POST-PQC STRATEGIES FOR FINANCIAL CYBERSECURITY

Catharina Cerny
Olga Mamlyga
Tatiana Mitrova
Oswaldo Zapata

Post-PQC Strategies for Financial Cybersecurity

Catharina Cerny,[1] Olga Mamlyga,[2] Tatiana Mitrova,[3] and Oswaldo Zapata.[4]

Abstract. The advent of quantum computing poses an imminent challenge to global cybersecurity, particularly for sectors where digital assets and critical infrastructure are at stake. While Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) offer transitional protections, their limitations highlight the need for systemic resilience that integrates hardware, software, and network safeguards. Hybrid quantum-classical attacks, accelerated by advances in artificial intelligence, further amplify risks, exposing vulnerabilities in financial systems, energy grids, and communication networks. This paper argues that fragmented, reactive security measures are no longer sufficient. Instead, a shift toward integrated, agile architectures is essential to withstand the accelerating complexity of threats.

1. Introduction

We agree with the consensus that **post-quantum cryptography (PQC)**[5] is essential for securing data in the era of quantum computers. However, it is important to recognize that PQC relies on our current understanding of mathematics, and significant advances in mathematical techniques could threaten the security of today's encryption methods. Achieving true post-quantum safety is therefore a challenging task. For example, in the **National Institute of Standards and Technology (NIST)** competition launched in late 2017, 82 candidate algorithms were submitted—23 signature schemes and 59 encryption/KEM schemes—of which 69 were considered complete and advanced to the first round[6]. After several rigorous evaluation rounds, on August 13, 2024, NIST announced the final versions of the first three PQC standards: FIPS 203, FIPS 204, and FIPS 205. The fact that, out of the original 82 submissions, only three algorithms have been standardized underscores the complexity of this effort. It should also serve as a reminder to the cybersecurity community that even these

[1] Senior Network Engineer.
[2] CEO, Quantum Scouts Aps, Engineering practical solutions in quantum technologies and networks, Member of "The Quantum Finance Boardroom" online community.
[3] Ph.D. International Economics, Research Fellow at the Center on Global Energy Policy at Columbia University.
[4] Ph.D. Theoretical Physics, Co-founder of "The Quantum Finance Boardroom" online community.
[5] For the reader's convenience, a glossary is provided at the end. Glossary terms appear in the main text in capital letters, and key takeaways are italicized for easier reference.
[6] https://csrc.nist.gov/pubs/ir/8240/final

finalists may not be definitively secure against future quantum or mathematical breakthroughs—they represent the best mathematical approaches available today.

From the perspective of highly skilled professional attackers, the introduction of PQC does not eliminate security concerns. In 2022, a Swedish research team demonstrated that even NIST-approved algorithms can be vulnerable at the implementation level. Using a **side-channel attack** combined with recursive machine learning (ML) techniques, they were able to compromise CRYSTALS-Kyber, the key exchange algorithm selected by NIST for standardization[7]. Their paper, "Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste", published in December 2022, highlighted that implementation weaknesses, rather than the mathematical design itself, can still pose significant risks. *This example underscores the need for ongoing scrutiny and robust implementation strategies as PQC transitions into practice.*

This side-channel attack reflects real-world conditions more closely than controlled academic experiments. Whereas academic research often isolates components under laboratory conditions or focuses on abstract mathematical models, skilled attackers typically approach systems holistically, seeking practical points of exploitation. Today, the range of available **attack vectors** has expanded considerably, enabling faster data harvesting and more immediate decryption attempts. Although we will not discuss specific offensive techniques—unlike publications sometimes referred to as "Hacker Bibles", which have leveraged legal loopholes to share potentially harmful information under the guise of education—we acknowledge the growing complexity of the threat landscape. Drawing on more than 30 years of experience at the highest levels of the IT industry, our engineers have been able to anticipate and counter known attack methods to date. *However, the emergence of* ***quantum-based*** *and* ***hybrid cyberattacks*** *signals a fundamental turning point: traditional defensive engineering approaches alone may no longer suffice.* Quantum-enabled attacks redefine the parameters of cybersecurity, requiring a reassessment of existing strategies.

