

The Nested Contexts of Quantum Understanding (NCQU) Framework: A Cyberpsychology Perspective on Quantum Cybersecurity Readiness and Organizational Adaptation

Troy C. Troublefield^{1,2,3} 

¹Department of Cyberpsychology, Capitol Technology University, Laurel, USA

²Department of Information Technology, Capella University, Minneapolis, USA

³Department of International Business, International School of Management, Paris, France

Email: dtroytroublefield@yahoo.com

How to cite this paper: Troublefield, T.C. (2026) The Nested Contexts of Quantum Understanding (NCQU) Framework: A Cyberpsychology Perspective on Quantum Cybersecurity Readiness and Organizational Adaptation. *Journal of Quantum Information Science*, 16, 343-386. <https://doi.org/10.4236/jqis.2026.163012>

Received: April 2, 2026

Accepted: July 11, 2026

Published: July 14, 2026

Copyright © 2026 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0). <http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

The emergence of quantum computing presents unprecedented challenges for cybersecurity professionals and organizations, requiring fundamental reconceptualization of cryptographic security paradigms. Despite widespread technical awareness of quantum threats, organizational preparedness for post-quantum cryptography transitions remains inadequate, suggesting that barriers to quantum adaptation extend beyond purely technical domains into psychological and organizational territories. This article introduces the Nested Contexts of Quantum Understanding (NCQU) Framework, a comprehensive theoretical model that integrates cyberpsychology principles with quantum cybersecurity implementation challenges. The NCQU Framework conceptualizes quantum understanding as an emergent phenomenon arising from the dynamic interaction of individual, social, and organizational dimensions operating across temporal, epistemological, and phenomenological spectrums. Through theoretically directed synthesis of research on cognitive biases, professional identity challenges, organizational sense-making processes, and uncertainty tolerance mechanisms, this research illuminates psychological barriers impeding quantum cybersecurity adoption despite available post-quantum cryptographic standards. The framework identifies critical factors including temporal discounting of future quantum threats, expertise entrenchment among classical cryptographers, ambiguity aversion toward quantum-resistant solutions, and organizational culture dynamics that systematically undermine Q-

Day preparedness. Drawing on Weick's sense-making theory, technology acceptance models, and cyberpsychology research on human-technology interaction, the NCQU Framework provides diagnostic capabilities for identifying specific barriers to quantum adoption and targeting interventions across individual, social, and organizational levels. Practical implications emphasize the necessity of integrating psychological readiness with technical implementations, including metacognitive training for paradigm flexibility, scenario-based planning to counteract temporal discounting, professional identity adaptation support, and organizational psychological safety protocols enabling productive engagement with quantum uncertainty. This research contributes to emerging understanding of quantum cybersecurity transitions as fundamentally socio-technical challenges requiring coordinated attention to cognitive, affective, social, and organizational factors alongside cryptographic algorithm selection and implementation capabilities.

Keywords

Nested Contexts of Quantum Understanding, Quantum Cybersecurity, Cyberpsychology, Post-Quantum Cryptography, Q-Day Preparedness, Organizational Psychology, Technology Adoption, Professional Identity, Cognitive Biases, Sense-Making Theory

1. Introduction

The global digital infrastructure is built on cryptographic foundations that are fundamentally vulnerable to quantum computing. Public-key cryptosystems, including Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Diffie-Hellman protocols, secure financial transactions, government communications, healthcare records, and critical infrastructure control systems worldwide [1] [2]. These cryptographic systems derive security from mathematical problems, integer factorization, and discrete logarithm computation, which classical computers cannot solve efficiently within practical timeframes. However, quantum computers operating through fundamentally different computational principles can solve these problems exponentially faster using Shor's algorithm, rendering current cryptographic protections obsolete [3] [4]. This impending cryptographic discontinuity presents not merely a technical challenge but a complex socio-technical transition requiring fundamental reconceptualization of security paradigms, organizational processes, and professional competencies.

Q-Day, the threshold moment when quantum computers achieve sufficient scale and stability to execute Shor's algorithm against real-world cryptographic implementations, represents an unprecedented convergence of technological capability and psychological uncertainty in cybersecurity history [5] [6]. Unlike gradual technological transitions, Q-Day constitutes a discontinuous shift in which security assumptions that have maintained decades of cryptographic prac-

tice collapse simultaneously across countless systems and organizations. Estimates for Q-Day arrival varies considerably, with projections ranging from 10 to 30 years, depending on quantum hardware advancement trajectories and error-correction breakthroughs [3] [5]. This temporal uncertainty, combined with the paradigmatic nature of quantum computing, poses distinctive psychological challenges for security professionals and organizations seeking to prepare for threats with indeterminate timelines for manifestation.

[7] completed its post-quantum cryptography standardization process in 2024, establishing quantum-resistant algorithms including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures [7]. These standardized algorithms provide technically viable alternatives to quantum-vulnerable cryptosystems, enabling organizations to begin transitioning toward quantum-resistant security architectures. However, despite widespread awareness of quantum threats within cybersecurity communities and the availability of standardized post-quantum alternatives, organizational adoption of post-quantum standards remains early-stage and uneven, with available assessments suggesting that a substantial portion of organizations continue to operate cryptographic systems known to be vulnerable to quantum attack while deferring systematic migration to quantum-resistant implementations [8] [9].

This awareness-action disconnect, coupled with high quantum threat recognition and inadequate preparedness behaviors, suggests that Q-Day readiness challenges transcend purely technical domains. Security professionals widely acknowledge quantum vulnerabilities, understand the implications of Shor's algorithm, and recognize the necessity of post-quantum cryptography, yet organizational implementation remains absent or minimal [6] [10]. This pattern indicates that barriers to quantum adaptation operate substantially in psychological and organizational rather than purely technical territories. Organizations exhibit predictable patterns of denial, deferral, and rationalization when confronting quantum threats with uncertain timelines, manifesting cognitive biases that systematically undermine appropriate preparation despite rational threat acknowledgment [5] [11].

Cyberpsychology, the study of human-technology interaction and psychological processes in digital environments, provides essential frameworks for understanding this preparation paradox [12] [13]. The field examines how cognitive biases, threat perception mechanisms, organizational psychology, and human decision-making processes influence cybersecurity behaviors and outcomes. Applied to quantum security contexts, cyberpsychology perspectives reveal that inadequate Q-Day preparation stems substantially from predictable psychological patterns rather than technical deficiencies or resource constraints. Organizations exhibit systematic temporal discounting of quantum threats, preferring immediate operational demands over future preparedness investments [5]. Security professionals experience ambiguity aversion toward post-quantum solutions with uncertain performance characteristics [14]. Classical cryptography specialists demonstrate expertise entrenchment, resisting quantum paradigms that challenge accumulated

professional knowledge [10]. Organizations exhibit collective optimism bias, systematically overestimating their quantum preparedness [6].

These psychological dynamics operate not in isolation but through complex interactions across individual, social, and organizational levels. Individual security professionals develop a quantum understanding within social networks that shape the interpretation and validation of quantum information. Social processes unfold within organizational contexts that enable, constrain, and direct quantum sense-making through resource allocation, cultural norms, and leadership priorities. Understanding develops across temporal horizons, connecting past experiences, present challenges, and future implications. Knowledge manifests across epistemological spectrums, from abstract theory to embodied practice. Professionals progress through phenomenological journeys, transforming confusion into commitment. These multiple dimensions interact simultaneously, creating emergent patterns of quantum comprehension that resist reduction to any single factor or level of analysis.

This article introduces the Nested Contexts of Quantum Understanding (NCQU) Framework, a comprehensive theoretical model integrating cyberpsychology principles with quantum cybersecurity implementation challenges. The NCQU Framework conceptualizes quantum understanding as emerging from nested individual, social, and organizational contexts, operating across temporal, epistemological, and phenomenological dimensions, and developing through identifiable developmental progressions. The framework provides systematic guidance for investigating the complex processes by which abstract quantum knowledge transforms into practical professional competence, illuminating the psychological barriers that impede quantum adoption despite technical awareness and available solutions. By identifying specific dysfunctions across multiple nested contexts and cross-cutting dimensions, the NCQU Framework enables targeted interventions addressing precise gaps in the quantum understanding ecosystem.

Before proceeding to the framework's theoretical architecture, three constructs central to this analysis require precise definition, as the literature employs them inconsistently. Quantum understanding refers to the cognitive and affective state in which an individual or organization has achieved sufficient comprehension of quantum computing principles and their cryptographic implications to make informed, actionable security decisions, a condition distinct from mere awareness that quantum threats exist. Quantum readiness denotes an organization's demonstrated operational capacity to execute a post-quantum cryptography transition, encompassing cryptographic inventory completion, algorithm selection, migration planning, workforce competency, and budget commitment; readiness is a measurable state of preparation, not an intention or posture. Q-Day preparedness, by contrast, is a broader construct incorporating both quantum readiness and the organizational resilience factors, cultural adaptability, leadership quantum literacy, psychological safety, and identity-adaptive workforce development, that determine whether a quantum-ready organization can sustain effective security op-

erations through and after the cryptographic transition event. Quantum understanding is the cognitive prerequisite for readiness; readiness is the operational prerequisite for Q-Day preparedness. The NCQU Framework is specifically designed to explain why organizations can possess quantum understanding without achieving readiness, and quantum readiness without achieving comprehensive Q-Day preparedness.

This research addresses three critical questions: 1) How do cognitive biases and psychological mechanisms explain inadequate organizational Q-Day preparation despite widespread technical awareness? 2) What role do professional identity, organizational culture, and social dynamics play in post-quantum cryptography adoption patterns? 3) How can cyberpsychology interventions enhance quantum readiness by addressing psychological barriers alongside technical implementations?

Nature and Scope of This article is a conceptual framework paper grounded in a theoretically directed narrative review of the scholarly literature. It does not employ a systematic or scoping review methodology; no search protocol, eligibility screening matrix, or PRISMA-style reporting was used. Instead, the review is organized around four thematic pillars: quantum computing and cryptographic vulnerability, cyberpsychology and technology adoption, organizational psychology and collective sense-making, and professional identity, each representing a domain of scholarship whose core findings bear directly on the quantum cybersecurity readiness problem. Literature was selected based on theoretical relevance and empirical significance, prioritizing peer-reviewed journal articles, authoritative handbooks, and established theoretical works cited in these domains. Where the abstract draws upon identified patterns and mechanisms in this body of work, that synthesis represents the authors' interpretive synthesis rather than a count of coded studies. Accordingly, references in this paper to the analysis of the literature should be understood as a narrative synthesis informed by scholarly judgment rather than a protocol-driven systematic review.

2. Literature Review

Quantum computing represents a major shift with profound implications for cryptographic security, leveraging unique properties like superposition, entanglement, and interference to solve problems that classical computing cannot feasibly address. Algorithms like Shor's have demonstrated the vulnerability of widely used cryptographic systems, such as RSA and elliptic curve cryptography, potentially undermining the foundations of secure communications. While current quantum computers are still in the NISQ era and unable to execute cryptographically significant attacks, advances in quantum hardware continue to progress rapidly. This uncertainty about the timeline for achieving cryptographically relevant quantum computers compels organizations to anticipate significant shifts in security planning and posture. As the transition to post-quantum cryptography begins, challenges related to implementation, cognitive adaptation to quantum par-

adigms, and professional identity must be addressed to ensure secure and effective adoption of quantum-resistant systems.

2.1. Quantum Computing and Cryptographic Security

Quantum computing represents a fundamental paradigm shift in computational capability, leveraging quantum-mechanical phenomena, including superposition, entanglement, and interference, to perform calculations that are impossible for classical computers [15]. Unlike classical bits existing in definite states of 0 or 1, quantum bits (qubits) exist in a superposition of both states simultaneously until measurement collapses the quantum state. Quantum entanglement enables correlations between qubits that have no classical analog, while quantum interference allows constructive and destructive combination of probability amplitudes. These quantum properties enable certain algorithms to achieve exponential speedup over classical counterparts for specific problem classes [16].

Shor's algorithm, developed in 1994, demonstrated that quantum computers could factor large integers and solve discrete logarithm problems in polynomial time, directly threatening cryptographic systems whose security relies on the classical computational intractability of these problems [4]. RSA encryption, widely used for secure communications, relies on the difficulty of factoring the product of large prime numbers. Elliptic curve cryptography relies on the computational hardness of the discrete logarithm problem in elliptic curve groups. Diffie-Hellman key exchange protocols similarly derive their security from the intractability of the discrete logarithm. Shor's algorithm renders all these systems vulnerable to quantum attacks once sufficiently powerful quantum computers become available [17].

