NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub

CyberSystem Journal Review Article

# Cyber-Physical System Security in the Age of Quantum Computing: Identifying Threats and Developing Mitigation Strategies

Hawraa Adil Nori[1]

[1] Computer Center, University of Babylon, 51002, Hilla, Iraq

* Corresponding Author: **Hawraa Adil Nori.** Email: hawraa.adel@uobabylon.edu.iq

**Abstract:** Cyber-Physical Systems (CPS) integrate heterogeneous hardware and software components across multi-layered architectures, enabling real-time interaction between computational elements and physical environments. The rapid evolution of quantum computing introduces a paradigm shift in the threat landscape for CPS security, as quantum algorithms — particularly Shor's algorithm — threaten to compromise widely deployed public-key cryptographic schemes such as RSA and ECC. This paper provides a structured analysis of quantum-induced threats to CPS and evaluates candidate mitigation frameworks, including Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). We present a taxonomy of attack scenarios organised by CPS layer, a comparative analysis of quantum-resilient defence models, and a conceptual risk-projection model illustrating how cryptographic breach probabilities may evolve as quantum hardware matures between 2025 and 2050. NOTE: All tabular data in this paper are based on conceptual simulations derived from theoretical models and existing literature; they are intended as illustrative benchmarks rather than empirically validated results. Our findings indicate that migration toward hybrid PQC architectures, combined with hardware-level security measures and regulatory modernisation, is the most pragmatic near-term strategy for CPS operators facing the quantum transition..

Access this article online

**Keywords:** Cyber-Physical Systems, Quantum Computing, Post-Quantum Cryptography, Quantum Key Distribution, Threat Mitigation, CPS Security

## 1. Introduction

Cyber-Physical Systems (CPS) are computational architectures in which digital processing elements hosted in data centres or cloud platforms are tightly coupled with physical processes through sensor-actuator networks. The emergence of scalable quantum computing introduces a class of threats qualitatively different from those addressed by conventional cybersecurity frameworks. Quantum algorithms such as Shor's algorithm can factor large integers in polynomial time, directly undermining the mathematical hardness assumptions on which RSA, ECC, and Diffie-Hellman key exchange are based. Although large-scale fault-tolerant quantum computers remain an active research area, the pace of progress suggests cryptographically relevant quantum computing may become practically available within one to two decades, creating an urgent preparedness challenge for CPS operators. Additionally, adversaries may already be

Received April 22, 2026; Revised May 9, 2026; Accepted May 26, 2026; Published June 11, 2026
https://doi.org/10.57238/csj.2026.1026

harvesting encrypted CPS traffic for future decryption the so-called 'harvest now, decrypt later' attack vector.

## 2. Cyber-Physical Systems

Cyber-physical systems (CPS) is where computer computational elements in data centers or cloud are interconnected with the physical world via billion-edge networks that the system control and monitor, which economic application and safety-critical applications have dependence on them.

Recent progress in quantum computing technologies and colossal investments behind national initiatives led one to believe that the world is approaching a quantum age. Quantum computing power may as fast as in a decade become available that would pose a physical security risk to the longevity of digital communication and data storage hence, hard infrastructure and growth potential.

Quantum threats can be used to exploit vulnerabilities in the previously secure information system, such as eavesdropping, deniable service, privacy violation, control system interruption, and others, all of which could have a great influence. As CPS is the backbone of important infrastructures, it is essential to address its security in the context of quantum computing. Robust quantum computing and the development of quantum algorithms have the potential to disrupt the computational hardening of sensitive information through the factorization of large numbers and elliptic-curve based cryptographic systems.

As a result, there is an urgent need for the development of strategies to enhance robustness and redundancy within cryptographic key distribution and/or storage, protecting critical data communication as well as control system configurations. These strategies must be multi-disciplinary as they need to draw from advances in mathematical, computing and physics fields. Since no single technological solution to quantum threats exists, robust cross-jurisdictional and multi-institutional collaborations will be needed to manage risks.

One of the goals of this paper is therefore to demystify quantum threats and, in so doing, enhance awareness within a wide technical, regulatory, and management range. Another goal is to enable preparedness and the institution of early security standards that can be adapted to future developments in computation technology.

This paper represents the input of a wide range of experts and researchers working in cyber security, data analysis, telecommunication and critical infrastructure case studies, and it is intended to inform and guide the establishment of security resilience in the coming quantum age. The paper has been broken into topical sections and followed by focuses on CPS models, design and security paradigms to elucidate the threats posed by quantum computing and how to actively respond to these threats.

## 3. Foundations of Cyber-Physical Systems Security

Cyber-Physical Systems (CPS) represent a class of engineered systems in which computational elements including embedded processors, networked controllers, and cloud-based analytics platforms are tightly coupled with physical processes monitored through sensor networks and actuated via motors, valves, and related effectors. This deep integration between digital and physical domains is not merely architectural; it is functional, in that the physical behaviour of the system is directly governed by computational outputs, and conversely, physical state variables continuously inform computational decision-making.

A power generation facility, for instance, relies on computational subsystems to interpret real-time sensor data and issue corrective actuation commands, thereby maintaining operational stability within prescribed safety envelopes.

The pervasiveness of CPS across critical infrastructure sectors including energy distribution, healthcare delivery, water treatment, and intelligent transportation reflects a broad societal dependency on automated, cyber-mediated physical control. This dependency, however, introduces a correspondingly broad attack surface:

A successful cyber intrusion into a CPS environment can propagate beyond the digital domain, inducing physical consequences that range from degraded operational performance to safety-critical failures with potential for irreversible harm. Responsible stewardship of such systems therefore demands that security be treated not as an ancillary concern but as a foundational design requirement.

Established security frameworks, including the NIST Cybersecurity Framework and the IEC 62443 series of industrial automation and control system standards, provide structured methodologies for identifying and mitigating threats such as unauthorised access, denial-of-service, and man-in-the-middle attacks.

These frameworks have, to date, operated under the implicit assumption that contemporary asymmetric cryptographic primitives particularly those underpinning public-key infrastructure and digital signature schemes furnish sufficient confidentiality and authenticity guarantees. Advances in quantum computing, however, fundamentally challenge this assumption.

