Atlantic Council

July 2025

Issue brief A US strategy to win the next conflict

Clementine Starling-Daniels

Amid rising global tensions and rapid technological change, the forthcoming National Defense Strategy is set to reshape US military strategy. Its success hinges on five key priorities.

Bottom lines up front

- In its forthcoming National Defense Strategy (NDS), the second Donald Trump administration must reaffirm that defending the US homeland—particularly against nuclear, cyber, space-based, and other strategic threats—is the foremost obligation of the Department of Defense (DoD) and the foundation of credible deterrence abroad. It should clearly prioritize China as the primary competitor of the United States, recognizing, recognizing the need to counter Beijing's influence not only in the Indo-Pacific but globally.
- The US military must pursue transformational changes in force structure, operational concepts, and joint warfighting doctrine to be able to effectively conduct integrated, multi-domain combined arms operations in an era of artificial intelligence and human-machine teaming.
- Space must be treated as a warfighting domain in its own right, as well as a critical enabler of US homeland defense and power projection, requiring increased investments in offensive and defensive space capabilities.

Shaping US defense in a time of evolving global threats

Who is the biggest threat to the United States—and what should the military do about it? Where should the United States position its forces around the world? How should the US military adapt to the age of artificial intelligence (AI) and the weaponization of space? These are just some of the questions that must be addressed in the next National Defense Strategy (NDS), the foundational document through which any new administration articulates its vision for US defense policy. Published by the Department of Defense (DoD), it establishes the principles that guide US military force design, capability development, global posture, operational planning, and resource allocation.

The second Trump administration's forthcoming effort is no ordinary NDS. It will define the DoD's defense posture, US force structure, and modernization priorities for the next four years in a period of intensifying strategic competition, rapid technological disruption, and evolving global threats. In March 2025, Secretary of Defense Pete Hegseth issued a classified interim strategic guidance on national defense, signaling the administration's initial defense priorities. While the full details of this guidance remain classified, publicly available information

provides a strong basis to assess its direction and anticipate key themes in the full NDS.[1]

This issue brief outlines five critical priorities that the DoD should address in its forthcoming NDS, offering considerations for implementation and identifying areas in which the department must adapt to meet the demands of this decisive strategic era. These priorities relate to the interim strategic guidance and are shaped by enduring strategic realities.

1. Defend the homeland

First, the NDS must do more than simply affirm homeland defense as the DoD's top priority and correct the shortcomings of previous strategies. These include the failure to clearly prioritize between defense and power projection, as well as an overly narrow focus on nuclear missile and terrorist threats. While every administration's NDS has listed homeland defense as its first principle, these documents have typically lacked specificity on how the DoD plans to strengthen this mission relative to other priorities. The forthcoming NDS has a crucial opportunity to provide that clarity.

The US homeland is not a sanctuary

Threats to the US homeland have changed fundamentally over the last two decades. Following 9/11, these threats were primarily characterized as terrorist attacks on US soil. Today, however, the potential and active threats to the US homeland are coercive military and nonmilitary activities conducted by adversaries. Peer-state competitors, transnational criminal groups, and terrorist organizations can hold targets within the US homeland at risk through a variety of kinetic and non-kinetic attack vectors. China, Russia, and other states might seek to compromise the ability of the United States to fight and win wars, or to deter US engagement altogether—especially its capacity to defend allied countries.

Homeland defense: A shift from projecting forward to protection closer to home

Traditionally, under previous administrations, homeland defense has been predicated on a layered approach, requiring the United States to project forces forward globally to neutralize threats abroad before they reach the US homeland.[2] Under the second Trump administration, the concept of homeland defense seems to be shifting to focus more on managing direct, nearby, and internal threats to the homeland. The administration is right to more urgently focus on threats closer to home alongside those emanating from further abroad—domestic and near-shore vulnerabilities to the United States abound, and US adversaries are willing to take advantage of them. A robust NDS can put these issues front and center. To do so, it will need to prioritize the most significant vulnerabilities to the United States and define the appropriate roles for both DoD and the Department of Homeland Security, sometimes leading and sometimes supporting state governments, civilian agencies, and the private sector.

Appropriate roles: Homeland defense versus homeland security

As threats to the US homeland abound, it is useful to revisit the overlapping but differing roles of US federal agencies and departments. The DoD's role in homeland defense is to protect the nation's "sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President."[3] The Department of Homeland Security (DHS) leads a concerted national effort to prevent terrorist attacks within the United States, protect US borders, manage the flow of people and products into and out of the country, coordinate emergency response through the Federal Emergency Management Agency (FEMA), and reduce risks to US cyber and physical infrastructure through the Cybersecurity and Infrastructure Security Agency (CISA).[4] The DoD both supports and is supported by civilian and law-enforcement agencies such as DHS and the Department of Justice, among many others.

