فريق التحرير | نشر في 25 March 2026,

How Did “Israel” Turn Iran’s Surveillance Cameras into an Assassination Tool?

Following the assassination of several top-tier Iranian commanders, many observers have been preoccupied with a pressing question: how did “Israel” manage to achieve such a deep level of penetration within a state saturated with security and surveillance?

The most striking paradox is that the very street cameras designed to tighten control over Iranian society appear, in wartime, to have been repurposed into an intelligence asset one suspected of aiding the enemy in tracking, monitoring, and identifying targets.

Western reports, particularly from the Associated Press and the Financial Times, have pointed to an Israeli breach of Tehran’s traffic camera network, allegedly used to monitor security details guarding sensitive facilities and to build digital profiles of their movements.

How, then, did this network come into being? Why was it vulnerable to infiltration? And what does this episode reveal about a surveillance state when its digital infrastructure turns into a strategic liability?

How Iran Built a Surveillance State

In the wake of the “Woman, Life, Freedom” protests in late 2022 sparked by the killing of Mahsa Amini by the so-called “morality police” over alleged violations of Iran’s mandatory hijab laws the Iranian authorities accelerated the development of a sweeping digital surveillance project.

In April 2023, police announced the installation of smart street cameras capable of sending warning messages to women deemed improperly veiled, with the stated aim of “preventing resistance to the law.”

A Reuters report at the time revealed plans to deploy facial recognition technology to match images against a national database and penalize violations, all in the absence of a personal data protection law. Yet the system’s expansion went far beyond dress code enforcement.

A schematic map of the surveillance equipment used in the tourist area of Isfahan, based on eyewitness information shared with Filterwatch.

Human rights reports indicated that the network was also used to track dissidents. Authorities reportedly collected mobile location data, collaborated with delivery applications, and encouraged citizens to report violations via the police-affiliated “Nazer” app, which allows users to submit license plate numbers and addresses of “offending” women.

This was corroborated by a United Nations report in March 2025, which stated that Iran uses road cameras, surveillance drones, facial recognition tools, and the “Nazer” app to enforce dress codes while intensifying penalties and social exclusion for violators.

In major cities, metro screens in December 2023 displayed passengers’ faces, ages, and genders an unsettling demonstration of AI’s vast capabilities operating without oversight, sparking protests within municipal councils.

The government also relied on the technical capacities of Chinese firms and foreign expertise. A study by the Stimson Center found that at least eight Chinese companies supplied Iran with facial recognition technologies and surveillance cameras.

Authorities further deployed communication interception devices, balloons, and drones to monitor protesters, sending nearly one million text messages and issuing fines to vehicle owners for hijab-related violations in 2023 alone.

The expansion and dispersion of this network spanning tens of thousands of cameras across cities, universities, and highways has transformed Iran’s civilian space into a densely monitored environment.

How Cameras Became a “Target Bank”

In March 2026, the Associated Press published an investigation citing an intelligence official and a knowledgeable source, claiming that “Tel Aviv” had hacked most of Tehran’s traffic cameras, transmitting their data to servers in “Israel” and using artificial intelligence to construct “lifestyle patterns” of personal security teams.

One such camera, positioned to observe vehicles parked by guards near secure compounds, reportedly enabled israelis to identify their home addresses, routes, and schedules. According to the report, planners accelerated assassination operations when cameras detected officials arriving at command centers, while mobile communication devices were disabled to ensure operational success.

This was not the first such account. The Financial Times reported that Israel’s Unit 8200 had infiltrated the camera network years earlier.

It noted that a camera on Pasteur Street was used to track vehicles belonging to the security detail of Supreme Leader Ali Khamenei, compiling detailed profiles of names, addresses, and behavioral patterns using advanced algorithms and movement modeling.

The report also suggested that “Tel Aviv” and Washington disabled nearby mobile towers during the assassination operation to prevent warnings. The Times of Israel echoed these claims, highlighting the role of AI-driven data analysis.

Iranian lawmakers have criticized the Ministry of Communications’ performance. MP Mahmoud Nabavian went as far as to suggest that “all intersection cameras are in Israel’s hands,” an implicit acknowledgment of the breach.

Iranian media, for their part, have avoided technical details, instead attributing the incident to “hybrid warfare” and speaking of destroyed communications infrastructure.

Why Was the System Vulnerable?

Iran’s surveillance history suggests that the state expanded these technologies faster than it could secure them. Due to international sanctions, authorities rely heavily on Chinese hardware, low-cost equipment, or pirated versions of Western software.

According to the Associated Press, sanctions have forced Iran to use outdated hardware and compromised software making systems easier to breach. The sprawling network, composed of thousands of interconnected devices without unified security standards, creates significant vulnerabilities.

When opposition hackers released footage from inside Evin Prison in 2021 and later claimed to have breached 5,000 cameras in 2022, it underscored a critical lesson: outdated, unsecured systems become strategic weak points.

Iranian policies have further widened these gaps. In May 2024, the government proposed legislation requiring private sector cameras to be linked to police networks and retain recordings for 20 days, alongside facial recognition enforcement against those refusing surveillance.

A surveillance camera in one of Tehran’s streets, April 9, 2023 (West Asia News Agency – WANA)

Such integration between public and private systems expands the attack surface, introducing devices that may not meet strict security standards. Security experts cited by Reuters in 2022 warned that the absence of data protection laws increases the risk of misuse and data leaks.

Moreover, the sheer density of surveillance invites attacks. A report by cybersecurity firm Check Point noted that Iranian hackers themselves had attempted to breach hundreds of cameras across the Middle East suggesting that such technologies have become integral to cyber warfare playbooks.

When Cameras Become Weapons of War

Iran is not alone in facing this dilemma. In recent years, camera hacking has become a recurring feature of hybrid warfare.

According to Wired magazine, every side in modern conflicts views the opponent’s cameras as a low-cost intelligence asset:

Russian forces have targeted surveillance cameras in Ukraine.

Hamas has attempted to hack cameras in “Israel.”

“Israel” has reported Iranian cyberattacks on dozens of its own cameras.

U.S. General Dan Caine stated at a security conference that cyber operations including communication disruptions and camera breaches were part of pre-war preparations against Iran. Experts warn that outdated devices and weak security protocols make such breaches a matter of time.

This phenomenon exposes the contradictions of the surveillance state. Cameras are not merely tools of social control; they are nodes within a global digital network accessible to adversaries. When such systems expand without safeguards and become instruments of political power, they can swiftly transform into intelligence assets for the enemy in times of war.

The accumulation of vast datasets on millions of citizens without adequate legal or technical protections creates a highly attractive reservoir for both external and internal hackers. In the Middle East, where security concerns intertwine with social control, control over smart technologies has become an extension of the broader struggle for power.

رابط المقال: https://www.noonpost.com/en/368615/