The Potential Future of Quantum Computing in Cyber Threats

1. Introduction: The Emerging Quantum Threat in Cybersecurity

Quantum computing, a paradigm shift in computation, harnesses the principles of quantum mechanics to perform calculations far beyond the capabilities of classical computers.[1] This revolutionary technology holds immense promise for advancements across various domains, including medicine, materials science, and artificial intelligence.[3] However, like many powerful innovations, quantum computing presents a dual-use dilemma, offering not only unprecedented benefits but also the potential for malicious exploitation, particularly within the realm of cybersecurity.[4]

This report aims to explore the potential future applications of quantum computing in the context of specific cyber threats, namely ransomware, malware, spyware, deepfake technology, and artificial intelligence-driven attacks. A critical aspect of this analysis is to assess the likelihood of these scenarios transitioning from theoretical possibilities to tangible realities, considering the current state of quantum computing development and comparing these potential threats with existing trends in cybercrime. Ultimately, the report will discuss the significant implications for the future of cybersecurity and the measures needed to mitigate emerging risks. The increasing pace of development in quantum computing, as highlighted by survey respondents indicating progress exceeding expectations [1], underscores the urgency of understanding and preparing for its potential impact on cybersecurity. The substantial investments being made in quantum technologies across various sectors further emphasize the need for proactive risk assessment and strategic planning.[1]

2. Quantum Computing Fundamentals and Their Relevance to Cyber Threats

Quantum computing operates on principles fundamentally different from classical computing, leveraging the unique properties of quantum mechanics such as superposition and entanglement.[6] In classical computers, information is stored and processed as bits, which can exist in one of two states: 0 or 1. Quantum computers, however, utilize quantum bits, or qubits, which can exist in a superposition of both 0 and 1 simultaneously.[6] This ability, combined with the phenomenon of entanglement where the states of multiple qubits become correlated in ways that classical physics cannot explain [6], allows quantum computers to perform certain calculations exponentially faster than even the most powerful classical supercomputers.[2]

The relevance of these capabilities to cybersecurity becomes apparent when considering algorithms like Shor's algorithm, a quantum algorithm that can efficiently factorize large numbers.[2] The security of many of today's public-key encryption algorithms, including RSA and ECC, relies on the computational difficulty of factoring such large numbers for classical computers.[2] A sufficiently powerful quantum computer running Shor's algorithm could potentially break these encryption methods in a matter of hours, rendering much of current secure communication vulnerable.[9]

Another significant quantum algorithm is Grover's algorithm, which provides a quadratic speedup for searching unsorted databases.[16] While this does not directly break symmetric encryption algorithms like AES, it reduces the effective key length, potentially making brute-force attacks more feasible with quantum computers.[16] The concept of "quantum advantage" refers to the point at which a quantum computer can solve a problem that is beyond the reach of even the most powerful classical computers.[7] Achieving quantum advantage in areas relevant to cyber threats could have profound implications for the security landscape. The fundamental shift in computational power offered by quantum computing, particularly its ability to efficiently solve problems currently considered intractable, poses a significant threat to the foundational cryptographic principles that underpin modern cybersecurity.[9]

3. The Impact of Quantum Computing on Ransomware

Quantum computing presents both a potential threat and a possible future enhancement to ransomware attacks. One of the most significant concerns is the capability of quantum computers to break the encryption currently used by ransomware. Ransomware often employs a combination of symmetric encryption (like ChaCha20 or AES) to encrypt files and asymmetric encryption (like RSA-2048) to protect the symmetric key.[40] Quantum computers, utilizing Shor's algorithm, could factor the large prime numbers used in asymmetric encryption, potentially within hours [42], making the decryption key easily obtainable.[9] This capability would undermine the current reliance on the computational difficulty of factoring for ransomware encryption security.[9] The primary threat quantum computing poses to current ransomware is its ability to break the asymmetric encryption used to protect the symmetric key, potentially eliminating the attacker's leverage by making decryption trivial. This could fundamentally change the ransomware business model.

However, a more concerning future scenario involves ransomware leveraging quantum-resistant encryption.[51] Advanced ransomware groups are predicted to

adopt post-quantum cryptography (PQC) algorithms to encrypt data, which are designed to withstand attacks from both classical and quantum computers.[51] This would make the encrypted data virtually impossible to recover for victims who have not transitioned to quantum-resistant decryption methods.[51] A significant future evolution of ransomware could be the adoption of quantum-resistant encryption, flipping the current scenario where attackers hold the decryption key to one where even the attackers might struggle to decrypt the data if quantum decryption methods advance unexpectedly. This would create an even more intractable problem for victims.

Furthermore, quantum computers' ability to perform complex computations at significantly faster speeds [2] could allow ransomware to encrypt large volumes of data much more rapidly than with classical computers.[46] This faster encryption could reduce the time available for detection and intervention by security teams, leading to more successful and widespread attacks.[46] The speed advantage of quantum computing could be weaponized by ransomware attackers to encrypt data across entire networks in a fraction of the time it currently takes, potentially overwhelming response capabilities.

Quantum-enhanced AI could also be used to develop more sophisticated methods for delivering and propagating ransomware within networks.[34] AI, potentially enhanced by quantum computing [34], could be used to create more targeted and convincing phishing attacks for initial ransomware deployment.[34] Quantum-enhanced AI could also improve the ability of ransomware to spread laterally across networks, identify valuable targets, and evade detection.[34] The combination of quantum computing and AI could lead to a new generation of ransomware that is not only harder to decrypt but also significantly more effective at infiltrating and spreading within victim environments.

Additionally, quantum computing's computational power could be used to analyze software and systems for previously unknown vulnerabilities (zero-day exploits) that could be leveraged for ransomware attacks.[34] Quantum computing might provide attackers with a powerful tool for discovering and exploiting weaknesses in software and systems, potentially giving them an advantage in deploying ransomware.

It is important to note the existence of current ransomware with "quantum" in its name, such as the Quantum ransomware family discovered in 2021.[59] However, these strains are rebrands of previous ransomware and do not currently utilize quantum

computing in their encryption process.[40] The naming likely capitalizes on the increasing public awareness and concern regarding the potential of quantum computing to break encryption.[59]

4. Quantum Computing and the Evolution of Malware

Beyond ransomware, quantum computing holds the potential to revolutionize the development and deployment of other forms of malware. As quantum computers become more prevalent, they will become lucrative targets for cybercriminals.[39] Malware specifically designed to attack quantum computers, such as "MalaQ" [64], can exploit vulnerabilities in the classical control systems and cause performance degradation or even complete failure of quantum circuits.[64] Attacks could also target the sensitive hardware components of quantum computers, potentially causing physical damage.[39] The emergence of quantum computers will create a new attack surface, with malware specifically designed to disrupt or damage these systems becoming a reality. Protecting quantum infrastructure will be a critical aspect of future cybersecurity.

Quantum-enhanced AI could also be leveraged to create malware with advanced evasion techniques, capable of bypassing traditional security solutions.[34] Quantum-enhanced AI could enable malware to learn and adapt its behavior in real-time to evade detection by signature-based and heuristic security tools.[26] This could lead to a new generation of highly sophisticated and persistent malware that is significantly harder to identify and remove.[26] The combination of quantum computing and AI could lead to malware that can effectively "think" its way around security defenses, posing a significant challenge to traditional cybersecurity approaches.

While not explicitly detailed in the provided snippets, the theoretical principles of quantum communication, such as quantum entanglement, could potentially be used to establish highly secure and difficult-to-intercept command and control channels for malware. Any attempt to eavesdrop would disturb the quantum state, alerting the communicating parties.[17] The unique properties of quantum communication could offer malware operators a virtually undetectable way to control infected systems, presenting a significant challenge for network security monitoring.

Quantum computing's ability to perform complex computations could allow attackers to analyze software code for vulnerabilities at an unprecedented speed and scale.[34] This could lead to the discovery of previously unknown weaknesses that could be exploited to develop highly targeted and effective malware.[34] Quantum computing

might provide attackers with a significant advantage in identifying and exploiting software vulnerabilities, potentially leading to more impactful malware attacks.

