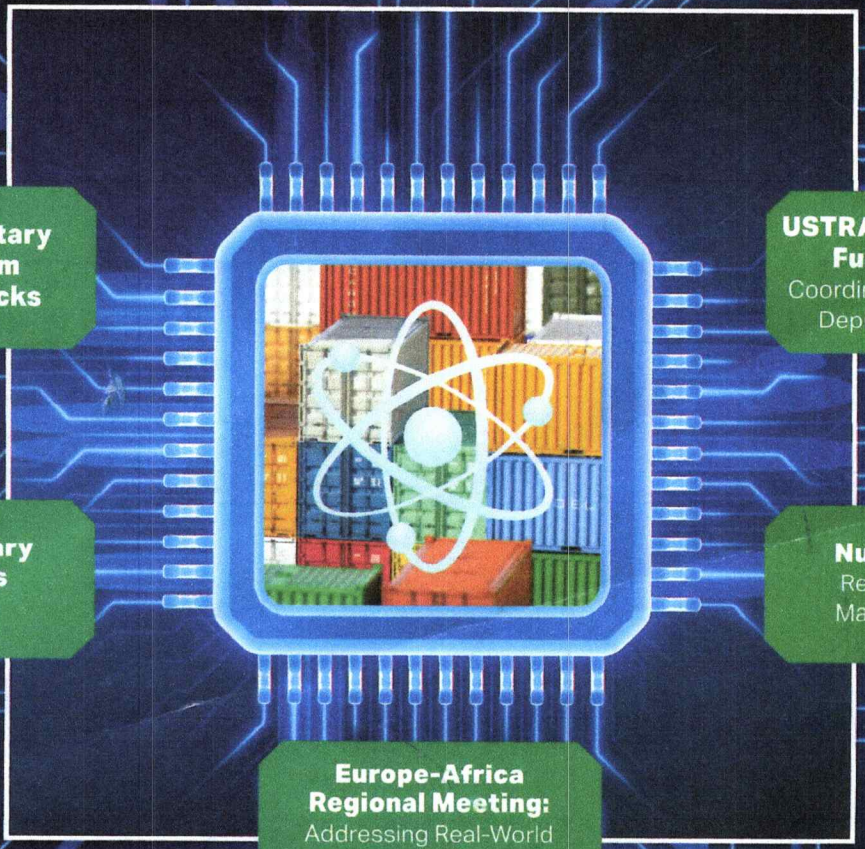
The Official Publication of the National Defense Transportation Association

DTJ Defense Transportation Journal

April 2026 www.ndtahq.com

SECURING THE SUPPLY CHAIN IN A CONTESTED ENVIRONMENT



Protecting Military Logistics from Quantum Attacks

USTRANSCOM'S Turbo Fusion Exercise
Coordinating a Large-Scale Deployment Scenario

Keeping Military Supply Lines on Track

Nuclear Power:
Reshaping Global Maritime Logistics

Europe-Africa Regional Meeting:
Addressing Real-World Challenges

GovTravels Highlights
Page 22

When Trucks, Trains, Ships, and Aircraft Become Endpoints:

Quantum-Ready OT Security for DoD Transport Fleets

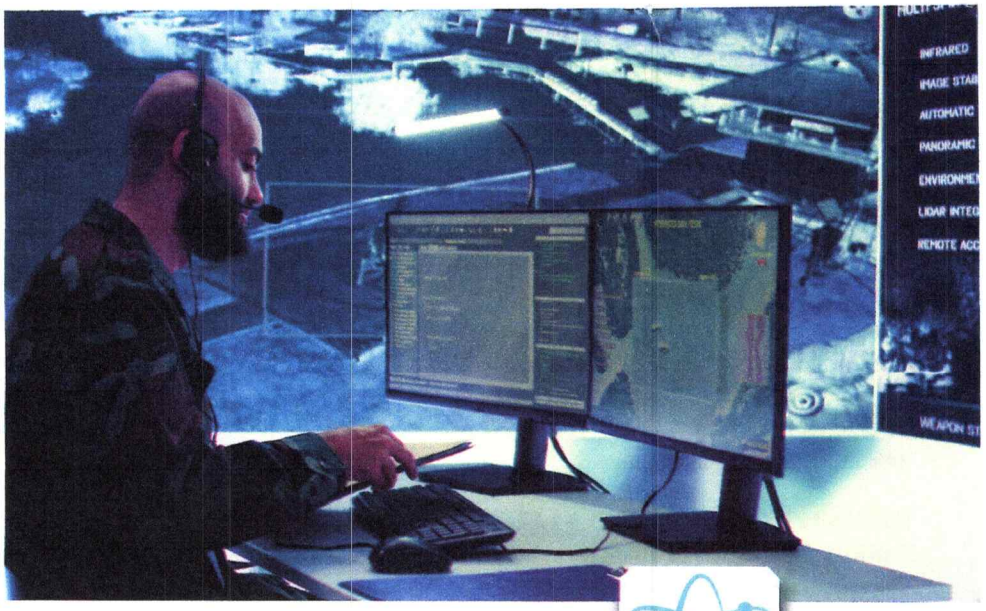
By Federico Simonetti, Chief Technology Officer, Xiid Corporation

