Scientific Research Publishing

Journal of Information Security, 2024, 15, 340-354
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Formulating and Supporting a Hypothesis to Address a Catch-22 Situation in 6G Communication Networks

Fazal Raheman

Blockchain 5.0 Ltd., Kesklinna Linnaosa, Tallinn, Estonia
Email: drfazal@bc5.eu

How to cite this paper: Raheman, F. (2024) Formulating and Supporting a Hypothesis to Address a Catch-22 Situation in 6G Communication Networks. *Journal of Information Security*, **15**, 340-354.
https://doi.org/10.4236/jis.2024.153020

Received: May 6, 2024
Accepted: July 7, 2024
Published: July 10, 2024

Abstract

2030 is projected as the year for the launch of the 6G (sixth generation) telecommunication technology. It is also the year predicted to introduce quantum computers powerful enough to break current cryptography algorithms. Cryptography remains the mainstay of securing the Internet and the 6G networks. Post quantum cryptography (PQC) algorithms are currently under development and standardization by the NIST (National Institute of Standards and Technology) and other regulatory agencies. PQC deployment will make the 6G goals of very low latency and low cost almost unachievable, as most PQC algorithms rely on keys much larger than those in classical RSA (Rivest, Shamir, and Adleman) algorithms. The large PQC keys consume more storage space and processing power, increasing the latency and costs of their implementation. Thus, PQC deployment may compromise the latency and pricing goals of 6G networks. Moreover, all the PQC candidates under NIST evaluation have so far failed, seriously jeopardizing their standardization and placing the security of 6G against the Q-Day threat in a catch-22 situation. This report formulates a research question and builds and supports a research hypothesis to explore an alternate absolute zero trust (AZT) security strategy for securing 6G networks. AZT is autonomous, fast, and low-cost.

Keywords

6G, Quantum Computing, PQC, Latency, Cost

1. Introduction

Hypotheses have a very important place and role in fundamental research [1]. In science and technology, everything moves around the hypothesis [2]. It is the

quintessence of the scientific research context, and its role has a central place and a special meaning in science. The hypothesis often becomes a basis for defining the next steps and dictates and leads the whole process of scientific research. Although the methods of hypothesis-generating research are less rigorous, they do not replace or undermine more rigorous hypothesis-testing or hypothesis-proving research methodologies. Building a hypothesis is important in building new paradigms that lay the foundation for discoveries. Except for a few rare, serendipitous inventions, almost all discoveries the world has ever seen begin with a **HYPOTHESIS**. Whether a hypothesis is eventually proven or disproven, it never loses its importance as the beginning of a journey to new knowledge. Historically, hypothesis-generating research has facilitated inventions that may not have been possible otherwise [3]. This report isn't hypothesis-testing or hypothesis-proving research designed to empirically answer a known research question [4]. It is an analysis that builds the hypothesis and formulates a research question that researchers can design their studies to answer.

1.1. Research Background and Research Methodology

This research adopts a narrative and integrative literature review approach, suitable for an entirely new subject matter that needs further exploration [5]. The exponential simultaneous growth of quantum computers (QC) and telecommunication networks offers new opportunities and problems. Through this review, the study aims to generate new perspectives on the security implications of QC on the projected technical specifications of 6G networks.

Formulating the research question is the first step in the research process and provides the foundation for framing the hypothesis. The research question should be feasible, interesting, novel, ethical, and relevant (FINER). Applying the FINER criteria can assist with ensuring that the question is valid and will generate new knowledge that has a global impact [6]. One such research question finds two next-generation technologies in conflict, substantially impacting the future of smart cities. Those technologies are quantum computers (QC) and 6G networks, which are projected to premiere in 2030. The development of these technologies happens in tandem with the development of smart cities, which are built on the principle of increased connectivity, networkability, and computing speed of the digital infrastructure. Quantum computers have shown that they can process certain tasks exponentially faster than classical computers. In late 2019, Google claimed it solved a problem that would take 10,000 years for the world's fastest supercomputer using a QC within 3 minutes [7]. Quantum computers are so powerful that they can cause havoc with encryption. The public key-based cryptographic algorithms and Elliptic Curve Cryptography (ECC) certificate protocols behind many currently used cryptographic schemes can be broken using QC [8], posing an existential threat to humanity [9]. Quantum computers also render the 6G networks vulnerable [10]. While many cybersecurity experts warn about the threat of "harvest now and decrypt later" (HANDL) attacks, few attest that they're already happening. Cybercriminals may already be

hoarding data for when QC becomes powerful enough to break current encryption standards [11]. Data is projected as the new fuel for the 21st century. It must be produced, stored, and transmitted securely and efficiently. 6G will soon be the backbone of our future societies [12]. Any vulnerability to the 6G networks needs to be urgently addressed.

