



INFORMATION SERIES

Issue No. 671

October 13, 2026

The Coming War in America: Iranian Threats to the U.S. Homeland

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.

War is coming to America.¹ In many respects it is here today. In the eyes of our avowed enemies, the U.S. homeland is a central battleground in the intensifying competition between divergent – indeed, irreconcilable – political systems and beliefs.

As a practical matter, the Islamic Republic of Iran has been at war with the United States for nearly fifty years. This despite numerous diplomatic efforts aimed at rapprochement and various agreements intended to curb Iran's nuclear weapons development program and regional ambitions. In light of high-intensity military operations conducted by the United States against Iran (Operations Midnight Hammer and Epic Fury) as well as severe economic measures such as blockades and targeting of illicit oil-smuggling networks, Iran's leaders will likely redouble efforts to target key U.S. government officials and institutions, various critical infrastructures, and the American people.

This paper highlights threats to the U.S. homeland posed by Iran and its agents and sympathizers. It describes plots hatched and operations conducted by Iran-affiliated organizations and personnel and describes actions taken by various Federal, state and local government organizations to identify, disrupt, and prevent such attacks. Lastly, it calls for comprehensively enhancing the U.S. homeland security posture in response to the growing threat posed by Iran, its proxies, and supporters.



History of Iranian Aggression Against the United States

Over the past half-century, Iran has planned and conducted numerous attacks against the homeland and U.S. Government personnel, civilians and facilities overseas—and, in the process, killed or injured thousands of Americans. A March 2, 2026 White House report noted that “For nearly half a century, the Islamic Republic of Iran—the world’s leading state sponsor of terrorism—has killed or maimed American citizens and service members through its own forces and proxy militias. More Americans have been killed by Iran than any other terrorist regime on Earth.”² According to the release, Iran has sponsored dozens of attacks on U.S. citizens since the Iranian Revolution of 1979.

As noted by a former FBI counter terrorism official, “Iran’s Islamic Revolutionary Guard Corps and its external operations arm, the Qods Force, have already demonstrated activity inside the United States across the two vectors that matter most: physical operations and cyber intrusions.... The United States has recently seen a cluster of them: charges against IRGC-linked actors targeting U.S. officials; public reporting on retaliatory rhetoric tied to the Iran war; media coverage of bounty offers; and FBI testimony outlining how Iran’s Axis of Resistance posture elevates homeland risk during conflict spikes abroad.... These activities map onto the spaces where Americans live, work, receive care, and expect normalcy.”³

And according to the Institute for Economics and Peace, “Official U.S. threat reporting states that Iran’s strategy is heavily reliant on a network of partners and proxies and on hybrid warfare, combining conventional capabilities with unconventional tools to threaten U.S. interests and allies while limiting the risk of direct conflict. The Islamic Revolutionary Guards Corps Quds Force is assessed by the U.S. National Counter Terrorism Center as providing guidance, training, funds, and weapons to partners and proxies, sustaining multi-theatre capabilities and preserving plausible deniability.... When outmatched conventionally, the Iranian regime tends to fall back on decentralised terrorism to impose costs on its adversaries.”⁴

Iranian Threats to the Homeland

Iran and its proxies clearly pose an immediate and multifaceted threat to the U.S. homeland. Several threat vectors, including terrorism, assassinations, anti-Semitic attacks, cyber warfare, and drone attacks, are discussed below.

Terrorism, Assassinations, and Anti-Semitic Attacks

The United States formally designated the Islamic Republic of Iran a “State Sponsor of Terrorism” in 1984 and since then Tehran has actively engaged in or directed an array of violent and deadly acts against the United States and its citizens globally. The United States also designated Iran’s Islamic Revolutionary Guard Corps (IRGC) a “Foreign Terrorist Organization” on April 15, 2019 for its direct involvement in terrorist plotting and operations.