The prospective availability of cryptographically relevant quantum computers capable of executing Shor's algorithm at scale threatens to render widely deployed asymmetric schemes, such as RSA and elliptic-curve cryptography, computationally tractable to adversarial attack. This emerging vulnerability necessitates a re-examination of the cryptographic foundations upon which CPS security currently rests, and motivates the investigation of post-quantum cryptographic alternatives suited to the operational and resource constraints characteristic of CPS deployments.

## 4. Quantum Computing and Its Implications for Cyber-Physical Systems Security

Quantum computing represents a paradigm shift in computational capability, deriving its power from two foundational principles of quantum mechanics: superposition and entanglement. Unlike classical bits, which occupy a definite binary state, a qubit can exist in a coherent superposition of both states simultaneously, enabling a quantum processor operating on $n$ qubits to explore an exponentially large state space in parallel. Entanglement further augments this capability by establishing non-local correlations between qubits, such that the measurement of one qubit instantaneously constrains the probabilistic outcomes of its entangled counterparts, irrespective of physical separation.

Collectively, these properties endow quantum computers with the ability to solve certain computational problems at speeds that are asymptotically unachievable by classical architectures.

Two quantum algorithms are of particular cryptographic significance. Shor's algorithm (1994) factors large integers in polynomial time $O((\log N)^3)$, directly undermining the computational hardness assumptions upon which RSA and elliptic-curve cryptography (ECC) are founded. Grover's algorithm (1996) provides a quadratic speedup for unstructured search problems, effectively halving the bit-security level of symmetric encryption schemes and necessitating a doubling of key lengths to maintain equivalent security margins.

Together, these algorithms constitute a systemic threat to the cryptographic infrastructure currently securing digital communications, including those operating within cyber-physical environments.

Contemporary quantum hardware encompassing superconducting qubit platforms developed by IBM and Google, as well as trapped-ion architectures from IonQ remains constrained by high gate error rates and limited qubit coherence times.

Cryptanalytically relevant attacks against RSA-2048 are estimated to require on the order of thousands of logical qubits and millions of error-corrected physical qubits, a capability that lies beyond the reach of present-day systems. Nevertheless, the trajectory of quantum engineering progress suggests that this threshold is being systematically approached, rendering the timeline of cryptographically relevant quantum computers a matter of active research and strategic concern rather than theoretical speculation.

The implications for cyber-physical systems are particularly acute. CPS environments are characterised by real-time operational constraints, heterogeneous hardware, and long deployment lifecycles — properties that complicate cryptographic agility and limit the feasibility of rapid post-deployment remediation. Furthermore, CPS deployments span sectors of critical societal infrastructure, including smart grids, industrial control systems, autonomous transportation networks, and process control plants, in which the computational and communication subsystems coexist within tightly coupled control loops.

A successful quantum-enabled cryptographic attack on such a system would not be confined to the cyber domain; it could propagate into the physical layer, disrupting actuation, compromising sensor integrity, or subverting control logic in ways that produce tangible, potentially irreversible harm. This dual-domain vulnerability motivates a proactive re-evaluation of the cryptographic foundations underpinning CPS security and underscores the urgency of transitioning toward quantum-resistant alternatives before cryptographically relevant quantum computing capability materialises.

## 5. Intersection of Quantum Computing and Cyber-Physical Systems Security

This intersection, quantum cyber physical systems (QCPS) is an essential yet less-explored area. Like other fields, there are also advantageous and disadvantageous chances within quantum technologies on the security of CPS. Quantum computing's ability to solve large computations, exponentially quicker than classical computers can, has the capacity to transform how CPSs can be secured. This power can be exploited to construct more secure cryptographic protocols, possibly undermining a number of widely employed ones [1].

This confluence is of particular interest for CPSs, since it introduces new challenges in assuring the integrity of system operation and new opportunities to penetrate complex simulations.

Current trend of examining and enhancing CPS security largely pays attention to already known vulnerabilities and threats in the community, while it has neglected a less studied but emerging threat which could alter current defensive mechanisms tremendously: quantum computing. The discussion opens by considering generalized repercussions of quantum threats to computing systems, and subsequently delves into how quantum computation may create new or influence previous attacks in the context of CPS security. To illustrate the timely, we look backward to recent events and disclosure of vulnerabilities by examining ways that CPS practitioners can get ready for a quantum tomorrow.

The arguments are further extended to how CPS practitioners and experts can be more proactive in addressing quantum threats. With quantum computing being more and more influential, the aim in this work is that organizing a classification of security approaches for CPS will improve the design of CPS security strategies against quantum attacks.

## 6. Threat Landscape in the Age of Quantum Computing

Recent advancements in quantum computing may create a new threat landscape for cybersecurity, having the potential to break classical encryption algorithms. As cyber-physical systems (CPS) continue to utilize more connectivity, an assessment of the threat landscape becomes even more pressing. On the cyber side, evolving quantum algorithms threaten traditional encryption technologies, which could have broad impacts on CPS, particularly for transformative technologies.

### 6.1 How will the Threat Landscape Change?

Quantum computing can be expected to amplify, transform, and introduce additional risks to traditional cybersecurity threats [1]. Owing to the rapid advancements in quantum algorithms, the processing power required to launch successful cyberattacks is likely to drop exponentially over the next decade.

There are many well-thought-out goals for quantum security that have yet to be met, such as the Post-Quantum Cryptography (PQC) timeline. Although these goals will likely provide a stronger foundation for the long-term future, there are marked gaps between them and the present state of technology. The delay in the full implementation of quantum-safe cryptographic systems and the proliferation of quantum computers are likely to coincide.

Meanwhile, the practicality of quantum-aided attacks on currently realized encryption systems is becoming plausible. Post-quantum and quantum-secure standards have already emerged, but many systems have yet to implement them exclusively. Results indicate a clear threat of nation-state actors launching cyberattacks against the infrastructures developed by other national actors, such as critical infrastructure.

Cybercrime groups could also target same-sector rival companies. Actors with high stakes, such as venture capital firms or other investors, targeting multiple R&D companies' infrastructures have already been highlighted as a concern. Cybercrimes are also affected, with nation-state actors targeting the largest global profit generators, a substantial reliance on new investments or mergers, acquisitions, joint ventures, and other typical nascent-technology deployment models.

