Atlantic Council

July 2025

Issue brief The border and beyond:
Homeland defense in an era of new strategic threats

Clementine Starling-Daniels and Amy Cowley

From launching cyberattacks to targeting critical infrastructure, US rivals are bringing the fight closer to home. Defending against these threats will require not just military might, but smarter defense planning, greater resilience, and military modernization.

Bottom lines up front

- The domestic systems that underpin US security and prosperity—including energy grids, digital and financial networks, the defense industrial base, and transportation infrastructure—are increasingly vulnerable to a broad spectrum of modern threats: conventional, nuclear, asymmetric, and digital. To address these persistent vulnerabilities, the Department of Defense (DoD)'s forthcoming National Defense Strategy (NDS) is expected to prioritize homeland defense.
- Responding to these complex threats requires a comprehensive approach to homeland defense that extends beyond border security. This approach must encompass missile defense and the protection of critical defense systems—such as space infrastructure—from cyberattacks and other forms of malign interference.
- In the NDS, the DoD must clearly define where it will take the lead and where it will support civilian agencies and the private sector. This includes reinforcing efforts to defend critical infrastructure and strategic nodes—such as energy grids, ports, digital systems, and industrial hubs—against cyber and physical attacks, long-range missile threats, and coercive economic activities.

Introduction

Threats to the US homeland have fundamentally changed from two decades ago. In the years following 9/11, the most pressing dangers came from terrorist groups intent on carrying out attacks on US soil. Today's threat landscape is broader and more complex. Peer-state competitors, transnational criminal organizations, and non-state actors now possess the means to target the US homeland through a range of kinetic and non-kinetic capabilities. These include long-range missiles, cyberattacks, sabotage, disinformation, and malign foreign influence—all tools designed to disrupt critical infrastructure, weaken public trust, and undermine the ability of the United States to project power abroad.

The traditional model of homeland defense has relied on a layered approach of projec-

ting military forces forward—intercepting threats overseas to prevent them from reaching the homeland. This "defense in depth" approach has long been central to US strategy. However, the second Donald Trump administration appears to be reshaping this model by placing greater emphasis on addressing threats much closer to and within US territory, a potentially fundamental shift in the concept of homeland defense.

This evolution reflects the reality that projecting power forward is no longer sufficient on its own. The US homeland is no longer a sanctuary; adversaries now possess the means and intent to exploit vulnerabilities inside the United States itself—through cyber intrusions, information warfare, long-range missile threats, and other gray-zone tactics—to constrain US military options and coerce strategic decision-making.

While this new focus appropriately highlights the need to protect critical assets closer to home, the Trump administration's approach has so far concentrated more narrowly on large-scale air and missile defense (including early proposals for a "Golden Dome for America") and on tightening the nation's land border security, particularly along the southern border.[1] To effectively achieve homeland defense, this shift must also address a broader set of domestic vulnerabilities. It must encompass the protection of critical infrastructure, the hardening of cyber and space systems, the safeguarding of the US research and innovation ecosystem, and defense against sabotage and malign interference toward other US centers of gravity. It also requires stronger coordination with civilian agencies and the private sector to ensure shared situational awareness and resilience. The National Defense Strategy (NDS) offers an opportunity to clearly define where the Department of Defense (DoD) should lead and where it should play a supporting role, while prioritizing defense, resilience, and redundancy across the interconnected systems that underpin US national power, military strength, and the daily functioning of society.

What is the DoD's role in homeland defense?

The DoD plays a critical but distinct role in homeland defense, defined as the protection of the nation's sovereignty, territory, domestic population, and critical defense infrastructure from external threats or other threats as directed by the president.[2] This mission runs in parallel to, and is distinct from, the broader homeland security mission led by the Department of Homeland Security (DHS), which coordinates federal, state, local, tribal, and territorial (SLTT) efforts to prevent terrorist attacks, secure borders, oversee the movement of people and goods, manage emergencies, strengthen cybersecurity, and safeguard critical infrastructure through other agencies. These agencies include the Federal Emergency Management Agency (FEMA), Customs and Border Protection (CBP), and the Cybersecurity and Infrastructure Security Agency (CISA).[3] While many of the tools necessary to secure the homeland reside within civilian agencies including DHS, the Department of Energy (DOE), the Department of the Treasury, the Department of Commerce, the Department of Transportation (DOT), and agencies like the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC)—the DoD has a critical, defined role in defending the homeland against external military threats and supporting resilience against strategic disruption. In extreme circumstances, DoD may be requested and authorized to provide Defense Support for Civil Authorities (DSCA); however, supporting such activities involves repurposing forces and capabilities planned for other missions.[4] As the range and magnitude of threats to the homeland increase, the DoD serves as both a supported and supporting partner to entities such as DHS and the Federal Bureau of Investigation (FBI).

