

The Most Likely Threats Facing the United States: A Publicly Documented Assessment

Prepared by:

J.P. “Jim” Stephens, MSN, RN

National Administrator, U.S. Army Auxiliary Activation Project

In Collaboration With: AI-Enabled Research and Analytical Support Systems

Publicly released national-security assessments consistently point to three primary threat vectors likely to affect the United States in the near term: cyber and critical-infrastructure attacks, coercive or hybrid military actions by major-state adversaries, and transnational criminal or terrorist activity. These risks emerge from distinct actors—primarily China, Russia, Iran, and various non-state groups—and reflect major intelligence findings across the U.S. government.

Cyber and Critical-Infrastructure Attacks

Cyber operations targeting critical U.S. systems remain the most probable and persistent threat to the homeland. According to the 2025 Annual Threat Assessment of the U.S. Intelligence Community, the People’s Republic of China (PRC), the Russian Federation, and the Islamic Republic of Iran possess the capability and intent to compromise U.S. networks at strategic depth.¹ *The Department of Homeland Security’s Homeland Threat Assessment 2025* similarly warns that adversaries are increasingly positioned to disrupt sectors such as telecommunications, energy, finance, transportation, and healthcare.²

Recent public reporting further reflects this trend. For example, Chinese-linked actor “Salt Typhoon” infiltrated multiple U.S. telecommunications systems, demonstrating both capability and willingness to penetrate critical infrastructure.³ Such intrusions may serve intelligence collection, coercive leverage, or pre-positioning for potential conflict escalation.

Given the maturity of these adversarial cyber programs and the vulnerability of many U.S. legacy systems, most analysts consider the likelihood of disruptive or damaging cyber operations against the United States to be **HIGH!**

Coercive or Hybrid Military Actions by Major-State Adversaries

Although a large-scale direct attack remains less probable in the short term, the United States faces a measurable risk of hybrid or limited military actions involving China, Russia, Iran, or North Korea. These actions could target U.S. forward bases, military assets in contested regions, or U.S. allies and partners in ways that threaten American strategic interests.

The Defense Intelligence Agency’s 2025 Worldwide Threat Assessment notes that global strategic competition is intensifying and that the U.S. homeland is increasingly exposed to

growing long-range capabilities among near-peer adversaries.⁴ Additionally, public reporting reflects unprecedented operational coordination among China, Russia, Iran, and North Korea.⁵

The PRC, in particular, possesses the full spectrum of capabilities required to strike U.S. forces or disrupt American military logistics across multiple domains, including space and cyberspace.⁶ These dynamics elevate the risk of coercive military action—either as part of regional conflicts (e.g., Taiwan, the Middle East, Eastern Europe) or as calibrated tests of U.S. resolve.

The overall likelihood of such events is **MODERATE TO HIGH**, depending on regional triggers, miscalculation, and geopolitical developments.

Transnational Crime, Illicit Trafficking, and Non-State Terrorism

The United States also faces a continuously evolving threat from transnational criminal organizations, terrorist networks, and hostile non-state actors. These groups may operate independently or with tacit support from state sponsors, especially Iran and its proxy networks.

The Center for Strategic and International Studies, summarizing U.S. intelligence testimony, notes that synthetic-opioid trafficking—primarily driven by Mexico-based cartels—kills more Americans annually than foreign terrorist attacks and represents one of the greatest immediate threats to U.S. domestic stability.⁷ Meanwhile, DHS emphasizes that lone-offender terrorism, foreign-inspired violence, and ideologically motivated actors remain capable of carrying out attacks within the homeland.⁸

While the damage from such incidents varies widely, their frequency and persistence make them moderately likely, with significant cumulative impact on public safety and national resilience.

Conclusion

Publicly documented assessments converge on a clear pattern: the United States is most likely to face cyber disruption, coercive hybrid actions by state adversaries, and persistent threats from transnational criminal and terrorist networks. These risks do not exist in isolation, and adversaries often combine digital, informational, and kinetic tools to exploit vulnerabilities across government, industry, and civil society.

Understanding these threats is critical for homeland security, defense planning, and the development of resilient civilian-military structures—including emerging initiatives designed to enhance national preparedness and surge capacity.

Notes (with links to references)

1. Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community 2025. Retrieved from:
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf?utm_source=chatgpt.com
2. U.S. Department of Homeland Security, Homeland Threat Assessment 2025. Retrieved from: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf?utm_source=chatgpt.com
3. “Salt Typhoon,” Wikipedia, accessed 2025. Retrieved from:
https://en.wikipedia.org/wiki/Salt_Typhoon?utm_source=chatgpt.com
4. Defense Intelligence Agency, 2025 Worldwide Threat Assessment: Statement for the Record. Retrieved from:
https://armedservices.house.gov/uploadedfiles/2025_dia_statement_for_the_record.pdf?utm_source=chatgpt.com
5. Craig McCarthy, “Spy Agencies Warn Russia, Iran, China and North Korea Are Teaming Up Against US Like Never Before,” New York Post, March 25, 2025. Retrieved from:
https://nypost.com/2025/03/25/us-news/spy-agencies-warn-russia-iran-china-and-north-korea-are-teaming-up-against-us-like-never-before/?utm_source=chatgpt.com
6. Idrees Ali and Patricia Zengerle, “China Presents Top Military, Cyber Threat to United States, US Report Says,” Reuters, March 25, 2025. Retrieved from:
https://www.reuters.com/world/china-presents-top-military-cyber-threat-united-states-us-report-says-2025-03-25/?utm_source=chatgpt.com
7. Center for Strategic and International Studies, “What Happened at the Trump Administration’s Annual Threat Assessment Hearing?” Retrieved from:
https://www.csis.org/analysis/what-happened-trump-administrations-annual-threat-assessment-hearing?utm_source=chatgpt.com
8. Department of Homeland Security, Homeland Threat Assessment 2025. Retrieved from:
https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf?utm_source=chatgpt.com