Cybersecurity in a Quantum Realm: Persuasive Language and Analogies in Academic Papers

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Yazmeen Younus Imam

Fall 2023

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

STS Advisor:

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

Quantum computing, a seemingly revolutionary technology, brings a new era in what a computer is capable of, but also unprecedented challenges and issues. "Cybersecurity researchers and analysts are rightly worried that [this] new type of computer, based on quantum physics rather than more standard electronics, could break most modern cryptography. The effect would be to render communications as insecure as if they weren't encoded at all," (Denning, 2019). This issue could be addressed through government policies, but that still requires much research, written academic papers, and articles to educate people on this subject. But, explaining the topic is not an easy task. The aim of this paper is to research how authors discuss this issue when writing about the intersection of cybersecurity and quantum computing, emphasizing the language and analogies that they use in their scientific papers.

Analogies are useful linguistic tools that help describe new complex technologies to people with no background in the field, but misuse can cause misconceptions and misunderstandings. With the new technology of quantum computing and the even newer technology of quantum resistant cybersecurity, it is important to emphasize the importance of language used to help people understand this issue at hand. Academics and researchers documenting their findings could find it difficult to explain their research without using language that can influence people's interpretation, understanding, and reaction to quantum computers as a security threat. Authors and researchers have a responsibility in choosing their words and metaphors, as these choices have a significant impact on shaping public and academic perception.

When an analogy incorrectly shows a technology's uses or its potential consequences, it can lead to untrue expectations. This is especially important to avoid regarding cybersecurity

and how people's personal information is protected. This emphasizes the need for examination of analogies in scientific articles. This paper examines the language and analogies in academic work on cybersecurity in the quantum world. In doing so, it will show how these analogies and persuasive language influence our understanding of quantum computing when it meets with cybersecurity.

Problem Definition

Quantum computing's sole purpose during its development was to create faster, better computers, but an unintended consequence was that these computers can break through almost all commonly implemented cryptography in the world. Most cryptography today is based on using mathematical algorithms to encrypt the data. These algorithms would take years for classical computers to decrypt, but could theoretically take only days for quantum computing. If hackers were to utilize quantum computers in their cyberattacks, they could access all personal information guarded by current cybersecurity. Dr. Walid Rjaibi and Dr. Sridhar Muppidi underline this exact issue by stating, "when large-scale quantum computers are available, that vast computing power could be implemented to break the encryption and learn about those communications," in "Quantum computing and cybersecurity: How to capitalize on opportunities and sidestep risks" (2018).

If quantum computers are more publicly available without regulations, hackers have access to one of their most desirable targets: medical records as they can be sold for a large profit or be used in fraud. Darren West stated to PBS in Grabenstein (2022), "Health data can be more valuable to hackers than financial data." Everyone has medical records, so this can greatly impact millions to billions of people whose personal records are now in even more danger of being stolen. Also according to Grabenstein (2022), health data breaches can leak a multitude of

sensitive information from hospital databases, which often includes both personal and financial details. Also, system shutdowns from cyberattacks are also detrimental to hospitals, Grabenstein explains further stating "...ransomware is particularly worrisome. That's when a hacker locks down networks and demands the victim pay a ransom to bring systems back online. In a health care environment, systems shutting down can have dangerous consequences." The aftermath of data breaches is intense and devastating to families, as seen in incidents like the cyberattack on the University of Vermont Medical Center, which had a terrible financial impact on families and disrupted critical healthcare services in the hospital. This further proves the need for cyber protection and safety that the rise of quantum computing threatens to break.

Luckily, new research within the last few years promises to improve security through new means such as quantum machine learning and quantum random number generation (Boutin, 2023). This is also why quantum *resistant* computing was created: to create more secure algorithms and encryptions to protect data so that even quantum computing cannot decrypt it. Though the process has started, there is still much time between it becoming common security protocols. "In 2016, the National Institute of Standards and Technology (NIST) initiated a process to solicit, evaluate, and standardize quantum-resistant cryptographic algorithms… The standardization process is expected to complete in 2022, at which point vendors can begin the decade-long process of deployment." said by Michaela Lee (2021).