1. Lily Kuo and Pei-Lin Wu, "Taiwan Reassured by Trump's Focus on Fending off China," *Washington Post*, March 31, 2025, https://www.washingtonpost.com/world/2025/03/31/us-pentagon-taiwan-defense-strategy.
2. Melissa Dalton, "DoD's Shifting Homeland Defense Mission Could Undermine the Military's Lethality," Center for Strategic and International Studies, April 22, 2025, https://www.csis.org/analysis/dods-shifting-homeland-defense-mission-could-undermine-militarys-lethality#h2-a-shift-in-u-s-defense-strategy-.
3. "Frequently Asked Questions," Under Secretary of Defense for Policy, US Department of Defense, last visited June 9, 2025, https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Hemispheric-Affairs/Homeland-Defense-Integration-and-DSCA/faqs/#Section1.
4. "What Does DHS Do?" US Department of Homeland Security, last visited June 9, 2025, https://www.dhs.gov/employee-resources/what-does-dhs-do; "About CISA," US Cybersecurity and Infrastructure Security Agency, last visited June 9, 2025, https://www.cisa.gov/about.

The most urgent threats

At the same time, the range of complex external threats to the homeland demands a broader and more proactive DoD posture. The department must step up in both lead and supporting roles across several critical areas, particularly: defending the homeland against missile threats; enhancing cyber defense through the role of the United States Cyber Command (CYBERCOM); and protecting critical defense infrastructure from myriad threats including foreign interference and cyberattacks. These areas represent the real front lines of homeland defense and are where the DoD should bring its unique capabilities to bear, while enabling and reinforcing the work of other lead agencies.

The DoD's role in border security

The administration has emphasized the importance of securing the border. However, in doing so, it must remain mindful of the importance of civilian-military boundaries. The NDS should tackle this issue directly by considering the ways in which the DoD can provide appropriate defense support to civil authorities (DSCA) without eroding US public trust in the military. Additionally, large, sustained deployments to the southern border will be quite costly, divert from other priorities, and impact readiness. The DoD should consider designating a portion of the overall force structure—most likely from the National Guard—to focus on this effort. Aligning an appropriate part of the military against this mission would allow that part of the force to train for the unique demands of DSCA and ensure that the rest of the force can focus on lethality in the context of great-power competition.

Missile and air defense

In addition to its vital support role, the DoD must lead on several missions central to homeland defense. This includes missile and air defense—both to counter traditional missile threats and to adapt to the proliferation of hypersonic and cruise missile systems. Strengthening the North American Aerospace Defense Command (NORAD) and investing in next-generation sensors and interceptors will be critical.

Critical infrastructure

The department should also more deeply integrate with other agencies to improve the protection, resiliency, and redundancy of—and the security of research related to—defense critical infrastructure. The DoD's Defense Critical Infrastructure Program (DCIP), part of its homeland defense role, defines defense critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of [them] would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[5] Within DHS, CISA—as part of Presidential Policy Directive 21 (PPD-21)—advances national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure across sixteen sectors.[6] As part of the NDS's prioritization of homeland defense, the DoD should focus on vulnerabilities to its own and non-DoD networked assets essential to global force projection and sustainment. These assets include obvious items, such as military installations, logistics and supply chains, communications systems, satellite infrastructure, and ground stations. The DoD must also protect assets less often considered, such as financial systems supporting military operations, production and manufacturing sites critical to the US defense industrial base (DIB), and other sources of military power.

Cyber defense

On the cyber front, the "defend forward" mission of the CYBERCOM—introduced during the first Trump administration—has centered on confronting threats before they reach US networks.[7] CYBERCOM has focused on conducting offensive cyber operations to gather intelligence and prepare military cyber capabilities for potential crises or conflicts. However, with a shift in the DoD's overall focus for homeland defense—from projecting forward to protecting assets closer to and at home—this could mean CYBERCOM plays a larger role in protecting critical defense infrastructure at home from cyber and digital threats. While CISA leads in strengthening US infrastructure resilience to cyber threats, a case can be made for an enhanced role for CYBERCOM in protecting critical defense infrastructure falling under DoD's purview. Regardless of how CYBERCOM's mission is scoped, its budget should be increased to support its mission set of disrupting external actors before they can carry out attacks on domestic infrastruc-

5. "DoD Protected Critical Infrastructure Program," Under Secretary of Defense for Policy, US Department of Defense, last visited June 9, 2025, https://policy.defense.gov/OUSDP-Offices/ASD-HDGS/Defense-Critical-Infrastructure-Program/.
6. "Critical Infrastructure Sectors," US Cybersecurity and Infrastructure Security Agency, last visited June 9, 2025, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.
7. Dave Weinstein, "The Pentagon's New Cyber Strategy: Defend Forward," Lawfare, September 21, 2018, https://www.lawfaremedia.org/article/pentagons-new-cyber-strategy-defend-forward.

