

SURVEY

Post-Quantum Cryptography and Nature-Inspired Cyber Defense: Strategic Readiness and Adaptive Techniques for Next-Gen Threat Response

SHISHIR KUMAR SHANDILYA¹, (Senior Member, IEEE), CHIRAG GANGULI²,
AJAY KUMAR³, IVAN IZONIN⁴, (Senior Member, IEEE),
AND MICHAL GREGUS⁵, (Member, IEEE)

¹School of Data Science and Forecasting, Devi Ahilya Vishwavidyalaya, Indore, India

²VIT Bhopal University, India

³Centre for Defence Engineering and Physical Science, Defence Academy of the United Kingdom, Cranfield University, SN6 8LA Shrivenham, U.K.

⁴Department of Artificial Intelligence, Institute of Computer Science and Information Technologies, Lviv Polytechnic National University, Lviv, Ukraine

⁵Faculty of Management, Comenius University Bratislava, 820 18 Bratislava, Slovakia

Corresponding author: Michal Gregus (Michal.Gregus@fm.uniba.sk)

ABSTRACT The emergence of quantum computing poses a transformative challenge to established cybersecurity protocols and traditional cryptographic systems, necessitating an urgent transition toward post-quantum cryptography. As quantum threats evolve from theoretical possibilities to practical risks, governments and industrial sectors are increasingly compelled to develop strategies for adopting quantum-resistant algorithms. This paper evaluates the global landscape of post-quantum security, with a specialized focus on the defense strategies adopted by technologically advanced nations. It investigates the efforts of these countries to construct quantum-resilient security architectures while addressing the distinct technical and resource constraints faced by developing nations. A primary contribution of this research is the analysis of the Industry Readiness Assessment Survey, which evaluates organizational awareness and technical preparedness within the specific context of India's digital and regulatory environment. The findings highlight the critical importance of mitigating "harvest now, decrypt later" threats through international cooperation and the development of sovereign transition plans. By synthesizing empirical survey data with strategic policy analysis, this paper provides a roadmap for securing national interests and ensuring long-term data integrity against future quantum computational capabilities.

INDEX TERMS Post-quantum cryptography, cryptographic agility, hybrid cryptographic schemes, Shor's algorithm, lattice-based cryptography, harvest now decrypt later, national quantum mission.

I. INTRODUCTION

Current digital security relies predominantly on cryptography, and public-key cryptography plays a central role. It is based on complex mathematical problems that cannot be easily solved by conventional computers, thus protecting online data and communications. However, the emergence of powerful quantum computers poses a significant threat. Such machines could leverage algorithms such as Shor's algorithm to efficiently break these mathematical foundations, making current security measures obsolete and jeopardizing online information privacy and security [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Cong Pu¹.

In response, researchers are actively developing post-quantum cryptography (PQC) methods designed to resist both classical and quantum attacks with an emphasis on seamless integration into existing network infrastructures [2]. This shift is particularly important because IT systems often remain in use for decades, and adversaries may be harvesting encrypted data now with the intent to decrypt it in the future using quantum capabilities. This strategy is known as "harvest now, decrypt later" [3].

Organizations such as the National Institute of Standards and Technology (NIST) in the United States are already working to standardize these emerging quantum-resistant security methods. Standardization is critical for guiding development and ensuring interoperability among systems globally

as we transition toward quantum-safe security. The historical shift from the Data Encryption Standard (DES) to the Advanced Encryption Standard (AES) took decades, highlighting the scale and complexity of such changes. Similarly, the implementation of Post-Quantum Cryptography (PQC) will require significant time and planning. Therefore, governments and organizations must act proactively to mitigate future threats [4], [5].

Quantum computing threatens the core of current digital security systems, including Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC). While traditional computers struggle to break the mathematical structures behind these cryptographic algorithms, quantum computers could do so with relative ease. Post-Quantum Cryptography (PQC) represents an immediate and necessary response to this looming security challenge. It aims to develop cryptographic techniques believed to be secure against classical and quantum computational threats [3]. This shift is not merely a technical evolution but a profound transformation in cybersecurity strategy to prepare for the quantum era. The threat posed by quantum computing to existing security systems is both real and pressing.

Although large-scale quantum computers are not yet operational, their anticipated arrival necessitates urgent preventive action. The “harvest now, decrypt later” threat is credible, as attackers may already be collecting encrypted information, intending to decrypt it once quantum capabilities become available. This defines the urgency of transitioning to quantum-resistant security to safeguard long-term sensitive data such as intellectual property, state secrets, financial records, and medical information. Without adequate preparation, we risk massive data breaches, loss of trust in digital systems, and potential collapse of critical online infrastructure with serious consequences for global cybersecurity [6].

This paper aims to address this pressing challenge through a comprehensive examination of post-quantum cryptography readiness. Its key objectives are:

- (1) To broadly define PQC and highlight the most promising approaches.
- (2) To outline the specific threats posed by quantum computing to existing security infrastructures.
- (3) To examine the strategies and considerations necessary for an effective and timely transition to PQC, with special emphasis on India’s unique challenges, opportunities, and strategic imperatives.

The paper will also review global efforts toward PQC standardization, explore international transition strategies, and present a detailed analysis of the current cybersecurity landscape in India. The findings of this paper are of significant importance for strategic decisions. The vulnerability of today’s security systems to quantum attacks directly endangers the confidentiality and integrity of digital infrastructure.

The international race to develop, standardize, and deploy PQC technologies is becoming a key arena of technological and strategic competition. A nation’s capacity to safeguard its digital assets in the post-quantum world will directly

influence its global standing and influence. A detailed understanding of the global PQC landscape, combined with a clear analysis of preparedness and strategic choices, is essential to shape effective policies.

With a focus on the Indian context, this paper seeks to provide actionable recommendations to support a resilient cybersecurity framework, protect national interests, and position India as a global leader in post-quantum security transformation [7], [8]. This will help secure India’s long-term diplomatic and national security interests and allow the formation of meaningful international partnerships in this rapidly evolving field.

II. THE QUANTUM COMPUTING THREAT LANDSCAPE

Quantum computing has progressed rapidly in recent years, shifting from theoretical ideas to experimental hardware. Although still in its early stages, this technology poses a growing threat to the cryptographic systems that currently secure digital communication and data. Understanding how quantum computers might break existing cryptographic systems is essential for assessing risks and planning the timely adoption of quantum-resistant technologies.

A. QUANTUM COMPUTING PROGRESS AND THE RISK TIMELINE

Quantum computers operate using principles like superposition and entanglement. Instead of classical bits that are either 0 or 1, quantum bits (qubits) can exist in both states simultaneously. This allows quantum machines to solve certain problems much faster than classical computers. Recent developments by companies such as IBM, Google, and Rigetti have increased the number of qubits in experimental devices, with some reaching over 100 qubits. They have developed quantum processors with over 100 qubits — IBM’s Eagle (127 qubits), Google’s Willow (105 qubits), and Rigetti’s planned over 100-qubit system by the end of 2025 [9], [10], [11].

However, these machines are still in the Noisy Intermediate-Scale Quantum (NISQ) era, where qubits are unstable and error-prone. For quantum computers to break strong encryption, they must have enough logical qubits that are error-corrected and can perform reliable operations. A Cryptographically Relevant Quantum Computer (CRQC) is a system that has the capability of breaking commonly used public-key encryption schemes (for example, RSA, ECC, and Diffie-Hellman) by executing algorithms like Shor’s. The currently available Quantum Computers are not stable enough to achieve this; however, this can be achieved in the coming years, which could threaten Internet security by making encrypted communication and stored data insecure. The timeline for building such a CRQC remains uncertain. Some estimates suggest that a risk may arise in 5 to 10 years, while others suggest that it could take 10 to 20 years or more [12], [13].

As shown in Table 1, the Quantum Threat timeline outlines the four phases: Low Risk now until 2027, moderate progress

TABLE 1. Quantum threat timeline.

Phase	Timeline	Threat Level
Phase 1	Now – 2027	Low
Phase 2	2027 – 2032	Medium
Phase 3	2032 – 2037	High
Phase 4	2037 onwards	Very High

by 2032, higher threat as fault-tolerant quantum computers emerges by 2037, and a very high risk from the mature quantum computing threats beyond 2037. This timeline highlights the need to enhance cryptographic preparedness in each phase.

B. SHOR'S ALGORITHM

Peter Shor proposed a quantum algorithm for factoring large numbers and solving discrete logarithms efficiently. These two problems are the mathematical foundations of widely used public-key cryptosystems like RSA and Elliptic Curve Cryptography (ECC) [8]. RSA gains its security through the computational complexity of factoring large composite numbers. But Shor's algorithm can do so in polynomial time, making RSA susceptible to attacks by quantum computers. Likewise, ECC, which is based on the hardness of the elliptic curve discrete logarithm problem, is also susceptible since Shor's algorithm can solve this with efficiency as well. This could be a major issue; once a Cryptographically Relevant Quantum Computer (CRQC) is developed, most of today's digital communications, secure transactions, and data protection mechanisms will be at risk instantly.

C. THE "HARVEST NOW, DECRYPT LATER" (HNDL) THREAT

Even prior to large-scale quantum computer realization, the "harvest now, decrypt later" (HNDL) strategy already poses a major threat. Under this strategy, attackers harvest and store encrypted data today and plan to decrypt it tomorrow when quantum decryption becomes possible. This has serious implications, including the exposure of sensitive data such as government secrets, medical records, and intellectual property. It also undermines trust in the long-term integrity of encrypted data and provides a strategic benefit to other attackers who can get retrospective access to sensitive communications and documents. These threats highlight the urgency to move to post-quantum cryptography before the quantum threat becomes a practical reality [14].

D. IMPACT ON CRITICAL INFRASTRUCTURE, NATIONAL SECURITY, AND THE ECONOMY

- **Critical Infrastructure:** Secure communication is essential for utilities, transport, and telecom systems.

A breach can result in blackouts, service interruptions, or safety hazards.

- **National Security:** Secure military, diplomatic, and intelligence communication would be at risk. Quantum decryption could enable espionage or undermine national defense.
- **Economic Stability:** Financial transactions, digital commerce, and cryptocurrencies depend on secure encryption. A breach could cause loss of confidence, fraud, and widespread disruption.

