ZEROFOX INTELLIGENCE

Flash

Iran Situation Update

F-2026-01-27a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Ransomware, Threat Actor, Geopolitics

January 27, 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 10:00 AM (EST) on January 27, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Iran Situation Update

Key Findings

- The Iranian government is reportedly conducting a brutal crackdown on anti-regime protests. Media reports have stated the death toll is as high as 35,000 protestors; however, human rights researchers have thus far confirmed approximately 6,000 are dead, with at least 18,000 deaths still under investigation.
- In response to the crackdown, the United States has moved an aircraft carrier and several destroyers into the region. This likely indicates a U.S. intention to force Iran to ease the crackdown measures, stop executing protesters, and establish a more peaceful stance towards its neighbors in the Middle East. If Iran does not comply, it is very likely that a U.S. military strike will occur in the next two weeks.
- Anti-regime activists briefly took control of Iran's state-run television to broadcast calls for further protests, and Iranian-backed threat actor collective "Handala Hack" used Starlink to conduct attacks against Israeli targets—despite a nationwide internet shutdown.
- Regardless of any military responses, cyber operations targeting Iran are almost certain to continue—and will likely increase—for the foreseeable future. Both the United States and Israel likely view the government in Iran as weak and are very likely to use cyber warfare to disrupt Iran's repression apparatus.

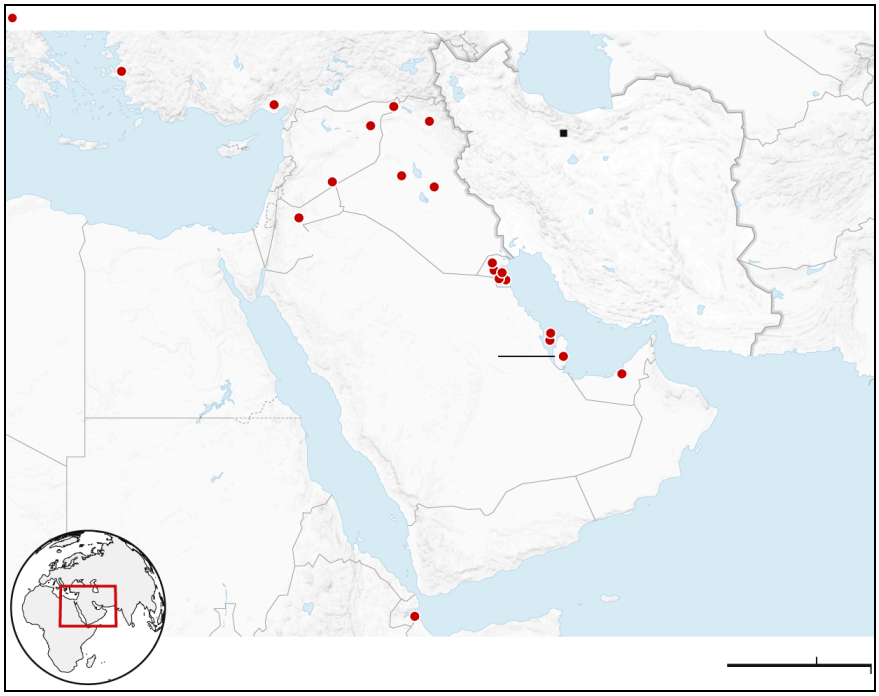
Details

The Iranian government is reportedly continuing a brutal crackdown on anti-regime protests. Media reports have stated the death toll is as high as 35,000 protestors;[1] however, human rights researchers have thus far confirmed approximately 6,000 are dead, with at least 18,000 deaths still under investigation.[2] Despite the brutal government response, the protests appear to be continuing, though the number of daily protesters has likely fallen.

Anti-government protests began on December 28, 2025, when Iran's merchant class, known as "bazaaris", took to the streets to protest the collapse of the Iranian rial—which lost 16 percent of its value in December 2025 alone.[3] In the early weeks of 2026, the protests grew to surpass the 2022 Masha Amini and 2009 Green Movement actions and are likely to become the largest and most consequential uprising since the 1979 Islamic Revolution.

- In response to Iran's continued crackdown, the U.S. Navy has moved the *USS Abraham Lincoln* and several guided-missile destroyers to the region. This is almost certainly intended as a power projection message to Tehran, but the fleet could also be used to conduct strikes to force Iran to comply with U.S. demands to stop killing civilians.
- The U.S. military has evacuated some troops from Qatar, United Arab Emirates, and other Gulf nations—likely to mitigate potential casualties in the event the allies strike Iran and Iran retaliates by attacking bases in the region.

[1] hXXps://www.iranintl[.]com/en/202601255198
[2] hXXps://www.en-hrana[.]org/day-thirty-of-the-protests-from-internet-disruptions-to-the-pursuit-of-the-injured/
[3] hXXps://infohub[].kz/tote/article/irans-protests-intensify-as-rial-collapses-inflation-hits-72-elite-rifts-widen.html



U.S. military bases in the Middle East

Source: hXXps://www.theguardian[.]com/world/2026/jan/23/trump-says-us-armada-heading-middle-east-iran-death-toll

The movement of U.S. forces into the region indicates a U.S. intention to force Iran to ease the crackdown measures, stop executing protesters, and establish a more peaceful stance towards its neighbors in the Middle East. If Iran does not comply, it is very likely that a U.S. military strike will occur in the next two weeks.

