Statement before the

House Permanent Select Committee on Intelligence

"25 Years After 9/11: Confronting the Next Generation of Threats"

A Testimony by:

Seth G. Jones

President, Defense and Security Department, Center for Strategic and International Studies

July 21, 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 "25 Years After 9/11: Confronting the Next Generation of Threats." CSIS does not take policy positions. The views expressed in this testimony are my own and do not necessarily reflect those of my employer.

In the aftermath of the terrorist attacks on September 11, 2001, the 9/11 Commission was invaluable in identifying the nature of the evolving terrorist threat, U.S. intelligence gaps, and policy recommendations. As the final 9/11 report concluded, "Countering terrorism has become, beyond any doubt, the top national security priority for the United States. This shift has occurred with the full support of the Congress, both major political parties, the media, and the American people. The nation has committed enormous resources to national security and to countering terrorism."[1] Yet 25 years later, the international landscape, the threats to the United States, and intelligence challenges have dramatically evolved.

Today, the United States and its allies face a serious and growing threat at home and abroad from an authoritarian axis led by China that also includes countries such as Russia, Iran, and North Korea. The number of democratic and free countries in the world has declined for an astounding 20 consecutive years, highlighting the dangerous march of authoritarianism.[2] China and the Chinese Communist Party (CCP) present the most serious threat to the United States, including to the U.S. homeland. Beijing is building conventional capabilities in all the domains of warfare, a growing arsenal of nuclear weapons, and a range of irregular and gray zone capabilities in such areas as offensive cyber operations, influence operations, covert action, subversion, and economic coercion. Russia, Iran, North Korea, terrorist groups, and other state and non-state actors also present threats to the United States.

As this testimony argues, the U.S. homeland is increasingly under threat from state and non-state actors. While the U.S.'s geographic position between two oceans was once a major source of security, the United States is now witnessing an end of this sanctuary and U.S. intelligence agencies need to adapt. First, U.S. adversaries—such as China, Russia, and North Korea—have significantly advanced their conventional and nuclear capabilities to strike the U.S. homeland. In addition, nuclear weapons are no longer a deterrent against conventional strikes against the homeland. Both Israeli and Russian cities have been targeted by adversary drones, cruise missiles, and ballistic missiles, even though both countries possess nuclear weapons. Second, there has been a major evolution in irregular and gray zone threats to the U.S. homeland, such as offensive cyber operations, autonomous and AI-enabled unmanned systems, espionage, and AI-enabled influence campaigns on social media. Ukraine's Operation Spider Web was a stark reminder that drones can be used to conduct strikes deep inside an adversary's territory. So was Volt Typhoon, the Chinese cyber campaign that infiltrated U.S. critical infrastructure.

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton, 2004), 361.
[2] Freedom House, *Freedom in the World 2026* (Washington, DC: Freedom House, 2026), 2, https://freedomhouse.org/report/freedom-world/2026/growing-shadow-autocracy.

The rest of this testimony is divided into four sections. The first provides an overview of emerging conventional threats, including China. The second section outlines the threat from irregular and gray zone actions. The third assesses the end of sanctuary and the growing threat to the U.S. homeland. The fourth section provides intelligence recommendations for Congress.

Accelerating Conventional and Nuclear Threats

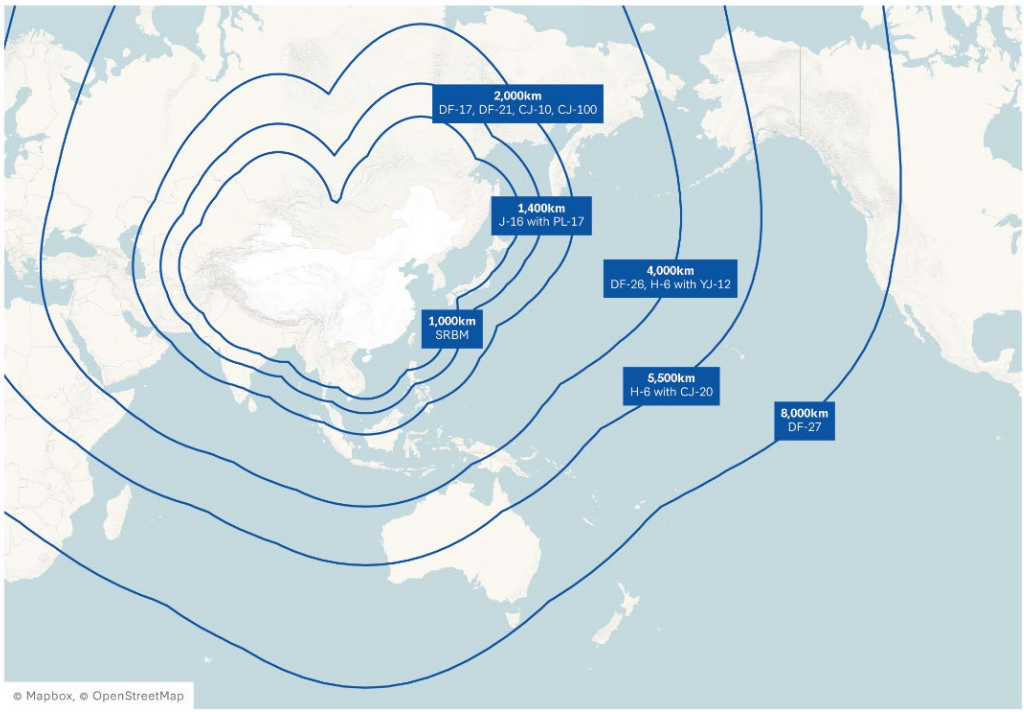
The United States faces an evolving conventional threat from an axis of adversaries. The anchor of the axis is Beijing due to its size and military, economic, and technological power. China has rapidly modernized its military through military-civil fusion in all the major domains of warfare, such as air, maritime, land, space, cyber, and nuclear. The People's Liberation Army (PLA) possesses formidable air and naval power, long-range precision strike systems, and advanced space and cyber capabilities that can threaten the United States. China's defense industrial base is producing substantial numbers of ships, aircraft, tanks, and other military systems at an alarming rate, and China is devoting significant resources to AI, quantum, and other technologies with defense applications. The U.S. military has lost "overmatch"—the ability to militarily overwhelm an adversary—in a war against China.[3]