1. "Executive Order 14186: The Iron Dome for America," Federal Register, January 27, 2025, https://www.federalregister.gov/documents/2025/02/03/2025-02182/the-iron-dome-for-america; Eleanor Watson, "Trump Announces $25 Billion and Architectural Design for 'Golden Dome' Missile Defense System," CBS News, May 20, 2025, https://www.cbsnews.com/news/trump-golden-dome-25-billion-dollar-missile-defense/.
2. "Homeland Defense," Under Secretary of Defense for Policy, US Department of Defense, last visited June 15, 2025, https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Hemispheric-Affairs/Homeland-Defense-Integration-and-DSCA/faqs/#Section1.
3. "About CISA," US Cybersecurity and Infrastructure Security Agency, last visited June 15, 2025, https://www.cisa.gov/about; "What Does DHS Do?" US Department of Homeland Security, last visited June 15, 2025, https://www.dhs.gov/employee-resources/what-does-dhs-do.
4. Hannah D. Dennis, Kristy N. Kamarck, and Nicholas M. Munves, "Defense Primer: Defense Support of Civil Authorities," US Congress, April 9, 2025, https://www.congress.gov/crs-product/IF11324.

Protect defense facilities and defense critical infrastructure

To effectively fulfill its homeland defense mission, the DoD must strengthen its efforts to safeguard the infrastructure that underpins US military readiness and national resilience. This includes not only physical assets like bases and supply chains, but also digital networks, industrial systems, and space-based platforms that are essential for projecting and sustaining the US military force globally. These systems are increasingly vulnerable to both kinetic and non-kinetic threats from state and non-state actors—and they can disrupt US defense operations, delay crisis response, and degrade deterrence.

The DoD's Defense Critical Infrastructure Program (DCIP) provides the framework for identifying, assessing, and protecting infrastructure that is essential to national security. It defines defense critical infrastructure as systems or assets that are physical or virtual, whose incapacitation would severely impact national defense, economic security, public health, or public safety.[5] These are not merely military installations or command centers, but a broader set of strategic enablers dispersed across civilian and commercial sectors.

While CISA, under DHS, leads broader federal efforts to protect critical infrastructure across sixteen nationally designated sectors, the DoD plays a vital role in defending infrastructure that directly supports or intersects with military operations.[6] Under Presidential Policy Directive 21 (PPD-21), CISA coordinates risk assessments, threat mitigation, and resilience planning across a wide array of civilian infrastructure systems. The DoD's role is crucial in ensuring, through close coordination with CISA, that defense and military-relevant infrastructure—whether operated by the DoD or privately owned—is adequately defended against emerging threats.

To strengthen homeland defense, the next NDS should prioritize the DoD's increased investment in, and coordination with, civilian efforts to protect critical infrastructure relevant to US defense and security. This includes identifying and focusing on vulnerabilities across interconnected systems that support military operations, such as military bases and installations, transportation and logistics hubs, supply chains, energy grids that power military installations, communications infrastructure, the defense industrial base, critical space infrastructure, and other digital and financial systems that support military operations. Many of these assets lie outside the traditional defense enterprise but are essential for enabling sustained military action and preventing coercive external influence that impacts defense decision-making.

This broader set of assets overlaps with what can be described as the US national centers of gravity, or the foundational systems and institutions that support US power, credibility, and stability. Historically, US strength has rested on the effective integration of diplomatic, informational, military, and economic power. That strength, however, is not abstract. It relies on a complex web of infrastructure, technology, and public trust that adversaries increasingly seek to exploit.

These centers of gravity include the physical and functional systems that make US power possible, and which are now being targeted precisely because of their importance. They span sectors such as the following.

