Statement before the House Permanent Select Committee on Intelligence

"Persistent Competition and Legacy Architecture"

A Testimony by:

Seth G. Jones
President, Defense and Security Department,
Center for Strategic and International Studies

September 2, 2026

Chairman Crawford, Ranking Member Himes, and distinguished members of the Committee, thank you for the opportunity to testify before the House Permanent Select Committee on Intelligence on the subject of "Persistent Competition and Legacy Architecture." Thank you also for the publication of *Review of the 9/11 Commission Report*, which was released on August 31, 2026.[1] CSIS does not take policy positions. The views expressed in this testimony are my own and do not necessarily reflect those of my employer.

Americans have felt remarkably safe at home from foreign enemies, particularly since the United States became a superpower after World War II. Even after the 9/11 terrorist attacks, only 19 percent of Americans expressed concern about foreign threats, according to a survey by the Chicago Council on Global Affairs.[2] The U.S. homeland is protected by the Atlantic and Pacific Oceans, as well as relatively friendly neighbors to the north and south. The U.S.'s nuclear arsenal has also been a strong deterrent against would-be attackers, including the Soviet Union during the Cold War. The United States arguably became even more secure after the Cold War during the "unipolar moment" because it far surpassed every other country in military, economic, and technological power.[3] In 2005, The United States accounted for roughly half of all global military spending—nearly as much as the rest of the world combined.[4]

Today, however, the U.S. homeland is more vulnerable than it has ever been in recent times from state and non-state adversaries. China, Russia, and North Korea have significantly advanced their conventional and nuclear capabilities to strike the U.S. homeland from the air, sea, land, space, and cyber domains—and U.S. defenses have not kept pace. Some wargames and tabletop exercises of a U.S.-China conflict now include Chinese missile and drone strikes against U.S. military bases and critical infrastructure in the homeland, along with cyber and space-based attacks.

In addition, a major evolution in technology and tactics have increased the threat of subversion and gray zone attacks in the U.S. homeland. Drones can strike almost any target in the United States, as Ukraine's Operation Spiderweb demonstrated. State and non-state actors are building drones with longer ranges, higher payloads, more autonomy, a greater ability to evade countermeasures, and AI that allows for swarming—bad news for U.S. critical infrastructure, military bases, and even sports stadiums and outdoor concert venues. Generative and agentic AI allow state and non-state adversaries to conduct offensive cyber operations that can destroy or

---

[1] House Permanent Select Committee on Intelligence, *Review of the 9/11 Commission Report* (Washington: U.S. House of Representatives, August 31, 2026), https://docs.house.gov/meetings/IG/IG00/20260831/119513/HRPT-119-1.pdf.

[2] Lama El Baz and Jinwan Park, *Americans More Concerned about Threats at Home Than Abroad* (Chicago: Chicago Council on Global Affairs, January 30, 2024), https://globalaffairs.org/research/public-opinion-survey/americans-more-concerned-about-threats-home-abroad.

[3] See, for example, Stephen G. Brooks and William C. Wohlforth, *World Out of Balance: International Relations and the Challenge of American Primacy* (Princeton, NJ: Princeton University Press, 2008). On the unipolar moment see Charles Krauthammer, "The Unipolar Moment," *Foreign Affairs*, Vol. 70, No. 1, 1990, https://www.foreignaffairs.com/articles/1990-01-01/unipolar-moment.

[4] Stockholm International Peace Research Institute, *SIPRI Yearbook 2006: Armaments, Disarmament and International Security* (Stockholm: Stockholm International Peace Research Institute, 2006), https://www.sipri.org/yearbook/2006/08#:~:text=The%20USA%20is%20responsible%20for%2048%20per,and%20Rita%20also%20played%20an%20important%20role.

damage critical infrastructure, and advances in AI let adversaries conduct more effective disinformation campaigns to inflame public opinion and sow discord.

The United States is not prepared for this end of sanctuary and, as 9/11 showed, the psychological, strategic, and political consequences of a homeland attack are incalculably high. U.S. air and missile defenses have gaps, domestic laws and policies are antiquated in protecting against drone attacks, critical infrastructure is vulnerable to advanced cyberattacks, and federal, state, and local entities in the United States are unprepared and uncoordinated for these new threats.

The Vanishing Moat

The U.S. homeland has been relatively secure from foreign adversaries since at least World War II for several reasons. The first is geography. The United States has benefited from two major bodies of water to its east and west—the Atlantic and Pacific Oceans—and relatively benign neighbors to its north and south.