INFORMATION SERIES

Issue No. 671 | October 13, 2026

As reported by *ABC News* in March, “The Department of Homeland Security (DHS) has warned of potential lone-wolf and cyberattacks amid the ongoing strikes in Iran, according to a law enforcement bulletin. ‘Iran and its proxies probably pose a persistent threat of targeted attacks in the Homeland, and will almost certainly escalate retaliatory actions—or calls to action—if reports of the Ayatollah’s death are confirmed.’”⁵

ABC News also subsequently reported that “The U.S. has intercepted encrypted communications believed to have originated in Iran that may serve as ‘an operational trigger’ for ‘sleeper assets’ outside the country, according to a federal government alert sent to law enforcement agencies.... The intercepted transmission was encoded and appeared to be destined for ‘clandestine recipients’ who possess the encryption key, the kind of message intended to impart instructions to ‘covert operatives or sleeper assets’ without the use of the internet or cellular networks.”⁶ Likewise, *Fox News* reported that “American counterterrorism agencies are quietly monitoring suspected sleeper cells on U.S. soil in the wake of joint U.S.–Israel strikes on Iran, stepping up surveillance amid heightened fears of possible retaliation from Iran-linked operatives or sympathizers.”⁷

Such concerns are certainly not new. A 2020 Department of Homeland Security (DHS) Bulletin warned, “Iran and its partners, such as Hizballah, have demonstrated their capability to conduct various operations in the U.S.... Based on Iran’s historic homeland and global targeting patterns, the financial services and energy sectors, maritime assets, as well as U.S. Government and symbolic targets represent consistent priorities for Tehran’s malicious operational planning. Homegrown Violent Extremists sympathetic to Iran could capitalize on the heightened tensions to launch individual attacks, with little or no warning, against U.S.-based Iranian dissidents, Jewish, Israeli, and Saudi individuals as well as against the U.S. Government infrastructure and personnel.”⁸

Then Attorney General Pam Bondi in June 2025 stated that “well over 1,000” Iranian nationals have illegally entered the U.S. in recent years and asserted that various federal agencies are scrutinizing that population for signs of illegal activity.⁹ And on March 6, 2026 the Justice Department announced that an Iranian intelligence agent, Asif Merchant, had been convicted of terrorism and murder for hire in connection with a foiled plot to assassinate U.S. politicians and government officials, including President Donald J. Trump.¹⁰

Also earlier this year, U.S. Immigration and Customs Enforcement agents arrested a former member of Iran’s IRGC with suspected Hezbollah ties, a former Iran Army sniper, and a terror watchlist suspect during a sweep targeting illegal Iranian migrants across the country.¹¹ And in May 2023, the Justice Department announced that Alexi Saab was sentenced to 12 years in prison for receiving military-type training from Hezbollah, an Iranian-supported terrorist group. By Saab’s own admission, he surveilled “soft targets” in the U.S. for potential future attacks.¹²

General Gregory Guillot, Commander of US Northern Command, recently testified to Congress that “Given its diminished capabilities, Iran’s most viable threat vector toward the homeland remains homegrown violent extremists inspired to conduct attacks on Tehran’s behalf.”¹³ And according to former Under Secretary of Homeland Security John Cohen, “Iran



INFORMATION SERIES

Issue No. 671 | October 13, 2026

has an extensive presence in Canada, Mexico, Central America and South America, where they have both IRGC and intelligence service personnel. They work closely with criminal organizations within the United States to conduct physical attacks. Iran also has an extensive information operation capability and has regularly sought to inspire, inform, even facilitate destructive and violent activities within the United States by posting online content and exploiting divisive current events for the purposes of enabling and facilitating destructive and even violent demonstrations.”¹⁴

As reported in *TIME*, “A gunman opened fire at a bar in Austin, Texas, the day after the initial strikes on February 28, killing three people and injuring more than a dozen others in what is being investigated as a potential act of terrorism. The suspected gunman was wearing a t-shirt with an Iranian flag design at the time of the attack.... Federal authorities have reportedly issued warnings about potential Iranian attacks within the U.S. since the beginning of the war, raising particular concern about cyberattacks and transmissions that could activate ‘ sleeper assets’ outside of Iran.”¹⁵

The threat from Iran and its proxies extends to the U.S. private sector. Multiple Government organizations issued a notice in November 2024 warning Defense Industrial Base contractors of possible efforts by foreign actors to conduct sabotage operations against their facilities.¹⁶ Such potential sabotage operations could slow the production and distribution of critical war materiel being used to support U.S. military operations against Iran.