- **Nuclear weapons capabilities and production infrastructure**: This includes the US nuclear triad, its supporting command and control, production and assembly sites for warheads and complete weapons, and weapons storage. The survivability of nuclear weapons is essential for strategic deterrence, and protection of weapons production and storage is important for endurance, especially in protracted or sequential conflicts.
- **Conventional military facilities**: Military bases, airfields, naval ports, weapons depots, testing ranges, and other facilities based within the United States are core sources of US military strength and power-projection capability.
- **Energy infrastructure**: The national power grid, oil and gas pipelines, refineries, and distribution networks are essential not only because of the basic services that impact everyday life, but also for military readiness and economic activity.
- **Transportation and logistics hubs**: Major ports (e.g., in California, Virginia, and Texas) and rail and highway chokepoints are vital for the flow of goods and military logistics.
- **Critical manufacturing and the defense industrial and technology base**: Facilities that produce military platforms, munitions, and other equipment are central to sustaining a prolonged conflict in any theater of war. Software factories, chip fabrication plants, and medicine manufacturers that support warfighters are as essential as aircraft, ships, and tanks.

5. "DoD Protected Critical Infrastructure Program," Under Secretary of Defense for Policy, US Department of Defense, last visited June 15, 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 15, 2025, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

- **Space infrastructure**: Space-based positioning, navigation, and communication satellites are crucial to operations across various military, industrial, and commercial applications. Ground stations and launch facilities are essential features of the space ecosystem.
- **Financial systems and services**: The US economy relies on a stable banking system, digital payments, and access to global markets. Banks, payment systems, capital markets, and digital financial infrastructure ensure the stability of the US economy.
- **Digital and communications infrastructure**: Internet backbones, telecommunication systems, and cloud infrastructure ensure continuity in government, business, and emergency response.
- **The chemical sector**: Facilities and production lines that are involved in the use, manufacturing, storing, transportation, and delivery of chemical materials are essential to global supply chains and US national security.
- **Dams and waterways**: This includes infrastructure that manages water supply, treatment, and flood control, such as dams, reservoirs, and treatment plants. These systems support essential services including hydroelectric power, municipal and industrial water use, agricultural irrigation, inland shipping, and environmental management, making them vital to both public health and economic activity.
- **Emergency services**: First-responder systems, including police, fire, emergency medical services (EMS), and emergency communications networks are vital to managing crises and maintaining public order.
- **Food production and distribution**: Agricultural infrastructure, processing facilities, and distribution networks are essential to national stability, especially in crisis scenarios during which supply chains might be disrupted.
- **Government services and facilities**: Federal, state, and local government offices and coordination centers are central to ensuring governance and public confidence.
- **Healthcare and public health hubs**: Hospitals, pharmaceutical manufacturing, and public health coordination centers are critical for national well-being and healthcare resilience.
- **Nuclear reactors, materials, and waste**: Nuclear energy infrastructure, including reactors and storage facilities for materials and waste, must be safeguarded due to the potential for catastrophic impact if they are compromised.
- **Information networks and infrastructure**: The systems and platforms that transmit and shape information—including social media, broadcast media, and digital communications—are increasingly being targeted to erode public trust, amplify unrest, and weaken institutional legitimacy.
- **Academic and research institutions**: Universities, national laboratories, and research organizations conduct innovation-critical work tied to defense and national security.

While it is not in the DoD's remit to protect all of the national centers of gravity, fulfilling its priority of protecting the homeland effectively means the DoD should work with other agencies to prevent persistent vulnerabilities to centers of gravity that may directly or secondarily impact critical defense infrastructure and military planning. These systems are not merely enablers of everyday life in the United States; they are strategic assets that adversaries are increasingly targeting to undermine US strength and domestic stability. They are also likely targets of attack to deter future US involvement in crises or conflicts featuring US allies and partners. These assets must be defended. If adversaries perceive that the United States is unable to effectively protect these systems, they will be targeted.

What threats exist to this critical infrastructure?

Today, threats to the homeland—and, indeed, to individual assets—can come from multiple domains in both overt and covert ways that are sometimes difficult to attribute but might cause significant damage to the United States.

China and Russia might employ overt coercive strategies, using the threat of strikes on the US homeland to shape US decision-making in a crisis. Covert attacks on US systems and financial investment in critical infrastructure can give adversaries access, leverage, and information. Denying adversaries the leverage of holding US territory at risk (from physical or cyber interference) is essential to preserving strategic stability and daily life, and ensures that the United States can project power, support allies, and manage crises at home and abroad without being constrained by fears of paralyzing attacks at home.

Cyber operations have the potential to disable critical infrastructure. Documented cyberattacks against US utility companies, pipelines, and transportation networks by China, Russia, Iran, and North Korea have increased in recent decades.[7] Increased competition in space poses a threat to satellite-enabled communications, navigation, and early warning capabilities. Information warfare erodes trust in US institutions. And long-range strike capabilities offer adversaries the ability to physically target key infrastructure in US territory. Compounding these risks is the growing threat of limited coercive nuclear strikes, which could be used to intimidate the United States into delaying or abandoning a military response abroad.