Governments are expected to step up protection efforts, but seed-persistence times may only come about after irreversible severe damage. Indications of such strategies could spur rivals to similarly step up their own pre-emptive protection strategies, escalating the cyber-physical arms race. The outcome could be a devastating, abrupt drop in technological efficiency, with corresponding reverberations in the overall economic and possibly military dominance. It is stressed that these scenarios are not mere talk; vested parties could rapidly catalyze such fevered situations. What is more, the doomsday timeframes could actively be composed in efforts to illicit irrational reactions.

## 7. Vulnerabilities in Cyber-Physical Systems

Cyber-Physical Systems (CPS) present a plethora of vulnerabilities that may allow an adversary to launch an attack endangering the system's assets, safety, and privacy of information. This paper identifies a taxonomy of threats, vulnerabilities, possible attacks, and existing defences in CPS and IoT. FPGA and smart grid are considered use case-dependent CPS administered for the study. Sporadic incidents of CPS attacks, as well as a taxonomy of the attacks, are included. Existing security measures of various CPS types are examined considering their protection of CPS from non-cyber-attacks (e.g., device malfunctioning and human errors).

It proposes a cyber-physical security framework which incorporates the CPS-related security aspects of an overall CPS. Finally, there is a discussion on the Automatic Code Transformation (ACT) system, which is a defence indicated for FPGA-based CPSs considering particular use cases.

Cyber-physical systems (CPS) represent a blending of control, communication, and computing. Real environments in cyber-physical systems are often monitored and/or controlled by numerous sensors such as flow meters, position sensors, temperature sensors, current/voltage sensors. The sensors can be tampered causing inaccurate readings [2].

Various industrial processes such as the smart grid system can be modelled as a set of ordinary differential and algebraic equations. These models are solved by aggregating the data from multiple sensors. The sensor readings may be tampered to increase or decrease the frequency of the data aggregation, making the system more or less sensitive and susceptible in the long term to voltage/power stability issues [1].

Various actuators such as power cords, batteries, pumps, etc. consume energy in cyber-physical systems. By tampering with the non-intrusive energy metering systems, the energy consumption can be hidden. In the electrical grid interpole communication relays are essential for the communication of RTUs and IEDs. However, too much communication might generate excessive CPU usage leading to a delayed signal and lost connectivity effectively compromising the functionality of the distribution grid system by introducing stability issues.

## 8. Quantum Threats to Cyber-Physical Systems

In this section, the threats of quantum computing against Cyber-Physical Systems (CPS) are systematically analysed. Threat scenarios are described surrounding anticipated quantum capabilities, sketching paths for the undermining of conventional security practices. Shor's algorithm can solve integer factorisation and the elliptic-curve discrete logarithm problem in polynomial time, rendering RSA and ECCthe cryptographic schemes securing most CPS communication and authentication infrastructure vulnerable to a sufficiently powerful quantum computer. This directly threatens the integrity of encrypted control traffic, authenticated firmware updates, and remote-access credentials across CPS deployments.

In this section, the threats of quantum computing against Cyber-Physical Systems (CPS) are dissected. Threat scenarios are described surrounding anticipated quantum capabilities, thus sketching paths for the undermining of conventional security practices. The scenarios are explained in the context of known cases where either such threats are demonstrated or the means of implementing the attacks is understood. Firstly, advancements in quantum computing is mentioned, which may enable powerful quantum algorithms that threaten the security of classical public-key encryption such as RSA and ECC.

General Examples of Shor's Algorithm In short I am listing some classical ways we use too many factors 6.3, and then mentioning that using this attack on RSAT is a breeze 15 /? .

The vast majority of secure classical encryption schemes are based on hardness factors such as integer factorization or the elliptic-curve discrete logarithm problem (DLP), both of which Shor's algorithm can solve in polynomial time, thus rendering many contemporary cryptographic protocols irrelevant [1].

Secondly, we discuss our thoughts on a broader security area relevant to CPS which quantum devices are employed attacking beyond what they presently have. For instance, adversaries may use quantum computing to cryptanalyze control signals with sensitive instructions.

This would then enable malicious cyber manipulation of the physical elements ruled by such CPS. Where there are integrity checks or digital signatures for control mess ages, adversaries have quantum-enabled attacks on the physical actuation level, such as sending false stimulus that jams actuators of sensors.

In these cases, the credibility of security-critical CPS has implications for several parties. This study highlights the challenges found in such systems, where hybrid threats can take place at the digital and physical layers of the infrastructure. Therefore, a security mindset of large scope in terms of information assurance, product quality is required to enable both the safe operation and sustainable deployment for critical services society depends upon.

## 9. Mitigation Strategies

Overview and Frameworks Concern has been growing over the potential impact of quantum computing on CPS security. Effective mitigation requires a multi-layered strategy combining near-term and long-term measures. Near-term priorities include:

- Cryptographic inventory and agility assessment identifying all uses of quantum-vulnerable cryptography and assessing migration feasibility.
- Hybrid cryptographic deployment implementing schemes combining classical and post-quantum algorithms.

Worrisome has been growing over what potential impact quantum computing could have on security when it comes specifically to Cyber Physical Systems (CPS). Several solutions and models are presented in this paper to harden

the strength of CPS against quantum computer driven 11 threats.

The approaches covered all aligning of this being within cyber security guidelines to deliver practical guidance that industry could take away and action. Recommendations of focus include applying existing best practices, adapting cyber security strategies for quantum-susceptible systems, and investing in new quantum-resistant technologies. Best practices are reviewed to consider potential modifications for increased resiliency in the face of any form of an attack.

Focus is also placed on real-time adaptation, to which quantum technologies have grown in number of applications, and CPS enclosure. Recommendations are also outlined on addressing quantum threats. Beyond that, Quantum Key Distribution and Post-Quantum Cryptography are also mentioned as upcoming technologies. Some development and research problems are outlined.

To illustrate the wide-ranging threat presented by quantum computing, we present detailed examples of attacks that are enhanced using a quantum computer. Some of these attacks could shut down industrial operations. There are analyses of sectors that have been covered by these studies: chemistry, oil refining, paper-making, beverage production and food processing. The study covers a large variety of plants, from small fermenters to big distillation columns. Lastly, the importance of state-firm-regulator cooperation is emphasized. A related project for multidisciplinary efforts in controlling the quantum threat and constructing full-fledge vigilantly adaptive security involves deciphering two dead words from a cryptic book.

