IF Insight Forward

AI in the Iran Conflict

Corporate Exposure and the new Defense Industrial Base

Artificial intelligence is increasingly embedded across the operational architecture of modern warfare. The conflict highlights how commercial technology platforms are becoming integral components of the defense industrial base.

Operational Lessons From AI-Enabled Warfare

This report examines how the conflict illustrates structural changes in the relationship between commercial technology and military capability. The U.S. campaign against Iran illustrates how AI-enabled capabilities are becoming embedded across the strike enterprise rather than appearing as discrete weapons. Software and machine intelligence are used to accelerate multiple stages of operations, including the processing of intelligence, target generation, strike planning, and the coordination of low-cost attritable drones operating over resilient commercial connectivity. These systems shorten the interval between sensing, decision-making, and execution.

The operational architecture visible in this conflict also reflects a broader change in the composition of defense capability. Frontier AI models, cloud and compute infrastructure, satellite communications, and autonomy software increasingly function as operational enablers rather than supporting technologies. As a result, the defense industrial base is evolving toward a hybrid structure in which traditional defense primes remain central but operational effectiveness depends heavily on commercial technology firms whose platforms and infrastructure are integrated directly into military operations.

Figure 1: Low-Cost Uncrewed Combat Attack System (LUCAS)

The conflict also highlights how the United States is combining "affordable mass" with AI-enabled decision infrastructure. The reported combat debut of the Low-Cost Uncrewed Combat Attack System (LUCAS), a low-cost one-way attack drone designed to mirror the cost-imposition strategy of Iran's Shahed systems, reflects a shift toward attritable strike at scale.

The more significant development lies in the acquisition and production model behind the system. LUCAS reflects an approach built around rapid fielding, modular design, and open architecture that allows payloads and communications packages to be integrated quickly. Systems that can be deployed in months rather than years and produced at far lower cost alter the economics of sustained operations.

As platform costs fall and system numbers increase, the value of coordination software, communications networks, and AI-assisted planning rises sharply. These systems allow large numbers of inexpensive platforms to operate as a coordinated strike capability.

A central effect of AI in this conflict is the compression of decision cycles. AI-enabled systems appear to have been used to accelerate several stages of the kill chain, including the processing of large volumes of intelligence, generation of target candidates, prioritization of options, and recommendation of strike packages and weapon–target pairings.

This compression shifts the operational constraint in strike planning. The limiting factor becomes less the availability of target data and more the speed at which command structures can evaluate, approve, and execute complex strike sequences.

AI does not need to operate as a fully autonomous weapon system to produce this effect. Systems that rapidly generate and prioritize strike options narrow the time available for human review. The result is higher operational tempo, the ability to manage larger numbers of potential targets, and increased political sensitivity around accountability, legal review, and oversight.

Autonomous systems in this conflict appear to be scaling through orchestration rather than through fully independent platforms. Reporting describes the use of orchestrator software designed to coordinate multiple autonomous systems by managing tasking, routing, communications, and deconfliction. This approach allows a small number of operators to supervise many platforms simultaneously.

This model provides the operational basis for swarm-adjacent and distributed strike operations. Effectiveness depends less on the autonomy of individual systems and more on the software that coordinates them.

The orchestration layer therefore becomes a critical control point. It sits between the human operator and the autonomous fleet and defines how systems are tasked, how constraints are applied, and how human oversight is maintained. Operational doctrine and rules governing autonomy are partly implemented through this software layer. As a result, governance and regulatory scrutiny are likely to focus heavily on the orchestration systems that manage autonomous operations.

Communications infrastructure forms another critical component of this operational model. Networked warfare depends on resilient connectivity, and the conflict highlights the extent to which commercial satellite systems can become operational dependencies.

LUCAS development was reportedly paired with satellite communications options that may include Viasat capabilities and SpaceX's Starlink or Starshield, although specific connectivity arrangements in the conflict have not been publicly confirmed. These systems illustrate how commercial connectivity providers, terminal manufacturers, encryption and key-management suppliers, and cloud-edge integration firms are becoming integrated into the delivery of military capability.

AI and the Changing Defense Industrial Base

As commercial connectivity becomes embedded in operational systems, it functions both as a strategic asset and as a potential vulnerability. Satellite networks and associated infrastructure may attract increased attention from procurement authorities, regulators, and adversaries. Disruption, infiltration, or reputational pressure targeting these networks could become a pathway for degrading U.S. operational effectiveness.

These operational patterns suggest that AI is becoming a functional component of the defense industrial base rather than a supplementary capability. Historically, the defense industrial base was defined primarily by manufacturing capacity for platforms and munitions. It now increasingly includes software development, data integration, model training and inference infrastructure, and secure deployment environments.

Within this structure, the most strategically important suppliers may be those that can integrate intelligence sources, accelerate operational planning, run models securely in classified environments, and maintain reliable connectivity across distributed systems operating under contested conditions.

