

The New Logic of Deterrence

Integrating AI, Autonomy, and Industrial Capacity

By David F. Helvey

For decades, deterrence rested on a simple proposition: *convince a potential adversary that the costs of aggression would outweigh any conceivable gains.*

Military capability served as the principal currency of credibility, and was measured in platforms, inventories, readiness, force posture, and the demonstrated ability to impose costs on the aggressor, or deny the aggressor any benefits of its aggression. That logic has not disappeared. But its foundations are shifting in ways that demand a fundamental reexamination of how we think about deterrence in strategic competitions.

Artificial intelligence, autonomous systems, and industrial capacity are converging to reshape how military power is generated, sustained, and applied. Together, they are creating a new form of competitive advantage based on translating commercial innovation into military and operational capabilities faster than an adversary. For policymakers, it is less about who fields the most advanced platform than it is about who can build the military and industrial systems that can deliver strategic, operational, and tactical effects at speed and scale.

Precision Meets Mass

The United States' asymmetric advantage in precision warfare was built, not inherited. Cold War [investment in precision-guided munitions and networked systems was designed to offset Soviet numerical superiority](#), obviating a need for reciprocal investments in conventional force elements, or relying on the threat of nuclear escalation. Those investments paid decisive dividends in conventional campaigns that followed in the immediate post-Cold War period. Desert Storm, the Balkans, Iraq, and Afghanistan validated the proposition that technological superiority could substitute for numerical mass, even as the same tools proved less decisive in the counterinsurgency and stability operations that followed. That assumption remains broadly valid, but the margin of conventional dominance is no longer assured.

China, for example, has spent decades modernizing the People's Liberation Army (PLA) while building an industrial and technological base of unprecedented scale. [The U.S. Department of Defense's 2025 Annual Report to Congress](#)

[on Military and Security Developments Involving the People's Republic of China](#) details Beijing's continuing pursuit of modernization through indigenous innovation, industrial policy, and military-civil fusion that integrates commercial and defense sectors in ways that are difficult to replicate elsewhere. Russia, meanwhile, has invested in AI-enabled drone vision systems that have evolved rapidly under combat conditions in Ukraine, and in AI-assisted disinformation capabilities that contest the cognitive domain as aggressively as the physical one. The challenge, in this context, is not simply that adversaries are catching up with the United States. They are competing, and generating competitive advantage, on different terms.

What differentiates this era from the Cold War is not the fact of industrial competition — both the United States and the Soviet Union understood that manufacturing capacity was a strategic asset — but its character. Cold War rivals built largely parallel, siloed industrial bases, separated by ideology, geography, and tightly controlled technology transfer. Today's competition runs through shared commercial infrastructure. The semiconductors, cloud platforms, and AI models

About the Institute for Security and Technology

The Institute for Security and Technology (IST) is the 501(c)(3) critical action think tank that unites technology and policy leaders to create solutions to emerging security challenges.

IST stands at the forefront of convening policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance

national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

powering global commerce are the same ones that underpin the most advanced military systems. That entanglement means no competitor can fully wall off its industrial base, and no alliance can assume that technological advantage, once established, will hold.

What Russia's war in Ukraine has made concrete is a related point: precision has not surrendered to mass, nor mass to precision. They have merged. Low-cost, attritable systems now deliver precision effects at scale, vindicating neither the precision-dominant nor the mass-dominant model but a synthesis of both. Strategic competition is now a contest between rival innovation ecosystems in which the ability to design, manufacture, field, and regenerate capability matters as much as the capability itself.

AI as a Force Multiplier

Artificial intelligence sits at the center of this transformation, and its most consequential national security implications may have little to do with large language models or commercial applications.

Modern military operations generate enormous volumes of data from satellites, sensors, unmanned systems, intelligence platforms, logistics networks, and open sources. Human operators cannot efficiently process, prioritize, and act on this information in real time. AI bridges data and decision, compressing timelines and enabling organizations to operate at a pace that would otherwise be impossible. That compression offers significant decision advantage, of course, but is not without risk: in crisis, shortened decision windows also reduce the opportunity for de-escalation, and at the nuclear threshold — where the consequences of miscalculation are irreversible — the speed advantage that AI confers may operate directly against strategic stability.