This research identifies a potential catch-22 situation in developing 6G networks and generates two research questions to build and support a hypothesis. Section 1.2 articulates a problem statement that the state-of-the-art needs to resolve to mitigate the 6G security problem originating from the introduction of quantum computing. Section 1.3 presents an analysis of the problem. Section 1.4 describes the purpose of this research in the form of research questions that this paper attempts to answer and briefly presents a concise summary of the related work. In Section 1.2, the state-of-the-art is challenged with the research questions that set the backdrop for this paper. Section 2 frames the hypothesis that eliminates the complexities ingrained in legacy systems to build support for the quantum-safe hypothesis on the future of 6G security. Sections 2.1 and 2.2 review the AZT (Absolute Zero Trust) approach and its impact on the efficiency of the 6G network. Section 3 lays down the limitations of this study. Section 4 discusses the possible future if this research meets its goal and opens up a debate amongst 6G researchers for testing and proving the hypothesis.

1.2. Problem Statement: The Catch-22 Situation

Research on 6G networks currently faces a catch-22 situation, perhaps not envisaged when the 6G targeted parameter goals were planned [12]-[14]. However, as we approach the QC era, the security threats to 6G networks from QC have become real [11], resulting in new challenges in achieving at least three of the eight 6G goals, as illustrated in **Figure 1** (highlighted in red-colored circles) and listed herein:

1) 1000 times lower cost compared to 5G,
2) Reliability Resilience, Security on account,
3) Very low latency.

1.3. Problem Analysis

6G networks face diverse challenges, such as resource-constrained mobile devices, difficult wireless resource management, high complexity of heterogeneous network architectures, explosive computing and storage requirements, and privacy and security threats. 6G is targeted as a global communication facility with approximately 1 Tb/s user bit rate and less than 1 microsecond latency [13]. Zhang et al argue that 1000 times price reduction from the customer's viewpoint is the key to the success of 6G [14] (**Figure 1**). The simultaneous advent of QC and 6G compels the upgradation of network security as the powerful QC will be able to break the current encryption standards. Given the projected arrival of fully functional QC by 2030 and the projected timeline for the 6G launch, there's an urgent need to bolster defenses against Q-Day threats to 6G networks. Com-

munication security experts aggressively pursue Post Quantum Cryptography (PQC), so NIST (National Institute of Standards and Technology) is standardizing the PQC algorithms to get them production-ready. However, PQC development faces two types of obstacles.

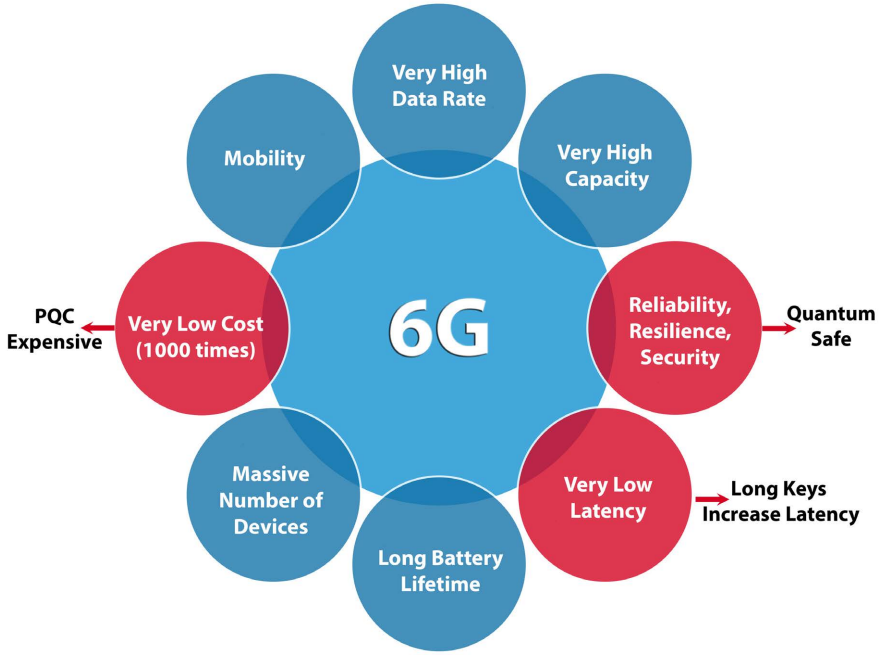

Figure 1. Impact of quantum computing on the projected goals of 6G networks.

1) Firstly, none of the 82 candidate PQCs in NIST's standardization initiatives so far have proven to be unbreachable [15].

2) Secondly, the PQC deployment will make the 6G goals almost unachievable as most PQC algorithms rely on keys much larger than those in classical algorithms and will likely have a higher computational cost than the current RSA methods. These large keys consume more storage space and processing power, increasing the time and costs of their implementation. There are substantial storage and computational costs and latency implications of PQC depending on the length of the keys ciphertext and signature size, the computational efficiency of their encryption, encapsulation, signature verification and private key decryption, decapsulation, and signing operations.

Not counting its operational cost or energy efficiency, a recent high-performance implementation of CRYSTALS-Dilithium achieved the best-known latency as low as 16.8 microseconds on an Artix-7 at 142 MHz chip [16]. This is manifold higher than the 1-microsecond target set for 6G networks. Moreover, PQCs are computationally expensive [17] and a likely obstacle to the desired 1000 times price reduction [14].

