A Unified Classification Model for Quantum-Enabled Cyberattacks

Simas Krušniauskas[1], Šarūnas Grigaliūnas[2] and Rasa Brūzgienė[2]

[1]Department of Infrastructure and Services, Kaunas University of Technology, Kaunas LT-51368, Lithuania
[2]Department of Computer Sciences, Kaunas University of Technology, Kaunas LT-51368, Lithuania

Abstract

The rapid development of quantum computing is reshaping the cybersecurity threat landscape by undermining classical cryptographic assumptions and introducing new technical, operational, and organizational vulnerabilities. Existing cybersecurity threat frameworks insufficiently address quantum-enabled risks, particularly those related to post-quantum cryptography (PQC) migration, hybrid infrastructures, and long-horizon threats such as store-now-decrypt-later attacks. This paper aims to develop a unified classification model for quantum-enabled cyberattacks that integrates cryptanalytic, protocol-level, operational, and human-factor dimensions into a structured analytical framework. The proposed model formalizes attack characterization through multidimensional parameters including attack vector, required quantum capability, exploited weakness, impact level, and temporal horizon, enabling systematic risk assessment. Experimental evaluation using simulated network traffic datasets demonstrated the model's applicability for threat classification, risk scoring, and prioritization of PQC migration efforts. Results indicate that cryptanalytic and data-harvesting attacks present the highest long-term risk, while operational and human-factor vulnerabilities remain critical in the near term, highlighting the need for a comprehensive, multilayered approach to quantum cybersecurity readiness.

Keywords

Quantum cybersecurity, Post-Quantum cryptography, Threat classification, Crypto-agility

1. Introduction

The emergence of quantum computing is expected to fundamentally reshape the cybersecurity threat landscape by weakening the computational assumptions underpinning widely deployed cryptographic systems. In particular, quantum algorithms enable speedups for problem classes that are infeasible for classical machines at scale, creating direct risks to public-key cryptography and altering the effective security margin of symmetric primitives. Shor's algorithm is widely recognized as a disruptive factor for RSA, Diffie–Hellman, and elliptic-curve cryptography, as it enables polynomial-time solutions to integer factorization and discrete logarithms, threatening the confidentiality and authenticity guarantees of contemporary public-key infrastructures [1]. In parallel, Grover's algorithm reduces the effective security level of symmetric encryption and hashing by offering a quadratic speedup for unstructured search, motivating revised key-length and system design assumptions for long-term protection [2][3]. Simultaneously, organizations pursuing post-quantum cryptography (PQC) must often adopt transitional architectures - such as hybrid key exchange and mixed deployments across endpoints and services - where implementation complexity, performance constraints, and negotiation logic can create new exploitable conditions [4][5][6]. These factors collectively elevate the need to treat quantum cybersecurity not only as a cryptographic problem, but as a multi-domain risk-management challenge that spans technical controls, operational governance, and human-centered vulnerabilities.

Despite increasing attention to PQC adoption and quantum-era threat anticipation, many widely used cybersecurity frameworks and practices remain oriented toward classical attacker models and do not explicitly encode quantum capability assumptions or transition-state vulnerabilities. Similarly, organizational cybersecurity governance frameworks emphasize risk management and resilience, yet

*IVUS 2026: Information Society and University Studies 2026, May 12, Kaunas, Lithuania

simas.krusniauskas@ktu.lt (S. Krušniauskas); sarunas.grigaliunas@ktu.lt (Š. Grigaliūnas); rasa.bruzgiene@ktu.lt (R. Brūzgienė)

0009-0007-5982-3430 (S. Krušniauskas); 0000-0001-9268-9244 (Š. Grigaliūnas); 0000-0002-0816-8700 (R. Brūzgienė)

Copyright © 2026 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-06

CEUR-WS.org/Vol-4317/paper25.pdf

they provide limited granularity for describing quantum-specific attack vectors and prioritizing mitigations across cryptographic, protocol, operational, and human domains [7].

The central problem addressed in this paper is the absence of a unified and structured classification approach capable of consistently describing quantum-enabled cyberattacks across cryptanalytic, protocol (network), operational (systemic), and human (organizational) dimensions. This limitation complicates threat modeling, weakens PQ readiness assessment, and reduces the effectiveness of prioritization during PQC migration - especially in contexts where hybrid cryptography, partial deployment, and long-term data confidentiality requirements coexist. The aim of this paper is to propose a unified classification model for quantum-enabled cyberattacks that supports systematic characterization of threats and enables consistent risk-oriented prioritization of PQ cybersecurity activities, including PQC migration planning and governance. The contribution of the authors' is as follows:

- A unified classification model integrating cryptanalytic, protocol, operational, and human quantum-enabled cyber threats into a single structured framework.
- A formal multidimensional representation that captures attack vector category, required quantum capability, exploited weakness type, impact level, and temporal horizon.
- A practical demonstration of the model using generated network-observable datasets and a composite risk scoring mechanism to rank quantum-enabled threats and inform prioritization decisions.

