Considering the Implications of Artificial Intelligence, Quantum Computing, and Cybersecurity

Dominic Rosch-Grace and Jeremy Straub
Department of Computer Science
North Dakota State University
Fargo, ND, USA
dominic.rosch@ndsu.edu, jeremy.straub@ndsu.edu

***Abstract*—This paper considers the impact of using artificial intelligence and quantum computing as part of a cyber defense strategy and the deterrence, defense, and offensive capabilities that it provides. A model for this is presented and discussed.**

Keywords—artificial intelligence, AI, quantum computing, cybersecurity

I. Summary

Nuclear deterrence and mutual assurance of destruction have successfully prevented the use of nuclear weapons for decades. This concept has been applied to cyberwarfare [1] and the deterrence value of quantum computing [2], as well as its importance for national security [3], have also been previously considered. Building on this, the concept of applying key components of artificial intelligence and quantum computing to cyber-defense is evaluated in this paper. The efficacy of quantum computing (QC) and artificial intelligence (AI) as deterrent capabilities, as offensive capabilities, and as defensive capabilities are considered. This, the ability of AI agents to analyze vast quantities of data, and its potential use in tandem with the encryption-breaking capabilities of future QCs suggests that QC and AI may have a symbiotic relationship and a key role in building the next generations of cyber-defense capabilities. This can create a notable benefit for a possessing state and the potential for significant threats for a state whose adversaries possess these technologies (particularly without a given state possessing them itself as a deterrent).

Based on this analysis, it is recommended that national security organizations evaluate the risks associated with adversaries possessing capable AI and quantum computing systems and their potential for threatening the computing and computing-controlled resources that society depends on. The idea of using AI, QC, and cybersecurity practices to bolster the capabilities of one-another is also reviewed. Many capabilities, inherent to these individual areas, which can be applied to the development of the other areas, are discussed. Based on this analysis, a model for mutual advancement between AI, QC, and cybersecurity is presented. This model is based on the notion that progression, in one of the three areas, can also lead to beneficial developments in the others.

II. Introduction to Artificial Intelligence and Quantum Computing

This section presents a brief review of artificial intelligence and quantum computing. AI is a branch of computing that works towards designing and developing machines and algorithms that provide computerized decision-making capabilities which may (or may not) be similar to humans, in both their form and accuracy. Some AI techniques seek to simulate, or even surpass the capabilities of human cognition [4]. Others are single-purpose tools for a particular application area. AI has been shown to be an effective tool for military decision making, as it can expedite the process of synthesizing large quantities of data and can make subsequent data-driven predictions with high accuracy [5]. The potential for AI applications, in multiple areas of military operations (such as logistics, cyber-operations, command and control, and autonomy [6]), has been extensively studied.

Another rapidly growing area of technological development is QC. QC harnesses elements of quantum mechanics to perform calculations [7]. By doing so, quantum computers are able to perform some calculations faster than classical computers, largely due to quantum parallelism [8], [9]. Unlike classical computers, which use bits, the elementary unit of information used in QCs is the quantum bit, often referred to as a qubit. A qubit can maintain a probabilistic superposition of two discrete states (0 and 1) concurrently, enabling considerable speed enhancements for certain problems. Some of the potential uses for future QCs are based on their prospective ability to break certain modern forms of encryption [10]. Techniques such as Shor's algorithm show that future quantum computers may be able to break encryption methods, such as RSA, significantly faster than classical computers [11]. In response to this, research has been launched to prepare for these capabilities [12].

III. Implications of Quantum Computing and Artificial Intelligence for Cybersecurity

AI has long been discussed as a potential tool for attacking and defending software and systems. Particularly, because of the real world impact that their failure can have, cyber-physical systems have been targeted and shown to be vulnerable to AI-based attacks [13]. In addition to the potential for AI agents to be harnessed for malicious purposes, the technology has also been considered as a tool to improve upon the cyber-defense practices society depends on. For example, Sarkar, et al. [14] considered the possibility of leveraging AI to automate cyber-defense practices and use a learning capability.