Even without the advent of quantum computers, numerous attack vectors remain available, and it is evident that adversaries are making significant gains. Many of these alternative attack methods are already well understood, and effective defenses can be designed to counter them. *The key to safeguarding data—whether preventing ransomware and extortion or securing cryptocurrencies and stablecoins for the long term—lies in engineering.* A robust security solution must be complex and **multilayered**. True resilience emerges when overlapping safety measures create redundancy across multiple defense layers. In such a system, even if attackers succeed in breaching one, two, or even a substantial fraction of defenses, the overall system can remain secure. This principle of layered engineering is not necessarily a matter of high cost, but rather one of expertise and practical implementation.

The article is organized as follows: Section 2 examines the limitations of Post-Quantum Cryptography (PQC), highlighting why it may not represent the most practical or resilient path forward. Section 3 explores the growing role of artificial intelligence (AI) in enabling novel and more sophisticated forms of cyberattacks. Section 4 discusses the role of NIST in standardizing PQC solutions and the challenges this process entails. Section 5 situates these

[7] https://eprint.iacr.org/2022/1713

developments within their geopolitical context, emphasizing the global implications of a technological arms race among nations. In Section 6, we emphasize the potential consequences of a quantum attack on energy infrastructure. Section 7 considers the advances in quantum computing and their potential to undermine existing cryptographic systems. Finally, Section 8 concludes by underscoring the urgent need for integrated solutions to build systemic resilience and prepare for a new era of cyber threats amplified by quantum technologies. For clarity and reference, a glossary of key terms is provided at the end of the article.

2. PQC: A Fragile Shield

Post-Quantum Cryptography (PQC) should not be regarded as a standalone solution for securing data and systems. Even in advanced security environments, PQC on its own has proven insufficient—and it is likely to remain so—for protecting critical assets.

In practice, encryption is only as strong as the broader environment in which it operates. Its effectiveness depends on the security of the operating system, the integrity of network defenses, and the behavior of end users. If these elements are neglected, breaches are inevitable, leading to the loss of data, financial resources, reputation, and potentially much more. For instance, widely used operating systems have been scrutinized for decades by some of the most capable and persistent adversaries worldwide. The same applies to network traffic and communication infrastructures, which are frequent targets of sophisticated attacks.

State-sponsored groups have demonstrated the ability to conduct highly complex, long-term operations, particularly against critical infrastructure. Sectors such as energy, water supply, healthcare, defence, and finance have all faced targeted campaigns. In some cases, advanced malware remained undetected for years—for example, attackers exploited Microsoft systems within Microsoft's own infrastructure networks for at least five years. *These incidents highlight that the failures stemmed from vulnerabilities caused by poor maintenance and a lack of adequate cybersecurity expertise.*[8]

Organizations that take security seriously are not immune to compromise. *Many large enterprises struggle to keep pace with the rapid evolution of malicious techniques. A common pattern is that smaller and mid-sized companies develop innovative and effective defensive solutions, only to be acquired by larger corporations that often fail to integrate those technologies properly.*

Even leading security vendors have faced incidents more severe than public disclosures suggested. In some cases, official denials conflicted with evidence of continued breaches, and patches released in response proved ineffective once attackers had already obtained deep system access.

---

[8] https://www.deepinstinct.com/blog/malicious-office-files-20-years-of-microsoft-office-exploits; https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/.

When operating systems and networks remain vulnerable, attackers can exploit them regardless of PQC adoption. PQC alone cannot guarantee safety. Cybercriminals are already capable of downloading and decrypting data in real time, though in practice decryption is not always their primary objective. In many cases, attackers are less interested in stealing data than in maintaining hidden, long-term access, deliberately disrupting critical operations, or using their control to demand ransom or other forms of extortion. *These threats do not depend on the advent of quantum computing. Moreover, artificial intelligence has become a powerful enabler, allowing even less skilled adversaries to launch sophisticated attacks without requiring advanced expertise.*

Public Key Infrastructure (PKI) is widely used to distribute cryptographic keys, but it also represents a significant vulnerability in the context of PQC. Although PKI has been a foundational security mechanism for decades, its practical implementation introduces weaknesses. For example, users or recipients are often required to manually install certificates into their browsers or software. While administrators can perform this task remotely, in practice it is more commonly left to end users. Proper validation requires checking all certificate fields, yet this rarely occurs, creating opportunities for attackers. *This human factor is one of the common reasons certificate-based systems are exploited, and the introduction of PQC does not address this problem.*

Pre-installing certificates on devices, such as laptops, could mitigate some risks, but this does not resolve the challenge of certificate renewal, since certificates are time-limited. *Ultimately, only carefully engineered and comprehensive security solutions can improve resilience at scale.*

Attackers may also impersonate a **Certificate Authority (CA)**. If a system's protective tools fail to raise an alarm, malicious certificates can be trusted by devices, enabling unauthorized access. The risk extends further: adversaries frequently target the servers that store CA data, manipulating certificate databases to compromise large numbers of users at once.