The remainder of this paper is organized as follows. Section 1 summarizes quantum computing foundations and the cybersecurity implications of quantum algorithms and transition-state risks. Section 2 presents a taxonomy of quantum-enabled cyberattacks while Section 3 introduces the proposed unified classification model and defines its dimensions and classification procedure. Section 4 presents the use case, including dataset generation and the classification workflow. Section 5 reports experimental results, including classification matrices, risk scores, and prioritization rankings. Section 6 concludes the paper and outlines directions for future work.

2. Taxonomy of Quantum-Enabled Cyberattacks

2.1. Cryptanalytic Attacks

We need to understand that by developing quantum technologies and capabilities, a multi-tiered threat landscape emerges that challenges the fundamental assumptions of modern cryptography. [8] When talking about a taxonomy of quantum-enabled cyberattacks, it can be categorized from mathematical vulnerabilities to systemic and human-oriented weaknesses.

To begin with, it is necessary to discuss cryptanalytic attacks. These are the attacks in which Shor's and Grover's algorithms take place. As discussed earlier, Shor's algorithm represents an existential threat to asymmetric cryptography by exponentially speeding up integer factorization and discrete logarithms [9]. Although classical computers with well-known hardware would take trillions of years to crack a 2048-bit RSA key, a sufficiently powered quantum computer would be able to derive the private key from a public certificate in a matter of minutes or even seconds, rendering RSA, ECC, and DSA obsolete [9][10].

Talking about Grover's algorithm, furthermore, it can be said that it is not as destructive as Shor's, but Grover's algorithm accelerates searches of unstructured databases with quadratic speedup and in doing so reduces the effective bit security of symmetric keys [11][9]. It can be said that search of unstructured database basically is the task of guessing a symmetric key or finding a hash collision. [9] This algorithm can reduce AES-128 security level to 64 bits, and this would be vulnerable to future quantum systems. [9] While talking about halving of key length, same goes with AES-256 where Grover's algorithm can reduce its security level to 128 bits. [12] It is worth mentioning that Grover's algorithm target the integrity of hash functions [9]. This algorithm effectively weakens standards such as SHA-256 by halving their complexity from $O(2^n)$ to $O(2^{n/2})$ where n - bits, for example: SHA-256 search complexity would be decreased from 2^{256} to 2^{128}. [9]

2.2. Protocol and Network Attacks

Until now, we have been talking only about breaking individual algorithms, although quantum technologies go beyond that by undermining the protocols that ensure secure communication and identity. It is well known that TLS, SSH, and IPsec, which are network security protocols, rely on public-key exchanges to establish secure sessions which are known to be really vulnerable to quantum computing abilities [13].

Additionally, advancements in quantum technologies will allow attackers to forge digital signatures using Shor-based cryptanalysis - derive private keys from public certificates. This will enable attackers to impersonate entities in real time and bypass Certificate Authorities (CAs). This would collapse the Public Key Infrastructure (PKI) trust framework [13], and quantum-enhanced Man-in-the-Middle (MITM) attacks will become more frequent occurrences.

In these days, post quantum security is quite a hot topic and everyone is trying to mitigate future risks by implementing hybrid mechanisms or in this case they can be called - hybrid handshakes. Hybrid mechanism is when both, classical and post-quantum algorithms are being used [5]. It is implemented in such way, that information stays secure as long as one of the algorithms stays intact and unbroken [5].

On the other hand, there is a great chance of downgrade attacks while using hybrid mechanisms. This means that the complexity of transition phase can be exploited by forcing systems to use weaker protocols. For example, attackers can force system to use legacy (TLS 1.2) protocols, by manipulating negotiation process, instead of using post quantum secure version of the protocol (for example Kyber-TLS) [13].

2.3. Operational and Systemic Attacks

Transitioning to post-quantum cryptography is a very complex task, organizations should review all of the used infrastructure, cryptographic algorithms, used protocols, and so on. They need to have a clear vision and plan how they are going to move toward a more advanced and secure future. While transitioning to quantum-safe architectures, “reality gaps” can arise and be exploited by attackers - these are called operational and systemic attacks.

The PQC transition phase can be exploited by forcing systems to negotiate using classical cryptographic protocols, which are weaker than post-quantum ones and which should not be used [13]. Additionally, poor implementation of hybrid models may lead to inconsistencies. There is a chance that some of the system components will not be secured correctly or remain using quantum unsafe cryptography or protocols which would lead to single point of failure in the system, with an open door to attackers. Also, it should not be forgotten, that it is impossible to update and upgrade everything at once, so there is a big chance, that classical and quantum secure parts of the infrastructure are going to coexist.