This recognition is gaining traction across Allied defense establishments. NATO's 2024 revised AI Strategy, for example, reflects both sides of the equation by integrating AI into military capabilities while emphasizing interoperability, resilience, and responsible use. The investment priority is consistent: AI-enabled command and control, intelligence analysis, and logistics optimization, all oriented toward reducing the time between observation and action.

But AI's military significance extends beyond the battlefield. AI is also an industrial capability. Manufacturers use it to optimize production processes, identify bottlenecks, predict maintenance requirements, and accelerate engineering cycles. Defense firms deploy it to shorten development timelines and streamline supply chains. AI simultaneously amplifies military effectiveness and industrial performance. This dual-use character explains its central position in contemporary strategic competition. A military that decides faster than its adversary enjoys an operational advantage; a nation that innovates, produces, and adapts faster enjoys a

strategic one.

Autonomy as a Scaling Mechanism

If AI provides speed, autonomy provides scale.

Autonomous systems have moved rapidly from niche applications to central components of military planning across air, land, maritime, cyber, and space domains. Their appeal is straightforward: most advanced militaries face persistent constraints on manpower, budgets, and force structure. Autonomous systems expand operational reach, increase persistence, distribute risk, and generate mass without proportional increases in personnel.

The [Department of Defense's Replicator Initiative](#), announced in August 2023, reflects this logic directly. Replicator seeks to field thousands of attritable autonomous systems capable of complicating adversary planning and imposing operational dilemmas at scale. In unveiling the initiative, then-Deputy Secretary of Defense Kathleen Hicks was explicit: it was designed to counter an adversary possessing "more ships, more missiles, and more people."

The war in Ukraine has provided a vivid and ongoing illustration of what this can look like by demonstrating the operational utility of low-cost autonomous and semi-autonomous systems, rapid software adaptation, distributed innovation, and commercially derived technologies. Ukrainian forces and supporting industries have repeatedly modified drones, integrated commercial capabilities, and adjusted operational concepts at a pace that would have been difficult to imagine in earlier eras. Zero Line Defense, which deploys acoustic and visual sensor networks along the front line to provide awareness without personnel exposure, extended that model beyond strike platforms to sensing and surveillance. The pattern is consistent: deploy, observe, modify, redeploy. Software updates generate operational effects far faster than traditional acquisition timelines.

This matters acutely in the western Pacific, where any contingency involving Taiwan would unfold across vast distances, placing extraordinary demands on logistics, sustainment, and force distribution — conditions under which the ability to field large numbers may prove as strategically significant as the performance of any single platform.

Industrial Capacity as Strategic Endurance

Neither AI nor autonomy can deliver meaningful strategic advantage without industrial capacity, which remains the most underappreciated dimension of contemporary debates on defense innovation and deterrence.

Military organizations focus naturally on platforms, software, and operational concepts. But those elements rest on a broader foundation: manufacturing facilities, supply chains, skilled labor, energy infrastructure, semiconductors, cloud services, and maintenance ecosystems. Defense-industrial

scaling also faces a structural capital problem: demand is lumpy and politically contingent, investment timelines routinely exceed a decade, and neither traditional venture capital nor annual appropriations reliably fund the build-ahead-of-demand that genuine regeneration requires. Industrial capacity is what determines whether innovation can be translated into sustained capability, and whether a force can absorb losses and keep fighting.

Ukraine offers two distinct industrial lessons. The first concerns adaptation: from the earliest days of the conflict, Ukrainian forces demonstrated that institutional flexibility and political will — not industrial scale — can generate extraordinary capacity. Commercial drones were weaponized within weeks; tactics were adjusted faster than any procurement system could respond. The second concerns endurance. Russia's inability to sustain precision munitions production and replace losses at pace has narrowed its operational options in ways that industrial planning decisions made years earlier determined. Western defense-industrial systems revealed parallel constraints: cold production lines, absent multiyear procurement commitments, and a post-Cold War drawdown in surge capacity that left allies unable to replenish stocks at the rate the conflict demanded. Political will shapes what a nation chooses to field; industrial capacity determines how long it can sustain that choice.

