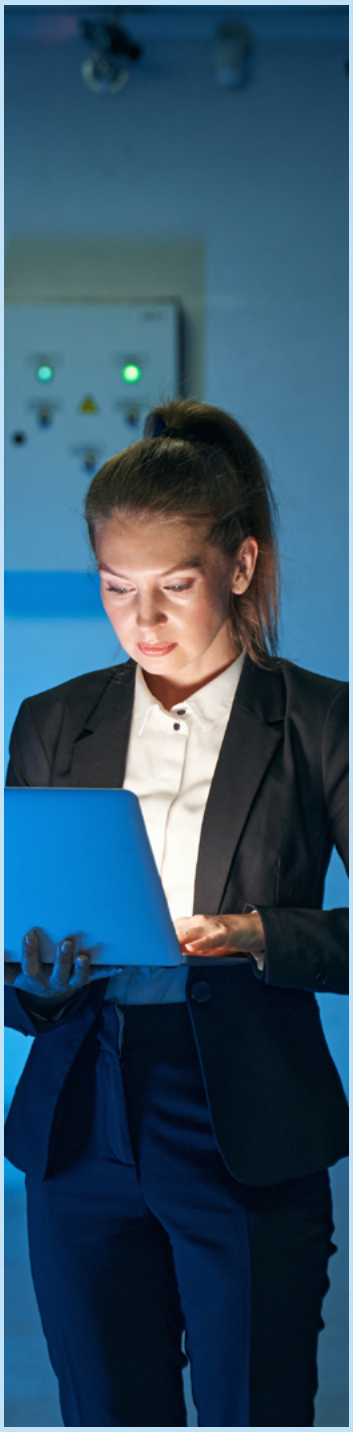
VIEW POINT



RISING NETWORK THREATS IN THE QUANTUM ERA: AI-DRIVEN CYBERSECURITY AND POST-QUANTUM RESILIENCE

Infosys®
Navigate your next

ABSTRACT

As digital technologies become embedded across critical sectors including transport, banking, and telecommunications, organizations must carefully consider the implications of what is known as Quantum Computing. As a move beyond classical computing, Quantum computing introduces new opportunities and risks, particularly when combined with Artificial Intelligence (AI). Together, these capabilities significantly reduce the time required to compromise classical cryptographic algorithms. Traditional cryptographic algorithms such as RSA, ECC, and classical digital signature schemes face increasing risk in a post-quantum future. While symmetric encryption such as AES remains comparatively resilient, asymmetric key exchange and signature mechanisms are particularly vulnerable to quantum attacks. The convergence between AI, quantum, and cybersecurity highlights the opportunities and challenges in three of the most important industry sectors to ensure strength in depth at speed, efficiency, and the evolving landscape of cyber threats, and how they themselves evolve and appear.

In 2026, the cybersecurity landscape is changing fundamentally at a speed which is revolutionizing how we use AI, influenced by Machine Learning (ML), Quantum Computing, Cybersecurity, and Data. Traditional cryptographic controls that once protected sensitive systems are no longer sufficient when viewed against long-term data exposure risks. Adversaries can increasingly target data that was previously considered well-protected, exposing long-term confidentiality risks.

With the continued advancement of AI and its proven value, and as AI systems increasingly leverage quantum-accelerated computing models, the risk of decrypting sensitive data encrypted using conventional methods grows significantly. This impending threat emphasizes the need for the development of quantum-resistant encryption techniques. Another major challenge in cybersecurity is the persistence and evolution of sophisticated cyber-attacks, not only from state-sponsored actors and criminal gangs, but increasingly from individuals in the future.

The combined power of quantum computing, machine learning, and AI presents a material shift in the cybersecurity risk profile. The power of Quantum, ML, and AI is now a nuisance to cybersecurity from state-sponsored cyber-attacks to ransomware, phishing scams, and targeting individuals in positions of authority, using a combination of sophisticated techniques and asset devices with software which can crack protective measures in minutes rather than in months and years. The shift from broad-based attacks to highly targeted, AI-assisted campaigns has materially altered the threat–risk paradigm. As attacks become more intricate and complex, traditional security measures are not enough to protect against unparalleled computational power. Quantum computing has the potential to provide advanced threat detection and mitigation capabilities that surpass the limitations of classical computing and must be used now in 2026 and beyond to help combat and improve advanced threat detection coupled with GenAI, AI, and ML.

As we see much more integration of modern technology, but also network macro/micro segmentation to protect environments and the leveraging of zero trust architecture and policy.

External Document © 2026 Infosys Limited

It seems we have arrived back at the infancy of IT to further enhance our lives. However, this progress also introduces significant risks. Critical sectors such as finance, utilities, telecommunications, manufacturing, and healthcare must be proactively protected before this technology is exploited for large-scale cyberattacks. If left unaddressed, it impacts these estates and creates systemic risk that requires proactive reinforcement of cybersecurity controls.

