Insibidi Publishers

Research Article

Quantum Supremacy: Readiness, Risks, and Global Initiatives in Digital Security and Infrastructure

Mulima Chibuye[1]*, Jackson Phiri[2]

[1] University of Zambia; Mulima.Chibuye@cs.unza.zm
[2] University of Zambia; Jackson.Phiri@cs.unza.zm
* Correspondence:

Abstract: This paper examines the readiness of countries and organizations for quantum supremacy, expected by 2033 or sooner. As quantum computers threaten modern encryption systems, we investigate current research progress, global initiatives for infrastructure preparation, and associated risks and mitigation measures. Using resources like Google Scholar, IEEE Xplore, and ACM Digital Library, we conduct a literature review on quantum computing advancements. The study applies the Technology Acceptance Model to assess quantum computer adoption and uses the Pareto principle to analyse the top 20% of wealthy and upper-middle-income nations. We also present a case study on the United States' efforts. By exploring measures to protect digital spaces and prevent unauthorized access, this work contributes to assessing global preparedness for quantum supremacy.

Keywords: Quantum Advantage; Quantum Supremacy; Post Quantum Security; Digital Infrastructure; Cloud Computing

Citation: Chibuye, M., & Phiri, J. (2025). Quantum supremacy: Readiness, risks, and global initiatives in digital security and infrastructure. *Journal of Artificial and Data Intelligence*, 1(1).

Academic Editor: Johnson Ihyeh Agbinya

Received: October 9, 2024
Accepted: July 29, 2025
Published: September 8, 2025

1. Introduction

Quantum supremacy, is achieved when quantum computers can perform tasks impossible for classical computers [1] [2]. Unlike classical computers using binary bits, quantum computers use qubits that can exist in multiple states simultaneously. This capability poses significant risks to current encryption methods. For example, Shor's algorithm can break RSA encryption in polynomial time, with a complexity indicated in the Big O notation equation (1) below, a feat intractable for classical computers [3].

$$O((\log(n)^2 * (\log(\log(n)) * (\log(\log(\log(n))))) \quad (1)$$

This paper explores the implications of quantum supremacy, its potential impacts, and challenges. We examine policies for quantum computer development and use the Technology Acceptance Model (TAM) to assess adoption readiness. The Pareto principle is applied to select the top 20% of wealthy and upper-middle-income countries for analysis. We begin by defining digital security and infrastructure.

1.1 Digital Security and Infrastructure

Digital security encompasses measures to protect data during storage and transmission across various media. This includes personal devices like flash drives and large-scale infrastructure such as data centres and telecommunications networks. A key method for data protection is public/private key cryptography, which relies on the computational difficulty of factoring large numbers into primes. While classical computers struggle with this task, quantum computers could theoretically break these encryption methods. This capability of quantum computers poses significant security risks to current digital infrastructure and highlights the urgent need for quantum-resistant encryption techniques. As quantum computing advances, the security of internet transactions, storage media, and digital infrastructure faces unprecedented challenges, necessitating the development of robust, quantum-proof security measures.

1.2. Understanding Classical Computer

A Classical Computer is what we generally see every day. It is the computer that runs the operating system on modern smartphones; it runs Microsoft Windows and Linux operating systems. Classical Computers are based on a model called the Von-Neumann Architecture, which is a general structure of the hardware that is modularized and where each module performs specific tasks that are controlled by a Central Processing Unit. The different modules in the Von Neumann architecture are the arithmetic and logic unit, the memory unit, the central processing unit and the control unit. In most systems today, the CPU and Control are integrated components. Another distinguishing characteristic of classical computers is that they rely on an encoding of information in the form of bits or zeros and ones to represent information. It might be interesting to note that all logic and logical representations can be coded into digits, and while the most popular system in use today is the decimal system, computers use binary systems (0,1) because it is easy to create hardware that can manipulate those digits by mathematical calculations to produce output from input. Generally, all computing systems have an input source, a data processing system, and an output. Now that we have discussed what classical computers are, we can now investigate quantum computers.

1.3. Understanding Quantum Computers

A quantum computer is very different from a classical computer and does not use the Von Neumann architecture, although there are some implementations that might borrow from the Von Neumann architecture; generally, memory manipulation in quantum computers is different from classical computers. There are different types of quantum computers in experimental use and development today, and each uses a different architecture. While there are generally agreed upon standards on classical computers, there is still an ongoing race to create an efficient quantum computing architecture, hence the various types in experimental use and development today. The broad standards of quantum computers are indicated in the Table 1 below.

2. Literature Review

2.1 Types of Quantum Computers

There are six main types of quantum computers in use today, and although their technologies are still relatively novel and still being explored, it is expected that the final standards in quantum computer architecture will be based on the broad categories in Table 1 below.

Table 1. Types of Quantum Computers.

Architecture	Principle
Superconducting Quantum Computers	Uses superconducting circuits as qubits, manipulated by microwave pulses and read by measuring electrical response.
Trapped Ion Quantum Computers	Employs trapped ions as qubits, manipulated by lasers and read using photodetectors.
Topological Quantum Computers	Utilizes anyons as qubits, manipulated by braiding operations and read through anyon measurements.

Quantum Annealers	Solves optimization problems by finding lowest energy states, with qubit states inferred from system energy configuration.
Silicon Quantum Computers	Uses silicon-based qubits, manipulated by voltages or magnetic fields, and read using single-electron transistors or charge sensors.
Photonic Quantum Computers	Employs individual photons as qubits, manipulated by optical devices and read by measuring photon properties.

