G1VE TECHNOLOGIES

QUANTUM COMMAND. AI AT THE EDGE.

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

Sep 22, 2026

Original source

https://www.linkedin.com/pulse/quantum-command-ai-edge-carrington-mba-lssmbb-ctpra-grca-grcp-dfgae/

Why Post-Quantum Resilience, Federated Intelligence, and Mission Assurance Are Becoming the Joint Force Advantage

I. The Most Important Quantum Signal This Summer Did Not Come From A Quantum Computer. It Came From AI.

The most consequential quantum-security development of the summer may not have come from a quantum laboratory.

It came from Artificial Intelligence.

In late July, an AI model identified a mathematical vulnerability in HAWK, one of the digital-signature algorithms being evaluated through the National Institute of Standards and Technology (NIST) 's Post-Quantum Cryptography standardization process. The HAWK development team subsequently withdrew the algorithm from consideration.

The National Institute of Standards and Technology (NIST) was explicit that the discovery did not compromise its already-finalized Post-Quantum Cryptography standards, including ML-KEM and ML-DSA.

But the strategic implication reaches much further than one candidate algorithm.

AI is no longer merely something that must be secured by cryptography.

AI is increasingly becoming part of the machinery used to interrogate, test, challenge, and validate cryptography itself.

That matters because the United States is simultaneously accelerating three technology transitions that are usually discussed separately.

AI is moving toward operational workflows.

Quantum technology is moving from laboratory investment toward national capability.

And the cryptographic architecture protecting government, intelligence, critical infrastructure, logistics, identities, software, sensors, models, and command systems is being rebuilt beneath both of them.

Those are not three independent transitions anymore.

They are becoming one.

And the organizations that recognize that convergence early will be better positioned to preserve something far more important than technological advantage.

They will preserve trusted command at machine speed.

II. The Quantum Deadline Is Not 2035. The Operational Deadline Has Already Started.

For years, Post-Quantum Cryptography could be treated as a future-state architecture problem.

That interpretation became much harder to sustain in June 2026.

Executive Order 14412 directed an accelerated Federal migration toward the National Institute of Standards and Technology (NIST) -approved Post-Quantum Cryptography. The order establishes milestones for high-value assets and high-impact systems and directs the Federal Acquisition Regulatory Council to develop procurement requirements affecting covered contractors.

Two days later, the Office of Management and Budget Memorandum M-26-15 converted that policy direction into an execution model.
Federal agencies were directed to develop PQC migration plans, establish internal governance, prioritize high-impact systems and High Value Assets, integrate cryptographic migration with modernization, and build toward a risk-prioritized Federal transition.
The migration sequence now extends from discovery and planning in 2026–2027, through pilots and early migration in 2027–2028, prioritized key-establishment migration through 2030, signature migration in 2031, and broader migration through 2035.
That sequence changes the leadership question.
The question is no longer:

- When will quantum computers become powerful enough to matter?

...The better question is:

- How long will it take to discover, replace, validate, fund, acquire, field, and continuously manage every vulnerable cryptographic dependency across an operational enterprise?

Those are profoundly different timelines.
A cryptographically relevant quantum computer does not need to exist today for quantum risk to affect today's architecture.
The Office of Management and Budget explicitly prioritizes systems containing data expected to remain mission-sensitive in 2030. The White House 's June order also identifies the risk of adversaries collecting encrypted information now for potential decryption later.
For the Intelligence Community, Joint Force, Combatant Commands, cyber forces, logistics enterprise, critical infrastructure operators, and Defense Industrial Base, the consequence is straightforward: Data lifetime has become part of the threat model.