Quantum computing offers an opportunity to enhance security throughout the infrastructure chain and interconnected solutions and systems. It has become clear that integrating quantum computing into cybersecurity strategies presents a proactive and necessary approach to enhance resilience and enable robust cryptographic protocols. As we navigate the current challenges in 2026 and beyond, it becomes clear that integrating Quantum Cryptography ensures a more comprehensive protection against cybersecurity challenges and explores the opportunity to harness these to drive efficient and effective responses at speed and velocity.

External Document © 2026 Infosys Limited

ADVANCED QUANTUM CRYPTOGRAPHY AND CYBERSECURITY WITH AI AND ML MEASURES

Given the increase in cybersecurity threats, interconnected devices, and continued digitization of critical infrastructure, the potential for cyber-attacks is reaching cross-cutting industries and not confined to just one. The use and prioritization of effective cybersecurity protocols to protect sensitive data, services, platforms, and applications and reduce disruption of IoT/OT, assets and devices requires expedited cyber resilience coupled with enhancements to stay ahead of adversaries. The evolution of attack vectors and the threats within those vectors now leverage advanced methods to hack, deny, and exfiltrate data with ease. Conversely, advanced cybersecurity measures, controls, and cryptography need to evolve. Traditional cybersecurity methodologies and encryption techniques are now themselves susceptible to sophisticated attacks such as "harvest now, decrypt later" (HNDL). This reality necessitates a major shift towards quantum-resistant algorithms, coupled with further innovative security solutions, as part of next-generation system protection.

Whilst never fully secure, it can aid in decision making and reactive measures to negate a cyber-attack and the collective consequences of the attack, downstream towards supply chains as well as upstream to customers. The financial losses, damage to reputation, and disruption of critical and sensitive systems underscore the requirements for robust rebuttal in using quantum cryptography algorithms to protect and defend the digital ecosystem and maintain confidentiality, integrity, and availability of data services and infrastructure that leverage it.

As such, the development of cutting-edge and innovative cybersecurity measures is more important than ever to mitigate the ever-evolving cyber threats and actors to ensure security measures stay ahead. The key potential of quantum computing and advanced cryptography technologies lies in leveraging quantum-safe symmetric and asymmetric encryption to deliver greater speed and efficiency when securing large volumes of critical data, while ensuring robust key exchanges, particularly when communicating with untrusted parties.

External Document © 2026 Infosys Limited

Algorithm	CNSA 2.0 Suite Algorithm	NIST Standard Available	Type	Purpose	Replaces
LMS	Yes	Yes	Stateful hash-based digital signature scheme	Code and Firmware signing	ECDSA, RSA encryption algorithm
XMSS	Yes	Yes	Stateful hash-based digital signature scheme	Code and Firmware signing	ECDSA, RSA
ML-DSA	Yes	Yes	Lattice-based	All digital signing use cases	ECDSA, RSA
ML-KEM (Kyber)	Yes	Yes	Lattice-based	Key Xchange	ECDSA, RSA, Diffie-Hellman (key exchange)
ML-SLH	No	Yes	Stateful hash-based	All digital signing use cases	ECDSA, RSA
FALCON	No	No	Lattice-based	All digital signing use cases	ECDSA, RSA

This layered, lattice-based encryption approach, combined with a proactive security posture, is essential to ensuring a secure and trustworthy digital arena amid the relentless cyber threats and challenges we are witnessing in 2026 and beyond.

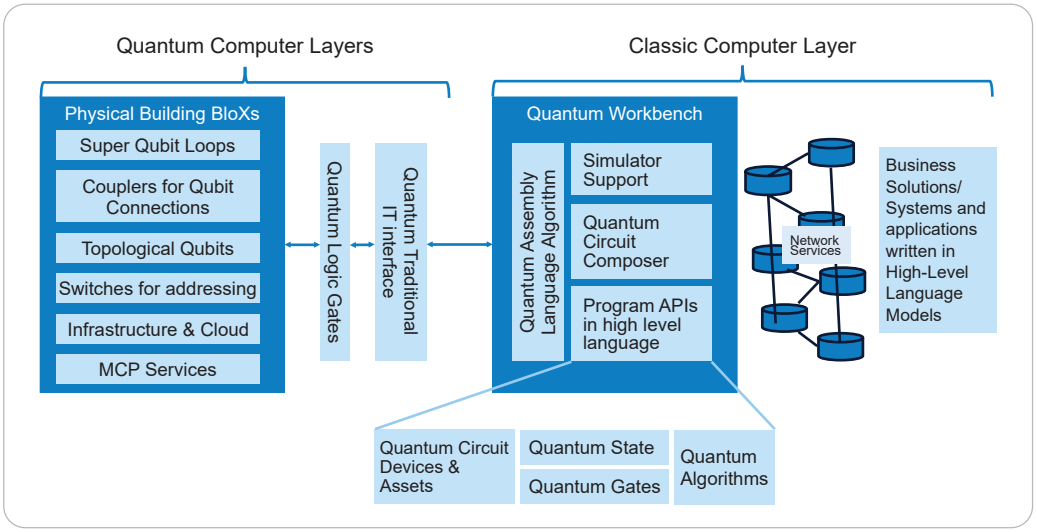
External Document © 2026 Infosys Limited