Some AI techniques are capable of scanning large quantities of available data and identifying and inferring about patterns within them. Data regarding cyber-attacks and methods could, for example, be processed by an AI to facilitate the identification of how an attack could occur and – for a defender assessing their

979-8-3503-2028-2/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCI58124.2022.00252

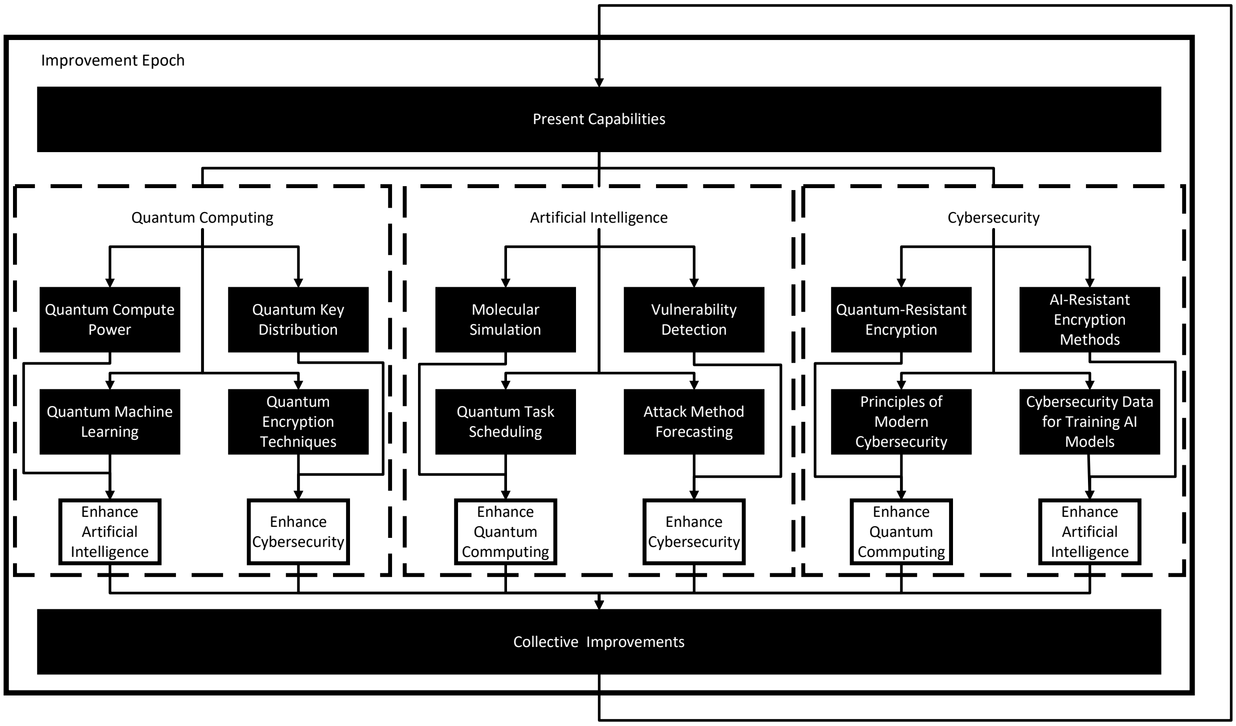
Improvement Epoch
Present Capabilities
Quantum Computing
Artificial Intelligence
Cybersecurity
Quantum Compute Power
Quantum Key Distribution
Molecular Simulation
Vulnerability Detection
Quantum-Resistant Encryption
AI-Resistant Encryption Methods
Quantum Machine Learning
Quantum Encryption Techniques
Quantum Task Scheduling
Attack Method Forecasting
Principles of Modern Cybersecurity
Cybersecurity Data for Training AI Models
Enhance Artificial Intelligence
Enhance Cybersecurity
Enhance Quantum Commputing
Enhance Cybersecurity
Enhance Quantum Commputing
Enhance Artificial Intelligence
Collective Improvements

Figure 1. Model of mutual support between AI, QC, and cybersecurity.

own systems – how to defend against it. An AI system with these capabilities could prospectively mitigate the threat of attacks, assuming it was given the resources to learn how to defend against them. Similarly, AI may also be an effective tool for cybersecurity personnel to use to identify potential vulnerabilities in their software and systems. Some AI techniques can cover a vast search space – such as all areas of a target software application – while identifying patterns that may indicate a program vulnerability. This could be used to find software vulnerabilities to repair, thus, improving the defense capabilities of the program in question. AI could also be used to carry out offensive cyberattacks.

