardware for direct access to quantum computing capability, as well as keeping these assets under quantum cryptographic protection.

E. Preparing for Adversary Quantum Cryptography

Beyond the aforementioned, which improve society generally and provide targeted homeland security benefits, preparations for quantum cryptography are urgently needed. Some algorithms that are robust with regards to quantum cracking [17] have been developed and yet others are under development. Systems must be migrated to use these techniques as rapidly as possible; cyber-physical systems operating on a classical encryption framework are a key example of this need. Similarly, network traffic should also be transitioned to a quantum cryptographic framework as a means of securing it. Care must also be given as to what information is sent classically encrypted as any information that is transmitted could conceivably be decrypted by an eavesdropping adversary within a number of years.

F. Quantum Key Distribution and Data Transmission

Quantum key distribution is a considerable area of interest for quantum technology research. Transmission of quantum states between two parties allows secured data transfer [46], [47], safeguarding the security of information transmission. This approach should be considered when establishing a security framework for the future of a nation's cyber-defenses. With quantum data transmission, if a third party were to access a secure transmission between a sender and receiver, a moderating system or administrator could know that the line was accessed, as observation by a third party would change the quantum state of the transmission.

G. Application Area Development

Developing and implementing technologies to secure military assets, communication traffic, and other essential systems will be needed. With proper planning and implementation, these systems can benefit from the efficiency and security of quantum computing. Implementation of quantum computing by a nation allows the nation to innovate and thrive; while a failure to prepare combined with adversary quantum computer access can cause issues ranging from impaired international relations to divulged military and other secrets to compromised personal information. Asymmetric quantum computing capability not only directly threatens the cyber-defense of the nation state lacking in quantum technology. It also poses the risk of that nation state falling behind in certain key areas that may provide indirect tactical advantages through quantum computing capability. An example of this would be an adversary harnessing quantum simulation for pharmaceutical development, giving them leverage over opposing nation states with their now superior pharmaceutical developments.