Defense transportation professionals face a fundamental tension: modernizing logistics systems for speed, capacity, and precision while protecting operational security from increasingly sophisticated adversaries. Today's transport fleets blend Operational Technology (OT) and Information Technology (IT) in ways that create both unprecedented capability and risk.

The challenge is compounded by mismatched timelines. While IT infrastructure refreshes every three to five years, the platforms that carry warfighters and sustain global operations are built to last decades. A KC-46 inducted into service today will still be flying beyond 2050. Even the humble FMTV tactical truck, equipped with GPS, diagnostics, and wireless connectivity, will serve well into the 2030s.

Yet the cryptographic algorithms protecting the data these platforms generate — movement schedules, maintenance logs, geolocation tracks, partner coordination — were not designed for threats that will emerge over their lifetimes. Adversaries already exploit this vulnerability through "Harvest Now, Decrypt Later" (HNDL) campaigns that intercept encrypted DoD logistics data today to decrypt with quantum computers tomorrow.

Cyber solutions developed for other long lifecycle critical infrastructure — industrial control systems, power grids, water treatment facilities, medical devices — are now proven at scale and directly applicable to defense transportation. By embedding crypto agility and quantum resistant architectures into fleet OT today, U.S. Transportation Command (USTRANSCOM) and its commercial partners can future-proof the backbone that keeps forces supplied, mobile, and ready in contested environments.



THE OPERATIONAL TECHNOLOGY EXPLOSION IN MILITARY LOGISTICS

A decade ago, most military vehicles were endpoints only in the physical sense. They moved cargo and people, period. Today, even legacy platforms have been retrofitted with systems that generate, transmit, and store data: satellite terminals for beyond line of sight communication, telematics modules tracking fuel consumption and engine hours, AIT tags broadcasting container contents, and wireless diagnostic interfaces on the motor pool or flightline.

Military Sealift Command vessels, Air Mobility Command aircraft, and Army Transportation Command movements now feed real-time status into the Joint Deployment and Distribution Enterprise, enabling visibility that was unthinkable a generation ago. That visibility has measurably improved readiness and responsiveness, but it has also turned every truck, train, ship, and aircraft into an attack surface.

This isn't theoretical. In 2024, cybersecurity researchers documented a 39% increase in attacks targeting automotive and smart mobility ecosystems, with 60% of successful intrusions capable of affecting millions of connected devices. Defense logistics operates in that same ecosystem, often relying on the same commercial telematics providers, cellular networks, and over the air update mechanisms that civilian fleets use. When an adversary compromises a commercial fleet management platform, they don't distinguish between Amazon delivery vans and contract carriers hauling munitions to a defense transportation hub.

By embedding crypto agility and quantum resistant architectures into fleet OT today, USTRANSCOM and its commercial partners can future proof the backbone that keeps forces supplied, mobile, and ready in contested environments.

WHY LEGACY OT CAN'T BE RIPPED AND REPLACED

Unlike enterprise IT, where server refreshes are disruptive but manageable, defense transportation OT is woven into platforms that cannot be easily modified. Aircraft avionics systems are certified for airworthiness under strict configuration control; changing a cryptographic module can trigger recertification processes that take years and cost millions. Ships' integrated bridge systems and machinery control consoles are designed for 20-year service intervals. Ground vehicles fielded under urgent operational needs often lack the software hooks to accept security patches without a depot-level rebuild.

Security professionals call these "unmodifiable systems" that must be secured as is, without replacing vulnerable components. In the commercial world, this challenge is most visible in industrial control

systems (ICS) and SCADA environments, such as power plants and water treatment facilities, where downtime is measured in millions of dollars per hour and firmware updates require months of testing.

Defense transportation faces the same constraints, complicated by platforms that operate in hostile electromagnetic environments, across contested networks, and often in coalition operations where security architectures must interoperate with allied systems on their own timelines.