In addition to direct offensive and defensive operations, there are a number of other ways that AI can aid national security, such as by enhancing the efficacy of conventional warfighters. Additionally, software for managing military logistical decision-making could use AI agents. AI techniques, such as fuzzing, could also be used to detect and correct vulnerabilities in a nation-state's own tools and to detect and attack vulnerabilities in adversaries' tools. The use of quantum computing for this has been previously discussed [15].

AI could also be used to benefit QC. An AI multi-agent system, for example, could be developed and tasked to optimize different environmental and configuration parameters to mitigate quantum computing noise to the greatest extent possible. The resulting QC system could be better suited for implementing quantum cryptographic methodologies – and for other tasks – which could then be used to strengthen a nation's cyber-defense and offensive capabilities.

QC also has key offensive and defensive roles in cybersecurity. Shor's Algorithm, a QC algorithm for factoring large integers in polynomial time (faster than classical computing) [16], provides one example. As many current forms of encryption rely upon the computational difficulty of factoring large integers, the ability of a quantum computer to factor large integers quickly poses a considerable threat [17].

Although AI and QC face a variety of challenges [18], [19] that may limit their development and, thus, practicality for some applications, the concept of using them synergistically should be considered to enhance national security.

To this end, synergies may be exploited, such as the ability of AI agents to synthesize vast quantities of data [20] and quantum computers' capability to perform data processing tasks faster than their classical counterparts [16]. AI agents may assist in the development of QCs and QCs may facilitate the development of and host increasingly capable AI systems.

IV. Model

A model is proposed, which is presented in Figure 1, that considers multiple national security-relevant factors. It includes AI, QC and cybersecurity, facilitating trade-off analysis. Characteristics of AI, QC and cybersecurity are analyzed to evaluate how these tools can be used to enhance national security. The cyclical nature of development, the support capabilities between AI, quantum computing, and cybersecurity, and the potential use of the three technology areas as catalysts for the development of the others must also be considered. The symbiotic relationship between these three distinct technologies and areas of research and the analysis of nation states' current and future capabilities for developing QC and AI technologies are also key considerations.

In particular, Figure 1 highlights how developments in AI, QC and cybersecurity can result in increased technological capabilities for the party possessing each technology. The model is presented in terms of an iterative progression of improvement epochs. Each epoch is an arbitrary unit of time in which at least one of the three technologies enjoys an improvement. These improvements contribute to the collective capabilities of the possessing state and are, thus, technological abilities that can be used during subsequent iterations of advancement, further bolstering the capabilities of other technologies.

The model demonstrates how advances in each area can contribute to the advancement of the other two areas. Several examples of such advances are provided.

For example, QC can aid AI via QC processing power and quantum computing machine learning techniques. QC processing power can be used to enhance existing artificial intelligence techniques (see [21]) and to support the development of new ones. QC machine learning techniques are new techniques designed specifically to benefit from the capabilities of quantum computers.

QC can, similarly, aid cybersecurity by providing quantum key distribution and quantum computing encryption techniques. Quantum key distribution facilitates the secure distribution of encryption keys, via using properties of quantum computing to determine whether the transmission has been intercepted by a third party or not. Quantum encryption techniques make use of quantum computing processing to perform encryption.

Artificial intelligence aids quantum computing through molecular simulation – which can help to develop more robust quantum computers and remove system noise – and providing computational capability scheduling. It can aid cybersecurity through automating vulnerability detection and projecting how an adversary may attach a system.

Finally, cybersecurity can aid the other two technology areas by helping to secure them, using modern best practices. It can also advance the disciplines via the development of QC and AI technique—resistant encryption capabilities. Cybersecurity can also aid AI research by providing relevant data for training AIs that will work in the cybersecurity area.

