ZEROFOX INTELLIGENCE

Flash

Military Strikes on Iran – SITREP #31: April 2, 2026

F-2026-04-02a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics, Deep and Dark Web

April 2, 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 April 2, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Military Strikes on Iran – SITREP #31: April 2, 2026

| Key Findings

- U.S. President Donald Trump has continued vacillating between threatening to escalate the Iran conflict and winding it down. Iran made its most significant acknowledgement to date that it is open to talks, without conceding on previous demands. There is now a roughly even chance the U.S. military will scale back its operations after meeting only some of its stated goals, such as removing layers of Iran's leadership and debilitating its weapons program. This would very likely leave Iran in control of the Strait of Hormuz (SoH), which Trump has suggested is possible.

- Although additional reinforcements for ground operations are anticipated, the U.S. military likely possesses enough existing capabilities to launch such operations now. There is a roughly even chance the United States winds down the conflict after pursuing military goals such as seizing Iran's enriched uranium, conducting operations against Iranian nuclear facilities and critical infrastructure, or further reducing Iran's ability to control the SoH.

- On March 31, 2026, the Islamic Revolutionary Guard Corps (IRGC) issued a warning to 18 companies (including 16 U.S. and two Dubai-based companies), threatening them with attack for their alleged support of U.S. and Israeli war efforts. The IRGC suggested that employees stay away from their places of work in order to "preserve their own lives."

Latest Developments

The United States continues to send mixed messages about the war with Iran. On March 31, 2026, President Trump reiterated his threat to target Iran's energy sector if it did not reopen the SoH and agree to a peace deal by April 6.[1] However, later on March 31, Trump signaled he was considering ending the conflict even with Iran still in control of the SoH, predicting the U.S. military would end its bombing campaign within two to three weeks.[2] He went on to suggest the United States had largely accomplished its military goals and would leave it to other countries to resolve issues with the SoH.

Strait of Hormuz

President Trump called on nations dependent on the SoH for oil—particularly NATO members in Europe—to make efforts to retake control, suggesting they should "just TAKE IT."[3]

- European nations have reportedly approved a coalition to enforce freedom of navigation in the SoH—but only after the war ends.[4]
- Non-combatant producing countries in the region, such as Saudi Arabia and the United Arab Emirates (UAE), are reportedly considering joining such a coalition because their economies are heavily dependent on maintaining a secure SoH. Specifically, the UAE is prepared to join the U.S. military in forcibly reopening the SoH.[5]

[1] hXXps://foreignpolicy[.]com/2026/03/30/trump-iran-war-peace-talks-progress-kharg-island-ghalibaf-energy-oil-pakistan/
[2] hXXps://www.facebook[.]com/CSPAN/videos/917975487811661/
[3] hXXps://truthsocial[.]com/@realDonaldTrump/posts/116323481956698353
[4] hXXps://www.axios[.]com/2026/03/19/strait-hormuz-coalition-allies-statement-uk
[5] hXXps://www.wsj[.]com/world/middle-east/uae-iran-war-strait-of-hormuz-9836ecbb

- The urgency for these Gulf states stems from the Iranian Parliament passing the "Strait of Hormuz Management Plan" on March 30, which establishes Iranian control over the SoH, allowing it to impose a toll on vessels and likely prohibiting passage for vessels allied with the United States or Israel.[6] It is likely unrealistic for any Gulf state to accept this status quo of Iran exercising a toll on access to the SoH.

The United States is less impacted by an Iran-controlled SoH for oil compared to other nations, as it is an oil and gas exporting nation.

- After President Trump suggested his openness to a long-term Iranian-controlled SoH, Brent crude (the global benchmark for oil prices) increased, while West Texas Intermediate (WTI), the U.S. equivalent, declined.[7]
- A military operation to reopen the SoH would also very likely go beyond two to three weeks. Given the lack of immediate U.S. need for SoH energy supplies, there is a roughly even chance that President Trump will decide against such an operation, which will almost certainly cost U.S. lives.

While direct oil supply is less of a U.S. concern, the United States still depends on critical commodities from the Middle Eastern region, such as fertilizer and helium. These materials are vital for semiconductor chip production, which is dominated by Asia and heavily reliant on Middle Eastern oil and gas. Moreover, U.S. energy exporters are unlikely to benefit from Iran's ability to dictate energy price shocks.

If Iran maintains control of the SoH after the war, energy flows will likely remain intermittent, and prices are almost certain to remain elevated over the short term. If shipments through the SoH do not recover, the global economy will likely suffer via higher inflation and slower.

Iranian Response

Despite President Trump's comments forecasting a quick end to the war without Iran needing to make concessions, Iran is likely focused on the U.S. military buildup in the

[6] hXXps://understandingwar[.]org/research/middle-east/iran-update-special-report-march-31-2026/
[7] hXXps://oilprice[.]com/oil-price-charts/

region and likely views Trump's statements as an attempt to calm markets. Iran has pointed to these deployments as evidence that the United States is not serious about reaching a peace deal and is secretly planning a ground attack.[89]

There is a roughly even chance that Trump is signaling his willingness to abandon the SoH to pressure Middle Eastern and NATO allies to absorb a greater share of the war burden. With some 5,000 U.S. troops having arrived in the region in recent days and more on their way, the U.S. military very likely has the capabilities to launch some form of ground operation now, which almost certainly expands its range of options.