2.2. Progress in Quantum Computation

The concept of quantum computation was introduced by Physicist Richard Feynman, who proposed that classical computers were incapable of solving certain types of problems, such as quantum phenomena, and since the physical world was quantum in nature, he therefore proposed that instead, quantum computers be investigated for solving such problems[4]. The possibility of using quantum computers to simulate physics is possible thanks to the principle of the universality of computation. This concept is primarily associated with the Church-Turing thesis, which proposes that any calculation or computation that can be performed by a Turing machine (an abstract mathematical concept of computation) can also be performed by any other "universal" computing device given enough time and resources. Therefore, given that a quantum computer has enough resources and is a computing device, it can solve problems that a classical computer can solve. Currently, however, there are certain problems that current quantum computers cannot solve as efficiently as classical computers. However, since we can establish that quantum computers are universal computers, we know that eventually, given enough time, we will achieve quantum supremacy. However, this might not necessarily mean that all problems would be solved faster or more efficiently on a quantum computer than on a classical computer. With the background given, below is a summary in tabular form on the progress of quantum computers since the proposition by Richard Feynman.

Table 2. Selected Events in Quantum Computation.

Year	Event
1982	Theory on Quantum Computation [4]
1985	Theoretical Quantum Turing Machine is proposed
1990	Quantum error correction paved the way for practical quantum computers
1994	Shor’s algorithm shows that factoring very large numbers into their primes is possible in reasonable time which is still intractable for classical computer.
1996	Grovers algorithm, Seth Lloyd proof on simulating physics
2011	IBM Develops 2 Qubit Quantum Logic Gate
2015	IBM show quantum error correction by combining superconducting qubits in lattice arrangement
2017	IBM Create 20 Qubit machine
2018	IBM unveil 50 qubit machines
2019	Google Sycamore solves problem that would take a classical computer 10,000 years

2.3. The Technology Acceptance Model - TAM

As we will use the Technology Acceptance Model (TAM) to assess the current state of work and adoption by both nations and corporations within the quantum computing space, it is important to define what TAM is and how the rating will be conducted. TAM is a well-documented tool for assessing the acceptance and use of new technology, and it also gives an indication as to whether a certain technology is ready for adoption or not. There are 3 metrics that are used in TAM, and these are explained below.

2.4. Perceived Ease of Use

In the Technology Acceptance Model (TAM), perceived ease of use refers to how effortlessly a user expects to use a technology. For quantum computing, this is influenced by factors like the learning curve, interface usability, documentation clarity, educational resources, and technical support. Given quantum computing's complex nature, efforts to simplify interfaces, provide user-friendly tools, offer comprehensive training, and ensure robust support are crucial. Companies like IBM and Google are already offering cloud-based platforms with interactive tutorials to increase perceived ease of use. As quantum technology matures and integrates with existing IT infrastructures, its perceived ease of use is likely to increase, potentially leading to wider acceptance and adoption.

2.5. Perceived Usefulness

Perceived usefulness, the second key metric in the Technology Acceptance Model, measures how much a user believes a system will improve their performance or solve problems. For quantum computing, this relates to its potential benefits over classical computing in areas like computational speed, problem-solving, and data encryption. To be adopted, quantum computing must demonstrate clear advantages in efficiency, cost-effectiveness, versatility, or scalability. Countries or corporations will find it useful if it offers significant benefits in sectors such as data security, financial modelling, drug discovery, weather forecasting, and artificial intelligence. The perceived usefulness may vary based on specific needs, resources, and objectives, and is likely to increase as the technology matures and its applications become more evident.

3. Methodology

This paper uses a systematic literature review to attain all the highlighted objectives. Specifically, we explore the following digital libraries for our information: Google Scholar, ACM Digital Library and IEEE Explore.

3.1. Research Questions

1. What is the current progress of the quantum computing field?
2. What are the initiatives being taken globally to prepare for quantum supremacy?
3. What are the risks associated with the attainment of quantum supremacy?
4. What mitigation measures have governments and private corporations taken to prepare for quantum supremacy?

3.2. Objectives

1. To explain the current progress in quantum computing technology.
2. To explore global initiatives to make infrastructure ready for quantum supremacy.
3. To explore the risks associated with quantum supremacy.
4. To explore current mitigation measures by both governments and private corporations.

3.3. Inclusion Criteria

1. The literature must be recent, defined as having been published within the last three years.
2. The source of the material should be reputable and academically oriented, limited to Google Scholar, IEEE Xplore, and the ACM Digital Library.
3. For the ACM Digital Library, only articles with available artifacts (e.g., code, datasets, software) are included.
4. The type of material must be either journal or conference articles, encompassing reviews, case studies, and empirical and theoretical research papers.

3.4. Exclusion Criteria

1. Any work that is older than 5 years and any work from sources other than Google Scholar, IEEE Explore and the ACM Digital Library
2. Articles from sources other than Google Scholar, IEEE Xplore, and the ACM Digital Library are excluded to maintain the academic rigor of the study.
3. Any works that do not have associated artifacts on the ACM Digital Library are excluded.
4. Any literature type other than journal or conference articles, such as books, editorials, theses, and dissertations, is excluded.
5. Any similar studies already captured in the literature that do not add new or unique insights to the research are excluded.

For this research, since we are interested in the application of quantum computers specifically to technological issues, we restricted our themes to digital security and infrastructure.

Table 3. Search Strings.