If the current obstacles to PQC standardization are overcome and PQC succeeds in NIST's standardization process, the critical challenge of latency and cost containment looms large over 6G networks. These networks demand ultra-low

latency (beyond current PQC capabilities) to power real-time applications seamlessly. Therefore, cybersecurity solutions that offer blazing-fast, low-latency performance are undeniably crucial. Regardless of the fate of PQC algorithms in the NIST standardization initiative, the urgency of such solutions remains paramount in fortifying future 6G networks against quantum threats.

1.4. Purpose of the Research and Related Work

The existing systems cannot handle the ever-growing latency and connectivity needs of the Internet of Everything. 6G communication networks are expected to provide global coverage, enhanced spectral/energy/cost efficiency, better intelligence level and security, etc. To meet these requirements, 6G networks will rely on several new enabling technologies, *i.e.*, air interface and transmission technologies and novel network architecture, such as waveform design, multiple access, channel coding schemes, multi-antenna technologies, network slicing, cell-free architecture, and cloud/fog/edge computing [18]. To build an intelligent and open 6G network, each node should have sufficiently low-latency communication and computing resources to support low-cost, self-evolving intelligent operations. The data rate will triple in 6G, be fifty times quicker than the quickest 5G network with a tenth of the latency, support the range of devices ten times, and be more reliable. 6G will be able to connect everything, integrate different technologies and applications, support holographic, haptic, space, and underwater communications, and it will also support the Internet of Things. The future networks' design is anticipated to balance technological innovation, economic and environmental sustainability, and human-centric values.

In next-generation networks, everything will be fully connected, fulfilling the requirements of ubiquitous connectivity over wireless networks. This rapid growth will transform the world of communication with more intelligent and sophisticated services and devices, leading to new technologies operating over very high frequencies and broader bands. To achieve the objectives of the 6G networks, several key technology enablers need to be performed, including massive MIMO (Multiple-Input Multiple-Output), software-defined networking, network function virtualization, vehicular to everything, mobile edge computing, network slicing, terahertz, visible light communication, virtualization of the network infrastructure, and intelligent communication environment [19]. To achieve those goals, 6G will have several new paradigm shifts. Security is the most challenging of them. Early 6G researchers often ignored the impending threats to this encryption-dependent communication network from Quantum Computers (QC), which are becoming more real with each passing day. The situation will worsen when QC with sufficient qubits arrives to break current encryption algorithms. The Cloud Security Alliance launched a countdown to Y2Q (years to quantum) that predicts just under six years until QC can crack current encryption [20]. They pick April 14, 2030, as the deadline by which the world must upgrade its IT infrastructure to meet the Y2Q threat (**Figure 2**). Even

NATO and the White House recognize the threat and are preparing for Y2Q [21]. In April 2021, the Ransomware Task Force, a group of industry experts, submitted a report entitled "*Combatting Ransomware—A Comprehensive Framework for Action*" to the US government [21]. On May 12, 2021, in response to this report, President Biden [22] issued an Executive Order entitled "*Improving the Nation's Cybersecurity*," which requires that the US advance towards a "*Zero Trust Architecture*," as described by the NIST (National Institute of Standards & Technology) [23]. However, even the standard Zero Trust architecture, which remains policy-based, may not be enough for autonomous networks like the 6G [13].

Figure 2. Countdown to Q-Day (Y2Q). Credit: Cloud Security Alliance [20].

QC wields unprecedented computing power, posing a formidable threat to future 6G infrastructure. Their ability to break traditional encryption could compromise the security of sensitive data transmitted over 6G networks. As QC seems so close to becoming a reality, any cybersecurity strategy ignoring QC may be short-sighted. QC will never replace classical computers for real-world general-purpose tasks, nor are they intended to do so. QC will become integral to high-performance computing (HPC) for specialized use cases only for various important scientific tasks [24].

To safeguard the future of communication, quantum-resistant security standards are imperative. The global response to the impending Q-Day threat is evident in initiatives such as NIST's program for developing quantum-safe encryption standards, which began in November 2017 with the submission of 82 candidates for post-quantum cryptography (PQC) algorithms. PQC is being aggressively developed to secure our cryptography-dependent digital infrastructure in a Zero Trust (ZT) cloud computing continuum recommended by NIST [25]. In 2019, the results of its first round of 82 PQC candidates entering the standardization process were published [26]. In 2022, two of the four finalist PQC candidates were demolished by ethical hackers using standard computing devices, sending a shockwave within the cybersecurity community. Last year, a Swedish group [27] and a French team of cryptographers cracked the remaining finalist PQCs (CRYSTALS-Kyber and CRYSTALS-Dilithium) [28]. PQCs [29], particularly the NIST finalist, Kyber [30], remain vulnerable to side-channel attacks. With all the PQC candidates failing, NIST's standardization process is seriously jeopardized. QC indeed appears more detrimental to human interests than the

benefits it delivers [31]. A solution is therefore urgently needed.