Second is the U.S.'s military power, including its nuclear capabilities. The United States has been a formidable superpower for over eight decades, giving the military the ability to respond to attacks with devastating force. The U.S.'s nuclear arsenal, including its survivable second-strike nuclear capability, has strengthened deterrence. As U.S. President Dwight D. Eisenhower argued, "We now have a broadly based and efficient defensive strength, including a great deterrent power, which is, for the present, our main guarantee against war … Military power serves the cause of security by making prohibitive the cost of any aggressive attack."[5]

Third, U.S. security measures after 9/11 helped protect the homeland from the main threat at the time—terrorism. The USA Patriot Act and subsequent steps increased the ability of U.S. agencies to collect intelligence at home and abroad. U.S. policymakers created the Department of Homeland Security, Office of the Director of National Intelligence, and National Counterterrorism Center to better defend the homeland and share information across multiple agencies against terrorist threats. The United States also expanded Joint Terrorism Task Forces and Fusions Centers to coordinate intelligence across federal, state, and local agencies and target terrorists that were plotting attacks against the homeland.

While essential at the time to deal with the threat of terrorism, the United States is in a new era with evolving threats. Geography is no longer a guarantee of security, nor is U.S. conventional and nuclear might a deterrent against conventional or subversive attacks. In addition, the U.S.'s post-9/11 architecture, which was designed to protect the homeland from terrorists, is largely obsolete.

The Erosion of Conventional and Nuclear Deterrence

China, Russia, and North Korea have significantly improved their conventional and nuclear capabilities to strike the U.S. homeland. China possesses a growing arsenal of land-based

[5] Dwight D. Eisenhower, "Annual Message to the Congress on the State of the Union," January 9, 1958, https://www.presidency.ucsb.edu/documents/annual-message-the-congress-the-state-the-union-10.

intercontinental ballistic missiles, such as the DF-41, which can hit targets across the United States; sea-based submarine-launched ballistic missiles, such as the JL-3, which can be launched from the PLA Navy's nuclear powered submarines off the west or east coasts of the United States; and aircraft, such as the H-6N bomber, that can launch land-attack cruise missiles and air-launched ballistic missiles against the U.S. homeland. According to one Chinese analysis, a possible objective of China in a war would be to "damage and attack key enemy strategic passages and lines of communication and conduct long-range precision strikes against the enemy's strategic overseas bases and strategic targets in its own territory, alone or jointly with other services."[6]

Russia possesses a wide range of land-based intercontinental ballistic missiles, such as the RS-28 Sarmat and RS-24 Yars, capable of hitting the U.S. homeland; submarine-launched ballistic missiles, such as the Bulava, that can strike the continental United States from the Arctic or Pacific; and Kh-101 and Kh-102 air-launched cruise missiles. Finally, North Korea has intercontinental ballistic missiles, such as the Hwasong-18 and Hwasong-19, capable of hitting the U.S. homeland.

To complicate matters, the U.S. homeland faces a growing threat from space-based systems. China can strike targets in the U.S. homeland using a Fractional Orbital Bombardment System, which it can pair with a hypersonic glide vehicle. This system places a warhead into low Earth orbit, allowing it to approach the U.S. homeland from unpredictable vectors—such as the south—and bypass traditional northern-facing early warning radar and missile defense networks. The Chinese government is likely conducting research on orbital strike weapons, which are projectiles launched from space that can hit the U.S. homeland or other targets on Earth.

China has also developed an array of direct-ascent anti-satellite weapons, directed energy weapons, and electronic warfare systems designed to target U.S. satellites in low Earth orbit and geosynchronous Earth orbit. Space-based attacks could disrupt critical infrastructure and daily life in the U.S. homeland, including degrading GPS and navigation, grounding commercial flights, and disrupting logistics networks that rely on satellite tracking for freight. Russia is developing a nuclear anti-satellite weapon that, if deployed and detonated, could degrade or destroy satellites in its path and within the same orbital region, seriously disrupting activity in the U.S. homeland. Russia continues to develop counterspace weapons and other capabilities that could severely undermine U.S. military command, disrupt missile warning and missile tracking networks, and paralyze GPS-dependent infrastructure such as financial transactions, power grids, and cellular communications.

