



INFORMATION SERIES

Issue No. 650

February 10, 2026

The Coming War in America

Christopher A. Williams

Christopher A. Williams previously held senior positions in the U.S. Congress and Department of Defense. He also chaired the Defense Policy Board. He currently serves as an independent consultant.

Introduction

As overseas threats to U.S. national interests intensify, America's enemies can be expected to carry the fight to the U.S. homeland. The reason for this is clear: The U.S. homeland is a ripe target for such attacks. America has significant systemic societal vulnerabilities, limited defensive capabilities, and exploitable gaps and seams between various organizations responsible for identifying threats and defending the homeland.

Today America is under attack by adversary nations, terrorist groups, transnational criminal organizations, violent illegal immigrants, and radicalized or disgruntled U.S. citizens. News stories and official Government reports provide ample evidence of attacks on U.S. critical infrastructures, plots to assassinate current and former government officials, illicit penetrations of key U.S. government facilities including military bases, attacks on U.S. lawmakers, and more.

America's political leaders must resolve—on a bipartisan basis—to rapidly and comprehensively address the growing vulnerability of the homeland. An essential first step in developing a strategy and plan of action to secure the homeland is to understand the magnitude and scope of the threat. This effort can be aided by forecasting realistic scenarios of how the coming war in America could play out.

This *Information Series* article briefly outlines four scenarios. By no means are these the only scenarios that are relevant to the coming war in America. But hopefully they will help shine a



light on the growing vulnerability of the U.S. homeland and reinforce the need for urgent remedial action.

Scenario 1: Adversary Attempts to Influence the Outcome of U.S. Elections Through a Campaign of Targeted Political Violence and Assassinations

This scenario takes into account the growing threat of foreign-inspired politically-motivated violence and the impact such actions could have on the outcome of the 2026 and/or 2028 elections – and on U.S. domestic politics more broadly.

Russia, Iran, China, North Korea and their proxies are capable of conducting attacks on targeted individuals across the globe. Russia's GRU military intelligence service has demonstrated its willingness and ability to conduct assassinations of enemies of the Putin regime, particularly in Europe.¹ In addition, Russia has sent undeclared intelligence operatives to live and work in the United States.² Such "illegals" or "sleeper agents" could potentially be directed by Putin to conduct assassinations or sabotage here in the American homeland.

Iran has launched plots to assassinate key senior U.S. government officials, including President Trump, a former Secretary of State, and a former national security advisor to the President, as well as U.S. citizens who are critical of the Iranian regime.³ U.S. Attorney General Pam Bondi recently warned that the Department of Justice is on "high alert" for threats posed by Iranian operatives operating inside the United States.⁴

U.S. Immigration and Customs Enforcement agents have recently arrested numerous Iranian nationals illegally in the United States, including a former member of Iran's Islamic Revolutionary Guard Corps with suspected Hezbollah ties, a former Iranian army sniper, and a terror watchlist suspect, during a sweep targeting illegal Iranian migrants across the country.⁵

During Chinese Communist Party (CCP) General Secretary Xi Jinping's visit to San Francisco in November 2023, human rights demonstrators were met with organized harassment and violent assaults by pro-CCP agitators. Investigations by media outlets and human rights groups found evidence of direct Chinese government involvement in organizing and funding the counter-protests and associated violence.⁶ Those actions demonstrate that CCP leaders are not averse to fomenting violence inside the United States when it suits their purposes.

Director of National Intelligence Tulsi Gabbard recently stated that at least 2,000 Afghans in the U.S. have ties to terrorism.⁷ An Afghan national was charged with the November 2025 murder of National Guard Specialist Sarah Beckstrom and wounding of Guard member Andrew Wolfe just a few blocks from the White House.⁸

North Korea has conducted several assassination attempts on foreign soil. Since 2008, Pyongyang has been linked to at least six attempted assassinations in South Korea, China and Malaysia.⁹ Furthermore, Russia, China, Iran or North Korea could outsource assassinations and other politically-motivated violent operations to terrorist groups or disaffected individuals in the United States in an attempt to conceal their involvement in such plots.