ture—through hunt forward, defend forward, and persistent engagement, while supporting CISA in defense of US critical infrastructure.[8]

Space infrastructure

As part of the DoD's homeland defense mission, the Pentagon should put a higher priority on hardening and protecting US space ground stations. The ground stations that control US satellites and receive telemetry are inadequately secured and vulnerable to interference or attack.[9] The US military is heavily reliant on satellites to command and control forces; obtain intelligence, surveillance, and reconnaissance (ISR); project US forces globally; and protect the homeland from kinetic attacks. To safeguard these vital systems, it is imperative that the US Space Force and US Space Command (SPACECOM) work—in close coordination with other federal agencies and commercial partners—to significantly bolster ground station security through targeted investment, threat-informed standards, and collaborative exercises to identify and mitigate vulnerabilities.

Sabotage and malign interference

Another way the DoD can improve homeland defense is by increasing its support—through intelligence or other means—to agencies that conduct counterintelligence operations against foreign adversaries operating within the United States, law-enforcement agencies that prevent sabotage of US infrastructure, and agencies focused on preventing malign foreign investment in US critical infrastructure or in adjacent land. DoD support to civilian departments and the private sector is paramount to help reduce vulnerabilities, especially to systems essential to defense mobilization and continuity of government. This includes more focused efforts to protect energy systems, ports, logistics hubs, and the defense industrial base.

Research security

Another important consideration for the DoD's role in homeland defense is the threat posed by inadequate research security at academic institutions or laboratories that conduct scientific, technological, and defense-related research and development in support of the DoD and other departments. While open research environments and international collaboration are fundamental to scientific and technological advancement and must be protected, securing federally funded research data and intellectual property from foreign access, interference, or sabotage is key.[10] Current research security standards are not always adequately set or consistently adhered to across every research institution, posing risks to US defense.[11] The DoD, in concert with the Department of Energy and other agencies, should work with its academic partners to set and reinforce adequate research standards. This includes implementing robust processes for vetting foreign research partners and donors to mitigate risks of inappropriate influence or espionage, ensuring transparency in research activities, ensuring that affiliations comply with federal regulations, and protecting US intellectual property.[12] These efforts must strike a careful balance—preserving an open and innovative academic environment while guarding against undue surveillance or constraints on scientific inquiry.

2. Prioritize China globally—not just regionally

The next NDS is likely to place a sharper focus on China as the primary competitor of the United States. This prioritization marks a shift from the approaches taken under both the first Trump administration and the Joe Biden administration. While both administrations emphasized great-power competition and treated China as the pacing threat, the persistence of crises in Europe and the Middle East diluted the intended prioritization of China, leading to attention being split across

8. "Cyber 101: Hunt Forward Operations," US Cyber Command Public Affairs, November 15, 2022, https://www.960cyber.afrc.af.mil/News/Article-Display/Article/3219164/cyber-101-hunt-forward-operations/; "Cyber 101—Defend Forward and Persistent Engagement," US Cyber Command, October 25, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.
9. Matthew Heideman, "Why We Need to Take Satellite Ground Station Security Seriously," *SpaceNews*, June 4, 2024, https://spacenews.com/why-we-need-to-take-satellite-ground-station-security-seriously/.
10. "Hearing to to [sic] Examine Research Security Risks Posed by Foreign Nationals from Countries of Risk Working at the Department of Energy's National Laboratories and Necessary Mitigation Steps," US Senate Committee on Energy and Natural Resources, February 10, 2025, https://www.energy.senate.gov/hearings/2025/2/hearing-to-to-examine-research-security-risks-posed-by-foreign-nationals-from-countries-of-risk-working-at-the-department-of-energy-s-national-laboratories-and-necessary-mitigation-steps.
11. Emily G. Blevins, "Federal Research Security Policies: Background and Issues for Congress," US Congress, May 20, 2025, https://www.congress.gov/crs-product/R48541.
12. "Global Consequences of Inadequate Research Security in Academia," Strider, December 4, 2024, https://www.striderintel.com/blog/global-consequences-of-inadequate-research-security-in-academia/.

regions. According to reporting on Hegseth's interim strategic guidance, the next NDS is expected to treat China not just as a priority but as the United States' priority competitor.[13]

The NDS is likely to push for a stark realignment that prioritizes China alongside homeland defense. Until and unless these two priorities are sufficiently resourced and addressed, other areas must be accepted as lower priorities. This represents a shift from balancing global threats to solving the most dangerous one—a mindset that will require strategic and resource discipline.

Prioritization is welcome in any strategy. It is easy to direct the DoD to balance threats. But without commensurate resources provided to adequately address the full range of threats the department is tasked with addressing, risk is being assumed but not articulated.

