

# Iran's hybrid war with United States, Israel

## Competition in cyber, cognitive domains

By Razia Bahrami

Expert at Institute for Political and International Studies

### OPINION

Tensions between Iran, on one hand, and the United States and the Israeli regime, on the other, have developed over several decades and have been shaped by political, military, and ideological factors. These tensions intensified following the assassination of Iranian Major General Qasem Soleimani by the United States in January 2020, alongside ongoing disputes over Iran's nuclear program and its regional role. During two periods when diplomatic negotiations between Iran and the United States were underway, Washington carried out two separate military attacks against Iran, effectively undermining the diplomatic process. After the multi-day second operation that started on February 28, 2026, Iran fulfilled its promise to retaliate strongly, and the confrontation gradually assumed a regional dimension.

From the early stages of this second conflict, the Israeli regime expanded the electronic dimension of the confrontation through cyber operations and attacks on electronic infrastructure. At the same time, Iran's closure of the Strait of Hormuz extended the conflict into the economic and energy domains. As a result, the war evolved into a hybrid conflict encompassing military, economic, energy, media, electronic, and even agricultural and industrial arenas. Tensions escalated to the point that the president of the United States openly threatened to destroy Iran's infrastructure. The confrontation between Iran and the Israeli regime has moved beyond conventional warfare into a complex and technologically driven domain. Under the cease-fire, the conflict is now unfolding across cyber, electronic, and information dimensions, placing the vital infrastructure of both sides under constant threat. The following sections examine various aspects of this new form of warfare — from cyber operations to cognitive warfare.

#### Cyber warfare against electronic infrastructure

As mentioned before, the recent conflict between Iran and the Israeli regime has taken on new dimensions, extending beyond direct military confrontation. The war is now being waged in cyber, electronic, and information spaces, with both sides leveraging advanced technologies to gain superiority. Cyber and electronic attacks carried out during two US and Israeli strikes in 2025 and 2026 can be analyzed across the following dimensions:

##### 1. Cyber warfare and vulnerabilities

Recent events have shown that despite claims of cyber superiority, both sides possess vulnerabilities in their digital infrastructures. Reciprocal attacks targeted banks, cryptocurrency exchanges, government services, and information networks, with the intensity of operations increasing severalfold compared to previous years. In June 2025, the hacker



On the 78th nightly gathering since the start of the 2026 US-Israeli war in Tehran, Iran, a woman and a toddler take a selfie with the blue and pink drones that became famous when Iranian armed forces started sending messages on their retaliatory drones and missiles.

● AHMAD MOEINI JAM/IRNA

group "Predatory Sparrow" disrupted the operations of Iran's Sepah Bank and inflicted damage on the Nobitex cryptocurrency exchange. Months later, on March 11, 2026, a missile strike targeted a Sepah Bank building, tragically resulting in the martyrdom of several employees.

**2. Attacks on infrastructure** Cyberattacks on financial, communication, and security infrastructures on both sides caused temporary disruptions. Hactivist groups and security structures employed methods such as DDoS attacks, phishing, and targeted intrusions to disable systems. Reports of such reciprocal attacks were circulated in Iranian and Hebrew-language media in January 2026.



The image, reportedly published by the now-infamous news agency SalamPix, showing protesters holding hands in unity during the January 2026 riots in Iran is reviewed by DW to be AI-generated and fake.

● DW



##### 3. Electronic warfare against drones

Drone warfare emerged as one of the primary arenas of confrontation. Both sides sought to disrupt GPS signals, sever communication links, inject false data, and employ artificial intelligence to divert or neutralize drones.

##### 4. Cyber defense structures

The Israeli regime relied simultaneously on specialized electronic warfare units and air defense systems, while Iran employed networks of electronic defense, indigenous counter-drone systems, and retaliatory cyberattacks.

##### 5. Expansion of the conflict into digital space

The spread of warfare into the internet and social media introduced numerous new actors — more than one hundred cyber groups — into the battlefield. Internet restrictions, real-time information dissemination, and an increase in online attacks were defining features of this phase.

##### Cognitive and narrative warfare

The digital battlefield was not limited to technical intrusions; misinformation, psychological operations, and efforts to influence public opinion also played a crucial role. The rapid transmission of information on social media became a key factor in



Groups of Iranian citizens participated in nightly gatherings and marches over several weeks. Yet due to digital communication restrictions and weaknesses in transmitting domestic narratives to the global arena, these reactions received limited international media and social media coverage, and thus the voices of segments of Iranian society were largely unheard in the global narrative battlefield.

shaping perceptions.