In addition, a new wave of anti-Semitism, encouraged and supported by Iran and its proxies, has swept the nation. According to a June 22, 2025 DHS bulletin, “Multiple recent Homeland terrorist attacks have been motivated by anti-Semitic or anti-Israel sentiment, and the ongoing Israel-Iran conflict could contribute to U.S.-based individuals plotting additional attacks.... The conflict could also motivate violent extremists and hate crime perpetrators seeking to attack targets perceived to be Jewish, pro-Israel, or linked to the U.S. government or military in the Homeland.”¹⁷ In this regard, a suspect died in an attack on a West Bloomfield, Michigan synagogue on March 13, 2026, in what the FBI said was a “targeted act of violence against the Jewish community.” The FBI labeled the attack as a “Hezbollah inspired act of terrorism” against Michigan’s largest Jewish temple.¹⁸ And the Anti-Defamation League recently issued an “Audit of Anti-Semitic Incidents in the United States.”¹⁹ That report noted that the number of Anti-Semitic acts in America rose from 942 in 2015 to 9,354 incidents in 2024 – an astonishing increase. Iran is a major contributor to this trend as a result of its support to groups and individuals who promote anti-semitism in America.

Cyber Threats

The cyber threat posed by Iran and its proxies to the U.S. homeland includes a broad range of sophisticated cyber probes, prepositioning of malware, and attacks. A Cybersecurity and Infrastructure Security Agency (CISA) advisory issued in 2024 noted that Iran maintains a robust cyber program and is capable of carrying out attacks with temporary disruptive effects against critical infrastructure in the United States.²⁰ On April 7, 2026, multiple U.S.



INFORMATION SERIES

Issue No. 671 | October 13, 2026

Government agencies warned that “Iran-affiliated advanced persistent threat actors are conducting exploitation activity targeting internet-facing operational technology devices, including programmable logic controllers (PLCs)... This activity has led to PLC disruptions across several U.S. critical infrastructure sectors ... resulting in operational disruption and financial loss.” It called upon U.S. companies to urgently review the tactics, techniques and procedures and evidence of compromise for indications of current or historical activity on their networks, and take action to reduce the risk of compromise.²¹ And in July of this year, CISA issued another warning to U.S. organizations of ongoing Iranian-affiliated cyber activity targeting internet-connected operational technology (OT) devices, provided indicators of compromise and detection guidance, and recommended mitigation steps to protect against these attacks and strengthen resilience.²² The most recent Iranian attacks were focused primarily on U.S. drinking water and wastewater systems.

Drone Threats

Drones, including small unmanned aerial systems (sUAS), have become a high-value, low-cost tool of nation-states and subnational organizations, including entities allied with or motivated by Iran, for conducting operations against U.S. targets. There have been numerous reports of unauthorized drone flights over sensitive U.S. military installations in recent years. These include reported overflights of Wright Patterson Air Force Base in Ohio, various military bases in New Jersey, Langley Air Force Base in Virginia, Vandenberg Space Force Base in California, and more.²³ In this regard, numerous unauthorized drones were recently spotted over Barksdale Air Force Base—one of the largest and most important military airfields in the U.S. arsenal that houses B-52H Stratofortress long-range, nuclear-capable bombers.²⁴ Drone incursions over domestic U.S. military bases and critical infrastructure have surged in the last few years.

ABC News reported that in March 2026 the FBI issued a warning to police departments that Iran sought to attack California with drones in retaliation for the on-going attacks on Iran by the United States and Israel. According to that news report, “‘We recently acquired unverified information that as of early February 2026, Iran allegedly aspired to conduct a surprise attack using unmanned aerial vehicles from an unidentified vessel off the coast of the United States homeland, specifically against unspecified targets in California, in the event the U.S. conducted strikes against Iran’, according to the alert distributed at the end of February.”²⁵

There is no publicly available information that specifically attributes the aforementioned drone incursions to Iran or Iranian-inspired actors. However, Iran and/or its proxies may be practicing drone operations in an effort to hone their skills and test America’s defenses in advance of future attacks on U.S. military bases and other important targets. These actors may be seeking to replicate Operation Spider’s Web, the sophisticated Ukrainian drone attack that destroyed several Russian long-range strategic bomber aircraft.²⁶



Conclusion

Iran and some of its supported terrorist organizations, criminal groups, and individual actors—working independently or in concert—could severely disrupt the U.S. economy, cause significant loss of life, and create chaos in the United States. Especially in the context of the continuing hostilities in the Mideast, Iran and its proxies could carry out attacks—including bombings, drone strikes, cyber attacks, terrorism, and other actions—to damage ports, bridges, highways, airports, railways, power generation stations, water supplies, and more. Likewise, they could seek to assassinate Federal, state and local government officials and other noteworthy public figures.