- There is a roughly even chance the United States unilaterally ends its campaign after achieving limited military goals, such as degrading Iran's missile, nuclear, and naval capabilities over the next two to three weeks. This scenario would very likely leave Iran in control of the SoH, a possibility Trump suggested.
- Alternatively, there is a similar probability the U.S. military attempts to limit Iran's control over the SoH by blockading Iranian ships or conducting military operations that degrade Iran's ability to target commercial ships, such as seizing key positions like Kharg Island. However, any U.S. attempt to seize Iranian territory will likely elicit an escalation from Iran and Iran-aligned groups and would very likely lead to casualties among U.S. ground troops.

Despite these concerns, Iran's President Masoud Pezeshkian did signal that the country is open to ending the conflict—particularly after Trump suggested Iran could maintain control of the SoH with its military-political establishment intact.[10] However, Iran has not indicated it is moderating its demands and has stated it would only end the conflict if there are guarantees against future U.S. aggression, international sanctions are lifted, and recognition of Iran's right to develop nuclear technology is recognize—terms that have previously been unpalatable to the United States.

- Trump's remarks likely signaled that a peace agreement is not necessary for the United States to end the war. Moreover, his comments that the war would conclude with the United States having eliminated Iran's ability to obtain a

[8] hXXps://www.nytimes[.]com/2026/03/29/us/politics/us-marines-middle-east-iran-war.html
[9] hXXps://www.nbcnews[.]com/world/iran/iran-waiting-possible-us-ground-assault-troops-rcna265665
[10] hXXps://www.euractiv[.]com/news/iran-has-necessary-will-to-end-war-but-seeking-guarantees/

nuclear weapon and that the current government was superior to the previous leadership suggest the United States will not pursue diplomatic talks aimed at limiting Iran's nuclear weapons program or further pursuing regime change beyond what has been achieved in Operation Epic Fury. This scenario also implies that Iran will maintain its ability to exert control over the SoH.

- Iran's President Pezeshkian has very likely lost influence, as the IRGC has consolidated control following the death of Supreme Leader Ali Khamenei—and the likely incapacitation of his successor, Mojtaba Khamenei. Early in the conflict, Pezeshkian apologized to neighboring countries that had been affected and approved the suspension of attacks against them unless Iran was targeted by those countries.[11] Pezeshkian retracted his apology the next day, reportedly under pressure from IRGC hardliners. While Pezeshkian's comments likely reflect a minority position in Iran, the IRGC almost certainly rejects this position—especially since the IRGC is likely distrustful of any U.S. or Israeli security guarantees. However, if Iran is able to reach an agreement without conceding its core demands, the IRGC will likely support the outcome.

Iran is unlikely to halt its attacks until it has confirmed the United States is ending the conflict. To this end, on March 31, 2026, the IRGC issued a warning to 18 companies (including 16 U.S. and two Dubai-based companies) threatening them with attack for their alleged support of U.S. and Israeli war efforts.[12] The companies named in the warning included:

- Apple
- NVIDIA
- Cisco
- HP
- Intel
- Oracle
- Microsoft
- Google
- Meta

[11] hXXps://edition.cnn[.]com/world/live-news/iran-war-us-israel-trump-03-07-26
[12] hXXps://www.cnbc[.]com/2026/04/01/iran-irgc-nvidia-appple-attack-threat.html

- IBM
- Dell
- Palantir
- JP Morgan
- Tesla
- General Electric
- Boeing
- Spire Solutions (a UAE-based cybersecurity solutions and services provider)
- G42 (a UAE-based artificial intelligence company)

The IRGC suggested that employees stay away from their places of work in order to "preserve their own lives." Additionally, the IRGC stated the companies should expect destruction of their businesses beginning at 8:00 PM Tehran time on April 1, 2026.[13]

Both the IRGC and Iran's Ministry of Intelligence and Security (MOIS) likely have robust networks across the United States and Europe and are very likely capable of conducting terroristic attacks against civilian targets, such as the companies named in the warning. Iran has already demonstrated its willingness and ability to recruit operatives during the course of the current conflict, even hiring agents via Snapchat to conduct operations on its behalf.[14]

The IRGC threats against U.S. and Dubai-based companies should be considered legitimate and taken seriously. Iran almost certainly has the capability and the motive to conduct lethal operations against civilian entities it has deemed as supporting U.S. and Israeli military operations. As the conflict continues, the likelihood of Iranian-directed, terroristic attacks in the West is increasing.

