Quantum-Ready Security for Contested Operations

How Catalyst Delivers Zero Trust
When You Cannot Trust the Network

Executive Brief
February 2026

The Problem: Contested environments have connectivity — but the network itself is hostile. Adversaries reroute traffic, hijack BGP, issue fraudulent certificates, and record encrypted data for future quantum decryption.

The Solution: Catalyst is a decentralized zero trust service mesh with post-quantum encryption on every link. It requires no centralized infrastructure, operates through disconnection, and protects data against both current and quantum-era threats.

The Operating Reality

Contested environments have connectivity — and the network itself is hostile. The Russia–Ukraine conflict proved that internet access survives sustained military operations. When Russia invaded in February 2022, Ukrainian internet traffic dropped roughly one-third on the first day [1] — then recovered to 85–90% of pre-war levels within weeks [2]. Starlink terminals were active within 48 hours, eventually reaching over 150,000 daily users [3]. Cellular networks continued operating through sustained bombardment. The network was degraded, contested, and sometimes rerouted — but it was not gone. And when adversaries control or influence that infrastructure, connectivity itself becomes a weapon:

- **Traffic rerouting.** After occupying Kherson, Russian forces rerouted local internet through Rostelecom for passive surveillance of all unencrypted traffic [4].
- **BGP hijacking.** Rostelecom conducted BGP hijacks affecting thousands of routes, silently redirecting traffic through Russian infrastructure [5].
- **Fraudulent TLS certificates.** Russia created its own TLS Certificate Authority, enabling machine-in-the-middle interception of HTTPS traffic [6].
- **Satellite link destruction.** Russian GRU operators wiped Viasat KA-SAT modems across Europe on invasion day, disabling satellite communications for Ukrainian military units [7].
- **Deep packet inspection.** Myanmar's military junta deployed Chinese-manufactured DPI equipment at ISP peering points for real-time interception [8].

Coalition Sharing Exposes the Problem

These threats are compounded when coalition and allied partners must share data across contested networks. NATO, Five Eyes, and UN missions routinely require multiple organizations to exchange information over infrastructure controlled by different — sometimes adversarial — sovereign entities. Each hop exposes both the network vulnerabilities and the security architecture flaws of every participating organization.

No single entity controls the network end-to-end. No single certificate authority is trusted by all parties. Traditional solutions — VPNs, centralized PKI, SASE gateways — assume trusted infrastructure at the center. In contested and coalition environments, the center may be compromised, unreachable, or nonexistent.

Being Left of Quantum Capability

NIST finalized post-quantum cryptography standards in August 2024 [9], including ML-KEM (FIPS 203 [10]) for key encapsulation. The NSA's CNSA 2.0 mandates PQ algorithms in all National Security Systems by 2030 [11]. The goal is to deploy post-quantum encryption *before* quantum computers are operationally capable — not after.

The urgency is **Harvest Now, Decrypt Later**: adversaries recording today's encrypted traffic for future quantum decryption. In contested environments where traffic is already being intercepted and rerouted, HNDL is the expected operating model. Organizations that wait for quantum capability to arrive before migrating will find their historical traffic already compromised.

How Catalyst Solves This

Catalyst is a distributed service mesh that connects organizations into a unified data-sharing fabric without centralized infrastructure. It is modeled after BGP — the protocol that routes the internet — but adapted for application-layer service discovery and encrypted data exchange.

Post-Quantum Encryption on Every Link

Every byte of traffic between Catalyst nodes travels inside a QUIC tunnel encrypted with X25519MLKEM768 — a hybrid cipher combining classical X25519 with post-quantum ML-KEM-768. This is the base layer: always present, not optional, independent of what applications run on top.

Applications that add their own mTLS get a second, independent encryption layer inside the QUIC tunnel. The two layers use different Certificate Authorities, different key material, and different SPIFFE identities. An adversary who compromises one layer still faces the other.

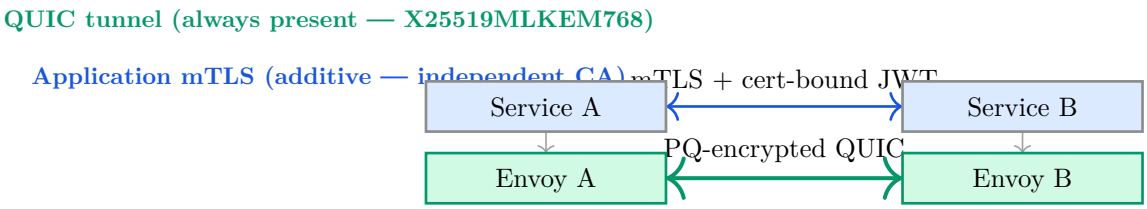

Figure 1: Dual-layer PQC: QUIC base (always present) + application mTLS (additive)

QUIC is particularly suited to contested environments: resilient to packet loss, faster PQ connection establishment than TCP/TLS [12], and better absorption of larger PQ key sizes. Envoy handles all encryption — applications connect to localhost and never manage TLS themselves [13].

Zero Trust Without Centralized Infrastructure

The DoD Zero Trust Strategy mandates zero trust across all systems by FY2027 [14], built on NIST SP 800-207 [15] and the CISA ZTMM v2.0 [16]. Most implementations (including DISA's Thunderdome [17]) require persistent connectivity to cloud SASE infrastructure. When the network is denied, disrupted, intermittent, or limited (DDIL), these centralized models fail.