Meanwhile, cyber operations almost certainly continue on both sides of the brewing international conflict. On January 18, 2026, anti-regime activists briefly took control of Iran's Badr satellite, which broadcasts state-run television. The hijacked broadcast played messages from the exiled Crown Prince Reza Pahlavi, the son of Iran's last Shah (who himself was overthrown by the Islamic Revolution in 1979).

Screen capture of Reza Pahlavi's message

Source: hXXps://x[.]com/IranIntl_En/status/2012971768202301549

In the messages, the Crown Prince urged protesters to continue their resistance and called for security forces to put down their arms and join a wider revolution against the Islamic Republic. The hacked broadcast occurred around 9:30 PM local time and lasted for approximately 10 minutes.[4]

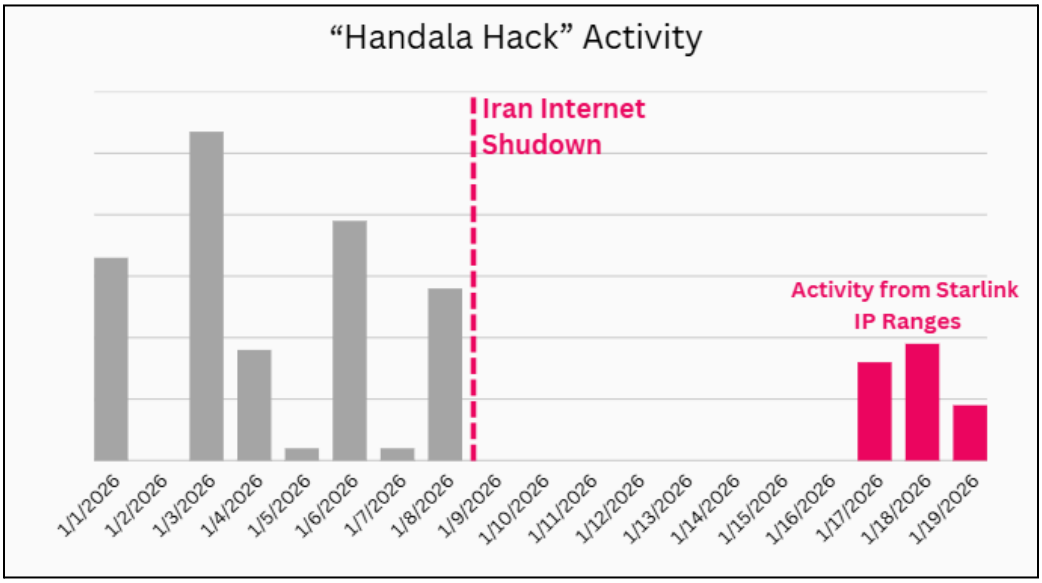
The fact that activists were able to gain access to Iranian satellite communications demonstrates that the regime's efforts to control communications is not perfect. There is a roughly even chance that this hack of Iranian state television was conducted with assistance from Israel or Western intelligence agencies. In the event of U.S. military strikes, it is almost certain more operations will strive to take control of Iranian airwaves and spread anti-government messages.

On January 17, 2026, cybersecurity researchers reportedly observed the return of Handala Hack, a threat actor associated with Iran's Ministry of Intelligence and Security (MOIS). Due to the almost total shutdown of internet connectivity by the Iranian government, Handala Hack is now routing their traffic through Starlink IP address ranges,

[4] hXXps://securityaffairs[.]com/187055/hacktivism/hacktivists-hijacked-iran-state-tv-to-broadcast-anti-regime-messages-and-reza-pahlavis-protest-appeal.html

utilizing the Elon Musk-owned technology to operate while the rest of the country lacks even basic online connections.[5]

Handala Hack is almost certainly focusing their operations entirely on Israeli targets. The collective is well-known for conducting attacks against Israel in support of MOIS operations and wider-regime strategic objectives.



Handala Hack activity

Source: hXXps://www.iranintl[.]com/en/202601205735

Additionally, the Iranian regime has reportedly been highly successful in suppressing and jamming Starlink—at least for civilian use. According to at least one report, GPS-spoofing by regime security agencies has rendered Starlink barely usable.[6]

While Hadala Hack's use of Starlink is likely serving regime objectives, it is also almost certainly giving away threat actor positions. With the threat of U.S. military action looming, it is likely an operational security shortcoming for state-sponsored threat actors to make themselves so visible. The United States is very likely to target infrastructure in

[5] hXXps://www.forbes[.]com/sites/zakdoffman/2026/01/20/irans-hackers-caught-using-elon-musks-starlink-to-attack-israel/?ss=cybersecurity

[6] *Ibid.*

Iran that supports regime stability and projects Iranian military force—this almost certainly includes MOIS facilities and hackers.

As the situation in Iran continues to move from persistent uprising to repressive government response, it is very likely the United States will conduct military operations—unless the recent U.S. Navy show of force in the region results in Iran complying with U.S. demands. In the event of regional conflict, Iran likely has few military options, but ballistic missile strikes against U.S. bases and allies in the region are very likely. Additionally, Iran maintains the last-ditch option of closing the Strait of Hormuz; however, this is unlikely unless the government of the Islamic Republic believes it is in an existential survival scenario.

Regardless of any military responses, cyber operations targeting Iran are almost certain to continue—and will likely increase—for the foreseeable future. Both the United States and Israel likely view the government in Iran as weak and are very likely to use cyber warfare to disrupt Iran's repression apparatus. Iran's cyber defenses are unlikely to be as strong as Western offensive capabilities, which will likely make Iranian networks vulnerable to sophisticated attacks. U.S. and Israeli cyber operations would almost certainly focus on further weakening the regime and limiting the ability of Iranian security forces to control the ongoing protests.

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%