The NDS has the opportunity to bring to life a focused China strategy. This will require recalibration of US force structure and posture toward China and the Indo-Pacific, coupled with a global—not merely regional—approach to competition with China.

A global focus on competition with China

Too often, discussions about competing with China default to the Indo-Pacific theater alone. While that region remains the most likely locus of military confrontation, China competes with the United States globally; as such, the United States must approach competition with China through a global lens. From port infrastructure projects in Africa to rare earth mineral mining and dual-use space facility investments in Latin America and the Caribbean, China is steadily building a network of influence, access, and advantage that extends well beyond the Western Pacific. Limiting the DoD's focus to the Indo-Pacific would allow China to outflank the United States in regions where its presence is increasingly uncontested.

Therefore, a truly China-focused NDS must be global in orientation. This necessity means that all combatant commands—not just US Indo-Pacific Command (INDOPACOM)—must see China as part of their core mission. US Southern Command (SOUTHCOM) and US Africa Command (AFRICOM) play a crucial role in preventing China from gaining a foothold in the Western Hemisphere and in Africa, where institutions and critical infrastructure are increasingly subject to Beijing's influence. These regions might not warrant a large conventional military footprint, but they require a sustained presence, intelligence efforts, and partnership building—missions in which US Special Operations Forces (SOF), cyber forces, and interagency cooperation are particularly valuable.

Functional combatant commands, such as US Special Operations Command (SOCOM) and CYBERCOM, must be sufficiently integrated into this global campaign. These forces can compete below the threshold of armed conflict, disrupting Chinese gray-zone activities and helping shape the strategic environment in regions where the US conventional force presence is limited. From training partners and collecting intelligence to countering Chinese information operations, SOF units offer cost-effective tools that reinforce a global approach to competition with China.[14]

Force structure and posture alignment

A China-focused defense strategy must also reshape how the US military is structured and where it is based. In terms of force structure, the Pentagon should prioritize capabilities that enhance deterrence and warfighting capacity in the Indo-Pacific: long-range fires, survivable strike platforms, distributed logistics, and infrastructure protection. Investment should favor systems that can operate across vast distances and in highly contested domains, such as the B-21 bomber, *Virginia*-class submarines, unmanned systems, and space-based ISR.

Importantly, these investments are not theater exclusive. The mobility and flexibility of long-range assets allow them to be rapidly redeployed to other regions if needed, giving the US military the ability to respond globally.

Force posture must follow suit. The United States should double down on forward-deployed forces in the Indo-Pacific—especially in the First and Second Island Chains—by securing basing rights and expanding facilities in key areas such as the Philippines, Japan, Australia, and the Mariana Islands. These moves are essential not only for deterrence but for crisis response and rapid reinforcement in the event of conflict. However, posture changes must be calibrated globally. Redeploying

13. Zachary Cohen and Oren Liebermann, "Pentagon Tasked with Providing 'Military Options' to Ensure US Access to Panama Canal, Memo Says," CNN, March 14, 2025, https://edition.cnn.com/2025/03/13/politics/pentagon-panama-canal-options/index.html; Clementine Starling-Daniels and Theresa Luetkefend, "Questions Congress Should Ask about DOD 'Peace through Strength' Plan," *Defense News*, April 16, 2025, https://www.defensenews.com/opinion/2025/04/16/questions-congress-should-ask-about-dod-peace-through-strength-plan/.

14. Clementine G. Starling-Daniels and Theresa Luetkefend, "The Next Decade of Strategic Competition: How the Pentagon Can Use Special Operations Forces to Better Compete," *Atlantic Council*, January 14, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-next-decade-of-strategic-competition-how-the-pentagon-can-use-special-operations-forces-to-better-compete/.

assets from Europe or the Middle East must be accompanied by credible plans to mitigate risk—whether through burden sharing or shifting with allies, rotational forces, or regional partner capacity building.

Managing global risk

To succeed, prioritizing competition with China must be accompanied by a realistic assessment of where the United States can accept greater risk. This includes identifying specific capabilities, missions, and regions that can be deprioritized without sacrificing US interests. For example, heavy armored formations and short-range tactical fighter fleets—optimized for past conflicts—should be re-evaluated if they do not meaningfully contribute to Indo-Pacific warfighting or global power projection.

Similarly, the DoD must clearly communicate what it will and will not do in lower-priority theaters. This will allow allies to plan accordingly and take on greater responsibility. Rather than divesting entirely from regions like Europe and the Middle East, the United States should shift its focus from providing combat mass to supplying niche capabilities that enable allies and partners to lead. For example, European allies must assume a greater share of regional deterrence, while Gulf partners should continue investing in their own capabilities to counter regional threats. For the United States, strategic reprioritization in these theaters should mean maintaining influence and security without shouldering the full operational burden.

