

CBRNE Readiness in the Age of Edge Decision-Making: A Technical and Strategic Imperative

The Threat Landscape: Convergence at the Tactical Edge

The 2025 global CBRNE threat environment is no longer compartmentalized; it is integrated, asymmetric, and edge-accelerated. Adversaries exploit dual-use technologies, permissive scientific environments, and open-access knowledge to disrupt detection and response architectures. The increasing confluence of chemical, biological, radiological, nuclear, and explosive threats with cyber operations and artificial intelligence (AI) capabilities has produced a multi-domain threat vector designed for strategic ambiguity and tactical surprise.

Chemical threats have evolved beyond legacy agents to include repurposed industrial materials (e.g., fentanyl analogs, chlorine), and designer compounds like Novichok. Biological risks are catalyzed by democratized synthetic biology, antimicrobial resistance, and the proliferation of gain-of-function research with minimal oversight. Radiological threats now include unsecured isotopes and deliberate sabotage of medical or energy infrastructure, while nuclear risks reflect both strategic proliferation and the operational deployment of tactical warheads in gray zone conflict theaters. Explosive threats are increasingly hybridized employing autonomous delivery platforms (e.g., drone swarms), electronic warfare, and kinetic payloads in converged attacks.

We're living in a world where the consequences of natural disasters, industrial accidents, and deliberate attacks are no longer clear. Floods, fires, and storms disrupt infrastructure and public health. At the same time, global instability and displacement are pushing more people into vulnerable environments. Layered on top of that is our deep reliance on interconnected systems where a cyberattack on a water plant or a power grid can cause cascading effects that look a lot like sabotage, even if they weren't.

In this new operating environment, the threshold between what's natural, what's accidental, and what's intentional is blurring. That makes attribution harder. It slows our response. And it creates openings that our adversaries are prepared to exploit. The mission we

share across government, industry, and academia is to bring clarity, speed, and resilience to that uncertainty, using every tool at our disposal including artificial intelligence to stay ahead of the next crisis.

This convergence demands a technical architecture capable of distributed sensing, autonomous assessment, and edge-level decision dominance the cornerstone of AI-enabled readiness.

Edge-Oriented Decision Superiority: Lessons from Operation Midnight Hammer

Operation *Midnight Hammer* (22 June 2025) serves as a great example of edge-deployed, AI-orchestrated decision cycles. **As publicly reported, seven B-2 Spirits executed a 7,000-mile**

mission to neutralize hardened Iranian nuclear targets at Fordow, Natanz, and Isfahan with pinpoint precision. The operation leveraged over 125 integrated platforms airborne, cyber, and maritime while maintaining complete electromagnetic and operational surprise.

Open-source intelligence attributes the mission's success to a cohesive AI infrastructure. Decision cycles traditionally measured in hours were compressed into minutes through real-time weaponeering, deception planning, and route optimization. Multimodal fusion engines integrated satellite imagery, electronic order-of-battle, and open-source intelligence to algorithmically prioritize targets and select penetration vectors. Simulation

agents powered by digital twins of the B-2 and its payload likely iteratively computed thousands of route permutations under constraint to choreograph synchronized multi-domain entry.

This is not merely an exercise in automation it is a demonstration of distributed AI executing in contested domains, with decision authority delegated to edge nodes, bounded by policy, and audited through model interpretability.

AI as a CBRNE Mission Multiplier: From Theater Strike to Tactical Shield

The doctrinal implications for the CBRNE community are profound. If AI can fuse and orchestrate 125 assets across multiple warfighting domains for

nuclear target suppression, it can equally coordinate chemical sensor data, radiological plume tracking, bioagent dispersion modeling, and casualty telemetry to enable real-time exposure forecasting and adaptive logistics.

AI-driven CBRNE readiness shifts the strategic focus from detection to disruption. Predictive models trained on environmental, biological, and operational signatures can provide anticipatory warning, optimize evacuation or containment paths, and algorithmically cue supplies from antidotes to specialized PPE via prescriptive logistics engines operating at the tactical edge.

This reframes the industrial imperative: open architectures, calibrated models, and low-SWaP (size, weight, and power)

edge-compute hardware are no longer research initiatives they are prerequisites for survivability.

Policy Synchronization and AI Governance: Section 1621 as a Systems Integrator

Section 1621 of the FY25 NDAA codifies a structural realignment vital to this future. By establishing the Assistant Secretary of Defense for Nuclear Deterrence and Chemical Biological Policy and Programs with statutory oversight of policy, acquisition, and sustainment across the nuclear enterprise Congress has effectively created a civilian systems integrator for strategic deterrence.

This office, now responsible for supervising AI-enabled applications

across the deterrence enterprise (e.g., predictive warhead maintenance, machine-speed NC3 anomaly detection, algorithmic cross-checking of targeting data), serves as both an architectural and governance model. Direct access to the Secretary of Defense eliminates latency in aligning doctrine with technological capability, while unified oversight across triad modernization, sensor integration, and command architectures fosters coherent acquisition across traditionally siloed efforts.

The CBRNE community should mirror this integration: fusing bio-surveillance, nuclear forensics, radiological hazard detection, and digital command structures under a unified AI-governance framework.

Edge Intelligence for Indications and Warnings (I&W): A Model-Based Doctrine

Modern CBRNE defense requires a pivot from monolithic, centralized command to model-driven, edge-deployable autonomy. AI enables this shift through:

Sensor Fusion: Multi-spectral, cyber-physical, and biosurveillance streams aggregated and interpreted at the edge, not just the cloud.

Model Calibration: Adaptive learning systems update priors in real-time using Bayesian inference, graph neural networks, and reinforcement learning to reflect environmental or adversarial shifts.

Prescriptive Logistics: AI agents simulate supply chains under disruption,

recommending optimal resource allocation and delivery timing under contested logistics.

Such systems elevate I&W from event detection to pattern anticipation, enabling the CBRNE force to intervene within the adversary's decision cycle. (Proactive and Predictive Risk Assessment conducted continuously)

Doctrinal Edge: From Human-in-the-Loop to Human-on-the-Loop

The concept of *human-on-the-loop*—in which AI systems recommend, simulate, and even act within bounded autonomy before human adjudication is no longer theoretical. CBRNE scenarios where seconds matter (e.g., aerosolized

bioagent dispersion, radiological device detonation) demand edge autonomy with pre-defined response constraints and model interpretability.

The future of AI-governed CBRNE decision-making requires:

- . **Distributed Model Execution:**
Federated learning architectures that maintain accuracy across disconnected edge nodes.
- . **Explainable Decision Chains:**
Auditable logic that justifies each alert, recommendation, or action traceably.
- . **Policy-Constrained Autonomy:**
Machine agents that understand legal, ethical, and domain-specific rulesets for engagement.

Conclusion: Rebuilding Deterrence Through Data-Centric Defense

Reviving the defense industrial base is not about building more it's about building smart. Academia, startups, and prime contractors must converge to deliver interoperable systems that support edge inference, continuous learning, and human-machine collaboration under operational constraint.

AI in the CBRNE space is not an experiment; it is an obligation. It compresses time, extends reach, and elevates precision in decision-making at the moment of consequence. From Operation Midnight Hammer's strategic choreography to the statutory fusion of policy and acquisition under Section 1621, the template for data-centric deterrence is here.

The question is not *if* we integrate AI into our sensing, warning, and response architecture but how soon, how responsibly, and how decisively we act.