INFORMATION SERIES

Issue No. 650 | February 10, 2026

Transnational criminal organizations (TCOs) have brought increased violence, drug trafficking, extortion, human trafficking and smuggling, and illicit firearms to cities and towns across America.¹⁰ TCOs operating in the United States include the notorious MS-13 gang and Tren de Aragua. Mexican drug cartels such as the Sinaloa Cartel and the Jalisco New Generation Cartel have a presence in almost every state. Each of these TCOs have been formally designated by the U.S. government as a “foreign terrorist organization.”¹¹ These and other TCOs could launch attacks on U.S. politicians and/or against polling places during upcoming national election cycles.

Attacks on U.S. politicians have risen sharply. The last several years have witnessed an arson attack on Pennsylvania Governor Josh Shapiro’s residence apparently motivated by hatred of Jews;¹² the attempted murder of Congressman Steve Scalise;¹³ an attack at the San Francisco home of then-Speaker of the House of Representatives Nancy Pelosi;¹⁴ and more. President Trump has survived at least two assassination attempts.

The leader of the U.S. Capitol Police recently testified that “[t]he past year alone saw threats against Members [of Congress] increase to a staggering 9,400 in one year – more than double over the past ten years. That is a huge increase, and given the current political climate, one that is likely to continue an upward trend.”¹⁵ In this regard, many believe the Secret Service, the U.S. Capitol Police, and other organizations responsible for preventing such attacks on American politicians are woefully under-resourced.¹⁶

Given the razor-thin margins that separate the majority and minority parties in both the U.S. House of Representatives and the U.S. Senate, successful efforts to assassinate or debilitate just a few legislators could determine which party controls one or both houses of Congress. Such a scenario would likely inflame domestic tensions and could result in institutional gridlock that inhibits the ability to pass vital legislation. In addition, assaults at U.S. election polling stations may occur in 2026 and 2028. Such actions could undermine voter confidence and lead to prolonged counting of votes, which would spawn accusations of an unfair election. They also could fan the flames of extremism and lead to calls for political retribution or additional acts of domestic violence.

Scenario 2: Adversary Operations to Disrupt the U.S. Economy, including Physical and Cyber Attacks on U.S. Critical Infrastructures

Attacks on various U.S. critical infrastructures, from cyber attacks to physical sabotage, could cause severe disruptions to essential services, leading to public health/safety risks and massive economic damage. Such attacks could severely threaten U.S. domestic political and economic stability by disrupting daily life, inhibiting business operations, and cutting critical supplies and utilities.

Secretary of Homeland Security Kristi Noem recently testified that, “Terrorists and criminals with a variety of motivations continue to incite, and occasionally conduct, physical attacks against a range of targets. This past year, they mobilized against major commercial sites, government offices, transportation gateways, energy systems, and healthcare facilities.



INFORMATION SERIES

Issue No. 650 | February 10, 2026

Critical infrastructure targets are often selected based on opportunistic factors, such as accessibility or the ability to wreak widespread havoc.... Foreign adversaries pose a strategic threat to public safety, and their objectives may include disrupting national morale, undermining public trust, or exploiting symbolic events for geopolitical messaging.”¹⁷

America’s adversaries are continuing to conduct cyber operations to identify and exploit vulnerabilities in U.S. critical infrastructures. As noted by then-FBI Director Christopher Wray, “China’s hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities.”¹⁸ A senior FBI official recently testified that “The current state of the cyber threat landscape is one of interconnected and callous actors who have the tools to paralyze entire school systems, police departments, healthcare facilities, and other entities. China, Russia, Iran, North Korea and criminal ransomware continue to be the top cyber threats facing the United States.... In 2024, the FBI received thousands of reports from critical infrastructure organizations that were affected by cyber incidents, with the most pervasive cybercriminal threat being ransomware. This threat is enormous in terms of the losses, the number of active variants, and the disruptive effects. The FBI’s Internet Crime Complaint Center received over 3,100 reports of ransomware incidents in 2024.”¹⁹

The potential direct and indirect impacts of such attacks on various U.S. critical infrastructures could be significant. For example, an inwardly-focused America, forced to react to major domestic challenges, could be viewed by our adversaries as an opportunity to launch aggressive operations abroad.

Scenario 3: Adversary Attacks to Degrade or Delay U.S. Munitions Production and Distribution

This scenario involves adversary operations to impede the production and distribution of munitions and other critical war materiel via attacks on U.S. military bases, ports, railways, airfields and Defense Industrial Base (DIB) facilities.