The conflict indicates that operational effectiveness can depend as much on compute infrastructure, data workflows, and mission software as on the physical performance of the platform or munition itself.

This shift also has political implications for the companies involved. Employee activism and external pressure campaigns have increasingly targeted corporate participation in military AI development, often demanding greater transparency or opposing specific applications such as large-scale surveillance or fully autonomous weapons.

These pressures can affect several aspects of corporate operations, including contract pursuit and execution, recruitment and retention, and leadership credibility. Firms whose technologies become integral to national security programs may therefore face persistent governance challenges.

Companies increasingly need to define internal boundaries for acceptable use while remaining able to meet government requirements that may evolve quickly during periods of conflict. Tensions are most likely where advanced AI capabilities intersect with classified deployments, targeting processes, and systems that support high-consequence operational decisions.

Vendor selection in AI-related defense programs is increasingly influenced by political considerations. As governments treat AI capability and deployment access as elements of national power, procurement decisions can signal trust, alignment, and perceived reliability. These signals may shape which companies gain access to sensitive operational environments and which are excluded.

Supply chain risk is particularly important because it illustrates how quickly a commercial supplier can be viewed as either a strategic asset or a strategic liability. Disputes that originate in corporate governance or acceptable-use policies can be interpreted as indicators of reliability in national security contexts.

For corporate leadership, the risk lies in the possibility that governance positions are interpreted as reluctance to support government programs. This can lead to exclusion from procurement opportunities, reputational pressure within policy circles, or unfavorable regulatory treatment.

The economics and structure of defense procurement are also evolving in ways that affect corporate strategy. The reported use of open architecture and government-owned design intellectual property in systems such as LUCAS, combined with an emphasis on multiple manufacturers, suggests a procurement model that relies less on single prime contractors and more on distributed production across several suppliers.

For industry, this approach can lead to faster recompetes, margin pressure in commoditized hardware production, and greater competition around integration capabilities. Differentiation may increasingly depend on payload modularity, communications integration, quality assurance at scale, and the ability to sustain reliable supply.

This model also alters bargaining dynamics. When the government owns the system design and can source production from multiple vendors, supplier leverage declines unless firms control key integration layers, manufacturing capacity, or specialized subsystems.

The approach may indicate how the United States intends to expand defense production rapidly by standardizing designs, reducing vendor lock-in, and distributing manufacturing across a broader supplier base.

Corporate Exposure and Governance Risk

As commercial technology platforms become more integrated into military operations, the exposure of these firms to security and political risks increases. Companies operating in frontier AI, cloud infrastructure, autonomy software, satellite communications, and related supply chains may become targets for cyber intrusion, intellectual property theft, and operational disruption.

These firms may also face influence campaigns intended to weaken public legitimacy, divide internal workforces, or increase political pressure against their participation in defense programs.

Legal, regulatory, and investor pressures can reinforce these dynamics, particularly if public narratives frame corporate participation in defense technology around themes such as excessive automation, surveillance concerns, or profiteering during conflict.

As corporate technologies become embedded in national security capabilities, the risk environment surrounding these firms increasingly overlaps with national security risk itself. Companies operating in these sectors therefore need to treat geopolitical pressure, cyber activity, and political scrutiny as part of their normal operating environment.

The implications for corporate governance are significant. Companies whose technologies intersect with defense AI programs will likely need organizational structures capable of managing both technical and political exposure. In practice, this places defense AI posture within enterprise governance, including clear decision authority, escalation mechanisms, and policy frameworks designed to withstand political controversy.

Firms participating in national security markets may also require operating models that can accommodate compressed procurement timelines and evolving government requirements while maintaining strict compliance and documentation standards. Internal policies defining acceptable use, disclosure practices, and technology governance can help reduce internal conflict while supporting participation in sensitive programs.

Operational readiness in these markets increasingly depends on trusted supply capabilities, including security engineering, software provenance, model governance, secure deployment pipelines, and auditable controls compatible with classified environments. At the same time, political volatility surrounding military AI is likely to persist, requiring companies to incorporate activism risk, reputational exposure, and procurement-related political pressures into enterprise risk management and scenario planning.

The U.S.–Iran conflict illustrates a broader shift from AI as a specialized capability to AI as infrastructure of power. Technologies such as frontier models, cloud infrastructure, autonomous systems, and satellite connectivity are becoming embedded in the operational architecture of military capability.

As this transition continues, companies operating in these sectors will play a more direct role in national security outcomes. Their competitive position will increasingly depend on their ability to deliver operationally relevant technologies while maintaining governance structures capable of operating under geopolitical pressure and domestic political scrutiny.

Say Hello. Anytime.

@insightforward.co.uk

GEOPOLITICAL INTELLIGENCE

ANALYSIS | CONSULTING | TRAINING