Furthermore, quantum machine learning algorithms could potentially be used to develop malware that can dynamically alter its code and characteristics, making it difficult for signature-based detection systems to identify.[74] Quantum machine learning could contribute to the evolution of malware that can actively evade detection by changing its "fingerprint," requiring more sophisticated behavioral analysis techniques for defense.

5. Enhancing Spyware Capabilities with Quantum Technology

Quantum computing holds the potential to significantly enhance the capabilities of spyware across various aspects, including data collection, analysis, and stealth. Spyware often intercepts encrypted communications.[75] Quantum computers running Shor's algorithm could break the public-key encryption used to secure these communications, allowing attackers to access the plaintext data much faster than with classical computers.[46] This would significantly enhance the value of data collected through spyware, especially for long-term surveillance operations ("harvest now, decrypt later" attacks).[6] Quantum computing's ability to break encryption could turn vast amounts of currently indecipherable intercepted data into actionable intelligence for spyware operators, posing a severe threat to privacy and security.

Spyware collects massive amounts of data, including keystrokes, browsing history, and location information.[75] Quantum-enhanced AI could analyze this data much more efficiently, identifying patterns, relationships, and valuable insights that might be missed by classical analysis techniques.[34] Quantum-powered AI could transform spyware from a tool that passively collects data into an active intelligence-gathering platform capable of rapidly sifting through vast amounts of information to pinpoint critical details.

Quantum sensors offer unprecedented sensitivity and precision in detecting minute changes in physical quantities like magnetic fields, gravity, and time.[110] These sensors could potentially be used in advanced spyware to detect the presence of individuals, monitor their movements with high accuracy (even indoors or underground), or even intercept faint electromagnetic signals.[110] The integration of quantum sensors into spyware could lead to a new level of environmental surveillance capabilities, going beyond traditional software-based spying.

Finally, quantum computing might assist in developing new obfuscation techniques for spyware code, making it harder for antivirus software to identify.[112] It could also potentially be used to create spyware that operates at a quantum level, making it invisible to classical detection methods.[112] Quantum computing could contribute to the creation of "next-generation" spyware that is not only more effective at gathering information but also significantly more difficult to detect and remove from compromised systems.

6. The Intersection of Quantum Computing and Deepfake Technology for Malicious Purposes

The intersection of quantum computing and deepfake technology presents a significant area of concern for future cyber threats. Training deep learning models for deepfake generation is computationally intensive.[115] Quantum machine learning algorithms could potentially speed up the training process due to quantum parallelism and enhanced computational capabilities.[34] This would allow malicious actors to create and deploy sophisticated deepfakes more quickly and efficiently.[34] Quantum computing could lower the barrier to entry for creating high-quality deepfakes by reducing the time and computational resources required for training the underlying AI models.

Quantum computing's ability to process and generate high-dimensional data from low-dimensional latent spaces [117] could lead to the creation of deepfakes with enhanced realism and fidelity.[117] This could make it increasingly difficult for humans and even current AI-based detection systems to distinguish between real and fake content.[117] Quantum computing could push the boundaries of deepfake realism, making it virtually impossible to identify manipulated media, with significant implications for trust in digital content.

Furthermore, quantum-enhanced AI could be used to develop deepfake generation models that are specifically designed to evade the artifacts and inconsistencies that current detection algorithms look for.[58] This could lead to a continuous arms race between deepfake creators and detection system developers.[123] Quantum computing could give deepfake creators an advantage in the ongoing battle against detection, leading to more sophisticated and harder-to-spot manipulated media.

The ability to quickly and easily create highly realistic and difficult-to-detect deepfakes using quantum computing could significantly amplify the scale and impact of disinformation campaigns.[117] These advanced deepfakes could also be used in

more effective and targeted social engineering attacks, potentially leading to greater success in phishing and other malicious activities.[124] Quantum-accelerated deepfake generation could become a powerful tool for malicious actors to manipulate public opinion, sow discord, and conduct highly effective social engineering attacks.

7. Quantum Computing's Influence on AI-Driven Cyber Threats

The synergy between quantum computing and artificial intelligence has the potential to significantly influence the landscape of cyber threats. AI is already used to automate various aspects of cyberattacks, such as vulnerability scanning and exploit deployment.[51] Quantum computing could significantly accelerate the execution of these AI-driven tasks, allowing for faster and more widespread attacks.[57] Quantum computing could supercharge the automation of cyberattacks, allowing malicious actors to launch and execute attacks at speeds that are difficult for human defenders to counter.

AI algorithms, potentially enhanced by quantum computing, can analyze vast amounts of data to identify vulnerable targets and tailor attacks accordingly.[34] This could lead to more successful attacks with a higher rate of compromise.[34] Quantum-enhanced AI could enable cyber attackers to identify and target their victims with greater precision, increasing the likelihood of a successful breach.

AI is also used to create malware that can evade detection.[51] Quantum computing could significantly enhance AI's ability to develop sophisticated evasion techniques, allowing malware and attacks to bypass even advanced security solutions.[34] Quantum computing could lead to a new era of highly sophisticated and elusive cyber threats that can effectively hide from and bypass current security measures.

Furthermore, AI is already used to create more convincing and personalized social engineering attacks and phishing emails.[5] Quantum computing could further enhance AI's ability to craft highly sophisticated and effective social engineering attacks that are extremely difficult for users to recognize as malicious.[58] Quantum computing could amplify the effectiveness of social engineering attacks, making them a more significant threat to individuals and organizations.

Finally, quantum machine learning could significantly accelerate the analysis of software and systems for security vulnerabilities.[34] This could lead to the faster discovery of zero-day exploits, giving attackers a window of opportunity before patches are available.[34] Quantum computing could provide attackers with a powerful

tool for finding and exploiting previously unknown vulnerabilities, potentially leading to widespread security breaches.

8. Assessing the Timeline: The Development of Quantum Computing and the Feasibility of These Threats

Quantum computing is rapidly evolving, with increasing interest and investment from academia, industry, and government.[1] The pace of development is considered faster than expected by many in the field.[1] Current quantum computers exist but are still in the early stages of development [134], with experimental and commercial systems available.[131] Companies like IBM, Google, Microsoft, and SpinQ have developed quantum processors with increasing qubit counts [7], with IBM aiming for over 4,000 qubits by 2025 [7] and Microsoft targeting a million qubits with its Majorana 1 chip.[46] However, the majority of quantum systems are still in development or testing phases [131], and the number of operational quantum computers globally remains limited, around 100-200 in 2025, but is growing steadily.[131]

IBM's Condor processor has 1,121 qubits [131], while Atom Computing has a system with 1,180 qubits.[131] Quantinuum's H2-1 processor has 56 physical qubits.[137] Google's Willow chip has 105 qubits.[131] Qubit stability, measured by coherence time and error rates, remains a significant challenge.[3] High-fidelity qubits are crucial for complex computations.[3] Microsoft's Majorana 1 aims for more stable qubits through its topological architecture.[132] Google's Willow has demonstrated low error rates.[127] Quantinuum achieved 99.9% 2-qubit gate fidelity.[42]

Scalability (increasing the number of qubits) and error correction/fault tolerance are the most significant technical challenges facing quantum computing.[1] Current quantum computers are prone to errors due to noise and decoherence.[3] Quantum error correction (QEC) is essential for building reliable quantum computers but requires a large number of physical qubits to create a single logical, error-corrected qubit.[3] Researchers are making progress in error correction techniques [3], with Google's Willow demonstrating below-threshold error correction [147] and Microsoft and Quantinuum entangling 12 logical qubits.[155]

Predictions for the emergence of cryptographically relevant quantum computers (CRQCs) vary, ranging from within the next 5 years to 30 years.[2] A significant portion of experts believe that CRQCs could exist within the next 10-15 years.[2] Some experts express concern that the timeline might be shorter than anticipated due to rapid advancements and the potential impact of AI on quantum development.[42] The Global

Risk Institute's Quantum Threat Timeline Report 2024 estimates a 19-34% chance of a CRQC by 2034.[42]

Breakthroughs in quantum hardware, such as Microsoft's Majorana 1 chip, powered by topological qubits designed for scalability and error protection [46], and Google's Willow chip, demonstrating significant error reduction with qubit scaling [18], could potentially shorten the timeline for the development of CRQCs. Significant progress is also being made in quantum error correction (QEC), which is crucial for achieving fault-tolerant quantum computation.[1] Demonstrations of logical qubits with improved lifetimes and reduced error rates are a key milestone [154], and Google's Willow has shown error correction increasing exponentially with qubit scaling.[150]