Year	Event
1. What is the current progress of the Quantum Computing field?	Recent advancements in Quantum Computing OR State-of-the-art Quantum Computing technologies OR Latest developments in Quantum Computing research OR Progress and breakthroughs in Quantum Computing OR Advances in Quantum Computing hardware and software
2. What are the initiatives being taken globally to prepare for quantum supremacy?	Global efforts towards Quantum Computing readiness OR Initiatives for infrastructure development in Quantum Computing worldwide OR Global programs for preparing for quantum supremacy OR International collaborations in Quantum Computing research OR Government initiatives for Quantum Computing adoption
3. What are the risks associated with the attainment of Quantum Supremacy?	Security risks of Quantum Supremacy OR Vulnerabilities in current encryption systems due to Quantum Computing OR Implications of Shor's algorithm for RSA encryption OR Privacy risks in the era of Quantum Supremacy OR Threats to digital security posed by Quantum Computing

4. What mitigation measures have governments and private corporations taken to prepare for Quantum Supremacy?	Government strategies for Quantum Computing readiness OR Corporate initiatives in Quantum Computing security OR Policy measures to address Quantum Computing risks OR Investments in Quantum Computing infrastructure by governments OR Public–private partnerships in Quantum Computing research

4. Results

Regarding the recent advancements in quantum computing, we confined our results to information that is available in the last 5 years. What we noted on Google Scholar was that the results after the 10th page were not concerned with our search strings and were very generic, while the results in the ACM Digital Library and IEEE Xplore were much more targeted. However, we also noted that the 2 journal and conference sites provided much more useful information that was also ordered automatically according to the relevance of our search strings. ACM and IEEE Xplore also had results that were not concerned with our targeted search strings by on average the 2nd page. It can also be noted that the number of overall results was greater on Google, followed by ACM and IEEE Xplore. We also noted that the results in the ACM Digital Library were the same for the first 2 research questions.

4.1. Progress on Quantum Computers, Global Initiatives, Risks and Mitigation Measures

This section addresses the research questions and objectives regarding the current progress on quantum computing, the initiatives to prepare for the advent of quantum supremacy or quantum advantage, the risks associated with quantum supremacy and the mitigation measures being undertaken by governments and corporations to prepare for quantum supremacy. We present our results in tabulated format. The number of articles found in each case was analysed from the abstract, and those that fell within the specific criteria of the needed themes are indicated in Table 4 which illustrates the significant research gap in quantum computing related to infrastructure and digital security themes. While Google Scholar yielded the most articles, the relevance of the results was notably lower compared to specialized databases like the ACM Digital Library and IEEE Xplore. This discrepancy highlights the need for targeted research efforts focusing on practical applications, especially in developing quantum-resistant digital infrastructures. The search strings used are indicated in Table 3 - Search Strings. We focused on practical applications of quantum computing that have been proven to directly affect our assessment based on the technology acceptance model. The results were then filtered first from the title and then from the abstract. Furthermore, those results that were selected from the abstracts were analysed to determine whether they addressed the two key points of our research, namely, whether they addressed themes associated with digital security or issues surrounding infrastructure post-Quantum Supremacy.

Table 4. Progress in Quantum Computing – Objective 1.

Source	Total Results from search	Theme - Infrastructure
Google Scholar	16,700	[5], [6], [7], [8], [9], [10], [11]
ACM Digital Library	3,068	[12]
IEEE Xplore	251	[13], [14], [15]

Table 5. Preparation for Quantum Supremacy - Objective 2.

Source	Total Results from search	Theme - Infrastructure
Google Scholar	11,900	[16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30]
ACM Digital Library	3068	[12]
IEEE Xplore	14	[31], [32]

Table 6. Risks associated with Quantum Supremacy.

Source	Total Results from search	Theme - Infrastructure
Google Scholar	59	[33], [34], [35]
ACM Digital Library	3066	-
IEEE Xplore	7	[36]

Table 7. Risks associated with Quantum Supremacy.

Source	Total Results from search	Theme - Infrastructure
Google Scholar	7000	[27], [37], [38]
ACM Digital Library	3788	-
IEEE Xplore	-	-

4.2. Analysis of Table 4 to Table 7 Results

Google Scholar consistently yielded the highest total results across all categories, significantly outperforming ACM Digital Library and IEEE Xplore. However, the number of articles relevant to digital security and infrastructure themes was notably lower than the total results. This discrepancy highlights a significant gap between the volume of quantum computing research and its relevance to critical areas of digital security and infrastructure. The underrepresentation of these themes in quantum supremacy research indicates a pressing need for increased focus from academia, industry, and policymakers. The apparent deficit in research on preparing infrastructure for quantum computing is particularly concerning. As quantum technology evolves, the strain on current infrastructure will increase. Without adequate preparation, we risk being ill-equipped to harness quantum technology's full potential when it becomes available. It is crucial for the global community, especially governments, corporations, and academia, to prioritize digital security and infrastructure in quantum computing research. This focus would help mitigate potential risks and facilitate a smooth transition into the quantum era.

4.3. Quantum Computer Adoption

Here, we look at the state of adoption or work being done on QC by the top 20% of wealthiest nations and middle-income nations, respectively. As a start, we obtain our results for the wealth of nations from the World Bank 2021 report, which, in addition to using GDP as a measure of a nation’s progress, also expands the nature of wealth to include the estimated combined known natural resource wealth that can be exploited in the interim[39]. It also classifies countries into 4 categories as high-income, upper middle-income, lower middle-income and low-income countries, as indicated in Table 8 below. When we apply the Pareto principle to the top 20% of wealthy nations and the top 20% of middle-income nations based on 2018 and 2022 data provided by the World Bank, we have the following list of countries in Table 9 that are reviewed in this work and assessed using the technology acceptance model (TAM) as concerns quantum computing.

