MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

The Invisible Battlefield: Information Operations in the 12-Day Israel–Iran War

Harsh Yadav

October 28, 2025

Summary

Israel and Iran treated the information domain as a battleground, where legitimacy and perception were as crucial as kinetic outcomes. Israel's campaign focused on delegitimising the Iranian regime and reinforcing its own image as a stable and responsible regional power. Iran's efforts were aimed at sustaining cohesion, projecting strength, and countering Israeli narratives.

Introduction

Sun Tzu had recognised that 'All warfare is based on deception'. In contemporary times, this idea has evolved into what military doctrines describe as Information Operations (IOs). NATO defines IO as

> a staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences in support of mission objectives.[1]

Information operations involve a coordinated effort to shape how different audiences, including enemy forces, domestic populations and the international community, think, feel and respond during conflict. These operations combine tools such as psychological influence, cyber activities, strategic communication and media management to gain an advantage in the information environment. Similarly, the U.S. Joint Doctrine (JP 3-13) views IO as:

> The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.[2]

These concepts were very much in evidence during the 12-day war between Israel and Iran, from 13 to 25 June 2025. Alongside the exchange of missiles and drones, both states also engaged in a struggle to shape domestic and international narratives. Israel sought to undermine the legitimacy of Iran's regime and highlight internal unrest, while Iran attempted to project military prowess and national unity. These parallel campaigns unfolded across social media platforms and digital news outlets, with AI-generated content transforming the information sphere into a critical battleground. The conflict marked a significant evolution in hybrid warfare, where the contest for influence in the information domain became inseparable from military and cyber operations.

Israel's Information Operations

Israel set as its central goals several operational objectives for its information-operations campaign against Iran, notably emphasising regime change, promotion of liberation and freedom, and countering Iranian narratives. These narratives were promoted by the Ministry of Foreign Affairs (MFA) and the Israel Defense Forces (IDF)

[1] **"Allied Joint Doctrine for Information Operations"**, NATO, January 2023.

[2] U.S. Joint Chiefs of Staff, **"Information Operations"**, U.S. Department of Defense, 20 November 2014.

officials. Simultaneously, it sought to limit panic and reassure domestic audiences by reporting interception figures and operational successes. By highlighting the effects of strikes and asserting air superiority over Iran through official social-media posts and animated visualisations, Israel demonstrated that IO are not merely a supportive tool, but an integral part of modern warfare. This dual approach served both to maintain domestic morale and shape external perceptions, highlighting how IO became an instrument of reassurance and influence.

Since the initial days of the conflict, Israel has launched a sophisticated campaign to spotlight internal disturbance within Iran. A notable early example came from Israeli Prime Minister Benjamin Netanyahu, who on 13 June 2025, released a video message on his official X (formerly Twitter) account in which he was seen addressing the people of Iran. In his statement, he said, "Our fight is not with you; our fight is with the brutal dictator who oppressed you for 46 years. I believe that the day of your liberation is near."[3] In this video, he framed Israel as a protector not only of its own people, but also of its Arab neighbours, by stating,

> Our actions against Hezbollah led to the establishment of a new government in Lebanon and the collapse of Assad's murderous regime in Syria. Now the people of these countries has a chance of different future, a better future.[4]

The video further asserted that Iran's ambitions extended beyond Israel, posing threats to cities in Europe and ultimately to the US, through its long-range missiles, which are capable of carrying nuclear warheads. He also mentioned that Iran calls Israel "small Satan" and America the "great Satan", thereby portraying the conflict as part of a larger ideological struggle.

This direct address by the Israeli Prime Minister was not merely a political statement; it reflected the strategic use of leadership communication as an instrument of IO. By framing Israel as a protector of its own people, the Arab neighbours and European countries, Netanyahu sought to expand the cognitive boundaries of the conflict, beyond a bilateral contest with Iran and also portray Israel's actions as legitimate and necessary. This message aimed to make a moral and strategic impact on domestic and international audiences. The appeal to the Iranian people shows that from the initial days of the conflict, the primary focus of Israel was to delegitimise the Iranian regime.