U.S. and allied bases, surface vessels, and aircraft operating in the first and increasingly second island chains—the latter of which extends from Japan south through Guam and New Guinea—are highly vulnerable to Chinese cruise, ballistic, and hypersonic missiles. U.S. forces are still not sufficiently dispersed throughout the Pacific and lack underground fuel bladders, underground storage bunkers for munitions and other materiel, and enough area and point defenses. Iranian attacks against U.S. facilities in the Middle East during Operation Epic Fury should be a wake-up call about the nature of the threat, though China has significantly greater capabilities than Iran.

Russia, North Korea, and Iran also possess significant conventional capabilities. Russia continues to build a range of land-based intercontinental ballistic missiles, submarine-launched ballistic missiles, and cruise missiles. North Korea possesses a growing arsenal of intercontinental ballistic missiles, short- and medium-range ballistic missiles, cruise missiles, and ballistic missiles capable of carrying hypersonic glide vehicles. Collectively, these North Korean systems have greater range, mobility, survivability, and launch secrecy, which threaten the United States and its regional allies such as South Korea and Japan. As demonstrated during Operation Epic Fury, Iran possesses a range of missiles and drones capable of hitting U.S. and allied target across the Middle East and beyond.

[3] On overmatch, see the work of David Ochmanek, such as David A. Ochmanek et al., *Inflection Point: How to Reverse the Erosion of U.S. and Allied Military Power and Influence* (Santa Monica, CA: RAND Corporation, 2023), 21, 32, 177, https://www.rand.org/pubs/research_reports/RRA2555-1.html; and Octavian Manea, "Interview with David Ochmanek," Small Wars Journal, March 11, 2025, https://smallwarsjournal.com/2025/03/11/interview-with-david-ochmanek/.

Figure 1: China's Conventional Strike Capabilities and Ranges



Source: U.S. Department of Defense, Military and Security Developments Involving the People's Republic of China 2025 (Washington, DC: DOD, 2025), 79, https://media.defense.gov/2025/-Dec/23/2003849070/-1/-1/1/ANNU-AL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF.

CSIS

As discussed later in this testimony, China, Russia, and North Korea's expanding conventional and nuclear capabilities increasingly threaten the United States—including the U.S. homeland—in ways that did not exist in the aftermath of 9/11.

Evolving Irregular and Gray Zone Threats

The United States also faces an evolving set of irregular—or gray zone—threats. Actions below the threshold of conventional warfare have long been an important component of statecraft.[4] U.S. military doctrine refers to these types of actions as "irregular warfare."[5] Others have used such terms as gray zone activity, political warfare, asymmetric conflict, and low intensity conflict.[6] Regardless of the term, the main components include:

[4] See, for example, Max Boot, *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present* (New York: W.W. Norton, 2013).
[5] On irregular warfare see, for example, Seth G. Jones, *Three Dangerous Men: Russia, China, Iran and the Rise of Irregular Warfare* (New York: W.W. Norton, 2021).
[6] See, for example, Hal Brands, *The Twilight Struggle: What the Cold War Teaches Us about Great-Power Rivalry Today* (New Haven: Yale University Press, 2022); Kathleen H. Hicks, et. al., *By Other Means, Part I: Campaigning in the Gray Zone* (Washington, DC: Center for Strategic and International Studies, 2019); Tim Weiner, *The Folly and the Glory: America, Russia, and Political Warfare 1945-2020* (New York: Henry Holt, 2020); Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and