[13] hXXps://www.mirror[.]co[.]uk/news/world-news/breaking-iran-google-apple-microsoft-36950306

[14] 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

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

Handala Hack Team

On April 1, 2026, pro-Palestinian hacktivist group Handala Hack Team claimed to have compromised St. Joseph County, the U.S. state of Indiana's centralized IT infrastructure following an allegedly prolonged reconnaissance with access spanning state's prosecutor office, law enforcement, and health systems. The collective reportedly exfiltrated over 2 TB of sensitive data and destroyed 12 TB from core servers; in addition, Handala Hack Team publicly released 2,000 alleged internal documents, alongside a mass fax campaign distributing the breach details across organizations in the United States.

- Exposure of law enforcement, judicial, and healthcare data is likely to disrupt local governance and ongoing investigations, while the public release and mass dissemination tactics are likely to degrade public trust and influence similar waves of operations by other ideologically aligned actors.
- This operation also likely reflects a shift of the collective's focus toward psychologically disruptive campaigns targeting U.S. civic infrastructure.

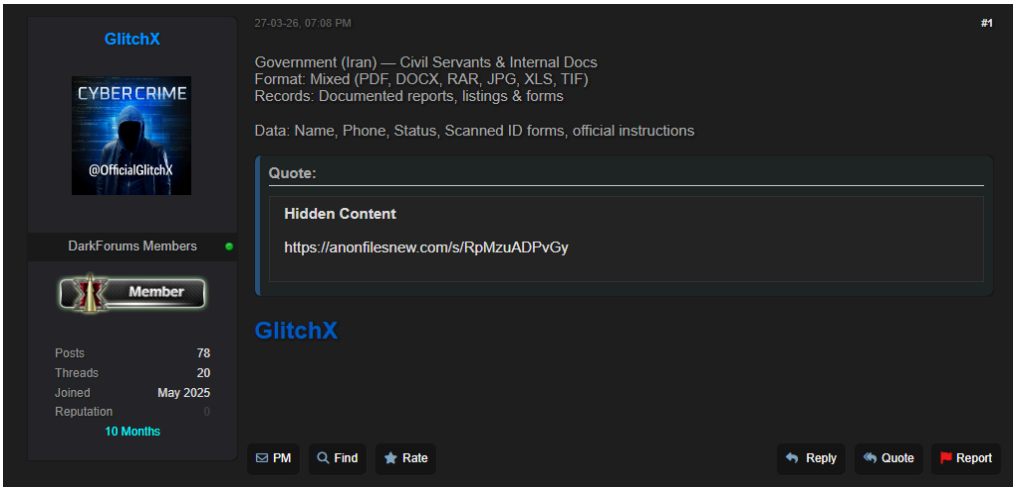
On March 31, 2026, Handala Hack Team claimed to have compromised IranWire, allegedly exfiltrating a large volume of correspondence, affiliate lists, and sensitive data, with its illicitly gained access further used to identify and monitor individuals linked to the outlet. IranWire is a digital news outlet allegedly funded largely by the U.S. State Department and influenced by Western political ideology, despite presenting itself as an

independent journalism outlet focused on Iranian politics, society, culture, and economy.[15][16]

- Given ongoing speculation regarding IranWire's alleged affiliation with Western-aligned entities, it is likely that Handala Hack Team targeted the outlet. Targeting media the Iranian regime would consider pro-Western or that has the ability to propagate uncontrolled information in the region is especially likely in light of Iran's documented enforcement of strict, state-controlled censorship.[17]

Dark Web Forum Activity

On March 27, 2026, a long-standing and untested actor known as "GlitchX" on the deep web forum Dark Forums posted a download link to a repository allegedly containing data belonging to the Iranian government, including information on civil servants and internal documents. The post stated that the dataset comprised mixed file types (DOC, PDF, RAR, JPEG, XLS, TIF) and included names, phone numbers, scanned identification forms, and official instructions.



GlitchX's post on Dark Forums
Source: ZeroFox Intelligence

On March 25, 2026, GlitchX posted a data sample and a download link to a repository purportedly containing approximately 240,000 records related to IRGC personnel. The data was described as being in .txt format and allegedly included full names, dates of

[15] hXXps://fpa[.]org/iranwire-where-professional-and-citizen-journalism-meet-2/
[16] hXXps://www.noirnews[.]org/p/iranwire-us-government-funded
[17] hXXps://rsf[.]org/en/war-iran-journalism-crisis-access-information-restricted-and-reporters-work-amid-bombs

birth, Social Security numbers (SSN), addresses, phone numbers, and identification details.

- Iran does not use the same SSN system as the United States and instead has a 10-digit national identification number.[18] The use of the term "SSN" in the original post likely shows the threat actors' ignorance of the Iranian system.

GlitchX first joined the forum in May 2025, and—despite having made 76 posts and contributing to 20 threads—the actor has not yet garnered a reputation score within the forum. At the time of writing, the credibility of the actor cannot be determined; thus, there is a roughly even chance that the free-to-download information is authentic.

[18] hXXps://www.ecoi[.]net/en/document/2021485.html

| 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%