National security law in 2026: Legal adaptation in a constrained security economy

By Scott Nuzum, Esq., Wiley

DECEMBER 19, 2025

As 2025 draws to a close, national security discussions on the surface continue to center on geopolitical rivalry, technological competition, and the pace of innovation. These themes remain important, but as we enter 2026, a subtler, though increasingly consequential, reality is taking shape.

Legal and regulatory frameworks that once operated largely in the background of national security strategy and technical deployment are now evolving more directly in response to how national security objectives are actually being pursued.

Over the past decade, the United States has confronted a series of challenges and constraints that cannot be resolved through policy aspirations alone. These include operational limitations, environmental and permitting barriers, supply chain fragility, and the legal complexity of a deeply interconnected, but increasingly strained, global economy.

As we enter 2026, the defense-tech market appears to be internalizing a broader lesson that resonates across the national-security economy: Resilience depends as much on realism and integration as on technical ambition.

The response now emerging is not a sharp break from prior approaches, but a turn toward pragmatism, one that relies on law in new ways to protect interests, manage vulnerability, allocate risk, and operate deliberately within those constraints.

What follows are four areas where these dynamics are likely to become more visible and pronounced in 2026.

Defense-tech investment: operational credibility, supply-chain realism, and accelerating M&A

The defense technology sector has proven a robust area for private-sector investment, with significant capital inflows across U.S., European, and Australian markets. While investment in this sector is likely to remain strong in 2026, the criteria for what constitutes an attractive company are shifting.

The market, particularly in the United States, is crowded with ventures built around ambitious concepts, often highly engineered, software-heavy, or optimized for idealized conditions rather than operational reality. Many of these systems have performed well in simulation or controlled testing over the past several years, yet have struggled when exposed to battlefield conditions, supply-chain disruption, or the realities of scaled manufacturing.

In response, investor and acquirer attention is increasingly focused on technologies shaped by use rather than theory. Foreign systems tested under real operational conditions, particularly those emerging from allied environments with active conflict experience, are receiving heightened scrutiny and interest.

At the same time, domestic technologies that have resisted over-engineering and instead prioritized manufacturability, maintainability, and resilience under constrained conditions are being reassessed more favorably. These characteristics are increasingly viewed as indicators of durability rather than compromise.

This shift is already influencing acquisition strategy. Established defense contractors and mid-tier integrators are showing greater willingness to pursue mergers and acquisitions involving proven subsystems or platforms, rather than underwriting lengthy internal development cycles for untested concepts.

From a legal perspective, these targets often present lower uncertainty. Export-control issues have been confronted, cybersecurity and supply-chain risks are better understood, and operational limitations are known rather than hypothetical.

The growing openness to allied technology does not reflect diminished confidence in domestic innovation. Instead, it reflects a recognition, sharpened by experience, that isolation carries its own risks. Insular development strategies can obscure dependencies, inflate complexity, and delay deployment.

As we enter 2026, the defense-tech market appears to be internalizing a broader lesson that resonates across the national-security economy: Resilience depends as much on realism and integration as on technical ambition.

Critical minerals and rare earths: from independence to legally managed dependence

Critical minerals and rare earths will remain central to U.S. national-security planning in 2026, but there is growing acceptance that complete separation from China is neither legally nor economically achievable in the near term. China's dominance extends beyond extraction into processing, refining, and magnet production, segments of the supply chain that cannot be replicated quickly, even with sustained political commitment.

Domestic alternatives continue to face structural constraints. Environmental and land-use regimes impose timelines and litigation risks that make rapid scale-up of U.S. production difficult. These constraints are not new, but their strategic implications have become more apparent over the past several years and are unlikely to dissipate simply because security concerns have intensified.

At the same time, there remains increased interest in innovative approaches to rare earth and critical mineral production designed to reduce environmental impact and permitting delays. These include alternative extraction techniques, recycling and recovery from waste streams, and modular or co-located processing models that fit within existing industrial footprints.

While these approaches show promise and may play an important role over time, their ability to scale meaningfully and meet national security demands remains limited in the near term.

As a result, policy and legal frameworks entering 2026 are shifting away from the language of independence and toward managing unavoidable dependence. Procurement rules increasingly emphasize traceability and risk mitigation. Export controls and sanctions are calibrated to specific technologies or end uses rather than entire categories of materials.

Diversification strategies aim to reduce exposure to disruption rather than eliminate foreign inputs altogether. Allied sourcing plays a growing role, often alongside an implicit recognition that Chinese participation will persist at certain stages of processing for the foreseeable future.