- Information and influence operations, including psychological operations and propaganda.
- Offensive cyber operations and electronic warfare.
- Support to state and non-state partners, such as guerrillas and proxy forces.
- Covert and clandestine actions by intelligence and special operations forces, including sabotage and subversion.
- Economic coercion.[7]

Countries carry out these types of operations for several reasons. First, they allow military and intelligence agencies to conduct coercive activities below a level that is likely to trigger a costly or risky conventional war. Second, irregular and gray zone activity is relatively inexpensive for perpetrators. Unlike conventional war, these activities generally do not require vast sums of money or cause the perpetrator to suffer substantial casualties. Some of these actions—such as offensive cyber and influence operations—can also be done from a state's own territory, a third country, or virtual networks that lie far from the target country. Third, these actions are often deniable and difficult to attribute. Targeted governments are frequently cautious about attributing them because they fear escalation or want to protect intelligence sources and methods.[8] Fourth, actions below the threshold of conflict can impose costs on targeted countries. For example, Russian sabotage operations in Europe have caused hundreds of millions of dollars in damage to undersea cables, rail infrastructure, pipelines, and other infrastructure. Defensive measures to protect physical and cyber infrastructure can also be expensive.[9]

China: The most significant long-term threat to the United States likely comes from China, which uses a wide range of tools below the threshold of armed conflict to expand the influence of the CCP and weaken the United States. While some of these Chinese actions are overt, many are designed to be covert and deniable. The U.S. public and other international audiences are often unaware of the nature and scope of these activities, including those that target companies, government agencies, universities, news media, digital platforms, and other organizations. China's activities are wide ranging and include:

- *Intelligence Operations:* China's intelligence services, such as the Ministry of State Security (MSS) and Ministry of Public Security (MPS), are engaged in extensive human

---

Giroux, 2020); Linda Robinson, et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND 2018); Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," Prism, Vol. 7, No. 4, 2018, pp. 31-47; George F. Kennan, "Organizing Political Warfare," April 30, 1948, History and Public Policy Program Digital Archive; Hal Brands and Toshi Yoshihara, "How to Wage Political Warfare," *National Interest*, December 16, 2018.

[7] See, for example, Jones, *Three Dangerous Men*; Hicks, *By Other Means*; Robinson, *Modern Political Warfare*.

[8] Charlie Edwards and Nate Seidenstein, *The Scale of Russian Sabotage Operations against Europe's Critical Infrastructure* (London: International Institute for Strategic Studies, August 2025), 4.

[9] Edwards and Seidenstein, *The Scale of Russian Sabotage Operations against Europe's Critical Infrastructure*; Carri Ginter and Marcus Niin, "We Are Advising Finnish and Estonian Energy Companies on Obtaining Insurance Compensation as a Result of the Damage to the Balticconnector Gas Pipeline," Sorainen, July 25, 2025, https://www.sorainen.com/deals/we-are-advising-finnish-and-estonian-energy-companies-on-obtaining-insurance-compensation-as-a-result-of-the-damage-to-the-balticconnector-gas-pipeline/.

intelligence, signals intelligence, and other types of intelligence collection as part of irregular warfare and gray zone operations—including intimidating Chinese diaspora in the United States. Chinese intelligence operations are not just pervasive, but they are used to plan and execute all of China's other irregular warfare activities. The 2026 conviction of John Rogers, a former senior adviser for the Federal Reserve Board of Governors who collaborated with Chinese intelligence, is only the most recent example of the Chinese intelligence threat to the United States.[10] In addition, China is also expanding its intelligence collection overseas against the United States, such as building signals intelligence platforms in such countries as Cuba and constructing space ground stations in such countries as Argentina.[11]

- *Cyber Operations:* Chinese organizations, including units within the People's Liberation Army (PLA), are involved in aggressive cyber campaigns against U.S. companies, universities, government agencies, media, think tanks, nongovernmental organizations, and other targets. These efforts are designed to help China leapfrog ahead of the West by skipping the extensive and time-consuming research and development phases for new technologies. China's cyber operations are also intended to influence foreign and domestic audiences, conduct long-term surveillance and intelligence gathering (such as Salt Typhoon), and assist with offensive military campaigns (such as Volt Typhoon).

- *Information and Disinformation Operations:* China is engaged in extensive information and disinformation activities overseas—including in the U.S. homeland—designed to influence decisionmaking and popular support to gain a competitive advantage. Beijing seeks to tightly control the image of China abroad, including influencing companies, organizations, and individuals that criticize China, from the National Basketball Association to Hollywood studios.

- *United Front Work:* China is involved in aggressive efforts to extend its reach overseas through united front work, which involves activity to protect and bolster the image of China and the CCP. United front work includes activities conducted in support of China's soft-power agenda that seek to influence individuals who are positioned to amplify China's preferred messaging on political, economic, and academic issues.