We should not forget about PQC supply chain risks. There is always a chance that attackers might tamper with compilers, this states that intellectual property might be stolen or even circuit designs might be at the risk of theft [14]. Also, there is a second part of this security flaw, where during compilation process, when compromised compiler can tamper with hardware configuration files, altering data encoding or other crucial parts of the codes [14].

2.4. Human and Organizational Vulnerabilities

It should not be forgotten that humans themselves might be the weakest link in the chain. As technology advances, humans remain the main components that operate these innovations. During PQC migration, a significant chance of human error persists. PQC migration and implementation may be quite challenging, as a large amount of legacy software will need to be updated or re-coded. The complexity of systems will grow as PQC algorithms require larger key sizes and greater computational power. In mismanaged, misconfigured and poorly optimized environments and infrastructures, this can lead to resource exhaustion, or, in other words, make it easier for attackers to execute DoS attacks [13]. In addition, misconfigured PQC protocols such as TLS or IPsec can enable numerous attacks: privilege escalation, downgraded communication paths [13].

It should not be forgotten that PQC migration does not prevent all threats. PQC might mitigate the risks based on encryption, but organizations are still vulnerable to social engineering and phishing

attacks [15]. That is because these types of attacks do not depend on the infrastructure itself, but are targeted at people working in a certain organization, the attackers try to trick those people and in this way gather the required information for further exploitation [15]. One more of the problems that arises with quantum acceleration and AI is that those two tools will be able to produce highly realistic deepfakes which will make it even easier to fool people and gain information, which is much needed for adversaries [13].

It might sound harsh, but the truth is that some of the companies are on the brink of survival. That is because the transition to PQC is going to be time-consuming and resource consuming. Some of the companies will not be able to hire professionals with sufficient knowledge required for PQC integration, or might lack cybersecurity resources to maintain their products or services in as high level of security as before PQC. [16]

3. Unified Classification Model

3.1. Model Dimensions and Quantum Capability Mapping

Let an attack instance $a \in \mathcal{A}$ belong to the set of quantum-enabled cyberattacks. The unified classification function is defined as:

$$\mathcal{C}(a) = (V(a), Q(a), W(a), I(a), T(a)) \quad (1)$$

where $V(a)$ denotes the attack vector category, $Q(a)$ the required quantum capability, $W(a)$ the exploited weakness, $I(a)$ the impact level, and $T(a)$ the temporal horizon.

Building upon the previously introduced taxonomy, the attack vector dimension $V(a)$ is defined over four principal categories:

- $\mathcal{V}_0$ - Cryptanalytic attacks, including asymmetric cryptography attacks and symmetric cryptography attacks;
- $\mathcal{V}_1$ - Protocol and network attacks, including insecure hybrid handshakes, downgrade paths during PQC negotiation, and Harvest-Now-Decrypt-Later (HNDL) attacks;
- $\mathcal{V}_2$ - Operational and systemic attacks, including migration weaknesses, partial PQC deployment, and supply-chain risks;
- $\mathcal{V}_3$ - Human and organizational vulnerabilities, including misconfiguration, social engineering, and phishing.

The quantum capability dimension $Q(a)$ expresses the level of quantum resources required for successful execution:

- $\mathcal{Q}_0$ - No quantum resources required;
- $\mathcal{Q}_1$ - Quantum-assisted or quantum-enhanced classical attacks;
- $\mathcal{Q}_2$ - Full quantum capability required (e.g., execution of Shor's or Grover's algorithms).

The exploited weakness dimension $W(a)$ is defined as:

- $\mathcal{W}_0$ - Cryptographic;
- $\mathcal{W}_1$ - Protocol;
- $\mathcal{W}_2$ - Implementation;
- $\mathcal{W}_3$ - Configuration;
- $\mathcal{W}_4$ - Human.

Impact level $I(a)$ captures the severity of consequences:

- $\mathcal{I}_0$ - Low (minimal information exposure);
- $\mathcal{I}_1$ - Moderate (service disruption or degradation);
- $\mathcal{I}_2$ - Critical (loss of confidentiality, integrity, or privilege escalation).

Temporal horizon $T(a)$ reflects when the attack becomes feasible:

- $\mathcal{T}_0$ - Short-term (feasible with existing technology);
- $\mathcal{T}_1$ - Mid-term (feasible in the near future);
- $\mathcal{T}_2$ - Long-term (feasible upon major quantum breakthroughs).