THE HARVEST NOW, DECRYPT LATER THREAT TO LOGISTICS DATA

Transportation security professionals understand traditional cyber threats such as ransomware, denial of service, and data exfiltration. HNDL represents a different calculus. Rather than exploiting data immediately, adversaries intercept and store encrypted communications, betting that quantum computers — expected to achieve cryptographic relevance within the next decade — will allow them to decrypt that traffic retroactively.

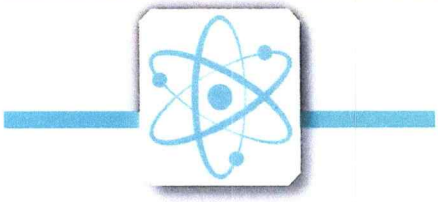
For defense logistics, this threat is especially pernicious because transportation data retains intelligence value for decades. A sealift manifest encrypted and transmitted in 2026 still reveals force disposition, supply chain dependencies, and partner nation cooperation patterns when decrypted in 2035. Predictive maintenance data can reveal operational tempos and deployment patterns. Even seemingly mundane GPS tracks, aggregated over months, can expose doctrine, training areas, and prepositioning strategies.

Per NSA guidance, nation state actors are actively harvesting encrypted government and defense traffic today, anticipating that cryptanalytically relevant quantum computers will render current encryption algorithms — Rivest Shamir Adleman (RSA), elliptic curve cryptography (ECC), and even some implementations of AES — vulnerable within 10 to 15 years. For OT systems designed to operate for 20 to 30 years, this timeline is a planning reality.

THIRD-PARTY VENDORS AND SLEEPER CELLS IN THE LOGISTICS CHAIN

The logistics cyber problem even harder to solve is due to third-party vendors and potential "sleeper cells" embedded in the ecosystem. Commercial carriers, telematics providers, maintenance depots, and software vendors all connect into the data flows that sustain warfighter mobility. A compromise in any one of these environments can give adversaries indirect access, often without touching a .mil network directly.

Photo Credit: Xiid Corporation



In a globally distributed logistics enterprise that depends on thousands of partners, it is unrealistic to assume every node is always clean.

Sleeper cells — compromised systems, implants, or even insiders that sit quietly inside partner or subcontractor environments — can watch, exfiltrate, and wait for a favorable moment, or simply participate in HNDL campaigns by siphoning encrypted traffic for future quantum decryption. In a globally distributed logistics enterprise that depends on thousands of partners, it is unrealistic to assume every node is always clean.

This is where deterministic, outbound-only, process-bound architectures matter. Instead of assuming that every vendor or node can be perfectly defended, they assume compromise is possible and focus on blocking expansion. Even if a sleeper cell resides on a partner system, it cannot pivot into mission systems if there are only tightly scoped, cryptographically enforced, process-to-process connections.

BUILDING CRYPTO-AGILITY INTO FLEET OT

Rather than wait for quantum-resistant algorithms to mature and then retrofit decades-old platforms, the solution is to architect transportation OT systems today with crypto-agility: the ability to swap cryptographic algorithms without hardware changes, extensive recertification, or operational downtime.

This is already happening in critical infrastructure. The National Institute of Standards and Technology (NIST) has published three post quantum cryptographic standards — ML KEM (Kyber), ML DSA (Dilithium), and SLH DSA (SPHINCS+) — designed to resist attacks from both classical and quantum computers. The National Security Agency's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) mandates that National Security Systems transition to these algorithms on a phased timeline, with full implementation required by 2035.

For defense transportation, this means:

1. **Inventory crypto dependencies across the fleet.** Every telematics module, satellite terminal, and diagnostic interface uses encryption. Transportation commands need to know which algorithms are in use, which systems can be upgraded remotely, and which require hardware replacement or gateway solutions.
2. **Prioritize upgrades for long-lived, high-value data flows.** Not all logistics data have equal intelligence value. Movement orders, partner coordination, and classified cargo manifests warrant immediate migration to post

quantum encryption. Routine maintenance logs for nonsensitive systems can follow a longer timeline.

3. **Design outbound-only process-to-process communication architectures.** Traditional OT cybersecurity still has vehicles, trains, ships, and aircraft using publicly routable IP addresses and open inbound ports to communicate with command centers and logistics hubs. This creates persistent attack surfaces that adversaries can scan, probe, and exploit. Modern architecture eliminates this exposure entirely by using secure connections that make fleet assets undiscoverable to external reconnaissance while maintaining full operational capability.