PRINCIPLES OF QUANTUM COMPUTING

The principles originate from quantum mechanics and apply to quantum computing, including the ability to solve intricate calculations and computational problems, leveraging 'qubits' as the equivalent of classical 'bits' (the smallest unit of data used in a computer operation). While classical bits can either hold the value 0 or 1, qubits can hold multiple possible values at once through a property called 'superposition.' Qubits can exist in a superposition of states and hold the value 0, 1, or both simultaneously. The state of superposition allows quantum computers to process a greater amount of information simultaneously compared to classical computers. For instance, a 4-qubit quantum computer can hold 16 different numbers at the same time, allowing it to perform multiple calculations simultaneously. This makes quantum computers potentially much faster than classical computers for tasks such as factoring large numbers or simulating quantum systems. When a quantum calculation is complete, measuring the qubits, which is needed to extract a usable result, it collapses them to one value. This characteristic enables quantum computers to efficiently handle complex algorithms and factor large numbers at speeds that surpass classical computers, making them particularly suitable for cryptographic applications.

The other variable within Quantum Cryptography Qubit is 'entanglement' also known as Quantum 'Interference'. An occurrence factor where the state of one qubit is directly related to the state of another, no matter the distance between them. A state of quantum entanglement between qubits is called 'coherence.' Each qubit can hold many more values than a classical bit, and entanglement enables quantum computers to connect multiple qubits to perform operations on an exponentially larger set of data than classical computers and with fewer resources. These computers then provide ranges of possible answers to these operations, reducing calculation times greatly.

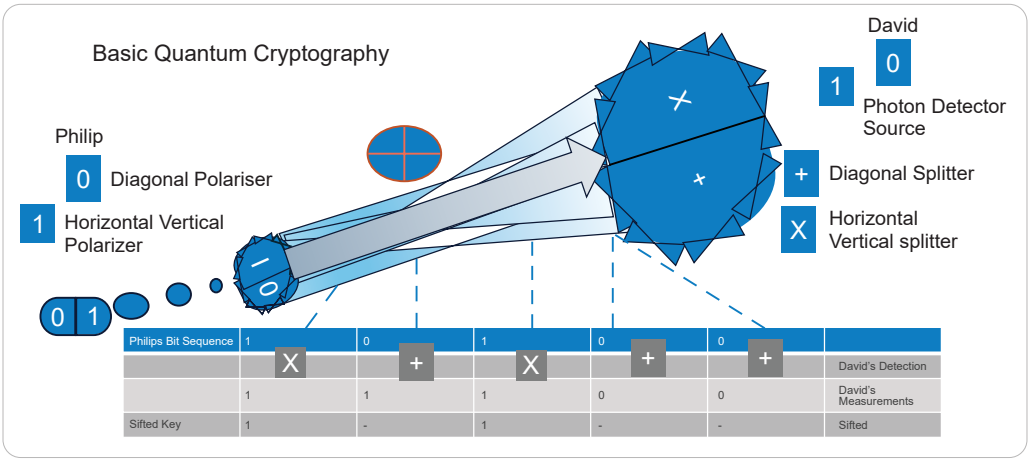
Consequently, this enables quantum computers to have the ability to process and analyse vast amounts of data in parallel, along with its potential to advance encryption techniques, optimize AI whilst opening up new resistant measures in cybersecurity, which are therefore standardized as encryption algorithms that themselves can delay and resist an attack by another quantum computer.



External Document © 2026 Infosys Limited

QUANTUM COMPUTING IN CRYPTOGRAPHY

Current and traditional cryptography techniques, such as early AES, ECC, and RSA rely on the difficulty of factoring large 'algorithm' numbers for security. However, quantum computers can efficiently reason large numbers using algorithms like Shor's and Grover's algorithm, which presents a substantial risk to the security of encrypted data. In response to this threat, the cybersecurity community has been focused on developing Post-Quantum Cryptographic (PQC) algorithms that can resist quantum-based attacks. PQC encompasses many encryption techniques, including lattice-based cryptography, hash based, code-based cryptography, and multivariate cryptography. Others include Quantum Fourier Transform (QFT), used as part of Shor's enhancement for mean period findings over Quantum Phase Estimation (QPE), enabling efficient and effective innovation at speed, and used in ML and simulations. Quantum Approximate Optimization Algorithm (QAOA) has potential use in BFSI industries, Retail/MFG, and AI, solving combined problems through optimization.



These methods are designed to withstand the computational power of quantum computers, thereby reducing the risk posed by quantum-based attacks on traditional cryptography solutions and systems. The adoption of post-quantum cryptographic algorithms is expected to enhance cybersecurity by offering robust protection against potential threats from quantum computing. Artificial Intelligence (AI)-based algorithms can manage and optimize quantum 'keys', adapting to security needs in real-time and ensuring that data transmission between parties is impenetrably secure.

For next gen PQC, Quantum Key Distribution (QKD) generates keying material for an encryption algorithm that provides confidentiality. Such keying material can also be used in symmetric key cryptographic algorithms to provide authentication and integrity if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not offer any means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or pre-placed keys to provide that authentication. Furthermore, the confidentiality services offered by QKD can be provided by quantum-resistant cryptography, which is less expensive with a better understood risk profile.

