



| Flash |

Military Strikes on Iran – SITREP

#12: March 7, 2026

F-2026-03-07a

Classification: TLP:CLEAR

Criticality:HIGH

Intelligence Requirements: Geopolitics, Hacktivism, Cyberattacks

March 7, 2026

Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 07:45 AM (EST) on March 7, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | Military Strikes on Iran – SITREP #12: March 7, 2026

| Key Findings

- Iran’s president apologized to neighboring Gulf countries and approved the suspension of attacks against them, unless an attack on Iran comes from those countries, a move likely aimed to increase ceasefire pressure on the U.S. through energy price shocks and other economic disruptions.
- Public statements from U.S. President Donald Trump and military movements indicate the U.S. military campaign is likely escalating in the short term; and although Iran is signaling openness to certain concessions to end the conflict, the U.S. is insisting on Iran’s unconditional surrender, terms which Iran currently rejects.
- Iran claimed an attack on another oil tanker while the U.S. announced details of its insurance policy to restart traffic in the Strait of Hormuz (SoH). The U.S. policy will likely not deter Iranian aggression in the Strait as long as Iran maintains the ability to impact energy shipping, a key element of Iran’s strategy to end the conflict on terms it finds acceptable.

| Latest Details

On March 7, 2026, in a prerecorded address on state TV, Iran's President Masoud Pezeshkian apologized to neighboring countries that have been affected by their actions in the conflict.¹ Pezeshkian further stated that its temporary leadership council had approved the suspension of attacks against them unless an attack on Iran came from those countries.

- There is a roughly even chance this is an attempt by Pezeshkian to de-escalate the war and limit its potential adversaries. Iran is likely suffering firepower shortages, particularly for ballistic missiles, and limiting attacks will likely preserve ammunition for a prolonged conflict.
- More likely, Iran is seeking to enhance ceasefire pressure. Iranian attacks have overwhelmingly targeted nearby Gulf States in what is likely a deliberate tactic by Iran to increase ceasefire pressure by causing energy price shocks and other economic disruptions.
- Iran claims the attacks are aimed at U.S. military positions based in these countries, and with the U.S. and Israel escalating their targeting of Iran, there will very likely be continued attacks against Iran coming from these Gulf countries, risking further Iranian military targeting of those Gulf countries.
- On March 7, Dubai Airport, the region's busiest, was temporarily suspended after the airport was struck by Iranian drones,² highlighting the continued risk Iranian attacks present to its Gulf neighbors.

Iran's announcement follows media reports that Saudi and Omani leaders are reaching out to Iran to negotiate a ceasefire,³ while influential figures in Gulf States are criticizing

¹ [hXXps://edition.cnn.com/world/live-news/iran-war-us-israel-trump-03-07-26](https://edition.cnn.com/world/live-news/iran-war-us-israel-trump-03-07-26)

²

[hXXps://www.hindustantimes.com/world-news/emirates-suspends-dubai-flights-amid-fresh-missile-scare-west-asia-abu-dhabi-explosion-bangs-us-iran-war-101772867917809.html](https://www.hindustantimes.com/world-news/emirates-suspends-dubai-flights-amid-fresh-missile-scare-west-asia-abu-dhabi-explosion-bangs-us-iran-war-101772867917809.html)

³ [hXXps://www.washingtonpost.com/politics/2026/02/28/trump-iran-decision-saudi-arabia-israel/](https://www.washingtonpost.com/politics/2026/02/28/trump-iran-decision-saudi-arabia-israel/)

the ongoing U.S.-Israeli operations.⁴ Pezeshkian went on to say that several countries have reached out to negotiate without going into detail. Egypt, Oman, Qatar, and Turkey have publicly offered to broker negotiations since the war began on February 28.⁵