Because these systems are interconnected, failure in one can cascade into others, magnifying the impact [15].

E. LIMITATIONS OF CURRENT QUANTUM COMPUTERS

Despite rapid progress, current quantum computers still face major limitations [3]:

- **Limited number of logical qubits:** Today's machines do not have enough stable, error-corrected qubits to run algorithms like Shor's at a meaningful scale.
- **Short coherence times:** Qubits lose their quantum state quickly, making long computations difficult.
- **High error rates:** Quantum operations are noisy, requiring advanced error correction that adds overhead and complexity.
- **Scalability Challenges:** Scaling quantum systems while maintaining control and stability is a huge technical hurdle. These systems require ultra-low temperatures and advanced control mechanisms.
- **Crosstalk Mitigation:** Reducing the interference between qubits to preserve coherence and computation accuracy.
- **Precise Qubit Control:** Ensuring accurate control of each qubit while minimizing the impact on the surrounding qubits.

These barriers mean that CRQCs may still be some years away. However, because the eventual threat is so significant, preparation must begin now. Governments, companies, and researchers around the world are already working on standards and solutions for post-quantum cryptography.

III. GLOBAL LANDSCAPE OF POST-QUANTUM CRYPTOGRAPHY

The global shift toward Post-Quantum Cryptography (PQC) represents a coordinated effort involving governments, standardization bodies, academic and research institutions, and industry stakeholders. This shift is driven by increasing awareness of the threats quantum computing creates to traditional cryptographic systems, especially those that protect national security, financial services, and critical infrastructure.

As shown in Table 2 highlights the development and degradation of Secure Hash Algorithm 1 (SHA-1) from the time it was standardized in 1995 to the discovery of theoretical vulnerabilities in 2005 to its complete collision in 2017 caused browsers to reject SHA-1 certificates. It also points to the

TABLE 2. Timeline to replace cryptographic algorithms.

Year	Event / Milestone
1995	SHA-1 Standardized (NIST)
2001	SHA-2 Standardized (NIST)
2005	SHA-1 Theoretical Weakness Identified
2017	First Full SHA-1 Collision Demonstrated
2017–2018	Browsers Stop Accepting SHA-1 Certificates
2024	Post-Quantum Cryptography (PQC) Final Standards Released (NIST)
2025–2030	CNSA 2.0 / CNSA 3.0 Compliance Window
2033	Increased Quantum Computing Capabilities
2038 (Est.)	Quantum Threat Probability ~50%
Ongoing (2020s–2030s)	“Harvest Now, Decrypt Later” Risk

development of post-quantum cryptography standards by the National Institute of Standards and Technology (NIST) (2024–2025) and to the “harvest now, decrypt later” threat, with quantum computers anticipated to become a 50% threat by the year 2038 [16].

A convergence of regulatory mandates, policy frameworks, and collaborative research is shaping the road map for a quantum-resilient future. In the United States, NIST is spearheading one of the most significant initiatives through its rigorous PQC standardization process, which includes detailed guidance on algorithm selection, risk assessment, and migration strategies. Parallel efforts are being undertaken in Europe, where entities such as the European Union Agency for Cybersecurity (ENISA). And the European Telecommunications Standards Institute (ETSI) is actively developing standards and best practices to support quantum-safe transitions [17].

Various other industry sectors, most notably finance, energy, telecommunications, and technology, are also engaged in pilot deployments and evaluations of quantum-resistant cryptographic algorithms. These include both standalone PQC schemes and hybrid models that combine classical and quantum-safe techniques to ensure backward compatibility and robust security during the transition phase. Organizations such as Palo Alto Networks and PwC have emphasized the urgency of proactive preparation, advocating for phased implementations, cryptographic inventory assessments, and cross-sector collaboration to mitigate the operational risks associated with quantum threats [18], [19].

Collectively, these global initiatives signify a strategic and forward-looking approach to secure digital infrastructure in the post-quantum era, reinforcing the need for harmonized standards, agile migration plans, and sustained international cooperation.

A. COUNTRY-SPECIFIC ANALYSIS

Countries all over the world are making tactical steps to migrate to post-quantum cryptography (PQC) in anticipation of the possible threats of quantum computing to current cryptographic infrastructures (Table 3). The United States is taking a leading position internationally through NIST’s standardization of PQC algorithms. The White House published a National Security Memorandum (NSM-10) that requires all Federal Civilian Executive Branch (FCEB) agencies to conduct an inventory of cryptographic systems and initiate transition planning. The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) are also spearheading joint activities to assist the critical infrastructure and private sector in preparing for a scalable transition, focusing on cryptographic agility and secure interoperability [2]. Large cloud vendors and technology firms are already testing NIST-accepted PQC algorithms in actual implementations [20].

Australia is leading the way with a clear and well-established aspiration of being quantum safe by 2030, led by its Cyber and Infrastructure Security Centre (CISC) [17], which is working closely with operators of critical infrastructure to create roadmaps and provide for flexible migration. Canada has a phased and risk-led approach from its Centre for Cyber Security, which has issued comprehensive guidance to federal departments and agencies to list the quantum-vulnerable assets and develop plans for eventual PQC adoption in various IT environments. India, although still in the initial stages of official PQC transition planning, has shown increasing strategic interest. The National Security Council Secretariat (NSCS) and Ministry of Electronics and Information Technology (MeitY) are promoting research through grants and initiatives like the National Quantum Mission (NQM). The Defense Research and Development Organisation (DRDO) and research institutes such as the Indian Institute of Technology (IIT) Madras and Indian Institute of Science (IISc) are developing indigenous PQC plans and quantum-secure protocols of communication [21]. Discussions in the Indian Computer Emergency Response Team (CERT-In) and the National Informatics Centre (NIC) are working on establishing first-line benchmarks for crypto audits and trial deployments within government infrastructure.

The United Kingdom is implementing a cross-sector security-focused strategy. The UK, via the National Cyber Security Centre (NCSC), has issued detailed guidance on quantum threat preparedness, including crypto agility, threat modeling, and hybrid implementation strategies. R&D is being supported by the government in the form of the UK National Quantum Technologies Programme (NQTP), and regulators such as the Bank of England are evaluating sectoral influence on finance. The UK has followed NIST’s lead on cybersecurity but has also played a key role in helping Europe and Commonwealth countries work together on post-quantum cryptography and secure quantum-ready networks.

TABLE 3. Global post-quantum cryptography (PQC) strategies.

Country	PQC Algorithms	Timeline
Australia	NIST	Full national transition targeted by 2030, with gradual sectoral adoption starting earlier.
Canada	NIST	Strategic planning phase through 2025–2026, followed by phased PQC implementation.
China	China-specific	Initial program development and algorithm planning from the mid-2020s, with an implementation roadmap to follow.
France	NIST	Transition phase commencing from 2024.
Germany	NIST	Early planning and readiness initiatives are ongoing through 2025, ahead of formal migration.
United Kingdom	NIST	Gradual, phased transition by 2035, prioritizing critical infrastructure first.
United States	NIST	Implementation of post-quantum standards and systems is scheduled for 2023–2033, following
		NIST standardization cycles.

China is on a parallel and independent path with massive investments in indigenous PQC standards and the deployment of large-scale quantum communication networks, including a quantum backbone across Beijing-Shanghai and satellite-based QKD programs [22], [23]. The Czech Republic, France, and Germany are moving towards NIST's candidate algorithms, but in the process of adapting them as national security protocols. The French Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) and German Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI) are already making investments in R&D and pilot deployments of quantum key distribution (QKD) and hybrid approaches, mainly for government and defense communication security.

The European Union, through ENISA and Horizon Europe, is aligning PQC initiatives among member states by defining shared timelines, encouraging cross-border pilots, and publishing sector-based guidance. Cryptographic agility

to keep systems responsive as standards shift is given a high emphasis. Israel has emphasized financial and cyber-critical sector readiness for PQC through its National Cyber Directorate, while Italy, through its Agenzia per la Cybersicurezza Nazionale (ACN), is developing early-stage frameworks and research networks. Japan is implementing PQC throughout its tech value chains with government-industry-academia collaboration. Netherlands, the Dutch National Cyber Security Centre (NCSC) published guidelines advocating for the adoption of quantum-safe cryptography to ensure long-term confidentiality against potential quantum threats.

All these efforts are guided by NIST's standards, but each country adjusts the timing and rollout based on its own priorities, risks, and goals for digital independence. Table 3 presents a comparative summary of country-wise efforts in Post-Quantum Cryptography (PQC), including the algorithms under consideration, published guidance, and projected migration timelines.

The broad view on post-quantum cryptography migration is a mix of actions, all tending towards the need to protect digital wealth from looming quantum attacks. Some of the nations that have established clear timelines, released detailed guidance, and even selected national PQC sets of algorithms, in some cases, include the United States, the United Kingdom, Australia, and South Korea. Others, including Canada, the European Union, Germany, France, Japan, and the Netherlands, are actively working to align with NIST standards, creating their own recommendations, and making special priorities within specific sectors such as finance or critical infrastructure. While countries such as New Zealand, Singapore, Spain, Italy, and Israel may not have extensively publicized their strategies, they are actively advancing their readiness for the quantum era through focused initiatives within government departments and key sectors.

B. MULTILATERAL AND BILATERAL COOPERATION

1) MULTILATERAL PARTNERSHIPS

India, which is emerging as a technologically advanced country and has strategic global alliances, is a key influencer in defining the discourse and action for PQC. The country participates in different multilateral platforms to provide its inputs, share research collaborations, and advocate for PQC solution development.

The G20, a coalition of global leading economies, is also instrumental in influencing the global digital arena. Its emphasis on the digital economy and cybersecurity offers an important platform for solving PQC challenges. G20 efforts can help to create international standards, promote collaborative research and development efforts, and induce widespread PQC technology adoption among member states. India, being one of the prominent members of the G20, is an active member of its Digital Economy Working Group and contributes to the discussion and exchange of best practices on cybersecurity and digital infrastructure, which find direct application towards implementing PQC. During its participation in the G20 mechanism, India can push for views from its

side, engage with the other leading economies, and advance policies favorable to its national interests and world security concerns.