- *Irregular Military Actions:* The PLA Navy, PLA Air Force, PLA Rocket Force, People's Armed Forces Maritime Militia, Coast Guard, research organizations, and private security companies linked to China are involved in widespread efforts to expand Chinese influence below the threshold of armed conflict. Chinese organizations are involved in

[10] U.S. Department of Justice, "Former Adviser to Federal Reserve Board of Governors Sentenced to Federal Prison Term," July 15, 2026, https://www.justice.gov/opa/pr/former-adviser-federal-reserve-board-governors-sentenced-federal-prison-term.
[11] Matthew P. Funaiole, Brian Hart, Aidan Powers-Riggs, Joseph S. Bermudez, Jr., "At the Doorstep: A Snapshot of New Activity at Cuban Spy Sites," Center for Strategic and International Studies, May 6, 2025, https://features.csis.org/hiddenreach/snapshots/cuba-china-cdaa-base/; and Matthew P. Funaiole, Dana Kim, Brian Hart, Joseph S. Bermudez Jr., "Eyes on the Skies: China's Growing Space Footprint in South America," Center for Strategic and International Studies, October 4, 2022, https://features.csis.org/hiddenreach/china-ground-stations-space/.

near-seas activities (which focus on securing Chinese interests around such areas as the South and East China Seas) and far-seas activities (which are global in scope).

- *Economic Coercion:* China is increasingly engaged in the threat or imposition of economic costs and inducements to influence decision-making and popular support across the globe to gain a competitive advantage. There has been considerable focus on the Belt and Road Initiative as part of a broader effort to influence foreign governments. Another concerning Chinese initiative is the Digital Silk Road, which aims to spread Chinese influence through telecommunications, e-commerce, hardware, software, big data, artificial intelligence/machine learning, and other digital infrastructure across the globe.

These tools are not mutually exclusive but are overlapping, reinforcing, and occasionally even duplicative and competitive. Multiple organizations are involved, such as the PLA, Ministry of State Security, Ministry of Public Security, United Front Work Department, and Ministry of Foreign Affairs. A wide range of non-state or quasi-state actors are also involved, from hacktivists to private security companies.

Figure 2: Chinese Organizations Involved in Irregular and Gray Zone Activity

ORGANIZATION	EXAMPLES OF ACTIVITY
China Coast Guard	Conducts maritime operations, including around disputed territory.
People's Armed Forces Maritime Militia	Conducts maritime operations, including around disputed territory.
People's Armed Police	Conducts internal security, riot control, disaster response, and maritime rights protection.
People's Liberation Army	
— *PLA Air Force*	Conducts air operations—including with unmanned aircraft systems (UASs)—in disputed territories and harasses specific commercial activities.
— *PLA Army*	Orchestrates land-based operations to collect intelligence and conduct subversive activities.
— *PLA Navy*	Harasses and disrupts specific commercial activities in disputed territories and sails into contested territory in the East China Sea, Senkaku Islands, and other areas.
— *PLA Rocket Force*	Orchestrates land-based operations to collect intelligence and conduct subversive activities.
— *PLA Strategic Support Force*	Conducts offensive cyber operations, intelligence collection, and information operations.
Ministry of Foreign Affairs	Orchestrates information, disinformation, and misinformation activity and engages in subversive efforts to expand Chinese influence and power.
Ministry of Industry and Information Technology	Oversees China's network infrastructure and coordinates with technology companies and universities.
Ministry of Public Security	Monitors dissidents and foreigners, particularly those located within China.
Ministry of State Security	Conducts intelligence operations (including against members of the Chinese diaspora) through human intelligence, signals intelligence, and other means; oversees counterintelligence; conducts cyber operations, including offensive cyber operations; and orchestrates a range of subversive activity.
United Front Work Department	Conducts information, disinformation, and misinformation activity to protect and bolster the image of China and the CCP, including by pressuring individuals and organizations overseas.

China has several strategic goals in conducting irregular and gray zone activities. The most important is preservation of the CCP's rule. Another is expanding Chinese influence and weakening the United States as part of balance-of-power competition. These goals are in line

with China's national strategy of achieving "the great rejuvenation of the Chinese nation on all fronts."[12]

Russia: Russia (and the Soviet Union before it) have a long tradition of conducting irregular and gray zone activities. During the Cold War, the Soviet Union developed an aggressive campaign to influence populations across the globe in ways that aided Soviet interests and undermined the United States and its allies, which was best captured in the phrase "active measures" (or активные меры).[13] Today, Russian active measures support several types of foreign policy objectives:

- Influence public opinion through psychological operations in Europe, the United States, and other countries to support Russian interests.
- Coerce governments, companies, or individuals to stop taking specific actions, such as curbing military and other assistance to Ukraine.
- Deter countries, companies, or individuals from taking specific actions, such as escalating the type and amount of military aid to Ukraine.
- Deter Russian soldiers, government officials, and citizens from defecting to the West.
- Create fissures between governments, especially between NATO allies.
- Undermine the democratic norms and values that underpin the West.