## 10. Cryptographic Solutions for Quantum-Resistant Security

The rise of quantum computing leads to new threats to the security in Cyber-Physical Systems (CPS). Classical cryptographic primitives, protecting many aspects of these systems, will be broken by a quantum computer capable of doing efficient large number factoring or discrete logarithm problem-solving.

As the field of quantum computing advances, this foreknowledge of computation would enable adversaries to gain unauthorized access to an encrypted conversation, a secure facility, system processes or otherwise access or alter sensitive data and capabilities. Acknowledging this, the research community began to design cryptographic primitives that are believed to be secure against quantum adversaries, which can process information much faster than a classical computer in certain settings (so-called post-quantum or quantum-resistant cryptosystems).

In this section, we concentrate on a new analysis of the emerging lattice-based and hash-based post-quantum cryptographic algorithms in contrast to their conventional cryptographic analogs with respect to potential candidates for quantum-safe CPS security applications. It also underscores the substantial advantages to be gained by migrating to quantum-resistant systems sooner, rather than waiting on new cryptographic standards s and these are already available through no-cost proactive steps.

Latest advances in quantum computing have raised questions about the aptitude of today's cybersecurity. The major vulnerability introduced by technological progress is clearly superiority in computing power, particularly with respect to integer factorization and discrete logarithm problems on which are based the RSA and ElGamal public key crypto-systems [1]. The first quantum algorithm significantly sped up factoring and discrete logarithms, and in short order led researchers to the study of quantum-resistant cryptographic algorithms. In response to this challenge, companies have started programs for standardizing cryptographic algorithms that are estimated to be secure in the future.

In contrast to conventional approaches, quantum computers process information through quantum bits, enabling them to tackle numerous issues exponentially faster. As classical cryptographic systems drawn from a set of commonly shared parameters would prove vulnerable to this new adversary, lattice-based cryptography has emerged as a possible alternative due to its perceived resilience against both quantum and classical computational attacks. Unlike other alternatives, lattice-based cryptography is rooted in well-known undeveloped computational problems that have resisted significant research efforts for over three decades.

Some uncertainties exist, however, due to the nascent deployment and research on deployment security such as key-size selection. With this unprecedented threat, investments and advances in lattice-based cryptography appear more important than ever, and potentially secure cryptographic systems based on lattices have been proposed.

## 11. Quantum Key Distribution for Secure Communication

Following the discovery of quantum algorithms capable of factoring large numbers or computing discrete logarithms exponentially faster than the best known classical algorithms, the assumption that many of the algorithms underlying classical public-key cryptography will become breakable by a quantum computer has sparked significant attention in the security community 4.

While a large-scale quantum computer has yet to be built, the potential threat of quantum computing to the traditional cryptographic infrastructure has been seriously considered, leading to investments in post-quantum cryptography. However, new quantum algorithms for fixed-key cryptography used in symmetric ciphers have not been found. Hence current symmetric cryptographic integrity checks except for key sizes can be considered secure against quantum computers.

One potential approach would consider the use of Quantum Key Distribution (QKD) for such key distribution, providing security even in the presence of a quantum adversary [4,5]. QKD was first proposed in 1984, and the principles of QKD are derived from the unsettling discovery in its infancy that quantum mechanics can under certain conditions violate the intuitive axioms of locality, realism, and free choice (or freedom).

Fulfilling the necessary conditions for such a violation results in correlations between the two parties that can be noticed by the parties involved. A sophisticated protocol utilizing this idea can turn said correlations into secret shared keys with an adversary bound to introduce errors into the system. Such errors are detectable in the form of discrepancies in the check sum values of the generated keys. Any such check sum discrepancies provoke deposit of the current generation, as these can no longer be deemed secret.

The existence of QKD safeguarded against quantum adversaries implies a correspondence with the potential attack scenarios of an actual adversary implementing advanced quantum algorithms that cannot be met with traditional key distribution methods. Given these premises, it follows that the widespread institution of QKD in critical infrastructures would theoretically provide a safeguard against quantum adversaries. Nevertheless, while QKD is able to supply a unique level of security, it is not without security issues.

## 12. Post-Quantum Cryptography in Cyber-Physical Systems

Cyber-Physical Systems (CPS) are pervasive physical-world systems that monitor physical processes through sensors and actuators and effect changes on the processes through control valves, motors, and pumps using information transfer over networked systems. Many CPS applications interface with a human counterpart and provide feedback to it. For example, healthcare monitoring systems can alert a patient that their blood pressure is too high, or a patient with a heart monitor can be advised that they should call an emergency responder as their heart rate is dangerously low.

Post-quantum cryptography is promoted as a mitigation strategy for the impact of quantum computing on cybersecurity. It explains concepts of post-quantum cryptography and presents examples specifically tailored to CPS networks. Real-world applications and case studies illustrate successful post-quantum cryptographic implementations, and a roadmap is suggested for organizations adopting cryptographic methods resilient to quantum attacks [1].

CPS are embedded computing systems with cyber and physical components. Traditionally, cryptographic solutions are structured such that the encrypted data is sent across the communication channels. This data contains information that is to be communicated between networked systems, perhaps identifying a plant variable, an upper bound on power consumption, or a command to perform a function. Cryptographic algorithms are applied to this data, ensuring data integrity and/or confidentiality.

Post-quantum cryptography is a method of implementing cryptographic algorithms resistant to attack by a quantum computer. With rapid developments in quantum computing, classic cryptographic techniques are expected to become insecure. To ensure continued system security, migration towards post-quantum cryptographic techniques is essential. CPS are part of life's daily infrastructure but are currently opaque, yet a rich source of topics for new quantum algorithms or systems.

## 13. Secure Hardware Design in Quantum Computing Era

Safety-critical cyber-physical systems (CPS) employed in infrastructure or other sectors are heavily relying on their hardware counterparts as a foundational element. These systems are susceptible to cyber as well as software or hardware-based quantum cyberattacks as quantum technologies enabling these cyberattacks flourish. Thereof it is essential to develop hardware solutions that possess the ability to operate resiliently in the evolving quantum landscape. Here a framework that supports designers while designing secure hardware for the context of the maturing quantum technologies is outlined.