The potential implications of Iranian or Iranian-sponsored and -motivated attacks on America are significant:

- Such attacks could interfere with local, regional and national transportation systems, slow the supply of consumer goods thereby significantly damaging the U.S. economy, and cause other serious societal problems.
- 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, a successful effort to kill or debilitate only a few members of the majority political party could result in the minority party taking effective control of one or both houses. Such a scenario would likely inflame domestic tensions and could result in institutional gridlock that inhibits the ability to pass vital legislation.
- Attacks on airports, sea ports, and military bases could dramatically slow the flow of forces and equipment from the U.S. homeland in support of overseas military operations.
- Destructive cyber attacks could greatly damage various U.S. critical infrastructures and impact the livelihood and well-being of millions of Americans.
- The assassination of President Trump and one or more of his key advisors could seriously interfere with national-level decision making and would have profound political implications.
- An inwardly-focused America, forced to respond to a series of debilitating attacks in the homeland, could open the door to overt hostilities against U.S. friends, allies and interests across the globe by Russia, China, North Korea and other nations and terrorist groups and cause global upheaval on a scale not seen in decades. Our ability to respond in a timely and effective manner to foreign crises or conflicts, while U.S. military forces are engaged in operations in the Mideast and America is reeling from attacks on the homeland, could be severely tested.

To address these growing threats, Federal, state and local government organizations, and the U.S. private sector, must act expeditiously to strengthen America's homeland security and defense posture. This includes hardening U.S. critical infrastructures against cyber attacks;



INFORMATION SERIES

Issue No. 671 | October 13, 2026

implementing effective passive and active defenses against drone attacks; expanding law enforcement operations against known and suspected Iranian terrorists and their proxies; and strengthening intelligence collection and analysis of Iranian and other threats to the homeland.

¹ Christopher A. Williams, “The Coming War in America”, National Institute for Public Policy, *Information Series*, No. 650, February 10, 2026, <https://nipp.org/wp-content/uploads/2026/02/IS-650.pdf>.

² The White House, Press Release, March 2, 2026, <https://www.whitehouse.gov/releases/2026/03/the-iranian-regimes-decades-of-terrorism-against-american-citizens/>.

³ Kristin Shapiro, “The Iran Threat is Already Here,” *HSToday*, March 31, 2026, <https://www.hstoday.us/subject-matter-areas/counterterrorism/the-iran-threat-is-already-here/>.

⁴ “The Iran War and the Global Terrorism Threat, Global Terrorism Index 2026: Special Supplement,” Institute for Economics and Peace, Sydney, March 2026, <https://www.visionofhumanity.org/wp-content/uploads/2026/03/The-Iran-War-and-The-Global-Terrorism-Threat.pdf>.

⁵ Luke Barr, “Department of Homeland Security warns of potential attacks amid Iran operation,” *ABC News*, March 1, 2026, <https://abcnews.com/US/departments-homeland-security-warns-potential-attacks-wake-iran/story?id=130665784>.

⁶ Aaron Katersky and Josh Margolin, “Iran may be activating sleeper cells outside the country, alert says,” *ABC News*, March 9, 2026, <https://abcnews.com/US/iran-activating-sleeper-cells-alert/story?id=130897687>.

⁷ Amanda Macios, “Enemy within: Counterterrorism experts fear sleeper cells could be poised inside US,” *Fox News*, March 1, 2026, <https://www.foxnews.com/politics/after-u-s-israel-strike-kills-iranian-leaders-fbi-shifts-high-alert-home>.

⁸ “Summary of Iran-Related Terrorism Threat to the U.S. Homeland,” *Department of Homeland Security Bulletin*, January 18, 2020, <https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-18-2020>.

⁹ Kaelan Deese, “Pam Bondi says DOJ has ‘countless’ threat cases against the US amid Iran concerns,” *Washington Examiner*, June 24, 2025, <https://www.washingtonexaminer.com/news/3451597/pam-bondi-doj-countless-threat-cases-iran-concerns/>.

¹⁰ 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>.

