ZEROFOX INTELLIGENCE

Flash

Military Strikes on Iran – SITREP #30: March 31, 2026

F-2026-03-31a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics, Deep and Dark Web

March 31, 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 31, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Military Strikes on Iran – SITREP #30: March 31, 2026

| Key Findings

- A diplomatic agreement to end the conflict in the Middle East is unlikely by the April 6 deadline unless Iran or the United States weakens its demands, signaling targeting will likely continue—and the conflict will likely expand. The entry of Houthi rebels in Yemen (who are currently only targeting Israel) signals a growing risk of shipping and energy disruptions expanding beyond the Strait of Hormuz (SoH).

- With U.S. and Iranian differences on ceasefire demands unresolved, a U.S. military escalation is more likely than a diplomatic solution to end the conflict. Ongoing U.S. military deployments increase the likelihood the conflict will expand, which will likely involve targeting Iranian energy infrastructure or sending in ground forces before coming to a quicker end than is likely utilizing diplomacy alone.

- While ending the war quickly remains a priority, the prospect of doing so without a military escalation, including ground forces, has diminished—a probability reflected by economic indicators led by oil prices at the start of the week.

Houthis Join the Conflict as U.S. Troop Deployment Expands

Houthi rebels in Yemen officially entered the war, joining other Iran-aligned groups in Iraq and Lebanon, by launching ballistic missiles at Israel on March 28 and 30.[1][2] In an official statement, the group said it would continue operations until Operation Epic Fury, which targets Iran and Iran-aligned groups like Hezbollah, ceases.[3]

- The group has managed to effectively shut down the Red Sea supply chain since late 2023, when they entered the Israel-Hamas war, by forcing vessels to reroute. Although the group had not launched strikes on Israel or Red Sea shipping since the ceasefire in the Israel-Hamas war began in October 2025, the Houthis previously targeted military and commercial ships over 190 times between November 2023 and June 2024.[4] The lingering threat posed by the group is very likely still deterring most shipping, though some major shipping lines were exploring a return to the Red Sea before the Iran conflict began.[5]

- Given the distance between Yemen and Israel, the targeting of Israel is less significant than the signal the Houthis' participation sends to energy and shipping markets. While their official statement did not indicate an intent to target tankers or vessels transiting the southern Red Sea and the Bab El-Mandeb Strait, the Houthis almost certainly have the capability to do so. They threatened to resume targeting commercial shipping immediately following the initial U.S.-Israeli strikes on Iran but had held off on taking any further action until the March 28 attack on Israel.[6]

[1] hXXps://www.bbc[.]com/news/articles/cd6l5n8jv4yo
[2] hXXps://www.france24[.]com/en/middle-east/20260330-will-iranian-backed-yemen-houthis-rebels-block-the-bab-al-mandeb-strait
[3] hXXps://www.aljazeera[.]com/news/2026/3/27/houthis-warn-fingers-on-the-trigger-as-us-israeli-war-on-iran-continues
[4] hXXps://www.wilsoncenter[.]org/article/timeline-houthi-attacks
[5] hXXps://gcaptain[.]com/red-sea-comeback-falters-as-maersk-diverts-ships-back-around-cape/
[6] hXXps://gcaptain[.]com/houthis-signal-renewed-red-sea-shipping-attacks-after-u-s-israeli-strikes-on-iran/

The Red Sea has become a relatively safer alternative to the SoH since the latest war in Iran. Saudi Arabia is leveraging its Western port of Yanbu to distribute seven million barrels of oil daily onto global markets.[7] However, the port and the pipeline from eastern Saudi Arabia are well within Houthi ranges.

- If the Houthis target global shipping, it would likely expand the energy crisis by making another key supply chain impassable and removing an additional seven million barrels a day from global markets.

- Conducting simultaneous military operations to reopen the SoH and secure Red Sea navigation would very likely be extremely difficult. Furthermore, a military operation to reopen the SoH would almost certainly increase pressure from Iran on the Houthis to target Red Sea alternatives.

Despite this, the Houthis are not subordinate to Iran and are currently likely to avoid targeting vessels in the Red Sea or Saudi Arabia specifically. Since 2022,[8] Saudi Arabia and the Houthis have observed a truce that would almost certainly end if Saudi pipelines were targeted, leading Saudi Arabia to enter the conflict by striking Houthi locations in western Yemen. Unlike Hezbollah or Iranian-backed groups in Iraq, the Houthis control and govern territory in Yemen and risk turning the local population against them if they invite targeting from Saudi Arabia, the United States, or Israel. For now, the Houthis are likely balancing the need to be seen as participating on Iran's side while minimizing the risk of inviting foreign targeting.

Over the weekend, an additional 3,500 U.S. troops arrived in the region, with at least 2,000 more due to arrive by mid-April.[9] When the full deployment arrives, it will give the U.S. military ground capabilities to supplement its largely airpower-driven war. U.S. President Donald Trump, speaking to two different media outlets, indicated the troops could be deployed to seize Iran's Kharg Island oil, conduct a raid to extract its uranium, or take

[7] hXXps://www.reuters[.]com/business/energy/saudi-pipeline-pumping-7-million-bpd-oil-bypassing-hormuz-bloomberg-news-reports-2026-03-28/
[8] hXXps://arabcenterdc[.]org/resource/a-fragile-but-enduring-truce-in-yemen/
[9] hXXps://www.cbsnews[.]com/news/us-troops-uss-tripoli-centcom-middle-east-arrive-iran/

control of its broader energy infrastructure. Given the lack of progress on negotiations with Iran, these statements further signal the prospect of an expanded conflict.[10][11]

Ceasefire Probability Diminishing and Reflection in Markets

The prospect of Iran and the United States reaching an agreement to reopen the SoH by April 6, 2026,[12] is unlikely unless both sides weaken their demands. While there is likely some room for compromise, it is almost certainly limited. Some of Iran's demands, such as U.S. recognition of Iranian control of the SoH and an end to targeting Iranian proxy groups, directly contradict the stated mission of Operation Epic Fury. Certain U.S. demands, such as those related to Iranian nuclear and other weapons programs, are equally unlikely to be accepted by Iran.[13]

- Iran has effectively limited shipping in the SoH at little cost to itself, continuing to ship its own energy products while pressuring the United States for a ceasefire via energy price shocks. Iran is unlikely to voluntarily surrender its ability to selectively cut off oil supplies by determining who can use the SoH.

When markets opened on March 30, Brent crude rose 3.5 percent to above USD 116 per barrel.[14] While oil price futures (an indication of how long oil traders expect the conflict to impact energy prices) also increased, they remain well below current levels.[15] The significant short-term price increases coupled with lower long-term prices indicates that investors are not confident of a negotiated end to the war.

[10] hXXps://www.ft[.]com/content/3bd9fb6c-2985-4d24-b86b-23b788403lf5
[11] hXXps://www.wsj[.]com/politics/national-security/trump-weighs-military-operation-to-extract-irans-uranium-37427c8b
[12] hXXps://edition.cnn[.]com/2026/03/26/world/live-news/iran-war-us-israel-trump
[13] ZeroFox Intelligence Flash Report: Military Strikes on Iran – SITREP #29: March 27, 2026
[14] hXXps://edition.cnn[.]com/2026/03/30/business/oil-prices-rise-116-iran-intl
[15] hXXps://www.ice[.]com/products/219/Brent-Crude-Futures/data

The major U.S.-led stock indexes are so far down less than 10 percent since the conflict started.[16] This is likely because the supply chain disruptions from higher energy prices (such as higher transportation and materials costs) have only just begun; and to prevent further disruption, the war almost certainly needs to end soon; as a diplomatic ceasefire looks unlikely, a military escalation is likely.

Sleeper Cells

French authorities detained three suspects over an attempted bombing near Bank of America's office in Paris, which officials suspect was linked to the conflict. One of the three suspects in custody reportedly said he was contacted over Snapchat and paid EUR 600 for the task.[17] This is the latest in a series of plots and some successful attacks linked to Iran since Operation Epic Fury began.

- On March 14, explosives targeted a Jewish school in Amsterdam and a synagogue in Rotterdam.[18] A blast also took place outside the U.S. Embassy in Oslo on March 11.[19] On March 23, four ambulances owned by a Jewish charity in Golders Green, London, were torched.[20]

Iran has been accused of orchestrating attacks abroad by hiring criminals online in order to distance itself from the acts and maintain plausible deniability of its involvement.[21]

Cyber Activity

Coordinated cyber operations targeting government infrastructure and private-sector entities continue across Israel, Iran, and other Middle Eastern countries. These activities

16 hXXps://www.bloomberg[.]com/news/articles/2026-03-30/us-stock-futures-rise-as-oversold-signals-lure-some-dip-buyers
17 hXXps://www.lemonde[.]fr/en/france/article/2026/03/30/after-a-foiled-attack-outside-bank-of-america-in-paris-five-arrests-and-questions-over-iran-s-role_6751958_7.html
18 hXXps://www.lemonde[.]fr/en/international/article/2026/03/14/explosion-damages-jewish-school-in-amsterdam-no-injuries_6751434_4.html
19 hXXps://www.bbc[.]com/news/articles/cx2grl7lrrmo
20 hXXps://www.bbc[.]com/news/live/czj1m8xpk14t
21 hXXps://www.cnn[.]com/2026/03/28/politics/iran-recruitment-terror-plots-us

appear to be driven primarily by pro-Iranian, pro-Palestinian, pro-Israel, anti-Iran, and pro-Russian hacktivist collectives employing a combination of distributed denial-of-service (DDoS) attacks, website defacement, data exfiltration, and claimed intrusions into Industrial Control Systems (ICS).

Disinformation

Unverified reports circulating online claim the destruction of a facility in Dubai allegedly storing Ukrainian anti-drone systems, with assertions that the site was completely destroyed and 21 Ukrainian personnel were killed. However, Ukraine's Center for Countering Disinformation has debunked these rumors.[22]

Handala Hack Team

On March 27, 2026, pro-Palestinian hacktivist group Handala Hack Team claimed to have gained access to the personal Gmail account of U.S. Federal Bureau of Investigations (FBI) Director Kash Patel and then proceeded to release emails and personal images of the director. An FBI spokesperson has confirmed that Patel's emails have been targeted, further stating that the bureau has taken all necessary steps to mitigate potential risks associated with this activity.[23]

- Soon after the collective announced the breach on its official Telegram channel (@HANDALA_HPR2), the account disappeared from the platform. Along with the channel, the collective's leak site also became inaccessible.
- The threat collective now has a new Telegram channel under the handle @HANDALA_INTEL. Handala Hack Team also announced URLs for its new leak sites, which are down as of reporting.
- Hacking into a personal account of a high-ranking official is very unlikely to have any impact on the main servers or official communication networks used by government agencies. Rather, it is more likely to aid law enforcement in identifying where the attack originated from and tracking the perpetrators.

[22] hXXps://x[.]com/CforCD/status/2037869263654895842?s=20

[23] hXXps://www.reuters[.]com/world/us/iran-linked-hackers-claim-breach-of-fbi-directors-personal-email-doj-official-2026-03-27/

Before the leak sites became unavailable, on March 28, Handala Hack Team claimed to have wiped 4 TB of data allegedly associated with Good Food Store, the largest store in the U.S. state of Montana. On March 29, the collective allegedly breached the private communications and correspondence of Former Israeli Defense Minister Yoav Gallant.

Handala Hack Team's posts on its leak site
Source: ZeroFox Intelligence

Meanwhile, the U.S. Department of State's Rewards for Justice program is offering up to USD 10 million for information identifying or locating individuals linked to Iranian cyber groups involved in targeting U.S. critical infrastructure, including Parsian Afzar Rayan Borna and Handala Hack Team.[24]

- The operator of X account @GangExposed_RU has responded to the above call for action and claims to possess names, connections, and photos of key participants in the Iranian cyberattacks.[25] The account belongs to a self-proclaimed cybercrime investigator; its posts are primarily about the alleged identities of infamous hackers and threat actors.

[24] hXXps://x[.]com/RFJ_USA/status/2037587441482105045?s=20
[25] hXXps://x[.]com/GangExposed_RU/status/2037954367505223900?s=20

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%