External Document © 2026 Infosys Limited

Applications in Various Sectors

Banking and Finance

Quantum cryptography can secure financial transactions, ensuring that funds transfers, digital payments, and online banking activities remain confidential and tamper-proof.

Defence and Military

In an era of cyber warfare, quantum-secured communication can protect critical military data, strategies, and communications from potential adversaries.

Healthcare

With the increasing digitization of medical records, quantum cryptography can play a pivotal role in ensuring the privacy and security of sensitive patient data.

Telecommunications

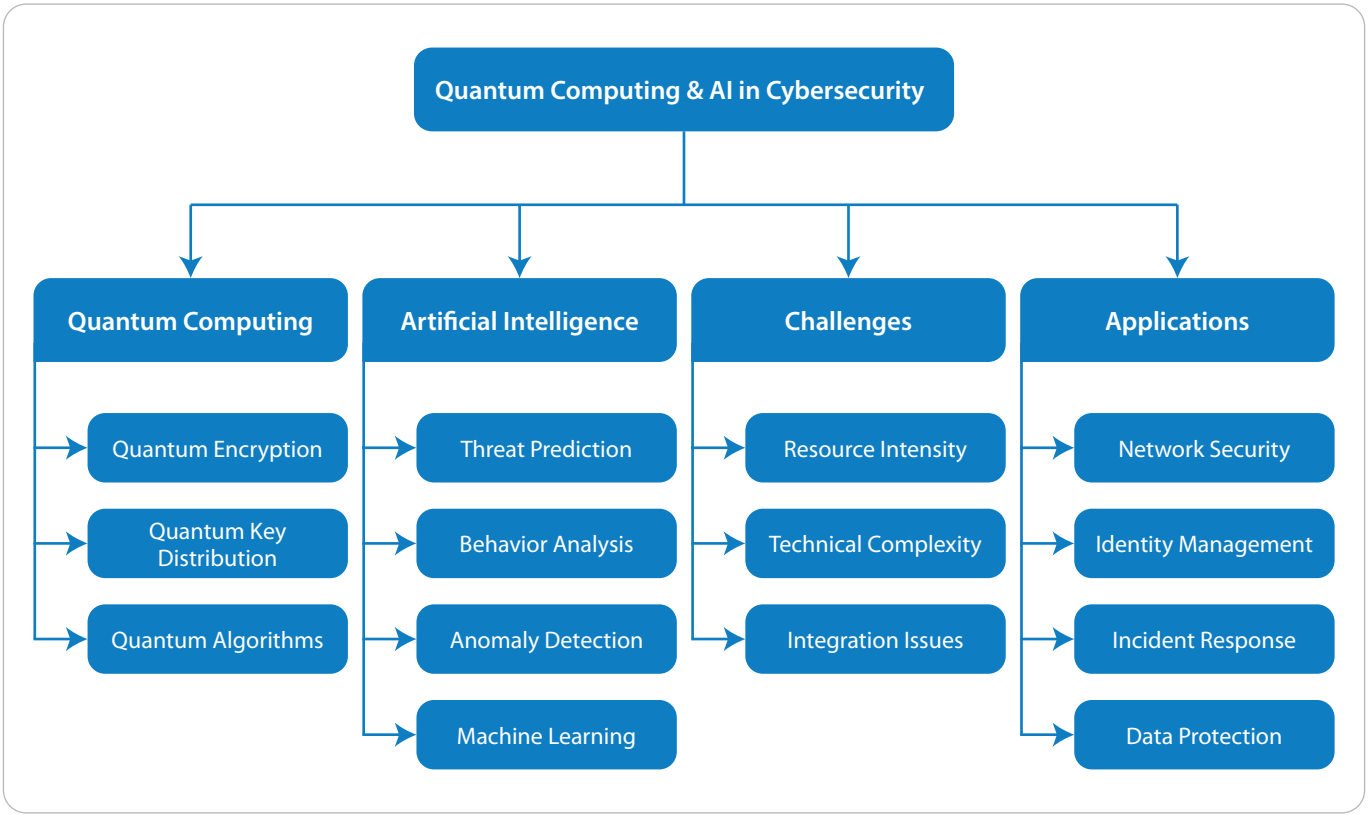
As the backbone of global communication, the telecom sector can benefit immensely from quantum cryptography, ensuring secure communication channels worldwide.

Classic Cryptography	Quantum Cryptography
Uses logic based on digital logic	Based on quantum theory
Sends digital signals using bits	Sends data through the use of particles or photon workbench 0,1, + and X characters sifted through diagonal, horizontal, and photon source make up
Typically doesn't have a range associated with it	Typically has a range associated with it that requires fibre optic wires and repeaters
Encryption is based on mathematical algorithms	Encryption is based on quantum properties

External Document © 2026 Infosys Limited

QUANTUM RESILIENCE AND THREAT DETECTION

Infosys has already leveraged AI to fuel business growth as a global organization over the last 24 months, investing collaboratively and building AI capabilities through R&D. Apart from its impact on Cryptography, quantum computing shows promise in taking ML and AI to a new level of improving threat detection and mitigation in cybersecurity. The exceptional computation power of quantum computers allows for efficient analysis of large-scale data sets and rapid identification of patterns that indicate cyber threats. By harnessing quantum computing's processing power, Artificial Intelligence can automate complex security protocols with a speed that is impractical with classical computing solutions. This includes the dynamic adaptation of encryption algorithms based on threat level analysis, enhancing the robustness of cyber defenses. The potential to accelerate data processing and pattern recognition will align with the changing landscape of cyber-attacks, where quick detection and response are crucial for mitigating the impact of security breaches, whilst having human oversight. Tasks such as network optimization, resource allocation, and vulnerability assessment can benefit from the computational efficiency of quantum algorithms, leading to more effective and proactive security strategies and deployments of services and systems.



