JOINT ADVISORY

TLP: CLEAR

Middle East Conflict and Critical Infrastructure

March 2026

INTRODUCTION

The conflict in the Middle East has security implications for critical infrastructure sector owners and operators across the globe. One potential threat is increased cyberattacks from Iranian state-sponsored actors, hacktivists, and cybercriminal groups aligned with Iran. Since Iran has launched cyberattacks during similar times of conflict, organizations should be prepared for the possibility of increased attacks. Additionally, there is a potential for physical attacks, which could be committed by homegrown violent extremists (HVEs) and include targets like public spaces and critical infrastructure entities.

Members of the National Council of ISACs (NCI) have collaborated on this joint bulletin to raise awareness across the critical infrastructure community of this common threat to critical infrastructure and global business more generally. Please note that any ISAC's participation in this advisory is not an indication that the ISAC or its individual members are experiencing increased threat actor activity.

TOP IRANIAN STATE SPONSORED CYBER THREAT ACTORS / GROUPS

Iran is a formidable adversary, hosting several prominent threat actors with a broad range of geopolitical objectives, including disruptive and destructive attacks, cyber espionage, and financially motivated cybercrime, at times collaborating with ransomware actors. Among the more proficient state-sponsored threat groups are:

- **Charming Kitten (APT35, Phosphorous)** is known for extensive spearphishing campaigns against U.S. political entities, military, and commercial facilities. The group also carries out cyber espionage to assist Iran in its geopolitical goals. Using social engineering, Charming Kitten commonly impersonates legitimate individuals such as journalists, researchers, and government officials to build trust. They will then lure victims to fake login pages for email or conference invites to steal credentials.
- **APT33 (Elfin)** is known for significant attacks on critical infrastructure, typically in the energy and aviation sectors in the U.S. and other Western countries. APT33 uses spearphishing in combination with malicious attachments, often luring victims with job opportunities or geopolitical topics, or masquerading as legitimate businesses via typosquatted domains. They also leverage password spraying to prey on accounts with weak authentication, and have been known to leverage zero-day vulnerabilities in IT products.
- **MuddyWater (APT37, Seedworm)** focuses on espionage, targeting a broad range of sectors, including government, defense, energy, telecommunications, and finance. They have conducted attacks in the Middle East, Asia, Africa, Europe, and North America. This group gains initial access primarily through spearphishing campaigns, delivering malicious attachments or links to targeted victims. In addition to developing custom malware to assist in their operations, MuddyWater typically leverages publicly known vulnerabilities and open-source tools to gain initial access and maintain persistence.
- **OilRig (APT34)** specializes in cyber espionage and intelligence gathering. While the threat actor has historically targeted critical infrastructure in the Middle East, their operations have extended to other regions, including the U.S. The group leverages spearphishing attacks, including LinkedIn phishing, to gain initial access and develops custom malware and exploits publicly known vulnerabilities. Notably, OilRig is known for leveraging compromised organizations to launch supply chain attacks against its primary targets.
- **Pioneer Kitten (Fox Kitten, UNC757)** is known for targeting critical infrastructure sectors across the U.S. They are notable for their focus on network infrastructure, exploiting VPN vulnerabilities (particularly in Pulse Secure, Citrix, and F5 devices) to establish persistent footholds. They have also been documented collaborating with ransomware affiliates and selling network access to other threat actors, making them a unique hybrid of espionage and financially motivated activity.

NON-STATE CYBER THREAT ACTORS TO WATCH

The distinction between hacktivists and state-sponsored threat actors is not always obvious. Many Iranian hacktivist groups are believed to have direct or indirect ties to the Islamic Revolutionary Guard Corps (IRGC) or other government entities. It is therefore not surprising that these hacktivist groups are closely aligned with the Iranian government's interests. Hacktivist group activity ranges from destructive attacks and data theft to more nuisance attacks, such as DDoS attacks and website defacements.