Current quantum computers remain in the Noisy Intermediate-Scale Quantum (NISQ) era, characterized by limited qubit counts, short coherence times, and high error rates that preclude the execution of Shor's algorithm on real-world key sizes [18]. However, quantum hardware capabilities continue advancing through improved qubit fabrication, error correction techniques, and quantum control mechanisms. The timeline for achieving cryptographically relevant quantum computers remains contested, with estimates ranging from 10 to 30 years, depending on assumptions about technical breakthroughs [3]. This temporal uncertainty poses distinctive challenges for organizational planning, requiring preparation for threats with indeterminate timelines for manifestation.

Post-quantum cryptography has progressed in parallel with advances in quantum computing, establishing cryptographic systems believed to resist both classical and quantum attacks [1]. NIST conducted a multi-year standardization process evaluating post-quantum cryptographic algorithms based on lattice problems, hash-based signatures, code-based cryptography, and multivariate polynomial systems. In 2024, NIST standardized several algorithms, including CRYSTALS-Kyber for key encapsulation mechanisms and CRYSTALS-Dilithium for digital signatures [7]. These standardized algorithms provide organizations with quantum-resistant alternatives, enabling cryptographic transitions before Q-Day arrival.

However, deployment of post-quantum algorithms introduces implementation challenges, including larger key sizes, different performance characteristics, and integration complexities with existing systems [19]. Lattice-based schemes typically require larger keys and ciphertexts than classical alternatives, increasing bandwidth and storage requirements. Performance profiles differ from classical systems, potentially requiring application-level modifications. System integration demands careful cryptographic inventory assessment, dependency mapping, and migration planning across heterogeneous technology stacks. These technical challenges interact with organizational factors, including resource constraints, competing priorities, and risk tolerance, to shape adoption patterns [9].

2.2. Cyberpsychology and Technology Adoption

Cyberpsychology examines psychological processes in human-technology interaction, investigating how digital technologies influence cognition, emotion, behavior, and social processes [12]. Applied to cybersecurity contexts, cyberpsychology illuminates psychological factors affecting security behaviors, threat perceptions, and technology adoption patterns. Research demonstrates that human factors often constitute primary cybersecurity vulnerabilities rather than technical system weaknesses, with psychological processes systematically undermining security implementations through cognitive biases, emotional responses, and social dynamics [13].

Risk perception theory establishes that humans assess threats through psychological dimensions, including familiarity, control, catastrophic potential, and personal vulnerability, rather than purely rational probability calculations [20]. Slovic's psychometric paradigm identifies dread risk, perceived lack of control coupled with catastrophic consequences, and unknown risk, new, unfamiliar threats, as primary factors intensifying perceived threat severity. Quantum computing risks encompass both dimensions, posing novel threats beyond most security professionals' direct experience and carrying potentially catastrophic consequences for cryptographic security. However, the abstract nature and temporal uncertainty of quantum threats create psychological distance that paradoxically reduces rather than enhances perceived risk, undermining preparedness despite objectively severe implications [5] [6] [20].

Temporal discounting theory explains the systematic human tendency to undervalue future outcomes compared to immediate consequences, even when future outcomes carry objectively greater significance [21]. This cognitive bias particularly affects cybersecurity decision-making when threats manifest on extended timelines, with distant threats receiving systematically less attention and resources than immediate operational demands. Research by [5] applied temporal discounting frameworks to quantum security contexts and demonstrated experimentally that security professionals systematically underweight quantum threats due to their perceived temporal distance. This temporal discounting effect holds even among professionals with a comprehensive technical understanding of quantum

vulnerabilities, suggesting that cognitive biases, rather than knowledge deficits, drive inadequate preparation patterns.

Construal level theory provides a complementary perspective on temporal distance effects, explaining how psychological distance, temporal, spatial, social, and hypothetical, influences mental representations and decision-making [11]. Psychologically distant events are construed abstractly, emphasizing general features while de-emphasizing concrete details and implementation specifics. Psychologically proximate events receive concrete construal, emphasizing feasibility, implementation details, and contextual constraints. Applied to quantum threats, this framework suggests that distant Q-Day timelines promote abstract construal focused on general quantum principles while obscuring concrete implementation requirements, migration planning specifics, and resource allocation decisions necessary for effective preparation.

Ambiguity aversion describes a preference for known risks over unknown risks even when unknown risks offer equivalent or superior expected outcomes [22]. Security professionals frequently exhibit ambiguity aversion when evaluating post-quantum alternatives, preferring familiar but quantum-vulnerable classical systems over unfamiliar quantum-resistant algorithms with uncertain performance characteristics. [14] applied quantum cognition models to security investment decisions, demonstrating robust ambiguity aversion effects impeding proactive resource allocation despite rational awareness of quantum vulnerabilities. This research reveals that decision-making under quantum uncertainty violates classical probability axioms, suggesting quantum-inspired cognitive models may better capture security professionals' actual reasoning patterns than standard rational choice theories.

The Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) provide established frameworks for understanding technology adoption patterns [23] [24]. TAM emphasizes perceived usefulness and perceived ease of use as primary determinants of adoption, while UTAUT extends this foundation with performance expectancy, effort expectancy, social influence, and facilitating conditions. Applied to post-quantum cryptography, these frameworks suggest adoption depends substantially on whether security professionals perceive quantum-resistant algorithms as useful for addressing genuine threats, easy to implement within existing systems, socially endorsed by professional communities, and adequately supported by organizational resources and infrastructure. Research indicates that all these factors currently impede post-quantum adoption, with professionals questioning threat immediacy, perceiving implementation complexity, lacking peer validation, and encountering insufficient organizational support [9].

2.3. Organizational Psychology and Collective Sense-Making

Organizational psychology examines collective decision-making, institutional behavior patterns, and cultural factors influencing organizational outcomes. Ap-

plied to quantum security contexts, organizational psychology illuminates how collective psychological processes determine institutional preparedness beyond individual-level cognition. Weick's sense-making theory explains how organizations collectively construct meaning from ambiguous environments through communication, shared narratives, and coordinated interpretation [25]. Q-Day requires organizational sense-making that constructs shared understanding of quantum threats, aligns interpretations across different organizational functions, and establishes collective priorities for quantum preparation.

Weick identifies seven properties characterizing organizational sense-making: identity construction, retrospection, enactment, social activity, ongoing process, extracted cues, and plausibility over accuracy. These properties illuminate quantum security challenges through multiple dimensions. Identity construction suggests quantum understanding depends on how security professionals conceive their roles and expertise relative to quantum threats. Retrospection indicates professionals interpret quantum computing by drawing upon past experiences with technological disruption and cryptographic transitions. Enactment emphasizes that organizations actively shape quantum threat environments through attention patterns and resource-allocation decisions, rather than passively responding to external realities. Social activity recognizes that quantum sense-making occurs through dialogue, negotiation, and collective interpretation rather than individual contemplation. These sense-making properties reveal quantum preparedness as fundamentally social and interpretive rather than purely technical achievement.

Organizational culture theory examines the shared values, beliefs, assumptions, and behavioral norms that characterize institutions [26]. Organizational culture powerfully influences quantum readiness through factors including innovation orientation, willingness to adopt new technologies, risk tolerance, capacity for investment under uncertainty, learning culture, openness to new knowledge domains, and psychological safety, comfort acknowledging limitations and uncertainties. Research by [6] demonstrates that organizational culture predicts quantum preparedness more strongly than technical resources or threat awareness, suggesting cultural factors as critical leverage points for intervention. Organizations with strong innovation cultures, high tolerance for uncertainty, and psychological safety that enables productive engagement with ambiguity demonstrate substantially higher quantum readiness than organizations with risk-averse, hierarchical cultures that emphasize established expertise.

The organizational mindfulness framework developed by [27] provides analytical tools for understanding how organizations maintain attention on emerging threats with uncertain timelines. Their framework identifies five characteristics of high-reliability organizations: preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise. Applied to quantum security, preoccupation with failure suggests organizations should maintain vigilance regarding quantum vulnerabilities despite the absence of immediate attacks. Reluctance to simplify indicates a reluctance to draw prem-

ature conclusions about quantum timelines or threat severity. Sensitivity to operations emphasizes monitoring quantum developments and progress in post-quantum implementations. Commitment to resilience involves developing adaptive capacity for cryptographic transitions under various quantum advancement scenarios. Deference to expertise requires cultivating quantum literacy, enabling appropriate evaluation of technical recommendations.

However, quantum security presents distinctive challenges for organizational mindfulness. Traditional high-reliability organizational contexts involve immediate operational threats with clear failure signals, enabling rapid feedback loops that reinforce vigilance. Quantum threats operate on extended, uncertain timelines without immediate feedback mechanisms. Organizations cannot verify the effectiveness of their quantum preparedness until Q-Day arrives, potentially decades after making those investments. This temporal disconnect between preparatory actions and outcome validation creates organizational learning challenges that are fundamentally different from those in traditional reliability contexts [27]. Organizations must maintain quantum mindfulness without reinforcing feedback, and require cultural and structural supports beyond those effective against immediate operational threats.

2.4. Professional Identity and Expertise Challenges

Professional identity theory examines how individuals construct self-conceptions through occupational roles, expertise domains, and career trajectories [28]. Security professionals, particularly cryptography specialists, develop professional identities centered on specific knowledge domains, methodological approaches, and problem-solving capabilities. These professional identities provide meaning, status, and career advancement pathways while simultaneously creating psychological investments in particular expertise domains that may resist paradigmatic change [10].

Quantum computing presents fundamental challenges to cryptographic professional identity by potentially rendering classical cryptography expertise partially obsolete. Cryptography specialists invest years developing mathematical sophistication, protocol knowledge, and security analysis capabilities within classical computational paradigms. Professional identity, career advancement, and workplace status derive substantially from this expertise. Quantum computing threatens these professional investments by introducing computational capabilities that break previously secure cryptographic systems and require fundamentally different mathematical foundations [17]. This identity threat triggers psychological responses, including anxiety about expertise obsolescence, defensiveness toward quantum paradigms, and avoidance of quantum learning opportunities that might reveal knowledge gaps.

Research by [10] documents pervasive concerns about professional identity among cryptography specialists confronting quantum threats. Their qualitative studies reveal that resistance to post-quantum approaches often stems not from technical disagreement but from challenges to professional self-efficacy and ex-

expertise identity. Mid-career cryptographers with substantial investments in classical expertise demonstrate particularly strong identity-threat responses, manifesting as minimization of quantum threat severity, skepticism toward the viability of post-quantum algorithms, or delayed engagement with quantum learning despite rational awareness of quantum vulnerabilities. These findings suggest quantum transitions require explicit attention to professional identity adaptation alongside technical training.

The concept of adaptive expertise contrasts with routine expertise in understanding patterns of professional development [29]. Adaptive expertise involves flexible application of knowledge to novel situations, maintaining learning orientation and cognitive flexibility when encountering new paradigms. Routine expertise excels at efficiently executing familiar tasks but shows reduced flexibility when paradigms shift. Deep classical cryptography expertise often develops as routine expertise optimized for classical paradigms, creating cognitive barriers to adaptive quantum thinking. Professionals with strong routine expertise may experience quantum transitions as more threatening than those with less accumulated classical expertise, generating a counterintuitive pattern in which greater technical knowledge correlates with increased psychological resistance [30].

Professional identity adaptation theories distinguish three response patterns when expertise domains face disruption: identity defense, minimizing the significance of threats and maintaining the emphasis on existing expertise; identity adaptation, integrating new competencies while redefining professional self-conception; and identity exit, transitioning to different specializations less affected by disruption [31]. Research on cryptographic professionals facing quantum threats documents all three response patterns, with some specialists minimizing the significance of quantum threats, others pursuing quantum education, and still others transitioning to non-cryptographic specializations. Organizational quantum readiness depends substantially on facilitating identity adaptation while minimizing defensive resistance and expertise attrition.

2.5. Human Factors in Quantum Computing

Human factors research examines cognitive, perceptual, and physical capabilities and limitations affecting human-system interaction [32]. Applied to quantum computing, human factors investigation reveals fundamental challenges in how humans conceptualize, interact with, and trust quantum systems. Quantum computing introduces cognitive demands extending beyond traditional computational thinking, requiring mental models accommodating superposition, entanglement, and probabilistic measurement outcomes fundamentally different from classical computing paradigms.

Cognitive load theory posits that limitations in working memory capacity constrain how much information humans can process simultaneously [33]. Quantum programming imposes a substantial cognitive load due to several factors: maintaining awareness of quantum state evolution across multiple qubits, reasoning

about probabilistic rather than deterministic outcomes, tracking entanglement relationships across quantum systems, and understanding measurement effects on quantum states. This cognitive load exceeds typical programming demands, necessitating specialized interface designs, visualization tools, and educational approaches that support quantum reasoning [34].