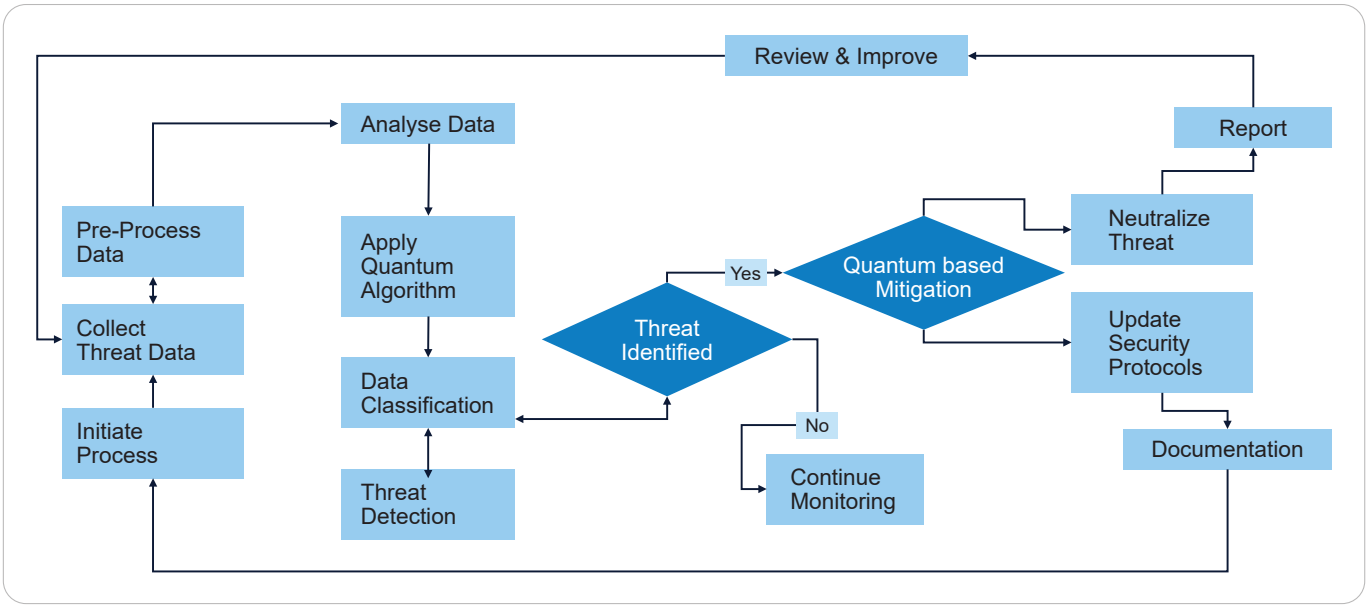
External Document © 2026 Infosys Limited

Feature	Classical Computing	Quantum Computing
Processing Power	Sequential, limited by transistor count	Parallel processing via qubits, exponentially faster
Encryption Security	Secure with RSA, ECC, AES	Can break classical encryption but enables quantum-safe cryptography
AI Applications	Slower machine learning training	Faster AI model training and pattern recognition
Cybersecurity	Vulnerable to advanced attacks	Can both weaken and strengthen cybersecurity
Data Processing	Linear, requires extensive computational resources	Non-linear, can process multiple possibilities at once
Commercial Availability	Widely available	Still in early-stage development

External Document © 2026 Infosys Limited

QUANTUM-ENHANCED SECURITY

As discussed above, with basic quantum cryptography, Quantum Random Number Generators from quantum computing provide a three-dimensional randomized algorithm towards cryptographic security. This unpredictable and unbiased random numbers enhance the robustness of cryptographic protocols.



Quantum secure communication utilizes the principles of quantum key distribution to establish secure and intrinsically unhackable communication channels. Quantum key distribution (QKD) uses these quantum properties such as uncertainty principles to facilitate the secure exchange of encryption keys between communicators with any attempt to intercept or eavesdrop on the communication would disrupt the quantum nature of the transmitted information, therefore alerting the communicating parties themselves to the presence of an intrusion. This innovative approach to secure communication shows enormous potential in protecting sensitive information against unauthorized access and interception, making it a valuable asset in cybersecurity measurements.

