Quiet Warfare: Bending Data and Perceptions in the Defense Industrial Base.

By
Greg Sharpe, Fellow

Published: May 14, 2026

Artificial intelligence is quietly redrawing the front lines of national security, and the United States' Defense Industrial Base (DIB) now sits in the crosshairs of a new style of conflict. What once looked like routine cyber incidents now appears as a persistent campaign that fuses digital intrusion, supply chain manipulation, and targeted information operations into a single pressure system aimed at the factories, laboratories, and logistics networks that keep American forces armed and ready.

When most Americans imagine national defense, they focus on the uniformed force and the platforms that dominate headlines. Behind that visible edge of power stands a sprawling, largely private ecosystem of designers, manufacturers, software firms, logistics providers, depots, and research institutions that convert national intent into fielded combat capability. Federal regulation describes this DIB as the combined government and private sector industrial complex that can research, develop, produce, and sustain weapon systems and their components at the scale required for military operations.

That chain is far more diverse than the marquee names on major defense contracts. It includes niche machine shops, regional logistics firms, university laboratories, software providers, and government facilities that share technical data and workflow information through a constant flow of digital exchanges. Design files, bills of material, maintenance records, and operational telemetry form the nervous system of this industrial organism. When the system is healthy, the nation can surge production and sustain readiness under stress. When it is strained, deterrence becomes much harder to demonstrate in a crisis.

This industrial nervous system is absorbing AI at high speed, often with limited guardrails. Across the DIB, machine learning supports predictive maintenance, defect detection, demand forecasting, scheduling, and supply chain visibility. Corporate leadership often has only a surface-level understanding of how thinking machines can erode corporate identity, trust, and reputation quietly, yet catastrophically.

For the strategist, this adaptation expands the terrain adversaries can probe. Industry surveys in the World Economic Forum's Global Cybersecurity Outlook 2026 report show that executives see AI as the primary driver of change in cybersecurity and regard AI-related vulnerabilities as the fastest-growing category of cyber risk. Organizations recognize that their attack surface is expanding as AI tools move into sensitive workflows, yet governance practices and security controls often lag deployment.

Hybrid campaigns against the DIB rarely announce themselves through spectacular outages. Security officials describe a patient pattern that begins with access and aims for endurance rather than immediate disruption. Once inside a network or supplier ecosystem, adversary teams map production rhythms, supplier dependencies, identity systems, and critical decision points where even modest delays can ripple across schedules and inventories. AI has become a force multiplier

for this reconnaissance, mining engineering files, and communications at machine speed and surfacing patterns that would take human analysts far longer to identify.

The contest is unfolding below the threshold of open conflict. Strategic competitors apply pressure through cyber intrusion, intellectual property theft, data manipulation, counterfeit insertion, and narrative operations designed to erode confidence in the U.S. capacity to arm itself and its allies. Hybrid pressure often manifests as subtle slowdown, rising cost, and creeping doubt rather than overt sabotage.

The stakes for deterrence are significant. Modern deterrence depends not only on visible platforms and war plans but also on an adversary's belief that the United States can sustain forces and generate combat power at speed. If competitors conclude that AI-enabled systems in the DIB are brittle or easily manipulated, the credibility of deterrence weakens. The 2026 National Defense Strategy emphasizes strengthening the industrial base as a pillar of national power, tying cyber resilience directly to the ability to deter and wage war.

Pentagon planners increasingly describe cyber activity against the DIB as a persistent campaign environment. Adversaries can pursue national security effects through intrusions into private networks and business processes that support critical programs.

The technical attack surface is broad because the DIB operates as a tightly coupled system. Engineering teams collaborate across companies, moving design data through shared tools and platforms. Components flow through multiple tiers of suppliers before the final assembly. A single compromised vendor can offer adversaries access to multiple programs. Hybrid campaigns exploit these seams.

The effect of these operations extends beyond physical outcomes. Manipulated or stolen data can become material for influence narratives that frame U.S. production as unreliable or compromised. Production delays caused by cyber incidents can be amplified to sow doubt among allies about American capacity.

Adversary teams also benefit from repetition. They have treated the DIB as a learning environment, refining tradecraft through continuous operations. Hybrid coercion in this context is deliberate and calibrated, remaining below the threshold that would trigger a national response while still generating uncertainty and doubt.

Emerging evidence suggests that agentic AI systems are beginning to automate portions of this intrusion lifecycle. Automated chains reduce the cost of probing many suppliers and narrow the window for defenders to respond. For smaller firms with limited security resources, the pressure can quickly become unmanageable.

Security experts argue that defending against such campaigns will require disciplined governance and architecture. Pre-deployment AI security assessment and continuous validation must become standard practice, covering model selection, data provenance, access control, logging, and periodic reevaluation.

Architectural choices will also play a critical role. Zero trust principles and micro segmentation can reduce the impact of intrusions by limiting movement across networks. For DIB operators, this means treating segmentation and strong identity controls as the default architecture.

The industrial context around these cyber efforts is already volatile. The aerospace and defense sector is managing supply chain disruptions and resource constraints while trying to scale production. This environment amplifies the effectiveness of cyber sabotage and influence operations because attacks land in systems that are already stressed.

The strategic logic behind adversary focus on the DIB is clear. By degrading confidence and throughput, competitors can undercut deterrence without open conflict. When intrusions are contained and production continues under pressure, the calculus of hybrid aggression shifts.

Hybrid warfare against the DIB aims to bend trust in the systems that generate combat power. If those trust systems are distorted through advanced technologies and coordinated information operations, the result is slower decisions, higher costs, delayed output, and a quieter form of coercion.

Mr. Greg Sharpe is a Fellow and the director of Communications and Marketing for the National Institute for Deterrence Studies and the Managing Design Editor for the Global Security Review. Greg has over 35 years of military, federal civilian, and defense contractor experience in the fields of database development, digital marketing & analytics, technology use case exploration and assessment, and as a USAF doctrine outreach and engagement analyst. The views of the author are his own.