U.S. Escalation Likely

U.S. President Donald Trump responded to Pezeshkian by threatening an immediate escalation in the conflict and a day earlier called for Iran's unconditional surrender.⁶ To this end, the U.S. announced several military maneuvers suggesting an escalation is likely over the coming days. On March 7, 2026, the U.S. announced it was sending its third aircraft carrier, USS George H. W. Bush, to the conflict zone.⁷

- The U.S. Army canceled a major training exercise for the headquarters element of the 82nd Airborne Division at Fort Bragg, raising speculation about a potential Middle East deployment. The unit maintains a brigade of roughly 4,000–5,000 troops ready to deploy within 18 hours.⁸
- Following a White House meeting, major U.S. defense contractors agreed to quadruple production of advanced “exquisite class” weaponry while expanding manufacturing capacity and increasing orders for medium-grade munitions.⁹
- The U.S. and South Korean militaries are in talks on redeploying some Patriot air defense systems based in South Korea to the Middle East.¹⁰

⁴ [hXXps://x.com/KhalafAlHabtoor/status/2029442279170293996?s=20](https://x.com/KhalafAlHabtoor/status/2029442279170293996?s=20)

⁵ [hXXps://www.theguardian.com/world/2026/mar/06/new-supreme-leader-anti-iran-us-propaganda-reformists](https://www.theguardian.com/world/2026/mar/06/new-supreme-leader-anti-iran-us-propaganda-reformists)

⁶ [hXXps://truthsocial.com/@realDonaldTrump/posts/116187586876366061](https://truthsocial.com/@realDonaldTrump/posts/116187586876366061)

⁷

[hXXps://www.timesofisrael.com/liveblog_entry/us-said-expected-to-deploy-3rd-aircraft-carrier-to-the-middle-east/](https://www.timesofisrael.com/liveblog_entry/us-said-expected-to-deploy-3rd-aircraft-carrier-to-the-middle-east/)

⁸ [hXXps://www.washingtonpost.com/national-security/2026/03/06/army-82nd-airborne-iran/](https://www.washingtonpost.com/national-security/2026/03/06/army-82nd-airborne-iran/)

⁹ [hXXps://x.com/PeteHegseth/status/2030023853296996747?s=20](https://x.com/PeteHegseth/status/2030023853296996747?s=20)

¹⁰

[hXXps://www.france24.com/en/middle-east/20260306-us-warns-bombardment-surge-as-israel-strikes-iran-lebanon](https://www.france24.com/en/middle-east/20260306-us-warns-bombardment-surge-as-israel-strikes-iran-lebanon)

The Pentagon is reportedly planning to request funds from Congress to replenish munitions used against Iran; missiles for the Patriot and THAAD air defense systems will be prioritized, as well as Tomahawk cruise missiles.¹¹ If these assets are used to assist in a ground forces operation or to target Iranian energy production sites, it would likely indicate the U.S. is prepared for a protracted conflict aimed at removing the Iranian military and political establishment.

Energy

The Trump administration released the first details of its plan to have the U.S. Development Finance Corporation (DFC) offer an alternative for maritime insurance to convince tankers back into the Strait of Hormuz (SoH),¹² where no ships are moving due to elevated insurance rates¹³ and the threat of being attacked.

- The U.S. reinsurance plan, starting at USD 20 billion worth of coverage, is likely not going to deter Iran military aggression or incentivise shipping companies to restart their routes through the SoH; shippers will likely need more assurance that Iran's ability to routinely attack ships in the SoH has diminished.

On March 7, 2026, Iran's Islamic Revolutionary Guard Corps (IRGC) claimed to have attacked an oil tanker in the Persian Gulf near the Strait of Hormuz.¹⁴ Even if Iran decreases its attacks on Gulf neighbors, it will very likely continue to target energy shipments in the region.

- Brent Crude prices have surged by over 10 percent in the past 24 hours, with the price settling at close to USD 93 per barrel at the time of reporting, a 28 percent weekly price spike for Brent Crude, the biggest since April 2020.¹⁵

¹¹

[hXXps://www.wsj.com/politics/national-security/pentagon-races-to-secure-money-for-iran-operations-munitions-277d0293](https://www.wsj.com/politics/national-security/pentagon-races-to-secure-money-for-iran-operations-munitions-277d0293)

¹² [hXXps://www.ft.com/content/d1d68d91-0d2c-4682-9204-01320a9320d4](https://www.ft.com/content/d1d68d91-0d2c-4682-9204-01320a9320d4)

¹³ [hXXps://foreignpolicy.com/2026/03/03/iran-strikes-hormuz-shipping-oil-2/](https://foreignpolicy.com/2026/03/03/iran-strikes-hormuz-shipping-oil-2/)

¹⁴

[hXXps://www.middleeasteye.net/live-blog/live-blog-update/iran-says-it-struck-malta-flagged-oil-tanker-near-hormuz](https://www.middleeasteye.net/live-blog/live-blog-update/iran-says-it-struck-malta-flagged-oil-tanker-near-hormuz)

¹⁵ [hXXps://www.cnbc.com/2026/03/06/iran-us-war-oil-prices-brent-wti-barrel-futures.html](https://www.cnbc.com/2026/03/06/iran-us-war-oil-prices-brent-wti-barrel-futures.html)

- This spike is almost certainly caused by the continuation of the conflict beyond the previously priced-in short duration, supply blockages due to the security crisis around the Strait of Hormuz, and reported (as well as planned) production cuts in the Middle East.
- Qatar’s Energy Minister Saad al-Kaab has stated that all exporters in the Gulf region will likely “call force majeure” in the next few days and stop oil exports. Iraq, Qatar, and Kuwait have reported pausing production to some degree because of declining storage capacity amplified by the transport blockade.¹⁶
- Maintaining leverage over these key Middle Eastern industries is almost certainly part of Iran’s strategy to end the conflict on terms it finds acceptable.

Sleeper Cells

Iranian loyalists or “sleeper cells” in countries perceived to be anti-Iran are very likely targeting entities that can cause the maximum damage to logistics infrastructure (such as fuel pipelines) or affect morale (religious symbols). Reports of disruption of cells and arrest of its members continue to emerge, from various countries perceived to be allied with the United States or Israel.

- Azerbaijan has reportedly “prevented terrorist acts and intelligence operations” conducted by entities linked to Iran’s Islamic Revolutionary Guard Corps (IRGC). The suspected targets included the Israeli embassy in Baku, a synagogue, Jewish community leaders, and the Baku-Tbilisi-Ceyhan pipeline (which carries over 30 percent of Israel’s oil imports).¹⁷

Sleeper cells capable of carrying out sabotage and acts of terrorism are very likely components of Iran’s asymmetric warfare regime, which focuses on hitting soft targets, often using proxy groups that allow Iran plausible deniability; fully degrading these capabilities is very unlikely in the short term.

¹⁶ [hXXps://www.ft\[.\]com/content/be122b17-e667-478d-be19-89d605e978ea](https://www.ft.com/content/be122b17-e667-478d-be19-89d605e978ea)

¹⁷

[hXXps://www.timesofisrael\[.\]com/azerbaijan-says-it-foiled-iranian-terror-attacks-on-synagogue-israeli-embassy/](https://www.timesofisrael.com/azerbaijan-says-it-foiled-iranian-terror-attacks-on-synagogue-israeli-embassy/)

| Cyber Landscape

The Iran conflict continues to spill into the digital infrastructure, with some state-aligned and other politically motivated threat collectives positioning for sustained operations. However, these attacks are very likely to be DDoS attacks, which will not cause major disruptions to the functioning of government infrastructure. Politically motivated collectives are very likely to continue DDoS and low-sophistication attacks against entities in the United States, Israel, and other countries perceived to be against Iran.

Iranian APT Muddy Water

Iranian state-sponsored threat collective MuddyWater (aka Sandworm) has been attributed to an intrusion attack that enabled malicious actors to establish footholds inside several U.S. organizations, including financial institutions, an airport, a non-profit entity, and the Israeli arm of a software service supplier serving defense and aerospace clients.¹⁸ Since the U.S.-led military campaign began in late February, MuddyWater has pivoted from conducting cyber espionage campaigns primarily in the Middle East and North Africa reportedly to the U.S. and Europe, according to public statements from the U.S. Military.¹⁹

- An espionage campaign linked to the group was observed recently targeting entities across the MENA region using phishing lures to deliver new malware loaders and backdoors capable of remote command execution, system reconnaissance, and persistent access.
- ZeroFox warns that parallel activity from other Iran-aligned actors could include reconnaissance against internet-exposed cameras and scanning of externally facing services, alongside hacktivist campaigns targeting U.S., European, and Israeli government portals and industrial systems, which could be used for influence operations or potential disruptive activity.

¹⁸ [hXXps://thehackernews.com/2026/03/iran-linked-muddywater-hackers-target.html](https://thehackernews.com/2026/03/iran-linked-muddywater-hackers-target.html)

¹⁹

[hXXps://www.cybercom.mil/Media/News/Article/2945592/iranian-government-sponsored-actors-conduct-cyber-operations-against-global-gov/#:~:text=The%20Federal%20Bureau%20of%20Investigation%20\(FBI\)%2C%20the,gas%2D%2Din%20Asia%2C%20Africa%2C%20Europe%2C%20and%20North%20America.](https://www.cybercom.mil/Media/News/Article/2945592/iranian-government-sponsored-actors-conduct-cyber-operations-against-global-gov/#:~:text=The%20Federal%20Bureau%20of%20Investigation%20(FBI)%2C%20the,gas%2D%2Din%20Asia%2C%20Africa%2C%20Europe%2C%20and%20North%20America.)

Prominent collectives

Iran-aligned hacktivist and Threat collectives continue to claim DDoS attacks, including access to CCTV camera networks, intrusion attacks into various entity networks in Israel and other Middle Eastern countries. Other campaigns have focused on Israeli public figures and the release of partial identity records of individuals allegedly linked to the Israeli military operating in Axis of Resistance countries.

- Threat collective 404 Cyber Team has claimed to hack into a network of Israeli CCTV cameras. The group has provided screenshots of CCTV footage. It also announced that it will launch a series of attacks “soon.”



Alleged CCTV access by 404 Cyber Team

Source: ZeroFox Intelligence

- 404 Cyber Team also claimed to hack into the servers of radar systems that allegedly is capable of disabling drones deep within Israel’s territories. The collective has not provided any evidence to support its claims. The claims are very likely exaggerated and have been made just to propagate the political agenda it supports.
- Anti-U.S. and anti-Israel threat collective DieNet has claimed to conduct DDoS attacks against websites associated with the government of the United Arab Emirates. Another politically motivated threat group RuskiNet claimed a DDoS attack against Israeli OMC Group, a cloud computing firm.



DieNet’s Telegram post

Source: ZeroFox Intelligence

- Pro-Iran threat collective “Handala Hack” claimed it breached Israeli military-linked accounts and released 26 pages of individuals allegedly connected to the IDF in Axis of Resistance countries, while withholding contact numbers. The group also claimed renewed deployment of “Naem” spyware capable of tracking devices including iPhone 12 Pro Max units.

Conclusion

Despite conciliatory statements from the Iranian government, it continues to signal it is preparing for a prolonged conflict, with its ability to impact energy supply chains a leading component of its defense strategy. It remains unclear if the U.S. is willing to maintain its maximalist demands in the face of a true energy crisis. Energy prices are only now surpassing levels that in previous years would have been seen as normal, while the crisis has yet to spread to other commodities. This gives the U.S. a limited window to escalate the conflict before the economic disruptions elevate further.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%