External Document © 2026 Infosys Limited

QUANTUM THREATS AND REGULATORY CONSIDERATIONS

The high-speed advancement of quantum computing presents unprecedented challenges for traditional cryptographic methodology. Quantum computers have the potential to efficiently factor large numbers using algorithms like Shor's algorithm, posing a significant risk to the security of encrypted data. In response to these quantum threats, cybersecurity focuses on developing post-quantum cryptographic algorithm(s) that resist quantum-based attacks. Various post-quantum cryptography techniques have been proposed, including 3-dimensional lattice-based cryptography, code-based cryptography, and multivariate cryptography. These encryption schemes aim to withstand the computational speed and power of quantum computers, ensuring that data remains secure in the quantum computing protect and defend scenario. As organizations prepare for the era of quantum computing, integrating post-quantum cryptographic algorithms is essential for fortifying the foundations of cybersecurity and safeguarding sensitive information from potential quantum-based attacks. Whilst quantum computing does not yet break the Internet today, the combination of the following: 1) Harvest-now, decrypt-later (HNDL) activity, 2) accelerating research that reduces resource estimates for Shor's algorithm, and 3) mandated timelines from standards bodies and governments, makes 2026 the year to move from planning to execution.

Quantum-resistant Encryption in Enterprise Services

As discussed, the quantum threat poses a risk to current cryptographic systems, government agencies, and enterprises increasingly require prioritizing the adoption of quantum-resistant encryption to protect their sensitive information assets and data. By examining the real-world applications of quantum-resistant encryption, we can gain valuable insights into the feasibility and effectiveness of post-quantum cryptography solutions in various operational settings. Future prospects and research directions as quantum computing progresses, is set to revolutionize the cybersecurity landscape, requiring significant evolution in encryption methods to protect and defend against adversaries. Quantum cybersecurity leveraging 3D lattice cryptography requires staying ahead of malicious adversaries. Currently what is seen as taking 50 years plus is now taking less than 5 minutes to hack, leveraging both AI and quantum services and solutions back against vulnerable organizations.

To enrich this, a focus on the development of quantum-resistant algorithms designed to counteract the superior computational capabilities of a quantum computer, is ensuring long-term data security against quantum threats. Combining quantum encryption with AI and security protocols offer a promising trajectory. This involves leveraging quantum communication channels and quantum cryptography to strengthen cybersecurity frameworks by integrating conventional encryption techniques and replacing them with quantum processes.

The application of quantum-resistant encryption across the Internet of Things (IoT), Operational Technology (OT), and cloud computing will require robust protection in the near future to safeguard business operations and crown jewels. This is essential to secure increasingly interconnected and distributed digital infrastructure and address contemporary security challenges.

Industries such as Telco, MFG, and BFSI is not limited to technological advancements but also encompasses the human and behavioral dimensions of secure communication. This must focus on quantum encryption's usability and user experience to facilitate broader adoption

External Document © 2026 Infosys Limited

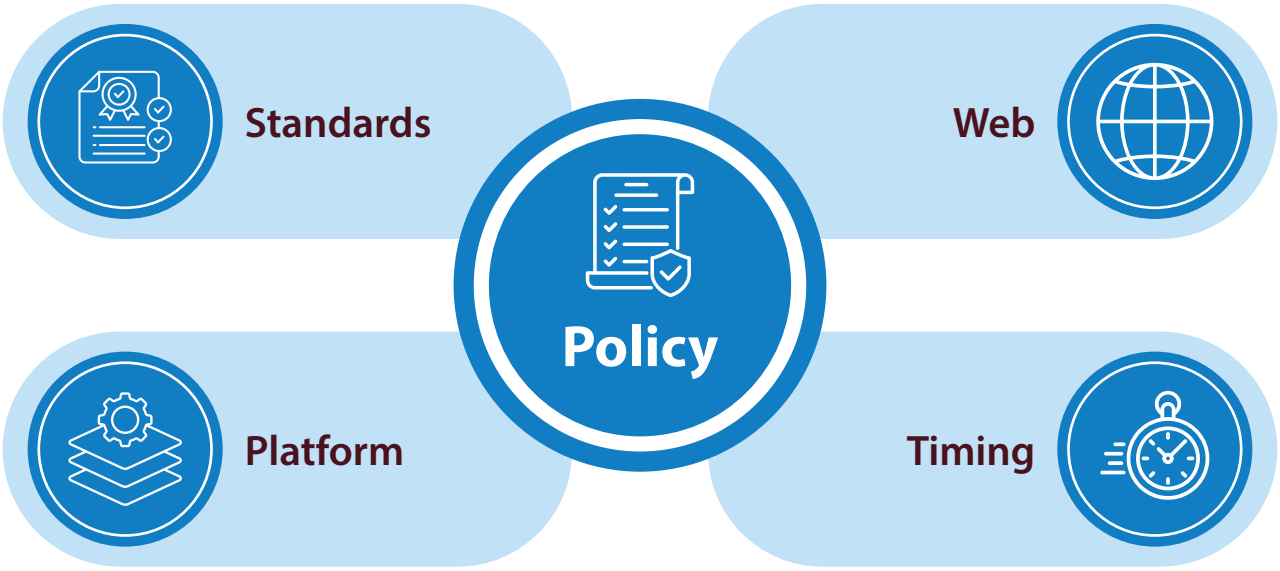
and practical implementation. Whilst we see speed and efficiency drivers through the use of AI, the optimization of hybrid models to harness quantum advantage must be leveraged fully. The design of more efficient quantum circuits tailored to specific machine learning tasks, which explore sensitive and critical quantum algorithms must not limit scalability of quantum technology, whilst developing quantum-AI data encoding methods.