Finally, a China-focused defense strategy must account for Beijing's growing alignment with other US adversaries—namely Russia, Iran, and North Korea—whose coordination increasingly reinforces China's strategic position. The DoD should integrate this reality into its prioritization framework by assessing how competition with these actors intersects with China-focused objectives and ensuring coordination with allies, partners, and interagency efforts accordingly.

3. Adapt combined arms for the age of artificial intelligence and autonomous systems

The forthcoming NDS must embrace a revitalized approach to combined arms warfare—one that leverages the advantages of AI and autonomous systems without assuming they are universally applicable or sufficient in all operational contexts. To execute joint all-domain operations (JADO) effectively, the DoD requires an integrated, joint force capable of delivering fires and maneuver in contested environments. This demands a purposefully designed mix of high-end and low-end capabilities—including AI and autonomous technologies—ensuring the force remains adaptable across a range of theaters and scenarios where human decision-making, legacy systems, or simpler platforms may still provide decisive advantage.

Since the last NDS was written in 2022, the world has seen significant advances in AI and autonomous systems. Public use and understanding of generative AI have rapidly increased since the launch of ChatGPT in late 2022. On the battlefield, Russia's invasion of Ukraine has driven both sides to develop autonomous and remote-controlled systems to gain an advantage—augmenting or, in some cases, replacing human operators in high-risk missions.[15] In the Middle East, Israel has leveraged AI to process intelligence and to enhance communications and surveillance against Hamas.[16]

These advancements have implications across every domain of military operations, from logistics and surveillance to direct engagement. This evolution in battlefield-tested technology and approaches to fighting presents the United States—and its adversaries—with new considerations for the future of warfare. To ensure the United States remains competitive, the forthcoming NDS must define the DoD's vision for the future fight, investment priorities for new technology compared to traditional platforms, and how the US military will structure and conduct combined arms operations in the age of AI and autonomy.

Traditional combined arms doctrine is built on the coordinated use of different types of forces—such as infantry, armor, artillery, and aviation—to apply strengths against enemy weaknesses and win battles. In the emerging operational environment, these elements will increasingly include uncrewed systems in all domains and machine-speed decision-making support tools.

15. Samuel Bendett and David Kirichenko, "Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine," Modern War Institute, January 10, 2025, https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/.
16. "How US Tech Giants Supplied Israel with AI Models, Raising Questions about Tech's Role in Warfare," Australian Broadcasting Corporation, February 21, 2025, https://www.abc.net.au/news/2025-02-22/how-us-tech-giants-supplied-israel-with-ai-models/104956164.

Air

Autonomy and AI will apply to every domain: land, air, sea, undersea, and space. For example, consider the air domain. In Ukraine, unmanned aerial systems (UAS) have played a transformative role, fundamentally changing the character of fighting near the front line and disrupting traditional force structure assumptions. Both Russia and Ukraine have employed UAS for ISR, targeting, and precision strikes—frequently at ranges that exceed those of conventional direct-fire systems. This ability to deliver effects across operational depths has shifted tactical and operational planning frameworks.[17]

UAS have also effectively democratized access to airpower, creating new challenges for air-defense systems. Air superiority, once the purview of advanced militaries with access to costly platforms and highly trained pilots, is now complicated by the widespread availability of low-cost, commercially available drones; state and non-state actors can contest control of the air littoral with even modest investments. This development has produced an increasingly dense and complex aerial battlespace, forcing militaries to rethink how they integrate both exquisite, crewed platforms—such as the F-35—and uncrewed systems to generate desired operational effects. At the same time, forces must adapt their defensive measures to detect, track, and neutralize adversary UAS. These considerations are not limited to the air domain; similar dynamics are unfolding across all warfighting domains as unmanned systems are increasingly used in modern operations.

Rethinking expendability and survivability of assets

The onset of relatively cheap uncrewed systems and platforms has shifted concepts around the expendability and survivability of US assets, and the appropriate high-low mix the force needs.

Traditionally, military planners categorized assets into two distinct classes: ammunition as expendable and high-value platforms as survivable. The proliferation of UAS has introduced a more nuanced framework. Assets can be classified into four tiers: expendable assets, such as conventional munitions, intended for one-time use; attritable assets, low-cost platforms whose loss carries minimal strategic impact; risk-tolerant assets, mid-range uncrewed assets that commanders prefer to retain but can accept losing if necessary; and survivable assets, high-value platforms or personnel that require protection.[18]

This framework allows commanders greater flexibility to manage risk, enabling a wider range of operational options tailored to specific environments rather than all-or-nothing decisions between risking critical assets or foregoing action.[19]

Capabilities to develop and acquire

In this context, the DoD must consider the capabilities the military needs for future fights, the right high-low mix, and which systems the Pentagon will acquire and divest from accordingly. A combination of high-end, expensive, technologically advanced weapons systems and low-cost, more readily available and adaptable options is needed.