Moreover, the importance of adopting a holistic view that combines hardware security from a CPS perspective and hardware security design principles is accentuated, while other key cybersecurity concepts are intentionally not given in detail and are out of scope. Increasing reliance of safety-critical CPS on hardware solutions poses unique challenges to security because of maturing quantum technologies. Many existing cyber-security solutions that

safeguard against attacks from classical computers are fundamentally vulnerable against quantum attacks.

Quantum-resistant hardware security measures include: Physical Unclonable Functions (PUFs), which generate device-specific cryptographic keys from manufacturing variation; Hardware Security Modules (HSMs) configured for post-quantum algorithms; secure boot implementations using hash-based signature schemes; and tamper-evident packaging for field-deployed CPS components. Future CPS hardware designs should incorporate cryptographic agility dedicated accelerators capable of implementing multiple PQC algorithm families.

Increasing reliance of safety-critical CPS on hardware solutions poses unique challenges to security because of the maturing quantum technologies now enabling cyberattacks. Many existing cyber-security solutions that safeguard against cyberattacks from classical computers are fundamentally vulnerable against attacks from quantum computers. Given these new and emerging capabilities of quantum technologies, it is reasonable to expect fundamentally new forms of cyberattacks.

Safety-critical CPS comprise systems of components that are closely coupled such that the safety of the system as a whole depends on the safety of the individual components 1. Wirting safety-critical, a system should be intended to prevent unsafe operations and to mitigate the consequences of an accident, with the aim to control the occurrence of an accident and/or dealing with an accident that has occurred.

implementation of proper safety measures can be deferred in favor of other properties. Implementation is then generally ad-hoc, and not the result of a well-defined methodology, always present through the life of the software. For this reason, it is important that software is developed according to best practices with security always in mind [6].

**Table 1. Simulation Variables for CPS Security Under Quantum Threats**

| Variable | Description | Expected Behavior | Range | Unit |
|---|---|---|---|---|
| Processing Power (QPU) | Quantum processing capability of attacker | Higher power → faster cryptanalysis | 10–1000 | Qubits |
| Network Latency | Delay between cyber and physical components | Increases vulnerability window | 1–500 | ms |
| Encryption Strength | Security level of communication | Stronger → lower compromise probability | 128–1024 | bits |
| System Response Time | Reaction time of CPS controller | Slower → higher disruption risk | 10–100 | ms |
| Attack Frequency | Number of attacks per unit time | Higher → more frequent risk exposure | 1–50 | attacks/hour |

Safety is ensured through a combination of measures, e.g. detection, response, containment, recovery, containment systems, and procedures. As safety largely depends on accurate function, ideally designed components are used in such systems. Unfortunately, the use of inherently safe components in software or hardware is difficult.

## 14. Secure Software Development Practices

Secure software development practices are of critical importance in ensuring the security of Cyber-Physical Systems (CPS) in the era of quantum threats. Quantum computers threaten to disrupt current key exchange methods by destroying the security of widely used IT systems. Thus, new fears of threats have arisen for CPS, a class of systems directly rooted and exposed to the physical world and depending on the feedback of the physical environment for essential functions.

Software is an essential part of this environment in that software issues regularly appear in security incident reports. Secure software and corresponding development practices should ensure that the implemented software is rugged and according to expectations, and that the system can resist various forms of attacks against the cyber component. The development of secure software often marginates however in favor of other features and properties. Especially for small development teams with time pressure, the

**Table 2. Hypothesized Quantum Attack Scenarios and System Impact**

| Attack Type | Quantum Exploit Mechanism | Targeted CPS Layer | Expected Impact | Mitigation Hypothesis |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Quantum Decryption | Shor's algorithm breaking RSA | Communication Layer | Full data exposure | Post-quantum encryption |
| Quantum Noise Injection | Manipulating sensor signals | Physical Layer | Incorrect actuator response | Quantum-resistant sensors |
| Quantum Spoofing | Entangled signal mimicry | Control Layer | False data integrity | Real-time authentication |
| Quantum Replay Attack | Re-sending captured entangled packets | Network Layer | System desynchronization | Timestamp validation |
| Quantum Malware | Exploiting hybrid computation | Application Layer | Persistent system control | Quantum anomaly detection |

**Table 3. Theoretical System Behavior Under Different Defense Models**

| Defense Mechanism | Quantum Tolerance | System Overhead | Expected Reliability | Implementation Complexity |
|---|---|---|---|---|
| Lattice-based Cryptography | High | Medium | 90% | Medium |
| Hash-based Signatures | Very High | High | 95% | Low |
| Code-based Encryption | High | High | 88% | Medium |
| Multivariate Cryptography | Moderate | Low | 80% | Low |
| Hybrid PQC-ML Model | Very High | Medium | 98% | High |

**Table 4. Simulation of Risk Probabilities with Quantum Evolution**

| Year | Quantum Computing Maturity Level | Probability of Cryptographic Breach | Expected System Downtime | Recommended Upgrade |
|---|---|---|---|---|
| 2025 | Prototype Quantum Systems | 0.05 | 1 hour/year | Partial PQC adoption |
| 2030 | Mid-scale Quantum Processors | 0.25 | 5 hours/year | Full PQC migration |
| 2035 | Large-scale Quantum Networks | 0.55 | 15 hours/year | Dynamic hybrid encryption |
| 2040 | Global Quantum Cloud | 0.80 | 30 hours/year | Quantum defense frameworks |
| 2050 | Mature Quantum Integration | 0.95 | 60 hours/year | Quantum-secure architectures |

**Table 5. Theoretical Performance of Quantum-Resilient CPS Frameworks**

| Framework Model | Encryption Scheme | Expected Quantum Resistance | Response Efficiency | Simulated Attack Success Rate |
|---|---|---|---|---|
| Q-Safe CPS | Lattice-based + ML Intrusion Detection | 98% | 92% | 2% |
| Hybrid PQ-CPS | Code-based + Classical | 95% | 88% | 5% |
| Quantum-Aware CPS | Hash-based + Entanglement Monitoring | 99% | 85% | 1% |
| ML-Augmented CPS | Neural + PQC Hybrid | 97% | 93% | 3% |
| Legacy CPS | Classical Encryption Only | 20% | 95% | 75% |

## 15. Risk Assessment and Management in Quantum Era

This section surveys representative implementations and pilot programmes in which quantum-resistant technologies have been applied to CPS-relevant environments. In the

energy sector, utilities in the United States and Europe have begun QKD pilot programmes for securing wide-area SCADA communications. In healthcare CPS, manufacturers of implantable medical devices have begun evaluating PQC for firmware-update authentication. In transportation CPS, research programmes including the European Quantum Flagship have explored quantum-secure communication for autonomous vehicle coordination and railway signalling systems. The IEC 62443 standards body has begun incorporating PQC requirements into next-generation security guidelines for industrial automation and control systems.