III. AI At The Edge Multiplies The Trust Problem.

At exactly the same moment that government is rebuilding its cryptographic foundation, AI is becoming more distributed.
That distribution is operationally necessary.
The United States Department of War 's FY26 Frontier AI Accelerator is evaluating how frontier models affect mission effectiveness, decision quality, workflows, doctrine, personnel, and compute requirements across different modalities and classification levels. The United States Department of War's stated performance objective includes optimizing its federated infrastructure to scale data, analytics, and AI adoption.
The United States Department of War has also continued expanding its enterprise AI environment. On August 31, it announced OpenAI ChatGPT Mil on GenAI.mil at Impact Level 5 for CUI workloads, describing a multi-model environment intended to scale across more than three million United States Department of War personnel and support planning, policy, logistics, administration, and other workflows.
Meanwhile, The Joint Staff 's FY26 budget justification describes decision-support applications interoperating with the DoW Super Intelligence Office - SIO (formerly CDAO) 's data environment and systems including Advana, Advana Edge, Maven Smart Systems, SUNet, and Army Vantage, integrated with the CJADC2 Data Integration Layer.

This is where the quantum issue stops being a cryptography-office issue.
Every time intelligence, models, agents, applications, sensors, APIs, identities, and mission data become more distributed, the number of trust relationships grows.
A headquarters can govern one model.
A Joint Force must govern models operating across:

- Land.
- Sea.
- Air.
- Space.
- Cyber.

...Across classification levels.
...Across cloud and edge.
...Across government and commercial infrastructure.
...Across allies, mission partners, contractors, sensors, autonomous systems, and disconnected or degraded environments.
...And every one of those relationships eventually depends on cryptographic assertions:

- Who signed the software?
- Who authenticated the device?
- Who issued the credential?
- Was the model artifact modified?
- Can the data lineage be trusted?
- Is the API request authentic?
- Is the command message legitimate?
- Is the model update authorized?
- Can the receiving node verify all of that while disconnected from the enterprise?

...AI at the edge therefore creates an uncomfortable reality: The more distributed the intelligence architecture becomes, the more consequential cryptographic trust becomes.
Federation without trusted identity is not federation. It is exposure.

IV. Quantum Is Also Moving From Research Portfolio To Operational Planning.

There is another reason this moment matters. The United States is not treating quantum solely as a defensive cryptography problem.
Executive Order 14413, issued June 22, directs an update to the National Quantum Strategy, establishes the Quantum Computer for Application Development and Discovery Science effort, requires further assessment of the national security implications of increasingly capable commercial quantum computing, and directs the Secretary of War Pete Hegseth to establish or designate activities supporting readiness for national security applications of quantum computing.
The order also directs the United States Department of War to identify at least three next-generation quantum sensor projects for prioritization toward fielding by September 30, 2028.
The Defense Advanced Research Projects Agency (DARPA) is attacking the problem from another direction.
Its Quantum Benchmarking Initiative is attempting to determine whether industrially useful, utility-scale quantum computing can be built by 2033. Rather than accepting vendor claims at

face value, the program progresses architectures through concept definition, R&D risk reduction, and government verification and validation.

As of the current program structure, the Defense Advanced Research Projects Agency (DARPA) describes QBI as a mechanism to separate technically credible pathways from quantum hype through independent assessment.

That combination is important. The United States is simultaneously:

- Preparing to use quantum capability;
- Preparing to measure quantum capability; and,
- Preparing to survive quantum capability.

That is the beginning of something larger than quantum computing policy. It is the beginning of a quantum readiness architecture.

V. Quantum Command Requires Four Trust Planes.

If AI, quantum, cyber, data, and Joint All-Domain operations continue converging, the future command architecture cannot be secured through one control framework at a time.

