SPECIAL COMPETITIVE
STUDIES PROJECT

Defense Paper Series

Ensuring Cybersecurity and Technological Readiness in the National Defense Strategy

The Honorable James Langevin (former House Representative D-RI)

This paper series includes discussion papers written by SCSP advisors regarding the development of the 2025 National Defense Strategy. The views and opinions expressed in this paper are solely those of the authors and do not necessarily reflect the views or positions of SCSP.

Executive Summary

Sustaining U.S. military advantage demands that cybersecurity, allied tech cooperation, and rapid adoption of autonomous systems, coupled with a scalable and technology-focused workforce, remain explicit components of the National Defense Strategy (NDS). A decade of NDS-driven work has clarified three enduring imperatives: focus on great-power competition, become a data-centric enterprise, and translate innovation into fielded capability. To lock in progress, the NDS should preserve cyber as a strategic line of effort, protect and expand AI upskilling, incentivize allied co-development, and maintain "Replicator-like" delivery pressure with clear accountability and funding. Quantitative goals and transparent metrics should anchor each pillar to survive leadership and budget cycles.

Background and Context

Over the past decade, the National Defense Strategy (NDS) has shifted from a counterterrorism-focused framework to one centered on sustained great-power competition. It now prioritizes three core lines of effort: enhancing force lethality and readiness, strengthening alliances and partnerships, and advancing business reform. Implementation by the Department of Defense has emphasized concentrating on the challenge posed by China, modernizing the force, and developing realistic joint warfighting concepts for contested domains. Under Secretary of Defense for Policy Elbridge Colby is leading the development of the forthcoming NDS, having also played a central role in shaping the 2018 strategy under the first Trump Administration.

Preserving Cybersecurity as a Strategic Pillar

Rumors that the next National Defense Strategy (NDS) will downplay cyber runs counter to a decade of evidence demonstrating that cyber capabilities are a decisive, cross-cutting driver of joint force advantage. The congressionally mandated NDS Commission has warned of diminishing U.S. advantages in contested domains—an erosion likely to accelerate fastest in cyberspace if it loses priority. Secure data and resilient networks are foundational to readiness and lethality; without them, force targets lack credibility. To sustain cyber as a central, measurable priority, the NDS should underscore the importance of both defensive and offensive cyber capabilities. This approach would affirm the Secretary's commitment to protecting DoD infrastructure and weapons platforms, while preserving the ability to hold adversaries at risk in and through cyberspace.

Maintaining cyber as a strategic pillar will require clear, outcomes-based metrics and sustained investment. Readiness should be tracked through measures such as mean time to detect and contain intrusions, mean time to patch (MTTP) vulnerabilities, and the proportion of assets meeting zero-trust baselines. Mission assurance must be evaluated by linking cyber posture directly to the operational availability of critical systems, including command-and-control nodes and space-ground links.

Enduring advantage will also depend on multi-year cyber investment floors protected from in-year reprogramming, with particular emphasis on zero trust, software supply chain security, and hardening of operational technology and industrial control systems. Finally, cyber effects—both offensive and defensive—should be fully integrated into major exercises and joint warfighting concept validations, with after-action cyber key performance parameters reported to senior leadership to ensure accountability and drive improvement.

The Importance of AI Workforce Development and Upskilling

AI is only as effective as the people who build, govern, and employ it. DoD's formal shift to a data-centric organization explicitly hinges on recruiting and developing a world-class data workforce with authority to shape key investment decisions. Protecting AI and data talent pipelines from episodic budget pressure—including recent reductions to workforce initiatives—must be a non-negotiable NDS commitment.

To achieve this, the strategy should expand and safeguard AI and data pipelines by restoring and growing dedicated funding lines for the AI workforce, with year-over-year increases in scholarships, apprenticeships, and in-service upskilling opportunities. Billet-fill targets should be established for critical roles such as AI/ML specialists, data engineers, MLOps experts, and model risk management roles across the Services and the Fourth Estate.

Continuous learning must be institutionalized by mandating baseline AI and data literacy for all officers and key civilian personnel, while creating advanced training tracks for operators, intelligence analysts, logisticians, and program managers. Skill attainment should be tracked through credentialing and role-based proficiency assessments tied directly to promotion and assignment decisions.

Finally, the safe and effective adoption of AI should be accelerated by scaling model validation, test and evaluation, and red-teaming capacity, coupled with timelines for model accreditation and refresh cycles. All programs of record should be required to include AI adoption plans that explicitly address data governance and cybersecurity dependencies, ensuring responsible and resilient integration across the force.

Partnerships, Allies, and Shared Technological Progress

Historically, the National Defense Strategy (NDS) has placed strong emphasis on the role of partners and allies, but this commitment should not be taken for granted. Previous strategies identified the strengthening of alliances and the cultivation of new partnerships as central to sustaining a competitive edge against great-power rivals. Implementation reporting underscored coordinated efforts to align partner capacity-building with U.S. modernization and joint warfighting concepts. Today, however, there are growing concerns that the forthcoming NDS may not prioritize allies and partners to the same degree as in past iterations.

To maintain and expand allied advantage, the strategy should include concrete measures to deepen cooperation. This could involve establishing allied artificial intelligence and data exchange programs, reciprocal training opportunities, and shared certification frameworks. Co-funding centers of excellence for AI test and evaluation and cyber mission assurance would strengthen shared technological foundations, accelerate innovation, and ensure partners can operate seamlessly alongside U.S. forces.

Coalition readiness should also be advanced through interoperable architectures, requiring coalition-ready data standards, identity and access management systems, and cross-domain solutions as prerequisites for participation in major programs. Finally, the United States should expand joint prototyping with allies in areas such as autonomy, electronic warfare, and resilient positioning, navigation, and timing (PNT), linking these efforts to long-term co-production and sustainment agreements to ensure enduring capability and shared burden. These steps anchor alliances in tangible technological capacity, not only policy alignment.

Maintaining Momentum on Autonomous Systems

The Department of Defense's modernization line of effort has emphasized investment in game-changing technologies and realistic joint exercises to validate emerging concepts. "Replicator-like" initiatives seek to accelerate this vision by fielding attritable, autonomous, and non-attributable systems at scale—complicating adversary targeting and safeguarding high-value assets. The principal risk lies in reverting to a platform-by-platform status quo if momentum stalls due to leadership transitions or changes in program branding.

To prevent regression, the Department should set clear, quantifiable delivery targets by publishing annual goals for quantity, cost-per-effect, and deployment readiness of attritable air, maritime, and ground systems, linking these targets directly to Service Program Objective Memorandum submissions. Funding and accountability must be locked in through fenced, multi-year investments with milestone-based gates, coupled with the designation of senior leaders responsible for progress and required to provide public updates. Finally, adoption should be driven through exercises by making autonomous swarming, human-machine teaming, and resilient communications core elements of joint training events, with mandatory post-exercise transition plans that move validated capabilities into programs of record. These measures keep the modernization flywheel turning from experiment to fielding, consistent with NDS implementation goals.