Trust in technological systems depends on predictability, reliability, and comprehensibility of system behaviors [35]. Quantum systems challenge traditional trust establishment through inherent probabilistic outcomes that vary between runs even with identical inputs. This introduces quantum trust uncertainty, making it difficult to establish confidence in systems with inherently variable outputs [36]. Unlike classical systems that provide deterministic results enabling verification and prediction, quantum systems require new trust-calibration approaches that accommodate probabilistic quality metrics, fidelity measures, and statistical confidence intervals. Interface designs must communicate these quantum-specific reliability indicators to support appropriate trust development, without either over-trusting flawed quantum implementations or under-trusting that impedes quantum technology adoption.

Uncertainty tolerance describes an individual's and an organization's capacity to function effectively amid ambiguity and incomplete information [37]. Quantum computing presents extreme uncertainty across multiple dimensions, including hardware development timelines, attack capability thresholds, optimal migration strategies, and appropriate preparedness investments. Security professionals vary substantially in uncertainty tolerance, with some exhibiting premature certainty, adopting specific solutions before standards solidify, while others demonstrate perpetual deferral, continuously postponing decisions until uncertainty resolves. Research suggests that structured uncertainty tolerance, acknowledging unknowns while establishing adaptive decision frameworks, enables more effective quantum transition management than extreme [9].

Educational approaches to quantum computing must address not only technical skills but also psychological adaptation to quantum-thinking paradigms. This includes developing comfort with probabilistic reasoning, tolerance for uncertainty, and flexibility in mental models, enabling paradigm shifts from classical to quantum computational frameworks. Research on quantum education reveals that traditional computer science pedagogies are insufficient for quantum contexts, requiring specialized approaches that incorporate cognitive adaptation support, misconception identification and correction, and progressive skill-development scaffolding for quantum complexity [34]. These educational challenges extend beyond academic contexts into professional training requirements for the security workforce and quantum upskilling.

3. The Nested Contexts of Quantum Understanding (NCQU) Framework: Theoretical Foundation

The Nested Contexts of Quantum Understanding (NCQU) Framework provides

a comprehensive theoretical model for examining how cybersecurity professionals develop a qualitative understanding of quantum computing implementation within complex organizational environments. The framework conceptualizes quantum understanding not as an isolated cognitive process but as an emergent phenomenon arising from the dynamic interaction of individual, social, and organizational dimensions operating simultaneously across multiple temporal and epistemological spectrums. At its core, the NCQU Framework recognizes that professionals' sense-making processes regarding quantum technologies cannot be adequately understood by examining technical knowledge alone, but rather require systematic attention to nested contextual layers within which understanding develops, cross-cutting dimensions shaping interpretive processes, and phenomenological journeys through which abstract quantum concepts transform into actionable professional knowledge.

The framework employs a concentric circles design representing the nested nature of contextual influences on quantum understanding, with each layer simultaneously containing and being shaped by the layers it encompasses. At the center resides Quantum Understanding itself, the focal point of meaning-making processes in which professionals construct an understanding of quantum computing's implications for cybersecurity practice. This core understanding is not conceived as a static body of knowledge but as a continuously evolving interpretive achievement that professionals actively construct through engagement with surrounding contextual layers. The central positioning emphasizes that while quantum comprehension is the ultimate focus of investigation, it cannot be separated from the multiple contexts that give it meaning, shape its development, and determine its practical application in professional settings.

3.1. Individual Experience Layer

The innermost contextual layer, the Individual Experience Layer, recognizes that quantum understanding emerges first and foremost from unique characteristics, backgrounds, and developmental trajectories of individual professionals. This layer encompasses four critical dimensions shaping how professionals encounter, interpret, and integrate quantum concepts into existing knowledge structures.

Professional identity operates as a foundational element, influencing what aspects of quantum computing professionals attend to, how they interpret quantum threats and opportunities relative to their role responsibilities, and what actions they consider appropriate given their self-conception as cybersecurity experts. Security professionals with strong cryptography identities may experience quantum computing as a fundamental challenge to professional self-conception, generating anxiety and defensive responses. Network security specialists may perceive quantum computing as a peripheral concern disconnected from primary responsibilities. Identity shapes not merely what professionals know about quantum computing, but also what they consider relevant to know, what learning investments they prioritize, and how quantum knowledge integrates with their professional self-

understanding [10].

Prior knowledge and cognitive schemas function as interpretive lenses filtering new quantum information through existing mental models of cryptography, computing, and security. Professionals with strong classical computing backgrounds may struggle to develop quantum intuitions that violate deterministic computational assumptions. Those familiar with probability theory may be more readily able to accommodate quantum measurement principles. Existing cryptographic knowledge provides a foundation for understanding post-quantum alternatives, but may also create cognitive entrenchment that resists paradigm shifts. Schema theory suggests that new information is assimilated into existing cognitive structures, when possible, but that accommodation, which requires schema modification, occurs reluctantly and generates cognitive discomfort [38] [39]. Quantum computing often requires schema accommodation rather than mere assimilation, creating learning challenges beyond simple knowledge acquisition.

Emotions and attitudes toward quantum technologies, ranging from anxiety about obsolescence to excitement about novel capabilities, color interpretive processes and influence engagement levels, learning persistence, and implementation advocacy. Anxiety about quantum threats may motivate proactive learning but can also trigger avoidance when perceived as overwhelming. Excitement about quantum opportunities may enhance learning motivation, but risk premature adoption before adequate understanding and development. Frustration with quantum complexity may undermine persistence in learning. Defensive attitudes toward quantum paradigms impede openness to quantum knowledge. Emotional responses are not merely epiphenomenal but actively shape quantum learning trajectories and implementation outcomes [6].

Skill development represents an ongoing process through which professionals translate abstract quantum concepts into practical competencies, moving from theoretical awareness toward hands-on capability in quantum-relevant security practices. Skills span the spectrum from conceptual understanding, grasping quantum principles intellectually, to analytical capability, evaluating quantum security implications, to implementation competence, deploying post-quantum cryptography, to strategic insight, integrating quantum considerations into security architecture decisions. Skill development unfolds through practice, feedback, and progressive challenge, requiring time investments and learning opportunities often absent in resource-constrained security operations [32].

3.2. Social and Collaborative Layer

Surrounding the individual layer, the Social and Collaborative Layer acknowledges that quantum understanding develops not in isolation but through interpersonal interaction and collective knowledge construction within professional communities. This layer captures how understanding is negotiated, validated, and refined through social processes extending beyond individual cognition.

Peer networks provide informal channels through which professionals share

quantum-related information, validate interpretations, and collectively make sense of ambiguous or contradictory developments in quantum. Network position influences access to quantum information, with centrally located professionals receiving diverse perspectives, while peripheral members may encounter limited or biased quantum information. Network homophily, the tendency to associate with similar others, may create echo chambers where quantum skepticism or enthusiasm becomes self-reinforcing without exposure to alternative viewpoints. Strong professional networks facilitate the diffusion of quantum knowledge but may also transmit misinformation or reinforce cognitive biases when network norms discourage critical evaluation of quantum claims [24].

Knowledge-sharing mechanisms, both formal and informal, enable professionals to access expertise beyond their individual competencies, drawing upon collective intelligence to navigate quantum complexity that exceeds any single person's comprehensive understanding. Formal mechanisms include training programs, technical documentation, and structured knowledge repositories. Informal mechanisms encompass hallway conversations, email exchanges, and social media interactions. Effective knowledge sharing requires psychological safety, comfort with admitting quantum knowledge gaps without status loss, and a shared vocabulary that enables quantum concept communication across expertise boundaries. Organizations vary substantially in their knowledge-sharing effectiveness, with some fostering collaborative quantum learning while others maintain siloed expertise, limiting the diffusion of quantum understanding [25].

Team dynamics shape how quantum implementation challenges are framed, discussed, and addressed, with group composition, communication patterns, and decision-making processes influencing which quantum approaches are considered viable and which are dismissed as impractical. High-performing teams demonstrate collective efficacy, shared belief in team capability to accomplish quantum transitions, enabling ambitious quantum initiatives. Teams exhibiting groupthink may prematurely converge on quantum strategies without adequate critical evaluation. Teams with power imbalances may defer to senior members' quantum views regardless of accuracy. Team psychological safety determines whether members raise quantum concerns, acknowledge uncertainties, or propose unconventional quantum approaches [26].

Communities of practice centered on quantum cybersecurity create spaces where professionals develop shared language, common frameworks, and collective standards for quantum understanding, transcending individual organizations. These communities may be informal interest groups, professional association committees, or multi-organizational working groups. Communities of practice enable cross-organizational learning, the establishment of best practices, and the development of professional norms regarding quantum preparedness. However, community influence can also constrain quantum thinking when dominant paradigms discourage alternative approaches or when community norms emphasize consensus over critical evaluation [39] [40].

3.3. Organizational Context Layer

The outermost layer, the Organizational Context Layer, positions quantum understanding within broader institutional environments that enable, constrain, and direct professional sense-making processes. This layer recognizes that individual and social processes of quantum comprehension occur within organizational settings, profoundly shaping what understanding means and how it manifests in practice.

Organizational culture and norms establish implicit expectations about quantum engagement, signaling whether quantum implementation represents a strategic priority or a peripheral concern, whether quantum experimentation is encouraged or discouraged, and whether quantum expertise enhances or threatens professional standing. Organizations with innovation-oriented cultures facilitate quantum exploration, resource allocation for quantum learning, and tolerance for experimentation with quantum implementations. Risk-averse cultures emphasize proven approaches, creating barriers to post-quantum adoption despite quantum vulnerabilities in current systems. Cultures valuing learning support quantum skill development; cultures emphasizing operational efficiency may view quantum training as unproductive time away from immediate demands [6].

Resources and support determine the material conditions for quantum learning, including access to training programs, quantum computing platforms, implementation budgets, and time allocated to quantum skill development beyond immediate operational demands. Resource availability does not automatically translate into quantum readiness; organizations with substantial resources may still demonstrate inadequate quantum preparation, whereas resource constraints definitively impede quantum transitions, requiring training investments, technology acquisitions, and implementation efforts. Resource allocation decisions reflect organizational priorities, with quantum resource commitment signaling quantum importance regardless of stated strategic goals [9].

Leadership vision articulates organizational narratives about quantum significance, framing whether quantum threats merit an urgent response or are distant concerns, and whether quantum capabilities offer competitive advantages or are costly distractions. Leaders shape attention patterns through what they discuss, what they resource, and what they reward. Quantum-engaged leadership maintains organizational focus on quantum preparation despite competing priorities and uncertain timelines. Quantum-dismissive leadership undermines preparation efforts regardless of technical staff quantum awareness. Leadership quantum literacy, understanding sufficient quantum principles to evaluate recommendations, enables informed strategic decisions rather than either premature commitment or perpetual deferral [27].

Strategic priorities position quantum cybersecurity relative to competing organizational objectives, influencing whether quantum implementation receives resource allocation, senior attention, and integration into long-term planning or remains subordinated to more immediate concerns. Organizations facing current

security incidents may deprioritize quantum preparation in favor of immediate threat response. Those pursuing growth initiatives may view quantum investment as diverting resources from revenue-generating activities. Strategic priority determination depends substantially on how leaders construe quantum threats, as existential risks demanding immediate attention or distant possibilities deferrable indefinitely. This organizational layer emphasizes that quantum understanding is never purely technical but is always embedded within institutional contexts that shape its meaning, urgency, and practical implications.

3.4. Cross-Cutting Dimensions

The NCQU Framework incorporates three cross-cutting dimensions operating across all contextual layers, representing fundamental aspects of quantum sense-making that cannot be confined to any single layer but instead permeate the entire understanding process.

3.4.1. Temporal Dimension

The Temporal Dimension recognizes that quantum comprehension develops across time, drawing upon past experiences while responding to present challenges and anticipating future implications. Professionals make sense of quantum computing by retrospectively examining prior encounters with technological disruption, using historical patterns to interpret current quantum developments and project future trajectories. Past experiences with cryptographic transitions, technology adoption, or security paradigm shifts provide interpretive frameworks for understanding quantum. However, retrospection can also yield misleading analogies when quantum discontinuities differ fundamentally from those of past transitions [25].

Present challenges focus sense-making on immediate implementation obstacles, resource constraints, and operational demands requiring a quantum understanding to address concrete problems rather than remaining abstract. Current organizational priorities, available technologies, and operational contexts shape what quantum knowledge seems relevant versus peripheral. However, present-focused can obscure long-term quantum implications when immediate operational demands crowd out future-oriented preparation activities [11].

Future anticipation shapes quantum interpretation through expectations about Q-Day timelines, post-quantum cryptography requirements, and career implications of quantum transitions. Professionals construct understanding that enables proactive preparation rather than reactive responses, developing quantum competencies before quantum threats materialize. The Q-Day timeline operates as a particularly salient temporal marker, creating urgency around quantum sense-making by establishing a specific time horizon when quantum threats may materialize, thereby transforming quantum understanding from academic interest into a professional imperative. However, timeline uncertainty creates temporal ambiguity, undermining preparation when professionals defer action in the hope of greater clarity that may never arrive [5].