Cyberthreats in a quantum computing era are, in general, a unique kind of risk. There is a potentiality that all the algorithms that are now secure will need to be revised as well as all attack algorithms that are currently infeasible with contemporary classical computing power will be feasible by quantum devices. Time to security breach has to be considered to make the risk quantification more accurate.

There is a rise in an industry around quantum computers which leads to their distribution as cloud services. This, in turn, can make attack scenarios prevalent where quantum computers can be rented to perform highly parallelizable quantum algorithms against known or fetched encrypted data. It can be possible that in the absence of standard encryption security, public and private key directories, and systems with digital signatures will simultaneously break down leading to general chaos of the cybersecurity environment.

Risk management methodology needs to be developed for robust risk assessment and management in the quantum landscape. Applicable methodologies for the identification and risk evaluation of risks that Cyber-Physical Systems are subjected to are outlined and possible threats stemming from the progress of information technologies related to quantum computing are elaborated. It is urged to take a proactive stance in risk management, particularly regarding potential quantum-specific threats. Frameworks and tools are available to support organizations in their quest for efficient risk assessment and management. They may also assist in risk assessment when stakeholders are different, but risks are shared in a quantum computing environment. Illustrative real-world practices, strategies, and achievements in risk management on common vulnerabilities and threats associated with information technologies and cyber-physical systems are captured and documented. Regarding attacks stemming from quantum devices, it is suggested to continuously update assessments of known quantum technology to knowledge of new advances and to dynamically adapt existing quantum safety protection.

## 16. Case Studies: Quantum-Resistant Cyber-Physical Systems

The goal of this research is to identify 15 impactful, real-world implementations of quantum-resistant technologies that bolster the security posture of Cyber-Physical System (CPS) networks. The threat of quantum attacks – a class of attacks that can break current cybersecurity encryption methods using quantum computers – is of rising concern in the IT sector. The threat is exacerbated by the emerging democratization of quantum computing, which could lead to the availability of a large-scale quantum computer in the hands of malicious entities before significant operations-related migration to quantum-resistant encryption methods can occur. This research provides a compendium of case studies to inform practitioners working on the implementation of quantum-resistant cybersecurity measures [3].

Each case study is generated through a high-level analysis of effective cybersecurity implementations; the focus is on strategies that could transfer to or inform the development of quantum-resistant cybersecurity for highly-specialized on-field IT networks like CPS.The quantum transition raises important ethical and legal questions for CPS operators, policymakers, and technology developers. At the data privacy level, the 'harvest now, decrypt later' attack model means that personal and commercially sensitive data collected by CPS today may be exposed to retrospective decryption. Organisations with legal obligations under data protection frameworks such as GDPR or HIPAA have an ethical and potentially legal duty to protect long-lived sensitive data by deploying quantum-resistant encryption promptly.

At the safety and liability level, questions of legal liability for operators who failed to implement available quantum-resistant protections will become increasingly pertinent as the quantum threat matures and PQC standards become well-established.

In this research, 15 impactful case studies of quantum-resistant technologies implemented in CPS networks are distilled. The case studies slice existing real-world deployments of quantum-resistant technologies according to the security improvements and strategies that are core to their success. The potential quantum security threat landscape and the strategic approach that can be adopted to investigate the response to quantum threats by those who operate large networks are discussed.

The objective is to find a direction for this industry and policymakers describing how real-world organizations are practicing and dealing with quantum threats. Additional

threats such as hash-based cyber threats and potential mitigation measures are considered.

## 17. Regulatory and Compliance Considerations

Existing U.S. Policies and Regulations: This subsection discusses existing and proposed policies, regulations, executive orders designed to maintain CPS security from the perspective of U.S.A. Consequences for CPS in a quantum threat context of these laws and the concerned frameworks are considered.

As there are no laws or any executive order in force that addresses in a focused way the security of CPSs with respect to quantum, general laws aimed at guaranteeing the protection of critical infrastructure apply. The analysis emphasizes the necessity of modernizing the regulatory environment to cover risks regarding quantum computing, and suggests that it would be Government's responsibility to introduce new regulations.

Very important values in organizations are the negative implications of non-compliance and the value of preventative compliance work. The latter involves work with partners to identify best practices, and migrate identified threats and countermeasures into appropriate regulatory text. This is consistent with what has been presented so far, but includes some text that does work in practice.

To address the future risks presented by quantum threats, it is necessary to further develop and apply quantum-safe cryptography, systems, and policies. While the availability of practical quantum computers remains uncertain, the U.S. Government should not only work to advance quantum-safe standards, protocols, and technologies, it should establish and implement regulations requiring or incentivizing CI operators to do the same.

Discussions of quantum communication and quantum key distribution are also made. A CPS-embedded strategy is absolutely essential, and joined efforts must be actively pursued. Consequently, standards must soon be established to address required regulatory frameworks federally within the DHS, DoD, and other relevant agencies. High-quality adherence to standards and regulation will be a critical factor for commercial growth through the creation of standards and regulations that can pinpoint easily overlooked CPS vulnerabilities 1. Hashed lists and a programmed emulation of security requirements of the end-target are beginning steps for this process. This encourages addressing compliance early in the development and acquisition process as to maximize innovation effort and choice of design freedom. Beyond compliance, these concerns implore the FCC to stress testing of defaults in transmitting/receiving rates and protocol versatilities.