Pro-Israel Telegram channels and X (formerly Twitter) accounts broadcast footage of previous protests, presenting them as real-time reactions to Israeli strikes. Hashtags

[3] Benjamin Netanyahu - נתניהו בנימין (@netanyahu), **"Moments ago, Israel launched Operation 'Rising Lion'…"**, X (formerly Twitter), 13 June 2025.

[4] Ibid.

such as #DownwithTheRegime and #FreeTehran trended on both local and global platforms and were sometimes coordinated by bot networks and diaspora influencers.[5] The IDF in an X post on 20 June 2025 shared a video with the caption "This is what it means to live under the Iranian Regime", compiling images from past protests and branding the Iranian government as "Regime of Terror". In this video, the speaker focuses only on the facts and narrative on how the Islamic Revolutionary Guard Corps (IRGC) and the Iranian government suppressed any protests that emerged in the past.[6] While the content was primarily based on historical events, the strategic impact of this video lay in shaping perception, portraying Iran as internally unstable and undermining regime legitimacy in the eyes of both domestic and international audiences.

The Iranian Ministry of Intelligence, in its report on 29 July 2025, described this conflict as a conventional military campaign, framing it as a hybrid war that included 'cognitive warfare' alongside 'psychological operations' and sabotage.[7] The report highlighted and accused the US, Israel and their allies of carrying out 'psychological operations, and cognitive and perceptual warfare' through social media and global media supported by advanced technologies such as artificial intelligence. This official framing clearly shows that Iran views IO not as peripheral, but as a central and long-term threat to its national security.[8] Iran's acknowledgement demonstrates that Israel's activities have strategic weight. These operations are perceived by adversaries as capable of influencing stability and national security, validating IO as a primary tool of hybrid conflict rather than a secondary tactic.

Israel's information machinery was aimed at shattering regime legitimacy among the Iranian people. For instance, a public statement from Israeli officials and military leaders, highlighting the messages of liberation and freedom, was released by the Israeli Foreign Minister Gideon Saar on his X account, stating: "We warned Iran time and again: stop targeting civilians! They continued, including this morning. Our response: Viva la Libertad, carajo! (meaning Long live freedom)." In this post, he also shared a video of the Evin Prison Blast, which is popular among the political prisoners of the Iranian regime.[9] While this video appears to be fake and was probably AI-generated, as confirmed by many fact checks of different news agencies, its strategic impact was clear, by showing that Israel was trying to show Iranian domestic repression to a global audience and simultaneously frame Israel as a

[5] Matt Murphy, Olga Robinson and Shayan Sardarizadeh, **"Israel-Iran Conflict Unleashes Wave of AI Disinformation"**, *BBC News*, 20 June 2025.

[6] Israel Defense Forces(@IDF), **"This is what it means to live under the Iranian Regime…"**, X (formerly Twitter), 20 June 2025.

[7] **"Institute for the Study of War (Critical Threats Project)"**, Iran Update, 28 July 2025.

[8] **"Silent Battle with NATO Intelligence in the 12-Day Imposed War"**, DefaPress, 29 July 2025.

[9] Rachel Baig, **"Fact Check: Viral Evin Prison Blast Video Is Likely AI Fake"**, *DW News*, 28 June 2025.

supporter of liberation and freedom. Later, this post was deleted, however, by the time it was removed, the intended impact of shaping perception and amplifying Israel's narrative had already been achieved.

Another example of IO by Israel was the 18 June 2025 TV hack. Iranian anchors were cut off mid-broadcast as protest imagery and slogans flooded the screen. Israel's UN envoy then shared the clip on social media, amplifying the message globally.[10] This operation mixed cyber intrusion with narrative warfare: by combining real footage of domestic unrest (woman, life, freedom, protests) with a call to action against the regime and aiming to delegitimise Iranian authorities in the eyes of their citizens. Another example of the use of the cyber domain of IO by Israel is reports which indicated that on 17 June 2025, the hacker group Predatory Sparrow, widely believed to have links with Israel, targeted Iran's Bank Sepah and a major cryptocurrency exchange, disrupting financial transactions and reducing confidence in state institutions.[11] This illustrates Israel's integration of technical cyber capabilities with cognitive influence, using multi-domain IO to maximise domestic disruption and international strategic messaging.