In addition to these capabilities, conventional attacks against nuclear-armed states have become more common. During the Cold War, the U.S.'s nuclear arsenal was a deterrent against Soviet conventional and nuclear attack against the homeland. But not anymore. Just look at recent wars in the Middle East and Europe. Iran and its partner forces have launched thousands of missiles, drones, and other stand-off weapons against Tel Aviv, Jerusalem, Haifa and other Israeli cities. Ukraine has ramped up attacks against nuclear-armed Russia by orchestrating thousands of strikes against Russian energy infrastructure, industrial base targets, logistics, and

[6] Quoted in Ryan D. Martinson, *On the PLAN's "Core Operational Capabilities"* (Newport, RI: China Maritime Studies Institute, U.S. Naval War College, 2024), https://digital-commons.usnwc.edu/cmsi-notes/9.

military bases. Russian cities like Moscow, St. Petersburg, and other Russian cities have come under attack.[7] In both cases, Israel and Russia's nuclear weapons failed to deter conventional attacks against their homelands, and advanced air and missile defense systems have struggled to stop incoming drones and missiles.

The implication is clear: the U.S.'s nuclear arsenal is unlikely to deter conventional strikes against the homeland. Even more concerning, the U.S.'s air and missile defense systems are porous. U.S. defense systems are unable to protect against large-scale, sophisticated intercontinental ballistic missiles from China or Russia using advanced penetration aids or hypersonic glide vehicles. The war with Iran has created additional problems for U.S. homeland defense by reducing the U.S.'s global supply of THAAD and Patriot interceptors. Both are essential for ballistic missile defense. In addition, homeland defense against land-attack cruise missiles launched from submarines or standoff bombers remains porous because of terrain-masking and low-altitude flight paths.

To highlight the problem, I have conducted several tabletop exercises with homeland security professionals that include scenarios in which a Chinese blockade of Taiwan escalates to a broader U.S. China war. In some instances, the United States struck military targets on the Chinese mainland that had attacked U.S. air, sea, and ground forces. The PLA responded by striking military bases and critical infrastructure targets in Hawaii, California, Washington, and other U.S. states with missiles and drones, including ballistic missiles launched from nuclear-powered submarines in the Pacific Ocean. At the same time, China conducted a series of offensive cyberattacks against U.S. military targets and critical infrastructure, such as electricity grids and water. China also conducted an aggressive disinformation campaign using agentic AI on social media platforms, which blamed the United States for starting the war. CSIS has also conducted a range of tabletop exercises, called Red Kraken, with members of Congress to examine Chinese offensive cyber operations that leverage AI.[8]

While these are only tabletop exercises, they illustrate the danger of escalation in a U.S.-China war. They also highlight how woefully unprepared the U.S. homeland is for external attack. U.S. bases and critical infrastructure lack sufficient active defenses, such as air defense systems that could identify, shoot down, and otherwise disrupt incoming Chinese missiles and drones. In addition, the United States lacks passive defenses, such as underground or hardened command-and-control centers, ammunition and fuel depots, and arms production factories.

Subversion at Scale

The introduction of new technologies and tactics have also increased the threat of subversion to the U.S. homeland.[9] State and non-state actors have long used subversion—also

[7] Seth G. Jones and Riley McCabe, *Russian Blood and Treasure: The Ballooning Costs of Putin's War* (Washington, DC: Center for Strategic and International Studies, July 2026), https://www.csis.org/analysis/russian-blood-and-treasure-ballooning-costs-putins-war.
[8] Benjamin Jensen and Emily Harding, "Red Kraken: The Coming Age of Agentic Cyber Strategy," Center for Strategic and International Studies, July 28, 2026, https://www.csis.org/analysis/red-kraken-coming-age-agentic-cyber-strategy.
[9] See, for example, Jill Kastner and William C. Wohlforth, "A Measure Short of War: The Return of Great-Power Subversion," *Foreign Affairs*, Vol. 100, No. 4, July/August 2021,

called irregular warfare, gray zone activity, and political warfare—to weaken their adversaries below the threshold of conventional warfare. These tools have traditionally included violence, physical sabotage against critical infrastructure, disinformation, and offensive cyber operations. While subversion is as old as warfare itself, new technologies and tactics are threatening the U.S. homeland in novel ways.

One example is the proliferation of drones, many of which are commercially available and increasingly using AI. Technological advances may soon allow state and non-state adversaries to fly drones in swarms, which involve multiple uncrewed systems that operate together as a single, coordinated unit. The war in Ukraine is a testing ground for drones, and such adversaries as China, Russia, and Iran are ramping up drone production and use. Drones can be deadly if used against the U.S. homeland. During Operation Spider Web in 2025, the Security Services of Ukraine, or SBU, covertly brought into Russia over a hundred drones inside of vehicles and damaged approximately one third of Russia's active bomber fleet.[10] The targets included Russian Tu-95 strategic bombers, Tu-22M3 long-range bombers, Tu-160 strategic bombers, and A-50 early warning and control aircraft deep inside Russian territory.