HOW DETERMINISTIC SECURITY ARCHITECTURES ENABLE MISSION-READINESS ON CONTESTED NETWORKS

A common objection to hardening fleet OT is the assumption that stronger security will degrade performance or complicate operations. The opposite is often true, especially in the degraded, intermittent, and limited bandwidth environments where military logistics operates.

Deterministic architecture establishes encrypted tunnels from the vehicle, train, ship, or aircraft to command infrastructure, rather than requiring platforms to accept inbound connections. This has several operational advantages:

Zero exposed endpoints. Because all communication is initiated by the platform, firewalls can remain fully closed, making assets undiscoverable to scanning and exploitation attempts. This is especially critical for platforms operating on commercial cellular networks, public Wi Fi at aerial ports of debarkation, or coalition networks where adversaries may already have a foothold.

Process-to-process segmentation. Rather than granting network level access to an entire vehicle, train, aircraft, or ship, modern tunneling technologies create isolated communication channels for each application — telematics, diagnostics, mission planning. Even if one system is compromised, adversaries cannot pivot laterally to other systems on the platform.

Triple-layer, quantum-resistant encryption. Defense grade architectures layer multiple encryption methods — TLS 1.3 for transport security, post quantum algorithms (Kyber, Dilithium) for key establishment and authentication, and AES 256 for data confidentiality. Even if one layer is compromised, the others continue to protect the data.

Reliable operation on dirty networks. Platforms must communicate over satellite links with high latency, tactical radios with intermittent coverage, and foreign cellular networks with unpredictable quality of service. Packet buffering and error correction, designed into quantum ready tunneling architectures, ensure that mission critical data — maintenance alerts, location updates, cargo status — reaches its destination even when the network degrades.

REAL-WORLD VALIDATION: DOD AUTHORITY TO OPERATE

In 2024, the U.S. Air Force Research Laboratory (AFRL) conducted penetration testing on Terniion™, a quantum ready, pre-emptive technology platform, and concluded that the patented system demonstrated "near invisibility" to external reconnaissance and was impenetrable to standard attack methodologies. This validation led to the company earning an unconditional Authority to Operate (ATO) from the Department of Defense — a designation not awarded to any other cybersecurity vendor. This signals that the technology is operationally proven, not experimental. Terniion is already protecting workloads for the Defense Health Agency, CI/CD pipelines for defense contractors, and sensitive data flows for federal agencies. The platform scales from a single tactical vehicle to global fleets with tens of thousands of platforms, with the ability to spin up secure tunnels in minutes and manage them from a single control plane.

PRACTICAL STEPS FOR U.S. TRANSPORTATION COMMAND

For USTRANSCOM components, commercial partners, and logistics organizations, the path forward isn't to wait for quantum computers to arrive and then react. It's to embed quantum-readiness into fleet modernization efforts already underway:

1. **Treat telematics and diagnostics as tactical data systems, not maintenance tools.** Every connected platform is a potential intelligence source for adversaries. Apply the same security rigor to fleet management systems that you apply to command-and-control networks.
2. **Demand crypto agility in new procurements.** When specifying requirements for next generation vehicles, aircraft, and vessels, include mandates for post quantum encryption and algorithm agile architectures. Commercial vendors are already building these capabilities for civilian critical infrastructure. DoD should leverage that investment.
3. **Pilot gateway based protections for legacy fleets.** For platforms that cannot be modified, small form factor gateways — Raspberry Pi class devices — can handle external communications using quantum resistant tunnels while legacy OT continues to operate unchanged. This "overlay" approach allows incremental hardening without triggering recertification or disrupting operations.
4. **Coordinate with allies and commercial partners on interoperable standards.** Coalition operations depend on seamless logistics integration. As the U.S. migrates to CNSA 2.0 and post quantum standards, allies and commercial carriers need clear guidance and transition timelines to maintain interoperability.

Transportation professionals have spent careers solving age-old problems centered on how to move mass and equipment faster, farther, and more efficiently. The connectivity that enables today's precision logistics creates vulnerabilities that adversaries are exploiting right now, betting that quantum computing will unlock the intelligence value of encrypted logistics data for decades to come.

We aren't locked into that future. By treating every transport as a cyber endpoint and embedding crypto-agility, adopting quantum-resistant encryption, and designing systems to operate securely on contested networks, we can ensure the strategic mobility backbone remains resilient against both today's threats and tomorrow's decryption capabilities. **DTJ**

ABOUT THE AUTHOR

Federico Simonetti serves as Chief Technology Officer at Xiid Corporation, where he leads development of quantum-resistant security architectures for critical infrastructure and defense systems. Contact Fed at federico@xiid.com.