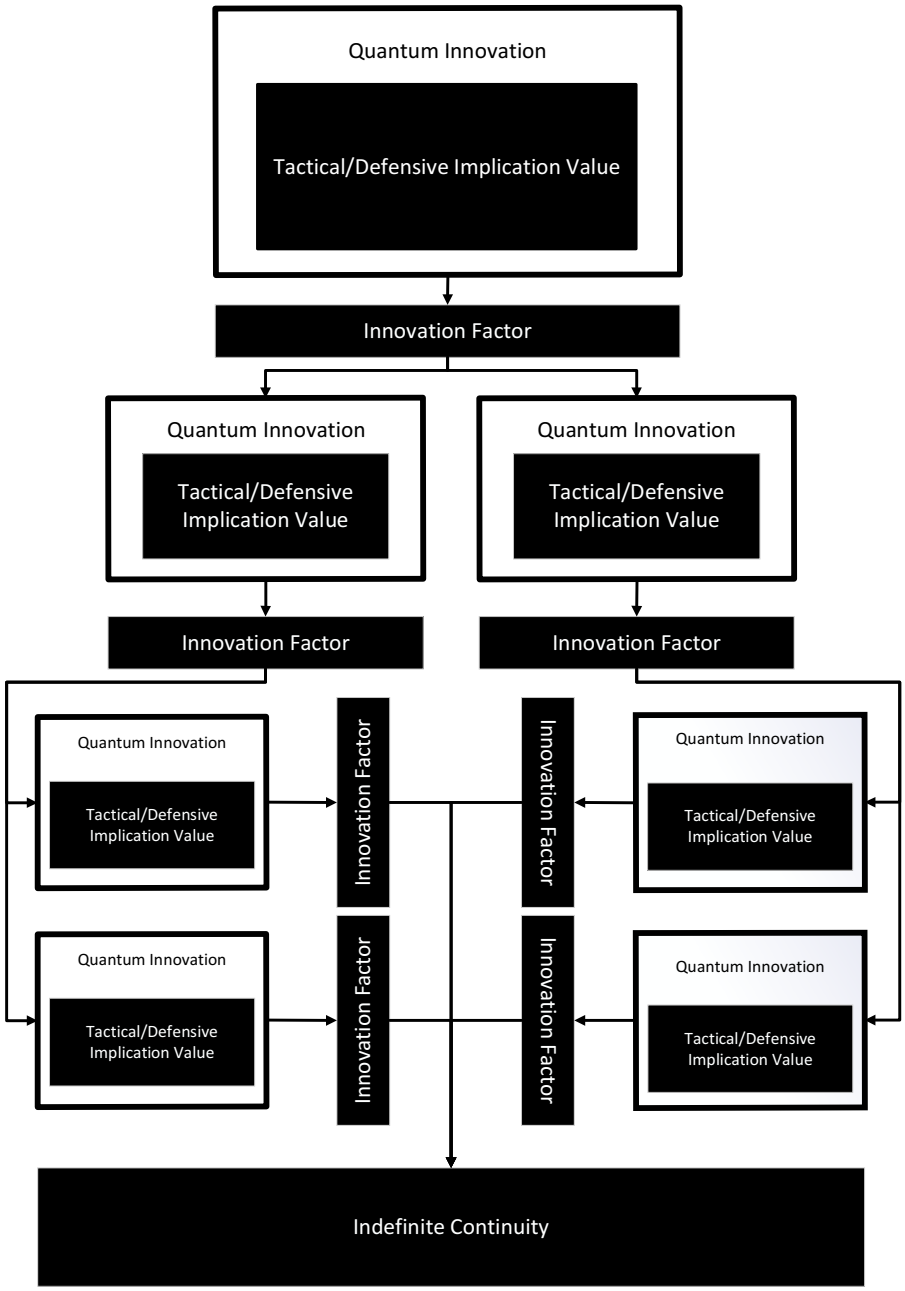
V. Analysis of Implications

This section considers how the different benefits and risks posed by quantum computing development by a nation, its allies and its adversaries should be assessed. Two models are presented and considered.

The first, presented in Figure 1, compares the impact of allied and adversary state quantum computing developments. The larger boxes represent nation states. This scenario depicts a nation with a single ally and two adversary nation states. As shown, the collective quantum computing advancements of a group of allied nations benefits all of them, as these allies will

presumably collaborate (to some extent) and share their knowledge of these developments. Conversely, adversary nations' advancements in quantum computing capability pose numerous threats to not only the defense integrity of the evaluating nation, but to its allied nations as well.

As shown in the diagram, individual quantum computing developments aggregate using a "weight" value. For this illustration, the weight is indicative of the value associated with a nation's quantum capability. The quantum computing capability weight of the evaluating nation is added to the total weight of quantum capability for allied nations, which directly opposes the collective weight of adversary nation states. As the tactical implications of quantum computing advancements have been stressed, it is imperative that the advancements of opposing nations are considered, as they pose a variety of threats to home/allied nation states. The evaluating nation state, as well as the allied nations, will need to maintain, if not surpass overall quantum computing capability relative to their opposition. In the figure, this is represented by the central bars. A national deficit in overall quantum computing development has the potential to put a nation's security at risk. An opposing nation with a quantum computing advantage could potentially enjoy military advantage or faster developments in the areas where quantum computing provides benefit, such as machine learning optimization and pharmaceutical development.



Innovation of quantum computing capabilities is also critical to assess. Quantum computing developments may drive other developments both due to the new technical knowledge that they uncover and make available to the broader community and by incentivizing nations whose adversaries seem to be gaining ground on them in quantum computing development, potentially creating a national security risk factor.

Figure 2 presents how a single quantum computing innovation has the potential to serve as the foundation for a cascade of consequential quantum innovations. In this case, an arbitrary quantum innovation, such as a new experiment leading to a breakthrough, provides the research landscape with new information to consider in their own studies as well as a national incentive to do so. A hypothetical scenario illustrating this is a new approach to mitigating decoherence rates in qubits. Following this approach, the methodology for keeping decoherence rates low is then harnessed by other research organizations throughout the research landscape, applying them to their own studies.

An example resultant innovation would be in a team of researchers utilizing the initial innovation as the basis for a large-scale, high-fidelity quantum computer for machine learning optimization. Continuing in this scenario, this innovation could serve as the catalyst for a variety of other quantum computing innovations, leading to an indefinite cascade of innovations that permeate throughout a given nation state, as well as its allied nation states. Advancements may also trigger development in concerned adversary states. Maintaining international quantum superiority is necessary to safeguard future

encryption implementations, as well as to facilitate scientific advancement.

VI. Conclusion

This document has provided an overview of multiple areas of consideration relevant to the need and process for the adoption of quantum computing for defense and homeland security purposes. The prospective benefits of quantum computing adoption are significant and range from enhanced scientific productivity and economic benefits to quantum computing's ability to enhance encryption and cybersecurity. If adversary nation states, state affiliated groups or terrorist groups obtain asymmetric quantum computing capabilities – either temporarily or for an extended period – the results could be quite problematic, as a robust quantum computing capability would allow the adversary to crack the passwords that protect data and secure key command systems on everything from water treatment plants to unmanned aerial vehicles.