To ensure analytical consistency, a quantum capability mapping is introduced to relate concrete quantum algorithms to the abstract capability scale. Execution of Shor's algorithm, which enables

polynomial-time integer factorization and discrete logarithm computation, corresponds to $\mathcal{Q}2$, as it requires a fault-tolerant quantum computer capable of breaking RSA, ECC, or DSA. Mitigation requires migration to post-quantum cryptographic schemes based on quantum-resistant hardness assumptions.

Grover's algorithm modifies brute-force search complexity as:

$$\mathcal{W}_C(n) = 2^n \Rightarrow \mathcal{W}_Q(n) = 2^{n/2}, \quad (2)$$

justifying increased key lengths as a compensatory strategy for symmetric cryptography. Attacks leveraging Grover-based quadratic speedup are likewise classified under $\mathcal{Q}_2$, as they require operational quantum computational capability.

3.2. Classification Procedure

Attacks are classified by identifying the dominant mechanism, assigning quantum capability requirements, mapping exploited weaknesses, and evaluating confidentiality, integrity, availability, and time horizon (Table 1).

Table 1
Cyberattacks classification matrix

Attack vector category	Quantum capability	Exploited weakness	Impact level	Temporal horizon
$\mathcal{V}_0$ - Asymmetric cryptography attacks	$\mathcal{Q}_2$	$\mathcal{W}_0$	$\mathcal{I}_2$	$\mathcal{T}_2$
$\mathcal{V}_0$ - Symmetric cryptography attacks	$\mathcal{Q}_2$	$\mathcal{W}_0$	$\mathcal{I}_2$	$\mathcal{T}_2$
$\mathcal{V}_1$ - Insecure hybrid handshakes	$\mathcal{Q}_0$	$\mathcal{W}_1$	$\mathcal{I}_0$	$\mathcal{T}_0$
$\mathcal{V}_1$ - Downgrade paths during PQC negotiation	$\mathcal{Q}_0$	$\mathcal{W}_2$	$\mathcal{I}_0$	$\mathcal{T}_0$
$\mathcal{V}_1$ - Harvest now, decrypt later attack	$\mathcal{Q}_2$	$\mathcal{W}_0$	$\mathcal{I}_2$	$\mathcal{T}_2$
$\mathcal{V}_2$ - Migration weakness	$\mathcal{Q}_0$	$\mathcal{W}_2$	$\mathcal{I}_1$	$\mathcal{T}_0$
$\mathcal{V}_2$ - Partial PQC deployment	$\mathcal{Q}_0$	$\mathcal{W}_2$	$\mathcal{I}_1$	$\mathcal{T}_0$
$\mathcal{V}_2$ - Supply-chain risks	$\mathcal{Q}_0$	$\mathcal{W}_4$	$\mathcal{I}_1$	$\mathcal{T}_0$
$\mathcal{V}_3$ - Misconfiguration	$\mathcal{Q}_0$	$\mathcal{W}_3$	$\mathcal{I}_2$	$\mathcal{T}_0$
$\mathcal{V}_3$ - Social engineering and phishing	$\mathcal{Q}_1$	$\mathcal{W}_4$	$\mathcal{I}_2$	$\mathcal{T}_1$

The presented cyberattacks classification matrix makes it easier to understand and see how crucial some of the attacks can be. As is known and accepted, the confidentiality and integrity are the most important things in all systems. So it would be smart to look at those threats that poses the greatest threat for that and try to prevent them in the beginning. Even though, for some of those attacks quantum technologies are not as advanced yet as they need to be, it has to be the priority to prevent them as soon as possible, because once the advancement will be made - it will be too late to solve those problems. Having this matrix by hand at any time it will be easier to see and understand what should be focused on in the first place and what should be secured and migrated to PQC as soon as possible.

4. Use Case

Figure 1 presents the general architecture of the unified classification model for quantum-enabled cyberattacks, where multidimensional attack attributes derived from synthetic network traffic datasets are mapped into a structured classification function. The resulting parameterized representation enables quantitative risk scoring and supports systematic evaluation and prioritization of quantum-enabled cyber threats within the experimental use-case scenario.

4.1. Dataset Generation

For each of the 10 attack sub-categories defined in the taxonomy (see Section 2), synthetic pcap traffic was generated capturing network-observable signatures. Table 2 summarizes the simulation approach for each category.