Table: Predicted Timelines for Quantum Computing and Encryption Breaking

Timeline	Prediction	Supporting Snippets
Near-Term (Next 5 Years)	Limited impact from quantum computing on breaking strong encryption. Potential for quantum-enhanced AI in attacks.	7
Mid-Term (5-10 Years)	Increased likelihood of cryptographically relevant quantum computers emerging. "Harvest now, decrypt later" becomes a significant threat.	2
Long-Term (10+ Years)	High probability of quantum computers breaking current public-key encryption. Widespread adoption of post-quantum cryptography necessary.	2

9. Theoretical Quantum Threats vs. Current Cybercrime Realities

Current cybercrime heavily relies on exploiting existing vulnerabilities in classical

systems using traditional methods like phishing, malware, and ransomware.[51] Quantum computing introduces the theoretical possibility of breaking fundamental cryptographic algorithms and developing new forms of malware and attack vectors.[4] While current cybercrime leverages classical vulnerabilities, quantum computing presents a paradigm shift with the potential to render current security measures obsolete and introduce entirely new threats. The focus of cybercriminals will likely evolve as quantum capabilities become available.

The increasing speed and automation of cyberattacks, often driven by AI [23], are characteristics that could be significantly amplified by quantum computing's processing power.[57] The growing sophistication of malware in evading detection [40] could be further enhanced by quantum-enhanced AI.[34] Existing trends in cybercrime, such as the increasing reliance on speed, automation, and evasion, suggest that quantum computing could act as a powerful force multiplier for current attack methods.

Given the potential for significant impact and the high value of compromised data, it is highly likely that sophisticated cybercriminals and nation-state actors will shift their focus towards exploiting quantum computing capabilities once they become accessible.[6] The high reward associated with successful cyberattacks, coupled with the immense power of quantum computing, makes it inevitable that malicious actors will seek to leverage this technology.

The "harvest now, decrypt later" (HNDL) threat, where adversaries collect encrypted data now with the intention of decrypting it in the future using quantum computers, is a significant concern.[9] This threat aligns with current trends of large-scale data exfiltration by cybercriminals and nation-state actors.[6] The "harvest now, decrypt later" threat is a tangible and growing risk, as evidenced by current data exfiltration activities, highlighting the long-term implications of quantum computing for data security.

Current cybersecurity defenses heavily rely on public-key cryptography algorithms like RSA and ECC.[9] These algorithms are theoretically vulnerable to attacks from cryptographically relevant quantum computers.[9] Therefore, current defenses will be inadequate against quantum-enabled cyber threats once CRQCs become available.[6]

10. The Imperative of Quantum-Resistant Cybersecurity Measures

The gathered information overwhelmingly indicates that the usage of quantum

computing in ransomware, malware, spyware, deepfakes, and AI for cyber threats is not merely fiction but a likely future reality. The potential for significant impact within the next decade, driven by advancements in quantum hardware and algorithms, necessitates an urgent and proactive response from the cybersecurity community.[2] The impending quantum threat necessitates immediate and decisive action to migrate to quantum-resistant cryptography to avoid a future where sensitive data is easily compromised.

Transitioning to post-quantum cryptography (PQC) is crucial to maintain the confidentiality and integrity of sensitive data in the face of quantum computing advancements.[9] This transition needs to begin now due to the potentially long timelines for implementation across complex systems.[2] NIST is actively leading the standardization effort for post-quantum cryptography algorithms [6], having released the first finalized standards in 2024 (FIPS 203, 204, 205).[56] These standards provide a framework for organizations to secure their systems against future quantum threats [46], and NIST is continuing to evaluate additional algorithms.[34]

However, implementing PQC involves significant challenges, including a lack of knowledge and expertise, the technical complexity of PQC technologies, performance impacts (larger key sizes and computational overhead), and the need for coordination across supply chains and vendors.[92] Many organizations lack the necessary know-how and personnel with expertise in quantum cryptography [143], and integrating new PQC algorithms into existing systems can be complex and may require hardware and software updates.[92] Cryptographic agility, the ability to quickly change cryptographic algorithms and protocols, is crucial for responding to the evolving quantum threat and potential vulnerabilities in PQC algorithms themselves.[2] Building systems with cryptographic agility will allow organizations to adapt more readily to the post-quantum era and respond to any unforeseen weaknesses in the newly adopted algorithms.

To mitigate the future quantum threat, organizations should take proactive measures, including conducting a thorough cryptographic inventory to identify vulnerable algorithms and systems.[2] Performing risk assessments to prioritize the transition of the most critical systems and data to PQC is also essential.[2] Pilot testing of NIST-standardized PQC algorithms in non-production environments will help organizations understand their performance characteristics and integration challenges.[2]

11. Conclusion: Navigating the Future of Cyber Threats in the Quantum Era

This report has explored the potential future usage of quantum computing across various cyber threats, including ransomware, malware, spyware, deepfake technology, and AI-driven attacks. The analysis indicates that while the widespread exploitation of quantum computing for malicious purposes is not yet a current reality, it is a highly likely scenario within the next decade. The ability of quantum computers to break current encryption standards, coupled with their potential to enhance AI-driven attacks and create new forms of malware, presents a significant and evolving threat to the cybersecurity landscape.

The profound implications of these future threats necessitate a paradigm shift in security strategies. Organizations and cybersecurity professionals must recognize the urgency of the situation and prioritize the transition to quantum-resistant security measures. The development and standardization of post-quantum cryptography by NIST are crucial steps in this direction, providing the necessary tools to safeguard against future quantum attacks. However, the implementation of PQC is a complex undertaking that requires careful planning, investment in expertise, and a commitment to cryptographic agility.

In conclusion, while the full realization of quantum-enhanced cyber threats is still on the horizon, the trajectory of quantum computing development and the potential for its exploitation by malicious actors make proactive preparation an imperative. Organizations must begin the journey towards a quantum-safe future now to protect their sensitive data and maintain the integrity of their systems in the face of this emerging technological revolution.

Works cited

1. Survey Report: The Current and Future State of Quantum Computing, accessed on April 12, 2025, https://www.quera.com/blog-posts/current-and-future-state-of-quantum-computing
2. A Comprehensive Guide to Quantum-Resistant Cryptography and Encryption - Entrust, accessed on April 12, 2025, https://www.entrust.com/resources/learn/post-quantum-cryptography-and-encryption
3. 2025 will see huge advances in quantum computing. So what is a quantum chip and how does it work? - CSIRO, accessed on April 12, 2025, https://www.csiro.au/en/news/All/Articles/2025/January/2025-huge-advances-in-quantum-computing
4. Cyber Security in the Quantum Era - Communications of the ACM, accessed on April 12, 2025, https://cacm.acm.org/research/cyber-security-in-the-quantum-

era/
5. How Artificial Intelligence and Quantum Computing are Evolving Cyber Warfare, accessed on April 12, 2025, https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/
6. What is Quantum Computing in Cybersecurity? - Balbix, accessed on April 12, 2025, https://www.balbix.com/insights/understanding-quantum-computing-in-cybersecurity/
7. Quantum computing: What leaders need to know now | MIT Sloan, accessed on April 12, 2025, https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now
8. What Is Quantum Computing? - IBM, accessed on April 12, 2025, https://www.ibm.com/think/topics/quantum-computing
9. Cybersecurity Quantum Attack - Identity Management Institute®, accessed on April 12, 2025, https://identitymanagementinstitute.org/cybersecurity-quantum-attack/
10. Quantum Computing and Post-quantum Cryptography PART 1 - André Schrottenloher, accessed on April 12, 2025, https://andreschrottenloher.github.io/docs/lectures/2024-01-cs-pqcrypto-part1.pdf
11. Quantum Computing Technology: Understanding the Basics | NYIT, accessed on April 12, 2025, https://online.nyit.edu/blog/quantum-computing-technology-understanding-the-basics
12. Quantum Computing Basics: A Beginner's Guide - BlueQubit, accessed on April 12, 2025, https://www.bluequbit.io/quantum-computing-basics
13. When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret | RAND, accessed on April 12, 2025, https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html
14. 2024-2025 CRA Quad Paper: The Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead - Computing Research Association, accessed on April 12, 2025, https://cra.org/wp-content/uploads/2025/01/2024-2025-CRA-Quad-Paper_-The-Post-Quantum-Cryptography-Transition_-Making-Progress-But-Still-a-Long-Road-Ahead.pdf
15. Quantum Computing's Next Chapter: The Willow Chip and the Future of Security, accessed on April 12, 2025, https://www.otmcyber.com/post/quantum-computing-s-next-chapter-the-willow-chip-and-the-future-of-security
16. Transitioning to Quantum-Safe Encryption - Delinea, accessed on April 12, 2025, https://delinea.com/blog/quantum-safe-encryption
17. What is Quantum Security and how does it Work? - The Quantum Insider, accessed on April 12, 2025, https://thequantuminsider.com/2023/07/17/quantum-security/
18. Is the Recent Quantum Hype by Google Willow's Chip a Threat to RSA