A strategic conversation between the United States, India, Japan, and Australia, on the Quadrilateral Security Dialogue (Quad) platform, also provides a critical means of PQC collaboration. With its emphasis on supporting a free, open, and secure Indo-Pacific region, the Quad appreciates the significance of emerging technologies and cybersecurity. PQC is complementary to these objectives because it is critical for ensuring the protection of sensitive information and vital infrastructure against potential threats of quantum computing [21].

India is a key member of the Quad, and its participation in the Quad’s working groups on emerging and critical technologies offers a basis for enabling collaborative research initiatives, sharing technology, and the establishment of shared security standards pertaining to PQC. India’s strategic engagement in the Quad allows it to work with its principal allies in developing and implementing PQC solutions that address the Indo-Pacific region’s unique security issues [24]. In addition to these particular platforms, India also actively participates in a wider array of global institutions and initiatives that have an important role to play in the global shift to PQC [25].

The “harvest now, decrypt later” threat requires a collective global action to safeguard sensitive information and avoid future security compromises. India is aware of this threat and actively promotes international cooperation to create and implement PQC solutions that can effectively counter it. Secondly, the creation and utilization of PQC requires a lot of resources and specialized knowledge. India, being endowed with a large number of skilled engineers and scientists, is in a good position to add weight to this endeavor. The country’s active engagement at multilateral platforms, its robust technology base, and strategic alliances position it as an important stakeholder in ensuring the future of quantum-safe cryptography [26].

2) BILATERAL PARTNERSHIP (INDO-UK)

The United Kingdom and India, while differing in technological maturity and regulatory frameworks, both prioritize cybersecurity as a national importance. The UK has a well-established cybersecurity ecosystem, spearheaded by the National Cyber Security Centre (NCSC), which provides robust guidance on securing critical infrastructure and leads proactive cyber threat intelligence initiatives. It also actively supports the transition to PQC through research funding and public-private collaboration, aligned with strategies outlined in its National Cyber Strategy.

India, on the other hand, is rapidly evolving its cybersecurity posture through initiatives such as the National Quantum Mission and Cyber Surakshit Bharat. India’s approach is more compliance-driven and capacity-building focused, with an increase in investments in indigenous cryptographic research and secure digital public infrastructure. However,

TABLE 4. Comparative cybersecurity aspects: UK and India.

Area	UK Focus	India Focus	Joint Policy Insight
Strategy	Clear cyber policies and planning	Fast growth and startup innovation	Build a joint cyber resilience roadmap
Regulation	Strong laws and reporting	Adapting rules for new tech	Align data and cyber laws for cooperation
Innovation	Research in AI and quantum security	Developing local cybersecurity tools	Launch joint R&D on post-quantum solutions
Skills	Advanced training programs	Expanding cybersecurity talent	Create shared training and exchange programs

while the UK exhibits a high degree of policy integration and readiness, India is still maturing in areas like post-quantum preparedness and standardized national guidance. In addition to their individual efforts, both countries have recognized the importance of collaboration in addressing emerging cyber threats. Bilateral partnerships, such as [27] and [28], to enhance information sharing and joint research on cybersecurity innovations. This collaboration strengthens both nations’ abilities to tackle common cybersecurity challenges, especially as the threat landscape evolves with the rise of quantum technologies.

Table 4 provides a comparative analysis of each country’s respective strengths, opportunities for mutual learning, and the potential policy impact arising from their collaboration. This comparison shows the shared interests and complementary strengths that both nations can leverage to strengthen their cybersecurity posture in the face of emerging threats, particularly in the context of Post-Quantum Cryptography (PQC) [29].

IV. PQC MIGRATION STRATEGIES AND READINESS

Transitioning to post-quantum cryptography requires a structured, multi-phase approach. This process must account for technical constraints, operational continuity, compliance obligations, and ecosystem coordination.

A. PROCESS OF BECOMING QUANTUM-SAFE

To implement the post-quantum transition effectively, organizations need a clear and structured procedure. Figure 1 illustrates a step-by-step process for organizations to transition toward a quantum-safe posture. It starts by allocating resources and raising awareness, where an in-house team is

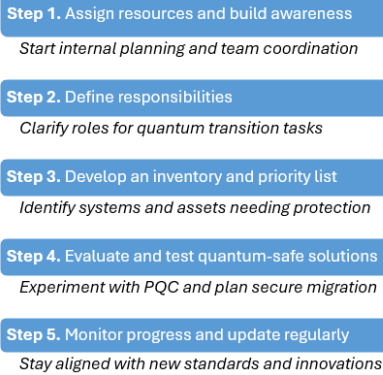


FIGURE 1. Steps for a quantum-safe organization.

established to oversee the journey towards quantum cybersecurity, including planning a budget and involving vendors. Step two is about defining responsibility and entails breaking down the process according to use cases to make it more feasible to accomplish. Third, organizations create an inventory and priority list by evaluating all systems, devices, and vendors on the basis of their security requirements, anticipated lifespans, and susceptibility to attacks.

The fourth step is to evaluate solutions, test, and experiment with quantum technologies such as PQC and QKD to protect assets and make future implementations. Finally, organizations will need to track progress, adapt policies, and work with industry experts to remain in line with continuing developments in quantum-safe computing.

B. KEY PILLARS FOR TRANSITIONING TO POST-QUANTUM CRYPTOGRAPHY

1) CRYPTOGRAPHIC INVENTORY AND RISK ASSESSMENT

Organizations must begin by conducting a comprehensive cryptographic inventory. This process identifies all instances where cryptographic algorithms are used within the applications, communication protocols, storage systems, and hardware modules. Each instance must be evaluated for algorithm type, key length, data sensitivity, and exposure window. Developing tools that automatically detect and inventory cryptographic assets within an organization is crucial. Such tools can identify where and how cryptographic algorithms are used, facilitating a more efficient and comprehensive migration to PQC.

2) HYBRID CRYPTOGRAPHY

Hybrid cryptographic schemes combine classical and post-quantum algorithms to maintain security under both threat models. For instance, a hybrid TLS (Transport Layer Security) handshake might include both an RSA key exchange and a Kyber-based KEM, ensuring that compromise of either alone does not jeopardize session confidentiality. Standards bodies, such as the Internet Engineering Task Force (IETF), have already begun defining such hybrid modes. Adopting hybrid cryptographic schemes that combine classical and post-quantum algorithms can provide

a transitional pathway to PQC. This approach ensures that if a post-quantum algorithm is later found to be vulnerable, the classical component still offers a layer of security. For instance, Apple's PQ3 protocol for iMessage integrates both elliptic curve cryptography and the Kyber algorithm, enhancing security against potential quantum threats [30].

3) TESTING, VALIDATION, AND INTEROPERABILITY

New cryptographic algorithms introduce variability in key sizes, message formats, and computational overhead. Organizations must therefore establish testbeds to evaluate PQC candidates under real-world conditions. Testing must include:

- Correctness under all supported use cases.
- Performance in constrained and high-load environments.
- Resistance to side-channel attacks and implementation flaws.
- Compatibility with communication protocols and certificate formats.

Interoperability testing is especially crucial for federated systems, where multiple vendors and agencies must align on supported cryptographic parameters.

4) DEPLOYMENT STRATEGIES AND LIFECYCLE MANAGEMENT

Deployment must be phased and context aware. Low-risk environments, such as internal tools or beta users, can serve as proving grounds for PQC. Critical infrastructure should be followed only after rigorous testing and auditing. Organizations must also plan for cryptographic lifecycle management. This includes procedures for key rotation, revocation, and secure disposal of deprecated algorithms. PQC introduces additional parameters, such as error correction and seed expansion, which must be handled with equal care.

5) TRAINING AND ORGANIZATIONAL AWARENESS

PQC deployment is not only a technical task. It requires training for developers, administrators, compliance officers, and procurement teams. Misconfiguration, poor key management, or insecure implementations can undermine even the most robust algorithm. Training programs should cover the rationale for migration, differences among algorithm families, and best practices for integration. Awareness initiatives must also engage executive leadership to ensure institutional support and strategic alignment.

V. CRYPTO-AGILITY

Crypto-agility gives organizations the ability to stay secure even as older encryption methods become outdated. It's about building systems that can quickly adapt to new cryptographic standards and threats, including those from quantum advances. To make this work, teams need clear visibility into where and how encryption is used across their systems and networks. Automation also plays a big role, making it

possible to update or swap out algorithms without causing disruptions.

Flexibility is key. Systems should be built to handle multiple algorithms and easily adopt new ones as standards evolve. The advantages are substantial: crypto-agility helps teams respond quickly to security incidents, makes future-proofing more realistic, and ensures business operations can continue smoothly, even if current encryption tools stop working.

To put crypto-agility into practice, organizations often need to modernize how they develop and manage cryptographic systems. That includes adopting service-based architecture and using cryptography-as-a-service platforms to handle key management and automate algorithm updates. This approach helps to ensure that the organization’s crypto infrastructure stays both secure and adaptable over time.

Once visibility is established, the next critical pillar is automation. Human intervention in key rollovers and the replacement of outdated algorithms introduces latency and increases the risk of errors. The infrastructure-as-code and cryptographic orchestration platforms should manage certificate lifecycles, key rotations, and rolling upgrades seamlessly and without any downtime. A SoK analysis reveals current trends in DevOps tooling and outlines best practices for embedding crypto-agility within Continuous Integration and Continuous Deployment (CI/CD) pipelines, enabling transitions from traditional to post-quantum algorithms in a matter of hours rather than months.

Adaptability, the third cornerstone, involves coding systems that work with multiple algorithms simultaneously. Plugin-like cryptographic building blocks, feature flags, or service-based constructs allow on-the-fly cipher switching without intrusive code rewrites. From a SoK point of view, contrasting architectures ranging from monolithic libraries to micro-services and cryptography-as-a-service solutions reveal trade-offs in latency, key management complexity, and resilience. Organizations must balance these factors to select a model that is both performance-oriented and agile enough to implement new PQC schemes as standards from organizations such as NIST solidify.

Table 5 illustrates the relationship between cryptographic configurations and the overall security of the application infrastructure. It highlights how elements such as Public Key Infrastructure (PKI), encryption algorithms, and policy frameworks serve as the foundation of a secure system, ensuring that well-configured cryptographic settings strengthen resilience, while misconfigurations increase vulnerability to threats [31].