A conflict in the Indo-Pacific will look different from the ongoing war in Ukraine—force projection and sustainment will be exceedingly more challenging across vast distances and denied environments, and the air and sea domains will feature prominently. The NDS should outline a vision for the Indo-Pacific fight that combines the complementary advantages of low-cost autonomous systems with high-end platforms and weapons. At present, the US military lacks both the optimal force composition and an operational concept for employing this capability mix to defeat the Chinese People's Liberation Army (PLA). To address this, the DoD must accelerate the rapid fielding of affordable autonomous systems, develop operational concepts that leverage a balanced combination of high-end and low-end assets, reform acquisition processes, and strengthen the defense industrial base to enable faster production and deployment of critical systems.[20]

The high-low mix should be understood as a deliberately uneven balance between high-end, exquisite, crewed platforms that command large numbers (or swarms) of low-end, autonomous, attritable, or expendable systems to deliver firepower and maneuver in operational environments. As the services develop the next generation of platforms and weapons, this high-low mix should be at the center of platform, weapon, and overall force design.

17. Matthew Slusher, "Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience," Center for Strategic and International Studies, May 2, 2025, https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience.
18. Ibid.
19. Ibid.
20. Stacie Pettyjohn, et al., "Build a High-Low Mix to Enhance America's Warfighting Edge and Deter China," Center for a New American Security, January 20, 2025, https://www.cnas.org/publications/commentary/strengthen-indo-pacific-deterrence-by-enhancing-americas-warfighting-edge.

Implications for combined arms

The challenge for the DoD is not simply to acquire new technologies, but also to integrate them into cohesive operational concepts and force structures. This addition will require rethinking training, command-and-control relationships, and sustainment models. Crewed-uncrewed teaming must become a routine feature of joint operations, with pilots, infantry, and naval crews regularly operating alongside and supported by autonomous systems. The services must also address critical issues of interoperability, data integration, and AI trust and assurance to ensure that these capabilities can be fielded at scale and used effectively in contested environments.

The next NDS should outline a roadmap for balancing investments in cutting-edge systems with legacy capabilities that remain essential for deterrence and combat power. Defense acquisition reform, expanded testing and evaluation, and more rapid operational experimentation cycles will be key to fielding and integrating promising technology. Importantly, the strategy must guard against creating brittle dependencies by ensuring autonomous systems enhance, rather than replace, existing systems and platforms.

4. Prioritize space as a strategic enabler

Space must receive significantly elevated prioritization in the forthcoming NDS that reflects its role as a strategic enabler of US homeland defense and military operations worldwide. In the twentieth century, control of the air meant dominance of the battlespace. In the twenty-first century, control of space will likely determine who prevails in conflict. Therefore, the United States must both deny China, Russia, and other adversaries to ability to exploit space for malign purposes or military advantage during wartime, and ensure the protection and freedom of US and allied operations in, through, and supported by the space domain. Space is not simply a supporting domain but an operational battlespace that underpins every element of modern warfighting and deterrence. Yet, despite its centrality, space remains under-resourced—as most recently evidenced in the President's Fiscal Year 2026 Discretionary Budget Request, which fell short of the investment required to sustain US space dominance or prepare for emerging threats.[21]

To address this, the budgets for both the US Space Force and SPACECOM must be substantially increased. These organizations are responsible for both securing the space domain and ensuring that US military forces can operate effectively across all other domains: air, land, sea, and cyber. Without assured access to space capabilities, the effectiveness of US power projection globally would be dangerously compromised—especially in the Indo-Pacific.

Increased threats in, from, and to space

The threat environment demands this prioritization. Both China and Russia are rapidly advancing their military and dual-use space capabilities, particularly counter-space systems designed to deter the United States from military engagement or to deny or degrade US access to space in crisis or conflict. These include electronic warfare systems, jammers, cyberattacks, and direct-ascent and co-orbital anti-satellite weapons. China and Russia's objectives are to exploit the US military's heavy reliance on space-based systems for critical missions such as ISR; long-range precision strike coordination; global communication; positioning, navigation, and timing (PNT); missile warning; and NC3. This space dependence extends beyond the military—it is foundational to the US economy, infrastructure, and daily civilian life.

Space is key to an Indo-Pacific strategy

A China-focused strategy requires particular attention to space as a contested domain. The Indo-Pacific is a theater defined by vast distances, across which the United States must coordinate joint and coalition operations. Space systems enable persistent situational awareness, early missile warning, secure and resilient communications, and precise targeting—capabilities essential to defending US interests and supporting allies and partners such as Taiwan. US planners should assume that in the opening phase of any conflict with China, Beijing would attempt to degrade or destroy US satellite constellations to "blind" and "deafen" US forces—disrupting critical ISR and communications systems to hinder a rapid and decisive US response. Such attacks would expand China's freedom of action in a theater where time, precision, and reach are decisive.