Testing and benchmarking against current cryptography models will be critical in assessing the superiority of quantum models. As quantum infrastructure evolves, machine learning applications will likely benefit from increased qubit counts, improved coherence times, and quantum error correction, driving the quantum advantage in practical cybersecurity applications. Through these combined efforts, AI, and machine learning, quantum computing is positioned to play a significant role in future cybersecurity solutions.

The future of quantum cybersecurity is inherently multi-disciplined, blending current cryptography algorithms, technology, and AI human-centric enhancements to ensure encryption resilience and effectiveness in the quantum computing age, safeguarding sensitive information against new threats.

Where Quantum Stands in 2026 and Why It Matters Now

2026 is the year where post-quantum migration moves from planning to execution, while AI-driven offense and defense both accelerate. The most immediate quantum risk is not a live break of RSA/ECC, but the "harvest-now, decrypt-later (HNDL)" pipeline; at the same time, AI agents and developer-side supply-chain compromises are shifting the attack surface from "breaking in" to "logging in." CISOs should treat crypto-agility and AI governance as board-level priorities and start rolling PQC into real traffic paths now.



External Document © 2026 Infosys Limited

Standards

NIST finalized the first three PQC standards in August 2024, FIPS 203 (ML-KEM) for key establishment, FIPS 204 (ML-DSA) for signatures (Dilithium), and FIPS 205 (SLH-DSA) for stateless hash-based signatures (SPHINCS+). NIST's guidance is explicit: organizations should begin migration now; NIST IR timelines deprecate vulnerable public-key algorithms by 2035 with earlier cutovers for high-risk systems.

Policy

NIST PQC standards (FIPS 203/204/205) are finalized. NSA's CNSA 2.0 lays out a federal roadmap to 2035, with near-term milestones (e.g., software/firmware signing and browser/TLS adoption first), and warns that RSA/ECC will not be sufficient in a quantum era. European Union & G7 coordination (2025–2026), the EU's coordinated roadmap expects Member State transition plans by December 31, 2026, with high-risk use cases secured by 2030 and broad transition by 2035.

Web

The web is moving, with real breaks along the way. Google shipped hybrid TLS (X25519+Kyber/ML KEM) in Chrome and QUIC; early rollouts showed middlebox breakage as oversized ClientHello messages encountered fragile appliances, useful warning that ecosystem debt exists and must be burned down. Chrome's post quantum key agreement remains on a deprecation-managed path, with modern codepoints for ML KEM hybrids. In 2026, CISA released lists of "widely available" PQC products, such as web browsers and cloud services, to accelerate industry adoption.

Platform

Microsoft announced general availability of ML KEM and ML DSA primitives across Windows 11/Server 2025 and .NET 10, making PQC deployable in enterprise stacks (TLS, code signing, PKI, VPN). This materially lowers the barrier to pilots in Windows-centric estates. Operational Technology (OT) awareness: CISA's OT guidance (TLP:CLEAR) highlights quantum risk pathways in IT/OT convergence and prescribes segmentation, crypto-agility, and lifecycle planning for upgrades where public-key functions exist (auth, signing, key exchange).

Timing

Threat timing is uncertain, but the window is closing. Resource estimation studies show continued downward pressure on qubit counts and runtimes for Shor, e.g., 2025–2026 research suggesting alternative codes (QLDPC) and distributed architectures can reduce the physical qubit footprint at engineering cost trade offs.

External Document © 2026 Infosys Limited

AI + Quantum: The 2026 Attack Surface

AI is industrializing offense. Threat-intelligence indicates AI-assisted campaigns scaling speed and throughput (credential abuse, targeted social engineering, exploit triage), with a strategic pivot from "break in" to "log in." AI also shortens attacker OODA (Observe, Orient, Decide, Act) loops and helps mine stolen data for high-value extortion targets.

PQC implementations are attackable even if algorithms are sound. 2025–2026 cryptanalysis shows higher-order side-channel attacks against Kyber/ML-KEM and Dilithium/ML-DSA on embedded targets; mitigation remains a significant engineering task (masking, constant-time, hardened reference code, anomaly detection).

AI-assisted credential theft and repo poisoning: AI-built phishing and malicious developer content that compromises workstations where PQC libraries, keys, and build artifacts live.

Quantum-cloud side channels:
As organizations experiment with QCaaS, multi-tenant leakage can expose circuit size, structure, or induce faults, an emerging but relevant risk to IP.

OFFENSE

AI compresses attacker timelines (recon -> initial access -> monetization), driving throughput more than novelty. Expect broader credential-stuffing, supply-chain pivots, and deepfake assisted social engineering against PQC program staff and PKI owners.