Strong configurations defend against security attacks, while crypto modifications, when weakly configured, might lead to issues exposing the system to possible intrusion. Crypto-agility is the foundation of any successful post-quantum cryptography (PQC) transition. Organizations that are not agile will be at risk of being overwhelmed by gigantic problems when quantum threats become reality. Without agile architecture, they might be compelled to recreate the entire system, which is a costly and risky step.

TABLE 5. Crypto agility framework.

Layer	Role / Function	Risk & Mitigation
Security Threat	Attempts to exploit system or crypto weaknesses.	<i>Risk:</i> Breach of data integrity and confidentiality. <i>Mitigation:</i> Continuous monitoring and threat intelligence.
Application Infrastructure	Hosts business logic and user data.	<i>Risk:</i> Vulnerabilities in the app or cloud stack. <i>Mitigation:</i> Regular patching, secure coding, and encryption.
Crypto Layer (PKI, Algorithm, Policy)	Manages keys, encryption algorithms, and access rules.	<i>Risk:</i> Outdated or weak cryptography. <i>Mitigation:</i> Adopt PQC (Post-Quantum Cryptography) and strong policies.
Secure Config	Proper setup ensuring encryption and compliance.	<i>Risk:</i> Misconfiguration or unauthorized change. <i>Mitigation:</i> Enforce configuration baselines and audits.
Crypto Changes	Updates or transitions in crypto algorithms/policies.	<i>Risk:</i> Transition errors causing exposure. <i>Mitigation:</i> Controlled rollout with testing and rollback plan.

In contrast, a crypto-agile system is architecturally designed to enable effortless substitution of cryptographic algorithms, making it possible for teams to incorporate PQC primitives without dismantling their current infrastructure.

One of the main advantages of an agile system is the possibility of incremental and low-risk testing. Instead of trying a “big-bang” migration that tends to break integrations and compromise user experiences, teams can spin up independent environments in which new PQC algorithms are tested, performance metrics gathered, and security properties checked. When enough confidence is achieved, the same changes can be deployed incrementally with minimal

disruption and instant rollback in the event of unexpected problems. The organization needs to stay aligned with evolving standards to ensure continued compliance and security. As organizations such as NIST move through the PQC standardization process, they can change algorithm parameters or even choose alternative candidates. Crypto-agility is sustained long-term resilience. Upcoming quantum or classical advances will again require cryptographic refreshes by necessity. Beyond protecting sensitive information, this response preserves operational continuity. Businesses maintain the ability to ensure compliance and trust during even quick transformations in the market.

In conclusion, achieving crypto-agility requires a structured, phased approach focusing on visibility, automation, adaptability, and standard alignment. Crypto-agility plays a pivotal role in establishing a resilient foundation for a smooth and secure transition to post-quantum cryptography. Organizations that adopt this proactive and systematic strategy will be prepared for the next quantum era without compromising compliance, performance, or security.

VI. PQC READINESS: AN INDUSTRY ASSESSMENT

The development of quantum computing poses a fundamental challenge to contemporary security infrastructure. This comprehensive survey investigates the current state of industry readiness for this post-quantum era through a dedicated survey, especially focused on the Indian Context.

This survey analysis highlights key areas of concern and potential for PQC transition while examining organizational understanding, strategic planning, and the implementation of quantum-resistant technologies. The analysis provides valuable insights into the preparedness landscape and shows the critical need for proactive engagement to secure the digital future.

A. ABOUT THE SURVEY

The survey, titled “Post-Quantum Cybersecurity: Assessing Industry Readiness, was designed with 20 analytical questions to evaluate the awareness, strategic prioritization, and technical preparedness of organizations in light of emerging quantum computing threats. With quantum computing likely to make many traditional cryptographic systems outdated, it’s becoming more important to assess how ready industries are, especially in light of India’s changing digital and regulatory environment. To ensure relevance and depth, the survey was shared through a curated post targeting cybersecurity professionals, technology executives, and risk management leaders across industries. LinkedIn’s organic reach among C-level and senior management professionals in India ensured that the survey gained visibility among the right decision-makers. Personalized invitations were also sent to a selected group of industry leaders, CISOs, CTOs, compliance heads, and policy stakeholders. The organizations who participated including their primary sector and geographic regions are displayed in Figure 2. These contacts were identified through prior professional engagements and industry collaborations, ensuring

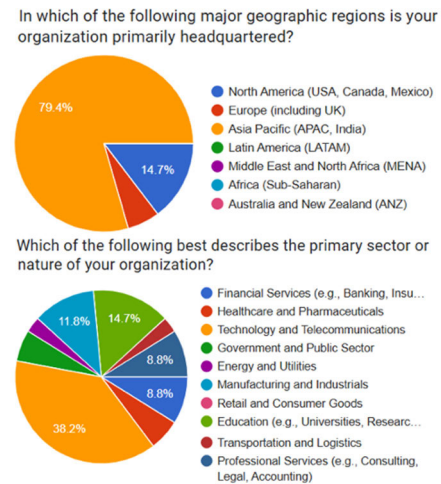


FIGURE 2. Organizations participated in the survey.

that feedback was captured from individuals with operational or strategic authority over cybersecurity initiatives. In total, 64 survey responses were recorded, of which 51 were validated based on completeness, respondent profile, and organizational role. These validated responses formed the basis of the analysis presented in this paper. Each participant was clearly informed that the survey was conducted strictly for educational and research purposes, and no personal information was collected.

The survey aimed to provide a snapshot of organizational preparedness for quantum-era cybersecurity challenges, with the following key objectives:

- To assess executive-level awareness and prioritization of quantum-related cybersecurity risks.
- To evaluate the extent of formal assessment, planning, and implementation of post-quantum cryptographic strategies.
- To understand the allocation of resources, financial, technical, and human, toward post-quantum preparedness.
- To benchmark readiness across sectors and organization types, especially within the Indian context, while performing global comparisons where relevant.
- To promote strategic dialogue and action around quantum-safe cryptography, risk governance, and regulatory implications.

By analyzing responses from verified decision-makers and technology leads, the analysis aims to act as both a diagnostic tool and a call to action, highlighting areas of strength, exposing critical gaps, and encouraging early and sustained investment in quantum-resilient cybersecurity infrastructure.

The following methodology presents the framework and validation protocols used to assess organizational readiness for the transition to Post-Quantum Cryptography (PQC):

- **Instrument Design & Construct Validity:** The presented research used a structured 20 questions survey to measure three major concerns: Cognitive Awareness (perception of threat and future projections), State-

gic Prioritization (mapping resource allocation against multiple mandates), and Technical Maturity (system compatibility and acceptance of quantum-proof models).

- **Validation & Bias Minimization:** The survey was professionally pre-piloted among a pool of subject matter experts to validate semantic accuracy while eliminating instrument bias using NIST PQC-approved terminology standards to synchronize all technical naming convention to exclude ambiguity.
- **Sampling & Data Integrity:** This presented study used purposive non-probability sampling, focusing on a high-fidelity strategic stakeholder sample, CISOs, and Security Architects. Data integrity was ensured through a multi-tier validation process, removing responses with missing data, as well as a threshold of professionalism, excluding non-Professional responses.
- **Methodological Limitations:** In order to provide scientific integrity, it is admitted that there may be a ceiling effect and a self-selection bias in favor of well-funded and involvement-rich organizations. Accordingly, the data is framed not as an industry average but as a Leading-Edge Benchmark that shows where the strategic leaders of an industry are presently positioned.

B. ANALYSIS

This analysis synthesizes findings from a comprehensive survey of organizations across various sectors and regions regarding their post-quantum cybersecurity (PQC) readiness. The data reveals significant strategic gaps despite growing quantum computing threats, with organizational maturity levels varying widely across respondents.

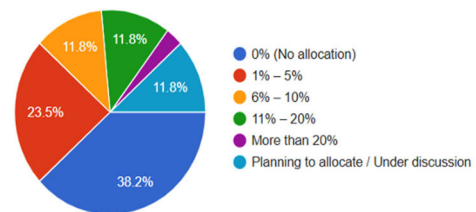
1) STRATEGIC POSTURE ANALYSIS

The analysis identifies a concerning bifurcation in organizational approaches to post-quantum cybersecurity. A substantial 45% of organizations categorize PQC as “not currently a significant priority,” creating significant vulnerability windows as quantum computing capabilities advance. In contrast, only a select cohort (24%) has elevated PQC to “high priority” or “critical/urgent” status within their risk management frameworks. This strategic misalignment is further evidenced by budget allocation patterns, where 34% allocate zero resources to PQC initiatives, indicating fundamental disconnects between emerging threat vectors and resource allocation decisions as shown in Figure 3.

2) TECHNICAL INFRASTRUCTURE ASSESSMENT

Respondent data reveals a critical divide between theoretical capability and practical implementation. A majority of organizations report infrastructure theoretically capable of integrating post-quantum protocols with “minor enhancements,” suggesting technical feasibility. However, execution lags severely behind this capability, with 73% of organizations reporting incomplete or non-existent cryp-

What percentage of your organization's budget is currently allocated to post-quantum cybersecurity preparedness activities?



As a senior executive, how high a strategic priority is preparing for quantum-related cybersecurity risks within your organization's broader risk management strategy?



How does your organization's cybersecurity budget allocation compare to industry peers and current market trends related to quantum preparedness?

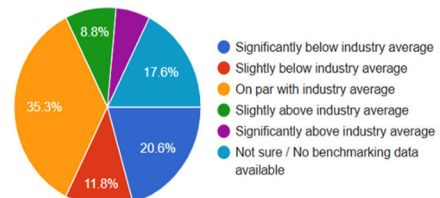


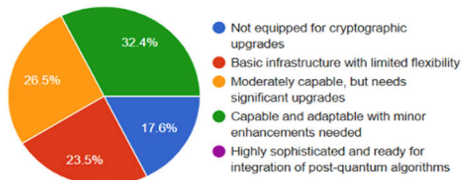
FIGURE 3. Strategic posture analysis.

tographic asset inventories, 69% lacking formal transition plans, and 62% conducting insufficient risk assessments. This capability-implementation gap creates security vulnerabilities even among organizations with adequate technical resources. The survey data also indicates the concerning levels of quantum vulnerability within existing cryptographic implementations. Approximately 14% of organizations report that 76-100% of their cryptographic algorithms are vulnerable to quantum attacks, while only 7% claim full quantum-safety across their cryptographic portfolio. This is identified based on the responses displayed in Figure 4. A particularly concerning aspect is that critical sectors, including financial services and government entities, report substantial exposure, potentially threatening essential infrastructure and services when quantum computing reaches its practical crypt-analysis capabilities.