While much research is happening on the technical aspects of quantum computing and cybersecurity, less attention is being paid to the linguistic and metaphorical framing of these issues. To examine this, one must delve deeper into the language and metaphors in the papers and articles on cybersecurity in the age of quantum computing. Whether the research paper or discussion article is centered around warnings or optimistic solutions, researchers' language

significantly impacts how society perceives and prepares for the quantum future. For instance, comparing quantum computers to a "double-edged sword" or "Pandora's box" might evoke a sense of foreboding, while also emphasizing both their potential benefits and their dangers.

Researchers might not always be critically thinking about the implications of the comparisons they write. So, this paper seeks to pay close attention to and dissect the analogies and influential languages present in scientific discourse on quantum computing, so that these researchers can be aware that their word choice has weight and implications. Addressing this oversight requires a close examination of the existing literature to observe the language choice and their intended and received implications. This paper will evaluate the extent to which these analogies are useful in understanding quantum computing and where they might lead to misunderstandings.

Research Approach

From “The Power of Analogies for Imagining and Governing Emerging Technologies,” Claudia Schwarz explains the concept of “analogical imagination,” which is a device that allows the discussion of new technologies. Analogical imagination is using analogies to connect one technology to another, making it easier to understand. Using this concept, one can go into how analogies function as more than just explanatory tools, instead they are very important literary devices to influence our perceptions and expectations of new technologies. This research approach is to analyze academic papers and articles on the topic of cybersecurity in quantum computing using Claudia Schwarz’s intellectual framework. Claudia Schwarz uses Paul Ricoeur’s definition of imagination who stated imagination is "the power of the possible that can assist in teasing out the potentialities of reality." It allows us to examine the descriptive and predictive power of analogies in influencing future perceptions of technology and how to

implement policies on this subject. This framework is very important for this research as it provides the approach to uncovering how analogies influence our understanding of the possible good and dangers of quantum computing in cybersecurity. This paper discusses insight into how the field of quantum computing is being framed and understood in the context of cybersecurity.

"An analogy is something that shows how two things are alike, but with the ultimate goal of making a point about this comparison." (*What is analogy?, 2021*). Analogies are literary tools used to help convey ideas and information to explain a topic more effectively. They are used in almost every research paper or academic article so the information in the text is more digestible for non-experts, especially when the topic is about new technology.

Schwarz-Plaschg explains in "The Power of Analogies" how analogies are used both to stimulate imagination and to frame technologies in specific ways, which in turn influences societal discussions and government policies. The author argues that while analogies push for imaginative thinking about new technologies, they can also restrict imagination by framing these technologies in unintended ways. This possible ambiguity of analogies is important in understanding their role in funding policies and governance approaches. This approach recognizes that emerging technologies such as quantum computing are exponentially complex and may require many, many analogies, sometimes even contradictory ones, to understand their complexities. Schwarz-Plaschg states, "Analogical imagination in this sense is akin to a mode of deliberation, which is characterized by a swinging back and forth between different analogies." By embracing diverse perspectives and also counter-analogies, analogical imagination avoids the pitfall of oversimplification that only using one analogy could lead to. Schwarz-Plaschg ends "The Power of Analogies" by saying that the complexity of multiple analogies can contribute to a more inclusive and holistic view of describing emerging technologies.

This paper's focus lies in the analogies drawn between quantum computing and existing sociotechnical systems. Researchers, often implicitly or explicitly, compare quantum computing to known systems to be more palatable and easier to understand when explaining its potential problems and advantages. This comparative analysis is a reflection of a deep cognitive process where the familiar is used as a reference point to comprehend something that does not yet make sense. It's crucial to consider how such comparisons can be both informing and also deceptive. On the one hand, they provide a framework for conceptualizing new technologies by anchoring them in the known. On the other, they can lead to misconceptions if the aspects of quantum computing are not fully described well or if the analogies are pushed beyond their appropriate limits. For example, comparing quantum cryptography to traditional encryption methods might highlight the increased security quantum algorithms offer. However, if this analogy does not account for the unique properties of quantum mechanics, it could falsely imply that quantum cryptography is just a stronger version of its classical counterpart, which it fundamentally is not.

