ZEROFOX INTELLIGENCE

Flash

Military Strikes on Iran – SITREP #28: March 25, 2026

F-2026-03-25a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics, Deep and Dark Web

March 25, 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 4:00 AM (EDT) on March 25, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Military Strikes on Iran – SITREP #27: March 25, 2026

| Key Findings

- U.S. President Donald Trump postponed threatened strikes against Iranian energy infrastructure and power plants for five days, pending the outcome of talks with Iran. Leading economic indicators such as oil prices and global stock markets very likely fluctuated based on Trump's statement, which has been widely interpreted as an acknowledgement that he is looking to end the war. The Iranian Foreign Ministry refuted Trump's claims about talks but acknowledged limited talks with third-party mediators.

- In the short term, the five-day extension likely signals that the conflict will not escalate further this week. However, fighting will likely continue, with Iran targeting Israel and Gulf countries; the latter are reportedly considering joining the war effort against Iran.

- There is a roughly even chance that the five-day delay is a tactic being used before Operation Epic Fury escalates to forcibly reopening the Strait of Hormuz (SoH) in April. However, the U.S. desire for a swift end to the conflict likely remains—regardless of the outcome of the latest talks.

Latest Details

The five-day delay came after President Trump's original threat on March 21 to target Iran's power plants and energy infrastructure unless the SoH was re-opened to commercial ship traffic within 48 hours, which Iran still has not done.[1]

- Iran's Islamic Revolutionary Guard Corps (IRGC) responded by threatening to escalate attacks on political and technological assets beyond the Middle East[2] and to anyone financing the U.S. military via treasury bonds, which includes nearly the entire world.[3]

After President Trump's statement that negotiations were underway, Brent crude oil prices dropped 11 percent by the end of March 23 to USD 99.94 a barrel after hitting nearly USD 114 earlier in the day,[4] while the S&P 500 stock index increased 1.2 percent.[5]

- This is likely a reflection of investor confidence that President Trump is eager for a resolution to the conflict, tempered with caution regarding the likelihood that Iran will continue to impact regional energy supplies beyond the conflict's end.

According to President Trump, Iran and the United States have reached agreement on 15 points, including for Iran to turn over nuclear material and not resume its nuclear program.[6]

- The unspecified items likely include options on re-opening the SoH, protecting regional energy infrastructure, limiting Iran's support for regional proxies, and supporting Iran's non-nuclear weapons program.

However, the Iranian Foreign Ministry refuted Trump's claims and denied any talks had taken place. Foreign Minister Abbas Araghchi confirmed that regional countries have

[1] hXXps://truthsocial[.]com/@realDonaldTrump/posts/116278232362967212
[2] hXXps://t[.]me/irna_1313/395618hXXps://t.me/irna_1313/395618
[3] hXXps://x[.]com/mb_ghalibaf/status/2035776169656676675
[4] hXXps://tradingeconomics[.]com/commodity/brent-crude-oil
[5] hXXps://www.wsj[.]com/livecoverage/stock-market-today-dow-sp-500-nasdaq-03-23-2026
[6] hXXps://www.cnn[.]com/world/live-news/iran-war-us-israel-trump-03-23-26

offered to serve as a go-between but stated that direct dialogue with the United States had not occurred.[7]

Turkey, Qatar, Pakistan, Oman, and Egypt are likely talking with intermediaries on both sides of the conflict, but it remains unclear if substantial talks that can end it are taking place.

- Iran is very unlikely to relinquish its control over the SoH voluntarily, as it likely views the threat of closing off the vital energy supply chain as key to avoiding future targeting by either the United States or Israel.

- Iran has also demanded reparations from the conflict, which are extremely unlikely.[8] However, unfreezing Iranian assets held in foreign bank accounts and rolling back sanctions would likely suffice.

Fighting Continues

Since President Trump's statement delaying strikes on Iranian energy targets, Iran has targeted the Israeli cities of Eilat, Dimona, and Tel Aviv with missile and drone attacks, as well as U.S. military bases across the Middle East. Saudi Arabia said it intercepted a drone, and Kuwait and Bahrain also reported attacks.[9] Iran reported U.S.-Israeli attacks that damaged a gas plant in the central city of Isfahan. There was also a strike on a pipeline supplying gas to the Khorramshahr Combined Cycle Power Plant in southwestern Iran.[10]

- Over the weekend, the Israel Defense Forces reportedly escalated strikes on infrastructure in the capital, Tehran,[11] while over 200 people were injured in the southern cities of Arad and Dimona, Israel, following repeated Iranian attacks.[12] U.S.

[7] hXXps://www.cnn[.]com/world/live-news/iran-war-us-israel-trump-03-23-26

[8] hXXps://www.reuters[.]com/world/middle-east/iran-toughens-negotiating-stance-amid-mediation-efforts-sources-say-2026-03-24/

[9] hXXps://www.reuters[.]com/world/asia-pacific/iran-sends-waves-missiles-into-israel-dismisses-trumps-talk-negotiations-fake-2026-03-24/

[10] hXXps://aje[.]news/b79m9v?update=4429845

[11] hXXps://www.nytimes[.]com/live/2026/03/22/world/iran-war-oil-trump

[12] hXXps://www.theguardian[.]com/world/2026/mar/21/wounded-iranian-missile-strikes-southern-israel

Treasury Secretary Scott Bessent said U.S. attacks were aimed at destroying Iran's fortifications along the SoH.[13]

Over the five-day period, expect a similar trend in targeting that avoids the escalatory implications of strikes on critical energy infrastructure. With Iran continuing to target Gulf countries, there are unverified reports that Gulf leaders have become more supportive of joining the war effort against Iran, fearful that the future of Middle Eastern energy will remain uncertain if the conflict ends with Iran's political and military leadership in place. Gulf states have refrained from responding to Iranian drone and missile attacks, likely because they want the war to end without their own water and energy infrastructure being hit.

- However, the Gulf states are more likely to join the conflict on the side of the United States and Israel if Iran extends its targeting to their own power and water plants. Saudi Arabia has reportedly agreed to give the U.S. military access to King Fahd Air Base, a reversal after previously saying its bases could not be used to attack Iran.[14]

Possible Escalation

Despite the economic optimism surrounding negotiations between the United States and Iran, there is a roughly even chance that the deadline will pass without a resolution and instead lead to an escalation by the U.S. military. The U.S. Department of War has requested USD 200 billion for the war effort,[15] which very likely signals a time frame of months. Hundreds of U.S. Marines are still heading to the conflict zone, reportedly as support to seize Kharg Island, Iran's main energy export terminal,[16] or for some other type of ground operation.

- An attack on Kharg Island's energy facilities would almost certainly disrupt most of Iran's oil exports and lead to a retaliatory escalation by Iran against other

[13] hXXps://www.nbcnews[.]com/politics/trump-administration/treasury-secretary-bessent-us-military-actions-iran-escalate-oil-rcna264608
[14] hXXps://www.wsj[.]com/world/middle-east/iran-gulf-states-offense-decision-b8d98ff9
[15] hXXps://apnews[.]com/article/iran-war-us-pentagon-972ec1bd956a2c3633e6ab7fff389791
[16] hXXps://www.stripes[.]com/branches/army/2026-03-24/karag-82nd-airborne-marines-iran-21167074.html

nearby Gulf energy targets, which would very likely send energy prices even higher.

- Kharg Island accounts for 90 percent of Iranian energy exports and is therefore the central revenue driver for the political and military establishment. A successful seizure of only Kharg Island is unlikely to end the conflict in the short term. Iran can likely re-route some energy to alternative terminals, very likely allowing it to maintain 25–30 percent of its export capacity. Iran has funded its government with fewer revenues as recently as 2020–2022, when U.S. sanctions restricted Iran's energy trade to less than 250,000 barrels per day.[17] Simultaneously hitting all the export nodes at once would very likely necessitate sending U.S. ground forces across Iran and maintaining them along the coast long-term. However, the threat of taking the island very likely remains part of U.S. leverage to pressure Iran into concessions.

- Another scenario utilizing U.S. ground forces in Iran includes seizing highly enriched uranium.[18] However, that is unlikely, as it requires going into central Iran and is even less likely to force concessions from Iran in the short term.

While some U.S. Marines are due to arrive within days of the de-escalation delay expiring, the bulk of the added Marines are being transported aboard the *USS Boxer* and will not reach the region until mid-April.[19] Therefore, the prospect of Operation Epic Fury forcibly reopening the SoH or taking Kharg Island is not likely until then.

If the five-day extension announced by President Trump expires without an agreement, the U.S. desire for a swift resolution to the conflict is unlikely to diminish; rather, coming to no agreement would more likely lead to a short-term escalation in the month of April to attempt to neutralize Iran's ability to close the SoH.

[17] hXXps://www.bloomberg[.]com/opinion/articles/2026-03-22/iran-war-trump-seizing-kharg-island-is-a-bad-idea-for-oil-reasons-too-mn1pgo70
[18] hXXps://www.nbcnews[.]com/politics/white-house/trump-weighing-several-options-us-troops-iran-rcna263909
[19] hXXps://news.usni[.]org/2026/03/20/boxer-amphibious-ready-group-11th-meu-deploy-from-california

On March 24, 2026, Iran's mission to the United Nations issued a statement that "non-hostile" vessels will be allowed to transit the SoH, provided they coordinate with the proper Iranian authorities.[20] However, even if the SoH is fully reopened, a return to normal operating procedures for the entire Middle Eastern energy sector will almost certainly not be immediate. Infrastructure has been damaged, and investors are unlikely to commit to rebuilding if renewed disruption seems likely.

- Iranian attacks on infrastructure and war-induced production shutdowns on oil and gas fields in Qatar, Iraq, Kuwait, and Saudi Arabia underscore the risk of new investments in the region. Investors may decide their capital is better spent investing in alternative supply chains that avoid the Middle East altogether.

- In addition to ground forces, maintaining an open SoH without the permission of the IRGC would likely require naval convoys for months or years, as well as a shipping premium indefinitely to deter the Iranian threat against tankers in the strait.

Without a ceasefire or ground troops, the U.S. Navy will almost certainly not risk its assets in the SoH—nor will commercial shipping. The Iranians now control who gets in and out of the Gulf, having established a permanent toll to pass the SoH; that will remain the case if the United States ends hostilities without an agreement. The Trump administration very likely wants to end the war while avoiding a major military escalation but is likely unwilling to end hostilities while Iran maintains control over the SoH. Therefore, the United States is likely to pursue a diplomatic de-escalation before a multinational effort to contest Iran's control over the SoH.

Cyber Activity

Coordinated cyber operations targeting government infrastructure and private-sector entities continue across Israel, Iran, and other Middle Eastern countries. These activities appear to be driven primarily by pro-Iranian, pro-Palestinian, pro-Israel, anti-Iran, and pro-Russian hacktivist collectives employing a combination of distributed

20 hXXps://www.aljazeera[.]com/economy/2026/3/25/iran-says-non-hostile-ships-can-pass-safely-through-strait-of-hormuz

denial-of-service (DDoS) attacks, website defacement, data exfiltration, and claimed intrusions into Industrial Control Systems (ICS).

Impacts to Digital Infrastructure and Information

Iran's nationwide internet shutdown has reached day 25, exceeding 576 hours, according to NetBlocks.[21] The restrictions have cut off public access to global communication channels; meanwhile, limited whitelisted accounts continue to operate, shaping domestic information flows and restricting external visibility. Various reports from the beginning of March indicated that the public and hacktivist collectives alike were most likely using Starlink devices in Iran to bypass the country's internet shutdown; however, this activity is likely to result in arrests or other penalties from the Iranian government.

- The Iranian Ministry of Intelligence and Security (MOIS) announced that intelligence agents arrested an alleged cell of U.S.-Israeli mercenaries who were planning to carry out attacks in Tehran. A Starlink device was among the seized weapons.[22]
- Threat collectives are reportedly using Starlink's facilities to stay online amid the conflict.[23]
- Iranian authorities reported the seizure of hundreds of Starlink satellite communication terminals, alleging the systems were smuggled into the country by U.S. and Israeli actors. Officials stated that unauthorized use of such devices constitutes a criminal offense subject to severe wartime penalties.[24]

On March 24, Amazon reported to Reuters that its Amazon Web Services (AWS) region in Bahrain was disrupted due to nearby drone activity, marking the second drone-related incident to impact Bahrain's AWS since the start of the U.S. and Israeli strikes against Iran.

---

[21] hXXps://www.aljazeera[.]com/news/liveblog/2026/3/24/iran-war-live-tehran-says-trumps-claims-of-peace-talks-fake?update=4429932

[22] hXXps://x[.]com/TheCradleMedia/status/2029141895134265602?s=20

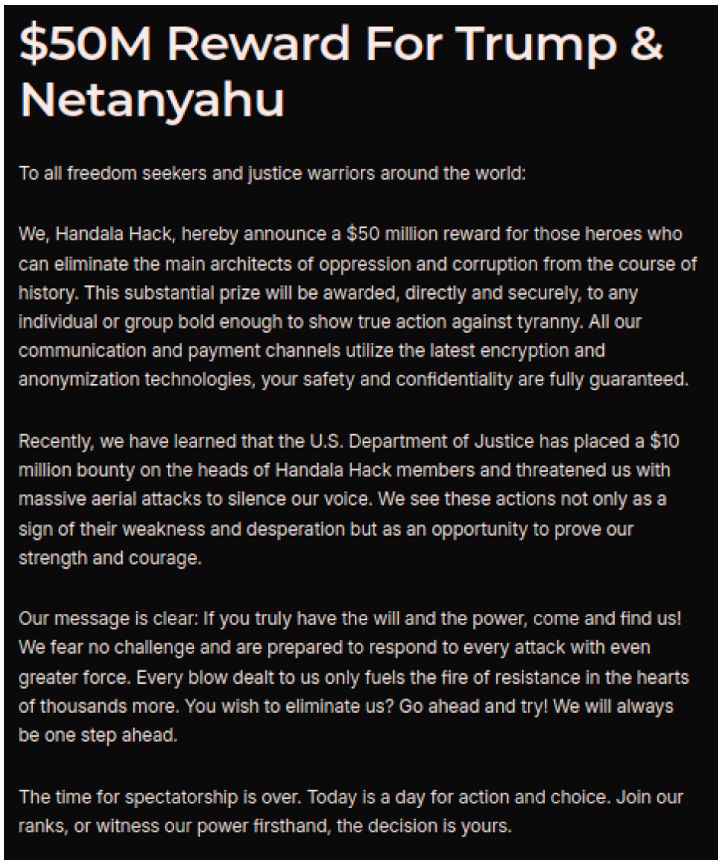
[23] hXXps://www.forbes[.]com/sites/thomasbrewster/2026/03/02/iran-hackers-use-elon-musk-starlink-to-stay-online/

[24] hXXps://x[.]com/AJEnglish/status/2033872994192216316?s=20

The company is shifting workloads to alternate regions, while the extent of damage and a recovery timeline remain unclear.[25]

Handala Hack Team

On March 24, 2026, pro-Palestian hacktivist group "Handala Hack Team" posted on its leak site offering a USD 50 million reward to anyone who can "eliminate the main architects of oppression and corruption from the course of history," almost certainly referring to President Trump and Israeli Prime Minister Benjamin Netanyahu. In the post, the group claims that the U.S. Department of Justice (DOJ) placed a USD 10 million "bounty on the heads of Handala Hack members."



$50M Reward For Trump & Netanyahu

To all freedom seekers and justice warriors around the world:

We, Handala Hack, hereby announce a $50 million reward for those heroes who can eliminate the main architects of oppression and corruption from the course of history. This substantial prize will be awarded, directly and securely, to any individual or group bold enough to show true action against tyranny. All our communication and payment channels utilize the latest encryption and anonymization technologies, your safety and confidentiality are fully guaranteed.

Recently, we have learned that the U.S. Department of Justice has placed a $10 million bounty on the heads of Handala Hack members and threatened us with massive aerial attacks to silence our voice. We see these actions not only as a sign of their weakness and desperation but as an opportunity to prove our strength and courage.

Our message is clear: If you truly have the will and the power, come and find us! We fear no challenge and are prepared to respond to every attack with even greater force. Every blow dealt to us only fuels the fire of resistance in the hearts of thousands more. You wish to eliminate us? Go ahead and try! We will always be one step ahead.

The time for spectatorship is over. Today is a day for action and choice. Join our ranks, or witness our power firsthand, the decision is yours.

Handala Hack Team's post
Source: ZeroFox Intelligence

25
hXXps://www.reuters[.]com/world/middle-east/amazon-says-awss-bahrain-region-disrupted-following-drone-activity-2026-03-24/

The collective's claims are very likely, in part, a response to the U.S. DOJ allegedly seizing four domains associated with Handala Hack Team's cyber operations (handala-hack[.]to, handala-redwanted[.]to, justicehomeland[.]org, and karmabelow80[.]org), as reported by the DOJ on March 19.[26] According to the DOJ's release, Handala Hack Team is allegedly one of several personas used by a hacking unit within Iran's MOIS psychological operations.[27]

- The following day Handala Hack Team restored these domains and has since continued posting.

In addition, unconfirmed social media posts and articles circulating online suggest that a varying number of Handala Hack Team members have been injured or eliminated in U.S. and Israeli led airstrikes in Iran; the posters have alleged both that this was simply the effect of collateral damage and that the collective was targeted. Some reports claim that two critical leaders of Iran's MOIS, allegedly "handlers" or otherwise associated with operating Handala Hack Team, were killed in airstrike attacks.[28][29]

- At the time of writing, ZeroFox has not observed the collective address these claims on any of its communication channels or sites.

[26] hXXps://www.justice[.]gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations
[27] hXXps://www.reuters[.]com/technology/iran-linked-hackers-restore-website-after-us-seizes-domains-2026-03-20/
[28] hXXps://www.irishexaminer[.]com/news/arid-41814761.html
[29] hXXps://www.forbes[.]com/sites/the-wiretap/2026/03/17/us-strikes-killed-iranian-cyber-chiefs-but-the-hacks-continued/

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%