Algorithm?, accessed on April 12, 2025, https://www.catonetworks.com/blog/is-recent-quantum-hype-by-google-willows-chip-a-threat-to-rsa-algorithm/
19. Quantum Computing and the Future of Cybersecurity - The National CIO Review, accessed on April 12, 2025, https://nationalcioreview.com/articles-insights/information-security/quantum-computing-and-the-future-of-cybersecurity/
20. Why Quantum Computing Capabilities Are Creating Security Vulnerabilities Today, accessed on April 12, 2025, https://securityintelligence.com/posts/quantum-computing-creating-security-vulnerabilities/
21. Why organizations should prepare for quantum computing cybersecurity now - EY, accessed on April 12, 2025, https://www.ey.com/en_us/insights/innovation/why-organizations-should-prepare-for-quantum-computing-cybersecurity-now
22. What is the cyber security risk from quantum computing? - KPMG Australia, accessed on April 12, 2025, https://kpmg.com/au/en/home/insights/2024/04/cyber-security-risk-from-quantum-computing.html
23. Quantum is coming — and bringing new cybersecurity threats with it - KPMG International, accessed on April 12, 2025, https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html
24. Quantum computing: the inevitable threat to information security - TheNextWeb, accessed on April 12, 2025, https://thenextweb.com/news/quantum-computing-threat-information-security-inevitable
25. Quantum cyber threats are likely years away. Why — and how — we're working today to stop them - Mastercard Newsroom, accessed on April 12, 2025, https://newsroom.mastercard.com/news/perspectives/2024/quantum-cyber-threats-are-likely-years-away-why-and-how-we-re-working-today-to-stop-them/
26. Cybersecurity in the Quantum Risk Era - Booz Allen, accessed on April 12, 2025, https://www.boozallen.com/insights/ai-research/cybersecurity-in-the-quantum-risk-era.html
27. The Rise Of Quantum Computing In Cyber Security - MetaCompliance, accessed on April 12, 2025, https://www.metacompliance.com/blog/cyber-security-awareness/quantum-computing-cybersecurity
28. Quantum Computing: Transforming The Future Of Cybersecurity - Forbes, accessed on April 12, 2025, https://www.forbes.com/councils/forbestechcouncil/2024/08/09/quantum-computing-transforming-the-future-of-cybersecurity/
29. Quantum computing cybersecurity risk: PwC, accessed on April 12, 2025, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/quantum-computing-cybersecurity-risk.html
30. Quantum Cybersecurity Explained: Comprehensive Guide, accessed on April 12,

2025, https://thequantuminsider.com/2024/03/13/quantum-cybersecurity-explained-comprehensive-guide/
31. Quantum computing could threaten cybersecurity measures. Here's why – and how tech firms are responding - The World Economic Forum, accessed on April 12, 2025, https://www.weforum.org/stories/2024/04/quantum-computing-cybersecurity-risks/
32. What Is Quantum Computing's Threat to Cybersecurity? - Palo Alto Networks, accessed on April 12, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity
33. Quantum Computing and Cybersecurity - Preparing for a New Age of Threats - LevelBlue, accessed on April 12, 2025, https://levelblue.com/blogs/security-essentials/quantum-computing-and-cybersecurity-preparing-for-a-new-age-of-threats
34. Quantum Computing's Impact on Cybersecurity and the Road Ahead - SecureWorld, accessed on April 12, 2025, https://www.secureworld.io/industry-news/quantum-computing-impact-cybersecurity
35. The status of quantum computer development - BSI, accessed on April 12, 2025, https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer.html
36. For the first time ever researchers crack RSA and AES data encryption - Reddit, accessed on April 12, 2025, https://www.reddit.com/r/QuantumComputing/comments/1gwhafk/for_the_first_time_ever_researchers_crack_rsa_and/
37. Could Quantum Computers Quickly Crack Ransomware Encryption?, accessed on April 12, 2025, https://security.stackexchange.com/questions/265866/could-quantum-computers-quickly-crack-ransomware-encryption
38. Is AES-128 quantum safe? - Cryptography Stack Exchange, accessed on April 12, 2025, https://crypto.stackexchange.com/questions/102671/is-aes-128-quantum-safe
39. Some Initial Thoughts about Quantum Malware - Columbia Academic Commons, accessed on April 12, 2025, https://academiccommons.columbia.edu/doi/10.7916/adrm-1j61/download
40. A Detailed Analysis of the Quantum Ransomware | SecurityScorecard, accessed on April 12, 2025, https://securityscorecard.com/wp-content/uploads/2024/01/Research-A-Detailed-Analysis-Of-The-Quantum-Ransomware.pdf
41. Use Quantum To Protect Against Data Ransom Cyberattacks Today - Forbes, accessed on April 12, 2025, https://www.forbes.com/councils/forbestechcouncil/2024/07/02/use-quantum-to-protect-against-data-ransom-cyberattacks-today/

42. Cyber Insights 2025: Quantum and the Threat to Encryption - SecurityWeek, accessed on April 12, 2025, https://www.securityweek.com/cyber-insights-2025-quantum-and-the-threat-to-encryption/
43. Q-Day: Estimating and Preparing for Quantum Disruption in Cybersecurity | Secureworks, accessed on April 12, 2025, https://www.secureworks.com/blog/predicting-q-day-and-impact-of-breaking-rsa2048
44. Quantum Computing Breakthrough: A New Era for Data Encryption - Ready Networks, accessed on April 12, 2025, https://www.readynetworks.com/quantum-computing-breakthrough-a-new-era-for-data-encryption/
45. What Is Quantum Encryption, How Does It Work, and Will It Save Us From Cybercriminals?, accessed on April 12, 2025, https://www.arcserve.com/blog/what-quantum-encryption-how-does-it-work-and-will-it-save-us-cybercriminals
46. Microsoft's Quantum Chip Breakthrough Accelerates Threat to Encryption, accessed on April 12, 2025, https://www.infosecurity-magazine.com/news/microsoft-quantum-chip-encryption/
47. Demystifying the Connection Between Quantum Computing & Encryption - Portal26, accessed on April 12, 2025, https://portal26.ai/demystifying-the-connection-between-quantum-computing-and-encryption/
48. Quantum Computing: Decrypting The Future - Cybercrime Magazine, accessed on April 12, 2025, https://cybersecurityventures.com/quantum-computing-decrypting-the-future/
49. What Is Quantum Computing's Threat to Cybersecurity? - Palo Alto Networks, accessed on April 12, 2025, https://www.paloaltonetworks.in/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity
50. Quantum Computing and Cybersecurity – Preparing for a New Age of Threats | MSSP Alert, accessed on April 12, 2025, https://www.msspalert.com/native/quantum-computing-and-cybersecurity-preparing-for-a-new-age-of-threats
51. Kaspersky predicts quantum-proof ransomware and advancements in mobile financial cyberthreats in 2025, accessed on April 12, 2025, https://www.kaspersky.com/about/press-releases/kaspersky-predicts-quantum-proof-ransomware-and-advancements-in-mobile-financial-cyberthreats-in-2025
52. The Next Wave of Ransomware Attacks: Quantum Computing - A Critical Imperative, accessed on April 12, 2025, https://www.halcyon.ai/blog/the-next-wave-of-ransomware-attacks-quantum-computing-a-critical-imperative
53. Kaspersky predicts quantum-proof ransomware and advancements in mobile financial cyberthreats in 2025, accessed on April 12, 2025, https://me-en.kaspersky.com/about/press-releases/kaspersky-predicts-quantum-proof-ransomware-and-advancements-in-mobile-financial-cyberthreats-in-2025