For their part, NATO allies have responded by increasing defense spending and expanding munitions production. The European Commission's first-ever European Defence Industrial Strategy, unveiled in March 2024, makes resilience, production readiness, and collaborative capability development core strategic. Across the Indo-Pacific, the recognition is similar: deterrence depends not only on forces in being but on the capacity to regenerate them. Semiconductor manufacturing, critical minerals, supply-chain security, and investment screening are national security policies as much as economic ones.

The Splintering of Deterrence Ecosystems

Far from producing a more coherent deterrence order, the convergence of AI, autonomy, and industrial capacity is fragmenting it. In a multipolar world, the critical inputs to military power — semiconductors, rare earth minerals, AI talent, advanced manufacturing capacity, cloud infrastructure — are distributed across dozens of countries, many of which maintain relationships with each side of a given competition. Middle powers are hedging. Supply chains cross ideological lines. The technology ecosystem underpinning modern military capability cannot be divided neatly into allied or adversarial.

That fragmentation is the central strategic challenge and it is why integration among like-minded partners can no

longer be held as aspirational. It is a security imperative. The United States and its allies and partners retain significant advantages: world-class universities, deep capital markets, innovative defense firms, sophisticated military organizations, and extensive alliance networks. But those advantages are dispersed, and dispersed advantages can be exploited, disrupted, or outpaced by adversaries operating with greater institutional coherence.

Sustaining deterrence requires knitting these assets into cohesive, resilient networks — deliberately, and faster than the splintering dynamic erodes them. Trusted production networks, interoperable digital infrastructure, common standards, and collaborative innovation mechanisms may become as strategically important as traditional military interoperability. Organizations such as NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund — the world's first multi-sovereign venture capital fund, backed by 24 Allies with one billion euros committed — are early attempts to build that architecture. Their significance lies less in what they have produced than in what they represent: a recognition that technological advantage must be actively constructed and defended.

Workforce development is equally non-negotiable. AI-enabled defense ecosystems require software engineers, data scientists, advanced manufacturers, and cyber specialists whose recruitment runs across domains like immigration policy, education funding, and industrial strategy that defense planners rarely control but can no longer ignore.

Lastly, the governance dimension is unavoidable. AI-enabled systems introduce failure modes with no analog in conventional military technology: data poisoning, spoofing, and automation bias can produce catastrophic outputs from inputs that appear routine. Speed and scale are advantages in competition but, as discussed above, and especially in a nuclear context, they are liabilities in crisis. Democratic alliances must build governance frameworks as adaptive as the technologies they govern and move faster than adversaries can exploit the gaps between them.

Conclusion

The logic of deterrence has always depended on capability and credibility. What is shifting is the source of each. For most of the post-Cold War period, deterrence was a function of what a nation possessed: forces in being, precision platforms, forward presence, nuclear arsenals. It is now becoming a function of what a nation can generate, sustain, and reconstitute under pressure — and how quickly it can do so relative to an adversary.

A force that cannot be regenerated at pace provides a

deterrent that erodes under sustained competition. Alliance networks that cannot coordinate production, innovation, and industrial capacity will not hold when it counts. Possessing superior capabilities at the outset of a competition is necessary. It is not sufficient.

What the convergence of AI, autonomy, and industrial capacity demands, therefore, is not simply investment in new

platforms or programs. It demands a governing architecture — spanning governments, industry, and allied nations — capable of integrating dispersed advantages into coherent, sustained strategic effect. Whether democratic alliances can build that architecture faster than competitive pressures erode it is, in the end, the question on which their deterrence posture will stand or fall.

About the Author

David F. Helvey is Distinguished Fellow for Defense Strategy and Indo-Pacific Security at the Institute for Security and Technology (IST). He previously served as a senior official in the U.S. Department of Defense, with responsibilities for Indo-Pacific and Euro-Atlantic security, alliance management, and defense policy. The views expressed here are his own and do not represent the views of the U.S. Department of Defense.

The Institute for Security and Technology and the authors of this report invite free use of the information within for educational purposes, requiring only that the reproduced material clearly cite the full source. This report is written and published in accordance with the Institute for Security and Technology's [Intellectual Independence Policy](#). The authors are solely responsible for its analysis and recommendations. The Institute for Security and Technology and its supporters do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.