The Technology Acceptance Model (TAM) was selected due to its robust framework for evaluating user readiness and acceptance of emerging technologies. TAM has been extensively validated and stands as a leading scientific paradigm for explaining and predicting user acceptance across a spectrum of technological deployments[40]. The Pareto principle was employed to focus on the top 20% of high-income and upper-middle-income countries, as these nations are likely to lead quantum technology advancements. This approach ensures that the analysis is both targeted and impactful, highlighting the critical disparities and opportunities in quantum computing readiness. We use the Pareto principle to prioritize the most impactful elements within our study, a scientifically validated method widely employed across various research and management disciplines especially if the data is Paretian on analysis[41], [42].

Table 8. Risks associated with Quantum Supremacy.

Group	July 1, 2022, for FY23 (new)
Low Income	<1,045
Lower-middle income	1,046-4,095
Upper-middle income	4,096-12,695

Table 9. Analysed Countries - TAM - Quantum Computing.

Country	Classification	Estimated Wealth – GNI Per Capita
United States	High Income	$65,283
Switzerland	High Income	$63,020
Norway	High Income	$62,280
Ireland	High Income	$61,640
Luxembourg	High Income	$61,080
Iceland	High Income	$60,960
Denmark	High Income	$59,410
Netherlands	High Income	$58,560
Sweden	High Income	$57,830
China	Upper Middle Income	$11,590
Brazil	Upper Middle Income	$10,110
Mexico	Upper Middle Income	$9,750
Turkey	Upper Middle Income	$9,380
Argentina	Upper Middle Income	$8,820
Colombia	Upper Middle Income	$8,630
South Africa	Upper Middle Income	$8,560
Indonesia	Upper Middle Income	$8,420
Thailand	Upper Middle Income	$8,320

4.4. Applying TAM to Selected Countries

The approach to assess the Technology Acceptance Model for the selected countries in Table 9 above follows the flow indicated below. We term these assessment criteria numbered AC1 to AC4.

1. Check whether corporations in those countries or governments have a quantum computing policy or initiatives. This was done by Google and Microsoft Bing searches and focused only on sources that were only corporate or government information.
2. Check if actual work is being done to build quantum computers, this helped us identify whether we can then answer the question as to the ease of use, which would

not make sense if there were currently no initiative to build a quantum computer or no existing quantum computer in place.

3. Generally, technology that is at the point at which it is classified as easy to use would be adopted by a sizeable number of individuals outside the R&D space, and this can be seen by studies such as the Gartner Hype Cycle[43], [44]. Therefore, we check through search engines whether there is some level of adoption other than use within the R&D space.

4. To assess the final point, which is the usefulness of the technology, we again see if there are practical applications underway by corporations or those selected governments to solve real-world problems. In each country's case, we ask if there are practical solutions to known real-world problems, and if yes, we ascertain that the technology is useful.

5. If the answer to all 4 questions above was yes and there was proof through searches on the internet, we concluded that the country was ready to embrace quantum computing.

Respective search strings for each of the 5 points are indicated in Table 10 below. As highlighted earlier, searches were conducted on Google and Bing. Search results must then be manually analysed to filter only those that fit the inclusion criteria, such as sources from official corporate or government websites.

Table 10. TAM Search Strings.

SN	Search String
1	government or corporate quantum initiative [COUNTRY NAME]
2	building quantum computer or planning [COUNTRY NAME]
3	Quantum computing as a service, public access [COUNTY NAME]
4	Practical quantum computer use [COUNTRY NAME]

Table 11. TAM Results.

Country	AC1	AC2	AC3	AC4	TAM Readiness
United States	Yes[45]	Yes	Yes	Yes	Yes
Switzerland	Yes	Yes	Yes	Yes[46]	Yes
Norway	Yes	Yes	Yes	-	No
Ireland	Yes	Yes	Yes	Yes	Yes
Luxembourg	Yes	Yes	Yes	Yes	No
Iceland	No	No	No	No	No
Denmark	Yes	Yes	No	No	No
Netherlands	Yes	Yes	No	No	No
Sweden	Yes	Yes	No	No	No
China	Yes	Yes	Yes	Yes	Yes
Brazil	Yes	Yes	No	No	No
Mexico	Yes	No	No	No	No
Turkey	No	No	No	No	No
Argentina	No	No	No	No	No
Colombia	No	No	No	No	No
South Africa	Yes	Yes	No	No	No
Indonesia	Yes	No	No	No	No
Thailand	Yes	No	No	No	No

The TAM evaluation of eighteen countries reveals:

1. Twelve countries have quantum initiatives (AC1), showing growing interest across income levels.
2. Nine countries are building quantum computers (AC2), indicating challenges in practical implementation.
3. Only four countries (US, Switzerland, Ireland, China) offer quantum computing as a service (AC3).
4. The same four countries have practical applications of quantum computers (AC4).
5. Only three countries (US, Switzerland, Ireland) are deemed TAM-ready for quantum computing.