America’s adversaries possess a broad range of capabilities for disrupting and degrading the DIB. Such measures could involve sabotage, drone strikes, cyber or ransomware and other attacks on facilities such as shipyards, aircraft manufacturing and munition production plants, associated component suppliers, as well as attacks on DIB personnel in order to slow the production of munitions and other vital war materiel. Any significant delay in the production and distribution of U.S. munitions and other critical wartime materiel could provide adversaries with a potentially decisive advantage.

Such attacks could be conducted by unmanned aerial systems. Drone incursions over domestic military bases have been a growing problem for officials since the mysterious unmanned flights over Langley Air Force Base in Virginia in late 2023 and other high-profile sightings. The Department of Defense has monitored hundreds of intrusions into the protected airspace above sensitive U.S. facilities over the past few years. In October 2025, a U.S. Northern Command official acknowledged that there were 230 drone incursions reported over military



INFORMATION SERIES

Issue No. 650 | February 10, 2026

installations between September 2023 and September 2024, which jumped by 82 percent to approximately 420 sightings reported over roughly the same period the following year.²⁰

This scenario could include cyber and/or physical attacks on U.S. electrical power generation plants, transportation grids, and other activities that support domestic wartime materiel production and distribution operations as well as ransomware attacks against U.S. small- and medium-sized businesses that produce key components in modern weapon systems. North Korean state-sponsored groups have conducted numerous ransomware attacks on American companies.²¹

Foreign intelligence service operatives, illegal immigrants, and others have repeatedly sought to penetrate U.S. military bases through so-called “gate-crashing,” coming ashore by boat, and other modalities.²² The FBI and Department of Defense have tracked hundreds of incidents of Chinese nationals posing as tourists attempting to breach U.S. military bases and other federal sites. Gaining access to sensitive DoD installations and other U.S. Government facilities could allow adversary personnel to assess U.S. military capabilities and posture, disrupt base operations, attack U.S. military and civilian personnel, and hinder the staging and transport of military personnel and vital equipment, among other purposes.

In this regard, the case of Qilin Wu is worth mentioning. This Chinese national entered the U.S. illegally in 2023 by crossing the Mexico-Arizona border near Nogales. He was arrested by U.S. immigration authorities, but was released due to a lack of detention space and was given an immigration removal proceeding scheduled for early 2027, officials said. Investigators caught him on December 2nd of last year near Whiteman Air Force Base, the home of the B-2 stealth bomber fleet. After initially receiving a warning, he reportedly returned to the base the very next day. Authorities then arrested him. In his possession were 18 photos and videos of the base, including perimeter fencing, a gate and military equipment.²³

Multiple U.S. Government agencies issued an advisory in November 2024 warning DIB contractors of possible efforts by foreign actors to conduct sabotage operations against their facilities.²⁴ The notice described examples of known threats, highlighted indicators of possible future attacks, detailed steps that can be taken to investigate such attacks, and provided contact information for the FBI and other Federal agencies to report suspicious activities or attacks. The advisory asserted that “The Russian government has been using its intelligence services to plan and conduct sabotage operations targeting Europe’s DIB – including private industry – in an attempt to undermine Allied support for Ukraine. Russia’s sabotage activities in Europe increase the risk to U.S. companies abroad and potentially at home. Such sabotage operations can sow fear and doubt, damage important infrastructure, disrupt commerce, or cause injury and death.”

Scenario 4: Adversary Attacks to Disrupt and Degrade U.S. National Decision Making and Strategic Military Operations

This scenario focuses on adversary operations to disrupt, degrade or destroy U.S. nuclear command, control and communications (NC3) and global missile defense battle management



INFORMATION SERIES

Issue No. 650 | February 10, 2026

command control & communications (BMC3) systems in the context of Chinese aggression in Asia and/or Russian attacks against NATO. Such attacks could include limited missile strikes and/or cyber attacks on select U.S. military facilities, networks and systems that perform vital NC3 and missile defense BMC3 functions, as well as anti-satellite (ASAT) attacks on U.S. satellites used for these and other functions.