- **Cyber Av3ngers (Sandcat)** has emerged as a significant threat to industrial control systems (ICS) and operational technology (OT) environments. The group tends to focus on ICS/SCADA-facing devices exposed to the internet, often exploiting default credentials and known vulnerabilities in industrial equipment. During the June 2025 Israel-Palestine conflict, CyberAv3ngers targeted Unitronics Vision Series programmable logic controllers (PLCs) used in various critical infrastructure industries. They exploited internet-accessible devices with default or no passwords (often communicating via the default TCP port 20256). In total, they compromised at least 75 devices.
- **Handala Group (Void Manticore)** has a strong focus on psychological operations and hack-and-leak campaigns. Handala primarily targets Israeli organizations, including organizations that support or conduct business within Israel. The group's primary initial access method relies on phishing, including SMS phishing (also referred to as smishing), where they masquerade as legitimate organizations offering support or solutions, with malicious links or attachments. Recent activity has shown a noticeable focus on supply-chain footholds — targeting IT and service providers to reach downstream victims. Notably, Check Point Research observed Handala campaigns originating from Starlink IP ranges and probing externally facing apps for misconfigurations and weak credentials. The group has announced that it will be intensifying operations due to the death of Ayatollah Ali Khamenei.
- **Cyber Islamic Resistance (Team 313/ CIR)** is a loosely coordinated umbrella collective operating within Iran's broader hacktivist proxy ecosystem. The collective recently began recruiting fellow hacktivists to better coordinate disruptive cyber campaigns. Iranian cyber proxies operating under the CIR banner claim interference across targets in the Middle East, the U.S., and parts of Asia. CIR is best characterized as a coordination mechanism rather than a single cohesive threat actor. The group was responsible for attacking at least nine health sector organizations in the 12-day war between Israel and Iran in June 2025.
- **The FAD Team (Fatimion Cyber Team)** is operating within Iran's broader proxy cyber ecosystem. The group is composed of pro-regime actors with a primary focus on wiper malware and permanent data destruction. The FAD Team has conducted global SQL injection campaigns, targeting a diverse range of victims, including military-affiliated organizations and educational institutions across multiple countries. On the ICS/OT front, the FAD Team has claimed responsibility for gaining unauthorized access to SCADA and PLC systems across multiple countries.

- **DieNet (DieNet v2 / v5)** is a decentralized hacktivist group that targets Israel and its allies. The group primarily uses DDoS attacks, but has also been observed conducting website defacements and data breaches. The group has been highly active since Operation Epic Fury began on February 28.

RISK ANALYSIS

For several days following the outbreak of the conflict, there was a noted decrease in cyber threat activity emanating from Iran. This could be caused by several factors, including a breakdown in command and control, cyber threat actors being reassigned to other responsibilities, and effective offensive cyber operations by the U.S. and Israel. However, there are signs of life in Iranian offensive cyber operations. In addition, there are confirmed disruptions to cloud services resulting from a kinetic attack, demonstrating, yet again, but in a new way, how physical security incidents can cause cyber impacts.

As an additional concern, we are seeing indications that Russia-affiliated actors are beginning to potentially align with Iranian actors. During the 12-day war between Israel and Iran in June 2025, Russian hacktivists were observed attacking Israeli critical infrastructure organizations. One example of this was the group Server Killers attacking Israeli health delivery organizations in response to the strikes on Iranian nuclear infrastructure.

Due to the current and similar ongoing situation, it is likely that this activity will also be prevalent throughout the 2026 conflict. In fact, the Russian hacktivist group NoName057(16) was observed attacking Israeli organizations with DDoS attacks on March 04, 2026. As the conflict continues, other Russian hacktivist groups may join the fray, exacerbating the existing risk to critical infrastructure organizations.

Physical Risk

The threat of targeted physical attacks in the U.S. homeland is a concern. Individuals in the U.S. may be motivated to mobilize to violence in response to U.S. and Israeli military operations. Notably, on March 1, two top Iranian religious leaders issued separate fatwas calling on Muslims worldwide to take revenge for the killing of the Iranian Supreme Leader. This increases concerns about U.S.-based homegrown violent extremists who are motivated by foreign terrorist organizations or Iran's Islamic Revolutionary Guard Corps (IRGC).

Historically, HVEs are often motivated to action by flashpoints, including geopolitical events. They often use simple tactics and readily available weapons such as firearms, vehicles, edged weapons, incendiary devices, or improvised explosive devices. Violent extremists typically target symbolic sites or events, which could include religious organizations, large public gatherings, government facilities, or critical infrastructure. For example, the perpetrator of the mass shooting attack at a bar in Austin, Texas, on March 1 is being investigated as potentially being motivated by the Middle East conflict.

In addition to lone actors mobilizing independently to commit acts of violence, U.S. officials have expressed concerns about the potential risk from Iranian "sleeper cells." The IRGC released a statement warning that "the enemy…will no longer have security anywhere in the world, even in their own homes." Federal and local law enforcement have boosted on-the-ground security in major U.S. cities as part of a precautionary posture, even though no specific, credible threats have been publicly identified.

MITIGATIONS

Companies are encouraged to adopt a thoughtful, comprehensive cybersecurity strategy that enables them to allocate limited resources most effectively. Companies worldwide should prepare for the likelihood of increased activity by Iranian-aligned actors. This includes understanding dependencies within your organization and developing continuity plans in case of a disruption to your operations or those of a critical supplier or partner.

