



Source: Decent.

The Quantum Equation: Hybrid Warfare, Unmanned Systems and Post-Quantum Vulnerabilities

An Analytical Assessment of Post-Quantum Cryptography, Command and Control Security, and European Sovereign Readiness

By Gerardo Spagnuolo

EXECUTIVE SUMMARY

The convergence of quantum computing and autonomous unmanned systems is redefining the parameters of contemporary hybrid warfare. The imminent vulnerability of classical asymmetric encryption (RSA, ECC) has prompted a global transition toward Post-Quantum Cryptography (PQC). However, recent theoretical disputes regarding lattice-based mathematical hardness reveal structural uncertainties. In contested operational domains, unmanned aerial vectors represent critical tactical nodes whose Command and Control (C2) integrity depends entirely on cryptographic agility.

1. Prologue: The Locks of the Modern World

Every hour, millions of invisible transactions sustain global stability. Encrypted tactical instructions are dispatched to autonomous drone swarms patrolling contested borders, high-value financial settlements are executed across continents, and secure governmental communications traverse optical backbones. Each of these interactions relies on an implicit, foundational pact: the mathematical algorithms safeguarding our digital assets are computationally trivial to construct in one direction, yet practically impossible to invert within reasonable timeframes using classical computation.

The advent of Quantum Computing with Cryptographic Relevance (CRQC) fundamentally destabilizes this architecture. The application of Shor's algorithm threatens to render traditional public-key infrastructures—specifically those grounded in integer factorization (RSA) and discrete logarithms over elliptic curves (ECC)—obsolete. In the theatre of modern hybrid conflict, kinetic power is paralyzed in the absence of resilient, uncompromised Command and Control (C2) channels. The operational imperative has therefore shifted toward Post-Quantum Cryptography (PQC). Yet recent scientific developments demonstrate that the transition toward quantum-resistant architectures is fraught with strategic ambiguity.

2. The August Tremor: Theoretical Scrutiny and Mathematical Realities

On the 3rd of August 2024, Daniel R. Simon, a distinguished researcher at Amazon Web Services (AWS), submitted a pre-print to the International Association for Cryptologic Research (IACR) repository. Simon's pedigree is formidable: his foundational work in the 1990s provided the theoretical catalyst for Peter Shor's quantum algorithm. Simon's pre-print posited a novel polynomial-time quantum algorithm capable of solving specific Learning With Errors (LWE) problems over mathematical lattices: the precise mathematical bedrock underpinning the National Institute of Standards and Technology (NIST) official PQC standards, namely **ML-KEM** (for key encapsulation) and **ML-DSA** (for digital signatures).

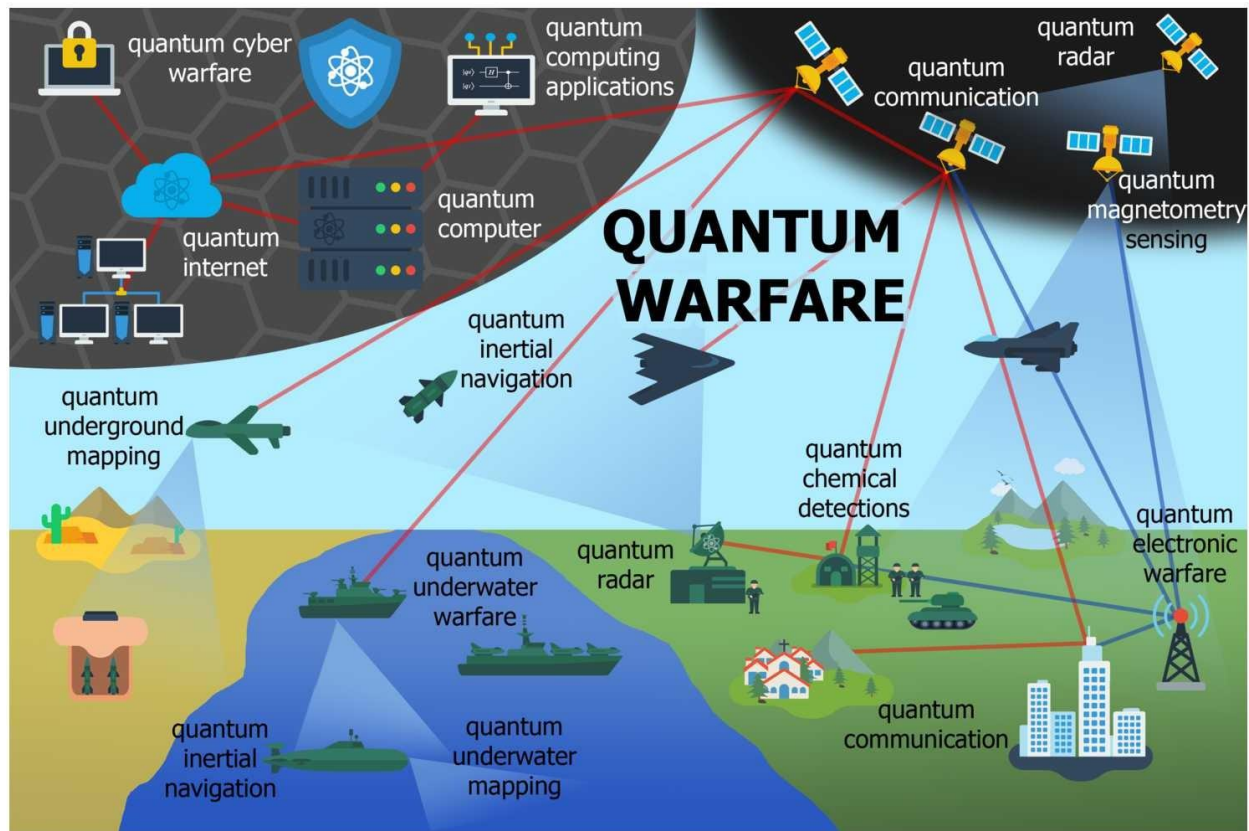
The initial media reaction was immediate, amplifying headlines claiming that the global PQC framework was on the verge of collapse. Strategic analysts, however, must disaggregate sensationalism from technical reality:

Peer-to-Peer Verification and Rigorous Debunking

Within days of publication, the global cryptologic community initiated an open, collaborative audit of Simon's proof. Daniel Apon, a leading researcher at **Anduril Industries** (a major American defence technology enterprise specializing in autonomous systems) published a rigorous rebuttal titled *The Search for Simon*. Apon identified a fatal logical gap within the proof's core construction (specifically regarding 'Lemma 3'). Simon acknowledged the limitation, demonstrating the self-correcting integrity of open scientific peer review.

The Persistent Residual Risk

Crucially, a parallel study authored by researchers at **Télécom Paris** (already peer-reviewed and accepted at a primary industry conference) established a formal mathematical bridge connecting the simplified theoretical problem targeted by Simon to the operational PQC constructions. While Simon's proposed path across this bridge was flawed, the structural connection itself is genuine. Consequently, current PQC standards rest upon a highly credible, yet fundamentally unproven, mathematical hardness assumption. A residual, theoretical margin of risk remains an enduring reality.



Source: Springer. Quantum technology for military applications.

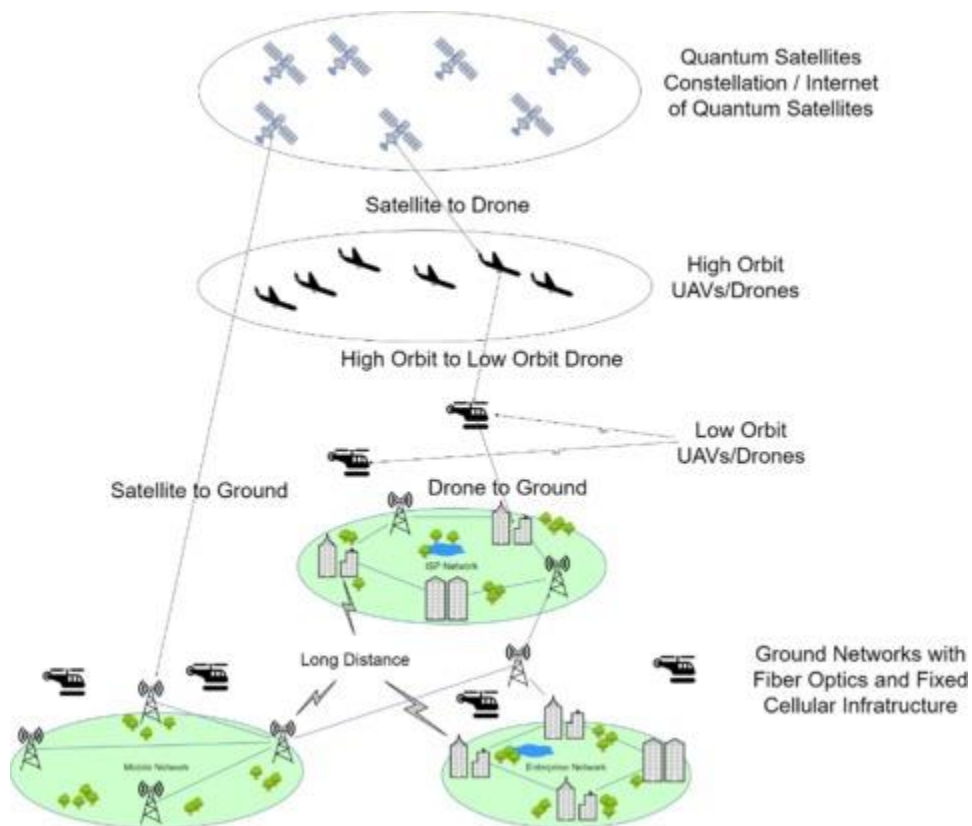
3. Unmanned Systems in Hybrid Warfare: The Critical Tactical Vector