The U.S. homeland is highly vulnerable to this type of attack. U.S. military bases and other critical infrastructure are already experiencing a high volume of unauthorized drone incursions, along with outdoor concerts, sports stadiums, and other public venues. There are hundreds of unauthorized drone intrusions around U.S. military bases in the homeland each year.[11]

In addition, advances in agentic AI give state and non-state actors a far greater ability to attack cyber defenses and target critical infrastructure. Agentic AI allows bad actors to conduct offensive operations at mass and scale in ways that have never been possible before. While the impact of cyberattacks is often overhyped, cyber weapons can be used in concert with conventional and sabotage operations. Countries like China have already started upping their game. As part of Volt Typhoon, China penetrated critical networks in the United States to conduct sabotage in case of a U.S.-China crisis. Some U.S. cyber defenses are shockingly poor. Too many municipalities in the United States lack basic cyber defense, and agentic AI is increasing the ease of conducting these types of attacks.

Finally, advances in AI allow state and non-state actors to conduct stepped-up disinformation campaigns in the United States to sow discord, inflame public opinion, and

---

https://www.foreignaffairs.com/articles/world/2021-06-22/measure-short-war; and Seth G. Jones, *Three Dangerous Men: Russia, China, Iran and the Rise of Irregular Warfare* (New York: W.W. Norton, 2021).

[10] James Marson, Jane Lytvynenko, and Serhii Bosak, "Inside Ukraine's Daring 'Operation Spiderweb' Attack on Russia," *Wall Street Journal*, December 9, 2025, https://www.wsj.com/world/europe/ukraine-russia-drone-attack-operation-spiderweb-24d821ab; and Masao Dahlgren and Lachlan MacKenzie, *Ukraine's Drone Swarms Are Destroying Russian Nuclear Bombers. What Happens Now?* (Washington: Center for Strategic and International Studies, June 2025), https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now.

[11] Michael Marrow, "With Daily Drone Incursions Over Bases, NORTHCOM Takes Aim Through Falcon Peak," *Breaking Defense*, October 10, 2025, https://breakingdefense.com/2025/10/drone-incursions-us-military-falcon-peak-2025-cuas/#:~:text=%E2%80%9CWe're%20between%20%5Babout%5D%20one%20and%20two%20incursions,roughly%20the%20same%20period%20the%20following%20year.

influence elections. The United States has always had an open democratic system, and political polarization is not new. But generative AI tools and a growing social media space have drastically lowered the costs of production and raised the list of potential targets. Large language models allow adversaries—from China and Russia to terrorists—to generate sophisticated video and audio content and amplify divisive domestic content.[12] In addition, agentic AI allows adversaries to execute actions on a scale that has been impossible. In 2026, China used AI to generate social media posts claiming that data center construction in the U.S. homeland was causing electricity spikes for American families.[13]

Fortifying the Homeland

The U.S. homeland is increasingly vulnerable. Moving forward, the United States needs to urgently develop capabilities, policies, laws, and structures to better protect the homeland. The following suggestions cut across multiple Congressional committees and would help prepare the United States "left of boom."

Active and Passive Defenses: One important step to protecting the homeland is to increase active defenses around critical infrastructure. Examples include upper-range systems for ballistic missiles, medium-range systems for cruise missiles, and short-range systems for drones. Also important is ramping up passive defenses, such as digging underground facilities for vital infrastructure and placing high-density and layered concrete barriers around ground systems, power-generation units, ammunition storage facilities, and barracks. Since it would be exorbitantly expensive to protect everything in the homeland, the initial goal should be beefing up defenses at critical bases and infrastructure that countries like China could target in a conflict. Examples include military command-and-control facilities, bomber bases, nuclear sites, air and missile defense systems, and naval bases in such states as Hawaii, California, Washington, Missouri, Virginia, Alaska, and Florida.

Golden Dome, the Trump administration's proposed national missile defense system, can play an important role in homeland defense. However, the near-term challenge is not the technology of Golden Dome—but the integration and organization of existing systems, which should be the focus. The U.S. military already has missile warning satellites, a global network of radars and sensors, ground-based interceptors in California and Alaska, and other federal, state, local, and commercial systems. Developing Golden Dome into an operational network that can track threats and coordinate responses in real time requires new operational concepts and clear authorities across military organizations and federal agencies to stitch together U.S. sensors and systems that already exist.

Counter-Drone Defenses: Drones present a particularly thorny problem for homeland security. Commanders at military bases and personnel protecting critical infrastructure often do not have the legal authority to destroy or degrade drones that illegally fly into their air space.