Table 2
Dataset generation: simulation approach per attack category

Attack vector category	Simulation Approach
$\mathcal{V}_0$ - Asymmetric cryptography attacks	TLS ClientHello bursts with RSA cipher suites; anomalous certificate-request patterns
$\mathcal{V}_0$ - Symmetric cryptography attacks	High-rate encrypted block probing (AES-128 block size)
$\mathcal{V}_1$ - Insecure hybrid handshakes	TLS 1.3 connections with mixed Kyber+classical extensions
$\mathcal{V}_1$ - Downgrade attacks	Injected ServerHello forcing TLS 1.0 during PQC negotiation
$\mathcal{V}_1$ - SNDL attacks	Bulk encrypted traffic mirrored to attacker collection server
$\mathcal{V}_2$ - Migration weakness	Same client connecting to both PQC and legacy end-points
$\mathcal{V}_2$ - Partial PQC deployment	Mix of PQC-protected and unprotected server connections
$\mathcal{V}_2$ - Supply-chain risks	Tampered firmware update traffic with forged hash signatures
$\mathcal{V}_3$ - Misconfiguration	HTTP probes against exposed crypto-management interfaces
$\mathcal{V}_3$ - Social engineering	DNS+HTTP traffic to PQC-themed phishing domains

4.2. General Schema of the Unified Classification Model

Quantum computing introduces threats that extend well beyond the direct cryptanalytic domain. Vulnerabilities emerge not only from algorithmic breakthroughs such as Shor's and Grover's algorithms, but also from the complex process of migrating to post-quantum cryptography — a process that exposes protocol weaknesses, operational gaps, and human errors. Capturing this breadth requires a classification framework that treats every relevant dimension on equal footing.

The unified model proposed in this work defines a classification function that maps each attack instance a to a five-dimensional descriptor (**Figure 1**):

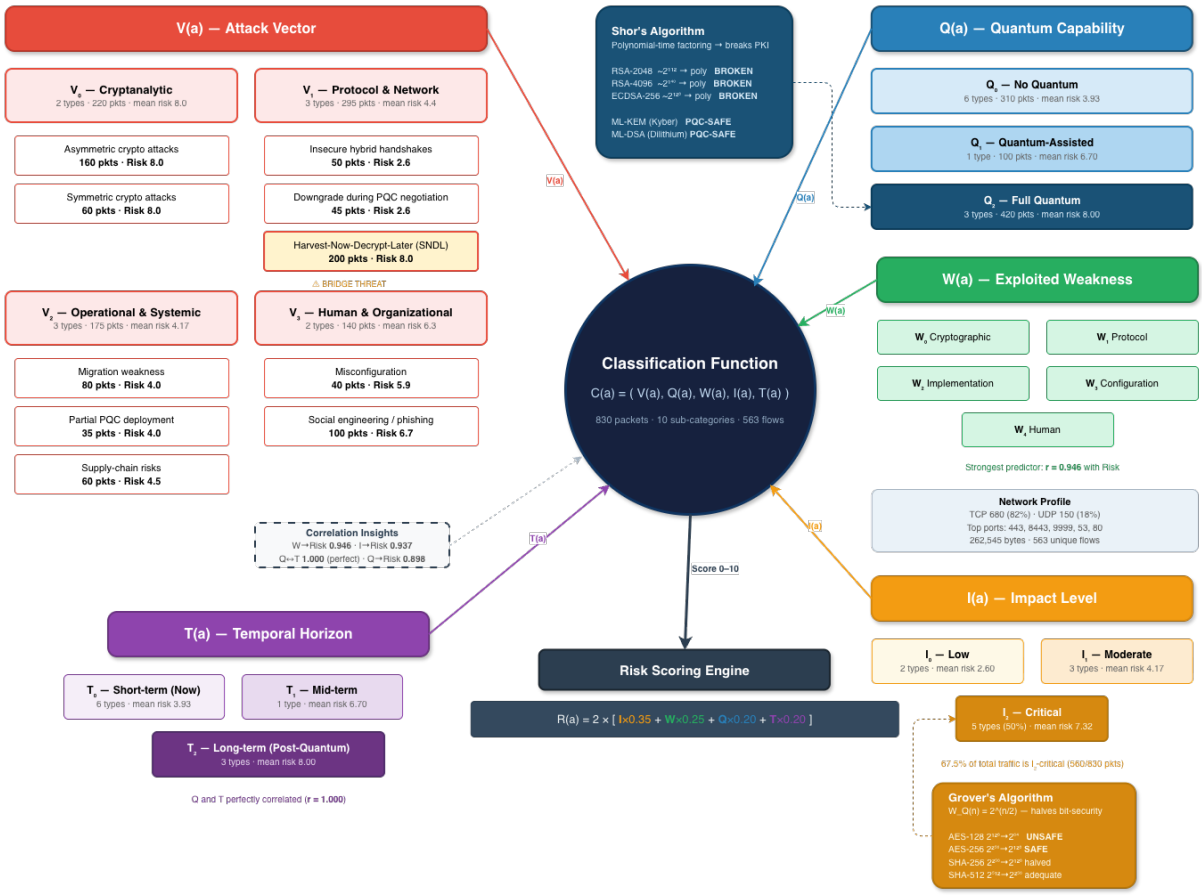


Figure 1: General schema of the unified classification model for quantum-enabled cyberattacks. Five dimensions feed the central classification function $\mathcal{C}(a)$, which outputs a composite risk score via the weighted formula $R(a) \in [0, 10]$.