3.4.2. Knowledge Spectrum Dimension

The Knowledge Spectrum Dimension captures epistemological range across which quantum understanding develops, recognizing that professionals navigate multiple knowledge types simultaneously. Abstract theory represents a conceptual understanding of quantum principles, superposition, entanglement, and quantum algorithms, providing foundational comprehension but remaining disconnected from practical application. Theoretical knowledge enables intellectual discussions about quantum computing but proves insufficient for implementation decisions that require concrete technical judgments.

Practical application translates theoretical knowledge into concrete security implementations, involving decisions about quantum key distribution deployment, post-quantum algorithm selection, and quantum-resistant architecture design. Practical knowledge develops through hands-on experience with quantum-relevant technologies, implementation projects, and troubleshooting quantum integration challenges. Bridging abstract theory and practical application is a critical transition point where many professionals struggle, possessing conceptual quantum knowledge yet unable to apply it effectively.

Tacit knowledge encompasses intuitive, experience-based understanding that professionals develop through hands-on quantum engagement, including judgment about when quantum approaches prove appropriate, recognition of quantum security patterns, and anticipation of challenges resisting explicit articulation. Tacit knowledge develops slowly through repeated practice and pattern recognition, distinguishing novices from experts. However, tacit knowledge transfer proves difficult, requiring mentorship relationships and apprenticeship models rather than formal instruction [40].

Embodied practice represents the deepest form of quantum understanding, in which professionals internalize quantum thinking to the point that quantum considerations become automatic aspects of security decision-making rather than requiring conscious deliberation. Embodied quantum practice manifests as the intuitive incorporation of quantum threat assessment into security architecture design, the automatic consideration of post-quantum alternatives when evaluating cryptographic implementations, and the instinctive recognition of quantum-vulnerable system configurations. This spectrum emphasizes that quantum understanding is not unidimensional but encompasses multiple knowledge forms that develop at different rates through different processes, and that comprehensive quantum competence requires integration across the entire epistemological range.

3.4.3. Phenomenological Journey Dimension

The Phenomenological Journey dimension traces developmental progression through which professionals typically advance in quantum understanding, acknowledging that quantum comprehension unfolds through identifiable stages characterized by distinct experiential qualities. The journey begins with confusion as professionals encounter quantum concepts that challenge classical computing intuitions, experience disorientation when quantum principles violate everyday

logic, and are uncertain about how quantum technologies relate to familiar security practices. Initial confusion is a normal developmental stage rather than an indication of inadequate capability, and it requires tolerance for temporary disorientation as quantum mental models gradually form.

Confusion transitions into curiosity as professionals move beyond mere bewilderment toward active inquiry, developing questions about quantum applications, seeking quantum learning opportunities, and engaging quantum material despite persistent uncertainty. Curiosity represents a critical motivational shift, enabling sustained learning engagement necessary for the development of quantum comprehension. However, curiosity can be undermined by frustration if learning resources prove inadequate, cognitive demands are excessive, or progress indicators are absent [41].

Curiosity enables comprehension as professionals construct coherent mental models of quantum computing, rendering previously confusing concepts intelligible, achieving sufficient understanding to explain quantum principles, evaluate quantum claims, and participate meaningfully in quantum discussions. Comprehension provides intellectual mastery of quantum concepts but does not automatically translate into confidence in implementation or professional commitment, requiring additional developmental stages [41].

Comprehension supports confidence as professionals develop assurance in their quantum judgment, trusting their ability to make quantum-relevant decisions, to offer quantum opinions without excessive hedging, and to take ownership of quantum implementation recommendations. Confidence emerges through successful application of quantum knowledge, positive feedback on quantum contributions, and social validation from peers and supervisors. Confidence enables professionals to act on their quantum understanding rather than remain paralyzed by uncertainty or defer to others' quantum expertise [42].

Confidence culminates in commitment where professionals embrace quantum cybersecurity as integral to professional identity and practice, actively advocating for quantum preparation, dedicating time and energy to quantum initiatives, and persisting through quantum implementation challenges. Commitment represents the transformation from viewing quantum computing as an external requirement to internalizing quantum awareness as a core professional responsibility. This phenomenological progression emphasizes that quantum understanding involves not merely cognitive development but affective and motivational transformation, with professionals' evolving relationship to quantum computing fundamentally reshaping professional self-conception and practice orientation.

3.5. Integrative Nature of the Framework

The integrative power of the NCQU Framework lies in its recognition that quantum understanding emerges from the simultaneous operation of all these components rather than from any single element in isolation. Individual professionals bring unique identities, knowledge, emotions, and skills to quantum sense-mak-

ing, but their understanding develops through social interaction with peers and teams, within organizational contexts that enable or constrain quantum engagement, across temporal horizons connecting past, present, and future, along knowledge spectrums spanning theory to embodied practice, and through phenomenological journeys transforming confusion into commitment.

The nested structure emphasizes that outer layers not only surround but also actively shape inner layers, with organizational contexts influencing social dynamics, social processes affecting individual development, and individual interpretations feeding back to reshape social and organizational realities. The cross-cutting dimensions penetrate all layers, ensuring that temporal, epistemological, and developmental considerations inform quantum sense-making at individual, social, and organizational levels simultaneously. This multi-dimensional, multi-layered conceptualization resists reductionist explanations that attribute quantum understanding patterns to single causal factors, instead revealing complex interdependencies that require systemic intervention.

The framework directly addresses the central problem: why high quantum awareness among cybersecurity professionals fails to translate into corresponding implementation. The NCQU Framework suggests this awareness-action disconnect arises not from simple knowledge deficits but from misalignment or underdevelopment across multiple nested contexts and cross-cutting dimensions. Professionals may possess adequate abstract theoretical knowledge yet lack practical application capabilities, or individual comprehension may exist without corresponding organizational support structures, or present challenges may dominate sense-making at the expense of future anticipation, or professionals may remain stuck in confusion rather than progressing toward commitment. By illuminating multiple dimensions along which quantum understanding develops and the various contextual levels that must align for understanding to translate into implementation, the NCQU Framework provides a comprehensive diagnostic tool for identifying specific barriers to quantum adoption and targeting interventions that address precise gaps in the quantum understanding ecosystem.

The NCQU Framework's theoretical originality lies in what it integrates and reconfigures rather than in displacing any single predecessor theory. TAM and UTAUT are adoption intention models: they explain whether individuals will choose to use a technology, treating adoption as a relatively discrete behavioral decision governed by perceived usefulness, effort expectancy, and social influence. The NCQU Framework treats quantum adaptation not as a decision point but as a sustained developmental process unfolding across nested contexts, making it analytically better suited to transitions, such as post-quantum cryptography migration, where adoption spans years, involves collective as well as individual sense-making, and requires identity-level transformation rather than a single acceptance choice. Weick's sense-making theory provides the interpretive and social architecture but is not inherently layered or diagnostic; it describes how organizations construct meaning without specifying which contextual levels operate

simultaneously or how to identify where comprehension has stalled. Organizational culture theory identifies culture as a powerful moderator but does not provide a multilevel mechanism that explains the pathway from individual cognition through social dynamics to organizational action. The NCQU Framework advances on this body of theory by combining nested contextual architecture, cross-cutting temporal and epistemological dimensions, and a phenomenological developmental sequence into a single diagnostic model, one capable of pinpointing, for any given organization, precisely which context or dimension is impeding the translation of quantum awareness into quantum readiness and, ultimately, into Q-Day preparedness.

3.6. Framework Propositions

The following six propositions make the NCQU Framework's central claims explicit and invite empirical scrutiny. Each proposition links one nested layer or cross-cutting dimension to a specific, measurable outcome relevant to quantum cybersecurity readiness. Proposition 1 (Individual Layer-Identity): Security professionals whose professional identity is strongly anchored in classical cryptographic expertise will exhibit greater resistance to post-quantum cryptography adoption, operationalized as longer time-to-training enrollment, lower post-quantum implementation advocacy scores, and higher rates of quantum threat minimization language, compared with professionals whose identity is organized around adaptive security problem-solving. Proposition 2 (Social Layer-Network Effects): Security professionals embedded in peer networks characterized by quantum skepticism will demonstrate lower quantum implementation intent and longer preparation timelines than those embedded in quantum-engaged peer networks, independent of individual technical knowledge levels. Proposition 3 (Organizational Layer-Culture Primacy): Organizational culture variables, specifically innovation orientation, uncertainty tolerance, and psychological safety scores, will predict post-quantum cryptography implementation progress more strongly than organizational resource endowment or executive threat awareness ratings. Proposition 4 (Temporal Dimension-Discounting): Organizations whose planning systems operate on cycles of twelve months or fewer will systematically defer quantum preparation milestones, exhibiting preparation delay as a function of temporal discounting intensity rather than resource scarcity or technical knowledge deficit. Proposition 5 (Knowledge Spectrum Dimension-Theory-Practice Gap): Organizations in which quantum education has been limited to conceptual awareness training, without hands-on post-quantum cryptographic implementation experience, will demonstrate lower implementation capability scores and longer cryptographic inventory completion timelines than organizations with laboratory-based or applied training programs. Proposition 6 (Phenomenological Dimension-Stage Threshold): Organizations in which fewer than thirty percent of senior security professionals have progressed beyond the comprehension stage of the phenomenological journey (i.e., have not yet reached confidence or commit-

ment) will fail to generate sufficient internal advocacy momentum to initiate post-quantum cryptography migration projects within a three-year planning window.

Figure 1 shows the three nested squares, organizational (outermost), social (middle), and individual (inner), which reflect the framework's core argument that quantum understanding is never isolated. Each square simultaneously contains and shapes the layers within it, which is why the amber core sits embedded across all three.

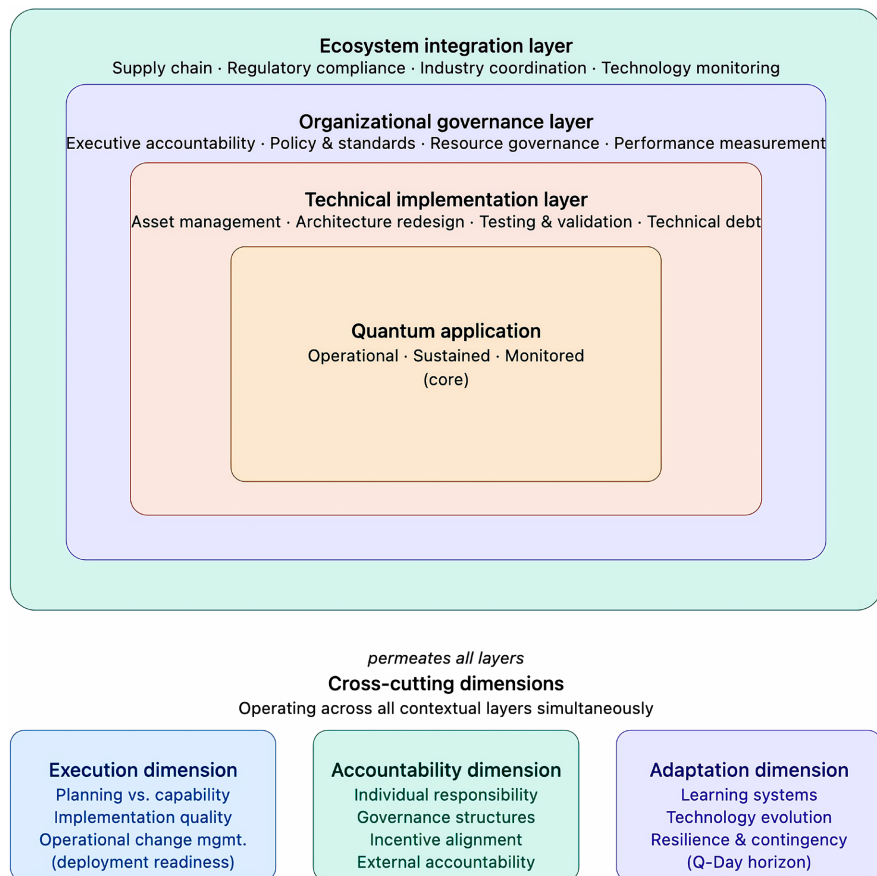


Figure 1. The NCQU framework.

The three cross-cutting dimensions below the separator are shown with dashed upward arrows to indicate that temporal, knowledge spectrum, and phenomenological journey dynamics aren't contained by any single layer; they permeate all three simultaneously. Each element is clickable to prompt a deeper explanation of that component.