This analysis suggests quantum computing is still in its initial stages but poised for rapid growth. The field is expected to attract significant resources and investments, potentially leading to more start-ups and increased funding in research. IBM's ambitious plans could catalyze industry-wide competition. The implications of quantum supremacy extend beyond corporate interests to national security, potentially revolutionizing cryptography, intelligence gathering, and data analysis. This is likely to stimulate strategic government investments in quantum computing. The quantum computing landscape is on the brink of significant change, driven by corporate competition, governmental strategies, technological advancements, and global resource allocation. It is also important to note that from the analysis conducted, qualitative factors significantly influence quantum computing readiness, complementing quantitative TAM metrics:

- Economic Barriers: Upper-middle-income countries face challenges in scaling infrastructure due to limited funding. For example, while China has significant government backing, nations like Brazil and South Africa struggle with practical implementations (AC2 in Table 11). High costs associated with quantum research and infrastructure act as a barrier to widespread adoption.
- Educational and Workforce Gaps: Nations with strong educational systems and workforce training programs, such as the U.S. and Switzerland, show higher TAM readiness (Table 9). These countries invest heavily in quantum education, ensuring a pipeline of skilled professionals.
- Cultural and Policy Impacts: The centralized approach in China facilitates rapid deployment but limits private-sector innovation, contrasting with the U.S. model that encourages diverse stakeholders. This cultural difference impacts perceived ease of use and usefulness, key TAM metrics.

Addressing these barriers requires targeted policies and investments, particularly in education and international collaboration.

4.5. Case Study – The United States Quantum Initiative

The United States has been engaged in the deliberate research and development of quantum computers since 1981 when Richard Feynman gave a talk on the possibility of simulating physics with a quantum computer. In 1985, Physicist David Deutsch from Oxford University published a paper on a theoretical Quantum Turing Machine[47], [48]. Since then, the field remained relatively theoretical until 1994, when Shor’s algorithm for factoring large numbers into primes resuscitated the research into this novel field. The possibilities of what quantum computers could provide in terms of drug discovery[49], protein analysis and overall speedups of the simulation of natural phenomena became apparent. This in turn brought in interest from the private sector with companies such as IBM deliberately funding research into quantum computers. This was closely followed by Google and NASA. From the onset, US entities had shown interest in the power of quantum computers.

The United States National Quantum Initiative (NQI) was launched in 2018 through an Act of Congress to deliberately stir the US into a Quantum superpower. This is the only country in the world that had quantum computing as law because the policy makers realized the benefits and potential threats that this technology may bring. The United States would deliberately want to maintain an edge on global influence by owning superior technology before it becomes mainstream; hence, as indicated in the preamble to the National Quantum Initiative Act, "To provide for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States", that government clearly understands that the technology poses a security risk and indeed economic benefits. Since the enactment into law of the quantum act, the country has seen increased investment in quantum computing with companies such as Google recently claiming that they had achieved quantum supremacy[50] but that has been refuted by several within the research space because while the results had some significant breakthroughs, the claim of supremacy was false because classical computers could still manage the computations that were used by the Google 53 qubit Sycamore quantum computer, the results could be replicated by a classical computer[51]. The US government has also spent approximately $3.5 billion on its quantum initiative, as seen in Figure 1 below.

The base budget is for research into quantum information science (QIS), while the NQI budget is generally concerned with government activities to prepare that country for the adoption of quantum technology though training and education. The US is deliberately preparing its citizenry for quantum advantage. Private entities have also played a significant role. IBM also announced that they would have a 100,000-qubit quantum computer by 2033[52].

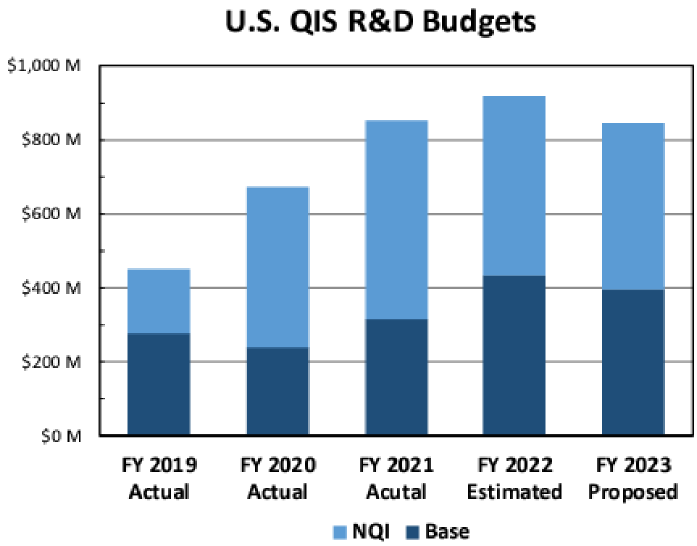

Figure 1. US Quantum Budget

IBM is working with a Tokyo Lap, so naturally, Japan would also benefit from such technology. The implications of that are quite outstanding and form the basis for our earlier indication as to when quantum supremacy would be achieved. To elaborate more on the implication, the quantum computer that IBM plans to build will be able to achieve the following.

- Break cryptography.
- Simulate complex systems.
- Solve optimization problems for industries such as materials science and manufacturing.
- Speedup machine learning by leaps and bounds.

The brief implications highlighted above would naturally already place the United States at the forefront of the technological race, creating an enormous gap between those that have the technology and those that do not have it. There is clearly interest from highly technologically aware countries, as China also announced that they have committed $15Bn[53] for research into this novel field, which would make it the single largest expenditure by any government once realized. Some researchers advocate for a more democratic access model to quantum technology, considering its vast implications across health, security, agriculture, and manufacturing sectors[20]. This case study underscores the strategic value of investing in quantum technology and the necessity of thoughtful, comprehensive planning in this rapidly developing field.

4.6. Comparative Analysis of Quantum Initiatives

The global landscape of quantum computing readiness demonstrates varied approaches and outcomes, influenced by economic, strategic, and technological factors.

