Iran adopts the strategy of chaos even in cyberspace

Published on 16/03/2026

A report by Maticmind highlights an intensification of cyber activities linked to Tehran: over 600 claims in one week. Not just sabotage, but above all psychological pressure, infiltration, and strategic espionage.

The war between Iran, Israel, and the United States is not only fought in the skies of the Middle East. For some time now, a second front has opened with increasing intensity in cyberspace, where Tehran seems to move according to a precise logic: sow chaos, increase pressure on adversaries, and build coercive tools to use over time.

This escalation is captured in a report by **Maticmind**, an Italian company of the Zenita group specializing in cybersecurity. According to the analysis, in the last seven days, there has been a significant increase in cybercriminal activity attributable to Iran: **over 600 attack claims**, with a **peak of more than 50 per day**, attributed to **47 different actors** and targeting sensitive objectives in **11 countries**.

Among the most targeted are **Israel and the United States**, followed by **Saudi Arabia, Jordan, and Kuwait**. But the range of action seems to extend beyond the Middle East. Also targeted were **Canada**, due to political support expressed to Washington and Tel Aviv, and other **European and NATO countries** with public positions considered aligned with Western interests.

Iran adopts the strategy of chaos even in cyberspace

The logic of Jang-e-Ashub

At the base of this offensive is what Maticmind defines as **"Jang-e-Ashub"**, or "war and chaos". According to the report, it is not a strategy designed to win a conflict with a single decisive blow, but rather a form of continuous, psychological, and negotiable pressure.

The model develops in several phases. The first is that of demonstrative attacks, such as **wipers** against Israeli or Saudi targets, useful to show Iranian response capability without leading to direct military confrontation. This is followed by a phase of threat amplification, where the perception of an imminent attack is fueled, and the adversary is destabilized.

The last step is the most delicate: the silent infiltration of the computer systems of the affected countries to obtain **persistent and dormant accesses**, to be activated at the opportune moment. In this way, cyber becomes a lever of indirect pressure, a tool to be used in moments of greater political or military tension.

For European organizations, observes Maticmind, the most immediate risk would not be so much that of a sudden blackout, but rather that of **prolonged espionage** and the exposure of the **cloud supply chain**.

More espionage than destruction

Behind the noise of the claims and the media impact of the attacks, the main objective seems to be one: **gather strategic information**.

Groups close to Tehran like **APT34, MuddyWater**, or **Charming Kitten** have been repeatedly associated with persistent operations within government, energy, and military networks in various Middle Eastern countries. In many cases, these actors have maintained access to compromised infrastructures for months, if not years, with the aim of extracting sensitive data related to military capabilities, diplomatic negotiations, and strategic technological assets.

The distinctive feature of the Iranian approach, the report emphasizes, is precisely this gradualness: silent accesses, information gathering, consolidation of presence, and building pressure margins to be used when the context makes it useful.

More than a super weapon capable of producing spectacular and immediate effects, Iranian cyber thus appears as a **strategic influence tool**: less visible than a missile, but potentially just as effective in wearing down an adversary, undermining their confidence, and increasing the political cost of confrontation.

Iran adopts the strategy of chaos even in cyberspace

An increasingly central front

In this scenario, cyberspace is increasingly confirmed as a crucial battleground. Not only for the possibility of hitting sensitive infrastructures and systems, but above all because it allows continuous pressure to be exerted without openly crossing the threshold of conventional war.

It is in this gray area, made of limited sabotage, infiltrations, propaganda, and espionage, that Iran seems to want to play a decisive part in its regional and international game. A game in which chaos is not a collateral effect, but a deliberate strategy.

News link: https://www.ansa.it/canale_tecnologia/notizie/tecnologia/2026/03/12/iran-maticmind-zenita-group-oltre-600-attacchi-cyber-in-7-giorni_f42bcbce-a8e5-4f9c-8675-42ef956e6b00.html