Throughout the operation, the IDF maintained a constant online presence, uploading animated and live videos, during the operation and strikes on Iran on their official YouTube channels and X account. IDF was constantly sharing the maps of the sirens operated during the Iranian missile strike and sharing posts like 'Attacking is not equal to targeting'.[12] By doing this, they were trying to create a narrative that Iran was attacking civilians, while Israel had only attacked military infrastructure. In another post, the IDF stated that Iran is a global threat and the IDF is standing between them and the world.[13] Through these communications, Israel pursued dual objectives of legitimising its own military operations by portraying them as precise and pre-emptive while simultaneously framing Iran as an aggressor, threatening not only Israel but also regional stability.

Thus, Israel created a narrative that its strikes were legitimate and that it is the power that protects the entire region from Iran.[14] The strategic intent is clear: Israel's IO did not merely report military activity but also attempted to form a narrative by

[10] **"Iran Blames Israel for Hacking State TV Broadcast With Calls for Uprising"**, *The Times of Israel*, 19 June 2025.

[11] Rohit Kumar Sharma, **"The 12-Day War: Cyber frontlines between Israel and Iran"**, Commentary, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), 11 August 2025.

[12] Israel Defense Forces (@IDF), **"We target, they attack. As simple as that…"**, X (formerly Twitter), 17 June 2025.

[13] Israel Defense Forces (@IDF), **"If we don't stop them, you're next…"**, X (Formerly Twitter), 17 June 2025.

[14] Israel Defense Forces(@IDF), **"We are the ones standing between you and Iran's terror…"**, X (formerly Twitter), 15 June 2025.

combining moral authority and regional security, thereby trying to influence public opinion and geopolitical discourse.

Iran's Information Operations

Iran's IO operational objectives were focused primarily on projecting military strength, maintaining regime legitimacy, and countering Israeli narratives. Iran sought to shape both domestic and international perceptions by exaggerating battlefield successes, crafting narratives of resistance, and mitigating the impact of Israeli information warfare aimed at destabilising the regime internally.

Iran launched an extensive campaign to amplify claims of military success against Israel, frequently circulating AI-generated and doctored videos depicting Israeli F-35 aircraft being shot down,[15] missile strikes on key locations such as Tel Aviv, or large-scale damage to Israeli facilities. Many of these claims, including the downing of an Israeli F-35, were later exposed as recycled footage; the international spokesperson of the IDF later called it "fake news" on his X (formerly Twitter) post.[16] However, by then, they had achieved their immediate objective of demonstrating strength and retaliation capability. The intent was not to convince international military experts, but to reassure domestic audiences that Iran could withstand and respond effectively to Israeli aggression. By doing so, Tehran sought to sustain morale at home and uphold the broader narrative of resistance that legitimises the regime in times of crisis.

Iran's Islamic Republic News Agency (IRNA) claimed multiple Israeli fighter jets were shot down, and the fate of the pilot is unknown.[17] The IDF immediately denied it and called it "Fake News". Many social media users who supported Iran used a photo of a Chilean navy aviator named 'Daniela Figueroa Scholz' from 2021[18] as a captured Israeli female pilot, which was entirely out of context. This episode illustrates Iran's reliance on rapid, sensationalist messaging to seize the information space before verification could challenge its narrative. In information warfare, speed often outweighs accuracy, a principle Iran used effectively.

Numerous viral posts showed the massive damage to big cities in Israel, like Tel Aviv and others. Fact checkers traced these to AI-generated images or video game

[15] **"Iran Claims Air Defence Shot Down Israeli F-35 Fighter Jet"**, *Iran Wire*, 14 June 2025.

[16] LTC Nadav Shoshani (@LTC_Shoshani), **"Fake News Detector: Iran didn't shoot down any Israeli fighter jets. They are trying to create a fake victory narrative, and it's not going very well…"**, X (Formerly Twitter), 14 June 2025.

[17] **"Iran Shoots Down Another F-35 Fighter Jet Belonging to Israel: Army"**, *Islamic Republic News Agency*, 14 June 2025.