PQC is the only defense currently explored by researchers and regulatory authorities to secure the Internet from the Q-Day threat. Although computer security heavily relies on cryptography, recent evidence indicates it can transcend beyond encryption by deploying ZVC (Zero Vulnerability Computing) technology [32]. A series of recent reports disclose a novel way to deal with the impending Q-Day threat by segregating all QC activities from mainstream Internet instead of deploying resource-intensive PQC on every Internet device [15] [32] [33]. It deployed a new Zero Vulnerability Computing (ZVC) paradigm that proposed a new computer architecture banning all third-party permissions to reduce the computer's attack surface to zero and achieve zero vulnerability [15] [32]-[35]. This approach delivers QC services to customers in a Quantum-as-a-Service (QaaS) business model [33] [34]. ZVC is an encryption-agnostic approach that can potentially render computers quantum-resistant by banning all third-party permissions, a root cause of most vulnerabilities. A 6G security approach can potentially expound on the principal objective of designing a ZVC computing environment that eliminates the complexities of the traditional multi-layered architecture of legacy computing devices and builds a minimalist, compact Solid-State Software on a Chip (3SoC) device that's robust, resilient, energy efficient, and with zero attack surface, rendering it resistant to malware, as well as future Q-Day threats [15] [32]-[35].

2. Framing the Hypothesis

This is hypothesis-generating research designed to generate and formulate a new research question. It is not a hypothesis-testing or hypothesis-proving research designed to empirically answer an already known research question [1]-[4]. The methods of hypothesis-generating research are less rigorous and do not replace or undermine more rigorous hypothesis-testing or hypothesis-proving research methodologies. Nevertheless, they are important in building new paradigms that lay the foundation for discoveries. Almost all discoveries begin with a hypothesis. Whether a hypothesis is eventually proven or disproven, it never loses its importance as the beginning of a journey to new knowledge that would not have been possible otherwise [3].

2.1. Generating the Exploratory Research Questions

Based on the latest peer-reviewed evidence on QC and its impact on 6G security via resource-intensive post quantum cryptography (PQC), the following research question is reasonable to explore:

Will the advent of quantum computers make the latency and pricing goals of 6G networks unachievable?

An affirmative answer to this question leads to exploring an approach to mitigate the adverse impacts of QC on 6G, which leads to a second research question:

Can Absolute Zero Trust (AZT) security architecture deliver autonomous quantum-safe security to 6G networks to guarantee its latency and price reduction goals?

In a structured research methodology, a hypothesis must be formulated, supported, tested, and validated to answer a research question unequivocally. Hence, a hypothesis is formulated and framed to answer the second question and render the concept a technological reality.

2.2. Formulating and Supporting the Hypothesis

Hypothesis: Absolute Zero Trust security architecture delivers autonomous quantum-safe security to 6G networks, guaranteeing their latency and price reduction goals.

In 2020, NIST defined Zero Trust as "*a term for an evolving set of cybersecurity paradigms that move defenses from traditional static, network-based perimeters to focus on users, assets, and resources* [36]." Zero Trust Architecture is proposed for securing 6G networks [37]. However, as illustrated in **Figure 3**, all Zero Trust initiatives are policy-based and cannot be autonomous unless empowered by AI [38] [39]. 6G is not just a communication technology but a backbone of all of a smart city's heterogeneous computing needs. It enables the future metaverse with sensors and IoT devices that need continuous autonomous control. Therefore, 6G networks must be autonomous. Hence, Zero Trust Artificial Intelligence is considered an essential component of 6G [40].

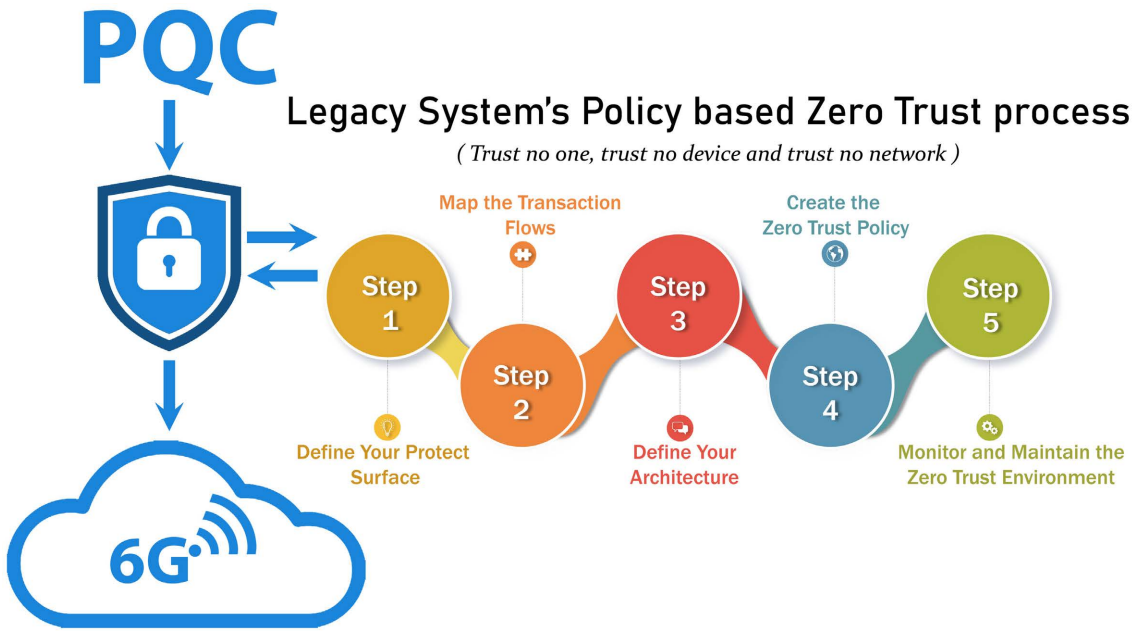

Figure 3. PQC implemented via standard Zero Trust architecture (policy based) increases the cost and latency of the 6G network.