At the same time, China's growing dependence on space for its own early warning, midcourse missile defense, and force coordination creates vulnerabilities the United States could exploit. Space has become central to Chinese military power, and to China's broader strategy of deterrence, coercion, and national power.

In this context, the Space Force and SPACECOM must prioritize both offensive and defensive capabilities to ensure US freedom of action in space, protect critical assets, and deny China's ability to leverage space for military advantage. This includes safeguarding space-based ISR, communications, and

21. "The President's FY 2026 Discretionary Budget Request," White House, last visited June 9, 2025, https://www.whitehouse.gov/omb/information-resources/budget/the-presidents-fy-2026-discretionary-budget-request/.

targeting while retaining the means to disrupt or degrade China's own space-dependent operations in conflict.

Prioritizing space in the NDS

The next NDS should recognize that space is not just a supporting domain; it is a contested operational environment that underpins every aspect of joint operations. From communications and navigation to early missile warning and intelligence gathering, space-based systems are foundational to deterrence, warfighting, and day-to-day military readiness.

To elevate space as a true priority in the next NDS, the DoD must significantly increase investment in rapid-launch and satellite replenishment capabilities to ensure resilience and continuity in the event of attack or degradation. It must also deepen partnerships with the commercial space sector to harness private-sector innovation, scale, and agility in developing next-generation systems. Additionally, the United States should augment military capabilities with hybrid commercial-military space architectures to leverage increasing private capacity. Developing countermeasures against anti-satellite threats—including space-based missile-defense systems and advanced electronic warfare capabilities—is equally essential to protect critical space assets.

Neglecting to prioritize space risks undermining the top two priorities in the forthcoming NDS—homeland defense and deterring China. Without assured US access to and freedom of action in space, China and Russia could shape the domain to their advantage—threatening US national security, economic stability, and the credibility of US deterrence—placing the nation's ability to prevail in high-end conflict at serious risk. Space will likely be one of the first fronts in future warfare. The NDS must reflect this reality with commensurate strategy, resources, and operational focus.

5. Deter strategic attacks on the homeland

To achieve the likely objectives of the next NDS (defending the homeland and deterring Chinese aggression), the United States must place renewed emphasis on addressing the risk of a strategic attack against the US homeland. Deterring such an attack—and, if deterrence fails, ensuring the ability to restore deterrence with the lowest level of damage consistent with acceptable political and military outcomes—is essential for two reasons.

First, the prospect of strategic attack gives adversaries potential leverage to coerce the United States into abandoning its support for allies and partners, or the chance to inflict military damage sufficient to impair the US ability to sustain such support, directly undermining the goal of deterring China. Second, US adversaries are capable of imposing costs on the United States—particularly through strategic attack—that would far outweigh the potential benefits Washington seeks to achieve through its global defense and foreign policies, thereby threatening the objective of securing the homeland itself.

The NDS should therefore prioritize a plan to deter and reduce the risk of strategic attacks on the US homeland, focusing on five mutually supporting pillars.

Deter a large-scale nuclear attack on the homeland

First, the United States must credibly deter large-scale nuclear attack on the US homeland—the only truly existential threat posed by other nation-states. This necessity demands a survivable nuclear second-strike capability, modernized NC3, and robust continuity-of-government measures. Key features of the existing deterrent posture—such as ensuring no single delivery system becomes a sole point of failure and avoiding reliance on capabilities that must be launched under attack to avoid destruction—remain essential for maintaining strategic stability. Completion of the ongoing nuclear triad and NC3 modernization programs is critical.

Prevent nuclear escalation in regional conflicts

Second, the United States must prevent nuclear escalation in regional conventional conflicts. Once nuclear use begins—even on a limited scale—there is a grave risk of uncontrollable escalation. To reduce this risk, US strategy must ensure that adversaries perceive no clear path to gaining advantage through nuclear use. This requires forward-deployed and credible theater nuclear options; strong and binding alliance commitments; conventional forces trained, equipped, and ready to operate in a nuclear-degraded environment; capabilities to defeat or blunt adversary limited nuclear options; and strategic damage-limiting systems that could constrain adversary confidence in achieving war aims through nuclear coercion or use. Moreover, US war plans and operational concepts must, where possible and consistent with war objectives, avoid threatening the types of targets that would heighten adversary fears of regime change or existential defeat—thereby reducing incentives for nuclear first use.