##### 1. AI-generated misleading images and content

The recent conflict witnessed a sharp increase in misleading content, particularly AI-generated materials circulating on social media. Advances in artificial intelligence tools have made the creation of fake images and videos easier, leading to a surge in posts attributed to AI-generated content on the X platform. Although this content still represents a small fraction of overall misinformation, it has introduced new complexities into the information ecosystem.

##### 2. Digital diplomacy or cognitive operations?

Donald Trump, by publishing more than three posts per day on the Truth Social platform, has played a prominent role in shaping global narratives. Analyses suggest that the primary objective of this continuous messaging is to influence financial markets, particularly oil markets, US stock exchanges, and equities. Evidence of suspicious transactions — such as stock purchases or oil trades conducted roughly 40 minutes before the publication of certain posts — points to the possible exploitation of insider information by specific actors for substantial profits. This approach adds new dimensions to the concept of information warfare and its impact on the global economy. On the opposing side, Dr. Mohammad Baqer Qalibaf, speaker of Iran's Parliament and head of the negotiating team, has sought to explain the hidden mechanisms of market manipulation to public opinion by publishing targeted analyses and data online. Meanwhile, reactions from users, media outlets, and even accounts affiliated with diplomatic institutions — such as Iranian embassies abroad — through replies, memes, and internet satire, have rapidly amplified war-related discussions in the public sphere. These interactions demonstrate how diplomacy and economics have become increasingly intertwined with the communicative and cultural dynamics of cyberspace.

##### 3. Lego-style animations in digital narrative-building by Generation Z

In recent years, Iran's Generation Z has creatively used digital media to discuss news events. One notable trend is the publication of short videos in a Lego-style animation format, produced by anonymous groups in Iran. These videos typically reconstruct news events in symbolic, humorous, or ironic ways and spread rapidly on social media due to their visual appeal and ease of production. Using Lego characters allows creators to present complex narratives in a simple and accessible format for younger audiences without depicting real individuals or scenes. As a result, this type of content has become a favored medium among younger generations for expressing experiences, reactions, and digital narratives.

##### 4. The strategic role of the Iranian diaspora in the conflict

During periods when domestic communications are disrupted or cut off, the resulting informa-

tion vacuum amplifies the voices of certain expatriate groups beyond their actual weight as access to diverse domestic narratives becomes limited. Under such conditions, some political factions within the Iranian diaspora are presented or perceived in international media as representatives of the opinions of 90 million Iranians, despite the fact that this image does not necessarily reflect the complex and multilayered reality of Iranian society.

Moreover, some migrants may believe that external pressure or international intervention can accelerate internal change — a perception rooted in their distance from domestic realities or their different experiences in Western societies. Consequently, the cognitive gap between the diaspora and domestic society often leads to narrative conflicts and deep misunderstandings, particularly when groups abroad assign themselves a role exceeding the actual capacity of the migrant community.

##### 5. The arena of lost narratives: a silenced voice

With the expansion of social media into the public sphere, contemporary conflicts have entered a new domain — one that unfolds less on the military battlefield and more within the realm of perception, narrative, and public opinion. During the Israeli regime's war against Gaza, a sudden and widespread shift occurred in the online space, as user-generated content formed waves of narratives that influenced public sentiment across many parts of the world. As a result, conflicts increasingly entered the cognitive domain, where imagery, storytelling, and information flows play a decisive role in shaping global perceptions.

In the recent conflict with Iran, the US president adopted a new strategic communication pattern, attempting to provide real-time and widespread war narratives directly to global public opinion. However, Iran's situation differed significantly from cases such as Gaza. Extensive disruptions and shutdowns of the internet inside the country prevented a large portion of Iranian society's narratives and reactions from reaching beyond national borders. As a result, global public opinion had limited access to direct representations of domestic social reactions.

This occurred despite the emergence of social mobilization within Iran, including street presence and demonstrations supporting the state and protesting foreign attacks. Groups of citizens participated in nightly gatherings and marches over several weeks. Yet due to digital communication restrictions and weaknesses in transmitting domestic narratives to the global arena, these reactions received limited international media and social media coverage, and thus the voices of segments of Iranian society were largely unheard in the global narrative battlefield.

##### Transformation of power in hybrid warfare

An examination of the dimensions