

U.S. Domestic Threat — Track Reference

The eight standing tracks, their documented cases, and current status · Verified through Sep 19, 2026

How to read this. Each track below is checked on both daily briefings. "No new developments" means the sources were pulled and returned nothing — it is not a claim that nothing happened. Court records, indictments and official releases are the primary evidence; treat anything else as allegation.

(a) Iran / Hezbollah U.S. Networks

Case	Detail
Asif Merchant Convicted Mar 6, 2026 · Brooklyn	Trained IRGC operative sent to the U.S. to recruit "stay-behind" agents. 2024 mission: recruit criminals to steal documents, stage a protest and murder a U.S. government official or politician. Arrested before leaving. Faces life
Mohammad Baqer Saad Dawood Al-Saadi Indicted May 28, 2026 · Manhattan	Kata'ib Hezbollah commander; self-described "like a son" of Qasem Soleimani. Directed 18 attacks across Europe in three months. Discussed attacking New York, California and Arizona ; urged killing Americans and Jews
Murder-for-hire vs. journalist Masih Alinejad	Multiple convictions in Brooklyn and Staten Island; two Russian organized-crime figures received 25 years. Dissidents on U.S. soil are a standing target set
Tennessee facilitator, guilty plea Apr 13, 2026	Domestic extremist provided a purported Hezbollah contact a list of 35,000 people affiliated with Israel — proof the network recruits outside its own ranks
17 Iranians charged, Aug 18, 2026	Cyber-theft campaign conducted for the IRGC

Cities of record: New York, California, Arizona, Washington D.C. · **Current status:** no new case in feeds reached Sep 19.

(b) Russian Hybrid Operations

- **Assassination and intimidation:** DOJ charged five people working for Russian intelligence with murder-for-hire and terrorism financing, including a plot to kill a Russian dissident living in the U.S. (Sep 15–16, 2026).
- **Undersea cables:** U.S., UK and Norwegian forces disrupted a covert Russian deep-sea directorate exercise rehearsing the capability to disable subsea cables without leaving a trace. Target link carried NASA-linked satellite data.
- **NATO airspace:** drone attack on Leipzig airport; drone incursion over Lithuania; Russian frigate fired flares at a Danish helicopter; French critical infrastructure ordered protected.
- **Cyber:** AI-accelerated espionage using automated operations, self-rewriting malware and WhatsApp companion-device hijacking; over 20 organizations, including people connected to U.S. foreign policy.
- **Sanctions:** the *Lindsey O. Graham Sanctioning Russia and Iran Act of 2026*, signed Sep 18 — 100% tariffs authorized on the five largest buyers of Russian energy, plus shadow-fleet and leadership sanctions. Watch China, India, Turkey, Hungary.

Recruitment method to understand: operators are hired over messaging platforms — petty criminals, migrants, teenagers — paid small sums to set fires, fly drones or photograph facilities. Many do not know who is paying. This is why "sleeper cell" is the wrong mental model.

(c) China Pre-Positioning

Program	Purpose and sectors
---------	---------------------

Volt Typhoon	Pre-positioned access in communications, energy, transportation and water systems across the continental U.S. and Guam. U.S. agencies assess with high confidence the intent is to disrupt in a crisis, not to spy. Living-off-the-land tradecraft and hijacked home routers
Salt Typhoon	Compromise of U.S. telecom carriers reaching lawful-intercept systems. The CIA's deputy director said in Sep 2026 it remains a real threat. T-Mobile physically cut a cable to expel the intruders
Fire Ant	Access to core routers, authentication servers and management hosts; hidden tunnels and suppressed security logs

Policy marker: the U.S. banned new foreign-made consumer routers in March 2026 because hijacked routers are the relay network. **Current status:** no new disclosure in feeds reached Sep 19.

(d) Jewish-Community Threat

- **Europe:** Sweden expelled an Iranian embassy employee over operations against Jewish and Israeli interests — including working with criminals. Germany arrested a synagogue arsonist; a woman wearing a Star of David was attacked with a broken bottle in Berlin.
- **U.S. plots:** Al-Saadi's attempted attacks in New York City and discussions naming California and Arizona; the Tennessee 35,000-name target list.
- **Travel and street:** assaults on Jews leaving services in Barcelona, Israeli tourists beaten in Montenegro, an axe attack on Israelis, hotels and parks refusing entry to Israelis.
- **Holiday windows:** **Yom Kippur Sep 20–21, 2026** and **Sukkot immediately following** are the highest-risk periods. Historically, Iran-linked and lone-actor plots cluster on Jewish holidays.

(e) Taiwan Strait Trigger

Rating	Means
GREEN	Routine gray-zone activity only
AMBER	A named exercise, a record incursion, or blockade language
RED	Live-fire encirclement, a boarding or seizure, or a declared quarantine

Current rating: AMBER — on political grounds only. No named PLA exercise, no live-fire zone, no blockade or quarantine language, and no Coast Guard boarding reported. This rating ties directly to track (c): a Strait crisis is the moment pre-positioned cyber access becomes usable.

Known blind spot. Taiwan's Ministry of National Defense site is unreachable — the English page returns 404, the daily activity page is JavaScript-rendered so automated retrieval returns no article text, and browser access to the domain is blocked. **The daily PLA aircraft and vessel tally therefore comes from Taipei coverage, not the source.** When the tally cannot be obtained, the briefing says so and does not guess a number.

Working military read: Japan Ministry of Defense Joint Staff press releases — mod.go.jp/js/press/index.html (Japanese; search 中国, 空母, ロシア, 共同訓練). This is the best open-source read on PLA carrier and aircraft movement through the first island chain.

(f) Strait of Hormuz & Energy Security

- **IRGC official threatened to block regional countries' oil exports** if Iran's own exports are halted, and urged stronger Iranian control of the Strait.

- **U.S. sanctioned an Iranian crypto exchange** accused of processing payments for "safe passage" through the Strait — evidence of an actual toll economy at the chokepoint.
- **Cyberattacks on two Texas-bound tankers.** The Coast Guard and FBI boarded both. The Coast Guard confirmed evidence of malicious cyber activity on the **VL Prosperity**. **No U.S. attribution has been issued** — Iranian media alleged engine-system breaches, which is a claim, not a finding.
- **Riyadh air-raid alerts** and explosions — the first time the escalation has triggered civil-defense alerts in the Saudi capital.

|(g) Japan / Indo-Pacific

- **PM Sanae Takaichi** travels to the U.S. from Mon Sep 21 and addresses UNGA; meetings with foreign leaders including President Trump are under arrangement. Cabinet support rose to 53% after her first reshuffle.
- **Japan MOD PLA disclosures** are the primary military read: Luyang III and Jiangkai II transits through Amami Oshima–Yokoto and Osumi Strait (Sep 16), a Dongdiao-class intelligence ship (Sep 14), Y-9 electronic-warfare sorties (Sep 3, 4, 7, 9), and recurring China–Russia joint patrols (Jul 21, 25, 29).
- **Watch:** Japan–China diplomatic friction, Japan's counterstrike capability milestones, U.S.–Japan cost-sharing, and Philippines basing moves.

|(h) AI Security & the AI-Incident Lane

- Frontier-lab disclosures and model-exploit reports
- AI-enabled attacks and autonomous agent breaches
- Regulator filings — the first agentic AI data breach reported to a national data-protection authority is the leading edge
- AI product vulnerabilities, and supply-chain attacks on AI development tooling