54. Ransomware Costs Surge as Quantum Computing Risks Loom: How Data Security Stocks Are Responding - PR Newswire, accessed on April 12, 2025, https://www.prnewswire.com/news-releases/ransomware-costs-surge-as-quantum-computing-risks-loom-how-data-security-stocks-are-responding-302266057.html
55. Next steps in preparing for post-quantum cryptography - NCSC.GOV.UK, accessed on April 12, 2025, https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
56. NIST Releases First 3 Finalized Post-Quantum Encryption Standards, accessed on April 12, 2025, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
57. Quantum Plus AI Widens Cyberattack Threat Concerns - Semiconductor Engineering, accessed on April 12, 2025, https://semiengineering.com/quantum-plus-ai-widens-cyberattack-threat-concerns/
58. Quantum Computing, Artificial Intelligence, and the Cybersecurity Threat Landscape, accessed on April 12, 2025, https://www.accessitgroup.com/quantum-computing-artificial-intelligence-and-the-cybersecurity-threat-landscape/
59. What is Quantum Ransomware? - SOC Prime, accessed on April 12, 2025, https://socprime.com/blog/what-is-quantum-ransomware/
60. Strategies to Prolong Quantum Ransomware Attacks - Darktrace, accessed on April 12, 2025, https://www.darktrace.com/de/blog/when-speedy-attacks-arent-enough-prolonging-quantum-ransomware
61. An In-Depth Look at Quantum Ransomware - Avertium, accessed on April 12, 2025, https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-quantum-ransomware
62. Quantum | SentinelOne, accessed on April 12, 2025, https://www.sentinelone.com/anthology/quantum/
63. Quantum ransomware attack hits Dominican Republic government agency - Acronis, accessed on April 12, 2025, https://www.acronis.com/en-sg/cyber-protection-center/posts/quantum-ransomware-attack-hits-dominican-republic-government-agency/
64. POSTER: MalaQ -A Malware Against Quantum Computer - ResearchGate, accessed on April 12, 2025, https://www.researchgate.net/publication/381399853_POSTER_MalaQ_-_A_Malware_Against_Quantum_Computer
65. What Is Quantum Cryptography? - IBM, accessed on April 12, 2025, https://www.ibm.com/think/topics/quantum-cryptography
66. Quantum Secure Communication with Entanglement-based Networks, accessed on April 12, 2025, https://www.aliroquantum.com/blog/quantum-secure-communication-through-entanglement-based-networks
67. Quantum cryptography - Wikipedia, accessed on April 12, 2025, https://en.wikipedia.org/wiki/Quantum_cryptography

68. Quantum cybersecurity, accessed on April 12, 2025, https://quantumcomputinginc.com/technology/quantum-cybersecurity
69. Quantum Key Distribution - What Is QKD? How Does It Work? - Toshiba Europe, accessed on April 12, 2025, https://www.toshiba.eu/solutions/quantum/products/quantum-key-distribution/
70. What is Quantum Security? - Palo Alto Networks, accessed on April 12, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-security
71. Quantum Cryptography, Explained, accessed on April 12, 2025, https://quantumxc.com/blog/quantum-cryptography-explained/
72. Is Quantum IP Security a Fraud - Microsoft Community, accessed on April 12, 2025, https://answers.microsoft.com/en-us/msoffice/forum/all/is-quantum-ip-security-a-fraud/6beb44a1-2ba6-4c53-b188-b815bbfb1343
73. Quantum Computing Cybersecurity Explained - NordPass, accessed on April 12, 2025, https://nordpass.com/blog/quantum-computing-cybersecurity/
74. (PDF) Quantum Guard: Pioneering Quantum-Based Malware Defense for IoT Devices, accessed on April 12, 2025, https://www.researchgate.net/publication/384243160_Quantum_Guard_Pioneering_Quantum-Based_Malware_Defense_for_IoT_Devices
75. What Is Spyware? Types, Risks, and Prevention Tips - SentinelOne, accessed on April 12, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-spyware/
76. www.cisa.gov, accessed on April 12, 2025, https://www.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf
77. Spyware: What is it, Types, and Prevention | CrowdStrike, accessed on April 12, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/malware/spyware/
78. What Is Spyware? Definition, Examples & More | Proofpoint UK, accessed on April 12, 2025, https://www.proofpoint.com/uk/threat-reference/spyware
79. Spyware - Wikipedia, accessed on April 12, 2025, https://en.wikipedia.org/wiki/Spyware
80. What Is Spyware? Definition, Examples & More | Proofpoint US, accessed on April 12, 2025, https://www.proofpoint.com/us/threat-reference/spyware
81. Spyware: What It Is and How to Protect Yourself - Kaspersky, accessed on April 12, 2025, https://usa.kaspersky.com/resource-center/threats/spyware
82. Spyware: Cybersecurity Explained | Vation Ventures, accessed on April 12, 2025, https://www.vationventures.com/glossary/spyware-cybersecurity-explained
83. spyware - Glossary | CSRC - NIST Computer Security Resource Center, accessed on April 12, 2025, https://csrc.nist.gov/glossary/term/spyware
84. www.secureworld.io, accessed on April 12, 2025, https://www.secureworld.io/industry-news/quantum-computing-impact-cybersecurity#:~:text=Cybercriminals%20and%20nation%2Dstate%20adversaries,%2C%20and%20AI%2Ddriven%20cyberattacks.
85. Quantum's Impact on Cybersecurity: The Hero and Villain - Viva Technology, accessed on April 12, 2025, https://vivatechnology.com/news/quantum-s-

impact-on-cybersecurity
86. The impact on cybersecurity | Introduction to Quantum Computing for Business, accessed on April 12, 2025, https://introtoquantum.org/applications/cybersecurity/
87. Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure - arXiv, accessed on April 12, 2025, https://arxiv.org/html/2404.10659v1
88. Quantum Computers: What Is Q-Day? And What's the Solution? - GovTech, accessed on April 12, 2025, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/quantum-computers-what-is-q-day-and-whats-the-solution
89. Quantum computers will be a dream come true for hackers, risking everything from military secrets to bank information. Can we stop them? - Live Science, accessed on April 12, 2025, https://www.livescience.com/technology/computing/quantum-computers-will-be-a-dream-come-true-for-hackers-risking-everything-from-military-secrets-to-bank-information-can-we-stop-them
90. The future has arrived for securing confidential data | Physics Today - AIP Publishing, accessed on April 12, 2025, https://pubs.aip.org/physicstoday/article/76/11/21/2917785/The-future-has-arrived-for-securing-confidential
91. Cracking with Quantum: What Breakthrough Research Means | Cyber Magazine, accessed on April 12, 2025, https://cybermagazine.com/articles/cracking-with-quantum-what-breakthrough-research-means
92. The Future of Quantum-Resistant Cryptography: A Data Security Perspective - Fortanix, accessed on April 12, 2025, https://www.fortanix.com/blog/the-future-of-quantum-resistant-cryptography-a-data-security-perspective
93. Quantum Computing and the Evolving Cyber Threat Landscape - The Soufan Center, accessed on April 12, 2025, https://thesoufancenter.org/intelbrief-2024-november-15/
94. The Rise and Risks of Quantum Computing in 2025 | Built In, accessed on April 12, 2025, https://builtin.com/articles/rise-risk-quantum-computing
95. A guide to ransomware - NCSC.GOV.UK, accessed on April 12, 2025, https://www.ncsc.gov.uk/ransomware/home
96. What Is Ransomware? - IBM, accessed on April 12, 2025, https://www.ibm.com/think/topics/ransomware
97. What Is Malware? - Types of Malware Attacks | Proofpoint US, accessed on April 12, 2025, https://www.proofpoint.com/us/threat-reference/malware
98. Ransomware - FBI, accessed on April 12, 2025, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware
99. www.crowdstrike.com, accessed on April 12, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/#:~:text=Ransomware%20is%20a%20type%20of,restore%20access%20to%20their%20files.