Today, Russia is involved in a range of aggressive irregular and gray zone activity in the United States, from offensive cyber operations to espionage and disinformation. One of many recent examples is a Russian and Chinese intelligence campaign to spread disinformation on social media platforms about AI data centers in the United States.[14] The Russian government has also conducted a campaign of sabotage and subversion—especially in Europe—designed to target countries, companies, and individuals that have provided support to Ukraine. Led by the Main Intelligence Department, or GRU, Russian attacks have included bombings, drone incursions, sabotage against undersea cables and pipelines, electronic attack, and cyber operations. Russia's strategy has likely been to coerce governments and companies to stop providing assistance to Kyiv, deter Russian soldiers and citizens from defecting to the West, sow fear and division, and undermine public support for the Ukraine war.

Iran: Iran and Iranian-linked groups, such as Lebanese Hezbollah and the Houthis in Yemen, also pose an irregular and gray zone threat to the United States. Ayatollah Khomeini established the Islamic Revolutionary Guard Corps in 1988 to expand and improve Iran's irregular warfare capabilities. The Quds Force ("Quds" is the Farsi word for Jerusalem) became

[12] "Full Text: 2023 New Year Address by President Xi Jinping," Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland, December 31, 2022, http://gb.china-embassy.gov.cn/eng/zgyw/202212/t20221231_10999475.htm.
[13] See, for example, Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999); Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); Soviet Covert Action (the Forgery Offensive): Hearings before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence, U.S. House of Representatives, 96th Cong. (February 1980) (statement of John McMahon, Deputy Director for Operations, Central Intelligence Agency).
[14] Steven Lee Myers and Dustin Volz, "China, Russia and Others Seek to Inflame Debate Over A.I. Data Centers," *New York Times*, July 9, 2026, https://www.nytimes.com/2026/07/09/business/china-russia-ai-data-centers.html.

Iran's elite paramilitary arm, roughly equivalent to a mix of U.S. special operations forces and CIA paramilitary forces. It gathers intelligence, trains and equips partner forces, and conducts assassinations and bombings outside of Iranian territory.[15] The Quds Force and Iranian-linked groups and individuals have plotted numerous attacks and assassinations inside the United States, including against U.S. President Donald Trump, former national security advisor John Bolton, and the Saudi ambassador to the United States.[16] Iran has also engaged in a wide range of other irregular and gray zone activities, such as offensive cyber operations and disinformation campaigns.

Terrorist and Other Threats: The United States faces a significant threat from a range of terrorist groups, criminal organizations, and other non-state actors. Unlike during the period after 9/11, there is no clear paramount threat from a group like al-Qaeda. Instead, the United States faces formal groups, loose networks, and lone actors who are plotting to kill Americans and spread fear in the United States or otherwise threaten important U.S. security interests.[17]

The End of Sanctuary

Based on these threats, the U.S. homeland is more vulnerable than it has ever been, signaling an end of U.S. sanctuary. The homeland has, of course, never been entirely secure. The British burned Washington (including the White House) during the War of 1812, al-Qaeda terrorists attacked the United States on 9/11, and the Soviets posed a serious nuclear threat to the United States during much of the Cold War. The Japanese also struck Pearl Harbor before Hawaii was a state. Nevertheless, the Atlantic and Pacific Oceans have helped insulate the U.S. homeland from external attack, along with relatively friendly neighbors to the north and south. Today, however, threats to the U.S. homeland are greater than they have ever been.

First, U.S. adversaries—such as China, Russia, and North Korea—have significantly advanced their conventional and nuclear capabilities to strike the U.S. homeland. China possesses a growing arsenal of land-based intercontinental ballistic missiles, such as the DF-41, which can hit targets across the continental 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 and can target locations across the U.S. homeland; 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. In addition, Russia possesses a range of land-based intercontinental ballistic missiles, such as the RS-28 Sarmat and RS-24 Yars, capable of hitting the U.S. homeland;

---

[15] Defense Intelligence Agency, *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance* (Washington, DC: U.S. Government Publishing Office, 2019), pp. 57-63.

[16] See, for example, U.S. Department of Justice, "Iranian Intelligence Agent Convicted of Terrorism and Murder for Hire in Connection with Foiled Plot to Assassinate U.S. Politicians and Government Officials," March 6, 2026, https://www.justice.gov/opa/pr/iranian-intelligence-agent-convicted-terrorism-and-murder-hire-connection-foiled-plot; and U.S. Department of Justice, "Member of Iran's Islamic Revolutionary Guard Corps (IRGC) Charged with Plot to Murder the Former National Security Advisor," August 10, 2022, https://www.justice.gov/archives/opa/pr/member-irans-islamic-revolutionary-guard-corps-irgc-charged-plot-murder-former-national.