A recent report discloses a seamless and autonomous absolute zero trust (AZT) security framework that runs continuously and autonomously without

monitoring the network [15] [41]. Such AZT is encryption agnostic and, therefore, quantum resistant. It is also light, energy-efficient, fast, and low-cost (Figure 4) as it does not rely on resource-intensive PQC.

Figure 4. 6G network secured via AZT is autonomous, fast, energy-efficient, and low-cost.

It is projected that by 2030, when 6G and QC are expected to be deployed, more than 100 trillion sensors will be manufactured and connected to the Internet [42]. Specifically, by examining previous generations of wireless communications, experts predict that 6G networks will offer a wireless connection for less than 0.1 US dollars/year, a 1000 times price reduction compared with conventional 5G systems. Hence, Zhang *et al.* concluded that a 1000-times price reduction, approaching 0.1 US dollars/year per connection for 6G, will be necessary to maintain the sustainable development of the smart society [12]. All the evidence suggests that QC is experiencing an inflection point [15] [34] [43] [44], compelling us to prepare for this new computing paradigm. Recent setbacks may jeopardize the original NIST timeline for PQC standardization, which was originally estimated at 15 years (2034) in 2019 for a full transition to a Quantum-safe Internet (Figure 5). Moreover, global PQC implementation is a massive undertaking that impacts each computing device in the entire Internet ecosystem. It is not just time-consuming but resource-intensive and expensive. By prioritizing developing and implementing cybersecurity solutions optimized for minimal latency, stakeholders can ensure the robustness and efficiency of 6G networks amidst the ever-evolving landscape of quantum technologies.