100. Ransomware 101 - CISA, accessed on April 12, 2025, https://www.cisa.gov/stopransomware/ransomware-101
101. Why post-quantum security planning must start today - Washington Technology, accessed on April 12, 2025, https://www.washingtontechnology.com/opinion/2025/03/why-post-quantum-security-planning-must-start-today/403692/
102. The Quantum Threat Timeline: Why Organizations Must Act Now - evolutionQ, accessed on April 12, 2025, https://www.evolutionq.com/post/the-quantum-threat-timeline-why-organizations-must-act-now
103. What Is Post-Quantum Cryptography? | NIST, accessed on April 12, 2025, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography
104. NIST recommends timelines for transitioning cryptographic algorithms | PQShield, accessed on April 12, 2025, https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/
105. Cryptographically Relevant Quantum Computers | InfoSec Global, accessed on April 12, 2025, https://www.infosecglobal.com/posts/when-will-cryptographically-relevant-quantum-computers-exist
106. Preparing for Post Quantum Cryptography - Oracle Blogs, accessed on April 12, 2025, https://blogs.oracle.com/security/post/post-quantum-cryptography
107. What Are the Implications of Quantum Computing for the Future of Data Security? | socPub, accessed on April 12, 2025, https://socpub.com/articles/what-are-implications-quantum-computing-future-data-security-17926
108. Fortifying the Digital Fortress: Insights on Ransomware, Exfiltration, and More - ShardSecure, accessed on April 12, 2025, https://shardsecure.com/blog/digital-fortress-ransomware-exfiltration
109. How Quantum Computing Will Change Encryption Forever - Bitdefender, accessed on April 12, 2025, https://www.bitdefender.com/en-us/blog/businessinsights/how-quantum-computing-will-change-encryption-forever
110. Inside Quantum Technology's “Inside Scoop:” Quantum and Stealth Technology, accessed on April 12, 2025, https://www.insidequantumtechnology.com/news-archive/inside-quantum-technologys-inside-scoop-quantum-and-stealth-technology/
111. Quantum Sensors—Unlike Quantum Computers—Are Already Here - Defense One, accessed on April 12, 2025, https://www.defenseone.com/ideas/2022/06/quantum-sensorsunlike-quantum-computersare-already-here/368634/
112. QNu Labs - QKD, QRNG, PQC, Quantum Cryptography Solutions, accessed on April 12, 2025, https://www.qnulabs.com/
113. QuamCore Emerges From Stealth With $9 Million to Build a Quantum Computer, accessed on April 12, 2025, https://www.securityweek.com/quamcore-emerges-from-stealth-with-9-million-to-build-a-quantum-computer/
114. Quantum Stealth : The Science of Invisibility - YouTube, accessed on April 12,

2025, https://www.youtube.com/watch?v=lwy5Mfq4Gdw
115. Hybrid Classical Quantum Learning Model Framework for Detection of Deepfake Audio - SciTePress, accessed on April 12, 2025, https://www.scitepress.org/publishedPapers/2025/132587/pdf/index.html
116. Generative Quantum Machine Learning for Finance - IonQ, accessed on April 12, 2025, https://ionq.com/resources/generative-quantum-machine-learning-for-finance
117. Deepfakes: The Technology of Deception and Quantum's Uncertain Future With the Problem, accessed on April 12, 2025, https://thequantumrecord.com/philosophy-of-technology/deepfake-technology-of-deception-and-quantum-future/
118. Quantum-Trained Convolutional Neural Network for Deepfake Audio Detection * Corresponding Author - arXiv, accessed on April 12, 2025, https://arxiv.org/html/2410.09250v1
119. Full article: PegasosQSVM: A Quantum Machine Learning Approach for Accurate Fake News Detection - Taylor & Francis Online, accessed on April 12, 2025, https://www.tandfonline.com/doi/full/10.1080/08839514.2025.2457207?af=R
120. Deepfake Audio Detection Using Quantum Learning Models - Inspire HEP, accessed on April 12, 2025, https://inspirehep.net/literature/2893110
121. [2410.09250] Quantum-Trained Convolutional Neural Network for Deepfake Audio Detection - arXiv, accessed on April 12, 2025, https://arxiv.org/abs/2410.09250
122. Quantum Machine Learning-based Detection of Fake News and Deep Fake Videos | Request PDF - ResearchGate, accessed on April 12, 2025, https://www.researchgate.net/publication/362008472_Quantum_Machine_Learning-based_Detection_of_Fake_News_and_Deep_Fake_Videos
123. (PDF) Quantum-Powered Deepfake Detection - ResearchGate, accessed on April 12, 2025, https://www.researchgate.net/publication/390056776_Quantum-Powered_Deepfake_Detection/download
124. Inside Quantum Technology's Inside Scoop: Quantum and Deepfake Technology, accessed on April 12, 2025, https://www.insidequantumtechnology.com/news-archive/inside-quantum-technologys-inside-scoop-quantum-and-deepfake-technology-2/
125. 2025 Cyber Security Predictions: The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation - Part 1 | DEVOPSdigest, accessed on April 12, 2025, https://www.devopsdigest.com/2025-cyber-security-predictions-the-rise-of-ai-driven-attacks-quantum-threats-and-social-media
126. Computer Viruses Are Evolving: From Creeper to Quantum-Resistant Malware, accessed on April 12, 2025, https://www.emazzanti.net/computer-viruses-are-evolving-from-creeper-to-quantum-resistant-malware/
127. Building more investment and support for quantum computing - The World Economic Forum, accessed on April 12, 2025,

https://www.weforum.org/stories/2025/04/quantum-computing-benefit-businesses/
128. 2025 Will See Huge Advances in Quantum Computing. So What is a Quantum Chip And How Does it Work?, accessed on April 12, 2025, https://thequantuminsider.com/2025/01/08/2025-will-see-huge-advances-in-quantum-computing-so-what-is-a-quantum-chip-and-how-does-it-work/
129. 5 Best Quantum Computing Companies of 2025 - Securities.io, accessed on April 12, 2025, https://www.securities.io/quantum-computing-companies-2025/
130. 2025 is the year of quantum computing (already) - Constellation Research, accessed on April 12, 2025, https://www.constellationr.com/blog-news/insights/2025-year-quantum-computing-already
131. How Many Quantum Computers Are There in 2025? - SpinQ, accessed on April 12, 2025, https://www.spinquanta.com/news-detail/how-many-quantum-computers-are-there
132. 6 Types of Quantum Computers You Need to Know in 2025 - SpinQ, accessed on April 12, 2025, https://www.spinquanta.com/news-detail/types-of-quantum-computers-you-need-to-know-in20250226071709
133. IBM will release the largest ever quantum computer in 2025 - Viasat Satellite Internet, accessed on April 12, 2025, https://www.rsinc.com/ibm-will-release-the-largest-ever-quantum-computer-in-2025.php
134. Do Quantum Computers Exist in 2025? The Answer is Yes - SpinQ, accessed on April 12, 2025, https://www.spinquanta.com/news-detail/do-quantum-computers-exist-in-the-answer-is-yes20250115030355
135. www.spinquanta.com, accessed on April 12, 2025, https://www.spinquanta.com/news-detail/do-quantum-computers-exist-in-the-answer-is-yes20250115030355#:~:text=We%20are%20still%20in%20the,work%20remains%20to%20be%20done.
136. Discover the World's Largest Quantum Computer in 2025 - SpinQ, accessed on April 12, 2025, https://www.spinquanta.com/news-detail/discover-the-worlds-largest-quantum-computer-in20250106092507
137. Quantinuum's H-Series hits 56 physical qubits that are all-to-all ..., accessed on April 12, 2025, https://www.quantinuum.com/blog/quantinuums-h-series-hits-56-physical-qubits-that-are-all-to-all-connected-and-departs-the-era-of-classical-simulation
138. Microsoft unveils Majorana 1, the world's first quantum processor ..., accessed on April 12, 2025, https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/
139. IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two - IBM Newsroom, accessed on April 12, 2025, https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