The phenomenological journey, in particular (confusion → curiosity → comprehension → confidence → commitment), captures the framework's most distinctive claim: that developing quantum competence isn't purely cognitive; it's an affective and identity-level transformation. That's the progression that distinguishes the NCQU from a simple knowledge model.

4. Cyberpsychology of Quantum Cybersecurity Implementation

Section 4 examines the psychological mechanisms themselves, the cognitive biases, identity dynamics, uncertainty responses, and trust deficits that individually and collectively impede quantum cybersecurity adoption; it does so without reference to how these mechanisms interact across organizational levels, which is the work of Section 5. The cyberpsychology dimensions of quantum cybersecurity implementation reveal systematic patterns of cognitive biases, emotional responses, and social dynamics that impede the adoption of post-quantum cryptography despite technical awareness and available solutions. Understanding these psychological mechanisms provides an essential foundation for developing interventions addressing human factors alongside technical implementations.

4.1. Cognitive Biases in Quantum Threat Perception

Temporal discounting is a primary cognitive bias undermining quantum preparedness, with security professionals systematically underweighting future quantum threats relative to immediate operational demands, despite a rational awareness that quantum vulnerabilities may prove more consequential than current security challenges. Research by [5] demonstrates that security professionals discount quantum threats based on perceived temporal distance, with threats projected decades into the future receiving dramatically less attention and resources than those manifesting within months or years. This discounting effect operates even among professionals with a comprehensive technical understanding of quantum computing principles and cryptographic vulnerabilities, suggesting that cognitive biases, rather than knowledge deficits, drive inadequate preparation patterns.

The temporal discounting effect intensifies through temporal uncertainty surrounding Q-Day timelines. When threat manifestation timeframes remain ambiguous, ranging from 10 to 30 years depending on assumptions about quantum hardware advancement, professionals tend to assign threats to the most distant plausible timeline rather than the most optimistic or median projection. This psychological default toward temporal optimism creates systematic preparation delays, with organizations deferring quantum transitions until timeline clarity emerges that may never arrive before Q-Day actually occurs [11].

Ambiguity aversion toward post-quantum cryptographic solutions represents the second critical bias pattern. Security professionals prefer familiar yet quantum-vulnerable classical cryptosystems over unfamiliar quantum-resistant alternatives, despite their equivalent or superior mathematical security properties. This preference stems from uncertainty about the performance characteristics of post-quantum algorithms, implementation requirements, and compatibility challenges. [14] demonstrates that security investment decisions under quantum uncertainty violate classical probability axioms, exhibiting robust ambiguity-aversion effects in which professionals defer post-quantum adoption, awaiting additional information that reduces ambiguity about implementation outcomes. How-

ever, this information may not arrive before Q-Day, creating a cognitive trap where ambiguity aversion indefinitely postpones necessary transitions.

Optimism bias manifests as a systematic overestimation of organizational quantum preparedness and an underestimation of quantum transition complexity. Drawing on survey and interview data from cybersecurity leadership across multiple sectors, [6] documents evidence of optimism bias in organizational quantum readiness self-assessments, finding that security leaders in that sample rated their preparedness higher than objective technical benchmarks indicated; whether this pattern generalizes broadly across organizational types and national contexts remains a productive question for future empirical work. This optimism bias operates through multiple mechanisms: availability heuristic, focusing attention on quantum awareness initiatives while neglecting implementation gaps, confirmation bias, selectively attending to evidence supporting preparedness while dismissing contrary indicators, and planning fallacy, underestimating time and resources required for cryptographic transitions. These cognitive patterns create false confidence, impeding the mobilization of resources and attention necessary for adequate quantum preparation.

Expertise entrenchment among classical cryptographers constitutes the fourth critical bias pattern, in which deep expertise in classical cryptography creates cognitive barriers to the adoption of the quantum paradigm. Professionals with substantial investments in classical cryptographic knowledge demonstrate systematic resistance to post-quantum approaches through multiple mechanisms: sunk cost fallacy, maintaining commitment to classical expertise despite quantum obsolescence, confirmation bias, interpreting quantum developments in ways minimizing threat to classical knowledge, and status quo bias, preferring familiar classical systems over unfamiliar quantum alternatives. Research by [30] reveals a counterintuitive pattern where greater classical cryptography expertise correlates with increased resistance to post-quantum transitions, suggesting an expertise paradox where knowledge becomes a barrier rather than an enabler of quantum adaptation.

4.2. Professional Identity and Competence Challenges

Professional identity threat constitutes central psychological barrier to quantum cryptography adoption, particularly among cryptography specialists whose career trajectories and professional status derive from classical expertise potentially rendered partially obsolete by quantum computing. [10] document pervasive identity concerns among cryptographic professionals confronting quantum threats, manifesting as competence questioning, uncertainty about ability to master quantum domains, career relevance anxiety, concerns about professional obsolescence, and emotional defensiveness, protective responses to quantum discussions threatening established expertise.

Identity threat triggers predictable psychological responses, including minimizing the quantum threat's severity, skepticism about the viability of post-quantum

algorithms, delayed engagement with quantum learning opportunities, and avoidance of quantum discussions, potentially exposing knowledge gaps. These defensive responses serve psychological functions, protecting professional self-esteem and status, but simultaneously impede quantum adaptation necessary for continued professional effectiveness. Organizations that inadequately address identity threats experience expert resistance to quantum initiatives, regardless of technical merit, stemming not from technical disagreement but from psychological defensiveness protecting threatened expertise domains.

The expertise paradox reveals that professionals with the greatest knowledge of classical cryptography often exhibit the strongest identity threat responses and the greatest resistance to quantum transitions. This counterintuitive pattern emerges because deeper investments in expertise create greater potential losses from quantum disruption. Early-career professionals with minimal investments in classical expertise experience quantum transitions as learning opportunities rather than threats, thereby maintaining cognitive flexibility and enabling rapid quantum skill acquisition. Mid-career specialists with substantial but not yet maximal classical expertise face the strongest identity threat, experiencing quantum computing as delegitimizing their accumulated knowledge before achieving senior status and justifying their expertise investments. Senior cryptographers with established reputations may experience less acute identity threats, possessing professional capital that transcends specific technical domains and organizational influence, enabling quantum transition leadership roles.

Professional identity adaptation requires explicit organizational support, including quantum skill development opportunities demonstrating organizational commitment to expertise evolution rather than expertise replacement, recognition systems valuing quantum learning alongside classical expertise to prevent perception that quantum engagement diminishes professional standing, and career pathway articulation showing how quantum competencies enhance rather than threaten professional advancement. Organizations successfully managing quantum transitions provide identity adaptation scaffolding, enabling professionals to integrate quantum knowledge into rather than replacing existing professional self-conceptions, framing quantum expertise as professional evolution rather than disruption.

4.3. Uncertainty Tolerance and Decision-Making under Ambiguity

Quantum security presents extreme uncertainty across multiple dimensions, including hardware development timelines, attack capability thresholds, optimal migration strategies, and appropriate preparedness investments. Individual and organizational capacity to function effectively amid this uncertainty, as well as uncertainty tolerance, substantially predict quantum readiness outcomes. Research identifies distinct patterns in how security professionals and organizations respond to quantum uncertainty, ranging from premature certainty to perpetual deferral, with structured uncertainty tolerance enabling the most effective navigation [37].

Premature certainty manifests when professionals or organizations adopt specific quantum solutions before standards solidify or adequate evaluation occurs, driven by discomfort with uncertainty and desire for resolution. Early post-quantum algorithm commitments may prove problematic if selected algorithms prove to have unexpected vulnerabilities or if standardization processes converge on alternative approaches. Premature certainty provides psychological comfort through uncertainty reduction but introduces implementation risks and potential need for costly solution changes. Organizations exhibiting premature certainty typically demonstrate low tolerance for uncertainty, preferring potentially suboptimal certainty over ambiguous but potentially superior alternatives.

Perpetual deferral represents the opposite response pattern, in which professionals or organizations continuously postpone quantum decisions, awaiting the resolution of uncertainty that never adequately arrives. Deferral provides psychological comfort by avoiding difficult choices amid ambiguity, but creates preparation failures when decisions are postponed until quantum threats materialize. Organizations exhibiting perpetual deferral rationalize inaction through various mechanisms: emphasizing timeline uncertainty to justify delays, requiring certainty levels that are unattainable before Q-Day, or assigning quantum responsibility without providing the resources or authority necessary for effective action. Perpetual deferral often masks underlying intolerance of uncertainty, with ambiguity avoidance driving continuous delay rather than rational decision-making under uncertainty.

Structured uncertainty tolerance represents an optimal response pattern, acknowledging unknowns while establishing adaptive decision frameworks operating under ambiguity. Organizations demonstrating structured uncertainty tolerance implement scenario-based planning that accounts for multiple quantum development trajectories, cryptographic agility that enables algorithm substitution as uncertainties resolve, incremental implementation approaches that provide flexibility as standards emerge, and continuous reassessment processes that adjust strategies as the quantum landscape evolves. Structured uncertainty tolerance maintains forward momentum amid ambiguity, avoiding premature commitment to potentially suboptimal solutions [9].

Metacognitive awareness of uncertainty responses and understanding one's own uncertainty tolerance patterns and biases enable more effective quantum decision-making. Professionals recognizing personal tendencies toward premature certainty or perpetual deferral can implement compensatory strategies, including seeking diverse perspectives, challenging natural inclinations, establishing decision-forcing mechanisms preventing indefinite postponement, and developing comfort with provisional decisions subject to revision as uncertainties resolve. Organizations benefit from metacognitive reflection on institutional uncertainty management patterns, identifying whether organizational culture systematically drives toward either premature certainty or perpetual deferral, and implementing structural countermeasures to address identified tendencies.

4.4. Trust and Verification in Post-Quantum Systems

Trust in post-quantum cryptographic systems faces distinctive challenges stemming from the novelty of mathematical foundations, limited operational history, and ongoing standardization processes. Classical cryptosystems benefit from decades of cryptanalytic scrutiny, real-world deployment experience, and professional familiarity, which breed confidence in their security properties. Post-quantum alternatives lack this accumulated trust foundation, creating psychological barriers to adoption beyond technical security equivalence [35].

Mathematical trust development requires security professionals to develop confidence in post-quantum mathematical foundations, including lattice problems, code-based cryptography, and hash-based signatures. However, these mathematical structures receive less emphasis in typical computer science and cryptography education than number-theoretic problems underlying classical cryptography. Professionals may intellectually accept expert assurances about post-quantum security while emotionally maintaining distrust stemming from unfamiliarity. This trust deficit impedes post-quantum advocacy and implementation leadership, with professionals reluctant to stake their reputations on cryptographic approaches they do not adequately understand at an intuitive level.

Implementation trust involves confidence that post-quantum cryptographic implementations correctly instantiate mathematical security properties without introducing vulnerabilities through coding errors, side-channel leakage, or integration failures. Classical cryptographic implementations benefit from mature libraries, extensive testing, and proven deployment patterns. Post-quantum implementations remain comparatively immature, with fewer battle-tested libraries, less deployment experience, and ongoing discovery of implementation vulnerabilities. Security professionals accustomed to vetted classical implementations are uncertain about the trustworthiness of post-quantum implementations, creating reluctance to deploy despite theoretical security adequacy.

Performance trust concerns whether post-quantum systems will satisfy operational requirements, including latency constraints, throughput demands, and resource availability. Post-quantum algorithms generally require larger keys, longer signatures, and different computational profiles than classical alternatives. Performance characteristics vary across post-quantum algorithm families, with some approaches offering better size characteristics but worse computational performance and vice versa. Security professionals must develop confidence that post-quantum performance profiles prove acceptable for specific applications, requiring hands-on experimentation and performance measurement rather than abstract assurances.

Verification challenges arise because post-quantum security properties cannot be directly empirically validated before Q-Day. Classical cryptography security can be continuously validated through attempted attacks, with the absence of successful breaks providing ongoing confidence. Post-quantum security against quantum attacks cannot be validated in the same way until cryptographically rel-

evant quantum computers become available, creating a verifiability gap in which professionals must trust theoretical security without empirical demonstration of quantum attack resistance. This verifiability gap creates psychological discomfort, as professionals are unable to establish confidence through their preferred verification mechanisms.

Table 1 outlines four key cyberpsychology dimensions influencing the implementation of quantum cybersecurity. The first dimension, cognitive biases, refers to mental shortcuts and tendencies such as temporal discounting, ambiguity aversion, optimism bias, and expertise entrenchment. These biases often impede resource allocation and decision-making related to post-quantum adoption, even when technical requirements are understood. The second dimension addresses professional identity challenges, noting that the transition to quantum cybersecurity can threaten the identity of classical cryptography specialists. This can provoke defensiveness, resistance, and slow learning investments, particularly in organizations that lack strong support for such transitions.

Table 1. Cyberpsychology dimensions of quantum cybersecurity implementation.