This brings us to a final and particularly critical point: the **Certificate Management System (CMS)**. The CMS distributes certificates to end devices, which then verify them against the Certificate Authority (CA) to establish trust. In most cases, this process is managed through operating system software or network management tools. However, if portions of source code or root certificates are stolen from major operating system vendors or network device providers, the trust chain can be undermined. In such cases, certificate distribution itself becomes a potential point of failure rather than a safeguard.

Notably, these vulnerabilities do not require quantum computing to exploit. Instead, they reflect longstanding structural issues in cybersecurity practices. In many organizations, strategic decision-making has historically prioritized cost efficiency over security, and senior security experts are often absent from executive leadership roles. This lack of representation may lead to insufficient consideration of cybersecurity as a critical factor for organizational resilience and continuity.

3. AI-powered Attacks

The rise of artificial intelligence has dramatically lowered the barriers to launching sophisticated cyberattacks. Tools that once required expert knowledge are now packaged in user-friendly formats, enabling even individuals with minimal experience to execute highly effective operations. Many of these tools are openly promoted, refined through global red-team exercises, and widely accessible. As a result, AI has pushed social engineering to unprecedented levels of sophistication, producing written, audio, and video content so convincing that even vigilant users can be deceived.

The insights presented here draw on the expertise of Quantum Scouts ApS specialists, who highlight several worrying trends. One involves AI-powered prompt injection, where attackers trick an AI system into revealing sensitive information it was trained on or into performing actions it was not intended to. Similarly, reverse-engineering can be used to uncover hidden details from databases, while prompt engineering allows attackers to phrase questions in ways that coax confidential information out of everyday business systems. At the same time, generative AI has supercharged social engineering—the art of deceiving people into sharing secrets—by producing fake emails, messages, or videos so convincing that they are nearly impossible to distinguish from real communication. As a result, phishing, once fairly easy to spot, is now highly polished and alarmingly effective.

These risks are compounded by machine learning, which allows attackers to analyse how individuals behave online—their writing style, habits, and even social connections—in order to craft extremely personal and convincing phishing attempts. But the threat goes beyond phishing. AI is also being used to scan networks for weaknesses, insert malicious code, and run ransomware campaigns automatically. Since **Ransomware-as-a-Service (RaaS)** is now sold like a subscription product, attackers no longer need advanced technical skills or expensive hardware. AI even helps them decide *when* to strike, identifying the moments when systems are least protected and most likely to fail.

Another emerging danger is fileless malware, a type of malicious software that runs entirely in a computer's memory rather than being stored on its hard drive. Because there are no traditional files to scan, standard antivirus programs often fail to detect it. AI makes this type of malware even more threatening by allowing it to adapt in real time, hiding its presence while still carrying out harmful actions. Some of the most advanced tools even use live encryption—constantly scrambling their own code—and continuously study a victim's security systems to find ways around them. Out of caution, the names of such tools are not mentioned here to prevent misuse.

AI is also making cyberattacks more autonomous. Certain malware can now "learn" how to avoid detection on its own, spreading through networks in minutes without human guidance.

Ransomware has become more destructive as well, with AI helping attackers identify and target the most valuable data—such as financial records, proprietary business databases, or intellectual property. By disguising itself as normal system activity and launching attacks during nights or weekends, AI-driven malware can remain hidden while causing maximum disruption. The impact has been dramatic: between late 2022 and mid-2025, phishing attacks surged by 1,200 percent, and today they account for nearly 70 percent of all cyber incidents. Strikingly, most of these attacks succeed not by exploiting technical flaws, but by manipulating human behaviour.

Together, these developments show that piecemeal security upgrades are no longer enough. *Critical sectors like finance can only be protected through carefully designed, multilayered defences that address every category of AI-driven threat, both now and in the future.*

The challenge of securing data is made even harder by vulnerabilities in existing cryptographic standards. In the United States, the National Institute of Standards and Technology (NIST) is the main body responsible for developing encryption protocols (see next section). However, by law, it must consult with the **National Security Agency (NSA)** during this process. While there is no public record of NSA involvement in NIST's Post-Quantum Cryptography (PQC) competition, history offers reasons for caution. In the mid-2000s, the NSA was accused of inserting a backdoor—a hidden weakness—into the Dual EC DRBG random-number generator, which NIST had approved as a global standard. This revelation severely damaged international trust in U.S.-led cryptography.