Chinese and/or Russian military objectives for such attacks could include hindering U.S. senior leaders' ability to rapidly assess and respond in a timely manner to adversary attacks, degrading the President's ability to communicate with the Secretary of Defense and senior military leaders, and more. Limited conventional, nuclear and/or cyber strikes against a relatively small set of U.S. targets could potentially severely degrade U.S. military capabilities and paralyze U.S. decision makers who may fear further escalation. Such attacks could be aimed at compellence—that is, forcing the U.S. to take a specific action or change its behavior in some way that benefits the adversary. Unlike deterrence, which seeks to prevent an action, compellence aims to achieve a positive outcome from the target state, often by instilling a sense of unacceptable risk or fear of escalation. This scenario appears to be consistent with Russian and possibly Chinese regional theories of victory.²⁵

As noted by U.S. Strategic Command Deputy Commander Vice Admiral Richard Correll, "Russia and China are expanding and modernizing their nuclear force capabilities, to include ICBMs [intercontinental ballistic missiles], and developing advanced hypersonic weapons. Additionally, Russia and China are developing or have already fielded new SSBNs [strategic missile-carrying submarines] with SLBMs [sea-launched ballistic missiles], strategic bombers, and novel weapons meant to defeat U.S. missile defense systems.... The efforts of these nations to modernize, expand, and develop new nuclear capabilities will increase the threat as these advanced weapon systems are fielded."²⁶

China is well into its accelerated strategic force modernization program that then-U.S. Strategic Command Commander Admiral Charles Richard described as "a strategic breakout."²⁷ As noted in a recent article, "The Chinese People's Liberation Army just offered the first public look at elements of all three legs of its still very new strategic nuclear triad at a massive military parade in Beijing in September [2025]. In recent years, U.S. officials have been outspoken about massive assessed increases in Chinese nuclear warheads and delivery systems. This includes the construction of vast arrays of nuclear silos for intercontinental ballistic missiles, as well as the development and fielding of more and more advanced road-mobile ICBMs. China is now fielding air-launched nuclear-capable ballistic missiles and is growing the size and capabilities of its fleet of nuclear ballistic missile submarines, as well."²⁸

Elements of China's and Russia's modernized strategic forces could be used in very limited strikes on the U.S. homeland. This could include attacks aimed at decapitating U.S. national and military leadership and destroying critical facilities and systems that play a central role in NC3 and global missile defense BMC3.

Russia and China are testing and fielding advanced counterspace (anti-satellite) systems to hold at risk U.S. satellites in all orbits, including space systems that contribute to nuclear C3 and missile defense BMC3. In addition to other ASAT capabilities and systems, Moscow is



INFORMATION SERIES

Issue No. 650 | February 10, 2026

developing a nuclear ASAT weapon that could be used either for coercion or to destroy most or all government and commercial satellites operating in low Earth orbit (LEO).²⁹ Detonation of such a weapon on-orbit could gravely damage U.S. military communications, precision navigation & timing, and intelligence surveillance & reconnaissance systems and thus degrade U.S. military operations aimed at countering foreign aggression.

As for the PRC, the U.S. Space Force recently reported that “Intelligence suggests the People's Liberation Army (PLA) likely sees counterspace operations as means to deter and counter U.S. military intervention in a regional conflict. It is actively developing and fielding a wide range of counterspace capabilities:

- In 2007, the PLA destroyed a defunct weather satellite in LEO with a direct-ascent antisatellite missile, creating more than 2,700 pieces of trackable debris that remain in orbit. The capability evolved into an operational system intended to target LEO satellites. The PLA actively trains on this system today.
- The Defense Intelligence Agency assesses the PLA probably intends to field ASAT weapons able to reach up to GEO at 36,000 km. In 2013, the PLA launched a ballistic object which peaked at 30,000 km, suggesting it may already have a basic ASAT capability against higher orbits.
- China is developing satellite “inspection and repair” systems that could also function as weapons. It has already launched multiple satellites to experiment with orbital maintenance and space debris clean-up. In January 2022, the SJ-21 satellite moved a derelict BeiDou navigation satellite to a graveyard orbit above GEO. This technology could be used in future systems to grapple other satellites.
- Multiple SJ-series and TJS-series experimental satellites have conducted unusual, large, and rapid maneuvers in GEO; tactics that could have several different military applications. In 2024, three Shiyao-24 (SY-24) experimental satellites in LEO were also observed conducting proximity operations.
- The PLA has multiple ground-based laser weapons able to disrupt, degrade, or damage satellite sensors. By the mid-to-late 2020s, the PRC could have higher-power systems able to damage satellite structures. PLA military exercises regularly incorporate jammers against space-based communications, radars, and navigation systems like GPS. Intelligence suggests the PLA may be developing jammers to target SATCOM over a range of frequencies, including U.S. military protected extremely-high-frequency (EHF) systems.”³⁰

