INTELLIGENCE SUMMARY (INSUM)

THREAT ASSESSMENT: IRAN & TERROR GROUPS OSINT-25-002-TA-IRN

DISTRIBUTION:
RELEASE FOR PUBLIC USE

23 JUNE 2025

INSUM REPORT | United States of America (USA) and Worldwide

THREAT ASSESSMENT – IRAN, ITS PROXIES, AND ALIGNED TERRORIST ORGANIZATIONS

THREAT ASSESSMENT | TERRORISM & CRIME

The Current and Escalating Threats and Violence With Iran: Implications for U.S. Citizens at Home and Abroad – June 2025

Following the escalation in hostilities between the United States and the Islamic Republic of Iran—specifically U.S. military strikes on Iran's nuclear infrastructure in June 2025—Iran and its network of aligned non-state actors have begun executing asymmetric and retaliatory operations targeting U.S. interests worldwide. This includes cyberattacks, political threats, propaganda campaigns, and proxy military activity. Iran's broader strategic doctrine—centered around deterrence through proxy warfare and plausible deniability—is likely to intensify in both digital and physical domains.

As the IRGC and Quds Force mobilize regional and global allies including Hezbollah, the Houthis, Hamas, Palestinian Islamic Jihad, and various Shi'a militias in Iraq and Syria, the threat to U.S. citizens, diplomats, businesses, and infrastructure has grown significantly. This assessment aims to outline the current security climate, project potential threat trajectories, and provide decision-makers and stakeholders with a structured Most Likely and Most Dangerous Course of Action (MLCOA/MDCOA) model for contingency planning.

Current Events & Escalations *(as of June 2025)*

1. Direct U.S.-Iran Escalation

- **Precision U.S. airstrikes (June 2025)** targeted Iran's nuclear infrastructure—specifically facilities at Fordow, Isfahan, and Natanz—which were assessed by U.S. and Israeli intelligence to be nearing weapons-grade enrichment thresholds.
- Iran's Supreme Leader and IRGC commanders have **vowed retaliatory action**, both overt and through proxy warfare, promising "everlasting consequences" against the U.S. and its allies.

2. Proxy Militant Mobilization

- **Hezbollah and Kata'ib Hezbollah** have elevated their alert status. Hezbollah has redeployed fighters closer to the Israeli border while Kata'ib Hezbollah and other PMF elements in Iraq have threatened U.S. troops stationed in Erbil and Al-Asad Air Base.
- **Houthi rebels in Yemen**, aligned with Iran, have resumed maritime drone and missile strikes in the Red Sea targeting international shipping—raising insurance rates and impacting global trade.

- **Hamas and Palestinian Islamic Jihad**, both funded and armed by Iran, have continued coordinated operations with support from Iranian Quds Force liaisons, drawing in regional actors such as Jordan and Egypt.

3. Cyber Warfare Surge

- **Iranian APT groups (Advanced Persistent Threats)** including APT33, APT34, and the "CyberAv3ngers" have launched:
  - **Phishing and ransomware campaigns** targeting U.S. public utilities, municipal services, and healthcare systems.
  - **DDoS attacks** on Israeli and U.S. financial institutions and telecommunications providers.
  - A **destructive malware attack** was detected targeting U.S. pipeline logistics, although it was thwarted early by CISA and private-sector cybersecurity partnerships.
- Reports indicate Iran is testing **AI-powered cyber payloads** for disinformation and psychological operations to manipulate U.S. public opinion.

4. Terrorist Messaging & Activation

- Intelligence intercepts suggest **increased chatter between IRGC-QF handlers and operatives in Lebanon, Syria, and Latin America** (notably Venezuela and Paraguay), with discussions of targeting Western interests.
- **"Sleeper cell activation" risk** is elevated: Pro-Iranian operatives or radicalized sympathizers within the West may receive financial support or ideological justification to carry out lone-wolf or coordinated attacks.
- Open-source social media accounts linked to Hezbollah and Iranian-affiliated clerics are broadcasting **calls to martyrdom and retaliation** specifically naming American targets in Baghdad, Dubai, and the U.S. homeland.