These threats require not only enhanced defensive capabilities but also deeper interagency coordination, improved infrastructure resilience, and a more proactive approach to domestic threat detection and response. While the DoD must remain within its statutory remit, today's threat landscape—marked by long-range precision strikes, cyber intrusions, and coercion—demands a comprehensive approach to homeland defense. The roles of the DoD and the military in protecting the homeland must account for how global military operations, defense of critical defense infrastructure, and domestic resilience intersect.

DoD priorities for homeland defense

The following subsections outline how the DoD can approach an enhanced role for itself in the following key areas of homeland defense: border security, homeland missile defense, cyber defense of critical defense infrastructure, space infrastructure defense, and improved research security.

1. Border security

The Trump administration has placed early emphasis on securing US land borders from external threats, but an effective homeland defense strategy demands a nuanced approach that protects US territory from both physical and cyber threats.

Recognizing the importance of land border security, the DoD plays a critical role in addressing regional challenges posed by external threats such as transnational organized crime, drug trafficking, and terrorism. Cartels and criminal networks have grown increasingly sophisticated, leveraging gaps in law enforcement coordination across borders. These networks both fuel the domestic drug crisis and present a broader security challenge by undermining the rule of law and public health. Additionally, transnational criminal organizations can erode state authority in neighboring countries, which can destabilize nations with important ties to the United States and create long-term regional security challenges.

While securing land borders is critical for homeland defense, proliferating threats are making air and maritime security increasingly difficult to secure, both within the homeland and in the approaches to it. The growth of uncrewed aerial and surface systems—including those accessible to civilians or easily hidden, as the recent Ukrainian strikes in Russia demonstrate—has made the air and maritime spaces increasingly difficult to monitor and control. While DHS bears much of the responsibility for securing the land borders, US Northern Command (NORTHCOM) and the North American Aerospace Defense Command (NORAD) are critical to air and maritime defense. This mission is not new to NORTHCOM or NORAD. However, the NDS should address two key considerations for a successful homeland defense strategy. First, defense of the air approaches to the United States relies heavily on Canadian support—Canada's friendship is vital to US security. Second, protecting US assets and citizens from uncrewed systems will require extensive coordination between the military (which tends to possess more robust sensing and decision capabilities) and civilian agencies (which are better able to respond within US borders).

As the DoD prioritizes border security, it is important for the NDS to acknowledge the limitations of the department's role in this mission. Beyond constitutional constraints on military use domestically, public trust in the armed forces depends partly on maintaining clear boundaries between military operations and domestic law enforcement responsibilities. The DoD should not assume a domestic security role within US territory. Instead, it should support civilian-led efforts, particularly those managed by the DHS and its components, including CBP. As the NDS considers the military's role in securing the homeland, it should clearly define the parameters of DoD involvement in border-related missions and ensure that its activities focus on deterring and responding to external threats, while preserving civilian leadership in domestic security operations.

7. "North Korea Cyber Threat Overview and Advisories," US Cyber and Infrastructure Security Agency, last visited June 10, 2025, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea; Hannah Rabinowitz and Sean Lyngaas, "FBI Director Warns that Chinese Hackers Are Preparing to 'Wreak Havoc' on US Critical Infrastructure," CNN, January 31, 2024, https://www.cnn.com/2024/01/31/politics/china-hacking-infrascture-fbi-director-christopher-wray/index.html; Stephen Webber, "Threats to America's Critical Infrastructure Are Now a Terrifying Reality," *Hill*, February 11, 2024, https://www.rand.org/pubs/commentary/2024/02/threats-to-americas-critical-infrastructure-are-now-a-terrifying-reality.html.

US border security remains an important element of the broader counterterrorism architecture, as border vulnerabilities can be exploited by individuals seeking to harm the United States. A robust homeland defense strategy must therefore integrate counterterrorism risk into the border security framework. While DHS, CBP, and other civilian agencies must remain the lead agencies on border security and enforcement, the DoD plays an important supporting role. The NDS should reaffirm this principle: the DoD supports, but does not supplant, the role of civilian agencies on domestic border security, including not using appropriated funds or personnel for missions that should be funded and staffed through civilian agencies of SLTT governments. The NDS should designate a portion of the National Guard to prioritize border security, ensuring that operations and maintenance resources and readiness rates are not degraded by sustained active-duty deployments. In the medium term, the DoD should also work with DHS to develop a border security strategy that sets clear policy goals and priorities for sustained DSCA operations. A coordinated and appropriately balanced approach to border security will be essential to homeland defense in an era of transnational and hybrid threats.