America’s adversaries clearly understand the potential value of disrupting or degrading U.S. national decision making and strategic military operations through kinetic, cyber or other attacks on U.S. missile defense BMC3 and nuclear C3 systems and processes, including critical U.S. national security space systems. According to Eric Edelman, “As the Strategic Posture Commission established by Congress noted in 2023, this is ‘an existential challenge for which the United States is ill-prepared, unless its leaders make decisions now to adjust the U.S.



INFORMATION SERIES

Issue No. 650 | February 10, 2026

strategic posture. One essential element of this challenge involves ensuring that the national command authority—the ability of the U.S. president and key military advisors to be in communication with U.S. nuclear (and conventional) forces at all times—remains intact and protected. This is a critical element of deterrence: If a nuclear-armed enemy perceives the command structure to be vulnerable, it may consider attempting a nuclear decapitation strike.”³¹

Conclusion

War is coming to America. Indeed, it is here now/today. This intensifying war will include tools and methods such as cyber attacks, drone strikes, terrorism, assassinations, sabotage, missile strikes, and more. The United States must urgently fashion and implement the policies, strategies, plans, programs, and operations needed in order to effectively counter such escalating threats. Nothing less than America’s survival is at stake.

¹ See, for example, Csongor Koromi, “NATO: There was officially a Russian plot to kill European weapons chief,” *PoliticoEU*, January 28, 2025, <https://www.politico.eu/article/nato-official-confirms-russian-plot-kill-european-weapons-chief-armin-papperger/>; and, Luke Harding, “The Skripal poisonings: the bungled assassination with the Kremlin’s fingerprints all over it,” *The Guardian*, December 26, 2018, <https://www.theguardian.com/news/2018/dec/26/skripal-poisonings-bungled-assassination-kremlin-putin-salisbury>; and, “Timeline: Alexander Litvinenko death case,” *BBC News*, January 27, 2015, <https://www.bbc.com/news/uk-30929940>.

² Federal Bureau of Investigation, “Operation Ghost Stories: Inside the Russian Spy Case,” October 31, 2011, <https://www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case>.

³ See, for example, Mike Levine and Aaron Katersky, “3 charged in Iran-linked murder plots with one targeting Donald Trump as revenge for killing Qassem Soliemani: DOJ,” *ABC News*, November 8, 2024, <https://abcnews.go.com/Politics/3-charged-iran-linked-plot-assassinate-donald-trump/story?id=115646874>. See also, “FBI hunting for Iranian spy who allegedly plotted assassination of Mike Pompeo, other US officials,” *New York Post*, March 24, 2024, <https://nypost.com/2024/03/04/us-news/fbi-hunting-for-iranian-spy-who-allegedly-plotted-assassination-of-mike-pompeo-other-us-officials/>.

⁴ Kaelan Deese, “Pam Bondi says DOJ has ‘countless’ threat cases against the US amid Iran concerns,” *Washington Examiner*, June 24, 2024, <https://www.washingtonexaminer.com/news/justice/3451597/pam-bondi-doj-countless-threat-cases-iran-concerns/>.

⁵ See, for example, Department of Homeland Security, “ICE Arrests 11 Iranian Nationals Illegally in the U.S.,” June 24, 2025, <https://www.dhs.gov/news/2025/06/24/ice-arrests-11-iranian-nationals-illegally-us-over-weekend>.

⁶ “Pro China activists harassed anti-Xi Jinping protesters in San Francisco,” *The Washington Post*, September 2, 2024, <https://www.washingtonpost.com/world/interactive/2024/chinese-communist-party-us-repression-xi-jinping-apec/>.

⁷ April Rubin, “Gabbard claims 2,000 Afghans in the U.S. have ties to terrorism,” *Axios*, December 212, 2025, <https://www.axios.com/2025/12/12/tulsi-gabbard-afghans-terrorism>.