¹¹ Ailin Vilches Arguello, “US Justice Department Warns of Threats to Jewish Targets as Concerns Mount Over Iranian Sleeper Cells,” *The Algemeiner*, June 26, 2025, <https://www.algemeiner.com/2025/06/26/us-justice-department-warns-threats-jewish-targets-concern-mounts-iranian-sleeper-cells/>.

¹² Department of Justice, “New Jersey Man Sentenced To 12 Years for Receiving Military-Type Training from Hezbollah, Marriage Fraud and Making False Statements,” May 23, 2023, <https://www.justice.gov/usao-sdny/pr/new-jersey-man-sentenced-12-years-receiving-military-type-training-hizballah-marriage>.

¹³ Statement of General Gregory Guillot, USAF, Commander, United States Northern Command and North American Aerospace Defense Command, before the Senate Armed Services Committee, March 19, 2026, https://www.armed-services.senate.gov/imo/media/doc/guillot_opening_statement1.pdf.

¹⁴ Connor Greene, “What Does the Iran War Mean for the Threat of Attacks in the US?,” *TIME*, March 14, 2026, <https://time.com/article/2026/03/13/iran-war-us-attacks-threat-cyberattacks-drones-terrorism-proxies/>.

¹⁵ Connor Greene, “What Does the Iran War Mean for the Threat of Attacks in the US?”; also see Josh Campbell, “US intelligence community ramps up warning of possible retaliatory attacks by Iran,” *CNN*, March 10, 2026, <https://www.cnn.com/2026/03/10/politics/us-intel-warning-retaliatory-attacks-iran>.



INFORMATION SERIES

Issue No. 671 | October 13, 2026

¹⁶ “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.

¹⁷ Department of Homeland Security, National Terrorism Advisory Bulletin, June 22, 2025, https://www.dhs.gov/sites/default/files/ntas/alerts/25_0622_S1_NTAS-Bulletin-508.pdf.

¹⁸ Caleb Holloway, “FBI releases details on motives in Michigan synagogue attack, confirmed act of terrorism,” *KATU.com*, March 30, 2026, <https://katu.com/news/nation-world/fbi-shares-new-info-on-investigation-into-michigan-synagogue-attack>.

¹⁹ Anti-Defamation League, “2024 Audit of Antisemitic Incidents,” April 22, 2025, <https://www.adl.org/resources/report/audit-antisemitic-incidents-2024>.

²⁰ Department of Homeland Security, “IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities,” December 18, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>.

²¹ Cybersecurity and Infrastructure Security Agency, “Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure,” April 7, 2026, https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a?utm_source=IranPLC202604&utm_medium=GovDelivery.

²² Cybersecurity and Infrastructure Security Agency, “Targeting Critical Infrastructure Programmable Logic Controllers,” July 22, 2026, <https://www.cisa.gov/news-events/news/cisa-fbi-epa-and-us-government-partners-update-warning-iran-affiliated-threat-actors-targeting>.

²³ See, for example, Howard Altman, “Drones Over U.S. Bases May Be Threatening Spy Flights: USNORTHCOM Commander,” *The War Zone*, February 13, 2025, <https://www.twz.com/news-features/drones-over-u-s-bases-may-be-threatening-spy-flights-northcom-commander>; and Howard Altman, “FAA Insider Opens Up About Drone Incursions Over Military Bases,” *The War Zone*, August 15, 2025, <https://www.twz.com/air/foreign-nexus-in-military-base-drone-incursions-detailed-by-government-insider>.

²⁴ Josh Margolin and Aaron Katsky, “‘Multiple waves’ or unauthorized drones recently spotted over strategic U.S. Air Force base, Lights on drones suggested the operators may be testing security responses,” *ABCNews.com*, March 20, 2026, <https://abcnews.com/International/multiple-waves-unauthorized-drones-spotted-strategic-us-air/story?id=131245527>.

²⁵ Josh Margolin, Aaron Katersky, Alex Stone and Luke Barr, “FBI warns Iran aspired to attack California with drones in retaliation for war: Alert,” *ABCNews.com*, March 11, 2026, <https://abcnews.com/US/story?id=130973820>.

²⁶ See, for example, Kateryna Bondar, “How Ukraine’s Operation ‘Spider’s Web’ Redefines Asymmetric Warfare,” Center for Strategic and International Studies, June 2, 2025, <https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare>.

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 Smith Richardson and Sarah Scaife Foundations 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/>.