Dimension	Key Insight
Cognitive Biases	Temporal discounting, ambiguity aversion, optimism bias, and expertise entrenchment impede resource allocation and decision-making for post-quantum adoption despite technical awareness.
Professional Identity Challenges	Quantum transitions threaten identity for classical cryptography specialists, leading to defensiveness, resistance, and delayed learning investments without organizational support.
Uncertainty Tolerance	Responses to ambiguity range from premature certainty to perpetual deferral, with structured uncertainty tolerance and adaptive decision-making frameworks proving most effective.
Trust in Post-Quantum Systems	Trust barriers involve mathematical unfamiliarity, implementation immaturity, performance concerns, and the inability to empirically validate post-quantum algorithms before Q-Day.

The third dimension, uncertainty tolerance, highlights how decision-makers react to ambiguity, either by making premature decisions or continually deferring action. The most effective approaches involve structured methods for tolerating uncertainty and adapting decisions as new information emerges. Finally, the dimension of trust in post-quantum systems reveals several barriers to trust. These include unfamiliar mathematical theories, the relative immaturity of implementations, concerns about system performance, and the fundamental issue that post-

quantum algorithms cannot be empirically validated before quantum computers become widespread. Together, these dimensions illustrate the psychological and organizational factors that are just as critical as technical challenges in successfully adopting quantum cybersecurity solutions.

5. Application of the NCQU Framework to Q-Day Preparedness

Whereas Section 4 identified the constituent psychological mechanisms of quantum adoption failure, Section 5 uses the NCQU Framework as an integrative lens to show how those mechanisms manifest differently and interact in compounding ways when viewed through the nested layers of the individual, social, and organizational, and across the three cross-cutting dimensions. The NCQU Framework provides a diagnostic lens for understanding organizational Q-Day preparedness failures, revealing how misalignments across nested contexts and cross-cutting dimensions create systematic barriers to quantum adoption despite technical awareness and available solutions. This section applies framework components to illuminate specific mechanisms through which individual, social, and organizational factors interact to produce inadequate quantum readiness.

5.1. Individual-Level Barriers Through the NCQU Lens

At the individual experience layer, quantum preparedness barriers manifest as professional identity conflicts, knowledge-skill gaps, emotional responses, and developmental-stage positioning. Security professionals who perceive quantum computing as an identity threat exhibit reduced engagement with quantum learning, delayed quantum skill development, and resistance to quantum implementation advocacy, regardless of rational threat awareness. This identity barrier operates independently of technical knowledge, with professionals possessing adequate quantum comprehension nonetheless avoiding quantum applications threatening established expertise domains [10].

Knowledge spectrum misalignment creates barriers when professionals develop abstract theoretical quantum understanding without corresponding practical application capabilities or tacit implementation knowledge. Many security professionals achieve the comprehension stage in the phenomenological journey, successfully explaining quantum principles and evaluating quantum claims, without progressing to the confidence stage, enabling quantum implementation leadership. This comprehension-confidence gap reflects knowledge spectrum positioning, emphasizing abstract theory without sufficient practical application experience. Organizations addressing this barrier must provide hands-on quantum implementation opportunities that enable the translation of theoretical knowledge into practical competencies and the development of tacit judgment.

Emotional responses, including anxiety about quantum complexity, frustration with the demands of quantum learning, and defensive reactions to quantum paradigm shifts, create affective barriers independent of cognitive understanding.

Professionals experiencing quantum topics as anxiety-inducing avoid quantum discussions, minimize quantum learning time and investment, and rationalize deferring quantum preparation despite intellectual awareness of its necessity. These emotional barriers require psychological interventions that address affective responses rather than merely transfer cognitive knowledge, including stress management support, confidence-building through graduated quantum challenges, and emotional validation acknowledging quantum learning difficulties.

Temporal dimension misalignment at the individual level manifests when professionals' sense-making emphasizes past experiences or present challenges while inadequately incorporating future quantum implications. Retrospective focus on past technological transitions may generate inappropriate analogies when quantum discontinuities differ fundamentally from historical patterns. Present-focused on immediate operational demands crowds out future-oriented quantum preparation when temporal discounting systematically underweights distant threats. Effective quantum readiness requires temporal integration connecting past experience interpretation, present challenge management, and future anticipation in a balanced fashion.

5.2. Social-Level Challenges in Quantum Understanding Development

The social and collaborative layer reveals how peer networks, knowledge-sharing mechanisms, team dynamics, and communities of practice shape patterns of quantum understanding that extend beyond individual psychology. Network effects amplify or dampen individual quantum engagement through social influence, peer validation, and collective sense-making processes. Professionals embedded in quantum-skeptical peer networks receive continuous reinforcement for deferring quantum preparation, encountering quantum-minimization narratives, emphasis on implementation complexity, and timeline optimism that discourages proactive quantum action. Conversely, quantum-engaged networks provide learning support, implementation encouragement, and validation for quantum preparation investments despite timeline uncertainties [24].

Knowledge-sharing effectiveness determines whether quantum expertise concentrates in specialist enclaves or diffuses broadly across security organizations. Siloed quantum knowledge creates single points of failure, where quantum preparedness depends on specific individuals whose departure would catastrophically reduce the organization's quantum capability. Inadequate knowledge-sharing mechanisms, the absence of quantum training programs, inaccessible quantum documentation, or insufficient quantum mentorship impede the diffusion of quantum understanding, despite individual quantum experts possessing relevant knowledge. Psychological safety for quantum knowledge sharing is particularly critical given quantum complexity and professional identity sensitivities, as professionals are reluctant to acknowledge quantum knowledge gaps when organizational culture punishes uncertainty.

Team dynamics shape quantum implementation approaches through collective decision-making processes, power structures, and communication patterns. Teams exhibiting groupthink may prematurely converge on quantum strategies without adequate critical evaluation, driven by the desire for consensus over thorough quantum assessment. Teams with power imbalances may defer to senior members' quantum views regardless of accuracy, which is particularly problematic when those senior members demonstrate quantum skepticism rooted in entrenchment in classical expertise. Teams lacking psychological safety discourage the acknowledgment of quantum uncertainty, forcing premature claims of quantum confidence rather than enabling productive engagement with quantum ambiguities.

Communities of practice influence quantum understanding through establishing professional norms, best practices, and collective standards for quantum preparedness. However, community influence creates a double-edged dynamic, enabling rapid quantum knowledge diffusion when communities embrace quantum preparation, but also constraining quantum thinking when dominant paradigms discourage a sense of quantum urgency. Professional communities that emphasize excellence in classical cryptography may implicitly devalue quantum competencies, creating status disincentives for quantum skill development. Communities exhibiting collective temporal discounting normalize quantum preparation deferral, establishing professional norms in which delayed quantum action is accepted practice rather than a preparedness failure requiring correction.

5.3. Organizational-Level Impediments to Quantum Readiness

The organizational context layer reveals systemic factors shaping quantum preparedness beyond individual and social processes. Organizational culture represents the primary determinant of quantum readiness, with innovation-oriented cultures facilitating quantum exploration while risk-averse cultures create barriers to post-quantum adoption despite quantum vulnerabilities in current systems. Research by [6] provides evidence consistent with the claim that organizational culture variables, specifically innovation orientation and psychological safety, show stronger associations with quantum preparedness indicators than technical resource endowment or stated threat awareness; this finding, while preliminary, is theoretically coherent with the organizational psychology literature and frames cultural transformation as a high-priority intervention target warranting replication in larger, more representative samples.

Resource allocation patterns signal organizational quantum priorities regardless of stated strategic intentions. Organizations claiming quantum importance but allocating minimal training budgets, implementation resources, or professional development time reveal quantum preparation as a rhetorical rather than an operational priority. Resource scarcity creates zero-sum competition between quantum preparation and immediate operational demands, with temporal discounting systematically favoring present over future investments. However, resource abundance alone proves insufficient; organizations with substantial re-

sources may still demonstrate inadequate quantum preparation when cultural factors, leadership attention, or strategic priorities fail to direct resources toward quantum initiatives [9].

Leadership vision and quantum literacy fundamentally shape organizational quantum trajectories through attention direction, resource authorization, and strategic framing. Quantum-engaged leaders maintain organizational focus on quantum preparation despite competing priorities and uncertain timelines, establishing quantum initiatives as legitimate claims on organizational resources and professional attention. Leaders lacking quantum literacy struggle to evaluate technical recommendations, oscillating between premature commitment to inadequately vetted solutions and perpetual deferral in the face of unattainable certainty. Leadership quantum literacy requires sufficient understanding to assess the quality of recommendations without attempting comprehensive technical mastery, while recognizing limitations and maintaining strategic oversight responsibility.

Strategic priority positioning determines whether quantum cybersecurity receives organizational commitment or remains perpetually subordinated to more immediate concerns. Organizations that treat quantum security as a technical implementation project rather than a strategic transformation systematically underestimate the complexity and scope of the quantum transition. Strategic quantum framing emphasizes long-term security posture implications, competitive positioning considerations, and organizational resilience requirements rather than narrow technical algorithm substitution. This strategic framing enables quantum initiatives to compete effectively for resources against immediate operational demands, regulatory compliance requirements, and revenue-generating activities otherwise dominating organizational attention.

5.4. Cross-Cutting Dimension Interactions in Q-Day Preparation

The temporal dimension creates systematic challenges in preparation through temporal discounting, timeline uncertainty, and future-focused difficulties. Organizations demonstrating strong present focus maintain attention on immediate security threats, operational incidents, and short-term performance metrics while systematically underweighting quantum threats that manifest over extended timelines. This temporal orientation reflects not merely individual cognitive biases but also organizational structures, incentive systems, and cultural patterns that reinforce short-term thinking. Quarterly performance reviews, annual planning cycles, and immediate threat-response protocols direct attention to present challenges, while quantum preparation spanning years or decades remains perpetually deferred [5].

Timeline uncertainty exacerbates temporal challenges by providing a rationale for deferring continuous quantum preparation. When Q-Day projections range from 10 to 30 years, organizations systematically select the most optimistic timelines, justifying delayed action rather than worst-case timelines demanding immediate preparation. This timeline optimism operates through motivated reason-

ing, where the desired conclusion, quantum preparation can be safely deferred, influences timeline interpretation and credibility assessment. Organizations must develop a temporal orientation that embraces the precautionary principle amid timeline uncertainty, preparing for the earliest plausible Q-Day scenarios while maintaining adaptation capacity if quantum advances prove slower than anticipated.

The knowledge spectrum dimension reveals preparation failures stemming from theory-practice gaps, in which organizations develop abstract quantum awareness without corresponding practical implementation capabilities. Security professionals widely understand the principles of Shor's algorithm, recognize quantum cryptographic vulnerabilities, and acknowledge the necessity of post-quantum cryptography at an abstract theoretical level. However, this theoretical knowledge remains disconnected from practical competencies, including cryptographic inventory assessment, post-quantum algorithm selection, integration architecture design, and migration project management. Organizations must enable knowledge spectrum progression from abstract theory through practical application to tacit judgment and embodied practice, requiring hands-on quantum implementation experience rather than merely conceptual quantum education.

The phenomenological journey dimension illuminates how professionals' developmental stage positioning affects organizational quantum readiness. Organizations where most security professionals remain in the confusion or curiosity stages lack the critical mass of confident quantum advocates needed to build implementation momentum. Organizational quantum readiness requires sufficient professionals to progress to the confidence and commitment stages, where they actively champion quantum initiatives, allocate personal time to quantum learning, and persist through quantum implementation obstacles. Organizations can accelerate phenomenological progression through targeted interventions, including confusion normalization, reducing anxiety about temporary disorientation, cultivating curiosity through compelling quantum use cases, providing comprehension support via effective quantum education, building confidence through successful quantum implementation experiences, and reinforcing commitment through recognition systems that value quantum engagement.

6. Implications and Recommendations

The section on implications and recommendations explores critical strategic priorities across four domains: security professionals, organizations, policymakers, and educators, to enable effective adaptation and preparedness for quantum transitions. For security professionals, a focus on cognitive flexibility, tolerance for uncertainty, and hands-on quantum implementation experience is vital for fostering adaptive expertise and overcoming psychological barriers associated with evolving quantum paradigms. In the organizational domain, the creation of a quantum-supportive culture, systematic education programs, and temporal orientation mechanisms ensures sustained quantum preparedness while mitigating

organizational resistance. Policymakers and standards bodies are encouraged to craft balanced regulatory frameworks, invest in workforce development initiatives, and provide actionable guidance that integrates both technical and psychological dimensions. Finally, educators and trainers must embed cognitive adaptation, progressive quantum skill development, and professional identity support into curricula to address the holistic challenges of quantum cybersecurity learning. Together, these strategies aim to comprehensively address technical, psychological, and cultural aspects of quantum readiness.