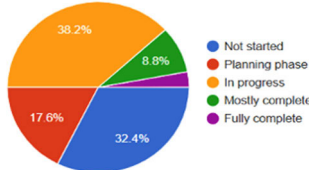
3) ECONOMIC BARRIER ANALYSIS

A significant correlation exists between perceived implementation costs and actual PQC budget allocation across surveyed organizations. This statistical relationship indicates a critical psychological barrier within organizational decision-making processes: entities anticipating higher costs tend to allocate disproportionately less budget, creating a self-reinforcing cycle of inaction. This pattern suggests that cost perception,

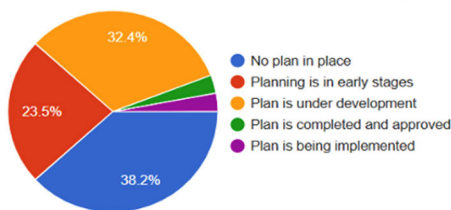
How capable is your organization's current technology infrastructure in integrating and managing post-quantum cryptographic protocols?



What is the current status of your organization's systematic assessment and inventory of cryptographic assets, including keys and certificates, that are susceptible to quantum-based attacks?



Does your organization have a documented plan for transitioning to post-quantum cryptographic algorithms?



Has your organization ever evaluated its risk assessment specifically to address potential quantum computing threats?

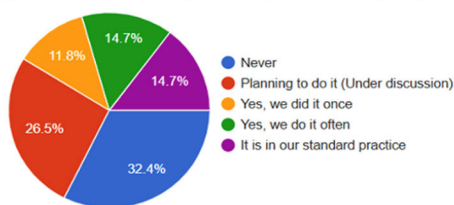


FIGURE 4. Technical infrastructure assessment.

rather than actual implementation requirements, may be the dominant factor suppressing investment in post-quantum security measures, even among organizations with adequate resources and awareness of the threat landscape.

4) BEHAVIORAL/AWARENESS MATURITY SEGMENTATION

Based on the responses (Figure 5 and 6), the organizations fall into three distinct maturity segments regarding their post-quantum preparedness. The largest segment, comprising 41% of respondents, demonstrates minimal readiness with no formal risk assessment procedures, absence of executive awareness, zero budget allocation, and no training initiatives related to quantum threats.

The second segment (38%) exhibits moderate awareness characterized by limited risk assessment completion, some executive awareness, modest budget allocation (1-5%), and general cybersecurity training without quantum specificity. Only the third segment (21%) demonstrates proactive preparation with comprehensive risk assessment practices, strong

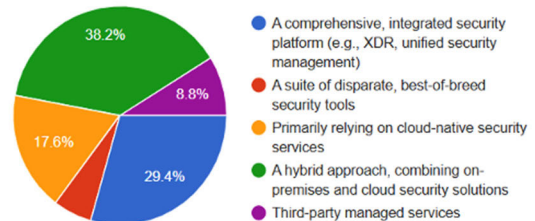
What is the level of executive-level awareness and support for post-quantum cybersecurity initiatives within your organization?



To what extent does your organization actively enables cybersecurity awareness and training among employees, with specific focus on probable quantum-related threats?



What is the primary security platform that currently is the foundation to your organization's cybersecurity defense architecture?



Considering the resource demands of post-quantum cybersecurity solutions, how significant is your organization's focus on optimizing the energy efficiency and reducing the carbon footprint of its cybersecurity infrastructure?

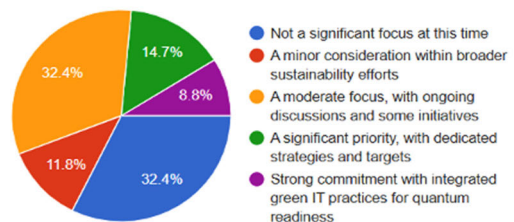


FIGURE 5. Behavioral/awareness maturity segmentation.

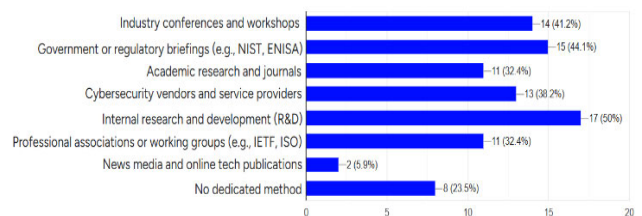


FIGURE 6. Methods of gathering information.

executive support, substantial budget allocation exceeding 5%, and specific quantum threat training programs.

5) SUSTAINABILITY CONSIDERATIONS

Despite growing regulatory pressures around digital infrastructure sustainability, 38% of surveyed organizations

TABLE 6. Comparison of PQC algorithms.

Algorithm	Type / Problem	Public Key Size	Signature / Ciphertext Size	Performance (Speed)
Kyber (ML-KEM) [32]	Lattice (Module-LWE)	800 – 1,568 bytes	768 – 1,568 bytes	Very High: Faster than classical ECDH in some cases.
Dilithium (ML-DSA) [33]	Lattice (Module-LWE/SIS)	1,312 – 2,592 bytes	2,420 – 4,627 bytes	High: Signing and verification are very efficient on modern CPUs.
Falcon [34]	Lattice (NTRU)	897 – 1,793 bytes	656 – 1,280 bytes	High: Extremely fast verification; signing is efficient but complex.
SPHINCS + (SLH-DSA) [35]	Stateless Hash-based	32 – 64 bytes	7,856 – 49,856 bytes	Low (Signing): Computationally intensive, requiring millions of hash calls.
Classic McEliece [36]	Code-based (Goppa)	261 KB – 1.3 MB	96 – 208 bytes	Fast Encryption but very slow key generation.

explicitly deprioritize energy efficiency in their cybersecurity infrastructure planning. Moreover, a moderate correlation between implementation costs and sustainability focus suggests many organizations view sustainability as a “premium” feature rather than an integral consideration in security architecture. This approach creates potential compliance and operational efficiency challenges as regulatory frameworks increasingly incorporate environmental impact requirements for digital infrastructure.

6) STRATEGIC IMPLICATIONS & RECOMMENDATIONS

The survey data presents a concerning picture of organizational readiness for post-quantum threats across multiple dimensions. Despite technical feasibility in many cases, organizational, budgetary, and awareness barriers are creating dangerous security gaps that could expose critical systems once quantum computing capabilities reach the threshold where traditional cryptographic protections become obsolete. Organizations must take immediate steps to address these gaps through structured, incremental approaches that combine technical assessment, strategic prioritization, and operational integration of post-quantum security measures.

For executive leadership, the analysis suggests three priority actions.

- Risk Frame Re-calibration, which explicitly includes quantum threats in enterprise risk frameworks with designated ownership and accountability.
- Budget Realignment using incremental, phased funding approaches to overcome psychological cost barriers.

- Targeted Executive Education focuses on the impact of business continuity rather than technical specifications to increase engagement and priority.

Cybersecurity functions should focus on immediate cryptographic census to inventory quantum-vulnerable assets, infrastructure readiness assessment to validate claimed adaptability through concrete testing, and training enhancement that integrates quantum-specific modules into existing security awareness programs. These tactical measures can significantly improve preparedness without requiring comprehensive strategic reorientation.

Technology architecture teams should prioritize cryptography planning with transition frameworks prioritizing critical systems, hybrid implementation approaches deploying quantum-safe algorithms alongside classical cryptography during transition periods, and sustainability integration that incorporates energy efficiency considerations during infrastructure upgrades. This balanced approach addresses both immediate security concerns and longer-term operational requirements.

VII. TECHNICAL COMPARISON OF LEADING PQC ALGORITHMS

Table 6 provides the comparison between leading Post-Quantum Cryptography (PQC) algorithms, their mathematical foundations, key sizes, and performance.

- **Lattice-Based Dominance:** Kyber and Dilithium have emerged as the front-runners for general adoption due to their “favoured balance” of security and computational efficiency. They outperform classical RSA in key exchange speeds and are competitive with ECC on modern hardware.
- **The Bandwidth-Latency Gap:** A significant trade-off in PQC is data usage versus processing time. For instance, algorithms like BIKE (code-based) may require more transmission bytes but less CPU time than alternatives like SIKE (isogeny-based, now broken), which utilised small keys but high processing power.
- **Hardware and Constrained Devices:** While PQC is practical on desktops, it poses challenges for IoT and embedded systems. On Raspberry Pi 4, PQC operations can be 45-50 times slower than on a modern PC. Lattice schemes are generally the most feasible for these devices, while SPHINCS + signing and McEliece key storage often exceed the resource budgets of low-power wearables.
- **Implementation Complexity:** Falcon provides smaller signatures than Dilithium, but its reliance on double-precision floating-point arithmetic makes it harder to implement consistently across platforms without introducing side-channel vulnerabilities.
- **Migration Strategy (Hybrid Approach):** Because PQC algorithms rest on newer, less time-tested mathematical assumptions than classical RSA/ECC, many institutions recommend hybrid deployments. This

involves combining a classical algorithm (like X25519) with a post-quantum one (like Kyber) to ensure the connection remains secure even if the PQC component is found to have a weakness later.

Nature-Inspired Cyber Security (NICS) can ensure that cryptographic infrastructures remain future-proof by allowing for the proactive substitution of primitives, such as hash functions or lattices, enabling a system to ‘evolve’ its defenses as new vulnerabilities or quantum algorithms are discovered. By prioritizing interoperability and strategic migration, nature-inspired principles facilitate a trusted end-to-end ecosystem that secures sensitive communications against the retrospective decryption risks inherent in the quantum era. Integrating nature-inspired principles into a post-quantum strategy is like building a futuristic digital immune system.