These risks are not just historical. In October 2024, *TechCrunch*[9] reported that a China-backed hacking group, Salt Typhoon, exploited lawful interception systems mandated by the **Communications Assistance for Law Enforcement Act (CALEA)**. This decades-old U.S. law requires telecom and internet providers to maintain special access points so government agencies can monitor communications. But these very access points were breached, enabling hackers to intercept internet traffic in real time—including calls and browsing histories. *The incident highlights a fundamental problem: legally mandated backdoors are inherently insecure. By design, they create openings that can—and eventually will—be abused.*

This leads to urgent questions. Can such backdoors withstand the power of advanced AI, which is designed to recognise patterns and exploit hidden weaknesses? What happens when quantum computers—capable of breaking today's encryption—are turned against these systems? And with the rise of hybrid quantum-classical attacks, which combine the strengths of both computing approaches, can any infrastructure deliberately built with access points truly remain secure?

[9]https://techcrunch.com/2024/10/07/the-30-year-old-internet-backdoor-law-that-came-back-to-bite/

For companies outside the U.S., another problem emerges: if their data passes through systems governed by American surveillance laws, how can they ensure privacy, trust, and independence? *In today's geopolitical climate, it is risky to assume that U.S. interests always align with those of international organisations or governments.* The CALEA breach makes clear the need for cross-border encryption strategies that reduce reliance on any single government-controlled infrastructure.

These examples are not an exhaustive list of risks, but they illustrate why caution is essential. *By adopting NIST's PQC standards, organisations must also accept the possibility of U.S. surveillance or access.* This raises a final, crucial question: What exactly is NIST, and how does its influence shape the security and trustworthiness of global cryptographic standards?

4. Are NIST's Solutions Viable?

The National Institute of Standards and Technology (NIST), part of the United States Department of Commerce, plays a central role in developing standards for Post-Quantum Cryptography (PQC). Its mission is to promote innovation and strengthen U.S. industrial competitiveness, and its PQC standardization effort has become the global reference point for post-quantum security. *While the process has produced promising candidates, reliance on NIST-led standards also underscores the need to weigh both the strengths and the limitations of a U.S.-centric approach to global cybersecurity.*

Recent developments suggest that PQC, while an important step forward, does not by itself ensure comprehensive security. Many successful attacks on high-value assets—such as cryptocurrencies and stablecoins—exploit vulnerabilities unrelated to quantum computing. According to security firm CertiK, scams and hacks in the first half of 2025 alone accounted for approximately $2.5 billion in investor losses. Two incidents were particularly significant: an estimated $1.5 billion was stolen from Bybit, one of the world's largest exchanges, and another $220 million was taken from Cetus. *These breaches demonstrate that systemic weaknesses in platforms and infrastructure can be exploited without quantum-based techniques.*

Emerging attack methods further reinforce this point. The **JSCEAL attack**, for example, used JavaScript-based payloads to extract sensitive data from cryptocurrency wallets and applications. Despite being directed at platforms marketed as secure, the attack revealed persistent gaps in endpoint and user-level protections. Such cases show that while PQC strengthens cryptographic foundations, it does not address broader security challenges in practice.

Even the strongest cryptography is ineffective if applications or user interfaces can be bypassed. The JSCEAL attack illustrates this principle: it did not compromise the mathematical foundations of the system but instead exploited weaknesses in the software stack. *This*

underscores a key tenet of cybersecurity: security is only as strong as its weakest layer. Developers and platform architects, particularly in the crypto space, must prioritize layered security strategies at wallet and dApp interfaces rather than relying on trend-driven solutions.[10]

Looking ahead to 2027–2029, actors with access to advanced quantum computing—such as state-sponsored groups—may target digital assets. The Hudson Institute estimates that a quantum attack on Bitcoin could result in losses exceeding $3 trillion. While Post-Quantum Cryptography (PQC) and quantum-resistant protocols are available, their effective implementation is critical to ensuring that cryptocurrencies and stablecoins remain secure and resilient components of the global financial system.[11]

Real-world incidents further highlight the limitations of cryptography alone. Even platforms such as Signal, which have adopted PQC, remain vulnerable if the underlying operating system is compromised. High-profile devices are routinely monitored, underscoring the need to safeguard both the location and accessibility of critical virtual assets.