Notably, there is overlap, as not all advancements fit into a single area and some may span two or more. The model projects that the advancement process could continue indefinitely, albeit with different specific advancements over time. This enables state actors possessing two or more of these technologies to continuously strengthen their technological capabilities.

V. Conclusion

The synergistic nature of QC, AI, and cybersecurity allows them to be leveraged to strengthen the tactical capabilities of a nation state. As shown by the model presented herein, improvements in each area may enhance the others, potentially creating a positive spiral of continuous advancements for a nation state. Because of this, the model demonstrates the importance of nation states investing in all three technology areas to develop or maintain technological superiority. These capabilities provide clear and important offensive, defensive, retaliatory and deterrent benefits.

References

[1] 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.

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

[3] D. Rosch-Grace and J. Straub, “Analysis of the Necessity of Quantum Computing Capacity Development for National Defense and Homeland Security; Analysis of the Necessity of Quantum Computing Capacity Development for National Defense and Homeland Security,” 2021 IEEE Int. Symp. Technol. Homel. Secur., 2021, doi: 10.1109/HST53381.2021.9619831.

[4] S. Dick, “Artificial Intelligence,” Harvard Data Sci. Rev., Jun. 2019, doi: 10.1162/99608f92.92fe150c.

[5] K. Van Den Bosch and A. Bronkhorst, “Human-AI Cooperation to Benefit Military Decision Making,” NATO Sci. Technol. Organ., no. June, 2018.

[6] K. M. Sayler and D. S. Hoadley, “Artificial Intelligence and National Security,” Congr. Res. Serv., 2019.

[7] V. Hassija et al., “Present landscape of quantum computing,” IET Quantum Commun., vol. 1, no. 2, pp. 42–48, Dec. 2020, doi: 10.1049/IET-QTC.2020.0027.

[8] H.-S. Zhong et al., “Quantum computational advantage using photons Downloaded from,” 2020.

[9] G. Casati and G. Benenti, “Quantum Parallelism - an overview | ScienceDirect Topics,” ScienceDirect, 2012.

[10] M. Möller and C. Vuik, “On the impact of quantum computing technology on future developments in high-performance scientific computing,” Ethics Inf. Technol., vol. 19, no. 4, 2017, doi: 10.1007/s10676-017-9438-0.

[11] 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.

[12] L. O. Mailloux, C. D. Lewis, C. Riggs, and M. R. Grimaila, “Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals,” IT Prof., vol. 18, no. 5, 2016, doi: 10.1109/MITP.2016.77.

[13] N. Kaloudi and J. Li, “The AI-Based Cyber Threat Landscape,” ACM Comput. Surv., vol. 53, no. 1, pp. 1–34, Jan. 2021, doi: 10.1145/3372823.

[14] I. H. Sarker, M. H. Furhad, and R. Nowrozy, “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,” SN Computer Science, vol. 2, no. 3. 2021, doi: 10.1007/s42979-021-00557-0.

[15] D. Rosch-Grace and J. Straub, “From Quantum Fuzzing to the Multiverse: Possible Effective Uses of Quantum Noise,” 2022, pp. 399–410.

[16] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” 2017, doi: 10.1038/nature23474.

[17] 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.

[18] B. W. Wirtz, J. C. Weyerer, and C. Geyer, “Artificial Intelligence and the Public Sector—Applications and Challenges,” Int. J. Public Adm., vol. 42, no. 7, 2019, doi: 10.1080/01900692.2018.1498103.

[19] A. Kandala, K. Temme, A. D. Córcoles, A. Mezzacapo, J. M. Chow, and J. M. Gambetta, “Error mitigation extends the computational reach of a noisy quantum processor,” Nature, vol. 567, no. 7749, 2019, doi: 10.1038/s41586-019-1040-7.

[20] N. Wiebe, A. Kapoor, and K. M. Svore, “Quantum deep learning,” Quantum Inf. Comput., vol. 16, no. 7–8, 2016, doi: 10.26421/qic16.7-8-1.

[21] N. Vasiljevic et al., “Machine learning & artificial intelligence in the quantum domain: a review of recent progress,” Reports Prog. Phys., vol. 81, no. 7, p. 074001, Jun. 2018, doi: 10.1088/1361-6633/AAB406.