⁸ U.S. Attorney’s Office, District of Columbia, “Afghan National Charged with the Murder of National Guard Soldier Sarah Beckstrom,” December 2, 2025, <https://www.justice.gov/usao-dc/pr/afghan-national-charged-murder-national-guard-soldier-sarah-beckstrom>.



INFORMATION SERIES

Issue No. 650 | February 10, 2026

⁹ Robert Windren, Ken Dilanian and Abigail Williams, “North Korea has a history of assassination attempts,” *NBC News*, November 21, 2017, <https://www.nbcnews.com/news/north-korea/north-korea-has-history-assassination-attempts-foreign-soil-n823016>.

¹⁰ See, for example, Magda Long, “When States Go Mob: The Criminalization of Modern Statecraft,” *Cipher Brief*, August 6, 2023, <https://www.thecipherbrief.com/gray-zone-criminal>.

¹¹ Office of the Spokesperson, “Designation of International Cartels,” U.S. Department of State, February 20, 2025, <https://www.state.gov/designation-of-international-cartels/>

¹² Victor Fiorillo, “The Josh Shapiro Arson Attack: What We Know. And What We Don’t,” *Philadelphia Magazine*, April 14, 2024, <https://www.phillymag.com/news/2025/04/14/josh-shapiro-arson-fire-motive/>.

¹³ Melissa Chan, “Congressman Scalise Was Shot at a Congressional Baseball Practice: Here’s What You Need to Know,” *Time Magazine*, June 14, 2017, <https://time.com/4817818/steve-scalise-alexandria-shooting/>.

¹⁴ “What is known about the attack on Speaker Pelosi’s husband,” *AP News*, October 29, 2022, <https://apnews.com/article/arrests-california-san-francisco-1582f7f07e277d65ce445c39de9a8bca>.

¹⁵ Statement of J. Thomas Manger, Chief of the U.S. Capitol Police before the Committee on Appropriations Subcommittee on the Legislative Branch, April 8, 2025, <https://docs.house.gov/meetings/AP/AP24/20250408/118104/HHRG-119-AP24-Wstate-MangerJ-20250408.pdf>.

¹⁶ See, for example, the “Report of the Independent Review Panel to review the U.S. Secret Service following the July 13, 2024 assassination attempt of President Trump in Butler, Pennsylvania,” https://www.dhs.gov/sites/default/files/2024-10/24_1017_opa-Independent-Review-Panel-Final-Report-and-Accompanying-Materials.pdf.

¹⁷ Testimony of Kristi Noem, Secretary of Homeland Security, before the House Committee on Homeland Security, “Annual Worldwide Threats to the Homeland,” December 11, 2025, <https://homeland.house.gov/hearing/worldwide-threats-to-the-homeland-3/>.

¹⁸ Didi Tang and Eric Tucker, “Chinese hackers are determined to ‘wreak havoc’ on U.S. critical infrastructure, FBI director Wray warns,” *PBS News*, January 31, 2024, <https://www.pbs.org/newshour/politics/chinese-hackers-are-determined-to-wreak-havoc-on-u-s-critical-infrastructure-fbi-director-wray-warns>.

¹⁹ Statement of Michael Glasheen, Federal Bureau of Investigation, “WorldWide Threats to the Homeland,” before the House Committee on Homeland Security, December 11, 2025, <https://homeland.house.gov/hearing/worldwide-threats-to-the-homeland-3/>.

²⁰ 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/>.

²¹ See, for example, Cybersecurity & Infrastructure Security Agency, “North Korea Threat Overview and Advisories,” <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea>.

²² See, for example, Gordon Lubold, Warren Strobel, and Aruna Viswanatha, “Chinese Gate Crashers at U.S. Bases Spark Espionage Concerns,” *The Wall Street Journal*, September 4, 2023, <https://www.wsj.com/politics/national-security/chinese-gate-crashers-at-u-s-bases-spark-espionage-concerns-cdef8187>; and, Danielle Wallace, “FBI tracks over 100 incidents of Chinese nationals posing as tourists to breach US military sites: report,” *Fox News*, September 4, 2023, <https://www.foxnews.com/politics/fbi-tracks-100-incidents-chinese-nationals-posing-tourists-breach-us-military-sites-report>.