VIII. ADAPTIVE CYBER DEFENSE: NATURE-INSPIRED CYBERSECURITY

Nature-Inspired Cybersecurity (NICS) is gaining traction as a powerful paradigm in addressing the challenges of Post-Quantum Cryptography (PQC). NICS leverages mechanisms observed in nature such as evolution, neural adaptation, immune responses, and swarm intelligence to develop adaptive, resilient, and self-optimizing cybersecurity systems. In PQC, NICS algorithms help to understand and balance the complex trade-offs between security strength, computational performance, and resource efficiency by optimizing algorithm parameters, enhancing cryptanalysis, and supporting system migration. For example, Genetic Algorithms (GAs) simulate natural selection to fine-tune PQC parameters like key size or error tolerance in lattice- or code-based schemes, achieving robust configurations against both classical and quantum attacks. Similarly, Particle Swarm Optimization (PSO) enables efficient searching of parameter spaces by simulating social behavior in swarms, providing faster convergence to optimal settings in hash-based and signature schemes.

The decentralized and adaptive features of NICS also provide unique value during organizational migration to PQC. Algorithms modeled after swarm intelligence like Ant Colony Optimization or Artificial Bee Colony can assist in network anomaly detection and resource allocation during transitions. These algorithms mimic the coordinated behavior of biological collectives to help manage the complex logistics of PQC rollout across systems, ensuring minimal disruption and maximum resilience. Moreover, the self-learning and continuous adaptation embedded in many NICS techniques provide the basis for long-term, evolving defenses that can respond to unforeseen vulnerabilities as both classical and quantum threats evolve.

A. COMPLEMENTARY TECHNOLOGIES

Except for NICS, other technological approaches also play key roles in PQC’s development. Quantum Genetic Algo-

rithms (QGAs) and Quantum Neural Networks (QNNs) combine nature-inspired principles with quantum computing capabilities, improving speed and efficiency in PQC-related tasks such as circuit design, cryptanalysis, and parameter tuning. Neural networks assist in side-channel analysis, message decoding, and quantum key distribution (QKD) optimization. Swarm intelligence supports anomaly detection and key management during migration. These technologies, while not nature-inspired in origin, complement NICS by expanding the analytical and operational toolkit available to secure PQC systems. Together, they form an ecosystem where adaptability, speed, and resilience define the future of quantum-safe cryptography [37], [38].

From these synergistic technologies, also emerging as a center pillar in post-quantum defense strategy is the broader paradigm of Nature-Inspired Cyber Security (NICS). NICS models mimic biological functions such as neural plasticity, genetic adaptability, ecological balance, and immune responsiveness to create cyber systems that are not just secure but also adaptive, decentralized, and learn from evolving threats. For instance, bio-inspired cryptographic frameworks can adapt parameters or rotations of keys in response to feedback from the environment, just like living things adapt to stimuli to survive. Artificial Immune Systems (AIS) can be trained to detect quantum communication channel anomalies as a backup line of defense in conjunction with cryptographic hardness. In the quantum-secure system domain, eco-systemic models driven by predator-prey dynamics or symbiosis can be employed to inform risk modeling and threat intelligence. Such models depict adversarial action and co-evolution, providing real-time forecasts of how quantum-capable adversaries will co-evolve and how defenses must respond in kind. Also, stigmergic communication, borrowed from swarm biology, is being applied to decentralized cryptographic key exchanges and group decision-making protocols now, which have special relevance in multi-agent quantum networks.

By integrating these principles, multi-layered, self-organizing security architectures are made robust and resilient for the future. Unlike classical security solutions that are rigid and signature-oriented, NICS-powered solutions stand out because of diversity, redundancy, and real-time learning principles that are increasingly critical in the unpredictable environment of quantum threat scenarios. As scientific progress unfolds, the convergence of NICS, quantum machine learning, and optimization technology is anticipated to develop autonomous cryptographic ecosystems capable of dynamically and actively shifting their security posture on many different threat scenarios.

B. ON-GOING RESEARCH

Ongoing research in Nature-Inspired Cyber Security (NICS) is focused on seeking novel means of enhancing cyber defense mechanisms by emulating natural systems and processes. This interdisciplinary field works to develop more

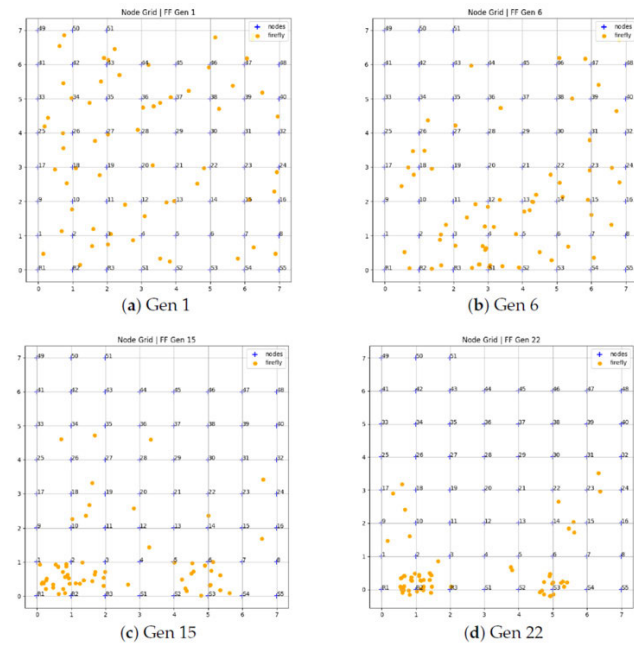


FIGURE 7. Firefly algorithm analyzing malicious nodes using NICS [39].

resilient, adaptive, and intelligent security solutions that can resist increasingly advanced cyberattacks. Current research is working on the use of nature-inspired algorithms and paradigms to address various cybersecurity issues, including intrusion detection, threat reduction, and building secure network infrastructures.

Researchers are also analyzing the effectiveness of certain nature-inspired algorithms for real-world applications in cybersecurity. As an example, researchers are showing the potential of meta-heuristic optimization algorithms such as the Artificial Bees Colony (ABC) in providing adaptive defense strategies, especially in cases of denial-of-service attacks by optimizing network traffic patterns and malicious node detection [40], [41] as shown in Figures 9 and 10. Methods like the Modified Firefly Optimization Algorithm are being investigated to enhance the Intrusion Detection System [39], as shown in Figures 7 and 8.

Also, the more generic idea of NICS involves instilling adaptive and resilient security technologies inherently robust against malicious behaviors, regardless of whether it is under noisy or uncertain circumstances. This applies nature-inspired security strategies like camouflage, deception, and disguise towards developing robust cybersecurity defenses [42]. Current research in this domain emphasizes a paradigm shift towards security methods that are more capable of duplicating the agility and robustness seen in nature-based ecosystems in order to generate more effective defenses against constantly evolving cyber threats.

Nature-inspired cybersecurity (NICS) imports the adaptive, self-organizing power of biological systems into the world of digital protection and is well-suited to enhance post-quantum cryptography (PQC) by adding resilience and flexibility where inflexible, purely mathematical approaches

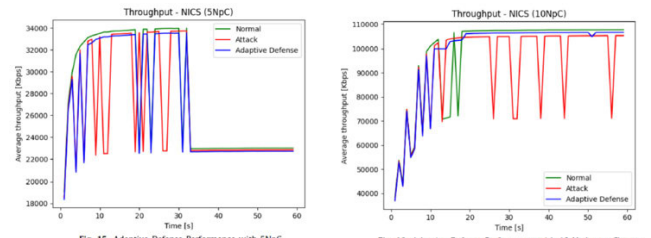


FIGURE 8. Throughput computation under attack using NICS [43].

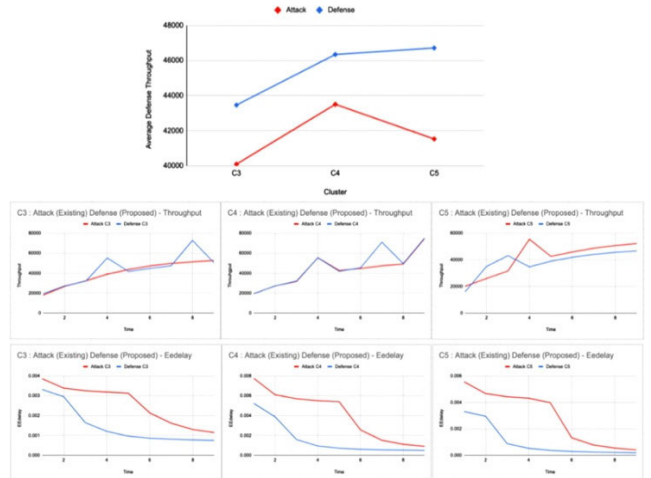


FIGURE 9. Throughput and End-to-End Delay difference on the application of NICS algorithm on an attack scenario [35].

can be undermined by quantum-age threats. Fundamentally, NICS exploits algorithms inspired by collective behavior like swarming insects or bioluminescent creatures to continuously test and harden cryptographic processes against both classical and quantum attackers. By integrating these dynamic, feedback-based methods into PQC protocols, defenders acquire an active defense layer that can quickly detect vulnerabilities, dynamically reconfigure cryptographic parameters in real time, and assign security tasks to a self-healing network, all of which are essential in an environment where quantum computing capabilities change unpredictably.

One of the most promising nature-inspired approaches is the Firefly Algorithm, which emulates how fireflies coordinate their bioluminescent flashes to find mates. In a cybersecurity setting, each “firefly” can be a candidate security setting, e.g., a specific selection of lattice parameters or signature variant in a PQC suite. By iterative communication (similar to light pulses), settings that exhibit lower estimated vulnerability produce more intense “flashes,” guiding the search process toward more secure settings. Translated to PQC, this implies that key-generation procedures can self-tune: in simulated or actual-time threat feedback, they settle on parameter values that optimize security margins against both classical attacks and projected quantum tactics. The outcome is a constantly tightened-up cryptographic stance that pre-emptively mitigates new quantum-fueled exploits before countermeasures are developed to target them.