5. DHS & Global Alerts

- The U.S. Department of Homeland Security (DHS) and State Department have issued:
  - A **“Worldwide Caution” advisory** for U.S. travelers abroad due to elevated risk of abduction, embassy bombings, and armed assaults.
  - A **Joint Intelligence Bulletin (JIB)** with the FBI identifying potential threats to Jewish and Iranian-American communities within the U.S.
- Several allied nations (UK, Germany, Canada) have **increased security postures** at airports, embassies, and government buildings citing credible threats from Iranian-linked actors.

6. Strategic Alliances & Escalation Indicators

- Iran has strengthened **military and intelligence-sharing with Russia and China**, potentially seeking diplomatic and technological backing in the event of a wider conflict.
- Reports suggest Iranian advisors and drones are operating within **Latin American narco-terrorist networks**, creating **a possible southern border threat vector** via proxy infiltration or smuggling of materials.
- **Increased coordination with Shi’a militias in Afghanistan and Pakistan** could enable indirect threats to U.S. interests in South and Central Asia.

Threats to U.S. Citizens Overseas

Threat Overview

- **Kidnappings, hostage-taking**: Iran-backed proxies may attempt abductions of U.S. citizens or dual nationals in regions like the Middle East (Lebanon, Syria) and North Africa.
- **Armed attacks** on consulates, embassies, and U.S. personnel by proxies or sleeper agents; detonations, IEDs, drones, and ballistic missiles are credible risks.
- **Demonstrations turning violent**: Iranian and anti-U.S. protests abroad risk targeting American tourists and businesses—especially in volatile countries.
- **Cyber threats**: Travelers and expats in hostile zones could be targeted by phishing, malware, or broader network disruptions aimed at sowing confusion.

MLCOA (Most Likely Course of Action)

- **Non-lethal harassment or surveillance**: Demonstrations, local harassment, or minor violent acts (e.g., vandalism, low-grade IEDs) around U.S. facilities and tourist zones.
- **Limited kidnapping attempts** by proxies seeking political leverage—but unlikely to result in mass abductions.
- **Cyber espionage/attacks** on U.S. nationals abroad via compromised free Wi-Fi, phishing, and spoofed apps.

MDCOA (Most Dangerous Course of Action)

- **Coordinated terrorist attack**—e.g., suicide bombing or armed assault targeting U.S. embassy/consulate or American tourist gathering.
- **High-profile hostage scenario** involving dual-nationals or Americans staged by Iran or Lebanese Hezbollah to force diplomatic concessions.
- **Ballistic missile/drone strike** on U.S. military evacuation flights or transit hubs near or around American congregations.

Threats to U.S. Citizens in the United States

Threat Overview

- **Cyberattacks**: Iran-linked state hackers or hacktivists likely to mount disruptions to critical infrastructure—energy, water, telecom—even if precision sabotage is unlikely.
- **Assassination plots**: Historical precedent—IRGC-sponsored murder-for-hire targeting U.S. political, Jewish-American, or Iranian diaspora figures fbi.gov.
- **Violent extremism**: Inspired acts by anti-Israel or anti-Iran individuals or groups (white supremacists, radical Islamists) leading to hate crimes, shootings, or IEDs in communities or at symbolic sites.

MLCOA

- **Low-level cyber intrusions** disrupting local infrastructure or informational integrity via DDoS, phishing campaigns, and ransomware.
- **Anti-Israel or anti-Muslim hate incidents**, such as vandalism or minor assaults against places of worship and community centers.
- **Foiled domestic plots**: Law enforcement likely to intercept low-tech attempts (e.g., pipe bombs, small arms attacks) inspired by international events.

MDCOA

- **Successful foreign-directed assassination attempt** on a U.S. political leader, dissident, or media personality linked to Iranian policy or culture.
- **Large-scale cyberattack** severely disrupting critical U.S. infrastructure (power grid, water, telecom), triggering social turmoil or even casualties.
- **Mass-casualty domestic terror attack** (e.g., targeting airports, government buildings, large public venues) orchestrated by an Iran-aligned extremist or proxy sleeper cell.