2. Homeland missile defense

The forthcoming NDS would be justified in giving higher priority to US homeland missile defense. While much attention is focused on cyber and gray-zone threats, the possibility of kinetic attacks on the US homeland cannot be discounted. In a conflict, the United States might well conduct conventional strikes on adversary homelands, so there is little reason to believe those states would exercise restraint in striking back. If adversaries launch missile strikes against the United States—either from long or short range (including launches from within US territory, as Ukraine did in Russian territory on June 1, 2025)—what would they aim to destroy? What impact would they have? And how sufficient are current US defenses against such strikes? These questions are critical for planners operationalizing both the NDS and Trump's call for a "Golden Dome for America."

US adversaries likely appreciate that a long-range kinetic attack on the US homeland could prove to be highly escalatory and, thus, will likely seek to deploy one only for one of two high-payoff reasons before or during a conflict. First, an adversary might seek to destroy or disrupt military or civilian infrastructure that would delay the ability of the United States to deploy forces overseas in defense of an ally or partner. Doing so might allow an adversary to realize a *fait accompli*—just the threat of such a maneuver might degrade allies' and partners' confidence in US extended deterrence. Second, an adversary might target civilian infrastructure as a way to impose consequences directly on the US population in an effort to degrade the popular will to fight.

For example, possible targets could include energy production and distribution facilities along the Gulf Coast, which concentrate a significant portion of the nation's refining capacity in a relatively compact geographic area.[8] Similarly, major ports serve as critical nodes for both commercial supply chains and military logistics.[9] Even a temporary disruption at any of these sites would reverberate across numerous sectors globally.

The US defense industrial base, particularly facilities involved in the production of precision munitions and essential platforms, would be attractive targets for a strike aimed at degrading long-term US force-generation capacity. Likewise, long-range radars, command-and-control nodes, and air- and missile-defense sites could be hit to delay or disorient the US response to follow-on attacks.

In the most extreme circumstances, Russia could threaten or conduct limited nuclear strikes on US military installations or isolated civilian infrastructure as part of an escalation ladder in lieu of initiating a large-scale nuclear exchange. Given the advent of China as a nuclear peer of the United States, it is possible that China could credibly take such an approach as well. Nuclear attack on the US homeland is made more likely if adversary regional limited nuclear escalation (which would probably precede a direct strike on the US homeland) fails to achieve the desired coercive effect, and if the United States fails to impose costs sufficient to restore deterrence.[10]

Current US missile-defense posture, scoped to address the intercontinental ballistic missile threat from North Korea and to protect the National Capital Region from air-breathing threats, is not designed to address limited, coercive missile threats from Russia and China against a wide range of US civilian and military infrastructure. Trump's "Golden Dome" initiative pro-

8. "Much of the Country's Refinery Capacity Is Concentrated along the Gulf Coast," US Energy Information Administration, July 19, 2012, https://www.eia.gov/todayinenergy/detail.php?id=7170.
9. "Ports Primer: 2.1 the Role of Ports," US Environmental Protection Agency, last visited June 15, 2025, https://www.epa.gov/ports-initiative/ports-primer-21-role-ports#:~:text=Our%20nation's%20ports%20are%20an,national%20defense%20and%20emergency%20preparedness.
10. Robert Soofer, "'First, We Will Defend the Homeland': The Case for Homeland Missile Defense," Atlantic Council, January 4, 2025, www.atlanticcouncil.org/in-depth-research-reports/report/first-we-will-defend-the-homeland-the-case-for-homeland-missile-defense/.

poses a significant investment in left-of-launch capabilities, sensors, and interceptors across domains to counter ballistic, cruise, hypersonic, and other airborne threats. Missile-defense investments, as part of the NDS, will help support this aspect of homeland defense. Beyond planned ground-based midcourse defense systems, the DoD should consider augmenting the projected US missile-defense architecture with an additional underlayer.[11] Furthermore, the DoD should develop plans to expand the current Ground-based Midcourse Defense (GMD) architecture and place greater emphasis on investing in future capabilities, including space-based sensors and interceptors. The DoD must also recognize the threat posed by smaller airborne vectors and create defensive architecture at critical defense infrastructure sites to combat such threats.[12]

3. Protecting defense critical infrastructure through cyber defense

Improving cyber protections of US defense critical infrastructure is another critical priority for the DoD's homeland defense mission, and it should be articulated in the NDS. Modern threats to the homeland increasingly arise in the form of non-kinetic attacks, which include cyber operations and electronic warfare that can disrupt and harm the United States without physical proximity. While non-kinetic, such attacks can have physical effects and are enticing to adversaries because they can exploit systemic vulnerabilities across the US digital, cognitive, and electronic landscapes; they are difficult to attribute to a specific actor, and they are often employed below the threshold of armed conflict, making consensus around proportionate response options less clear or decisive. Cyberattacks pose one of the most immediate and persistent threats to US infrastructure. Adversaries are increasingly able to probe, infiltrate, and even sabotage critical US networks through digital attack.