This paper also discussed the benefits associated with quantum computing technology development. National realization of quantum computing capability for certain research areas has the potential to expedite their progress, by virtue of quantum computing's inherent random capability, as well as the efficiency improvements for certain tasks by using quantum algorithms. These advancements can provide a nation state with a variety of benefits for areas that contribute to the safety of national defense, as well as their offensive capability, such as enhanced cryptographic defenses, quantum capable cyber-physical assets, such as drones, and better tools for advancements in some machine learning tasks, for example.

Acknowledgment

This work has been supported, in part, by the U.S. National Science Foundation (NSF award # 1757659).

References

[1] S. Teja Marella and H. Sai Kumar Parisa, "Introduction to Quantum Computing," in *Quantum Computing and Communications [Working Title]*, IntechOpen, 2020.

[2] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, and C. N. Asogwa, "An overview of quantum cryptography and shor's algorithm," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, 2020, doi: 10.30534/ijatcse/2020/82952020.

[3] Q. Zhang, F. Xu, L. Li, N. Le Liu, and J. W. Pan, "Quantum information research in China," *Quantum Science and Technology*, vol. 4, no. 4. 2019, doi: 10.1088/2058-9565/ab4bea.

[4] J. Straub, "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios," *Technol. Soc.*, vol. 59, p. 101177, Nov. 2019, doi: 10.1016/J.TECHSOC.2019.101177.

[5] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Proceedings of the 6th International Forum on Strategic Technology, IFOST 2011*, 2011, vol. 2, doi: 10.1109/IFOST.2011.6021216.

[6] W. Buchanan and A. Woodward, "Will quantum computers be the end of public key encryption?," *J. Cyber Secur. Technol.*, vol. 1, no. 1, 2017, doi: 10.1080/23742917.2016.1226650.

[7] A. Mashatan and O. Turetken, "Preparing for the information security threat from quantum computers," *MIS Q. Exec.*, vol. 19, no. 2, 2020, doi: 10.17705/2msqe.00030.

[8] Stephen Shankland, "Quantum computers could crack today's encrypted messages. That's a problem.," *Cnet*, May 2021.

[9] A. Taeihagh, H. Si, and M. Lim, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transp. Rev.*, vol. 39, no. 1, pp. 103–128, Jul. 2018, doi: 10.1080/01441647.2018.1494640.

[10] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23. 2020, doi: 10.1016/j.vehcom.2019.100214.

[11] J. Schneider, "The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war," *J. Strateg. Stud.*, vol. 42, no. 6, 2019, doi: 10.1080/01402390.2019.1627209.

[12] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *Int. J. Inf. Secur.*, 2021, doi: 10.1007/s10207-021-00545-8.

[13] C. G. Leela Krishna and R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," *Auvsi Xponential 2018*, pp. 0–5, 2018.

[14] D. Rosch-Grace and J. Straub, "Analysis of the Likelihood of Inevitable of Quantum Computing Proliferation," *Submitt. Publ. Technol. Soc.*, 2021.

[15] M. Huang, Z. Chen, Y. Zhang, and H. Guo, "A Gaussian-distributed quantum random number generator using vacuum shot noise," *Entropy*, vol. 22, no. 6, 2020, doi: 10.3390/E22060618.

[16] B. Muruganantham, P. Shamili, S. Ganesh Kumar, and A. Murugan, "Quantum cryptography for secured communication networks," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, 2020, doi: 10.11591/ijece.v10i1.pp407-414.

[17] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.

[18] I. M. Georgescu, S. Ashhab, and F. Nori, "Quantum simulation," *Rev. Mod. Phys.*, vol. 86, no. 1, 2014, doi: 10.1103/RevModPhys.86.153.

[19] F. Sun, H. Wang, and J. Zhou, "Simulation Integrated Management: A new type of simulation platform application for aerospace systems engineering," *Simulation*, vol. 93, no. 2, 2017, doi: 10.1177/0037549716676894.

[20] C. K. Filelis-Papadopoulos, G. A. Gravvanis, and P. E. Kyziropoulos, "A framework for simulating large scale cloud infrastructures," *Futur. Gener. Comput. Syst.*, vol. 79, 2018, doi: 10.1016/j.future.2017.06.017.

[21] D. Ristè *et al.*, "Demonstration of quantum advantage in machine learning," *npj Quantum Inf.*, vol. 3, no. 1, 2017, doi: 10.1038/s41534-017-0017-3.

[22] M. Sparkes, "Quantum computer helps to design a better quantum computer | New Scientist," *NewScientist*, Sep. 2021. .

[23] H. Ma, M. Govoni, and G. Galli, "Quantum simulations of materials on near-term quantum computers," *npj Comput. Mater.*, vol. 6, no. 1, 2020, doi: 10.1038/s41524-020-00353-z.