United States: The U.S. emphasizes private-public partnerships, with significant investments from both government initiatives like the National Quantum Initiative Act (2018) and corporate leaders like IBM and Google. The U.S. government alone has allocated approximately $3.5 billion toward quantum research and infrastructure, aiming to maintain its technological edge and mitigate risks. TAM analysis shows the U.S. is fully ready for quantum adoption, with initiatives spanning policy, R&D, and workforce training (Table 11).

China: China's centralized strategy is highlighted by its $15 billion investment in quantum technologies, the largest of any nation. While China lags behind the U.S. in practical adoption metrics (AC3 and AC4 in Table 11), its government-driven model ensures a cohesive approach to achieving quantum readiness. This includes quantum-encrypted communication systems and partnerships with academic institutions.

European Union: The EU adopts a collaborative model through its Quantum Flagship program, a €1 billion initiative fostering partnerships across member states. This approach emphasizes inclusivity and standardization, as evidenced by the development of common quantum standards. TAM readiness in the EU is uneven, with countries like Ireland leading in adoption metrics while others, such as Sweden, lag behind (Table 11).

Emerging Economies: Upper-middle-income nations like Brazil and South Africa are investing in quantum research but face challenges in scaling infrastructure and ensuring usability. TAM analysis shows limited readiness, with adoption mostly confined to academic research (Table 9).

This comparative analysis highlights how high-income nations with robust ecosystems and private-sector involvement lead quantum initiatives. In contrast, upper-middle-income nations rely on state-driven efforts, reflecting varied pathways to quantum readiness.

5. Recommendations

To address the challenges of quantum supremacy readiness and its implications, this paper recommends the following:

1. Adopt Quantum-Resistant Cryptography: Governments and corporations should prioritize transitioning to quantum-resistant encryption standards to safeguard critical data.
2. Enhance International Collaborations: Initiatives like the EU's Quantum Flagship demonstrate the value of cooperative approaches[54]. Expanding similar models globally could accelerate readiness.
3. Invest in Education and Training: Building a quantum-ready workforce through educational programs and technical training is essential for long-term success.
4. Develop Policy Frameworks: Policymakers should enact legislation supporting quantum research while addressing ethical concerns and cybersecurity risks.
5. Encourage Private Sector Participation: Public-private partnerships, as seen in the United States, can drive innovation and resource allocation.

6. Discussion and Conclusion

Quantum computing advancements and investments are predominantly concentrated in high-income countries, with a few exceptions like China and South Africa. This concentration is likely due to the significant financial resources required for quantum infrastructure development. The Technology Acceptance Model (TAM) analysis suggests that only 4 out of 16 assessed countries are ready to integrate quantum computing into everyday operations. While the immediate threat to global cybersecurity from quantum computers is currently low, continuous reassessment is necessary given the rapid pace of technological advancement. The nation's leading in quantum research are also major contributors to global technology infrastructure, suggesting they may be both the source of potential cybersecurity risks and the key to mitigating them.

The deployment of large-scale quantum computers is expected to coincide with upgrades to global digital infrastructure to ensure quantum resistance. This upgrade is crucial to protect critical information from potential quantum-enabled breaches. The enactment of data protection laws in many countries highlights the legal and ethical challenges alongside the technical ones. These regulations must be respected, especially considering the potential for quantum computers to crack current encryption standards.

6.1. Limitations and Future Direction

This study focuses on high-income and upper-middle-income countries, potentially limiting the generalizability of findings to lower-income nations. Additionally, the fast-paced nature of quantum research means that the analysed data may become outdated quickly. Future studies should explore the socio-economic and cultural factors influencing quantum technology adoption. Expanding the scope to include more diverse geographies and longitudinal analyses would provide a more comprehensive understanding of global readiness.

In conclusion, quantum supremacy presents both immense opportunities and significant challenges. These extend beyond technological difficulties into geopolitics, legal frameworks, and ethics. The current best approach involves vigilant monitoring of developments, creation of quantum-resistant infrastructure, and a focus on data protection laws that respect sovereignty in the quantum age.

References

1. A. Fedorov, N. Gisin, S. Beloussov, and A. Lvovsky, 'Quantum computing at the quantum advantage threshold: a down-to-business review', arXiv preprint arXiv:2203.17181, 2022.
2. D. Brennan, 'Quantum Computational Supremacy: Security and Vulnerability in a New Paradigm', 2018, doi: 10.21427/R351-0P36.
3. E. Gerjuoy, 'Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers', American Journal of Physics, vol. 73, no. 6, pp. 521–540, Jun. 2005, doi: 10.1119/1.1891170.
4. R. P. Feynman, 'Simulating physics with computers', Int J Theor Phys, vol. 21, no. 6–7, pp. 467–488, Jun. 1982, doi: 10.1007/BF02650179.
5. A. Ajagekar and F. You, 'Quantum computing and quantum artificial intelligence for renewable and sustainable energy: A emerging prospect towards climate neutrality', Renewable and Sustainable Energy Reviews, vol. 165, p. 112493, 2022.
6. M. S. Alam et al., 'Quantum computing hardware for hep algorithms and sensing', arXiv preprint arXiv:2204.08605, 2022.
7. T. Cova, C. Vitorino, M. Ferreira, S. Nunes, P. Rondon-Villarreal, and A. Pais, 'Artificial intelligence and quantum computing as the next pharma disruptors', Artificial Intelligence in Drug Design, pp. 321–347, 2022.
8. D. Rosch-Grace and J. Straub, 'Analysis of the Necessity of Quantum Computing Capacity Development for National Defense and Homeland Security', in 2021 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE, 2021, pp. 1–8.
9. C. Mangla, S. Rani, N. M. F. Qureshi, and A. Singh, 'Mitigating 5G security challenges for next-gen industry using quantum computing', Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 6, p. 101334, 2023.
10. N. M. Neumann, M. P. van Heesch, F. Phillipson, and A. A. Smallegange, 'Quantum computing for military applications', in 2021 International Conference on Military Communication and Information Systems (ICMCIS), IEEE, 2021, pp. 1–8.
11. B. Lau et al., 'Insights from incorporating quantum computing into drug design workflows', Bioinformatics, vol. 39, no. 1, p. btac789, 2023, doi: 10.1093/bioinformatics/btac789.

