National Security Risk Assessment: AI-Driven Acceleration of Asymmetric, CBRN, Mass Casualty, and Cyber-Physical Operations

DATE: November 5, 2026 PUBLISHED BY: Black Eagle Group

1. EXECUTIVE SUMMARY

The integration of generative artificial intelligence models, autonomous agentic workflows, and domain-specific computational tools has altered the operational environment for state adversaries and non-state actors. Artificial intelligence functions as an operational accelerator that lowers technical barriers across complex threat domains.

Historically, executing high-consequence operations—such as Chemical, Biological, Radiological, or Nuclear (CBRN) threat development, asymmetric kinetic attacks, mass casualty planning, and cyber-physical disruptions—required extensive state backing, specialized academic expertise, and extended planning horizons. Today, the availability of open-weight Large Language Models (LLMs), local offline execution environments, and computational design tools enables actors to streamline research, development, and target acquisition cycles. This assessment evaluates threat vectors across chemical weapons, radiological dispersal, improvised explosive devices (IEDs), mass casualty attack planning, and Purdue-model cyber-physical disruptions.

2. THREAT VECTOR ANALYSIS

A. Chemical Weapons & Toxic Material Synthesis

AI models and computational tools lower technical hurdles across the conceptualization and synthesis phases of chemical threats by leveraging dual-use algorithms originally developed for drug discovery and molecular research.

- **Generative Molecule Design & Toxicity:** Machine learning models and molecular libraries can be adapted to evaluate and prioritize molecular structures exhibiting high toxicity profiles, assisting actors in exploring candidate structures relevant to chemical threat agents.
- **Retrosynthesis & Precursor Evasion:** AI-driven retrosynthesis engines calculate alternative chemical synthesis pathways for restricted compounds, enabling actors to identify viable, commercially available, unscheduled precursors that bypass standard supply chain watchlists.
- **Reaction Parameter Optimization:** Predictive modeling tools assist in optimizing reaction parameters—including temperature, stoichiometric ratios, and solvent compatibility—thereby stabilizing improvised laboratory synthesis and minimizing operator exposure risks.

B. Radiological Materials: Dispersion & Acquisition

While AI does not alter the physical laws of fissile material enrichment, it optimizes the operational planning of Radiological Dispersal Devices (RDDs / "Dirty Bombs"). Autonomous OSINT agents cross-reference public registries and industrial radiography inventories to locate vulnerable commercial radioisotopes. Coupled with local meteorological feeds and Computational Fluid Dynamics (CFD) software, actors model urban wind shear and particulate settling to calculate explosive-to-isotope ratios for targeted contamination.

C. Asymmetric Weapons & Advanced IED Engineering

AI tooling assists non-state actors in transitioning from crude improvised devices to engineered explosive systems and optimized firing mechanisms.

- **Explosive Formulation & Precursors:** Retrosynthesis and formulation models assist in identifying alternative energetic mixtures and stabilizing improvised explosive formulations (HMEs) while reducing preparation hazards.
- **Microcontroller Firmware & Triggers:** Code-generation models automate the creation of embedded firmware for low-cost microcontrollers, facilitating the integration of encrypted RF triggers and anti-handling switches.
- **Generative CAD & Shaped Charges:** Generative design software calculates internal containment geometries and Munroe-effect liner configurations for 3D-printed devices to maximize directional penetration against infrastructure components.

D. Mass Casualty Terrorism & Active Shooter Planning

Adversaries utilize generative AI and multi-agent simulation frameworks to assist in operational planning and target evaluation during mass casualty incidents.

- **Weapon Selection & Evaluation:** Threat actors utilize offline LLMs to evaluate weapon performance criteria, magazine capacities, and concealment feasibility relative to target environments.
- **Real-Time Troubleshooting:** Localized AI models serve as reference guides for resolving mechanical stoppages or operational maintenance queries during tactical preparation.
- **Tactical Simulation:** Multi-agent workflows model crowd movement patterns, building layouts, and security response timelines across soft targets to identify optimal ingress and egress vectors.

E. Cyber Operations & Purdue-Model OT/ICS Disruption

The cyber domain involves machine-speed vulnerability discovery and direct manipulation of industrial control environments structured across the Purdue Enterprise Reference Architecture.

- **Automated Vulnerability Discovery (IT Levels 4/5):** Frontier models integrated with symbolic execution and fuzzing compress the discovery window for newly disclosed software flaws across enterprise IT and SCADA workstations.
- **Purdue Model Traversal (Levels 3 down to 0/1):** Specialized agents trained on vendor-specific PLC documentation (Siemens S7comm, Modbus TCP, DNP3) automate reconnaissance inside compromised IT/OT convergence boundaries, executing register manipulations to override safety instrumented systems (SIS).

3. COMPREHENSIVE THREAT SUMMARY MATRIX

Threat Vector	Primary AI Capability	Technical Barrier Lowered	Operational Impact on U.S. Interests
Chemical Weapons & TICs	Generative Molecule Analysis, Retrosynthesis	Identifies unscheduled precursors and alternative synthesis pathways.	Exploration of novel chemical threat structures and synthesis routes.
Radiological Dispersal (RDDs)	Autonomous OSINT, CFD Plume Modeling	Automates isotope source identification and dispersion physics modeling.	Planning high-consequence urban radiological contamination.
Asymmetric Weapons & IEDs	Chemical Predictors, CAD, Microcontroller LLMs	Automates firmware creation and energetic material formulation.	Fabrication of stabilized HMEs, shaped charges, and remote triggers.
Mass Casualty Terrorism	Agentic Simulators, Local LLMs	Aids in target reconnaissance, weapon evaluation, and routing simulation.	Optimized tactical planning for soft-target attacks.
Cyber-Physical (OT/ICS)	Automated Fuzzing, Protocol-Specific LLM Parsers	Compresses vulnerability discovery and protocol parsing timelines.	Purdue-model traversal resulting in physical infrastructure disruption.

4. INTELLIGENCE COLLECTION & OPSEC OPTIMIZATION

AI tools optimize adversary intelligence collection and operational security prior to execution. Autonomous multi-agent workflows scrape regulatory filings, GIS data, Shodan device indexes, and satellite imagery. Using Retrieval-Augmented Generation (RAG) across aggregated repositories, adversaries identify systemic single points of failure across interdependent infrastructure. Operating quantized open-weight models offline enables operatives to query technical documentation without leaving cloud API logs or dark-web tracking trails.

5. COMPREHENSIVE THREAT SUMMARY

The integration of artificial intelligence into the operational methodologies of state adversaries and violent extremist organizations presents distinct challenges across national security domains. By lowering technical barriers, accelerating research workflows, and enabling localized open-weight execution, AI empowers threat actors to streamline the planning of complex operations. Mitigating these risks requires comprehensive strategic alignment around hardware-anchored supply chain verification, Purdue-model OT anomaly detection, and proactive intelligence countermeasures.