Human factors also pose significant risks. The "never change a running system" mindset among system administrators can exacerbate vulnerabilities, making breaches inevitable. *Engineered solutions—ranging from improved administrative tools to partial automation of security tasks—can help mitigate these risks, strengthen system resilience, and reduce exposure to advanced attacks.*[12]

5. Implications for Global Security

In an earlier section, we highlighted how the U.S.-led standardization efforts, particularly through NIST, raise concerns for other nations that fear potential backdoors or surveillance built into cryptographic protocols. These trust issues are not abstract—they shape global cybersecurity dynamics by influencing which technologies countries adopt or reject.

In this global context, recent trends reveal a sharp increase in both the frequency and severity of attacks on critical infrastructure. Ransomware incidents and silent intrusions—malware embedded without immediate exploitation—underscore the growing sophistication and strategic planning of attackers. What was once hypothetical is now a tangible and imminent risk: large-scale, simultaneous attacks on power, water, healthcare, transportation, financial systems, and defense.

Several factors drive this heightened vulnerability. First, some nations and advanced threat actors have developed defensive infrastructures that grant them a strategic advantage, enabling them to withstand retaliatory cyber operations while preserving their offensive capabilities. Second, the interconnected nature of modern infrastructure increases the

[10] https://cyberpress.org/new-jsceal-attack-targets-crypto-app-users/

[11] https://www.hudson.org/technology/decrypting-crypto-cryptocurrencies-and-the-quantum-computer-threat

[12] https://www.it-ai-solutions.com/a-comprehensive-guide-for-system-and-network-administrators

likelihood of cascading failures, where an attack on one sector triggers disruptions across others, amplifying the overall impact. Third, decades of operational expertise allow advanced attackers to maintain persistent access to compromised systems, creating long-term vulnerabilities that are difficult to eradicate.

Taken together, these elements—advanced defense, offensive capabilities, and persistent access—supported by emerging quantum technologies (distinct from quantum computers), illustrate how coordinated, cross-sector attacks on critical infrastructure are no longer theoretical but feasible. This shifting balance of cyber capabilities demands urgent global attention.

China exemplifies these developments, positioning itself as a leader in **Quantum Key Distribution (QKD)**, a technology central to post-quantum security. In 2016, it launched the quantum satellite *Mozi/Micius*, creating the world's largest QKD network. This network—now extending into Russia and more recently South Africa—underscores the scale of China's investment in quantum infrastructure. Combined with the Golden Wall, China's vast internet monitoring and control system (formally known as the Great Firewall of China), these initiatives demonstrate how quantum technologies are being applied in practice to bolster national defense. However, QKD alone does not secure all network layers. Reports indicate that even the satellite has been compromised, leaving critical sectors, such as the power grid, vulnerable despite these advances.

In conclusion, the deployment of pseudo-quantum networks by China—and increasingly by Russia—demonstrates how quantum technologies are reshaping the cybersecurity landscape. *The threat to critical infrastructure is real, immediate, and escalating. Organizations must recognize that the window for implementing systemic, effective defenses is closing rapidly, and delays risk severe and far-reaching consequences.*

6. Implications for the Energy Sector

The energy sector is among the most vulnerable domains in the context of quantum and hybrid cyber threats. Unlike financial markets, where losses are primarily expressed in capital, attacks on energy systems inevitably lead to physical consequences – blackouts, fuel supply disruptions, equipment damage, and even industrial accidents.

Network infrastructures. Modern power grids rely heavily on digital dispatch platforms (SCADA/EMS). Their interconnectedness means that a local attack on one segment can trigger a cascading effect, resulting in widespread outages. The cyberattacks on Ukraine's power system already demonstrated how digital aggression can escalate into large-scale energy collapse.

Oil and gas. Pipeline and storage management systems remain priority targets for attackers. The Colonial Pipeline incident in the United States illustrated how ransomware can paralyze an entire region: physical fuel deliveries were halted for several days. Under quantum-enabled attacks, such scenarios could become faster and harder to detect.

Renewables and digitalization. The energy transition further amplifies vulnerability:

· the decentralization of energy systems,

· the rise of digital twins,

· the massive deployment of IoT devices in smart grids.

Each new element becomes a potential entry point. Attacks on distributed generation could lead not only to financial losses but also to a loss of confidence in the very model of sustainable energy.