²³ Bonny Chu, “Chinese national charged with photographing US stealth bomber base after illegal entry,” *Fox News*, January 8, 2026, <https://www.foxnews.com/us/chinese-national-charged-photographing-us-stealth-bomber-base-illegal-entry>.



INFORMATION SERIES

Issue No. 650 | February 10, 2026

²⁴ “Safeguarding the U.S. Defense Industrial Base and Private Industry Against Sabotage,” Joint Advisory of the National Counterintelligence and Security Center, Federal Bureau of Investigation, Air Force Office of Special Investigations, Army Counterintelligence Command, Defense Counterintelligence and Security Agency, and Navy Criminal Investigations Services, November 21, 2024, https://www.dni.gov/files/NCSC/documents/products/FINAL_Safeguarding_DIB_Against_Sabotage.pdf.

²⁵ See, for example, Keith B. Payne and David J. Trachtenberg, *Deterrence in the Emerging Threat Environment: What is Different and Why it Matters, Occasional Paper*, Vol. 2, No. 8 (Fairfax, VA: National Institute Press, August 2022), <https://nipp.org/papers/deterrence-in-the-emerging-threat-environment-what-is-different-and-why-it-matters/>; and, Mark B. Schneider, “The Implications of Russia’s New Nuclear Doctrine,” *Information Series*, No. 615 (Fairfax, VA: National Institute Press, February 5, 2025), https://nipp.org/information_series/mark-b-schneider-the-implications-of-russias-new-nuclear-doctrine-no-615-february-5-2025/.

²⁶ Vice Admiral Richard Correll, Advanced Policy Questions, Senate Armed Services Committee, October 30, 2025, https://www.armed-services.senate.gov/hearings/to-consider-the-nomination-of_vice-admiral-richard-a-correll-usn-to-be-admiral-and-commander-united-states-strategic-command.

²⁷ Aaron Mehta, “STRATCOM Chief Warns of Chinese ‘Strategic Breakout,’” *Breaking Defense*, August 12, 2024, <https://breakingdefense.com/2021/08/stratcom-chief-warns-of-chinese-strategic-breakout/>.

²⁸ Joseph Trevithick, “Golden Dome Missile Shield Key to Ensuring Nuclear Second Strike Capability: U.S. Admiral,” *The War Zone*, November 6, 2025, <https://www.twz.com/nuclear/golden-dome-missile-shield-key-to-ensuring-nuclear-second-strike-capability-u-s-admiral>.

²⁹ Marc Berkowitz and Chris Williams, “Russia’s Space-Based, Nuclear-Armed Anti-Satellite Weapon: Implications and Response Options,” Moorman Center for Space Studies, May 16, 2024, <https://nssaspace.org/wp-content/uploads/2024/05/Russian-Nuclear-ASAT.pdf>.

³⁰ U.S. Space Force, “Space Threat Fact Sheet,” September 2025, <https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/4297159/space-threat-fact-sheet/>.

³¹ Eric S. Edelman, “America’s Latest Problem: A Three-Way Nuclear Race,” *Foreign Policy*, June 2, 2025, <https://foreignpolicy.com/2025/06/02/us-nuclear-weapons-deterrence-command-control-nc3-decapitation-strike-china-russia-strategy-geopolitics/>.

The National Institute for Public Policy’s *Information Series* is a periodic publication focusing on contemporary strategic issues affecting U.S. foreign and defense policy. It is a forum for promoting critical thinking on the evolving international security environment and how the dynamic geostrategic landscape affects U.S. national security. Contributors are recognized experts in the field of national security. National Institute for Public Policy would like to thank the Sarah Scaife Foundation for the generous support that made this *Information Series* possible.

The views in this *Information Series* are those of the author(s) and should not be construed as official U.S. Government policy, the official policy of the National Institute for Public Policy, or any of its sponsors. For additional information about this publication or other publications by the National Institute Press, contact: Editor, National Institute Press, 12150 Monument Dr., Suite 125, Fairfax, VA 22033, (703) 293- 9181, www.nipp.org. For access to previous issues of the National Institute Press *Information Series*, please visit <http://www.nipp.org/national-institute/press/informationseries/>.

© National Institute Press, 2026