[17] Alexander Palmer, Daniel Byman, Alexander Margolis, Riley McCabe, and Erin Oppel, *Global Terrorism Threat Assessment 2026* (Washington, DC: Center for Strategic and International Studies, 2026), https://www.csis.org/analysis/global-terrorism-threat-assessment-2026.

submarine-launched ballistic missiles, such as the Bulava, that can strike the continental United States from the Arctic or Pacific; and Kh-101 (conventional) and Kh-102 (nuclear) air-launched cruise missiles that can hit the United States from Russian aircraft. Finally, North Korea has intercontinental ballistic missiles, such as the Hwasong-18 and Hwasong-19, capable of hitting the U.S. homeland.[18]

During the Cold War, the U.S.'s nuclear arsenal was a deterrent against Soviet conventional and nuclear attack, including through the concept of Mutually Assured Destruction. But nuclear weapons are no longer a deterrent to conventional attack. Iran has conducted multiple attacks against nuclear-armed Israel with cruise missiles, ballistic missiles, and drones, as have Iranian partner forces such as Lebanese Hezbollah and the Houthis in Yemen. In addition, Ukraine has ramped up attacks against nuclear-armed Russia by orchestrating a series of short-, medium-, and long-range strikes to disrupt and destroy Russian logistics and supplies. Ukraine has struck several types of Russian targets with conventional weapons:

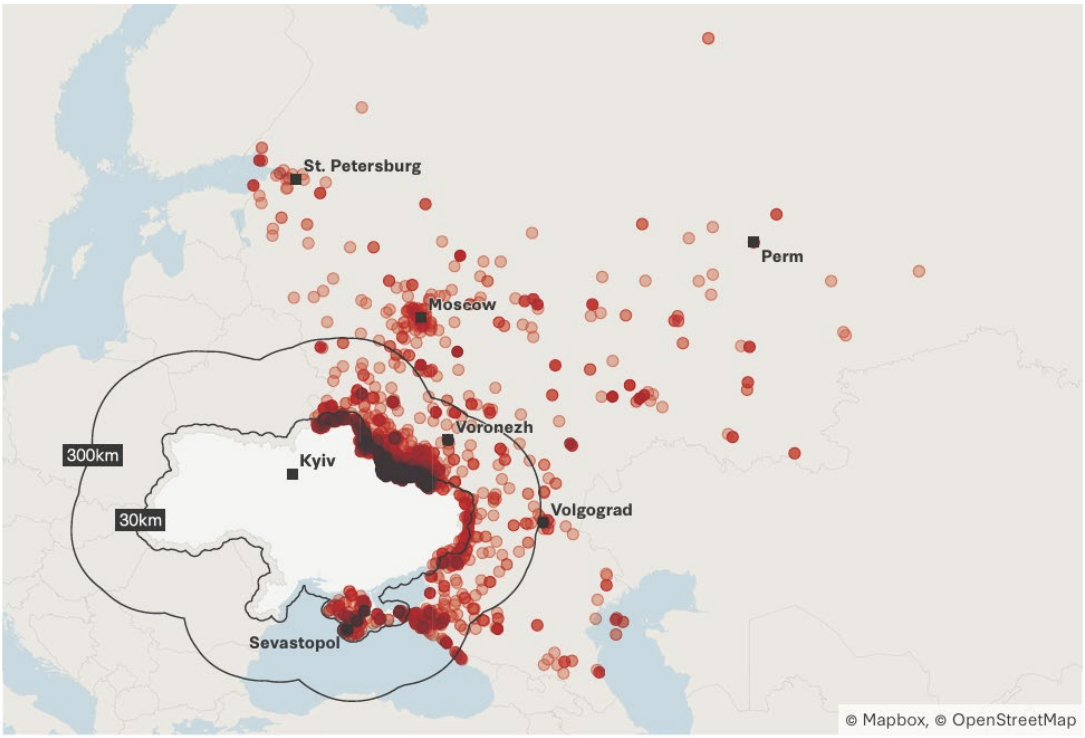
- Energy infrastructure, such as oil refineries, pumping stations, and fuel storage facilities and tankers.
- Industrial base targets, such as missile and drone production facilities, microelectronics plants, and semiconductor plants.
- Logistics targets, such as rail lines, roads, bridges, and munitions storage facilities, as well as vehicles and freight trains transporting military supplies.
- Military bases and other military targets, such as headquarters, command and control facilities, ships, aircraft, radar, air defense systems, drone launch positions, and electronic warfare systems.