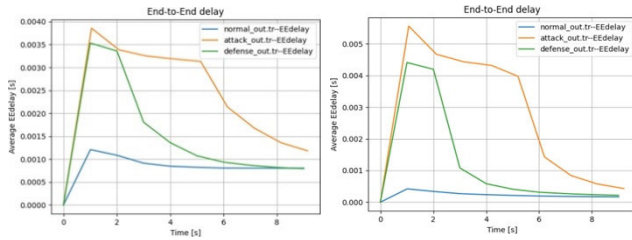


FIGURE 10. End-to-End delay computation under attack using NICS [41].

C. INTEGRATED FRAMEWORKS AND CASE STUDIES IN NICS - PQC

While NICS provides a conceptual foundation, recent research has shifted toward architectural models that address the specific implementation hurdles of Post-Quantum Cryptography (PQC). The following case studies illustrate the utility and technical integration of NICS within the PQC lifecycle.

1) THE BIOCRYPT QUANTUM SHIELD (BQS) FRAMEWORK

One of the most effective integrations is the BioCrypt Quantum Shield (BQS) system. This framework uses nature-inspired machine learning to manage the performance trade-offs of PQC algorithms. Unlike static security models, BQS treats system defense as an adaptive biological system. By using meta-heuristic optimization, BQS dynamically adjusts its cryptographic settings. Research conducted in 2024 showed that applying these NICS-based algorithms to PQC systems significantly improved security, raising “Quantum Resistance Level” scores from 5,000 to over 18,000 [44], [45].

2) TUNING OF PARAMETERS THROUGH GENETIC ALGORITHMS

Lattice-based cryptosystems, such as CRYSTALS-Kyber, rely on complex parameters like lattice dimensions and error distributions. Finding the ‘sweet spot’ for these settings is a difficult optimization problem. Studies from 2024–2025 have integrated Genetic Algorithms (GAs) to automate the discovery of optimal keys. By mimicking natural selection, these GAs identify solutions near the mathematical optimum in 15% fewer generations than traditional methods. This ensures that PQC tools are secure and efficient enough for resource-constrained IoT devices [46].

3) QUANTUM-BEHAVED PARTICLE SWARM OPTIMIZATION ALGORITHM IN NETWORK SECURITY

Migrating to PQC is a challenge for decentralized systems like Wireless Sensor Networks (WSNs). The Quantum-Enhanced Nature-Inspired Routing Algorithm (QENI-RA), proposed in late 2025, uses a Quantum-Behaved Particle Swarm Optimization (QPSO) mechanism. This swarm-based approach allows for dynamic clustering and manages the high computational costs of PQC. By imitating the collective behavior of biological swarms, it ensures both energy efficiency and data confidentiality. It achieves this through

layers based on Bennett-Brassard 1984 (BB84) Quantum Key Distribution and Kyber [47].

4) ARTIFICIAL IMMUNE SYSTEMS FOR SIDE CHANNEL PROTECTION

PQC algorithms are sensitive to side-channel attacks (SCA), such as power analysis during lattice operations. To protect against these leaks, researchers use frameworks that simulate Artificial Immune Systems (AIS). Just as human immune cells distinguish between “self” and “non-self,” an AIS-based countermeasure monitors the system’s “emission profile.” If a “pathogen” (an active SCA) is detected, the system triggers a “mutation” of the PQC masking parameters. This prevents the attacker from identifying the secret key [48].

In the post-quantum era, Nature-Inspired Cyber Security (NICS) focused on dynamic, self-organizing processes found in nature, so that the cryptographic systems can better adapt to quantum attacks. These techniques that range from Genetic Algorithm optimization to swarm-based routing demonstrate that NICS would be a key part of modern defense strategies.

IX. CONCLUSION

As quantum computing moves from theoretical concept to practical application, a strong response to the fundamental cryptographic risks posed by this technology is needed. The “harvest now, decrypt later” threat and the capability of Shor’s algorithm to render existing standards of encryption obsolete make it critical that the transition to quantum-resilient systems must proceed proactively. The study shows that integrating post-quantum cryptography will have to go beyond mere technical implementation and become a prime priority of national strategic policy, striking a fine balance between technological innovation and digital sovereignty. As per the findings of presented Industry Readiness Assessment Survey, it is clear that even as awareness grows, much remains to be done in terms of getting the technical infrastructure in place, besides enhancing cryptographic agility. The readiness of India needs to be strengthened by three major pillars: cryptographic flexibility, institutional capacity building, and indigenous innovation. National systems, including the Unified Payments Interface and the Aadhaar biometric identity program, would need to have sufficient support and guidance from the National Quantum Mission to achieve self-sufficiency. In conclusion, a national approach to be enabled with international collaboration and the creation of country-specific standards, is needed to secure the digital future. Future efforts are needed toward the deployment of hybrid classical-quantum cryptographic schemes in order to have seamless migration and ensure the confidentiality of sensitive information in the post-quantum era.

ACKNOWLEDGMENT

The authors would like to thank the Chevening Cyber Security Fellowship, in 2025, supported by U.K. Foreign,

Commonwealth and Development Office (FCDO), for the mentorship and resources provided during the development of this research.

REFERENCES

- [1] Palo Alto Networks. *What is Post-Quantum Cryptography (PQC)*. [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc>
- [2] SafeLogic. *National Cybersecurity Strategy Calls for Post-Quantum Cryptography Preparation*. [Online]. Available: <https://www.safelogic.com/blog/national-cybersecurity-strategy-calls-for-migration-to-post-quantum-cryptography>
- [3] NIST. *Post-Quantum Cryptography* [CSRC-NIST Computer Security Resource Center]. [Online]. Available: <https://csrc.nist.gov/projects/post-quantum-cryptography>
- [4] (2025). *Computing Research Association. 2024–2025 CRA Quad Paper: The Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead*. [Online]. Available: https://cra.org/wp-content/uploads/2025/01/2024-2025-CRA-Quad-Paper_The-Post-Quantum-Cryptography-Transition_Making-Progress-But-Still-a-Long-Road-Ahead.pdf
- [5] (2025). *The Quantum Insider. NIST Outlines Strategies for Crypto Agility as PQC Migration Stalls, Available for Public Comment*. [Online]. Available: <https://thequantuminsider.com/2025/03/07/nist-outlines-strategies-for-crypto-agility-as-pqc-migration-stalls-available-for-public-comment/>
- [6] University of Toronto. *What is Post-Quantum Cryptography?* [Fields Institute for Research in Mathematical Sciences]. [Online]. Available: <https://www.fields.utoronto.ca/news/What-Post-Quantum-Cryptography>
- [7] E. Barker. (2017). *Recommendation for Key Management: Part 1-General (NIST SP 800-57 Part 1 Revision 5)*. [Online]. Available: <https://tomorrowdesk.com/breakthrough/ibm-quantum-computing-4000-qubit>
- [8] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, May 1994, pp. 124–134. [Online]. Available: <https://tomorrowdesk.com/breakthrough/ibm-quantum-computing-4000-qubit>
- [9] Google Willow Quantum Chip. [Online]. Available: <https://blog.google/technology/research/google-willow-quantum-chip/>
- [10] IBM. *127-Qubit Quantum Processor Eagle*. [Online]. Available: <https://www.ibm.com/quantum/blog/127-qubit-quantum-processor-eagle>
- [11] Rigetti Computing. *Rigetti Computing Launches 84-Qubit Ankaa-3 System*. [Online]. Available: <https://investors.rigetti.com/news-releases/news-release-details/rigetti-computing-launches-84-qubit-ankaatm-3-system-achieves>
- [12] M. Mosca, "Quantum threat timeline," 2018, *arXiv:1804.00827*.
- [13] SlideTeam. *Quantum Threat Timeline—Quantum Risk Analysis and Data*. [Online]. Available: <https://www.slideteam.net/quantum-threat-timeline-quantum-risk-analysis-and-data-ppt-sample.html>
- [14] D. Aggarwal, A. Joux, A. Prakash, and M. Santha, "Quantum cryptanalysis of hash-based signatures," in *Advances in Cryptology—EUROCRYPT 2018*. Cham, Switzerland: Springer, 2018, pp. 465–497. [Online]. Available: <https://tomorrowdesk.com/breakthrough/ibm-quantum-computing-4000-qubit>
- [15] Identity Management Institute. *Quantum Threats To Identity and Access Management*. [Online]. Available: <https://identitymanagementinstitute.org/quantum-threats-to-identity-and-access-management/>
- [16] Medium. *Isogenies: The End Game for Public Key Encryption?*. [Online]. Available: <https://medium.com/asecuritysite-when-bob-met-alice/isogenies-the-end-game-for-public-key-encryption-14dbe4475eb1>
- [17] GSMA. *Post-Quantum Government Initiatives By Country and Region*. [Online]. Available: <https://www.gsma.com/newsroom/wp-content/uploads/Post-Quantum-Government-Initiatives-by-Country-and-Region-02-Mar-2025-Clean.pdf>
- [18] PwC. *Quantum Computing Cybersecurity Risk*. [Online]. Available: <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/quantum-computing-cybersecurity-risk.html>
- [19] Palo Alto Networks. *What is Quantum Computing's Threat to Cybersecurity?*. [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity>
- [20] AWS. *AWS Post-Quantum Cryptography*. [Online]. Available: <https://aws.amazon.com/security/post-quantum-cryptography/>
- [21] PSA. *QUIN Quantum CoE Report*. [Online]. Available: https://psa.gov.in/CMS/web/sites/default/files/psa_custom_files/QUIN_Quantum_CoE_Report_Final.pdf
- [22] The Quantum Insider. (2025). *China Launches Its Own Quantum Resistant Encryption Standard, Bypassing U.S. Efforts*. [Online]. Available: <https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard-bypassing-us-efforts/>
- [23] CAS. *Beijing-Shanghai Quantum Communication Network Put Into Use*. [Online]. Available: https://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml
- [24] Ministry of External Affairs. *QUAD Fact Sheet*. [Online]. Available: https://www.mea.gov.in/Portal/ForeignRelation/Unclassified_Quad_Brief_Feb_2025.pdf
- [25] PostQuantum. *India's Quantum Computing and Quantum Technology Initiatives*. [Online]. Available: <https://postquantum.com/quantum-computing/quantum-india/>
- [26] Sectigo. *Harvest Now. Decrypt Later Attacks: How They Relate To the Quantum Threat*. [Online]. Available: <https://www.sectigo.com/resource-library/harvest-now-decrypt-later-quantum-threat>
- [27] U.K. Government. *Framework for the U.K.-India Cyber Relationship*. [Online]. Available: https://assets.publishing.service.gov.uk/media/5f479d338fa8f53634f02624/Framework_for_the_UK-India_Cyber_Relationship_FINAL_for_upload_2020.odt
- [28] Chevening. *Chevening India Cyber Security Fellowship*. [Online]. Available: <https://www.chevening.org/fellowship/india-cyber-security/>
- [29] U.K. Government. (2022). *India-U.K. Cyber Statement*. [Online]. Available: <https://www.gov.uk/government/publications/prime-minister-boris-johnsons-visit-to-india-april-2022-uk-india-joint-statements/india-uk-cyber-statement-april-2022>
- [30] Apple. *iMessage With PQ3: The New State of the Art in Quantum-Secure Messaging at Scale*. [Online]. Available: <https://security.apple.com/blog/imessage-pq3/>
- [31] AppViewX. *Crypto Agility Education Center*. [Online]. Available: <https://www.appviewx.com/education-center/what-is-crypto-agility/>
- [32] Q. Khan, S. Purification, and S.-Y. Chang, "Post-quantum key exchange and subscriber identity encryption in 5G using ML-KEM (Kyber)," *Information*, vol. 16, no. 7, p. 617, Jul. 2025, doi: [10.3390/info16070617](https://doi.org/10.3390/info16070617).
- [33] S. Mandal and D. B. Roy, "A lightweight unified Keccak module for efficient hashing in ML-KEM and ML-DSA," in *Proc. Quantum Secur. Privacy Workshop*, New York, NY, USA, Oct. 2025, pp. 34–39, doi: [10.1145/3733825.3765279](https://doi.org/10.1145/3733825.3765279).
- [34] *FALCON: Fast-Fourier Lattice-Based Compact Signatures Over NTRU*. [Online]. Available: <https://falcon-sign.info/falcon.pdf>
- [35] H. Jayalaxmi, H. M. Brunda, S. S. Nayak, M. Sathya, and A. S. Hegde, "Benchmarking SLH-DSA: A comparative hardware analysis against classical digital signatures for post-quantum security," *Cryptol. ePrint Archive*. [Online]. Available: <https://eprint.iacr.org/2025/2273>
- [36] H. Singh, "Code based cryptography: Classic McEliece," 2019, *arXiv:1907.12754*.
- [37] R. Zhao and S. Wang, "A review of quantum neural networks: Methods, models, dilemma," 2021, *arXiv:2109.01840*.
- [38] R. Lahoz-Beltra, "Quantum genetic algorithms for computer scientists," *Computers*, vol. 5, no. 4, p. 24, 2016. [Online]. Available: <https://www.mdpi.com/2073-431X/5/4/24>
- [39] S. K. Shandilya, B. J. Choi, A. Kumar, and S. Upadhyay, "Modified firefly optimization algorithm-based IDS for nature-inspired cybersecurity," *Processes*, vol. 11, no. 3, p. 715, Feb. 2023. [Online]. Available: <https://www.mdpi.com/2227-9717/11/3/715>
- [40] C. Ganguli, S. K. Shandilya, M. Nehrey, and M. Havryliuk, "Adaptive artificial bee colony algorithm for nature-inspired cyber defense," *Systems*, vol. 11, no. 1, p. 27, Jan. 2023. [Online]. Available: <https://www.mdpi.com/2079-8954/11/1/27>
- [41] C. Ganguli, S. K. Shandilya, and I. Izonin, "Design and implementation of adaptive network stabilization based on artificial bees colony optimization for nature inspired cyber security," *J. King Saud Univ. - Sci.*, vol. 35, no. 5, Jul. 2023, Art. no. 102713. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1018364723001751>
- [42] C. Ganguli, S. K. Shandilya, M. Gregus, and O. Basystiuk, "Adaptive network sustainability and defense based on artificial bees colony optimization algorithm for nature inspired cyber security," *Comput. Syst. Sci. Eng.*, vol. 48, no. 3, pp. 739–758, 2024. [Online]. Available: <http://www.techscience.com/csse/v48n3/56525>