140. IBM's Quantum Computing: Roadmap to 4000 Qubit System by 2025 - Tomorrow Desk, accessed on April 12, 2025, https://tomorrowdesk.com/breakthrough/ibm-quantum-computing-4000-qubit
141. www.spinquanta.com, accessed on April 12, 2025, https://www.spinquanta.com/news-detail/discover-the-worlds-largest-quantum-computer-in20250106092507#:~:text=The%20world's%20largest%20quantum%20computer%20is%20here%2C%20featuring%201121%20record,the%20boundaries%20of%20quantum%20technology.
142. A new Microsoft chip could lead to more stable quantum computers - Reddit, accessed on April 12, 2025, https://www.reddit.com/r/QuantumComputing/comments/1it9u72/a_new_microsoft_chip_could_lead_to_more_stable/
143. Post-Quantum Cryptography (PQC) - Challenges and obstacles to adoption | IDEMIA, accessed on April 12, 2025, https://www.idemia.com/insights/key-obstacles-post-quantum-cryptography-pqc-adoption
144. Microsoft's Majorana 1 chip carves new path for quantum computing - Source, accessed on April 12, 2025, https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/
145. The Current State of Quantum Computing, accessed on April 12, 2025, https://www.computer.org/publications/tech-news/research/current-state-of-quantum-computing
146. Quantum Computing in 2024: Breakthroughs, Challenges, and What Lies Ahead, accessed on April 12, 2025, https://microtime.com/quantum-computing-in-2024-breakthroughs-challenges-and-what-lies-ahead/
147. Quantum Computers Cross Critical Error Threshold | Quanta Magazine, accessed on April 12, 2025, https://www.quantamagazine.org/quantum-computers-cross-critical-error-threshold-20241209/
148. Quantum Error Correction in 2025: Progress and Persistent Challenges - Java Code Geeks, accessed on April 12, 2025, https://www.javacodegeeks.com/2025/04/quantum-error-correction-in-2025-progress-and-persistent-challenges.html
149. Quantum computing in 2025: risk and reward - BI Foresight, accessed on April 12, 2025, https://biforesight.com/quantum/quantum-computing-in-2025-risk-and-reward/
150. Will 2025 mark the beginning of practically useful quantum ..., accessed on April 12, 2025, https://www.orfonline.org/expert-speak/will-2025-mark-the-beginning-of-practically-useful-quantum-computers
151. Practical quantum computing advances ramp up going into 2025 - Constellation Research, accessed on April 12, 2025, https://www.constellationr.com/blog-news/insights/practical-quantum-computing-advances-ramp-going-2025
152. Why do quantum computers need QEC - Riverlane, accessed on April 12, 2025,

https://www.riverlane.com/blog/why-do-quantum-computers-need-qec
153. Three New Error Correction Papers for the End of the Year - Quantum Computing Report, accessed on April 12, 2025, https://quantumcomputingreport.com/three-new-error-correction-papers-for-the-end-of-the-year/
154. Guest Post: What's Next for Quantum Error Correction?, accessed on April 12, 2025, https://thequantuminsider.com/2025/02/08/guest-post-whats-next-for-quantum-error-correction/
155. Quantum computing's six most important trends for 2025 - Moody's, accessed on April 12, 2025, https://www.moodys.com/web/en/us/insights/quantum/quantum-computings-six-most-important-trends-for-2025.html
156. Alice & Bob improve cat qubit error rates with 'squeezing' technique - SiliconANGLE, accessed on April 12, 2025, https://siliconangle.com/2025/03/11/alice-bob-improve-cat-qubit-error-rates-squeezing-technique/
157. The Next Big Cyber Threat Could Come from Quantum Computers... Is the Government Ready? - GAO, accessed on April 12, 2025, https://www.gao.gov/blog/next-big-cyber-threat-could-come-quantum-computers-government-ready
158. Quantum Computing and Cybersecurity: A Threat & an Ally for Security Solutions, accessed on April 12, 2025, https://www.provendata.com/blog/quantum-computing-cybersecurity/
159. The quantum threat: Addressing challenges in post-quantum cryptography - Outshift - Cisco, accessed on April 12, 2025, https://outshift.cisco.com/blog/post-quantum-cryptography-addressing-challenges
160. "What are the emerging threats in cybersecurity due to the adoption of quantum computing, and how can classical encryption techniques be adapted? | ResearchGate, accessed on April 12, 2025, https://www.researchgate.net/post/What_are_the_emerging_threats_in_cybersecurity_due_to_the_adoption_of_quantum_computing_and_how_can_classical_encryption_techniques_be_adapted
161. Evaluating Cryptographic Vulnerabilities Created by Quantum Computing in Industrial Control Systems | RAND, accessed on April 12, 2025, https://www.rand.org/pubs/research_reports/RRA2427-1.html
162. Technology Security - National Quantum Initiative, accessed on April 12, 2025, https://www.quantum.gov/security/
163. Timelines for migration to post-quantum cryptography - NCSC.GOV.UK, accessed on April 12, 2025, https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
164. The timelines: when can we expect useful quantum computers?, accessed on April 12, 2025, https://introtoquantum.org/essentials/timelines/

165. 2023 Quantum Threat Timeline Report Published - PostQuantum.com, accessed on April 12, 2025, https://postquantum.com/industry-news/quantum-threat-timeline-report/
166. Is Quantum Computing a Cybersecurity Threat? | American Scientist, accessed on April 12, 2025, https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat
167. The Evolution of Cyber Threats: Past, Present and Future, accessed on April 12, 2025, https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats
168. What Is a Ransomware Attack? - CrowdStrike.com, accessed on April 12, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/
169. Ransomware - Wikipedia, accessed on April 12, 2025, https://en.wikipedia.org/wiki/Ransomware
170. What is a Malware Attack? - Definition - CyberArk, accessed on April 12, 2025, https://www.cyberark.com/what-is/malware/
171. What is Ransomware? – Definition - CyberArk, accessed on April 12, 2025, https://www.cyberark.com/what-is/ransomware/
172. Ransomware - Definition | Trend Micro (US), accessed on April 12, 2025, https://www.trendmicro.com/vinfo/us/security/definition/ransomware
173. Ransomware Attack - What is it and How Does it Work? - Check Point Software, accessed on April 12, 2025, https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/
174. What is Malware? Malware Definition, Types and Protection - Malwarebytes, accessed on April 12, 2025, https://www.malwarebytes.com/malware
175. What Is Ransomware? - Definition, Prevention & More | Proofpoint US, accessed on April 12, 2025, https://www.proofpoint.com/us/threat-reference/ransomware
176. What Is Malware? Definition and Types | Microsoft Security, accessed on April 12, 2025, https://www.microsoft.com/en-us/security/business/security-101/what-is-malware
177. What is malware and how cybercriminals use it - McAfee, accessed on April 12, 2025, https://www.mcafee.com/en-us/antivirus/malware.html
178. What Is Malware? - Palo Alto Networks, accessed on April 12, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-malware
179. Can Quantum Computers crack RSA and AES? - Cryptography Stack Exchange, accessed on April 12, 2025, https://crypto.stackexchange.com/questions/105509/can-quantum-computers-crack-rsa-and-aes
180. Security Aspects of Quantum Machine Learning (SecQML) - BSI, accessed on April 12, 2025, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/QML/QML_Security_Aspects.pdf?__blob=publicationFile&v=4
181. QubitHammer Attacks: Qubit Flipping Attacks in Multi-tenant Superconducting Quantum ComputersThis work was supported in part by NSF grants 2223046 and 2312754. - arXiv, accessed on April 12, 2025, https://arxiv.org/html/2504.07875v1