$$\mathcal{C}(a) = (V(a), Q(a), W(a), I(a), T(a)) \tag{3}$$

The dimensions feed the central classification function $\mathcal{C}(a)$, which outputs a composite risk score via the weighted formula:

$$R(a) = 2 \times [I(a) \times 0.35 + W(a) \times 0.25 + Q(a) \times 0.20 + T(a) \times 0.20] \tag{4}$$

The resulting score $R(a) \in [0, 10]$ provides a single, comparable measure of urgency. Impact carries the greatest weight because it reflects the immediate consequence of a successful attack. The exploited weakness follows, as it determines the nature and effort of remediation. Quantum capability and temporal horizon share the remaining weight, capturing the strategic question of when and under what conditions the threat materializes.

5. Results

Table 3 presents the classification of all 10 attack sub-categories using the unified model dimensions and their computed risk scores. The results show that cryptanalytic attacks and the Harvest-Now-Decrypt-Later scenario achieve the highest risk score (8.0), reflecting their critical impact, long-term temporal feasibility, and requirement for full quantum capability.

In contrast, protocol-level downgrade and insecure hybrid handshake attacks exhibit significantly lower scores (2.6), primarily due to low impact classification and short-term feasibility. Operational and systemic migration weaknesses produce moderate risk scores (4.0-4.5), while human-factor attacks demonstrate comparatively elevated risk levels, particularly social engineering (6.7) and misconfiguration (5.9), due to their critical impact classification.

Table 3
Cyberattack classification matrix with risk scores

Attack ID	Pkts	V	Q	W	I	T	Risk
V0_asym	160	$\mathcal{V}_0$	$\mathcal{Q}_2$	$\mathcal{W}_0$	$\mathcal{I}_2$	$\mathcal{T}_2$	8.0
V0_sym	60	$\mathcal{V}_0$	$\mathcal{Q}_2$	$\mathcal{W}_0$	$\mathcal{I}_2$	$\mathcal{T}_2$	8.0
V1_hybrid	50	$\mathcal{V}_1$	$\mathcal{Q}_0$	$\mathcal{W}_1$	$\mathcal{I}_0$	$\mathcal{T}_0$	2.6
V1_downgrade	45	$\mathcal{V}_1$	$\mathcal{Q}_0$	$\mathcal{W}_2$	$\mathcal{I}_0$	$\mathcal{T}_0$	2.6
V1_sndl	200	$\mathcal{V}_1$	$\mathcal{Q}_2$	$\mathcal{W}_0$	$\mathcal{I}_2$	$\mathcal{T}_2$	8.0
V2_migration	80	$\mathcal{V}_2$	$\mathcal{Q}_0$	$\mathcal{W}_2$	$\mathcal{I}_1$	$\mathcal{T}_0$	4.0
V2_partial	35	$\mathcal{V}_2$	$\mathcal{Q}_0$	$\mathcal{W}_2$	$\mathcal{I}_1$	$\mathcal{T}_0$	4.0
V2_supply	60	$\mathcal{V}_2$	$\mathcal{Q}_0$	$\mathcal{W}_4$	$\mathcal{I}_1$	$\mathcal{T}_0$	4.5
V3_misconfig	40	$\mathcal{V}_3$	$\mathcal{Q}_0$	$\mathcal{W}_3$	$\mathcal{I}_2$	$\mathcal{T}_0$	5.9
V3_social	100	$\mathcal{V}_3$	$\mathcal{Q}_1$	$\mathcal{W}_4$	$\mathcal{I}_2$	$\mathcal{T}_1$	6.7

Table 4 ranks all attack types in descending order based on their computed risk score. The highest-priority threats are asymmetric cryptanalytic attacks, symmetric cryptanalytic attacks, and SNDL attacks, all scoring 8.0. These results confirm that attacks combining high impact with long-term quantum feasibility dominate strategic risk prioritization.