[24] "Quantum Computing of an Atomic Nucleus | Department of Energy," Aug. 2018. .

[25] Rick Mullin, "Let's talk about quantum computing in drug discovery," *c&en*, Sep. 2020.

[26] E. Zohar, "Particle physics: Quantum simulation of fundamental physics," *Nature*, vol. 534, no. 7608. 2016, doi: 10.1038/534480a.

[27] I. Boyd, "Simulation Of Electric Propulsion Thrusters," *Aerosp. Eng.*, vol. 30, no. 0704, pp. 1–30, 2011.

[28] K. Ghoos, "Accuracy-based simulation strategies for plasma edge simulations for nuclear fusion devices," no. June, 2019.

[29] J. A. Hadden and J. R. Perilla, "All-atom virus simulations," *Current Opinion in Virology*, vol. 31. 2018, doi: 10.1016/j.coviro.2018.08.007.

[30] M. C. Lusardi, I. Dubovoy, and J. Straub, "Determining the Impact of Cybersecurity Failures During and Attributable to Pandemics and Other Emergency Situations," 2020.

[31] L. Ferreira *et al.*, "Introduction to Grid Computing with Globus," *Redbooks*, 2003.

[32] A. Sungkar and T. Kogoya, "A REVIEW OF GRID COMPUTING," *Comput. Sci. IT Res. J.*, vol. 1, no. 1, 2020, doi: 10.51594/csitrj.v1i1.128.

[33] L. Lamata, “Quantum machine learning and quantum biomimetics: A perspective,” *arXiv*. 2020, doi: 10.1088/2632-2153/ab9803.

[34] D. Laganá, P. Legato, O. Pisacane, and F. Vocaturo, “Solving simulation optimization problems on grid computing systems,” *Parallel Comput.*, vol. 32, no. 9, 2006, doi: 10.1016/j.parco.2005.03.019.

[35] D. Horny, J. Schukraft, K. A. Weidenmann, and K. Schulz, “Numerical and Experimental Characterization of Elastic Properties of a Novel, Highly Homogeneous Interpenetrating Metal Ceramic Composite,” *Adv. Eng. Mater.*, vol. 22, no. 7, 2020, doi: 10.1002/adem.201901556.

[36] B. Xu *et al.*, “Integration of a computational grid and virtual geographic environment to facilitate air pollution simulation,” *Comput. Geosci.*, vol. 54, 2013, doi: 10.1016/j.cageo.2012.09.031.

[37] A. Montanaro, “Quantum algorithms: An overview,” *npj Quantum Information*, vol. 2, no. 1. 2016, doi: 10.1038/npjqi.2015.23.

[38] D. Kahn and J. Straub, “Developing a Software Engineering Framework for Quantum Systems,” *Submitt. to Innov. Syst. Softw. Eng.*, 2021.

[39] C. Xue, Z. Y. Chen, Y. C. Wu, and G. P. Guo, “Effects of Quantum Noise on Quantum Approximate Optimization Algorithm,” *Chinese Phys. Lett.*, vol. 38, no. 3, 2021, doi: 10.1088/0256-307X/38/3/030302.

[40] R. Harper, S. T. Flammia, and J. J. Wallman, “Efficient learning of quantum noise,” *Nat. Phys.*, vol. 16, no. 12, 2020, doi: 10.1038/s41567-020-0992-8.

[41] D. Rosch-Grace and J. Straub, “Body Area Networks: A Data Sharing and Use Model based on the Blackboard Architecture and Boundary Node Discovery.”

[42] J. Wood, “Quantum computing with a sparkle,” *Mater. Today*, vol. 11, no. 5, p. 1, 2008, doi: 10.1016/S1369-7021(08)70068-3.

[43] M. Hosseini, G. Campbell, B. M. Sparkes, P. K. Lam, and B. C. Buchler, “Unconditional room-temperature quantum memory,” *Nat. Phys.*, vol. 7, no. 10, 2011, doi: 10.1038/nphys2021.

[44] Y. H. Chen, S. Stearn, S. Vella, A. Horsley, and M. W. Doherty, “Optimisation of diamond quantum processors,” *New J. Phys.*, vol. 22, no. 9, 2020, doi: 10.1088/1367-2630/abb0fb.

[45] S.-Y. Hou *et al.*, “SpinQ Gemini: a desktop quantum computer for education and research.”

[46] L. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, “Long-distance quantum communication with atomic ensembles and linear optics,” 2001.

[47] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, “Secure quantum communication technologies and systems: From labs to markets,” *Quantum Reports*, vol. 2, no. 1. 2020, doi: 10.3390/quantum2010007.