Based on commonly seen cyber TTPs deployed by Iranian actors, companies are specifically encouraged to:

- Increase monitoring for spearphishing and credential theft.
- Review DDoS mitigation playbooks, and ensure response partners are on standby.
- Validate backup and recovery processes for critical systems, especially in their communications infrastructure.
- Remain vigilant for signs of supply chain compromise or attempts to leverage trusted relationships for lateral movement.
- Enable multi-factor authentication (MFA) wherever possible.

Amid this heightened threat environment, critical infrastructure organizations can take concrete steps to strengthen their physical security and reduce their vulnerabilities, which include but are not limited to:

- Join an information-sharing community.
- Conduct a risk and vulnerability assessment.
- Document emergency response plans, policies, and procedures.
- Exercise emergency response plans and other security contingencies.
- Conduct awareness training on the threats and risks facing critical infrastructure.
- Network with neighboring infrastructure entities and local law enforcement.

CONCLUSION

The threat environment is likely to remain highly volatile. Now is the time for companies to become familiar with Iranian-affiliated threat actors and their TTPs, test and assess their cybersecurity posture, strengthen their defenses, increase monitoring for suspicious activity, and remind employees to report suspicious emails and links. Preparedness is critical to resilience. Even attacks that do not directly target the U.S. could have cascading effects and disrupt U.S. companies. Given the interconnectedness of networks, it is possible that cyberattacks targeting Israel itself could cause collateral damage to U.S. companies, even if the U.S. companies themselves are not the intended targets.

Consider joining your sector-specific ISAC. ISACs are a cost-effective supplement to corporate security and cybersecurity teams, connecting peer analysts around common threats and enabling the kind of trusted, voluntary collaboration that makes the whole sector stronger. Voluntary collaboration with industry peers is invaluable, and it is never too late to join and engage.

THREAT REPORTS AND RESOURCES

Cybersecurity Resources

- CISA Iran Overview and Threat Advisories
  - https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran

- What Defenders Need to Know about Iran's Cyber Capabilities
  - https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/

- Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest
  - https://www.cisa.gov/sites/default/files/2025-06/joint-fact-sheet-Iranian-cyber-actors-may-target-vulnerable-US-networks-and-entities-of-interest-508c-1.pdf

- Situation Report: Middle East Escalation
  - https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026

- Cyber Threat Bulletin: Iranian Cyber Threat Response to US/Israel strikes
  - https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026

- Escalation in the Middle East: Tracking "Operation Epic Fury" Across Military and Cyber Domains
  - https://flashpoint.io/blog/escalation-in-the-middle-east-operation-epic-fury/

- Iranian Use of Cybercriminal Tactics in Destructive Cyber Attacks: 2026 Updates
  - https://www.halcyon.ai/ransomware-alerts/iranian-use-of-cybercriminal-tactics-in-destructive-cyber-attacks-2026-updates
- Alert: NCSC Advises UK Organisations to Take Action Following Conflict in the Middle East
  - https://www.ncsc.gov.uk/news/ncsc-advises-uk-organisations-take-action-following-conflict-in-middle-east
- Inside the Shadows: Understanding Active Iranian APT Groups
  - https://www.picussecurity.com/resource/blog/understanding-active-iranian-apt-groups
- Ongoing Iran Conflict: What You Need to Know
  - https://www.recordedfuture.com/blog/ongoing-iran-conflict-what-you-need-to-know
- Seedworm: Iranian APT on Networks of U.S. Bank, Airport, Software Company
  - https://www.securityweek.com/iranian-apt-hacks-us-airport-bank-software-company/
- SentinelOne Intelligence Brief: Iranian Cyber Activity Outlook
  - https://www.sentinelone.com/blog/sentinelone-intelligence-brief-iranian-cyber-activity-outlook/
- Iran War vs. Israel & U.S. Cyber Reflections
  - https://socradar.io/blog/cyber-reflections-us-israel-iran-war/
- Cyber Advisory: Increased Cyber Risk Amid U.S.–Israel–Iran Escalation
  - https://www.sophos.com/en-us/blog/cyber-advisory-increased-cyber-risk-amid-u-s-israel-iran-escalation

Physical Security Resources

- Operation Epic Fury: Potential Iranian Cyber Counteroffensive Operations
  - https://www.tenable.com/blog/operation-epic-fury-potential-iranian-cyber-counteroffensive-operations
- Could Iran attack on U.S. soil? "It is an all-hands-on-deck moment," security analyst says
  - https://www.cbsnews.com/news/could-iran-attack-us-homeland/
- Iran and Terrorism: What the U.S. Strikes Could Mean for Homeland Security
  - https://www.cfr.org/articles/iran-and-terrorism-what-the-u-s-strikes-could-mean-for-homeland-security
- Tehran’s Homeland Option: Terror Pathways for Iran to Strike in the United States
  - https://ctc.westpoint.edu/tehrans-homeland-option-terror-pathways-for-iran-to-strike-in-the-united-states/