- [43] S. K. Shandilya, S. Upadhyay, A. Kumar, and A. K. Nagar, "AI-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis," *Future Gener. Comput. Syst.*, vol. 127, pp. 297–308, Feb. 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167739X21003642>
- [44] K. V. Sharma, R. Betala, and V. N. V. L. S. Swathi, "Enhancing post-quantum cryptography security with BioCrypt quantum shield through nature-inspired machine learning," in *Multi-Disciplinary Trends in Artificial Intelligence*, vol. 15432. Singapore: Springer, 2025. [Online]. Available: https://doi.org/10.1007/978-981-96-0695-5_24
- [45] A. Kadu, A. Kulkarni, and D. Patil, "Secure data hiding using robust firefly algorithm," *Int. J. Comput. Eng. Res. Trends*, vol. 3, no. 10, pp. 550–553, 2016.
- [46] C. D. Harris, K. K. Schroeder, and J. Black, "A lattice-based method for optimization in continuous spaces with genetic algorithms," *Acta Astronautica*, vol. 228, pp. 957–971, Mar. 2025, doi: [10.1016/j.actaastro.2024.12.032](https://doi.org/10.1016/j.actaastro.2024.12.032).
- [47] K. Rajani, M. Archana, B. Rambabu, and M. Mounika, "Quantum-enhanced nature-inspired scheme for secure energy-aware routing in IoT WSNs," in *Proc. 3rd Int. Conf. Intell. Cyber Phys. Syst. Internet Things (ICoICI)*, Coimbatore, India, Sep. 2025, pp. 1191–1198, doi: [10.1109/icoici65217.2025.11253293](https://doi.org/10.1109/icoici65217.2025.11253293).
- [48] M. Azouaoui, J. W. Bos, B. Fay, M. Gourjon, Y. Kuzovkova, J. Renes, T. Schneider, and C. van Vredendaal, "Surviving the fo-calyipse: Securing PQC implementations in practice," Tech. Rep., 2022. [Online]. Available: <https://iacr.org/submit/files/slides/2022/rwc/rwc2022/48/slides.pdf>



SHISHIR KUMAR SHANDILYA (Senior Member, IEEE) received the D.Sc. and Ph.D. degrees. He is currently an Associate Professor with the School of Data Science and Forecasting, Devi Ahilya Vishwavidyalaya, India. He is also a Visiting Professor with Liverpool Hope University, U.K.; and Autonomous University of Tamaulipas, Mexico. He is a highly regarded author with published research works in reputed academic publishers, such as Springer, McGraw-Hill, IGI-USA, River Denmark, and Prentice Hall of India. He also has international and national patents and copyrights granted for adaptive cyber defense methods. His research interests include adaptive defense, explainable artificial intelligence, and nature-inspired cyber security (NICS). He has been awarded the prestigious Chevening India Cyber Security Fellowship hosted by Cranfield University, U.K., for the 2025–2026 academic year. He has received the IDA Teaching Excellence Award for distinctive use of technology in teaching by Indian Didactics Association, Bangalore, in 2016; and the Young Scientist Award by the MP Science Congress and the MP Council of Science and Technology for two consecutive years, in 2005 and 2006. He is a Cambridge University-Certified Professional Teacher and Trainer, a TEDx Speaker, and an ACM Distinguished Speaker. He is a NASSCOM-Certified Master Trainer for SOC Analysts.



CHIRAG GANGULI received the bachelor's degree in computer science and engineering (cyber security and digital forensics) from Vellore Institute of Technology. He is currently an accomplished Security Researcher and a Certified Ethical Hacker. He is also a Certified Lean Six Sigma Black Belt (LSSBB), which showcases his strong commitment to optimizing business processes and driving continuous improvement. His research interests include nature-inspired cyber security, adaptive defense, intrusion detection and prevention, and security data handling. He received the Best Paper Award for the paper titled "Data-Driven Approach to Network Intrusion Detection System Using Modified Artificial Bee Colony Algorithm for Nature-Inspired Cybersecurity," at AMLDA 2023 Conference.



AJAY KUMAR received the B.Eng. degree in mechanical engineering and the M.Sc. degree in automotive engineering. He is currently a Lecturer in vehicle mobility with the Centre for Defence Engineering and Physical Science, Cranfield University, specializing in the Weapons and Vehicle Systems Group. He is also the Course Director for the M.Sc. in Expeditionary Warfare Systems Engineering and Technology, delivered in USA. His clients include U.K. Ministry of Defence and QinetiQ. He possesses significant industry experience from his previous roles with Nissan and Jaguar Land Rover. His current scholarly interests focus on the effects of vehicle dynamics on intelligent vehicles, including off-road vehicle mobility, novel suspension concepts, and ride and handling.



IVAN IZONIN (Senior Member, IEEE) received the M.Sc. degree in computer science, in 2011, the M.Sc. degree in economic cybernetics, in 2012, the Ph.D. degree in artificial intelligence, in 2016, and the D.Sc.Tech. degree in artificial intelligence, in 2025. He is currently an Associate Professor with the Department of Artificial Intelligence, Lviv Polytechnic National University, Ukraine. His main research interests include computational intelligence, high-speed neural-like systems, non-iterative machine learning algorithms, and ensemble learning.



MICHAL GREGUS (Member, IEEE) received the Ph.D. degree (summa cum laude) in mathematical analysis from the Faculty of Mathematics and Physics, Comenius University Bratislava. Previously, he has worked in the field of functional analysis and its applications. His current research interests include management information systems, modeling economic processes, and business analytics.

...



DSPACE

<https://dspace.org/>

Post-quantum cryptography and nature-inspired cyber defense: strategic readiness and adaptive techniques for next-gen threat response

Shandilya, Shishir Kumar; Ganguli, Chirag; Kumar, Ajay; Izonin, Ivan; Gregus, Michal

2026-02

Institute of Electrical and Electronics Engineers (IEEE)

<https://doi.org/10.1109/access.2026.3663832>

Shandilya SK, Ganguli C, Kumar A, et al., (2026) Post-quantum cryptography and nature-inspired cyber defense: strategic readiness and adaptive techniques for next-gen threat response. IEEE Access, Volume 14, February 2026, pp. 27418-27434