In modern grey-zone and high-intensity conflicts, unmanned aerial, maritime surface, and ground vehicles (UAVs, USVs, UGVs) are no longer secondary assets; they function as primary, interconnected network nodes within broader C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) architectures. The reliance of these autonomous systems on asymmetric encryption exposes them to three profound hybrid threat vectors:

- **Harvest Now, Decrypt Later (HNDL):** Hostile state intelligence services actively intercept and archive encrypted radio telemetry, video feeds, and mission parameters transmitted between Ground Control Stations (GCS) and strategic long-endurance drones. While unreadable today,

this data vault will be decrypted retroactively upon the deployment of mature CRQC systems, exposing operational doctrines, electronic signatures, and historical intelligence tactics.

- **Swarm Hijacking and Authentication Spoofing:** Should an adversary exploit a structural weakness in digital signature schemes (ML-DSA, Module-Lattice-Based Digital Signature Algorithm), malicious actors could forge command authorization tokens or inject corrupted firmware updates. Entire autonomous swarms could be diverted, neutralized or co-opted without firing a single kinetic air-defence round.
- **Hardware Resource Bottlenecks:** PQC algorithms demand significantly larger key sizes, increased bandwidth, and elevated processing overhead compared to classic Elliptic Curve Cryptography. For tactical, battery-constrained drones operating at the edge, the computational burden of PQC directly competes with flight endurance and real-time processing latency, forcing a severe trade-off between cryptographic security and operational performance.



Source: Science Direct: *Futuristic view of the Internet of Quantum Drones*. The example is telecom based, but it is easily transposable to military structures.

4. The Geopolitics of Standardization: European Strategic Subsidiarity

A cold examination of the actors driving the post-quantum debate reveals a striking geopolitical asymmetry:

Domain / Actor		Institutional / Corporate entity	Strategic Function & Power
Primary Standardizer		NIST / NSA (USA)	Sets global mandatory technical cryptographic standards.
Defense & Vanguard	Industrial	Anduril, AWS, Cloudflare, Google (USA)	Drives hardware integration, threat verification, and transition timelines.
Fundamental Research	Academic	Télécom Paris, European Universities (EU)	Provides foundational mathematical proofs without industrial integration.
European Regulatory Core		Trilateral Axis: FRA / GER / NED	Shapes internal EU cybersecurity directives; excludes secondary member states.

While European academic institutions generate world-class cryptanalytic research, Europe remains absent from the executive governance chamber where commercial deployment schedules (e.g., the 2029 mandate set by US tech giants) and defence architectures are finalized. Furthermore, within the European Union, strategic direction is concentrated within a core directorate (France, Germany, Netherlands), leaving nations such as Italy in a passive, receptive posture despite possessing elite academic capital.

5. Strategic Imperatives: Institutionalizing Crypto-Agility

To mitigate systemic vulnerability and assert technological sovereignty, national cybersecurity agencies, such as Italy’s National Cybersecurity Agency (ACN), must transition from passive regulatory compliance toward active strategic orchestrators of **Crypto-Agility**. Crypto-agility defines the capacity to seamlessly swap underlying cryptographic primitives across hardware and software ecosystems without disrupting critical operational continuity.

Actionable National Roadmap for Critical Infrastructure Protection

- **Cryptographic Bill of Materials (CBOM):** Mandate the immediate compilation of comprehensive CBOMs across all operators of essential services within the National Cyber Security Perimeter, mapping every deployed algorithm, key length, and PKI dependency.
- **Hybrid Dual-Encapsulation Architectures:** Enforce dual-layer encryption combining classic ECC with PQC (ML-DSA/ML-KEM Module-Lattice-Based Key-Encapsulation Mechanism) across tactical communication links to ensure immediate resilience against HNDL (Harvest Now, Decrypt Later), while hedging against unexpected theoretical vulnerabilities in PQC schemes.
- **National PQC Sandboxing for Edge Hardware:** Establish dedicated physical and hardware-in-the-loop testbeds to evaluate the latency, power consumption, and bandwidth impacts of PQC implementations on constrained edge devices, including military unmanned systems.
- **Hardware Abstraction and Supply Chain Sovereignty:** Require hardware security module (HSM) vendors and software suppliers to decouple application logic from cryptographic primitives, enabling over-the-air (OTA) algorithm updates and eliminating vendor lock-in.

STRATEGIC IMPERATIVE

Strategic Conclusion: Hybrid warfare in the 21st century will not be decided solely by kinetic volume, but by the mathematical resilience of command architectures. European states must bridge the gap between academic brilliance and industrial execution. Establishing sovereign cryptographic agility is not merely a technical upgrade—it is a vital precondition for national autonomy.