Financial–energy interlinkages. Energy business operations increasingly depend on digital platforms: electricity trading, certificates of origin, and carbon markets. These systems face risks similar to cryptocurrency exchanges and may become prime targets for quantum cryptanalysis or hybrid attacks. Disruptions in such markets could trigger geopolitical consequences comparable to traditional energy crises.

Geopolitical dimension. For states, energy cybersecurity is not just an IT issue but a core element of national security strategy. Vulnerabilities in energy systems under conditions of sanctions, trade wars, and regional conflicts turn into tools of coercion. In the confrontation between "petrostates" and "electrostates," digital attacks on energy systems can become equivalent to strikes against oil or gas supply lines.

Ultimately, the integration of Post-Quantum Cryptography and multilayered security measures in the energy sector must be considered part of a broader energy security strategy. For the industry, this is not an auxiliary IT safeguard but a cornerstone of long-term resilience and geopolitical stability.

7. When Will the Quantum Threat Materialize?

While the exact timeline for the emergence of powerful quantum computers remains uncertain, it is prudent to prepare for a worst-case scenario. A coordinated attack involving one or more quantum computers, combined with existing supercomputers, could overwhelm today's cybersecurity defenses. In such a case, not only would encrypted data become vulnerable, but the core functionality of digital infrastructure could collapse. Every connected system—from financial platforms to energy grids—could be compromised, leading to widespread and long-lasting disruption. Under such circumstances, cybersecurity capabilities might regress by decades.

This possibility raises a critical question: can the global community truly claim to know the precise state of progress at the cutting edge of quantum mathematics, physics, and engineering? Given the national security implications and the immense strategic value of these

technologies, it is improbable that advances in fields such as quantum codebreaking are being disclosed in real time.

History reinforces this concern. The 2011 breach of RSA's security systems, for example, was not fully revealed to the public until years after it occurred, despite its severity.[13] Compared to such classical incidents, the consequences of undisclosed breakthroughs in quantum codebreaking would be exponentially more severe. In a global race to break increasingly complex encryption schemes, transparency itself could become a liability—since openly publishing capabilities may enable adversaries to weaponize them faster than defenders can respond.

This uncertainty fuels further questions. What if quantum computers are already more advanced than publicly acknowledged? What if fault tolerance has been quietly improved beyond admitted thresholds? And what if the machines described in public reports represent only prototypes, while classified facilities house more powerful, isolated systems? For instance, if a quantum computer were already capable of breaking RSA-2048 encryption within a week—even with noisy qubits—the strategic consequences would be profound.

Such a development would directly influence the trajectory of PQC. While breaking RSA-2048 is not equivalent to breaking PQC, two scenarios must be considered. First, a breach of RSA-2048 could indirectly expose new attack vectors against PQC-protected systems. Second, advances in hardware, paired with emerging quantum programming languages such as Qrisp and hybrid computational methods, may accelerate the timeline for direct attacks on PQC. Current estimates suggest that PQC may remain secure until approximately 2029–2033. *Yet two caveats stand out: even rigorously validated algorithms may conceal hidden flaws, and rapid progress in mathematics—especially when accelerated by AI and quantum computing—could quickly undermine today's assumptions. Reflecting this concern, NIST has already recommended a cautious approach, advising that PQC be layered on top of classical encryption methods, as resilience against hybrid attacks cannot be guaranteed.*

The risks posed by hybrid quantum-classical attacks are not hypothetical. Research suggests they can increase efficiency by up to 77% compared to classical techniques. When combined with potential NSA backdoors—deliberately engineered or exploited weaknesses in encryption systems that could allow covert access—and the widespread practice of 'harvest now, decrypt later,' the vulnerabilities of current encrypted data become even more pressing. *Many researchers warn that by 2033–2035, all networked systems could be susceptible to quantum or hybrid attacks. Given the accelerating pace of both AI and quantum computing, such projections appear increasingly credible.* Algorithms like Shor's demonstrate why: once implemented on sufficiently large machines, they can reduce the complexity of codebreaking exponentially—an insight that drove much of the early investment in quantum computing.

At the same time, new tools such as Qrisp are lowering barriers to entry. By automating hardware management and leveraging AI to optimize performance, they make it easier—even for less experienced users—to conduct attacks using quantum systems. Meanwhile, AI-driven mathematical research is accelerating the discovery of more efficient algorithms, enhancing

[13]https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/

both quantum and classical supercomputing capabilities. Taken together, these trends suggest that practical codebreaking, potentially including PQC, could emerge within the next four to five years—much sooner than the often-cited ten- to fifteen-year horizon.