Two central challenges exist in the cyber domain: deterrence and attribution. On deterrence, there is little evidence to suggest that the United States or other actors can deter offensive cyber activities beyond disrupting specific attacks in progress.[13] Shaping adversary behavior in cyberspace remains difficult. On attribution, unlike with missile strikes, the origin of a cyberattack is not always clear because sophisticated actors obscure their actions.[14] This obfuscation can create problems for decision-makers responding to such attacks—acting without high-confidence attribution risks miscalculation or escalation, while waiting for compelling evidence can delay responses. The difficulty of the attribution problem can also undermine public support for any response.

For the DoD's homeland defense mission, protecting defense critical infrastructure through stronger cyber defense is an urgent priority. US infrastructure and systems remain vulnerable—some are already compromised—and deterrence has largely failed to prevent malicious cyber activity. Moreover, the speed of attribution and response times likely cannot keep pace with the tempo of a high-end conflict, raising the risk of miscalculation or paralysis in crisis.

To counter these threats, the DoD must enhance its cyber posture for homeland defense. US Cyber Command (CYBERCOM)'s "defend forward" strategy (first implemented under the first Trump administration) has focused on disrupting threats before they reach US networks. While these operations have largely centered on forward defense, the emerging emphasis on defending assets closer to home raises the question of whether CYBERCOM's mandate should evolve accordingly. In particular, CYBERCOM could be called upon to play a greater role in protecting critical defense infrastructure alongside CISA, ensuring DoD-relevant assets such as military installations, space-based systems, and the defense industrial base are shielded from hostile cyber activity.

Whether through forward disruption or domestic defense, CYBERCOM's capabilities must be resourced and expanded to keep pace with adversary advancements. The next NDS should explicitly recognize the essential role of cyber operations in homeland defense and outline a framework for how CYBERCOM and CISA will collaborate, complementing each other's authorities and strengths. As cyber threats proliferate, defending forward will require a significant increase in cyberspace equipment and the expansion of both the Cyber National Mission Force and the Cyber Protection Force. These elements should grow in size and capacity to meet the demands of a contested and evolving digital battlespace, ensuring that the United States can detect, deter, and disrupt cyberattacks before they can inflict strategic harm.

11. Ibid.
12. Ibid.
13. James Andrew Lewis, "Deterrence and Cyber Strategy," Center for Strategic and International Studies, November 15, 2023, https://www.csis.org/analysis/deterrence-and-cyber-strategy.
14. Jake Sepich, "The Evolution of Cyber Attribution," American University, April 19, 2023, https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm.

4. Protect defense critical infrastructure, particularly space infrastructure

The DoD should also place renewed emphasis on securing and hardening US space ground infrastructure within its broader homeland defense mission. As with cyber operations, a considerable amount of US space power is employed in place—the forces might be allocated to a combatant command, but they conduct their operational mission from ground stations at their home bases. These terrestrial sites are particularly vulnerable, making them potential weak points that adversaries could disrupt or destroy to deny US space access.[15] Given the military's deep dependence on space-based assets for global force projection, communications, intelligence gathering, and missile warning, these terrestrial nodes are critical enablers of national defense. US Space Command and the US Space Force (USSF) must lead efforts to enhance the resilience of this infrastructure. That includes working closely with interagency partners and the commercial space sector to develop and implement stronger security standards, invest in system hardening, and conduct joint exercises that simulate potential threats and identify operational gaps. Safeguarding these capabilities is essential to maintaining the integrity and continuity of US defense operations in both peacetime and conflict.