My operational synthesis is that the architecture increasingly needs four interlocking trust planes:

1. Cryptographic Trust — Every device, workload, identity, API, software artifact, certificate, and command pathway must be able to transition away from quantum-vulnerable dependencies without requiring another enterprise rebuild. That means crypto-agility becomes a mission requirement, not merely a technical preference. The Office of Management and Budget 's implementation guidance goes unusually far here. It calls for automated discovery, configuration-driven cryptography, agile key-management infrastructure, and a continuously updated cryptographic inventory feeding a Cryptographic Bill of Materials.
2. Model Trust — A model operating at the edge must have a: Defensible identity. Version. Provenance. Approved operating boundary. Evaluation history. Permitted data classes. Known dependencies. Authorization state. Model governance without cryptographic enforcement eventually becomes documentation describing a system that may already have changed.
3. Data Trust — Federated intelligence depends on knowing what entered the decision environment and how it moved. ISR feeds, logistics telemetry, cyber indicators, targeting support data, maintenance information, supply-chain signals, autonomous-system inputs, and intelligence products cannot become indistinguishable blobs feeding an AI layer. The model may reason at machine speed. Its data still requires provenance.
4. Command Trust — This is the layer that ultimately matters. A technically valid model output is not automatically an authorized military decision. A cryptographically authentic command is not automatically a strategically correct command. A trusted AI architecture therefore requires the ability to establish not only who and what produced an output, but also who possesses authority to act on it.

That is where AI Governance, Zero Trust, mission command, cybersecurity, identity, data governance, test and evaluation, and Mission Assurance finally meet.

VI. The Acquisition System Is About To Become Part Of The Enforcement Layer.

The next mistake would be assuming all of this stays inside CIO, CISO, NSA, CDAO, or laboratory channels.

It will not. EO 14412 directs the FAR Council to develop a proposed rule requiring covered contractors to comply, by December 31, 2030, with applicable National Institute of Standards and Technology (NIST) FIPS requirements incorporating PQC-compliant algorithms.

The Office of Management and Budget 's M-26-15 separately instructs agencies to incorporate vendor and third-party software considerations into migration planning and specifically identifies third-party coordination as a required component of agency migration plans.

The National Security Agency is already pushing the National Security System ecosystem in the same direction.

The March 2026 Mobile Access Capability Package and updated Key Management Requirements introduced CNSA 2.0 objective requirements as the Commercial Solutions for Classified program advances toward Post-Quantum Resistant cryptography. The National Security Agency 's planning material describes a goal for registered CSfC solutions to have CNSA 2.0 algorithms or other post-quantum mitigations across cryptographic layers by 2030.

The National Institute of Standards and Technology (NIST) is also working the identity layer. Its June 2026 PIV working drafts examine how ML-KEM and ML-DSA could be introduced through a dual-stack approach supporting incremental PQC deployment while maintaining compatibility with existing credentials.

Read these signals together. PQC is moving toward:

1. Architecture requirements.
2. Identity requirements.
3. Cloud requirements.
4. Product requirements.
5. Contract requirements.
6. Supplier requirements.

...That creates a direct implication for the Defense Industrial Base. Future acquisition advantage will not come only from claiming a product is "quantum safe."

It will come from being able to prove where cryptography exists, which standards are implemented, how quickly algorithms can be replaced, what dependencies remain, and whether the entire delivery chain can migrate without breaking the mission.

The CBOM may eventually become to cryptography what the SBOM became to software supply-chain visibility.

And organizations waiting for the final contract clause before beginning discovery will have voluntarily surrendered years of preparation time.

VII. Three Moves For The Next 90 Days

Senior leaders do not need a quantum computer in their data center next quarter. They need visibility and architectural control. Three moves are actionable now:

1. Build The Cryptographic Mission Map — Do not stop at an enterprise inventory. Map cryptographic dependencies to mission consequence. Which certificates protect logistics? Which authentication chains protect command applications? Which PKI dependencies

protect operational identity? Which APIs connect AI workloads? Which encryption protects information that must remain sensitive into the 2030s? The objective is not a spreadsheet. The objective is knowing which mission fails when a cryptographic dependency fails.