There is a difficult balance between being clear and potentially misrepresenting technology in academic articles where complex topics like quantum computing are broken down for public understanding. The following analysis goes into how authors go about this in their writings. Four scholarly articles that were observed are: “Cyber Security in the Quantum Era” by Petros Wallden and Elham Kashefi, “Defending reality: Truth in an age of synthetic media” written by Mike Bechtel and Bill Briggs, “Is quantum computing a cybersecurity threat?” by Dorothy Denning, and lastly Michaela Lee‘s “Quantum Computing and Cybersecurity.” A content analysis is later conducted by reading and identifying the analogies or influential language used in these sources.

Academic articles about cybersecurity and quantum computing must use these analogies to explain the complex, complicated discussions surrounding their uses, implications, and consequences. But, misuse or over-simplification of these topics could lead to misinterpreting the issues at hand. By examining the four articles, insight into the use of analogies and influential language is gained. This will provide a better picture of the discourse surrounding quantum computing and its implications for cybersecurity.

Results

As discussed previously, the literary structure and word choice used in articles and papers can influence academic discourse and also sway public perception. Again an example being, comparing quantum computers to a "double-edged sword" or "Pandora's box" could suggest uneasiness, while also emphasizing both their potential benefits and their dangers. Similarly, describing the act of cybercriminals "stockpiling" data for future decryption could create an image of a ticking time bomb, emphasizing the looming threat. In exploring both the problems and the solutions, researchers might use analogies of "building digital fortresses" or "creating cybersecurity immune systems," suggesting a proactive and defensive stance against potential quantum and cyber threats. Figure 1 is a spectrum of analogies, ranging from strongly favoring the technology to warning about its potential impact.

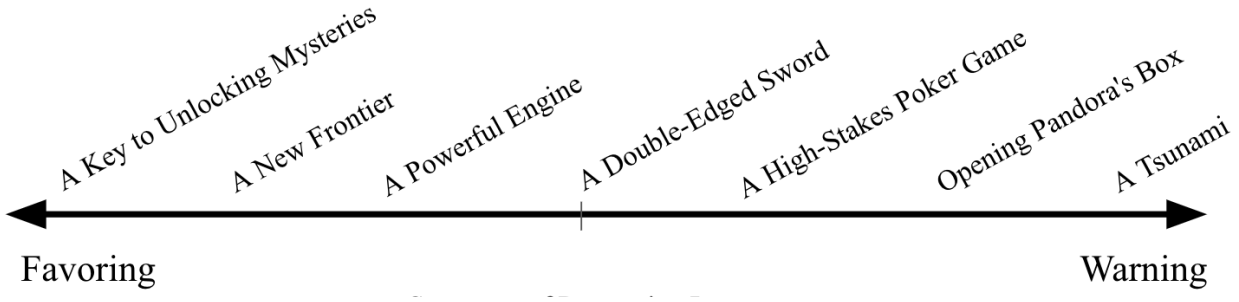

Figure 1. Spectrum of Persuasive Language Surrounding Quantum Computer (Created by author)

The language used, whether it portrays quantum computing as an ‘impending storm’ or a ‘new era of security’, undeniably influences the perception of this complex and possibly consequential technology. Analyzing and interpreting this language is the first step to get authors to be more cautious with their words.