Table 4
Priority ranking of quantum-enabled cyberattacks by risk score

#	Attack ID	Description	Risk	I	T
1	V0_asym	Cryptanalytic – Asymmetric crypto attacks	8.0	$\mathcal{I}_2$	$\mathcal{T}_2$
2	V0_sym	Cryptanalytic – Symmetric crypto attacks	8.0	$\mathcal{I}_2$	$\mathcal{T}_2$
3	V1_sndl	Protocol & Network – SNDL	8.0	$\mathcal{I}_2$	$\mathcal{T}_2$
4	V3_social	Human & Org – Social engineering	6.7	$\mathcal{I}_2$	$\mathcal{T}_1$
5	V3_misconfig	Human & Org – Misconfiguration	5.9	$\mathcal{I}_2$	$\mathcal{T}_0$
6	V2_supply	Operational – Supply-chain risks	4.5	$\mathcal{I}_1$	$\mathcal{T}_0$
7	V2_migration	Operational – Migration weakness	4.0	$\mathcal{I}_1$	$\mathcal{T}_0$
8	V2_partial	Operational – Partial PQC deployment	4.0	$\mathcal{I}_1$	$\mathcal{T}_0$
9	V1_hybrid	Protocol & Network – Insecure hybrid handshakes	2.6	$\mathcal{I}_0$	$\mathcal{T}_0$
10	V1_downgrade	Protocol & Network – Downgrade during PQC neg.	2.6	$\mathcal{I}_0$	$\mathcal{T}_0$

Human and organizational attacks occupy mid-to-high priority positions, with social engineering ranking fourth. Operational migration-related weaknesses follow in the middle tier, while insecure hybrid handshakes and downgrade attacks are positioned as lowest-priority threats in the current model configuration.

This ranking validates the model's ability to differentiate between mathematically catastrophic but future-dependent threats and immediately feasible but lower-impact vulnerabilities.

6. Conclusions and Future Work

6.1. Conclusions

This paper introduced a unified classification model for quantum-enabled cyberattacks and validated it through a synthetic experiment encompassing 830 network packets across ten attack sub-categories. The model's five-dimensional classification function $\mathcal{C}(a) = (V(a), Q(a), W(a), I(a), T(a))$ and its accompanying risk score $R(a) \in [0, 10]$ provide a structured, reproducible basis for evaluating threats that arise both from quantum algorithms and from the complex process of migrating to post-quantum cryptography.

Cryptanalytic attacks ($\mathcal{V}_0$) carry the highest individual risk scores, yet the majority of immediately exploitable threats belong to the operational ($\mathcal{V}_2$) and human ($\mathcal{V}_3$) categories, require no quantum

capability ($\mathcal{Q}_0$), and are feasible with current technology ($\mathcal{T}_0$). Organizations cannot afford to defer these near-term risks while preparing for longer-term quantum threats; both demand parallel and coordinated attention.

Critical-impact attacks are not concentrated in a single vector category; they span all four dimensions from $\mathcal{V}_0$ to $\mathcal{V}_3$. This distribution validates the central premise of the unified model — that quantum-era threat assessment must be multi-dimensional rather than purely cryptographic. A framework that addresses only algorithmic resilience will systematically underestimate the risks introduced by protocol weaknesses, operational gaps, and human vulnerabilities.

6.2. Future Work

The unified model complements rather than replaces frameworks such as MITRE ATT&CK and the NIST CSF. Future work should map the five classification dimensions to ATT&CK tactics, CSF subcategories, ISO/IEC 27001 controls, and NIST SP 800-61 workflows, giving SOCs a cross-reference for playbook selection and escalation. As manual classification does not scale, ML classifiers predicting the five-dimensional tuple $\mathcal{C}(a)$ from network observables would support real-time threat triage, and should be validated on large-scale, real-world traffic with benchmarking on accuracy, latency, and false-positive rates.

Longitudinal studies of attack distributions, quantum capability requirements, and risk scores–alongside the deployment of NIST-standardized algorithms (ML-KEM, ML-DSA, SLH-DSA) and hybrid schemes - would guide phased post-quantum migration. Since real-world risk is context-dependent, adaptive weighting by industry-specific vulnerabilities, infrastructure maturity, regulatory exposure, and asset criticality would tune the model to organizational context.

Finally, human and organizational factors carry substantial near-term risk despite low quantum requirements; investigation into social engineering, insider threats, governance gaps, and workforce readiness would strengthen multi-layered resilience in the quantum era.

7. Acknowledgements

Research was conducted as part of the execution of Project ”Development and piloting of Latvia-Lithuania cross-border quantum communication infrastructure (24-EU-DIG-Lat-LitQN)” (No. 101249607), funded by European Union under The Connecting Europe Facility (CEF) in Digital programme.

8. Declaration on Generative AI

During the preparation of this paper, the authors used generative AI tool (ChatGPT 5.2) for the revision of the English language. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

9. References

[1] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, C. N. Asogwa, An overview of quantum cryptography and shor’s algorithm, International Journal of Advanced Trends in Computer Science and Engineering 9 (2020) 7487–7495. URL: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse82952020.pdf. doi:10.30534/ijatcse/2020/82952020.