Catalyst implements zero trust without a center:

- **Decentralized PKI.** Each node generates its own Root CA on first boot. Trust between organizations is established through out-of-band certificate exchange — a USB drive, a secure file transfer, a face-to-face handoff. No central CA server is needed.
- **Certificate-bound tokens (RFC 8705 [18]).** Authorization tokens are cryptographically bound to specific TLS certificates. Stealing a token without the matching private key is useless. Tokens are minted locally by each node.
- **SPIFFE identity [19].** Every service carries a verifiable identity in its X.509 certificate, enforced on every mTLS handshake. No directory service or identity provider needs to be reachable.
- **Short-lived certificates.** Service certificates expire in 1 hour (configurable to 24h for DDIL). No revocation infrastructure (CRL, OCSP) is required — certificates simply expire.
- **BGP-style routing.** Nodes discover each other through direct peering. Routes propagate organically through the mesh. When connectivity is lost, each node continues operating with its last-known state.

This is not zero trust bolted onto a centralized architecture. It is zero trust that was designed from the ground up for environments where centralized infrastructure is compromised, unreachable, or nonexistent.

Multi-Party Coordination by Design

The decentralized trust model directly addresses the coalition problem. When two organizations decide to share data, they exchange Root CA certificates out of band and mint certificate-bound tokens defining what each peer is authorized to access. No shared infrastructure, no common identity provider, no VPN tunnel to a joint operations center.

Each organization maintains full sovereignty over its own security posture. Adding a new coalition partner requires only a certificate exchange and token mint — not re-architecting a shared PKI or negotiating access to centralized services.

Compliance and Deployment Readiness

Catalyst satisfies two converging compliance mandates in a single deployment:

Requirement	Standard	Catalyst Status
PQ key exchange	FIPS 203 (ML-KEM)	Deployed (X25519MLKEM768)
PQ signatures	FIPS 204 (ML-DSA)	Architecture ready
Mutual authentication	RFC 8705 + mTLS	Deployed
Zero trust architecture	DoD ZT / NIST 800-207	Aligned
CNSA 2.0 timeline	PQ by 2030	On track
DDIL operations	Army T-ICAM [20]	Native support

Table 1: Compliance posture

Post-quantum key exchange is not a roadmap item — it is deployed and confirmed working in Envoy 1.33+ with BoringSSL's ML-KEM implementation. PQ certificate signatures (ML-DSA) will be adopted as ecosystem support matures, with no changes required to service code or deployment topology.

Bottom Line
Catalyst delivers post-quantum, zero trust, decentralized security for organizations that operate where the network is hostile, the infrastructure is unreliable, and the adversary is already listening. It is deployed today, compliant with both CNSA 2.0 and DoD Zero Trust timelines, and requires no centralized infrastructure to function.

For technical depth on Catalyst's cryptographic architecture and PKI model, see: *Quantum-Ready Security for Contested and Disconnected Operations — Technical Whitepaper.*

References

[1] Cloudflare, "Internet Traffic Patterns in Ukraine Since February 21, 2022." [Online]. Available: https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/

[2] Chatham House, "The Internet Under Attack: Internet Resilience in Ukraine." [Online]. Available: https://www.chathamhouse.org/2024/08/internet-under-attack/04-internet-resilience-ukraine

[3] CircleID, "Starlink in Ukraine: What Three Years of Wartime Connectivity Taught Us." [Online]. Available: https://circleid.com/posts/starlink-in-ukraine-what-three-years-of-wartime-connectivity-taught-us

[4] O. Isik, "Russia Is Rerouting Internet Traffic From Occupied Ukraine Through Its Own Infrastructure." [Online]. Available: https://www.kentik.com/blog/how-ukraine-s-internet-routes-changed-during-the-russian-invasion/

[5] D. Madory, "Rostelecom Hijacks Major Networks in BGP Incident." [Online]. Available: https://www.kentik.com/blog/bgp-route-hijack-by-rostelecom/

[6] C. Cimpanu, "Russia Issues Its Own TLS Certificates." [Online]. Available: https://therecord.media/russia-creates-its-own-tls-certificate-authority

[7] SentinelLabs, "AcidRain: A Modem-Wiper Attack on Viasat KA-SAT." [Online]. Available: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

[8] Access Now, "Myanmar's Military Expands Internet Surveillance with Chinese Technology." [Online]. Available: https://www.accessnow.org/publication/myanmar-internet-surveillance/

[9] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization." [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[10] National Institute of Standards and Technology, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)." [Online]. Available: https://csrc.nist.gov/pubs/fips/203/final

[11] National Security Agency, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Algorithm Requirements." [Online]. Available: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[12] "A Quantum of QUIC: Post-Quantum Cryptography in QUIC," *arXiv preprint*, 2024, [Online]. Available: https://arxiv.org/pdf/2405.09264

[13] Envoy Proxy, "GitHub Issue #33941: X25519MLKEM768 confirmed working in Envoy." [Online]. Available: https://github.com/envoyproxy/envoy/issues/33941

[14] U.S. Department of Defense, "DoD Zero Trust Strategy." [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[15] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "NIST SP 800-207: Zero Trust Architecture." [Online]. Available: https://csrc.nist.gov/pubs/sp/800/207/final

[16] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model Version 2.0." [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model

[17] Defense Information Systems Agency, "DISA Thunderdome: Zero Trust Network Access for DoD." [Online]. Available: https://www.disa.mil/News/2024/DISA-Thunderdome-Prototype

[18] B. Campbell, J. Bradley, N. Sakimura, and T. Lodderstedt, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens." [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8705

[19] Cloud Native Computing Foundation, "Secure Production Identity Framework for Everyone (SPIFFE)." [Online]. Available: https://spiffe.io/

[20] General Dynamics Information Technology, "Zero Trust at the Edge: Securing Mission Partner Communications." [Online]. Available: https://www.gdit.com/perspectives/case-studies/zero-trust-at-the-edge-securing-mission-partner-communications/