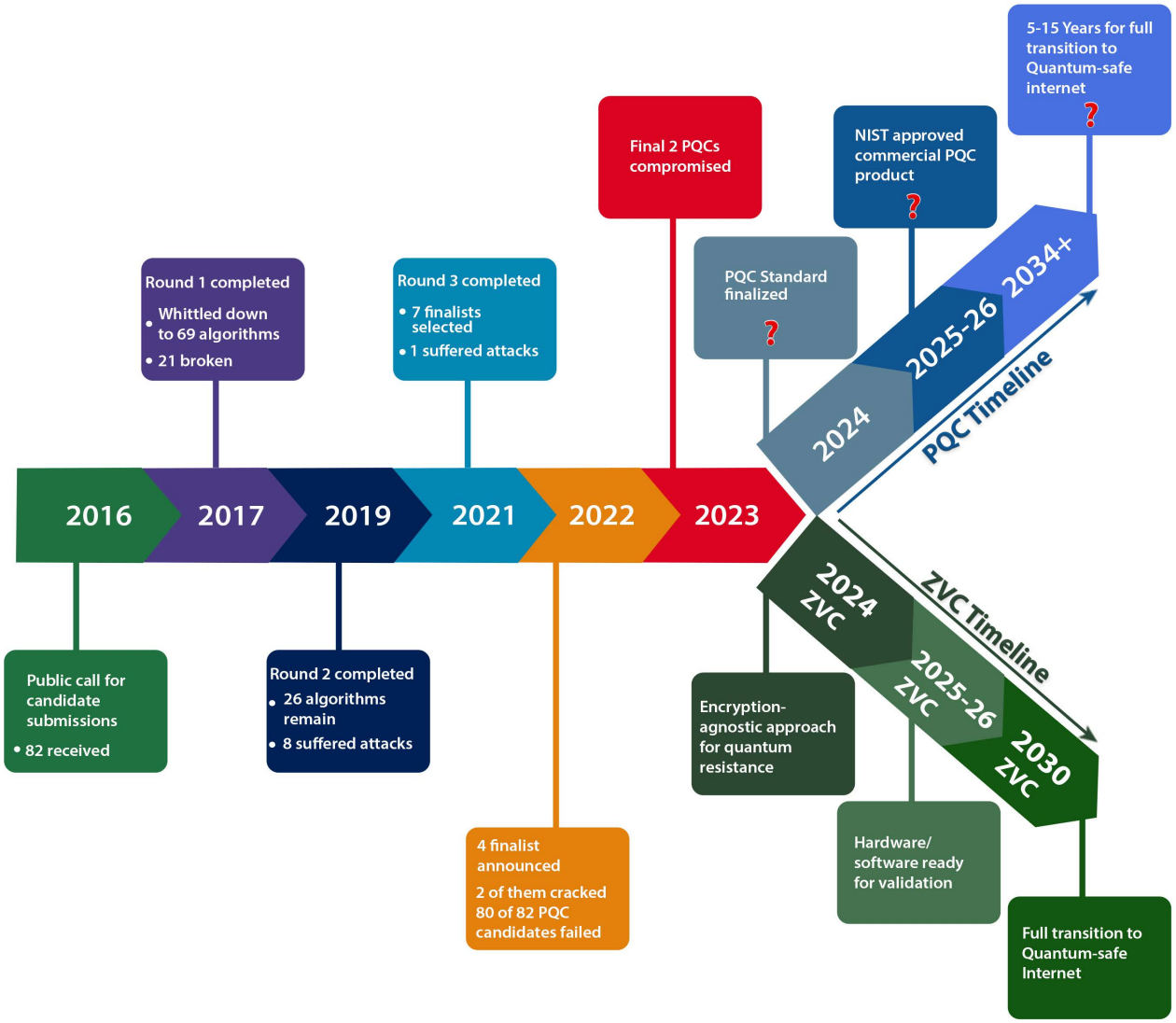

Figure 5. AZT Timeline in comparison to PQC and 6G. Adapted from Raheman F. Tackling the existential threat from quantum computers and AI [45].

3. Limitation & Caveats

This is not a hypothesis testing/validating research, which most peer-reviewed literature is, and should be. However, that does not underplay the importance of hypothesis-building research, on which almost all peer-review piggybacks for building the foundation of new knowledge [1]-[4]. You can't comprehensively test or prove a concept without methodologically framing and building a hypothesis for a new concept. More so when the subject matter is as hot and time-sensitive as Quantum Computing and 6G. This hypothesis-building research explicitly emphasizes the conceptual stage of the research and does not claim to be an improvement on an earlier report. The principal objective of this research is to make the hypothesis available to a broader community of 6G researchers for testing and proving or disproving it to help shape the future of 6G. This report is clearly no more than hypothesis-generating research intended to

build and formulate a hypothesis that researchers worldwide can design and investigate experiments to test and prove or disprove in the near future. Until such studies are conducted, great care should be taken to extrapolate the findings of this report to real-world settings [45]. Such studies begin by defining the specific research questions. What the process will be. What protocols will be designed to implement the process? What KPIs will be appropriate to evaluate and control the protocols [45]? Those and many other questions come to mind when planning the future of our 6G-powered digital infrastructure.

4. Conclusions

6G communication networks are envisioned to nurture the future of a ubiquitously connected data-intensive intelligent ecosystem powered by the complete automation of wireless networks spread across the ground, underwater, air, and space. Moreover, 6G is also envisaged to deal with the explosive growth in mobile traffic, which is estimated to be several 100 billion gigabytes (GB)/month by 2025 and trillions of gigabytes (GB)/month by 2030 [46] for emerging data-intensive speculative applications [47] within metaverse, AI and autonomous mobility space [48]. To serve these future applications better by seamlessly interconnecting a staggering number of heterogeneous devices, the next generation of mobile networks are, by and large, expected to be inherently softwarized, virtualized and cloudified systems [49]. Quantum computers slated to premiere around the same time in 2030, will adversely impact the security of such softwarization, virtualization, and cloudification of mobile networks, making it challenging to meet the projected 6G parameter goals.

This report contributes to the discourse on securing 6G networks without compromising their latency and pricing goals. The principal objective of this research is to identify the most serious pain points that 6G development is facing on account of QC, which is currently perceived as an existential risk to humanity by many experts. The research conducted a thorough literature review to generate a clearly articulated hypothesis that provides a credible path to mitigating the 6G pain points in a timely manner.

The empirical evidence in peer-reviewed literature provided enough basis to support the above hypothesis and afford sufficient motivation for 6G and QC researchers to further research to test and prove the hypothesis. This work introduces new ideas, new thinking, and a new understanding of network security, which can be helpful to researchers, thinkers, 6G and cybersecurity developers, regulators, and practitioners working to secure the future Internet.

Future research may be directed toward testing and proving the hypothesis to achieve adequate security of 6G, maintaining its latency and pricing goals. The concept enshrined in the hypothesis may invite more academic interest in peer review or grant writing, but they may not be too conducive to making any immediate real-world business decisions. They may face technological challenges until the concepts get rooted in our empirical multidisciplinary research me-

thods. This article intends to spark and encourage further, in-depth discussion around these topics as we owe the researchers and policymakers a clear vision of the future. As cyber threats to our digital infrastructures continue evolving, such research is crucial in ensuring the integrity and confidentiality of information across the Internet, reinforcing the overall cybersecurity landscape of our digital infrastructures.

Acknowledgements

The author is grateful to Tejas Bhagat and Sadiya Khan for their assistance in preparing this manuscript.

Conflicts of Interest

The author declares no conflict of interest.