The NDS must prioritize space infrastructure as a critical strategic enabler, and the subsequent defense budget should substantially increase resources to support US space capabilities. In particular, the DoD must work with civilian agencies to adequately secure vulnerable US ground stations, which remain critical nodes in the space architecture and attractive targets for adversary attack or disruption. This effort should include hardening physical security, improving cybersecurity measures, enhancing redundancy, and developing rapid capabilities. To protect these assets effectively, the USSF or other appropriate authority must be organized, trained, and equipped to protect critical space infrastructure from a wide range of threats, up to and including swarming autonomous systems. The Pentagon must also integrate and build on the DoD's Commercial Space Integration Strategy and the US Space Force's Commercial Space Strategy to fully ensure that new technology emerging from the commercial space sector is adequately secured. These steps are essential to deny adversaries the ability to exploit vulnerabilities in US-based space infrastructure and to sustain a US operational advantage in crisis.

5. Protect defense critical infrastructure from sabotage and malign interference

Another way the DoD should enhance homeland defense is by expanding its support to civilian agencies working to counter foreign threats operating inside the United States. This includes providing intelligence, analytical tools, and technical expertise to agencies conducting counterintelligence operations against adversary actors that attempt to infiltrate or manipulate US infrastructure, institutions, or domestic systems. In particular, the DoD can play a valuable role in supporting law-enforcement efforts to prevent sabotage of critical infrastructure and helping regulatory bodies identify and block malign foreign investment—especially in sectors or geographic areas with strategic defense relevance, such as land adjacent to military bases or facilities supporting national security missions.

Beyond cyberattacks, defense critical infrastructure might be vulnerable to financial investment by adversaries, which is often obfuscated or conducted through proxies. The White House published its America First Investment Policy, which outlines the need to combat visible and concealed (through partner companies or investment funds in third countries) foreign investment in the United States that is not in the US national interest, specifically calling out Chinese Communist Party investments.[16]

Adversaries increasingly exploit legal, financial, and industrial channels to gain access to sensitive assets or introduce vulnerabilities into key national systems. In this context, closer DoD coordination with entities like the FBI, DHS, the Committee on Foreign Investment in the United States, and the DOE can help ensure that national defense equities are fully considered in risk assessments and security decisions. The DoD's insights into the defense implications of infrastructure vulnerabilities—particularly in areas tied to force projection, logistics, and command and control—can help civilian agencies identify risks that might otherwise go undetected. DoD support to civilian departments and the private sector can also 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.

15. Matthew Heideman, "Why We Need to Take Satellite Ground Station Security Seriously," *Space News*, June 4, 2024, https://spacenews.com/why-we-need-to-take-satellite-ground-station-security-seriously/.

16. "America First Investment Policy," White House, February 21, 2025, https://www.whitehouse.gov/presidential-actions/2025/02/america-first-investment-policy/.

6. Protect defense critical infrastructure through improved research security

Research security is an underappreciated but critical component of a comprehensive approach to homeland defense and security. Many US research institutions, national laboratories, universities, and start-ups conduct work that is essential to national defense and military interests. Protecting research and development from espionage, sabotage, and intellectual property theft is vital to safeguarding core US strategic advantages: innovation prowess and academic and research excellence.

International collaboration—through data sharing, joint research, and the exchange of personnel—has driven scientific discovery and technological advancement. Yet it can introduce vulnerabilities. Some nations, particularly China, have exploited open research environments and international partnerships to gain access to sensitive information and talent, using legal, illegal, and extralegal methods, including industrial espionage and explicit exploitation of diaspora networks.[17]

While foreign nationals working and studying in the United States make invaluable contributions to US scientific and technological progress—and their rights and academic freedoms must be respected—the DoD and civilian agencies like the FBI must account for the risks associated with adversarial access to defense-relevant research and development ecosystems. This includes the potential exploitation of US universities, federally funded research centers, and private-sector companies by foreign intelligence services under the cover of legitimate academic or commercial collaboration.

Research security policies, education, and practices must be revised when needed, and rigorously applied and consistently enforced across the diverse landscape of institutions engaged in US basic and applied research. Today, adherence to research security standards remains uneven across this ecosystem, creating vulnerabilities that adversaries, particularly China, actively seek to exploit—including through talent recruitment programs, illicit technology transfers, and deceptive joint research initiatives.[18] These risks extend beyond academia to early-stage technology companies and defense start-ups, which can lack the resources and awareness to defend against sophisticated foreign espionage and influence operations.[19]

Strengthening research security requires a balanced approach that both preserves the openness vital to US innovation and ensures appropriate protections against malign foreign access. This demands enhanced education, transparent communication, and trusted partnerships between the federal government, research institutions, and industry, as well as improvements in policies, vetting procedures, contractual requirements, and oversight mechanisms.