As Figure 3 illustrates, Ukraine has conducted long-range strikes (greater than 300 kilometers from Ukrainian territory) against such cities as St. Petersburg and Moscow. Ukraine has also orchestrated medium-range strikes (30–300 kilometers) against targets in Kursk, Kaluga, Belgorod, and other oblasts. Finally, Ukrainian forces have carried out short-range strikes (less than 30 kilometers) against thousands of targets just across the border in Russia and in Russian-controlled areas of Ukraine, such as Crimea.[19]

The implication is clear: the U.S.'s nuclear arsenal is no longer sufficient to deter conventional strikes.

[18] See the overview of Chinese, Russian, and North Korean missiles at "Missiles of the World," Center for Strategic and International Studies, 2026, https://missilethreat.csis.org/missile/.
[19] On the role of strategic bombing, see, for example, Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996).

Figure 3: Location of Ukrainian Strikes in Russia, January 2025–June 2026



Source: CSIS estimates; Armed Conflict Location and Event Data Project (ACLED), https://acleddata.com; and Алеся Соколова, Ксения Сторожева [Alesiya Sokolova, Ksenia Storozheva], Интерактивная карта обстрелов России. Обновление в реальном времени. Военные действия затронули не менее 60 регионов страны [Interactive Map of Strikes in Russia. Updated in Real Time. Strikes Hit at Least 60 Regions], Новая газета Европа [Novaya Gazeta Europe], April 23, 2026, https://novayagazeta.eu/articles/2026/04/23/interaktivnaia-karta-obstrelov-rossii-obnovlenie-v-realnom-vremeni.

Second, there is an increase in irregular and gray zone threats and capabilities from state and non-state actors against the U.S. homeland. One example is the proliferation of commercially available, AI-enabled unmanned systems, which can be weaponized. Both Ukraine and Russia are building drones with longer ranges, higher payloads, a greater ability to evade electronic warfare and countermeasures, autonomy, and AI that allows for drone "swarming."[20] During Operation Spider Web in 2025, Ukraine smuggled drones into Russia inside of cargo trucks and conducted strikes that damaged or destroyed Russian military aircraft, including Tupolev Tu-95MS and Tu-22M3 strategic bombers.

U.S. military installations, nuclear power plants, and other critical infrastructure are experiencing a high volume of unauthorized drone incursions. Concerts, sports stadiums, transportation infrastructure, and other locations in the U.S. homeland are increasingly vulnerable to advanced unmanned air, ground, sea, and undersea systems. As Cathy Lanier, the Senior Vice President and Chief Security Officer of the National Football League, said at the Center for Strategic and International Studies in June 2026, "Our distance from our adversaries is

[20] Drone swarming is the use of multiple drones to communicate, coordinate, and operate cooperatively to achieve a common objective.

no longer a sense of safety for us … If you think about just one mass gathering attack, the Super Bowl, we have 70,000-80,000 people, but we have a global stage."[21]

Congress has made notable progress on countering drones, particularly with the passage of the Safer Skies Act. However, significant gaps in technology, bureaucracy, and implementation remain. There are still limited authorities for federal, state, and local officials to counter and mitigate the threat from drones. The Safer Skies Act does not grant counter-drone mitigation authority to private entities. Private venue operators, critical infrastructure owners, and hospitals remain legally barred from jamming or destroying unauthorized drones themselves. While the act provides a legal pathway for local authorities to intervene, commercial consumer drone technology is advancing much faster than the slow federal policy and equipment acquisition cycles. There is also a severe operational bottleneck caused by the Safer Skies Act's requirement that all state and local law enforcement have to be certified by a single federal schoolhouse: the FBI's National Counter-UAS Training Center in Huntsville, Alabama. More than 18,500 state, local, and correctional agencies depend on that training center, which opened in 2025.[22] But only 61 officers had been official certified by July 1, 2026.[23]

In addition, there has been a significant increase in the offensive cyber threat to the U.S. homeland. Unlike traditional Chinese hacking groups that historically focused on intellectual property theft or political espionage, Volt Typhoon's explicit mission was strategic sabotage of U.S. critical infrastructure—such as power grids, water systems, communications hubs, and transportation hubs—that could be triggered in the event of a U.S.-China crisis.

Intelligence Implications

Two and a half decades after 9/11, there is an urgent need to increase intelligence collection and analysis across federal, state, and local entities; identify and fix security gaps; and strengthen the American public's resilience against enemies at home and abroad. This committee possesses the unique bipartisan oversight and legislative authorities to reshape the intelligence community for a new era. The 9/11 commission was helpful in improving intelligence sharing and coordination against an evolving *terrorist* threat. But U.S. intelligence efforts are far too siloed, under-resourced, and unprepared to deal with the evolving *state-based* threat to the United States—especially a U.S. homeland that is increasingly vulnerable to attack. I have included below several suggestions for consideration:

- *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

[21] Cathy Laner, Panel on "The End of Sanctuary: The Evolution of Homeland Defense," Center for Strategic and International Studies, June 30, 2026, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2026-07/260630_Crank_End_Sanctuary.pdf?VersionId=B8ypvJOcPRuGue9bZC2JEv2MFKUmWhvb.
[22] Philip W. Rohlfing, "The Counter-UAS Certification Bottleneck," Lawfare, June 23, 2026, https://www.lawfaremedia.org/article/the-counter-uas-certification-bottleneck.
[23] Megan Norris, "New Federal Counter-Drone Rule Gives Local Police and Corrections Agencies Authority to Detect, Disable Dangerous Drones," Homeland Security Today, July 9, 2026, https://www.hstoday.us/subject-matter-areas/unmanned-vehicles/new-federal-counter-drone-rule-gives-local-police-and-corrections-agencies-authority-to-detect-disable-dangerous-drones/.

later, ODNI has failed to effectively achieve these results. Instead, it has added another layer of bureaucracy with ambiguous authority, little budget control or coordination, patchy leadership, and a tendency to complicate rather than improve intelligence sharing. Congress should consider a major review—either by Congress or a Congressionally-mandated national commission—of the ODNI based on the evolving national security landscape and policy needs. Should ODNI be abolished? Should it be replaced by a small, professional intelligence office, perhaps akin to the Office of Management and Budget, that focuses on coordination and deconfliction of such issues as counterintelligence, counterterrorism, and other threats? Should ODNI be significantly evolved in other ways? These are difficult—but momentous—questions that need to be urgently answered.

- *Section 702:* Section 702 of the Foreign Intelligence Surveillance Act allows a range of U.S. intelligence agencies—such as the National Security Agency, Central Intelligence Agency, and Federal Bureau of Investigation—to collect communications between foreigners overseas. With Congressional oversight and protection of U.S. citizens, the program has been successful. It has prevented terrorist attacks and aided in the conviction of international criminal groups, Russian and Chinese spies, and drug traffickers. But Section 702 lapsed on June 12, 2026, after Congress failed to pass an extension. While existing FISA court surveillance certifications may allow current intelligence collection to temporarily continue, the lapse has plunged U.S. intelligence agencies and telecommunications providers into a highly uncertain legal gray zone. Based on the multi-faceted state and non-state threats to the U.S. homeland, the right answer is clear: reauthorize Section 702.[24]

- *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.

- *Legislation Against Foreign Agents:* Enact stronger legislation that criminalizes foreign agents that harass, surveil, or conduct other types of actions against U.S. residents on American soil, a tactic frequently deployed by China and other governments. This should include strengthening the Foreign Agents Registration Act (FARA).

[24] See, for example, Emily Harding, "Section 702: Why Do We Need It?" Center for Strategic and International Studies, April 24, 2026, https://www.csis.org/analysis/section-702-why-do-we-need-it.

- *Critical Infrastructure Protection:* Expand the mandatory reporting requirements for cyber incidents and physical attacks orchestrated by state-backed groups attempting to compromise U.S. water, energy, transportation, and other critical infrastructure. Foreign adversaries are weaponizing advanced technology, including generative AI and micro-targeted digital campaigns, to inflame domestic political opinion, undermine trust in democratic institutions, and exploit vulnerabilities in critical infrastructure.

There are other steps that Congress should consider, but which fall outside of the jurisdictions of the House and Senate intelligence communities. One of the most significant is legislation that helps counter drone incursions in the U.S. homeland. While such legislation as the Safer Skies Act represents an important shift by granting state and local agencies the right to detect, track, and mitigate hostile drones, the legal and technical frameworks are still being established. Congress should also help ensure that the Department of Justice and the Department of Homeland Security have adequate appropriations to implement the mandatory national training and certification programs required for local officers. Congress should also build upon the Federal Communications Commission's recent actions and consider establishing a clear framework allowing vetted, high-risk critical infrastructure operators to deploy approved counter-UAS systems under direct federal or state and local law enforcement supervision.

The 9/11 Commission report was instrumental in arguing that the United States faced a "generational challenge" from terrorist groups that threatened the United States.[25] Today, there is a new generation of Americans and a new generational challenge—one based largely on adversary threats to the U.S. homeland and U.S. interests abroad. The United States is witnessing an end of sanctuary after decades of relative safety from foreign adversaries. President Dwight D. Eisenhower may have said it best in a radio address to the nation on May 19, 1953, when he emphasized the need for a sustainable defense of the nation, "A defense strong enough both to discourage aggression and beyond this to protect the nation—in the event of any aggression... This defense must, first of all, be one which we can bear for a long and indefinite period of time."[26]

[25] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.*
[26] Dwight D. Eisenhower, "Radio Address to the American People on the National Security and Its Costs," May 19, 1953, https://www.presidency.ucsb.edu/documents/radio-address-the-american-people-the-national-security-and-its-costs.