6.1. Implications for Security Professionals

Security professionals must recognize quantum transitions as requiring not merely technical learning but psychological adaptation, encompassing professional identity evolution, the development of uncertainty tolerance, and metacognitive awareness of cognitive biases that affect quantum decision-making. The NCQU Framework suggests several professional development priorities. First, professionals should cultivate adaptive expertise that emphasizes cognitive flexibility and a learning orientation over routine expertise optimized for classical paradigms. This involves approaching quantum computing as an opportunity for professional growth rather than a threat to established competencies, reframing quantum learning as the evolution of expertise rather than its replacement.

Second, professionals must develop a structured tolerance for uncertainty, enabling effective decision-making amid quantum ambiguities rather than oscillating between premature certainty and perpetual deferral. This requires metacognitive awareness of personal uncertainty-response patterns, recognition of cognitive biases, including temporal discounting and ambiguity aversion, and deliberate implementation of compensatory strategies that counteract natural cognitive tendencies. Professionals should establish personal decision-making frameworks that operate under uncertainty, including scenario-based planning, incremental commitment strategies, and continuous reassessment mechanisms.

Third, professionals should pursue hands-on experience in quantum implementation, enabling progression along the knowledge spectrum from abstract theory to practical competence and tacit judgment. Conceptual understanding of quantum physics is necessary but insufficient for effective quantum cybersecurity practice. Professionals must seek quantum implementation opportunities, including post-quantum algorithm experimentation, quantum-resistant architecture prototyping, and cryptographic agility implementation. These practical experiences develop embodied quantum practice where quantum considerations become intuitive rather than requiring conscious deliberation.

6.2. Implications for Organizations

Organizations must address quantum preparedness as a socio-technical challenge requiring coordinated attention to psychological, social, and organizational factors alongside technical implementations. The NCQU Framework identifies sev-

eral organizational intervention priorities. First, organizations should cultivate a quantum-supportive culture characterized by an innovation orientation, tolerance for uncertainty, an emphasis on learning, and psychological safety. Cultural transformation proves more predictive of quantum readiness than resource allocation or technical awareness alone, suggesting culture as the primary leverage point for organizational quantum preparation [6].

Cultural intervention strategies include leadership quantum literacy development, enabling informed strategic guidance, recognition systems valuing quantum learning alongside classical expertise to prevent status disincentives for quantum engagement, psychological safety protocols enabling productive acknowledgment of quantum uncertainties and knowledge gaps, and narrative framing positioning quantum transitions as organizational evolution rather than crisis response. Organizations demonstrating a quantum-supportive culture maintain quantum mindfulness despite extended timelines and competing priorities, sustaining attention to future quantum threats while managing current operational demands.

Second, organizations must implement systematic quantum education programs that address the progression of knowledge from abstract theory through practical application to tacit judgment. Traditional security training that emphasizes conceptual knowledge transfer is insufficient for quantum transitions that require hands-on implementation experience. Effective quantum education incorporates graduated implementation challenges, mentorship from quantum-experienced professionals, and safe experimental environments that enable quantum learning without operational risk. Organizations should establish quantum communities of practice that facilitate peer learning, knowledge sharing, and collective sense-making, thereby supporting individual quantum development.

Third, organizations should develop temporal orientation mechanisms that counteract temporal discounting and maintain future focus despite present operational demands. Scenario-based planning exercises that make quantum threats psychologically proximate through vivid Q-Day scenarios can counteract psychological distance effects. Establishing quantum preparation milestones creates intermediate goals, preventing perception of quantum transitions as remote future concerns. Integrating quantum considerations into present security decisions through quantum impact assessment requirements maintains quantum mindfulness across organizational activities. These temporal intervention strategies establish quantum preparation as an ongoing organizational priority rather than a discretionary future initiative.

Fourth, organizations must provide professional identity adaptation support, enabling security professionals to integrate quantum competencies without experiencing quantum engagement as threatening established expertise. Identity adaptation interventions include quantum learning opportunities demonstrating organizational support for expertise evolution, career pathway articulation showing quantum competency enhancement of professional advancement prospects, and

recognition systems validating quantum contributions alongside classical security expertise. Organizations successfully navigating quantum transitions frame quantum competency development as professional evolution enhancing rather than threatening career trajectories.

6.3. Implications for Policymakers and Standards Bodies

Policymakers and standards development organizations play critical roles in shaping organizational quantum preparation through regulatory requirements, industry guidance, and the provision of resources. The NCQU Framework identifies several opportunities for policy intervention. First, regulatory frameworks should incorporate sunset provisions for quantum-cryptographic algorithms, establishing clear timelines for deprecation. These regulatory deadlines counteract temporal discounting by creating legally enforceable quantum transition requirements, preventing indefinite deferral. However, sunset provisions must balance urgency against implementation feasibility, avoiding precipitous timelines that generate compliance resistance while preventing excessive timeline extensions that enable continued preparation neglect.

Second, government agencies should invest in quantum security workforce development programs that address both the technical and psychological dimensions of quantum transitions. Workforce development initiatives should emphasize hands-on quantum implementation training, enabling progression across the knowledge spectrum, providing professional development support, facilitating identity adaptation, and offering guidance on organizational change management, helping institutions navigate quantum cultural transformations. These programs prove particularly critical for resource-constrained organizations lacking internal quantum expertise development capabilities.

Third, standards bodies should provide clear guidance on best practices for implementing post-quantum cryptography while acknowledging the remaining uncertainties. Guidance documents must balance confidence, which enables adoption decisions, with humility regarding the evolving quantum landscape. Premature certainty claims risk credibility damage if recommendations require revision, while excessive emphasis on uncertainty enables perpetual deferral. Standards bodies should explicitly address psychological barriers to post-quantum adoption, providing not merely technical implementation specifications but also organizational change-management frameworks and professional-development guidance to support quantum transitions.

6.4. Implications for Education and Training

Educational institutions and professional training organizations must reconceptualize quantum cybersecurity education as requiring psychological adaptation support alongside technical knowledge transfer. The NCQU Framework identifies several educational intervention priorities. First, quantum curricula should explicitly address cognitive challenges, including the transformation of mental mod-

els from deterministic to probabilistic computation, the development of quantum intuition that transcends classical computing assumptions, and the cultivation of uncertainty tolerance that enables effective functioning amid quantum ambiguities.

Educational approaches should acknowledge and normalize confusion as an expected developmental stage rather than an indication of inadequate capability, reducing anxiety, and potentially triggering quantum learning avoidance. Curricula should provide progressive scaffolding for skill development, enabling learners to build quantum comprehension gradually rather than confronting full quantum complexity simultaneously. Metacognitive training should help learners recognize cognitive biases that affect quantum understanding, including temporal discounting, ambiguity aversion, and expertise entrenchment patterns that impede quantum adaptation.

Second, professional training programs must emphasize hands-on quantum implementation experience, enabling progression of knowledge beyond abstract theory. Traditional lecture-based cybersecurity education proves insufficient for quantum contexts that require the development of practical competence. Effective quantum training incorporates laboratory exercises with post-quantum cryptographic libraries, implementation projects addressing realistic migration scenarios, and troubleshooting experiences developing tacit judgment about quantum security challenges. These practical components should occur in safe learning environments where implementation errors generate learning opportunities rather than operational consequences or professional embarrassment.

Third, educational initiatives should explicitly address professional identity adaptation rather than assume that quantum learning occurs without identity considerations. Training should frame quantum competency development as professional evolution, enhancing career prospects rather than threatening established expertise. Case studies should highlight successful professional quantum transitions demonstrating the feasibility of quantum adaptation. Mentorship programs should connect learners with quantum-experienced professionals modeling successful identity integration. These identity-focused interventions reduce psychological barriers that purely technical training cannot address.

7. Discussion

The NCQU Framework advances theoretical understanding of quantum cybersecurity adoption by revealing how individual, social, and organizational psychological factors interact to shape quantum preparedness outcomes. Previous research examining quantum security challenges primarily emphasized technical dimensions, including algorithm development, implementation complexity, and performance characteristics. While acknowledging organizational barriers, prior work typically treated psychological factors as secondary considerations rather than primary determinants of quantum readiness. The NCQU Framework repositions psychological dimensions as central to quantum cybersecurity transitions, demonstrating that awareness-action disconnects stem fundamentally from cog-

nitive biases, identity threats, and organizational dynamics rather than merely technical deficiencies or resource constraints.

The framework's nested structure illuminates how quantum understanding emerges from the simultaneous operation across multiple levels rather than from any single causal factor. Individual quantum comprehension development occurs within social networks, shaping interpretation and validation, embedded within organizational contexts, enabling or constraining quantum engagement. This multi-level conceptualization resists both individualist explanations that attribute quantum readiness solely to professional capabilities and structuralist accounts that emphasize only organizational factors. Instead, the framework reveals complex interdependencies that require systemic interventions addressing individual, social, and organizational dimensions in coordination.

The cross-cutting dimensions provide analytical tools for examining how temporal orientation, knowledge-spectrum positioning, and the phenomenological development stage influence quantum understanding across all nested levels. Temporal dimension analysis reveals how past retrospection, present focus, and future anticipation interact to shape quantum sense-making, explaining why organizations with high present focus systematically defer quantum preparation despite rational awareness of future threats. Knowledge spectrum analysis illuminates theory-practice gaps where abstract quantum awareness fails to translate into implementation capability. Phenomenological journey mapping enables the identification of developmental-stage bottlenecks where professionals remain stuck in confusion or comprehension without progressing to the confidence and commitment stages necessary for effective quantum advocacy.

However, the framework also reveals limitations requiring acknowledgment. The nested contexts model emphasizes comprehensive understanding but may prove overwhelming for practitioners seeking targeted interventions. Organizations require diagnostic tools that identify the highest-priority barriers rather than comprehensive assessments that address all framework dimensions simultaneously. Future research should develop abbreviated assessment instruments enabling rapid identification of critical quantum readiness gaps while maintaining theoretical fidelity to the framework's multi-dimensional conceptualization. Additionally, the framework emphasizes qualitative understanding processes but provides limited guidance for the quantitative assessment of quantum readiness levels across framework dimensions. Development of validated measurement instruments would enable empirical research to test framework predictions and evaluate intervention effectiveness.

Several boundary conditions merit explicit acknowledgment to help readers assess the NCQU Framework's scope of applicability. The framework was developed with primary reference to medium-to-large organizations in sectors where cryptographic security is operationally significant, such as financial services, defense, healthcare, and critical infrastructure, and its diagnostic logic assumes that organizations have the structural differentiation (distinct IT, security, and leadership

roles) necessary for the nested layers to operate independently. In smaller organizations or flat-hierarchy environments, individual, social, and organizational dynamics may be so intertwined as to collapse distinctions the framework treats as analytically separable; in these contexts, the framework may require adaptation to a two-level rather than three-level nested structure.

The framework also assumes that post-quantum cryptography is a meaningful organizational obligation, which is most directly true for organizations operating in regulated environments or managing high-value data assets; for organizations with low cryptographic exposure, certain layers, particularly the organizational culture and strategic priorities dimensions, will exert less influence on quantum readiness outcomes. Finally, the phenomenological journey dimension describes a progression theorized from the literature on professional development and technology adoption in Western organizational contexts; its generalizability across national cultures with different orientations toward uncertainty, hierarchy, and professional identity warrants investigation before the framework is applied prescriptively in non-Western settings. These boundary conditions do not diminish the framework's utility but define the conditions under which its propositions are most directly testable and its interventions most directly applicable.

Returning to the three research questions posed in the Introduction allows the framework's contributions to be assessed directly. The first question asked how cognitive biases and psychological mechanisms explain inadequate organizational Q-Day preparation despite widespread technical awareness: the NCQU Framework answers that awareness without action is the predictable result of temporal discounting systematically underweighting distant threats, ambiguity aversion toward unfamiliar post-quantum alternatives, optimism bias inflating perceived readiness, and expertise entrenchment among classical cryptographers whose professional identity resists paradigm disruption, mechanisms that operate below the threshold of rational deliberation and therefore cannot be resolved through technical information provision alone. The second question asked what role professional identity, organizational culture, and social dynamics play in post-quantum cryptography adoption patterns: the framework identifies these as primary rather than secondary determinants, demonstrating that the social layer normalizes or counteracts quantum preparation through peer network effects and community-of-practice norms, that organizational culture predicts implementation progress more reliably than resource endowment, and that professional identity threat among cryptographic specialists generates systematic defensiveness whose organizational cost exceeds any individual's awareness of their own resistance. The third question asked how cyberpsychology interventions can enhance quantum readiness by addressing psychological barriers alongside technical implementations: the framework specifies that effective intervention must be multi-level and dimensionally targeted, addressing temporal discounting through scenario-based planning and milestone-driven urgency, identity threat through adaptive expertise framing and career-integrated recognition, knowledge spectrum gaps through la-

laboratory-based implementation training, and organizational culture through leadership quantum literacy development and psychological safety protocols, with no single intervention sufficient when multiple nested levels remain misaligned.