182. Chapter: Vulnerability of Quantum Information Systems to Collective Manipulation, accessed on April 12, 2025, https://dev.to/mikeyoung44/chapter-vulnerability-of-quantum-information-systems-to-collective-manipulation-1a56
183. Predominant Aspects on Security for Quantum Machine Learning: Literature Review - arXiv, accessed on April 12, 2025, https://arxiv.org/html/2401.07774v3
184. Quantum Circuit Reconstruction from Power Side-Channel Attacks - Department of Computer Science, accessed on April 12, 2025, https://www.cs.yale.edu/homes/piskac/papers/2024-TCHES.pdf
185. (PDF) Quantum Deep Neural Network Based Classification of Attack Vectors on the Ethereum Blockchain - ResearchGate, accessed on April 12, 2025, https://www.researchgate.net/publication/379347849_Quantum_Deep_Neural_Network_Based_Classification_of_Attack_Vectors_on_the_Ethereum_Blockchain
186. Attack Vectors of Quantum Computers - Sorin Boloș and Adrian Coleșa @ Quantum Village, DEF CON 32 - YouTube, accessed on April 12, 2025, https://www.youtube.com/watch?v=DefQhmpdgLg
187. Cybersecurity of Quantum Computing: A New Frontier - SEI Blog, accessed on April 12, 2025, https://insights.sei.cmu.edu/blog/cybersecurity-of-quantum-computing-a-new-frontier/
188. A novel model for malware propagation on wireless sensor networks - AIMS Press, accessed on April 12, 2025, https://www.aimspress.com/article/doi/10.3934/mbe.2024176?viewType=HTML
189. US20240073226A1 - Quantum computing machine learning for security threats - Google Patents, accessed on April 12, 2025, https://patents.google.com/patent/US20240073226A1/en?oq=US20240073226A1
190. Quantum Machine Learning in the Context of IT Security - BSI, accessed on April 12, 2025, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/QML/QML_in_the_Context_of_IT_Security.pdf?__blob=publicationFile&v=2
191. Research on Virus Propagation Network Intrusion Detection Based on Graph Neural Network - MDPI, accessed on April 12, 2025, https://www.mdpi.com/2227-7390/12/10/1534
192. Markov-Based Malware Propagation Modeling and Analysis in Multi-Layer Networks - MDPI, accessed on April 12, 2025, https://www.mdpi.com/2673-8732/2/3/28
193. Can quantum computers be infected by viruses? : r/QuantumComputing - Reddit, accessed on April 12, 2025, https://www.reddit.com/r/QuantumComputing/comments/kn8ahk/can_quantum_computers_be_infected_by_viruses/
194. Quantum Entanglement-Based Signature Detection for ... - OSF, accessed on April 12, 2025, https://osf.io/93upj/download/?format=pdf
195. The cybersecurity crossroads: AI and quantum computing could save or endanger us, accessed on April 12, 2025,

https://www.ynetnews.com/business/article/bjpsrj9y1g
196. Quantum AI Meets Cybersecurity: The Next Frontier in Threat Detection - Ena Vc, accessed on April 12, 2025, https://ena.vc/quantum-ai-meets-cybersecurity-the-next-frontier-in-threat-detection/
197. Researchers Develop Quantum-inspired Algorithm That Improves Cyber Attack Detection And Opens AI's 'Black Box', accessed on April 12, 2025, https://thequantuminsider.com/2024/03/28/researchers-develop-quantum-inspired-algorithm-that-improves-cyber-attack-detection-and-opens-ais-black-box/
198. Strategies to Prolong Quantum Ransomware Attacks - Darktrace, accessed on April 12, 2025, https://darktrace.com/blog/when-speedy-attacks-arent-enough-prolonging-quantum-ransomware
199. An Advanced Quantum-Entropy Based Ransomware Detection Mechanism - OSF, accessed on April 12, 2025, https://osf.io/6csq7/download/
200. Scientists create world's 1st chip that can protect data in the age of quantum computing attacks | Live Science, accessed on April 12, 2025, https://www.livescience.com/technology/computing/scientists-create-worlds-1st-chip-that-can-protect-data-in-the-age-of-quantum-computing-attacks
201. Challenges of Upgrading to Post-Quantum Cryptography (PQC), accessed on April 12, 2025, https://postquantum.com/post-quantum/pqc-challenges/
202. The Rise of Quantum-Resistant Cryptography, accessed on April 12, 2025, https://www.computer.org/publications/tech-news/trends/quantum-resistant-cryptography/
203. Challenges with Adopting Post-Quantum Cryptographic Algorithms: Final Version of Cybersecurity White Paper Published | NIST, accessed on April 12, 2025, https://www.nist.gov/news-events/news/2021/04/challenges-adopting-post-quantum-cryptographic-algorithms-final-version
204. Post-Quantum Cryptography | CSRC, accessed on April 12, 2025, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
205. NIST Post-Quantum Cryptography Standardization - Wikipedia, accessed on April 12, 2025, https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization
206. NIST Post-Quantum Cryptography Update - PKI Consortium, accessed on April 12, 2025, https://pkic.org/events/2025/pqc-conference-austin-us/WED_PLENARY_1000_Bill-N_Andrew-R_NIST-PQ-Crypto-Update.pdf
207. Post-Quantum Cryptography Is a Must to Protect Your Systems | Gartner, accessed on April 12, 2025, https://www.gartner.com/en/articles/post-quantum-cryptography
208. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process, accessed on April 12, 2025, https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process

209. NIST advances post-quantum cryptography standardization, selects HQC algorithm to counter quantum threats - Industrial Cyber, accessed on April 12, 2025, https://industrialcyber.co/nist/nist-advances-post-quantum-cryptography-standardization-selects-hqc-algorithm-to-counter-quantum-threats/
210. Post Quantum Cryptography: Algorithms & Security | Synopsys Blog, accessed on April 12, 2025, https://www.synopsys.com/blogs/chip-design/post-quantum-cryptography-algorithms-security.html
211. IR 8545, Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process | CSRC, accessed on April 12, 2025, https://csrc.nist.gov/pubs/ir/8545/final
212. NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption ..., accessed on April 12, 2025, https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption
213. PQC News: NIST announces HQC as fifth algorithm to be standardized - Utimaco, accessed on April 12, 2025, https://utimaco.com/news/blog-posts/pqc-news-nist-announces-hqc-fifth-algorithm-be-standardized
214. NIST selects backup algorithm for general encryption against quantum cyberattacks, accessed on April 12, 2025, https://fedscoop.com/nist-backup-algorithm-general-encryption-quantum-cyberattacks-pqc/
215. NIST PQC Standardization Process | HQC Announced as a 4th Round Selection, accessed on April 12, 2025, https://www.nist.gov/news-events/news/2025/03/nist-pqc-standardization-process-hqc-announced-4th-round-selection
216. 7 Predictions For Quantum Resilience In 2025 - Forbes, accessed on April 12, 2025, https://www.forbes.com/councils/forbestechcouncil/2025/01/24/7-predictions-for-quantum-resilience-in-2025/
217. Post-Quantum Cryptography | CSRC - NIST Computer Security Resource Center, accessed on April 12, 2025, https://csrc.nist.gov/projects/post-quantum-cryptography
218. What is Post-Quantum Cryptography (PQC)? - Palo Alto Networks, accessed on April 12, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc
219. Why the new NIST standards mean quantum cryptography may just have come of age, accessed on April 12, 2025, https://www.weforum.org/stories/2024/10/quantum-cryptography-nist-standards/
220. Post-Quantum Cryptography: Migrating to Quantum Resistant Cryptography | Trend Micro (US), accessed on April 12, 2025, https://www.trendmicro.com/vinfo/us/security/news/security-technology/post-quantum-cryptography-migrating-to-quantum-resistant-cryptography
221. Why IT Leaders are Fast-Tracking Post-Quantum Cryptography | Technology Magazine, accessed on April 12, 2025, https://technologymagazine.com/articles/why-it-leaders-are-fast-tracking-post-

quantum-cryptography
222. Why Isn't Post-Quantum Encryption More Widely Adopted Yet? : r/QuantumComputing, accessed on April 12, 2025, https://www.reddit.com/r/QuantumComputing/comments/1blpt3u/why_isnt_post_quantum_encryption_more_widely/
223. Quantum Cryptography: Challenges and Opportunities for Federal Agencies, accessed on April 12, 2025, https://fedtechmagazine.com/quantum-cryptography-challenges-opportunities-perfcon
224. Preparing your organization for the quantum threat to cryptography (ITSAP.00.017), accessed on April 12, 2025, https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017
225. Broadcom Delivers Industry's First Quantum Resistant Network Encryption, Enabling Real-time Ransomware Detection, accessed on April 12, 2025, https://investors.broadcom.com/news-releases/news-release-details/broadcom-delivers-industrys-first-quantum-resistant-network
226. The Cohesity post-quantum cryptography strategy, accessed on April 12, 2025, https://www.cohesity.com/blogs/the-cohesity-post-quantum-cryptography-strategy/