

Michael Doyle III

Old Dominion University

ENGL 211

Mr. Norris

2/17/2026

Research Question: How will quantum computing change modern cybersecurity practices?

A Conceptual Framework for Quantum Computing's Impact on Cybersecurity

Introduction

Quantum computing represents one of the most significant technological shifts in modern computer engineering. Unlike classical machines, quantum processors use superposition and entanglement to reach levels of computational power that traditional systems simply can't match. As these technologies continue to develop, their ability to break widely used encryption methods and reshape cybersecurity practices has become a serious concern for researchers, governments, and industry professionals who depend on secure digital infrastructure.

The urgency behind this shift isn't just technical; it's tied directly to human impact. Encrypted systems protect everything from medical records and financial accounts to personal communication and national infrastructure. If classical cryptography were to fail suddenly, the consequences would fall on real people: identity theft on a massive scale, financial instability, exposure of private health information, and disruptions to essential services. Groups that rely heavily on digital systems but have fewer resources, such as patients, students, military families, and small businesses, would be hit the hardest. This makes it critical to understand quantum-enabled threats before they become unmanageable.

Current cybersecurity frameworks rely on cryptographic systems such as RSA, ECC, and Diffie-Hellman methods that remain secure against classical attacks but are vulnerable to quantum algorithms like Shor's algorithm (Shor, 1997). Meanwhile, quantum-resistant or "post-quantum" cryptographic methods are emerging, but their readiness, scalability, and long-term reliability are still uncertain (NIST, 2016). Understanding how quantum computing will alter cybersecurity practices is essential not only for protecting organizations and national security but also for safeguarding the everyday digital lives of individuals. This project examines the current state of quantum computing, analyzes its projected impact on cybersecurity, and outlines a conceptual framework for how cybersecurity practices must evolve in response.

The preliminary findings suggest that quantum computing will fundamentally alter cybersecurity by weakening or even eliminating the effectiveness of classical encryption systems. Mosca et al. (2018), writing in *IEEE Security & Privacy*, argue that widely used algorithms such as RSA and ECC face complete compromise under sufficiently powerful quantum attacks. Chen et al. (2016), in the *NIST Post-Quantum Cryptography Report*, show that post-quantum cryptographic methods vary significantly in maturity, performance, and implementation feasibility. Research published in journals such as *Communications of the ACM* and the *Journal of Cybersecurity* also shows that while awareness of quantum threats is increasing, actual preparedness remains limited. Organizations hesitate because of unclear timelines, high implementation costs, and the lack of standardized quantum-resistant protocols.

Ethical concerns, especially “harvest-now, decrypt-later” strategies, add even more pressure. Attackers can collect encrypted data today and wait until quantum computers are strong enough to break it, putting long-term privacy at risk for hospitals, governments, and private companies.

Taken together, these findings reveal a clear gap in the existing scholarship. Research tends to focus on isolated pieces of the problem: algorithmic vulnerabilities, cryptographic alternatives, or ethical risks. Technical papers concentrate on the math, policy papers focus on governance, and industry reports highlight implementation challenges. What’s missing is a unified conceptual framework that connects these elements into a single model that cybersecurity practitioners can actually use for planning and decision-making. This project aims to fill that gap by developing an integrated framework that brings together technical vulnerabilities, ethical implications, and organizational readiness, offering a clearer path for preparing for quantum-enabled threats and transitioning responsibly toward post-quantum security systems.

The peer review process played a major role in shaping the final version of my proposal, especially the feedback I received from Emmanuel Somuah. The most helpful critique he offered focused on strengthening my emotional appeal in the introduction. He pointed out that while my opening was informative, it didn’t fully capture the real-world urgency of quantum-enabled threats. Implementing this suggestion, I revised the introduction to highlight the risks to medical records, financial data, and national infrastructure. This change made the stakes more relatable and helped me connect the technical issue to everyday people. Emmanuel also suggested narrowing my audience and clarifying my credibility. I incorporated this by refining my tone to speak more directly to cybersecurity practitioners and policy makers, while also emphasizing my academic background in computer engineering. I chose not to add a personal anecdote, even though it was suggested, because the genre of a research proposal prioritizes professionalism and evidence-based reasoning over personal storytelling.

Expanding the proposal to 500 words without becoming repetitive required careful genre awareness. Instead of adding filler, I deepened my explanations of key concepts, clarified

transitions, and expanded the discussion of the research gap. I focused on maintaining a professional tone by ensuring every added sentence contributed either context, clarity, or justification for the project's significance.

My understanding of my research question has also evolved significantly. At first, I viewed the topic mainly as a technical issue involving encryption. Through drafting and revision, I realized the problem is much broader, connecting ethics, organizational readiness, and long-term societal risk. This shift helped me frame my project not just as an analysis of algorithms, but as a conceptual framework that addresses the full ecosystem of cybersecurity in a quantum future.

References

Shor, P. (1997). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*.

<https://arxiv.org/abs/quant-ph/9508027> (arxiv.org in Bing)

National Institute of Standards and Technology (NIST). (2016). *Post-Quantum Cryptography Standardization Project*.

<https://csrc.nist.gov/projects/post-quantum-cryptography> (csrc.nist.gov in Bing)

Mosca, M. (2018). *Cybersecurity in an Era with Quantum Computers*. IEEE Security & Privacy.

<https://ieeexplore.ieee.org/document/8432210>

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography*. NISTIR 8105.

<https://doi.org/10.6028/NIST.IR.8105> (doi.org in Bing)