The central legal question for 2026 will not be whether the United States can eliminate dependence on China, but how it can structure that dependence to limit strategic risk. In the year ahead, continued refinement is likely around where Chinese inputs are acceptable, where they are not, and how exposure is monitored over time.

Procurement rules, export controls, sanctions authorities, and disclosure obligations will do much of the heavy lifting, shifting the emphasis from origin purity to visibility, control, and contingency planning.

Digital infrastructure: computers, cloud, and connectivity move into the national-security frame

As artificial intelligence has become increasingly integrated into daily life, there is growing recognition that digital infrastructure should be treated as a national security concern rather than a purely commercial endeavor.

Hyperscale data centers, cloud platforms, advanced computer clusters, and subsea cable networks underpin artificial intelligence development, intelligence analysis, military communications, and broader economic competitiveness. Over the past two years, the legal posture toward these assets has begun to shift in measurable ways.

Legal frameworks are increasingly being used to manage constraint, preserve optionality, and allocate risk in an environment marked by supply-chain fragility, geopolitical friction, and volatile policy signaling.

Regulatory signals are increasing in both number and frequency. Team Telecom, the federal interagency group that reviews foreign involvement in U.S. telecommunications infrastructure, has expanded scrutiny of cable landings and foreign participation in cloud and connectivity infrastructure. The Commerce Department has explored mechanisms to improve visibility into advanced computer resources accessible to foreign actors, particularly where those resources support AI training or sensitive workloads.

The Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) have engaged more directly on issues of cable resiliency, spectrum coordination, and the role of data centers within critical-infrastructure and energy planning. Congressional attention to computer concentration and cloud dependency has also intensified.

What changes in 2026 is not the emergence of these concerns, but their consolidation. Rather than isolated reviews or ad hoc conditions, companies should expect clearer reporting expectations, more consistent interagency coordination, and a growing reliance on national security risk frameworks to assess ownership, access, and control of digital infrastructure.

The emphasis is less on outright prohibition and more on visibility, monitoring, and enforceable mitigation.

For companies operating in this space, legal risk will increasingly be tied to architecture and governance decisions that were previously treated as technical or commercial. Questions of who can access computers where data is processed, how infrastructure is financed, and what foreign participation is permitted are becoming standard elements of national-security review and will continue as 2026 unfolds.

Extraterritorial controls and the practical friction of cross-border technology

The extraterritorial reach of national-security law is not new. For decades, export controls and sanctions authorities have asserted jurisdiction beyond U.S. borders.

What has changed with particular intensity over the past decade is the scope, coordination, and practical implications of these tools. As 2026 begins, what once felt episodic or theoretical is now influencing investment, compliance, and technology deployment decisions around advanced semiconductors, artificial intelligence, and quantum technologies.

Controls on software, AI models, training data, and cloud-based computer access raise difficult questions of scope and enforceability, but enforcement posture has steadily hardened. Sanctions and entity-list tools increasingly target technology stacks rather than discrete hardware components, further blurring the line between domestic regulation and global market participation.

In parallel, U.S. companies face expanding extraterritorial obligations abroad, particularly in the European Union, where digital market, cybersecurity, and operational resilience regimes impose structural requirements on globally operating firms. The interaction between U.S. national-security controls and foreign regulatory systems is creating real friction that companies must actively manage. We can expect that friction to only increase in the coming year.

Conclusion: managing constraint through law

Taken together, the four areas above suggest that the defining feature of national security law in 2026 is not doctrinal transformation, but functional adaptation. Legal frameworks are increasingly being used to manage constraint, preserve optionality, and allocate risk in an environment marked by supply-chain fragility, geopolitical friction, and volatile policy signaling.

Rather than attempting to resolve these tensions through rhetoric or absolutist objectives, the law is quietly providing the wiring that allows critical systems to continue operating across abrupt policy shifts and competing strategic narratives. In that sense, national security law in 2026 is less about declaring strategic intent and more about building the operational flexibility required to execute despite it.

About the author

Scott Nuzum is a special counsel in **Wiley**'s corporate practice, where he advises U.S. and international companies on cross-border transactions, strategic financings, and corporate structuring in sectors shaped by national security and regulatory considerations. He is based in Washington, D.C., and can be reached at snuzum@wiley.law.

This article was first published on Reuters Legal News and Westlaw Today on December 19, 2025.