The first article’s analogies and influential language that was analyzed is Petros Wallden and Elham Kashefi’s “Cyber Security in the Quantum Era” (2019). For context on this article, Wallden and Kashefi discuss the misconceptions in recent research in quantum cyber security in a way that's understandable for non-experts. It focuses on specific aspects of quantum cyber security research, clarifying facts about quantum computers and what can come from it, and researching post-quantum security. The article also addresses myths and realities about quantum computing. One example of an analogy in this article is when Wallden uses the concept of a "quantum revolution." This is used as an analogy to historical revolutions, suggesting that quantum technology can be as significant in science and technology. Wallden specifically says, "This has led to what is now called 'the second quantum revolution,' where the ability to manipulate quantum systems as desired is leading to an era in which a variety of new technologies will appear." This analogy, while showing the potential of quantum technology, favors quantum computing but could also understate its challenges and also does not touch on the consequences. "We are interested in using 'quantum gadgets,' usually with simple quantum devices (available with current state-of-the-art technologies), to boost classical protocols in a number of ways," is another use of an analogy. This suggests that quantum technologies are tools that provide more capabilities or further improvements to systems that already exist.

The second article is Michaela Lee‘s “Quantum Computing and Cybersecurity” (2021). This paper discusses what quantum computing is, using analogies to explain these complex

concepts. Additionally, the paper also goes into the impact of quantum computing on current encryption methods and the development of quantum-resistant cryptography in great detail. An analogy it uses, for instance, compares the qubits in quantum computing to spinning coins. A specific quote being, "To conceptualize these properties, envision a coin that has two states—heads or tails. That coin represents traditional bits. If you spun the coin, it would be both heads and tails at the same time (superposition). If you spun a pair of two entangled coins, the state of one would instantly change the state of the other (entanglement)." This illustrates the concepts of superposition and entanglement in a more understandable way. Another use of persuasive language is when Lee compares the process of integrating quantum computing in modern security to a 'long game', saying "The U.S. and its allies should anticipate the long game that will require continuity of effort, funding, preparation, and collaboration." This analogy more warns the reader and suggests that this technology requires strategic thinking, patience, and sustained effort over an extended period, much like a strategic game that evolves over time.

Next is "Defending reality: Truth in an age of synthetic media" (2023), written by Mike Bechtel and Bill Briggs. They talk about the impact specifically generative AI and quantum computing has on cybersecurity. It specifically discusses the threat of synthetic media in cyberattacks and how quantum machine learning could be used to improve cyber defenses, but also create more dangerous cyber threats. The article also emphasizes the need for enterprises to prepare for these imposing threats. The article has many instances of using "wave" as a metaphor or an analogy to compare the rapidity and impendingness of quantum computing's consequences. Bechtel and Briggs state, "A wave of artificially generated content is now targeting enterprises, exploiting vulnerabilities by impersonating trusted sources." This article also uses 'tool' analogies to describe how quantum computers can be used. Specifically saying,

"Social engineering is nothing new, and while synthetic media may give hackers a new tool in their toolbox." Lastly, "It has the potential to supercharge the problem of artificially generated content but also could be a boon to enterprises' cyber defenses." The word boon gives off the idea that this technology is a gift or a blessing that can be utilized and supercharge implies that quantum machine learning can enhance both the problems and fraud with cyberattacks and also the development of defenses against them.

In the last article, "Is quantum computing a cybersecurity threat?" (2019), Dorothy Denning discusses the possible risks of quantum computing to modern cryptography. It also goes into how quantum computers could break most modern cryptography, making almost all current encryption methods ineffective. Additionally, the article describes the basics of cryptography and explores quantum-resistant cryptography solutions. One example of an analogy used here is "At its most basic, encryption is the act of taking an original piece of information—a message, for instance—and following a series of steps to transform it into something that looks like gibberish." The word gibberish is used here to show how much more knowledgeable and capable a quantum computer is to a human, favoring the computer.