Extended deterrence

All of these measures support another important goal—extending deterrence of nuclear and nonnuclear strategic attack on US allies and partners and assuring these states trust in US deterrence. This extended deterrence supports another reported goal of the interim defense guidance—increased

burden sharing with allies.[22] Allies and partners, if they are subject to nuclear coercion which they lack the means to resist, are more likely to accommodate adversaries and withhold support for US and coalition military operations. Enabling allies to resist nuclear coercion will keep them in the fight as important partners and assets to US strategy. Conversely, failing to extend deterrence to allies facing potential existential threats could lead these states to develop their own nuclear weapons, which would undermine a central tenet of US foreign policy and likely raise global nuclear dangers.

Avoid over-reliance on conventional deterrence

Third, the United States and its allies must field conventional forces sufficient to deter major-power conventional war—without compromising the nuclear deterrent that underwrites escalation control. Conventional deterrence has historically been fallible; great powers have initiated wars despite apparent conventional disadvantage. US conventional success might also inadvertently increase adversary incentives to escalate to nuclear use if adversaries fear catastrophic regime loss. Without sufficient nuclear backstopping, a force overly optimized for conventional warfighting invites adversary calculations of nuclear escalation as a rational response. Flexible and credible US nuclear options remain essential both to deter escalation and, in certain scenarios, to offset potential US conventional inferiority—such as in simultaneous regional conflicts.

Deter nonnuclear, high-consequence strategic attacks

Fourth, the United States must retain a flexible declaratory policy and field adaptable strategic forces capable of deterring high-consequence, nonnuclear strategic attacks on the homeland. These could include biological attacks (e.g., the release of a genetically engineered pathogen), crippling cyber strikes on the US economic system, or massed precision conventional strikes on US nuclear forces or NC3 infrastructure. The US posture should preserve a degree of ambiguity about what thresholds could prompt nuclear retaliation, while maintaining the capacity for rapid, reliable attribution of such attacks—a necessary condition for credible deterrence.

Build homeland resilience against strategic attack

Fifth, the United States must enhance its capacity to absorb and recover from strategic attack. Resilience of warfighting capability, continuity of government, preservation of societal function, and sustaining national willpower in the aftermath of strategic attack are all essential both to limit damage and to deny adversaries confidence that such attacks could decisively undermine US strategy.

The imperative of prioritizing homeland deterrence in the NDS

Deterring large-scale nuclear attack on the homeland remains the cornerstone of national security because such attacks are capable of destroying the United States as a functioning society. Yet the requirements for such deterrence have grown more complex. Modern deterrence demands not only secure nuclear forces and command systems but also theater nuclear options, credible damage-limiting defenses, escalation-management tools, and homeland resilience measures. Failure to fully prioritize this mission in the next NDS would leave open dangerous vulnerabilities that adversaries such as China and Russia could exploit—ultimately placing both the defense of the homeland and the ability to deter aggression abroad at unacceptable risk.

Conclusion

As the DoD prepares to release the forthcoming NDS, the United States stands at a pivotal moment. The challenges ahead—including intensifying strategic competition with China, rapid technological change, and the emergence of new domains of conflict—demand a clear, focused, and forward-looking strategy. This issue brief has outlined five essential priorities that should shape the NDS: defending the homeland; treating China as the primary competitor on a global level; modernizing US forces for combined arms operations in the age of AI and autonomy; prioritizing space as a critical enabler; and deterring strategic attacks on the US homeland through a resilient and modernized deterrent posture.

Together, they form a comprehensive framework to protect US lives, interests, and values in an increasingly contested world. The forthcoming NDS is more than a policy document—it is an opportunity. Bold strategic vision must be met with necessary resources and capabilities to back it up. By embracing these priorities with clarity and commitment, the NDS can deliver a defense strategy that meets today's threats and secures the United States' future.

22. Cohen and Lieberman, "Pentagon Tasked with Providing 'Military Options' to Ensure US Access to Panama Canal, Memo Says."

Author biography

Clementine Starling-Daniels is the director and resident fellow of the Atlantic Council's *Forward* Defense program housed within the Scowcroft Center for Strategy and Security. She leads a team of staff and fellows focused on defense issues. Originally from the United Kingdom, she previously worked in the UK Parliament on NATO, European security, and defense issues. She received her BS from the London School of Economics and her MA from Georgetown University.

Acknowledgements

The author would like to thank Aaron Brady, senior US Air Force fellow at the Atlantic Council, for his input on the China, space, and combined arms sections of this issue brief—it's a pleasure to work with your talent! A big thank you to Mark Massa, deputy director for strategic forces policy in the Atlantic Council's *Forward* Defense Program, for his indispensable contribution to the strategic deterrence section and his peer review, which strengthened this brief. Finally, thank you to Amy Cowley, program assistant in the Atlantic Council's *Forward* Defense Program; Theresa Luetkefend, assistant director in the Atlantic Council's *Forward* Defense Program; and Curtis Lee, program assistant in the Atlantic Council's *Forward* Defense Program for their valuable inputs and peer review.