While the FBI and the DOE lead much of the coordination with civilian research institutions and private-sector entities, the DoD establishes the security standards and approval processes for DoD-funded researchers and institutions. Moreover, the DoD plays a key role in shaping the research security norms and best practices adopted across the broader federal research ecosystem. As dual-use technologies become increasingly central to national defense, safeguarding research programs beyond those directly funded by the DoD is essential. Enhanced interagency collaboration—particularly between the DoD, DOE, FBI, and other relevant departments—is critical to reducing vulnerabilities across the entire research and development enterprise that underpins US national security.

At stake is more than the protection of individual research programs or technologies; it is the safeguarding of the entire US innovation base—which is central to maintaining a long-term strategic and technological advantage. In an era of strategic competition, securing the integrity of the US research enterprise is critical, as this contest is not only about hardware and capabilities, but also about talent, ideas, and innovation itself.

Strengthen public-private and interagency coordination

A final important pillar to achieve homeland defense is a stronger, more institutionalized approach to public-private and interagency collaboration. Much of US critical infrastructure is owned and operated by the private sector. At the same time, responding to modern threats—including cyberattacks, gray-

17. Anna Puglisi, "Testimony before the Senate Committee on Energy and Natural Resources on 'Examining Research Security Risks Posed by Foreign Nationals from Countries of Risk Working at the DOE's National Laboratories and Necessary Mitigation Steps," US Senate, February 20, 2025, https://www.energy.senate.gov/services/files/4FB0285A-55E1-4C2B-88E2-CC475C69FAD5.

18. "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," Senate Committee on Energy and Natural Resources, February 20, 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.

19. John C. Cannon, Richard A. Meserve, and Maria T. Zuber, "Reconsidering Research Security," *Issues in Science and Technology* 4, 2 (2025), https://issues.org/reconsidering-research-security-gannon-meserve-zuber/.

zone threats, and long-range strikes—requires whole-of-government coordination that bridges defense, homeland security, intelligence, law enforcement, and emergency management. The DoD must reinforce these linkages as part of the NDS's homeland defense focus.

Joint homeland defense exercises that simulate complex, multi-domain threats (such as cyberattacks, space-based disruptions, disinformation campaigns, and conventional or nuclear strikes) against defense and civilian infrastructure should be conducted more frequently. These exercises should not be confined to military participation and should include private-sector actors in DoD scenario planning, continuity of operations testing, and red-teaming effort. These collaborations can surface hidden vulnerabilities, improve mutual understanding of interdependencies, and build a shared culture of resilience.

Conclusion

The Trump administration is right to rank homeland defense as one of its top defense priorities. It has the opportunity to make bold investments in the domestic strengths that undergird US national and military power and to address the myriad domestic vulnerabilities facing the United States today.

In today's strategic environment, protecting US citizens requires defending the foundational systems that enable US security, prosperity, and way of life. Energy grids, digital networks, transportation nodes, trusted information, and the US defense industrial base are not peripheral to national defense—they are primary targets in an era of hybrid threats.

As the DoD prepares its NDS, it must adopt a broader and more integrated approach to homeland defense—one that not only considers border security and missile defense, but also includes the resilience of defense critical infrastructure and coordinated responses to gray-zone threats. This comprehensive approach must be accompanied by clear delineation of where the DoD should lead and where, in areas of non-military security, civilian agencies should lead with DoD support. Public trust in the military, a vital national asset, depends on the DoD leading where its capabilities are essential and constitutionally appropriate, and supporting civilian agencies where they hold the mandate and expertise.

The challenge ahead is not only to defend US physical territory, but to defend the systems and institutions that define and sustain US power from external threats—and to invest in cross-domain resilience to ensure that the United States remains both protected and prepared.

Acknowledgements

The authors would like to acknowledge Tom Warrick, director of the Atlantic Council's Future of DHS Project; Trey Herr, director of the Cyber Statecraft Initiative in the Atlantic Council Technology Programs; and Stewart Scott, deputy director of the Cyber Statecraft Initiative, for their comments and feedback. They would also like to thank Mark Massa, deputy director for strategic forces policy of *Forward* Defense, for his input on the missile-defense section.

Author biographies

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. Originally from the United Kingdom, she previously worked in the UK Parliament on NATO and European security and defense issues. She received her bachelor's degree from the London School of Economics and her master's degree from Georgetown University.

Amy Cowley is a program assistant in the Atlantic Council's *Forward* Defense program housed within the Scowcroft Center for Strategy and Security. She holds a master's degree in international affairs from George Washington University and a bachelor's degree from Utah State University.