2. Bind AI Governance To Cryptographic Identity — Every model entering an operational federation should eventually be treated like a mission workload with a verifiable identity. Model version, signature, provenance, authority, configuration, evaluation status, permitted data classes, and operating boundary should travel with the artifact. A model card tells you what a system is supposed to be. Cryptographic verification helps determine whether the system in front of you is actually that system.
3. Move PQC Readiness Into Acquisition Before The Clause Arrives — Program offices, contracting organizations, CIOs, CISOs, acquisition executives, cloud providers, integrators, and suppliers should already be asking about crypto-agility. The valuable questions are increasingly practical: Can the product support ML-KEM? Can certificates migrate? Can cryptographic providers be replaced without recompilation? Can HSMs support both classical and PQC keys during transition? Can the supplier produce cryptographic dependency information? Can edge equipment absorb increased key, signature, bandwidth, memory, and compute requirements? Can the system remain interoperable during hybrid migration? Those questions belong in market research and architecture reviews now. Not after source selection.

VIII. Thought-Provoking Close — Command The Trust Layer

The defining competition is not AI versus quantum. It is not even AI plus quantum.

The deeper problem is whether the systems connecting intelligence, machines, people, sensors, software, data, logistics, identity, and command can remain trusted while both technologies accelerate.

AI is pushing decision-making outward.

Quantum is forcing cryptography forward.

Federated architectures are multiplying trust relationships.

JADC2 is connecting domains that were once easier to isolate.

The Intelligence Community increasingly requires data and models to move across boundaries without losing provenance.

Critical infrastructure and the Defense Industrial Base sit underneath the same technology supply chains.

And acquisition policy is beginning to translate the transition into requirements industry will eventually have to demonstrate, not merely acknowledge.

The future Joint Force does not need quantum hype.

It needs quantum readiness. It needs AI that can operate at the edge without outrunning governance.

It needs cryptography capable of changing without replacing the entire mission architecture.

It needs federated intelligence without federated ambiguity.

And it needs Mission Assurance that assumes tomorrow's technological advantage may depend on decisions made about today's invisible dependencies.

The next era of command will belong to organizations capable of maintaining trusted decisions across contested networks, changing algorithms, distributed models, uncertain data, and machine-speed operations.

Quantum Command is not command by a quantum computer.
It is command of the trust layer beneath the entire force.
That work has already started.

✨ Call to Action: Step Into the Arena ✨

Most professionals will read about the future. A select few will shape it.
If you are serious about staying ahead of the curve in Artificial Intelligence, Regulatory Compliance, and Enterprise Risk, this is where you need to be.
📩 Subscribe to Future Trends & Insights: AI to gain direct access to:

1. Strategic foresight on AI Governance & Ethical Deployment
2. Real-world applications across National Security & Mission Assurance
3. Advanced GRC, TPRM, and Regulatory Compliance frameworks
4. Emerging Fintech and Risk Intelligence innovations

⚔️ The landscape is shifting—fast. The gap between those who understand and those who execute is widening.
This is built for professionals responsible for decisions that carry consequence—not commentary.
📅 Ready to operationalize these insights and move beyond theory?
👉 https://calendly.com/g1ve-technologies
Let us translate insight into measurable, defensible outcomes—and build capability, not just conversation.

🔍 About the Author

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP is a National Security-aligned Artificial Intelligence Strategist/Tactician and Governance, Risk, and Compliance (GRC) Authority/Subject Matter Expert with over a decade of experience operating at the intersection of National Security, National Defense, Critical Infrastructure, Cybersecurity, AI Governance, Mission Assurance, Mission-Critical Systems, and Predictive Funding/Grant Intelligence.
As Managing Partner at G1VE Technologies, LLC and a Strategic Board Advisor, W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP architects and operationalizes enterprise-scale risk, compliance, and AI governance ecosystems across both Public and Private Sector environments—including Fortune 500/1000 organizations and Federal-aligned missions, where failure is not an option.
His work is centered on delivering Decision Advantage, strengthening Operational Resilience, and enabling organizations to navigate high-stakes, high-uncertainty environments with precision and confidence.
📡 Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP here to stay at the forefront of:

- Artificial Intelligence
- National Security
- GRC
- Cyber Risk
- Regulatory Strategy
- Mission Assurance