[18] **"Fact Check: Chilean Navy Pilot Falsely Said Online to Be an Israeli Pilot Captured in Iran"**, *Reuters*, 23 June 2025.

footage.[19] While such tactics risk undermining credibility in the long term, they are effective in the short term for creating confusion and eroding trust in Israeli capabilities. These operations serve the dual purpose of first strengthening domestic unity and contributing to psychological warfare by framing Israel as vulnerable.

These narratives were not limited to the claims by media houses and individuals, but Iranian officials and the state media were also a part of this information warfare. For instance, on 16 June 2025, IRNA announced that Iran had launched the "largest and most intense missile attack" on Israel.[20] Israel reported the firing of fewer than 100 Iranian missiles, with most being intercepted. Similarly, the governor of Varmir (near Tehran) claimed an Israeli F-35 had been shot down.[21] These exaggerations formed part of a coordinated state effort to reinforce Iran's deterrent image and to portray parity in the conflict, where the military balance was tilted towards Israel.

In addition to media and narrative operations, Iran leveraged several cyber tools against Israel. One of the most revealing features of Iran's cyber operations during the war was its effort to gather real-time information by hacking Israeli internet-connected closed-circuit television (CCTV) systems, to improve the precision of its missile strikes and for damage assessments.[22]

Complementing these offensive measures, Iran exercised strict control over the flow of information. During and after the ceasefire, Iran controlled the messaging and propaganda domestically. On the first day of the truce, there were instances of threatening text messages by the judiciary, warning that they could be prosecuted if they "follow or subscribe to pages affiliated with Israel".[23] On the other hand, Iranian state media emphasised martyrdom, resistance and loyalty to foster public support, featuring emotionally charged programming on the sacrifices of IRGC members, as well as glorifications of figures targeted by Israeli strikes.[24] Another example of Iran's effort to control information flow and prevent cyber-attacks by Israel was to implement complete internet blackouts as a defence mechanism.[25] This demonstrates Iran's effective use of IO not only in the offensive domain, but also in the defensive domain.

---

[19] **"Tech-fueled Misinformation Distorts Iran-Israel Fighting"**, *Arab News*, 24 June 2025.

[20] **"Iran Strikes Back at Israel With Missiles Over Jerusalem, Tel Aviv"**, *Reuters*, 14 June 2025.

[21] **"Iranian Official Claims Israeli F-35 Fighter Jet Shot Down Near Tehran"**, *Middle East Monitor*, 18 June 2025.

[22] Nima Khorrami, **"Digital frontlines: What the 12-day war revealed about the evolution of Iran's cyber strategy"**, The Middle East Institute (MEI), 4 August 2025.

[23] **"شهروندان به دادگستری تهدیدآمیز های‌پیامک ارسال بس؛آتش اول روز** (First day of ceasefire; threatening text messages from the judiciary sent to citizens)", *IRANWIRE*, 25 June 2025.

[24] **"Iran Says Powerful Military Response Forced Israel to Halt Aggression Unilaterally"**, *Press TV*, 24 June 2025.

[25] **"Tech in the Iran-Israel conflict: internet blackout, crypto burning and home camera spying"**, *The Guardian*, 24 June 2025.

Conclusion

The 12-day war between Israel and Iran showed that IOs have become a decisive part of modern warfare. Both states treated the information domain as a battleground, where legitimacy and perception were as crucial as kinetic outcomes. Israel’s campaign focused on delegitimising the Iranian regime and reinforcing its own image as a stable and responsible regional power. At the same time, Iran’s efforts were aimed at sustaining cohesion, projecting strength, and countering Israeli narratives. Both countries used offensive and defensive IO, which makes IO as crucial as other domains of warfare.

The conflict thus highlights a broader shift in how warfare will be conducted in the future. While IOs have been used in warfare for centuries, the increasing application of emerging technologies such as artificial intelligence and deepfakes adds a new layer of complexity to the way warfare is understood and strategies are formulated. For contemporary strategists, the Israel–Iran case demonstrates that success in future conflicts will depend not only on technological superiority and battlefield performance, but also on the ability to dominate the information environment.

About the Author

Mr. Harsh Yadav is Research Intern at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses