Realistic look at 12-day war

Iran engaged in asymmetrical intelligence warfare

A firefighter calls out to his colleagues at the scene of an explosion in a residential compound in northern Tehran, Iran, on June 13, 2025.
VAHID SALEMI/AP

ANALYSIS

The recent 12-day Israeli war against Iran served as a no-nonsense test of both sides' strategic capacities — a test that, while carrying its own political messages, brought to light intelligence weaknesses that had previously flown under the radar.

For those still stuck in the "pre-data" era, war means tanks and missiles. But hopefully, the recent 12-day conflict has driven home the fact that the real battle plays out in command centers, cyber networks, and intelligence circuits.

When an adversary, who's been posing as your enemy for years, knows the exact impact points, routes of access, and obstacles, while you're still in the dark about the most likely avenues of its attack, even a military edge in hardware can count for little due to this disparity in technology and intelligence.

What really matters in this and all recent wars is the objectives left on the table, the blind spots overlooked, and the intelligence missed.

Iran's information gaps, technological shortcomings, and cyber flaws in the recent military crisis can be broken down into tech, interception, and intelligence lag.

From battlefield to satellite

Reports indicate that Iran's cyber capabilities fell short against Israeli attacks in the early days of the war, to the point where Iran had to shut down the internet to ward off Israeli cyber offensives as there was no effective way to plug information leaks other than that.

Iran's Organization for Passive Defense, the IRGC Cyber Command, and the Cyber Police (a.k.a. the FATA police) — are tasked with fending off internal and external cyber threats. Yet, Iran also benefited from hacker groups during the war. One such group, Handala Hack, claimed to have dealt a blow to Israel's cyber infrastructure.

On the other hand, Israeli cyberattacks on banks and exchanges and even the GPS tracking of some top officials were reported, though some of these claims may have been hyped up for propaganda purposes.

The Predatory Sparrow group, apparently tied to Israeli intelligence, carried out serious attacks on Bank Sepah and the Nobitex crypto exchange, with The Wall Street Journal reporting that about $90 million in crypto was frozen during these attacks. ATM services also hit a snag in the first few days, but fortunately, the disruptions didn't drag on for more than two or three days.

Iran also launched numerous cyber offensives against Israel, but these were scattered and reactive, rather than proactive.

The war made it clear that there's a pressing need to set up a cyber-intelligence defense structure with offensive capabilities. Iran must also step up its game in real-time information management or C4ISR. C4ISR (which stands for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) relies on advanced technologies for each element.

Commanders must be able to get up to speed instantly and accurately, make coordinated decisions, direct forces and weapons purposefully, and, most importantly, keep tabs on the opponent's moves and information using existing tools.

In countries like the US, warfare revolves around network-centric operations, pushing C4ISR to the next level. For instance, in data fusion — pulling together multiple information sources like radars, satellites, drones, and intercepts — the process should yield more precise and actionable results, thanks to cutting-edge tech.

Israel has zeroed in on artificial intelligence, with systems like the ELS-8994 Starlight integrating disparate data on a single platform and delivering it to commanders in record time. Units like the Oz Brigade and Ghost Brigade combine ground, aerial, satellite, and drone data, enabling split-second decision-making.

Information is power

While Iran has recently gotten the ball rolling on electronic warfare and AI, it hasn't reached full throttle yet. The 12-day war should serve as a wake-up call to pick up the pace in this area.

Iran does have quality radars like Ghamar, which can gather imagery, but firstly, there's a need for a clear integration platform. Secondly, since drone and radar data are usually processed separately by the Army, IRGC, and Ministry of Defense, this slows down decision-making.

Another example is SIGINT (signals intelligence) technology. Israel has poured resources into these centers for years, with Unit 8200 standing out as the region's largest intelligence, interception, and code-breaking organization. This unit eavesdrops on officials from target countries like Iran and Lebanon, analyzes intercepted data, tracks radio, satellite, and internet signals, and cracks encrypted communications.

The Urim SIGINT Base, along with Hermes 900 and Heron TP drones equipped with powerful tracking gear, work around the clock as Mossad's auxiliary arms. During the recent 12-day war (June 13–25, 2024), Israeli intelligence officials claimed that by listening in and tracking Iranian security and military figures, they had pinpointed their locations and defense weaknesses — much of this carried out by Unit 8200 through decrypting military command messages.

Iran does have satellites, reconnaissance drones, and SIGINT trackers at sensitive borders but is still playing catch-up in developing these tools, with most data analysis still handled by humans rather than AI.

There's much more to say in this field — a field that opened up an invisible front in the recent war, a battlefield of signals and data. In a world where "information is power," falling behind in technology is more than just a technical gap. Iran must rewrite the rules and hold its ground in this arena. The rules of today's world don't allow anyone to just sit on the sidelines and watch the relentless battle of information and AI.

The article first appeared in Persian on Asriran news website.

> The war made it clear that there's a pressing need to set up a cyber-intelligence defense structure with offensive capabilities. Iran must also step up its game in real-time information management or C4ISR. C4ISR (which stands for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) relies on advanced technologies for each element.

The picture provided on September 1, 2021, shows Iran's state-of-the-art 3D radar, Alborz, being paraded during a special ceremony.
IRNA

An illustration of IAI-Elta's automated signal intelligence center of Israel
IDF