## 18. Ethical and Legal Implications

powered by Eventually through technological development industry will move from the classical into the quantum era touching infrastructures and other interrelated systems too. It is this industrial shift that precedes the legal and ethical leap in human self-comprehension that increases the urgency with which we need to highlight possible ethical conundrums.

As a result, to the same extent that quantum computers leapfrog existing devices in terms of power, research priorities will have to catch up with those new capabilities – and perhaps particularly so when it comes to ethics as concerns data privacy and security. The role of organizations as core actors in preventing unauthorized access to the sensitive data produced by citizens, consumers, or patients is becoming more prominent.

The analysis of the legal bases shows that there is good foundation to reflect upon and monitor the organizations' compliance. However, it is the organizations themselves who will decide how they can keep compliance and also their ethical sense. Hence, this study should aid a greater societal understanding and governance of the role that ethics are to play in cybersecurity as best practice and policy. Awareness is also generated by case studies and relationships are developed (with respect to the specific job) and recommendations are provided for further consideration.

Cyber-Physical Systems (CPS) are the increased integration of the digital and real world. Physical processes increasingly rely on CPS for monitoring, coordination and control turning them into part of critical infrastructure. The introduction of quantum computing could lead this infrastructure to enter a new domain that is largely unexplored.

A common belief is that a quantum computer with a large number of qubits will be an extremely powerful computer capable of doing calculations that are impossible on a classical computer. This computation power in the wrong hands, is a threat of cyber-physical attacks.

## 19. International Collaboration in Quantum Security

The global threat landscape has become more aggressive and digital transformation shot up the agenda of international cooperation and policy dialogue. The pervasive, connected and therefore vulnerable nature of the

world's critical infrastructure to cyber and other hybrid threats means it is a medium for the global projection of destabilizing activity found nowhere else. The problem might only get worse if quantum computing can beat us faster than we're able to protect ourselves.

As a new exponentiating technology of the i.p.r. driven variety, it is expected that a power imbalance in the world in security and economy (not to mention communication) will follow the coming into existence of a working quantum computer. As a large share of the world is currently unprepared for such a technological shift, addressing this gap is equivalent to promoting responsible, peaceful and safe quantum technology.

Quantum key distribution and networks, secure satellite communication, and development of quantum-safe algorithms are recognized as the most promising domains for international cooperation to increase resilience and advance policy-making. Additional investments in sharing best practices and workforce education increase readiness for the countless impacts of the quantum age [10]. Against the background of expanding cyber threat environment, policy discussions and existing cooperation among various international actors have intensified. Much of the status enjoyed by critical infrastructure is due to its pervasiveness and interconnectedness, making it an attractive target for hybrid and cyber threats.

In a networked world, an infrastructure attack probably would cause a chain reaction, collateral damage reaching across the border. Policy round tables are being held on the impact and response to hybrid and other external attacks on European and global infrastructure, where it is hoped that common knowledge and resources will be forthcoming. Preparing for change As risk born of technology and trade developments come to the fore, the makeup of the threat requires readiness.

No attention is generally paid to the threat of quantum computers being able to break traditional cryptography, and an effort to prepare for this attack (by developing quantum-resistant technologies or frameworks) is advocated. There is of course a focus around worst practice sharing among those better and less well prepared to tackle the quantum threat, securing critical infrastructure and enabling it to be resilient against an ever changing threat landscape.

## 20. Education and Training in Quantum Cybersecurity

Whereas policy regulation and security standardization serve data safety, education and training can arm the workforce with the essential quantum cybersecurity skills. Cybersecurity professionals in the CPS and IoT protection domain should be informed about quantum-safe methods and developments, as well as about potential transformation of cybersecurity by quantum technologies. So too, software developers of embedded control systems should be aware about attacks over quantum-resistant cryptosystems. In addition to a general increase in literacy in the languages of cybersecurity and quantum mechanics, the language-specific bridge between the CPS and QKD foundations is provided through this graduate lecture series. Furthermore, continuing cyber research would not only address the significant matters of IoT to improve its security postures in this accelerating but fragile domain, but also CPS researchers find that there are growth points for quantum cybersecurity.

It is an interdisciplinary approach, where cybersecurity classical computer science quantum mechanics and quantum safe algorithms hold important position for the design of resilient and efficient QSCs. The present education and training systems and the lack of action on quantum-safe algorithms serves as an entry barrier for this consideration. Guidelines on how to establish and sustain a powerful professional community to counteract the emerging threat of quantum cyber-attacks are subsequently outlined by academia, startups, think-tanks and government bodies. In addition to helping the regulators, simulators companies and cyber authorities do whatever they can to create a robust safety grid for the more and more quantum technology-ridden future, an immunity booster that intends to make things stronger as well is added with the intention of fortifying resilience and strengthening deterrence to encourage reflexivity for all [8,9].

Given the rapid advancing of second quantum revolution and massive investments in national strategies such as EU, US and China, it is found that the makeup of quantum technology has grown in opportunities significantly, which deeply reshaped our technological statuses and also social or political profiles. Concomitant with the growing dependency on and integration of quantum technology in everyday practice and cyber operations, the endemic vector of classical cyber exposure shifts from mere zero-days and malwares to quantum threats, thus demanding a quantum-like innovation in techniques and doctrines.It is important to note that classical security tools may prove inadequate against the increased processing power and unique algorithms available to quantum adversaries. The CPS community must adopt dedicated mitigation mechanisms. The conceptual simulations presented in Tables (1-5) provide a structured framework for thinking about quantum risk, not precise quantitative predictions. Actual breach probabilities and defence performance will depend on the specific characteristics of individual CPS

deployments and the pace of quantum hardware development both of which carry significant uncertainty. CPS stakeholders should act now by leveraging available PQC standards to begin the quantum migration process, while investing in research, education, and regulatory frameworks needed to ensure robust CPS security through the quantum transition and beyond.