References

[1] Kell, D.B. and Oliver, S.G. (2004) Here Is the Evidence, Now What Is the Hypothesis? The Complementary Roles of Inductive and Hypothesis-Driven Science in the Post-Genomic Era. *Bioessays*, **26**, 99-105. https://doi.org/10.1002/bies.10385

[2] Bulajic, A., *et al.* (2012) The Importance of Defining the Hypothesis in Scientific Research. *International Journal of Educational Administration and Policy Studies*, **4**, 170-176. https://doi.org/10.5897/ijeaps12.009

[3] Biesecker, L.G. (2013) Hypothesis-Generating Research and Predictive Medicine. *Genome Research*, **23**, 1051-1053. https://doi.org/10.1101/gr.157826.113

[4] Hartwick, J. and Barki, H. (1994) Research Report—Hypothesis Testing and Hypothesis Generating Research: An Example from the User Participation Literature. *Information Systems Research*, **5**, 446-449. https://doi.org/10.1287/isre.5.4.446

[5] Raheman, F. (2022) Sharonomics: A Radical Economic Theory for the Next Industrial Revolution and Beyond. *Theoretical Economics Letters*, **12**, 1710-1748. https://doi.org/10.4236/tel.2022.126094

[6] Willis, L.D. (2023) Formulating the Research Question and Framing the Hypothesis. *Respiratory Care*, **68**, 1180-1185. https://doi.org/10.4187/respcare.10975

[7] Gibney, E. (2019) Hello Quantum World! Google Publishes Landmark Quantum Supremacy Claim. *Nature*, **574**, 461-462. https://doi.org/10.1038/d41586-019-03213-z

[8] Maheshwari, A., *et al.* (2023) Is Quantum Computing a Cybersecurity Threat? Quantum Computing in Cybersecurity, 353-368. https://doi.org/10.1002/9781394167401.ch21

[9] Majot, A. and Yampolskiy, R. (2015) Global Catastrophic Risk and Security Implications of Quantum Computers. *Futures*, **72**, 17-26. https://doi.org/10.1016/j.futures.2015.02.006

[10] Ulitzsch, V.Q., Park, S., Marzougui, S. and Seifert, J. (2022). A Post-Quantum Secure Subscription Concealed Identifier for 6G. *Proceedings of the* 15*th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, San Antonio, 16-19 May 2022, 157-168. https://doi.org/10.1145/3507657.3528540

[11] Noone, G. (2023) Are Harvest Now, and Decrypt Later Cyberattacks Actually Happening? Tech Monitor.

https://techmonitor.ai/hardware/quantum/harvest-now-decrypt-later-cyberattack-quantum-computer

[12] Bertin, E., Crespi, N. and Magedanz, T. (2021) Shaping Future 6G Networks: Needs, Impacts, and Technologies. John Wiley & Sons.

[13] Aslam, A.M., Chaudhary, R., Bhardwaj, A., Budhiraja, I., Kumar, N. and Zeadally, S. (2023) Metaverse for 6G and Beyond: The Next Revolution and Deployment Challenges. *IEEE Internet of Things Magazine*, **6**, 32-39. https://doi.org/10.1109/iotm.001.2200248

[14] Zhang, S., Xiang, C. and Xu, S. (2020) 6G: Connecting Everything by 1000 Times Price Reduction. *IEEE Open Journal of Vehicular Technology*, **1**, 107-115. https://doi.org/10.1109/ojvt.2020.2980003

[15] Raheman, F. (2024) From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. *Journal of Computer and Communications*, **12**, 252-282. https://doi.org/10.4236/jcc.2024.123016

[16] Beckwith, Nguyen, D.T. and Gaj, K. (2022) High-Performance Hardware Implementation of Lattice-Based Digital Signatures. https://eprint.iacr.org/2021/1451.pdf

[17] Gupta, N., Jati, A., Chauhan, A.K. and Chattopadhyay, A. (2021) PQC Acceleration Using GPUs: Frodokem, Newhope, and Kyber. *IEEE Transactions on Parallel and Distributed Systems*, **32**, 575-586. https://doi.org/10.1109/tpds.2020.3025691

[18] You, X., Wang, C.X., Huang, J., *et al.* (2021) Towards 6G Wireless Communication Networks: Vision, Enabling Technologies, and New Paradigm Shifts. *Science China-Information Sciences*, **64**, Article ID: 110301.

[19] Salahdine, F., Han, T. and Zhang, N. (2023) 5G, 6G, and Beyond: Recent Advances and Future Challenges. *Annals of Telecommunications*, **78**, 525-549. https://doi.org/10.1007/s12243-022-00938-3

[20] Huttner, B. and Kalsi, M. (2022) Countdown to Y2Q: Working Group, Quantum-Safe Security. Cloud Security Alliance, March 9, 2022. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

[21] Keary, T. (2022) NATO and White House Recognized Post Quantum Threats and Prepared for Y2Q. Venture Beat, March 4, 2022. https://venturebeat.com/business/nato-and-white-house-recognize-post-quantum-threats-and-prepare-for-y2q/

[22] President Biden (2021) Executive Order on Improving the Nation's Cybersecurity. White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[23] Kerman, A., *et al.* (2020) Implementing a Zero Trust Architecture. Tech. Rep., MITRE Corp. https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf

[24] Johanssona, M.P., *et al.* (2021) Partnership for Advanced Computing in Europe Quantum Computing—A European Perspective. https://www.researchgate.net/publication/358281882_Partnership_for_Advanced_Computing_in_Europe_Quantum_Computing_-A_European_Perspective

[25] Szymanski, T.H. (2022) The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). *IEEE Access*, **10**, 45893-45930. https://doi.org/10.1109/access.2022.3169137

[26] Alagic, G., *et al.* (2019) Status Report on the First Round of the NIST Post-Quantum

Cryptography Standardization Process.
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303

[27] US Department of Commerce, National Institute of Standards and Technology: Washington DC, USA (2019).
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303