12. W. Kozlowski, A. Dahlberg, and S. Wehner, ‘Designing a Quantum Network Protocol’, in Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies, in CoNEXT ’20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–16. doi: 10.1145/3386367.3431293.
13. A. Kumar et al., ‘Survey of Promising Technologies for Quantum Drones and Networks’, IEEE Access, vol. 9, pp. 125868–125911, 2021, doi: 10.1109/ACCESS.2021.3109816.
14. D. Chandra, A. S. Cacciapuoti, M. Caleffi, and L. Hanzo, ‘Direct Quantum Communications in the Presence of Realistic Noisy Entanglement’, IEEE Trans. Commun., vol. 70, no. 1, pp. 469–484, Jan. 2022, doi: 10.1109/TCOMM.2021.3122786.
15. J. Martinis, ‘Building a Quantum Computer’, in 2023 International VLSI Symposium on Technology, Systems and Applications (VLSI-TSA/VLSI-DAT), HsinChu, Taiwan: IEEE, Apr. 2023, pp. 1–1. doi: 10.1109/VLSI-TSA/VLSI-DAT57221.2023.10134344.
16. Collins Aerospace, R. Walthall, S. Dixit, and Northrop Grumman Space Systems, ‘Impact of Quantum Computing in Aerospace’, SAE International, Jun. 2022. doi: 10.4271/EPR2022014.
17. T. Roberson, J. Leach, and S. Raman, ‘Talking about public good for the second quantum revolution: analysing quantum technology narratives in the context of national strategies’, Quantum Science and Technology, vol. 6, no. 2, p. 025001, 2021.
18. O. O. Olatunji, P. A. Adedeji, and N. Madushele, ‘Quantum computing in renewable energy exploration: status, opportunities, and challenges’, in Design, Analysis, and Applications of Renewable Energy Systems, Elsevier, 2021, pp. 549–572. doi: 10.1016/B978-0-12-824555-2.00019-8.
19. E. De Jong, ‘Own the Unknown: An Anticipatory Approach to Prepare Society for the Quantum Age’, DISO, vol. 1, no. 2, p. 15, Sep. 2022, doi: 10.1007/s44206-022-00020-4.
20. Z. C. Seskir, S. Umbrello, C. Coenen, and P. E. Vermaas, ‘Democratization of quantum technologies’, Quantum Sci. Technol., vol. 8, no. 2, p. 024005, Apr. 2023, doi: 10.1088/2058-9565/acb6ae.
21. D. Joseph et al., ‘Transitioning organizations to post-quantum cryptography’, Nature, vol. 605, no. 7909, pp. 237–243, May 2022, doi: 10.1038/s41586-022-04623-2.
22. O. Ezratty, ‘Mitigating the quantum hype’, 2022, doi: 10.48550/ARXIV.2202.01925.
23. A. Asfaw et al., ‘Building a Quantum Engineering Undergraduate Program’, IEEE Trans. Educ., vol. 65, no. 2, pp. 220–242, May 2022, doi: 10.1109/TE.2022.3144943.
24. A. Lele, ‘Quantum (Arms) Race’, in Quantum Technologies and Military Strategy, in Advanced Sciences and Technologies for Security Applications. , Cham: Springer International Publishing, 2021, pp. 145–172. doi: 10.1007/978-3-030-72721-5_9.
25. T. Dekker and F. Martin-Bariteau, ‘Regulating Uncertain States: A Risk-Based Policy Agenda for Quantum Technologies’, SSRN Journal, 2022, doi: 10.2139/ssrn.4203758.
26. K. Petrenko, A. Mashatan, and F. Shirazi, ‘Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization’, Journal of Information Security and Applications, vol. 46, pp. 151–163, Jun. 2019, doi: 10.1016/j.jisa.2019.03.007.
27. A. Purohit, M. Kaur, Z. C. Seskir, M. T. Posner, and A. Venegas-Gomez, ‘Building a Quantum-ready Ecosystem’, 2023, doi: 10.48550/ARXIV.2304.06843.
28. European Commission. Joint Research Centre., Standards4Quantum: making quantum technology ready for industry : putting science into standards. LU: Publications Office, 2020. Accessed: Jul. 15, 2023. [Online]. Available: https://data.europa.eu/doi/10.2760/882029
29. O. Van Deventer et al., ‘Towards European standards for quantum technologies’, EPJ Quantum Technol., vol. 9, no. 1, p. 33, Dec. 2022, doi: 10.1140/epjqt/s40507-022-00150-1.
30. M. Kop et al., ‘Towards responsible quantum technology, safeguarding, engaging and advancing Quantum R&D’, 2023, doi: 10.48550/ARXIV.2303.16671.
31. D. Martire, C. Origlia, S. Laurita, and A. Imbrogno, ‘Trends, key actors and use cases in QKD technologies: an analysis of the research and innovation frontier using web-based methods’, in 2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE), Matera, Italy: IEEE, Jun. 2022, pp. 1–4. doi: 10.1109/WOLTE55422.2022.9882827.
32. C. Teng et al., ‘Secure Interactive Architecture of Cloud Driving System Based on 5G and Quantum Encryption’, in 2021 5th CAA International Conference on Vehicular Control and Intelligence (CVCI), Tianjin, China: IEEE, Oct. 2021, pp. 1–6. doi: 10.1109/CVCI54083.2021.9661202.
33. X. Ren et al., ‘Building Resilient Web 3.0 with Quantum Information Technologies and Blockchain: An Ambilateral View’, 2023, doi: 10.48550/ARXIV.2303.13050.
34. T. G. Tan and J. Zhou, ‘Migrating Blockchains Away from ECDSA for Post-quantum Security: A Study of Impact on Users and Applications’, in Data Privacy Management, Cryptocurrencies and Blockchain Technology, vol. 13619, J. Garcia-Alfaro, G. Navarro-Arribas, and N. Dragoni, Eds., in Lecture Notes in Computer Science, vol. 13619. , Cham: Springer International Publishing, 2023, pp. 308–316. doi: 10.1007/978-3-031-25734-6_19.
35. [N. Alnahawi, N. Schmitt, A. Wiesmaier, and C.-M. Zok, ‘Towards Next Generation Quantum-Safe eIDs and eMRTDs – A Survey’, ACM Trans. Embed. Comput. Syst., p. 3585517, Mar. 2023, doi: 10.1145/3585517.
36. X. Chen, S. Xu, T. Qin, Y. Cui, S. Gao, and W. Kong, ‘AQ–ABS: Anti-Quantum Attribute-based Signature for EMRs Sharing with Blockchain’, in 2022 IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA: IEEE, Apr. 2022, pp. 1176–1181. doi: 10.1109/WCNC51071.2022.9771830.
37. A. Baitulmal and N. Adem, ‘Why should and how can quantum technologies be leveraged at national levels?’, IET Quantum Communication, vol. 4, no. 2, pp. 96–101, Jun. 2023, doi: 10.1049/qtc2.12057.