[2] G. L. Long, Grover Algorithm with zero theoretical failure rate, Physical Review A 64 (2001) 022307. URL: http://arxiv.org/abs/quant-ph/0106071. doi:10.1103/PhysRevA.64.022307, arXiv:quant-ph/0106071.

[3] B. Khanal, P. Rivas, J. Orduz, A. Zhakubayev, Quantum Machine Learning: A Case Study of Grover's Algorithm, in: 2021 International Conference on Computational Science and Computational Intelligence (CSCI), 2021, pp. 79–84. URL: https://ieeexplore.ieee.org/document/9798970. doi:10.1109/CSCI54926.2021.00088.

[4] M. Sosnowski, F. Wiedner, E. Hauser, L. Steger, D. Schoinianakis, S. Gallenmüller, G. Carle, The Performance of Post-Quantum TLS 1.3, in: Companion of the 19th International Conference on emerging Networking EXperiments and Technologies, ACM, Paris France, 2023, pp. 19–27. URL: https://dl.acm.org/doi/10.1145/3624354.3630585. doi:10.1145/3624354.3630585.

[5] D. Herzinger, S.-L. Gazdag, D. Loebenberger, Real-World Quantum-Resistant IPsec, in: 2021 14th International Conference on Security of Information and Networks (SIN), volume 1, 2021, pp. 1–8. URL: https://ieeexplore.ieee.org/document/9699255. doi:10.1109/SIN54109.2021.9699255.

[6] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, M. Liyanage, Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography, in: 2024 15th International Conference on Network of the Future (NoF), 2024, pp. 195–203. URL: https://ieeexplore.ieee.org/document/10741441. doi:10.1109/NoF62948.2024.10741441.

[7] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, Technical Report NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. doi:10.6028/NIST.CSWP.29.

[8] A. Al-Harbi, F. Alotaibi, M. Alsubaie, Quantum cryptanalysis: Evaluating the impact of shor's and grover's algorithms on modern encryption standards, Computer Science Journal (2025). URL: https://doi.org/10.57238/csj.2025.1012. doi:10.57238/csj.2025.1012.

[9] S. Ali, S. A. Wadho, K. R. Talpur, B. A. Talpur, K. S. Alshudukhi, M. Humayun, S. R. Talpur, M. A. A. Mamun, M. Naseem, A. Abro, D. B. Talpur, A. Shah, Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity—Threats, Mitigations, and Solutions, Computers and Electrical Engineering 128 (2025) 110649. URL: https://www.sciencedirect.com/science/article/pii/S0045790625005920. doi:10.1016/j.compeleceng.2025.110649.

[10] U. Orji, C. Ugwuishiwu, An overview of Quantum Cryptography and Shor's Algorithm, International Journal of Advanced Trends in Computer Science and Engineering (2020). URL: https://www.academia.edu/77334349/An_overview_of_Quantum_Cryptography_and_Shor_s_Algorithm. doi:10.30534/IJATCSE/2020/82952020.

[11] G. Brassard, P. Høyer, M. Mosca, A. Tapp, Quantum amplitude amplification and estimation, in: Quantum Computation and Information, volume 305 of Contemporary Mathematics, American Mathematical Society, 2002, pp. 53–74. URL: https://doi.org/10.1090/conm/305/05215. doi:10.1090/conm/305/05215, also available as arXiv:quant-ph/0005055.

[12] A. K. Malviya, N. Tiwari, M. Chawla, Quantum cryptanalytic attacks of symmetric ciphers: A review, Computers and Electrical Engineering 101 (2022) 108122. URL: https://www.sciencedirect.com/science/article/pii/S0045790622003743. doi:10.1016/j.compeleceng.2022.108122.

[13] Y. Baseri, A. Hafid, A. H. Lashkari, Future-Proofing Cloud Security Against Quantum Attacks: Risk, Transition, and Mitigation Strategies, 2025. URL: http://arxiv.org/abs/2509.15653. doi:10.48550/arXiv.2509.15653, arXiv:2509.15653 [cs].

[14] S. Deshpande, J. Szefer, What is quantum computer security?, 2025. URL: https://arxiv.org/abs/2510.07334. arXiv:2510.07334.

[15] Y. Baseri, V. Chouhan, A. Ghorbani, Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure, 2024. URL: http://arxiv.org/abs/2404.10659. doi:10.48550/arXiv.2404.10659, arXiv:2404.10659 [cs].

[16] A. Aslam, Quantum Computing Threats to Cryptography: A Comprehensive Analysis of Vulnerabilities, Countermeasures, and Future-Proofing Strategies, 2025. URL: https://www.researchsquare.com/article/rs-6795420/v1. doi:10.21203/rs.3.rs-6795420/v1, iSSN: 2693-5015.