Despite the gravity of this outlook, it is not without solutions. Many of the mathematical and physical foundations of quantum technologies are already well understood, and effective countermeasures can be designed today. By integrating robust hardware protections, resilient software architectures, and multi-layered safeguards, critical assets can be shielded. With proactive preparation, it is possible to mitigate risks and prevent the most severe consequences of the quantum era.

8. Conclusions

The prevailing patchwork approach in IT security—characterized by isolated fixes, fragmented defenses, and reactive measures—is no longer sustainable. Traditional methods have reached their limits, and the growing risk to critical infrastructure demands a shift toward architectures that integrate both physical and digital resilience. Without such measures, large-scale intrusions into critical systems—including power supply networks and financial services—remain a highly probable outcome. *A comprehensive framework must therefore combine robust hardware, secure software, and multi-layered safeguards to ensure that sensitive data cannot be easily stolen or decrypted over the long term.*

Emerging technologies such as Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) are often presented as solutions for long-term resilience, but their role remains limited and uncertain. PQC is costly, relatively immature, and untested under diverse real-world attack conditions, making it more of a transitional measure than a definitive safeguard. At the same time, ongoing mathematical advances will likely necessitate periodic re-encryption of sensitive data, underscoring the impracticality of relying solely on cryptography. True protection requires a systemic approach—integrating secure hardware, resilient operating systems, and fortified networks into a cohesive architecture that addresses vulnerabilities at every layer. This need is especially urgent in the financial sector, where even small weaknesses in infrastructure can escalate into rapid, large-scale economic losses. Until empirical evidence demonstrates that PQC meaningfully enhances resilience, organizations should pursue complementary strategies that balance cost, scalability, and long-term protection.

The urgency of this challenge is most visible in financial transactions, where artificial intelligence already threatens banking and cryptocurrency systems, and the rise of quantum and hybrid attacks will only intensify these risks in the coming years. With the total cryptocurrency market capitalization surpassing $3.8 trillion in July 2025, the scale of potential losses is immense. Cryptocurrencies and stablecoins are particularly high-value targets, with the latter expected to play a growing stabilizing role in national economies. Yet PQC alone cannot safeguard these assets; even if attackers are prevented from profiting directly, the loss itself imposes severe financial damage on holders. Lasting protection requires

rigorously engineered systems that integrate industrial-grade hardware with software resilient to quantum and hybrid threats—effectively creating a "quantum vault" capable of securing digital assets for decades despite advances in computing, mathematics, or insider compromise.

This example highlights a broader principle: as cybersecurity threats become increasingly complex, uniform or narrowly defined solutions are no longer adequate. The convergence of AI-driven exploits, quantum computing, and hybrid attack methods demands a fundamental rethinking of IT architecture. At the same time, the accelerating digital capabilities of other nations underscore that the threat is not abstract but strategic, with potential consequences for economic stability and national security alike. Moving beyond fragmented, patchwork defenses toward integrated and adaptive systems—grounded in deep technical expertise—is essential for achieving lasting resilience. In this way, cybersecurity can advance not only as a defensive imperative but also as a strategic foundation for trust, stability, and innovation in the quantum era.

Glossary

Certificate Authority (CA). A Certificate Authority is a trusted entity responsible for issuing and verifying digital certificates. CAs form the backbone of Public Key Infrastructure (PKI), as they vouch for the legitimacy of public keys and identities used in secure communications. However, if a CA is compromised or impersonated, attackers can issue fraudulent certificates, undermining the entire trust chain.

Certificate Management System (CMS). A Certificate Management System automates the issuance, renewal, distribution, and revocation of digital certificates within an organization. It ensures that devices and applications can verify certificates against trusted Certificate Authorities. Because CMS processes often depend on operating systems and network management tools, any compromise of those platforms or their root certificates can critically undermine security.

Communications Assistance for Law Enforcement Act (CALEA). A U.S. law enacted in 1994 requiring telecommunications and internet providers to design their systems with built-in capabilities for lawful government surveillance. While intended to aid law enforcement, these mandated access points create persistent security vulnerabilities that can be exploited by malicious actors.