38. J. R. Lindsay, 'Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage', Security Studies, vol. 29, no. 2, pp. 335–361, Mar. 2020, doi: 10.1080/09636412.2020.1722853.
39. W. Bank, The changing wealth of nations 2021: managing assets for the future. The World Bank, 2021.
40. F. D. Davis and A. Granić, The Technology Acceptance Model: 30 Years of TAM. in Human–Computer Interaction Series. Cham: Springer International Publishing, 2024. doi: 10.1007/978-3-030-45274-2.
41. J. Antony, 'Six sigma for service processes', Business Process Management Journal, vol. 12, no. 2, pp. 234–248, Mar. 2006, doi: 10.1108/14637150610657558.
42. P. Cirillo, 'Are your data really Pareto distributed?', Physica A: Statistical Mechanics and its Applications, vol. 392, no. 23, pp. 5947–5962, Dec. 2013, doi: 10.1016/j.physa.2013.07.061.
43. G. Strawn, 'Open Science and the Hype Cycle', Data Intelligence, vol. 3, no. 1, pp. 88–94, Feb. 2021, doi: 10.1162/dint_a_00081.
44. X. Chen and T. Han, 'Disruptive Technology Forecasting based on Gartner Hype Cycle', in 2019 IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA: IEEE, Jun. 2019, pp. 1–6. doi: 10.1109/TEMSCON.2019.8813649.
45. 'FACT SHEET: President Biden Announces Two Presidential Directives Advancing Quantum Technologies'. Accessed: Jul. 15, 2023. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/
46. Klaus Ensslin, '"Switzerland could play a key role in quantum technology"'. [Online]. Available: https://ethz.ch/en/news-and-events/eth-news/news/2022/12/nccr-qsit-switzerland-could-play-a-key-role.html
47. K. Thakur, A.-S. K. Pathan, and S. Ismat, 'Quantum Computing', in Emerging ICT Technologies and Cybersecurity, Cham: Springer Nature Switzerland, 2023, pp. 199–216. doi: 10.1007/978-3-031-27765-8_8.
48. 'Quantum theory, the Church–Turing principle and the universal quantum computer', Proc. R. Soc. Lond. A, vol. 400, no. 1818, pp. 97–117, Jul. 1985, doi: 10.1098/rspa.1985.0070.
49. Y. Cao, J. Romero, and A. Aspuru-Guzik, 'Potential of quantum computing for drug discovery', IBM Journal of Research and Development, vol. 62, no. 6, pp. 6–1, 2018.
50. F. Arute et al., 'Quantum supremacy using a programmable superconducting processor', Nature, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.
51. G. Kalai, Y. Rinott, and T. Shoham, 'Google's Quantum Supremacy Claim: Data, Documentation, and Discussion', 2022, doi: 10.48550/ARXIV.2210.12753.
52. 'Charting the course to 100,000 qubits'. IBM Research. Accessed: Jul. 16, 2023. [Online]. Available: https://research.ibm.com/blog/100k-qubit-supercomputer
53. 'Betting big on quantum'. Accessed: Aug. 02, 2023. [Online]. Available: https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/chart-of-the-day/betting-big-on-quantum
54. M. Riedel, M. Kovacs, P. Zoller, J. Mlynek, and T. Calarco, 'Europe's Quantum Flagship initiative', Quantum Sci. Technol., vol. 4, no. 2, p. 020501, Feb. 2019, doi: 10.1088/2058-9565/ab042d.