8. Conclusions

The NCQU framework provides a comprehensive theoretical foundation for examining how cybersecurity professionals and organizations develop quantum comprehension and navigate transitions to post-quantum cryptography. By conceptualizing quantum understanding as emerging from nested individual, social, and organizational contexts operating across temporal, epistemological, and phenomenological dimensions, the framework illuminates psychological barriers that impede quantum adoption despite technical awareness and available solutions. The awareness-action disconnect characterizing current quantum preparedness reflects not technical deficiencies but systematic patterns of cognitive biases, professional identity challenges, organizational culture dynamics, and social influence processes.

Temporal discounting systematically underweights future quantum threats relative to immediate operational demands, leading to preparation deferral despite rational threat acknowledgment. Expertise entrenchment among classical cryptographers creates resistance to post-quantum paradigms, threatening the accumulation of professional knowledge. Ambiguity aversion toward quantum-resistant alternatives with uncertain performance characteristics impedes proactive adoption decisions. Optimism bias leads to a systematic overestimation of organizational quantum readiness. These psychological patterns operate not as individual failures but as predictable cognitive responses to quantum threats characterized by uncertain timelines, paradigmatic disruption, and challenges to professional identity.

Professional identity threat constitutes a particularly significant barrier, with cryptography specialists experiencing quantum computing as potentially rendering classical expertise partially obsolete. This identity challenge triggers defensive responses, including threat minimization, quantum learning avoidance, and post-quantum skepticism, that serve psychological functions protecting professional self-conception but simultaneously impede necessary quantum adaptation. Organizations must provide explicit identity-adaptation support that enables professionals to integrate quantum competencies rather than replace existing professional self-conceptions.

Organizational culture emerges as the primary determinant of quantum readiness, with innovation orientation, uncertainty tolerance, learning emphasis, and psychological safety predicting quantum preparedness more strongly than technical resources or threat awareness alone. Organizations demonstrating quantum-supportive culture maintain quantum mindfulness despite extended timelines and competing priorities, whereas risk-averse or hierarchical cultures systematically defer quantum preparation regardless of stated strategic intentions. Cultural

transformation represents a critical intervention leverage point, requiring leadership quantum literacy, recognition systems that value quantum engagement, and psychological safety protocols that enable productive uncertainty acknowledgment.

The framework's practical implications emphasize integrating psychological readiness with technical implementations rather than treating quantum transitions as purely technical challenges. Effective quantum preparation requires scenario-based planning to counteract temporal discounting, metacognitive training to enhance paradigm flexibility, professional identity adaptation support, hands-on implementation experience to enable knowledge spectrum progression, and organizational psychological safety to enable productive engagement with quantum uncertainty. These psychological interventions prove essential complements to technical implementations, including post-quantum algorithm deployment, development of cryptographic agility, and design of quantum-resistant architectures.

Future research should empirically test the framework's predictions regarding quantum readiness determinants, develop validated assessment instruments to measure quantum understanding across the framework's dimensions, and evaluate the effectiveness of interventions addressing identified psychological barriers. Longitudinal studies tracking the development of quantum comprehension across phenomenological stages would illuminate developmental trajectories and identify critical transition points. Cross-cultural research examining patterns of quantum understanding across national and organizational cultures would enhance the framework's generalizability. Integration with organizational change management theories would strengthen prescriptive guidance for quantum transition leadership.

The quantum computing revolution tests not merely technical capabilities but also psychological resilience, the individual and collective capacity to maintain attention on uncertain future threats, tolerate the ambiguity inherent in quantum preparation, adapt professional identities to incorporate quantum expertise, and sustain organizational commitment despite extended timelines and competing priorities. Organizations that successfully navigate Q-Day will demonstrate not only cryptographic algorithmic mastery but also psychological readiness, enabling effective adaptation to paradigmatic uncertainty. The NCQU Framework provides a theoretical foundation and practical guidance for developing this essential psychological dimension of quantum cybersecurity preparedness, recognizing that technical solutions alone cannot overcome cognitive biases, identity threats, and organizational dynamics, ultimately determining whether organizations emerge from quantum transitions with security intact or face cryptographic collapse with catastrophic consequences. Understanding these nested contexts of quantum comprehension represents a critical prerequisite for organizational survival in the post-quantum era.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

- [1] Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., *et al.* (2022) Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST Interagency/Internal Report (NISTIR), 8309.
- [2] Bindel, N., Herath, U., McKague, M. and Stebila, D. (2017) Transitioning to a Quantum-Resistant Public Key Infrastructure. In: Lange, T. and Takagi, T., Eds., *International Workshop on Post-Quantum Cryptography*, Springer International Publishing, 384-405. https://doi.org/10.1007/978-3-319-59879-6_22
- [3] Mosca, M. (2018) Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*, **16**, 38-41. <https://doi.org/10.1109/msp.2018.3761723>
- [4] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, 20-22 November 1994, 124-134. <https://doi.org/10.1109/sfcs.1994.365700>
- [5] Ayanbode, T., Sahani, Y., Srinivasan, K., Kim, D.J. and Kang, K. (2024) Temporal Discounting in Quantum Security: An Experimental Investigation of Cybersecurity Professionals' Responses to Future Quantum Threats. *Computers & Security*, **137**, Article ID: 103614.
- [6] Possati, L.M. (2024) Quantum Computing and Organizational Mindfulness: Pre-Par-
ing for Paradigm Shifts in Cybersecurity. *Technology in Society*, **77**, Article ID: 102547.
- [7] National Institute of Standards and Technology (2024) Post-Quantum Cryptography Standardization: Announcing Four Candidate Algorithms. <https://csrc.nist.gov/Projects/post-quantum-cryptography>
- [8] Csenkey, B. and Bindel, N. (2023) Post-Quantum Cryptography: Current State and Quantum Mitigation. 2023 *IEEE European Symposium on Security and Privacy Workshops*, Delft, 3-7 July 2023, 620-628.
- [9] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., *et al.* (2022) Transitioning Organizations to Post-Quantum Cryptography. *Nature*, **605**, 237-243. <https://doi.org/10.1038/s41586-022-04623-2>
- [10] Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. and Bangash, Y.A. (2025) Profiling Post-Quantum Cryptography for IoT Security: A Software Engineering Approach. *IEEE Internet of Things Journal*, **12**, 1158-1177.
- [11] Trope, Y. and Liberman, N. (2010) Construal-Level Theory of Psychological Distance. *Psychological Review*, **117**, 440-463. <https://doi.org/10.1037/a0018963>
- [12] Attrill-Smith, A., Fullwood, C., Keep, M. and Kuss, D.J. (2019) The Oxford Handbook of Cyberpsychology. Oxford University Press.
- [13] Nobles, C. (2018) Botching Human Factors in Cybersecurity in Business Organizations. *Holistica—Journal of Business and Public Administration*, **9**, 71-88. <https://doi.org/10.2478/hjbpa-2018-0024>
- [14] Sozzo, S. (2021) Quantum Cognition and Decision Theories: A Tutorial. *Journal of Mathematical Psychology*, **104**, Article ID: 102579.
- [15] Nielsen, M.A. and Chuang, I.L. (2010) Quantum Computation and Quantum Information (10th Anniversary ed.). Cambridge University Press.
- [16] Montanaro, A. (2016) Quantum Algorithms: An Overview. *NPJ Quantum Information*, **2**, Article No. 15023. <https://doi.org/10.1038/npjqi.2015.23>

- [17] Bernstein, D.J. and Lange, T. (2017) Post-Quantum Cryptography. *Nature*, **549**, 188-194. <https://doi.org/10.1038/nature23461>
- [18] Preskill, J. (2018) Quantum Computing in the NISQ Era and Beyond. *Quantum*, **2**, Article No. 79. <https://doi.org/10.22331/q-2018-08-06-79>
- [19] Aydeger, A., Sarica, A.K., Behnia, R., Cebe, M., Akkaya, K. and Rahman, M.A. (2024) Mitigating Quantum Threats to Blockchain and Cyber-Security: Challenges and Opportunities in Developing Post-Quantum Blockchain and Cryptographic Standards. *IEEE Access*, **12**, 23345-23371.
- [20] Slovic, P. (1987) Perception of Risk. *Science*, **236**, 280-285. <https://doi.org/10.1126/science.3563507>
- [21] Frederick, S., Loewenstein, G. and O'donoghue, T. (2002) Time Discounting and Time Preference: A Critical Review. *Journal of Economic Literature*, **40**, 351-401. <https://doi.org/10.1257/jel.40.2.351>
- [22] Ellsberg, D. (1961) Risk, Ambiguity, and the Savage Axioms. *The Quarterly Journal of Economics*, **75**, 643-669. <https://doi.org/10.2307/1884324>
- [23] Davis, F.D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, **13**, 319-340. <https://doi.org/10.2307/249008>
- [24] Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003) User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, **27**, 425-478. <https://doi.org/10.2307/30036540>
- [25] Weick, K.E. (1995) Sensemaking in Organizations. Sage Publications.
- [26] Schein, E.H. (2010) Organizational Culture and Leadership. 4th Edition, Jossey-Bass.
- [27] Weick, K.E. and Sutcliffe, K.M. (2015) Managing the Unexpected: Sustained Performance in a Complex World. 3rd Edition, Wiley.
- [28] Ibarra, H. (1999) Provisional Selves: Experimenting with Image and Identity in Professional Adaptation. *Administrative Science Quarterly*, **44**, 764-791. <https://doi.org/10.2307/2667055>
- [29] Hatano, G. and Inagaki, K. (1986) Two Courses of Expertise. In: Stevenson, H., Azuma, H. and Hakuta, K., Eds., *Child Development and Education in Japan*, Freeman, 262-272.
- [30] Teitsma, M., Pors, J., Lucivero, F. and Swierstra, T. (2025) Professional Resistance to Emerging Technologies: Exploring the Expertise Paradox in Quantum Security Transitions. *Science and Public Policy*, **52**, 78-92.
- [31] Ibarra, H. and Barbulescu, R. (2010) Identity as Narrative: Prevalence, Effectiveness, and Consequences of Narrative Identity Work in Macro Work Role Transitions. *Academy of Management Review*, **35**, 135-154. <https://doi.org/10.5465/amr.2010.45577925>
- [32] Wickens, C.D., Helton, W.S., Hollands, J.G. and Banbury, S. (2021) Engineering Psychology and Human Performance. 5th Edition, Routledge. <https://doi.org/10.4324/9781003177616>
- [33] Sweller, J. (1988) Cognitive Load during Problem Solving: Effects on Learning. *Cognitive Science*, **12**, 257-285. https://doi.org/10.1207/s15516709cog1202_4
- [34] Barik, T., Denning, T., Pearson, J., Nushi, B. and Dittmer, T. (2021). Understanding Quantum Software Engineering. *Proceedings of the 43rd International Conference on Software Engineering: New Ideas and Emerging Results*, 25-28 May 2021, 40-44.
- [35] Lee, J.D. and See, K.A. (2004) Trust in Automation: Designing for Appropriate Reli-

- ance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, **46**, 50-80. <https://doi.org/10.1518/hfes.46.1.50.30392>
- [36] Aiken, M. (2016) The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online. Spiegel & Grau.
- [37] Hillen, M.A., Gutheil, C.M., Strout, T.D., Smets, E.M.A. and Han, P.K.J. (2017) Tolerance of Uncertainty: Conceptual Analysis, Integrative Model, and Implications for Healthcare. *Social Science & Medicine*, **180**, 62-75. <https://doi.org/10.1016/j.socscimed.2017.03.024>
- [38] Piaget, J. (1952) The Origins of Intelligence in Children. International Universities Press.
- [39] Wenger, E. (1998) Communities of Practice: Learning, Meaning, and Identity. Cambridge University Press. <https://doi.org/10.1017/cbo9780511803932>
- [40] Polanyi, M. (1966) The Tacit Dimension. Doubleday.
- [41] Walsh, R. (1995) Phenomenological Mapping: A Method for Describing and Comparing States of Consciousness. *Journal of Transpersonal Psychology*, **27**, 25-25. <https://drrogerwalsh.com/wp-content/uploads/2017/06/Phenomenological-Mapping-A-Method-for-Describing-Comparing-States-of-Consciousness-JTP-1995.pdf>
- [42] Salehi, Ö., Seskir, Z. and Tepe, İ. (2022) A Computer Science-Oriented Approach to Introduce Quantum Computing to a New Audience. *IEEE Transactions on Education*, **65**, 1-8. <https://doi.org/10.1109/te.2021.3078552>