[28] Ji, Y. and Dubrova, E. (2023) A Side-Channel Attack on a Masked Hardware Implementation of Crystals-Kyber. *Proceedings of the* 2023 *Workshop on Attacks and Solutions in Hardware Security*, Copenhagen, 30 November 2023, 27-37.
https://doi.org/10.1145/3605769.3623992

[29] Berzati, A., *et al.* (2023) A Practical Template Attack on CRYSTALS-Dilithium. Cryptology ePrint Archive 2023: 50.
https://api.semanticscholar.org/CorpusID:256361429

[30] Liu, Y., Liu, Y., Zhou, Y., Gao, Y., Qiao, Z. and Wang, H. (2024) A Novel Power Analysis Attack against CRYSTALS-Dilithium Implementation. 2024 *IEEE European Test Symposium* (*ETS*), The Hague, 20-24 May 2024, 1-6.
https://doi.org/10.1109/ets61313.2024.10567325

[31] Roy, K.S., *et al.* (2024) Analyzing CRYSTALS-Kyber's Susceptibility to Side Channel Attacks: An Empirical Exploration.
https://www.researchsquare.com/article/rs-4015385/v1

[32] Laura, D. (2022) Post-Quantum Crypto Cracked in an Hour with One Core of an Ancient Xeon. The Register, 3 August 2022.
https://www.theregister.com/2022/08/03/nist_quantum_resistant_crypto_cracked

[33] Raheman, F., Bhagat, T., Vermeulen, B. and Van Daele, P. (2022) Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. *Future Internet*, **14**, Article No. 238. https://doi.org/10.3390/fi14080238

[34] Raheman, F. (2022) The Future of Cybersecurity in the Age of Quantum Computers. *Future Internet*, **14**, Article No. 335. https://doi.org/10.3390/fi14110335

[35] Raheman, F. (2022) The Q-Day Dilemma and the Quantum Supremacy/Advantage Conjecture. https://www.researchsquare.com/article/rs-2331935/v1

[36] Raheman, F. (2022) Solid State Software on a Chip (3SOC) for Building Quantum Resistant Web 3.0 Computing Devices. US Patent Application, US29/842,535, June 15, 2022.

[37] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. National Institute of Standards and Technology, Tech. Rep.
https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[38] Chen, X., Feng, W., Ge, N. and Zhang, Y. (2024) Zero Trust Architecture for 6G Security. *IEEE Network*. https://doi.org/10.1109/mnet.2023.3326356

[39] Manan, A., Min, Z., Mahmoudi, C. and Formicola, V. (2022) Extending 5G Services with Zero Trust Security Pillars: A Modular Approach. 2022 *IEEE/ACS* 19*th International Conference on Computer Systems and Applications* (*AICCSA*), Abu Dhabi, 5-8 December 2022, 1-6. https://doi.org/10.1109/aiccsa56895.2022.10017774

[40] Home, D. (2022) Leveraging Software Defined Perimeter (SDP) Software Defined Networking (SDN) and Virtualization to Build a Zero Trust Testbed with Limited Resources. Advances in Security, Networks, and Internet of Things. Springer.

[41] Ahammed, T.B., Patgiri, R. and Nayak, S. (2023) A Vision on the Artificial Intelligence for 6G Communication. *ICT Express*, **9**, 197-210.
https://doi.org/10.1016/j.icte.2022.05.005

[42] Raheman, F. (2024) Tackling the Existential Threats from Quantum Computers and

AI. *Intelligent Information Management*, **16**, 121-146. https://doi.org/10.4236/iim.2024.163008

[43] David, K. and Berndt, H. (2018) 6G Vision and Requirements: Is There Any Need for Beyond 5G? *IEEE Vehicular Technology Magazine*, **13**, 72-80. https://doi.org/10.1109/mvt.2018.2848498

[44] Bhasin, A. and Tripathi, M. (2023) Quantum Computing at an Inflection Point: Are We Ready for a New Paradigm. *IEEE Transactions on Engineering Management*, **70**, 2546-2557. https://doi.org/10.1109/tem.2021.3103904

[45] Sotelo, R. (2021) Quantum Computing Entrepreneurship and IEEE TEMS. *IEEE Engineering Management Review*, **49**, 26-29. https://doi.org/10.1109/emr.2021.3098260

[46] Raheman, F. (2024) Tackling the Existential Threats from Quantum Computers and AI. *Intelligent Information Management*, **16**, 121-146. https://doi.org/10.4236/iim.2024.163008

[47] ITU (2015) IMT Traffic Estimates for the Years 2020 to 2030. Report ITU-R M. 2370-0, ITU-R Radiocommunication Sector of ITU. https://www.itu.int/pub/R-REP-M.2370-2015

[48] Tariq, F., Khandaker, M.R.A., Wong, K., Imran, M.A., Bennis, M. and Debbah, M. (2020) A Speculative Study on 6G. *IEEE Wireless Communications*, **27**, 118-125. https://doi.org/10.1109/mwc.001.1900488

[49] Saad, W., Bennis, M. and Chen, M. (2020) A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Network*, **34**, 134-142. https://doi.org/10.1109/mnet.001.1900287