Cyberattack Vectors. Cyberattack vectors are the pathways or methods that adversaries use to gain unauthorized access to systems or data. These include software vulnerabilities, phishing attempts, misconfigured networks, and physical side channels, among others. The expansion of digital infrastructures has multiplied potential attack vectors, making layered defense strategies essential.

Distribution of Cryptographic Keys. The distribution of cryptographic keys is the process of securely delivering encryption keys to authorized parties. In asymmetric systems, this often relies on PKI to bind public keys to identities via certificates. Weaknesses in distribution, whether through poor validation, compromised authorities, or insecure software, can undermine otherwise strong cryptographic protections.

Hybrid Attack. A hybrid attack combines classical computing techniques with emerging technologies, such as quantum computing or AI, to breach security systems. By integrating multiple methods, attackers can overcome defenses that might resist traditional or quantum-only attacks. Hybrid attacks are particularly concerning because they exploit the strengths of both approaches to maximize efficiency and impact.

JSCEAL Attack: The JSCEAL attack is a sophisticated malware campaign targeting cryptocurrency users through fake ads and malicious applications. It employs a multi-stage infection process, including system profiling and theft of wallet credentials, executed via Node.js to evade conventional security detection. The malware uses compiled JavaScript files to obfuscate code and bypass static analysis, making it difficult to detect. Active since 2024, JSCEAL has affected millions of users and impersonated numerous major crypto platforms, highlighting the evolving sophistication of cyber threats in the cryptocurrency space.

Multilayered Cybersecurity. Multilayered cybersecurity is a defense strategy that relies on overlapping and redundant protective measures across different system levels. By combining safeguards such as encryption, firewalls, intrusion detection, access controls, and user education, the overall system remains resilient even if individual defenses fail. This approach reflects the principle that no single security mechanism is sufficient against today's evolving threats.

National Institute of Standards and Technology (NIST). The U.S. National Institute of Standards and Technology (NIST) is a federal agency responsible for developing standards that ensure secure and reliable technologies. NIST has led the international effort to identify, evaluate, and standardize post-quantum cryptographic algorithms through an open competition. The agency's recommendations guide global adoption, but the process underscores the difficulty of selecting algorithms that remain secure against both classical and quantum threats.

National Security Agency (NSA). A U.S. government agency responsible for signals intelligence (SIGINT) and cybersecurity. It monitors global communications, protects classified government data, and develops cryptographic standards. While central to U.S. national security, the NSA has faced criticism for surveillance practices and alleged insertion of cryptographic backdoors.

Post-Quantum Cryptography (PQC). Post-Quantum Cryptography refers to cryptographic algorithms designed to remain secure against the computational power of quantum computers. Unlike traditional methods based on factorization or discrete logarithms, PQC relies on mathematical problems that are believed to resist quantum attacks, such as lattice-based constructions. While PQC represents a critical step in preparing for the quantum era, it remains dependent on current mathematical understanding and faces implementation challenges.

Public Key Infrastructure (PKI). Public Key Infrastructure (PKI) is a framework that enables secure communication and authentication by managing public and private cryptographic keys. It uses digital certificates to verify identities and establish trust between communicating parties. While widely adopted, PKI depends on careful implementation and certificate validation, making it vulnerable to misuse or exploitation.

Quantum Attack. A quantum attack uses the unique capabilities of quantum computers to break encryption or exploit vulnerabilities in digital systems. These attacks leverage quantum phenomena, such as superposition and entanglement, to solve problems much faster than classical computers.

Quantum Key Distribution (QKD): A method of secure communication that uses principles of quantum mechanics to generate and share encryption keys between parties. QKD ensures that any attempt to intercept or measure the key will disturb the quantum system, alerting the users to potential eavesdropping. While it provides theoretically unbreakable key exchange, QKD does not protect the entire network or data itself and is often limited by practical implementation challenges.

Ransomware-as-a-Service (RaaS). A criminal business model where cybercriminals develop and distribute ransomware—malicious software that encrypts a victim's files and demands payment for decryption. RaaS makes ransomware accessible to less-skilled attackers, who pay a fee or share profits with the developers.

Side-Channel Cyberattack. A side-channel attack exploits indirect information leakage from a system—such as power consumption, timing patterns, or electromagnetic emissions—rather than weaknesses in the algorithm itself. By analyzing these signals, attackers can infer secret keys or other sensitive data without directly breaking the cryptography. Such attacks highlight the importance of secure implementations in addition to strong mathematical foundations.