These examples of persuasive language and analogie reveal a spectrum of perspectives toward quantum computing and its implications for cybersecurity. At first, it seemed that these analogies were only tools, simplifying complex concepts for a public audience. However, with this evidence, it is seen that these analogies do more than explain; they can change a person's perception. With the most prominent analogy, the 'quantum revolution' analogy, emphasizes quantum computings potential, also glosses over the challenges and risks, leading to a false hope about quantum computing. On the other hand, analogies that would compare quantum

computing to a 'double-edged sword' or a 'ticking time bomb' could unintentionally cause resistance towards developing these technologies.

Conclusion

This paper shows that analogies, while important in simplifying and explaining complex concepts of quantum computing to a wider audience, can impact public and academic perceptions. The spectrum of language used in the analyzed texts ranges from showing quantum computing as a revolutionary advancement to warning of its potential threats to cybersecurity. These word choices reflect the authors' understanding and stance on the subject and also influence the reader's perception and understanding of quantum computing's role in cybersecurity.

This study can go further than academic discussion, talking about policy-making, technology development, and public understanding as the language used in scientific papers can sway policy decisions and the general public's attitude towards new technologies. This means, authors and researchers have a responsibility in choosing their words and metaphors. Analogies, while powerful tools for explanation, should be used with much thought behind, to ensure they do not oversimplify or misrepresent complex technological concepts.

However, the study also acknowledges certain limitations. The interpretation of analogies can be subjective, as different people can understand analogies very differently. Also, the growing field of quantum computing means that discussions and analogies may quickly become outdated, which means newer and newer language will keep being used on the topic, and older analogies will be outdated.

This research shows the need for responsible language use in scientific discussions, particularly in fields involving complex technologies like quantum computing. By

acknowledging the power and limitations of analogies in scientific literature, researchers and authors can contribute to a more informed discussion on quantum computing and its role in cybersecurity. This informed approach is valuable for describing scientific topics and also very important in creating responsible research, innovation, and policy-making of new technological eras.

Works Cited

Anderson, J. M., Anderson, S. R., Antal, L., Böhm, R., Carrier-Duncan, J., Chomsky, N., Clements, G. N., Cook, W. A., Crain, S., Culicover, P. W., Davidson, A., & Dik, S. C. (2002, July 22). Structural analogy and case grammar. Lingua. https://www.sciencedirect.com/science/article/pii/0024384186900355

Bechtel, M., & Briggs, B. (2023, December 6). *Defending reality: Truth in an age of synthetic media*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2024/tech-trends-combining-AI-with-quantum-computing-to-increase-cyber-security.html

Boutin, C. (2023, August 24). NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers | NIST. National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

Denning, D. (2019, June 14). *Is quantum computing a cybersecurity threat?*. American Scientist. https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat

Grabenstein, H. (2022, April 1). *Our private health information may be the target of a cyberattack. Are U.S. hospitals ready?* PBS. Retrieved October 12, 2023, from https://www.pbs.org/newshour/nation/our-private-health-information-may-be-the-target-of-a-cyberattack-are-u-s-hospitals-ready

Kumar, V., Bhat, S., Pedanekar, N. (2014). Automatically Retrieving Explanatory Analogies from Webpages. In: de Rijke, M., et al. Advances in Information Retrieval. ECIR 2014. Lecture Notes in Computer Science, vol 8416. Springer, Cham. https://doi.org/10.1007/978-3-319-06028-6_45

Lee, M. (2021, July). *Quantum computing and Cybersecurity*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

Rjaibi, W., Muppidi, S., & O'Brien, M. (2018, July 18). Quantum computing and cybersecurity: How to capitalize on opportunities and sidestep risks. IBM. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantumsecurity

Team, D. (2023, August 21). *Analogy: Understanding definition, examples & applications*. Daisie Blog. https://blog.daisie.com/analogy-understanding-definition-examples-applications/

Wallden, P., & Kashefi, E. (2019, April 1). *Cyber security in the Quantum Era*. ACM. https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext

What is analogy? definition and examples of analogy in literature - 2023. MasterClass. (2021, September 29). https://www.masterclass.com/articles/what-is-analogy