---

[12] Daniel Byman and V.S. Subrahmanian, *Artificial Intelligence and the Future of Terrorism* (Washington: Center for Strategic and International Studies, July 2026), https://www.csis.org/analysis/artificial-intelligence-and-future-terrorism.

[13] OpenAI, "PRC-Linked Influence Operations Are Targeting AI Debates in the US: June 2026 Threat Report," June 10, 2026, https://openai.com/index/prc-linked-influence-operations-ai-debates/.

Such legislation as the Safer Skies Act grants state and local agencies—though not private sector entities—a greater ability to detect and track hostile drones. But huge gaps remain. Legislation is needed to allow vetted operators the authority to deploy and use approved counter-drone systems under federal, state, and local law enforcement supervision. There are some risks, including the accidental jamming or shooting down of civilian aircraft. Mitigating these risks makes it essential to increase the number of state and local personnel trained at the National Counter-UAS Training Center in Huntsville, Alabama.

The Office of the Director of National Intelligence (ODNI): One of the most significant recommendations of the 9/11 Commission was to create an ODNI to coordinate and improve accountability across a stove-piped U.S. intelligence community. But 25 years later, ODNI has failed to effectively achieve many of these results. Instead, it has added another layer of bureaucracy with ambiguous authority, little budget control or coordination, and a tendency to complicate rather than improve intelligence sharing. As this Committee's publication August 2026 *Review of the 9/11 Commission Report* concluded, ODNI has also faced "bureaucratic bloat and inefficiencies."[14] Congress should consider establishing a National Commission to review the ODNI based on the evolving national security landscape and policy needs. Should ODNI evolve into a small, professional intelligence-management office, perhaps akin to the Office of Management and Budget? Should it be significantly evolved in other ways? These are difficult—but momentous—questions at the very moment that threats to the U.S. homeland are at an all-time high.

National Counterintelligence Agency: Intelligence-sharing between federal, state, and local intelligence agencies improved after 9/11 to counter terrorists, thanks in part because of such organizations as the National Counterterrorism Center. But it is woeful in dealing with today and tomorrow's threats. Terrorism is no longer the main threat to the homeland. Congress and the executive branch should consider establishing a National Counterintelligence Agency—an evolution of the National Counterintelligence and Security Center—to be the interagency hub for counterintelligence threats to the United States, akin to the National Counterterrorism Center. It would conduct threat analysis, information sharing, and strategic planning across the government to deal with state-based threats. As part of its duties, other U.S. intelligence community organizations should be required to share counterintelligence information with this agency.

Joint Terrorism Task Forces (JTTFs) and Fusion Centers: Congress should consider broadening the mandate for JTTFs and Fusion Centers to focus on state-sponsored threats. Expanding the formal charter will allow local agencies to tackle illicit corporate and criminal activities that are below the threshold for federal investigations, but are critical components of Chinese, Russian, and other foreign intelligence operations. There is also a national shortage at every level for sworn law enforcement personnel that are responsible for homeland security threats. To combat this, many agencies have employed civilians to fill the gap. Congress should consider supporting a grant-funded program to embed civilian Intelligence Support Officers into JTTFs and Fusion Centers, which would allow them to bridge the gap between local investigative data and federal intelligence feeds.

[14] House Permanent Select Committee on Intelligence, *Review of the 9/11 Commission Report*, 9.

A More Resilient Society

While these stepped-up defensive measures are necessary, the United States should respond forcefully to attacks against the homeland. Offense is also important. As President George Washington wrote, "offensive operations, often times, is the surest, if not the only … means of defence."[15]

Finally, the end of sanctuary requires a fundamental shift in mindset. At the core of a safer U.S. homeland is a more educated and resilient population. Resilience is a population's ability to resist and recover from external threats. Israel, Ukraine, Finland, and other countries in dangerous neighborhoods have long traditions of developing policies and plans to harden critical infrastructure, closely collaborate with the private sector, adapt laws, and communicate with the public. It is time for the United States to follow suit. As President Ronald Reagan remarked, "I have lived through two world wars. I saw the American people rise to meet these crises, and I have faith in their willingness to come to their nation's defense in the future. But it's far better to prevent a crisis than to have to face it unprepared at the last moment. That's why we have an overriding moral obligation to invest now … in restoring America's strength to keep the peace and preserve our freedom."[16] America is up to the challenge.

[15] W.W. Abbot, ed., *The Papers of George Washington: Retirement Series volume 4, April – December 1799* (Charlottesville and London: University Press of Virginia, 1999).
[16] Ronald Reagan, "Radio Address to the Nation on Defense Spending," February 19, 1983, https://www.presidency.ucsb.edu/documents/radio-address-the-nation-defense-spending.