DEFENSE

AI-augmented detection and automated response will be essential for middlebox tuning, certificate rollovers, and policy conflicts during PQC cutovers. But governance is mandatory and AI agents with shell access and repo rights have already shown failure modes and insider-like risk.

External Document © 2026 Infosys Limited

SUMMARY OF ETHICAL AND REGULATORY CONSIDERATIONS IN QUANTUM CYBERSECURITY

The intersection of quantum technology and cybersecurity raises various ethical and regulatory considerations that require thorough examination. Whilst we embrace the potential of quantum computing to transform encryption methods, it is essential to carefully navigate the ethical dimensions of utilizing quantum cybersecurity solutions responsibly. One of the primary ethical considerations revolves around the implications of quantum computing for data privacy/scrapping and security. As quantum-resistant encryption methods become essential for safeguarding sensitive information, assessing the ethical implications of potential variations in data security capabilities across different sectors and regions is crucial, especially in the collection, storage, and processing, whilst data provenance also plays a part towards ethical access and usage. Ethical frameworks that advocate for equity and fairness in implementing quantum-cybersecurity solutions are crucial in ensuring that the advantages of enhanced encryption are accessible to those who have a need to know, and not merely a nice-to-have access. Additionally, regulatory considerations are critical in shaping the adoption and deployment of quantum-cybersecurity solutions. As quantum-resistant encryption methods deploy, evolve, and mature, regulatory frameworks must adapt to address the unique characteristics of quantum technology and its implications for data protection. Banking, Financial Services and Insurance (BFSI), telecommunications, high-end manufacturing, and retail service industries, especially online, will need to balance innovation and regulatory compliance within a complex yet essential roadmap for establishing a secure and regulated environment for quantum-cybersecurity advancements.

The intersection of quantum technology and cybersecurity raises various ethical and regulatory considerations that require thorough investigation. As we embrace the potential of quantum computing to transform encryption methods, it is essential to carefully navigate the ethical dimensions of utilizing quantum cybersecurity solutions responsibly, whilst the abuse of its power may cause a myriad of disruptions, including threat vector attacks.

External Document © 2026 Infosys Limited

OUR VIEW FOR 2026 AND BEYOND

Quantum computing is not a panic button. It's a planning accelerant. With PQC standards finalized and platform support shipping, the credible risk in 2026 is failing to start, not over-rotating early. Meanwhile, AI is changing the shape of incidents more than their type, but that alone demands identity-centric defenses, hardened developer workflows, and crypto-agile architectures that can absorb PQC at production scale. Organizations that move now will shrink their HNDL exposure and avoid the worst migration shocks later.

ENCRYPT

- Encrypt today's traffic with tomorrow in mind: Prefer TLS hybrid ML-KEM-768 + X25519 where feasible
- Plan to migrate certificates and identity stacks to ML-DSA
- Keep SLH-DSA as your diversity fallback
- Map your plan to CNSA 2.0 and regional timelines (EU 2026 plans due)

ZERO-TRUST

- Zero-trust your developer estate + AI tools: Treat AI assistants, CLIs, and IDE extensions as semi-trusted executables
- Requires signed, vetted sources
- Monitor for silent exfiltration
- Isolate PQC keys and build chains
- Assessments for ML-KEM/ ML-DSA in embedded and HSM contexts

COMMUNICATE

- Communicate HNDL risk to the board
- Delay increases the volume of already-captured data that will become plaintext post-Q-day
- Tie PQC pilots to data longevity, not just system criticality
- Budget for implementation security, not just algorithms

External Document © 2026 Infosys Limited

CONCLUSION

In conclusion, quantum computing poses unprecedented challenges to traditional cryptographic methods, necessitating the development and integration of post-quantum cryptographic algorithms. As organizations and governments prepare for the quantum computing era, quantum-resistant encryption is increasingly prioritized to protect sensitive information. Studies show the integration of post-quantum cryptographic solutions provide valuable insights into the challenges and advantages of transitioning to quantum-resistant encryption qubit service. Quantum algorithms also optimize AI processes, enabling more robust encryption and rapid anomaly detection. This synergy promises robust protection against sophisticated cyberattacks, ensuring data integrity and security in an increasingly digital world.

The next generation focus is now set on enhancing quantum encryption, extending its applications to fields like the Internet of Things, and addressing the human-centric aspects of secure communication channels in telecommunication services and those that use them such as BFSI industries and high-volume invoicing and receipting in MFG sectors. Lastly, ethical and regulatory considerations are crucial in ensuring equitable access and compliance when implementing quantum-cybersecurity solutions, as our adversaries will be doing the same, trying to leverage AI and quantum for their own gains. Whilst we must look to achieve this, certain encryption algorithms that once took tens of years to break are now vulnerable in minutes.

ABOUT THE AUTHOR

Luke Smith

AVP – Senior Industry Principal

Luke, a seasoned security professional, brings extensive expertise in designing and implementing robust security frameworks, safeguarding sensitive data, and ensuring regulatory compliance. His proficiency in various cybersecurity frameworks, cloud platforms, and infrastructure security enables him to drive organizational success through strategic technical leadership.

External Document © 2026 Infosys Limited

For more information, contact askus@infosys.com

Navigate your next

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.