## 21. Future Directions and Emerging Technologies

The research and development of quantum-resistant encryption is engaged by all major cybersecurity companies and is at the forefront of the cybersecurity research agenda 1. As quantum computation matures, it is expected that the developed algorithms become deprecated with wider use of quantum computers in the realm of public record. However, this urgency to transition towards quantum-resistant encryption runs counter to the traditional, conservative, and slow-moving protocols for industry standardization. Essentially, industry has to voluntarily agree to switch out their old security methods for quantum ones on a designated day or within a specific time frame. While companies are investigating post-quantum cryptography, it is challenging in many regards due to the changed perspectives on threats, immaturity of the field, and lack of industry-wide agreement on standard set of protocols.

There is a lack of comprehensive reports that account for the range and complexity of threats that quantum computing can bring. There are a number of papers that consider specific cyber threats from quantum computation, mostly regarding femtotechnology and their implications on critical infrastructure and networked systems. It is noted that many of these reports are speculative about the capabilities of quantum computation and take a future deterministic view on its impact on cybersecurity. With a current inability to forecast the exact capabilities and the rate of development of quantum computing, the preferred approach is to understand the current standpoint and its potential cyber threats to infrastructure. This should verify the implications of current readiness and prioritize the development of defense mechanisms for its potential threats.

## 22. Conclusion and Key Takeaways

The rapid development of quantum computing and supporting technologies constitutes a critical, potentially catastrophic threat to the security posture of present day cyber-physical systems. This requires a consideration of these threats, and the formulation of strategies to mitigate them in these systems. This study has examined a collection of significant and possible consequences for CPS security during the quantum computing era. In addition to defining the ultimate quantum limits, the starting point of this discussion was an evaluation of the conventional security framework for CPS 1. Indeed, this facility is critical to develop a real understanding of the specificities actions that can be generated by the extra power offered by quantum apparatuses. Even more recently, the conversation has revealed and explored a threat landscape that can threaten the privacy, availability, and integrity of cyber-physical systems.

It is important to note with a word of caution that classical security tools may be in vain attenuated as against faster processing power and unique quantum adversary's algorithms. In order to be able to come up with a relevant response strategy, the CPS community must take into account dedicated mitigation mechanisms. To address the quantified threat, a variety of complex and creative techniques have been designed. The celebration of methods for dealing with quantum-enhanced vulnerabilities to this end would serve as a positive incentive towards the advancement in those new areas. The emerging decade is anticipated to experience a predominant and driving growth in these vulnerabilities and threats; so, for all cyber-physical system stakeholders should therefore be vigilant in ensuring the necessary defense mechanisms are in place.

**Conflict of Interest:** The authors declare no conflicts of interest.

**Funding:** This research received no external funding.

**Author Contributions:** The author contributed equally to this work. All authors read and approved the final version of the manuscript.

## References

[1] M. Barbeau and J. Garcia-Alfaro, "Cyber-physical defense in the quantum era," Scientific Reports, vol. 12, no. 1, p. 1905, Feb. 2022, doi: 10.1038/s41598-022-05690-1

[2] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, "Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition," Computers & Security, vol. 150, p. 104272, 2025, doi: 10.1016/j.cose.2024.104272

[3] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for quantum computing," arXiv preprint arXiv:2110.14701, 2021, doi: 10.48550/arXiv.2110.14701

[4] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum

cryptography," Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012–1236, Dec. 2020, doi: 10.1364/AOP.361502

[5] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Reviews of Modern Physics, vol. 92, no. 2, p. 025002, May 2020, doi: 10.1103/RevModPhys.92.025002

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Reviews of Modern Physics, vol. 81, no. 3, pp. 1301–1350, Sep. 2009, doi: 10.1103/RevModPhys.81.1301

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of Modern Physics, vol. 74, no. 1, pp. 145–195, Jan. 2002, doi: 10.1103/RevModPhys.74.145

[8] R. Renner, "Security of quantum key distribution," International Journal of Quantum Information, vol. 6, no. 1, pp. 1–127, Feb. 2008, doi: 10.1142/S0219749908003256

[9] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Transactions on Information Theory, vol. 41, no. 6, pp. 1915–1923, Nov. 1995, doi: 10.1109/18.476316

[10] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, no. 7705, pp. 400–403, May 2018, doi: 10.1038/s41586-018-0066-6

[11] A. Boaron, G. Boso, D. Rusca, C. Autebert, C. Agnesi, M. Perrenoud, M. A. Mohd Johari, F. Bussières, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," Physical Review Letters, vol. 121, no. 19, p. 190502, Nov. 2018, doi: 10.1103/PhysRevLett.121.190502

[12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature, vol. 549, no. 7670, pp. 43–47, Aug. 2017, doi: 10.1038/nature23655

[13] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature, vol. 582, no. 7813, pp. 501–505, Jun. 2020, doi: 10.1038/s41586-020-2401-y

[14] G. Zhang, J. Wang, Y. Liu, X. Guo, Z. Chen, Y. Li, H.-K. Lo, and Q. Zhang, "Large-scale quantum key distribution network and applications," Frontiers of Optoelectronics, vol. 12, no. 3, pp. 289–302, Sep. 2019, doi: 10.1007/s12200-019-0945-1

[15] E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric blind information reconciliation for quantum key distribution," Physical Review Applied, vol. 8, no. 4, p. 044017, Oct. 2017, doi: 10.1103/PhysRevApplied.8.044017

[16] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 1000 km optical fibres," Nature Photonics, vol. 16, no. 8, pp. 593–598, Aug. 2022, doi: 10.1038/s41566-022-01061-1

[17] B. Li, G. Zhang, C. Zhou, Y. Wang, W. Li, and Q. Zhang, "Measurement-device-independent quantum key distribution: Advances and perspectives," Quantum Science and Technology, vol. 6, no. 3, p. 033003, Apr. 2021, doi: 10.1088/2058-9565/abfd33

[18] W. Wang, B. Li, C. Zhou, Y. Wang, W. Li, G. Zhang, and Q. Zhang, "Experimental free-space measurement-device-independent quantum key distribution over 40 dB channel loss," npj Quantum Information, vol. 7, no. 1, p. 113, Jul. 2021.

**How to cite this article**

Nori, H. A., "Cyber-Physical System Security in the Age of Quantum Computing: Identifying Threats and Developing Mitigation Strategies," CyberSystem J., vol.3, no. 1, pp. 62-75, 2026. doi: 10.57238/csj.2026.1026

Access this article online