MLCOA vs MDCOA Summary Table

Threat Environment	MLCOA	MDCOA
Overseas	Harassment, protests, kidnappings, cyber espionage	Embassy attacks, mass hostage-taking, missile/drone assault
Domestic (U.S.)	Cyber nuisance, hate incidents, small plots thwarted	Foreign-directed assassination, infrastructure takedown, mass-casualty terror

Recommended Mitigations

- **Stay informed & avoid hotspots**: Register with STEP; avoid protests near U.S. facilities abroad.
- **Cyber hygiene**: Use VPNs, MDM policies, keep contacts secure, monitor for suspicious activity.
- **Physical awareness**: Increase vigilance near synagogues, mosques, consulates, and gatherings prone to violence.
- **Community reporting**: “If you see something, say something”—report suspicious behavior or online threats.
- **Emergency contingency planning**: Embassy evacuation protocols, ransom/hostage contingency policies, domestic shelter-in-place plans.

Assessment. The confluence of geopolitical escalation, proxy mobilization, and cyber warfare has elevated the threat environment to **a sustained high-risk posture** for U.S. citizens, both overseas and domestically.

Key Assessment Highlights:

- **Iran's Doctrine of Asymmetric Warfare** is fully in motion. Direct conventional retaliation by Iran is unlikely, as Tehran seeks to avoid full-scale war with the U.S. Instead, retaliation is unfolding through third-party militant groups, cyber disruption campaigns, and covert operations.
- **Cyber threats are the most scalable and likely vector for Iranian action** against U.S. interests. Iran has both the capability and intent to wage prolonged cyber and information warfare campaigns that could degrade public confidence, disrupt daily life, and sow political discord.
- **Proxy actors are likely to act independently but with Iranian support**, giving Tehran plausible deniability. This includes potential attacks on soft targets (e.g., hotels, transport hubs, embassies, or symbolic cultural/religious sites).

- **Domestic threats may manifest through lone-wolf attackers**, radicalized by Iranian propaganda or influenced by global events. The targeting of high-profile political figures, members of the Iranian diaspora, or Jewish/Israeli-American communities remains a key concern.
- **Strategic global realignment is a wildcard.** Iran's strengthening ties with Russia, China, and non-state entities in Latin America and Africa increase the possibility of **multi-domain, multi-theater threats**. This includes smuggling networks, foreign espionage, and potentially the covert movement of operatives or materials through U.S. borders.
- **Psychological operations (PSYOP) and disinformation** are intensifying. AI-generated deepfakes, fake news, and amplified conspiracy theories targeting elections, U.S. foreign policy, and national unity are already surfacing in hostile online environments, magnifying public distrust.

Strategic Outlook

Dimension	Short-Term (0–3 months)	Medium-Term (3–12 months)	Long-Term (12+ months)
Cyber Threat	Persistent phishing, DDoS, ransomware attacks	ICS/SCADA targeting; cyber-espionage	Infrastructure disruption, supply chain warfare
Physical Threat	Protests, soft target attacks abroad	Proxy strikes on U.S. embassies or forces	Large-scale or coordinated proxy terror plots
Domestic Risk	Hate crimes, isolated radicalized actors	Attempted assassinations, domestic terror	State-sponsored plots or critical infrastructure threats
Political Risk	Dis-info/PSYOP around elections	Global diplomatic backlash, sanctions tit-for-tat	Strategic erosion of Western alliances & deterrence

The escalations from recent U.S. strikes on Iran's infrastructure are heightening multi-domain threats—from kinetic actions by proxies to cyberattacks and strategic influence operations. While law enforcement and intelligence agencies are on heightened alert, the complexity of overseas and domestic threat vectors—especially asymmetric and cyber tools—calls for robust, multi-layered readiness.

Approved by:

G2 Department, Intelligence
Paladin Defense Group, Inc.
Headquarters, USA

Open-Source Intelligence (OSINT) Reporting
Unclassified (UNCLAS) (FOUO)