Monday, March 23, 2026

tomorrowsaffairs.com

TA Tomorrow's Affairs

Analysis of today
Assessment of tomorrow

By: TA | AP Insight

Fish in a barrel - have surveillance networks become a danger to authoritarian regimes after Iran?

The role of Israel's hijacking of Iran's street cameras in the killing of the country's supreme leader underscores how surveillance systems are increasingly being targeted by adversaries in wartime.

Hundreds of millions of cameras have been installed above shops, in homes and on street corners across the world, many connected to the internet and poorly secured.

Recent advances in artificial intelligence have enabled militaries and intelligence agencies to sift through vast amounts of surveillance footage and identify targets.

On Feb. 28, Israel vividly demonstrated the potential of such systems to be hacked and used against adversaries when Israel tracked down Iranian leader Ayatollah Ali Khamenei with the help of Tehran's own street cameras - despite repeated warnings that Iran's surveillance systems had been compromised, according to interviews and an Associated Press review of leaked data, public statements and news reports.

The use of hacked surveillance cameras among other intelligence in the operation to kill Khamenei was described to the AP by an intelligence official with knowledge of the operation and another person who was briefed on the operation.

Neither was authorized to speak with the media and both shared information on condition of anonymity.

Iran has installed tens of thousands of cameras in its capital in response to waves of protests, most recently in January, when massive nationwide demonstrations ended in a bloody crackdown that killed many thousands of Iranians.

That Tehran's cameras were compromised was no secret: the city's cameras were repeatedly hacked starting in 2021, and last year, a senior Iranian politician warned publicly that cameras had been compromised by Israel, posing a national security threat.

Conor Healy, director of research at surveillance research publication IPVM, said Khamenei's killing illustrates a pressing security dilemma for governments seeking to quash dissent.

"The irony is that the infrastructure authoritarian states build to make their rule unassailable may be what makes their leaders most visible to the people trying to kill them," Healy said. "Do you trust who is watching?"

Warning signs

For years, cybersecurity experts have warned that cameras could be hacked for war.

In 2019, security engineer Paul Marrapese discovered he could easily hack millions of cameras from the comfort of his home office in California.

Despite speaking up repeatedly since, the number of unprotected cameras only continues to grow.

A scan of unprotected camera feeds this year turned up nearly three million hits in almost every country in the world, Marrapese told AP, including nearly 2,000 cameras in Iran alone.

"There are millions and millions and millions of these throughout the world," Marrapese said. Many, he added, are trivially easy to hack: "They're just dumb little things. ... It's fish in a barrel."

Companies have advertised cameras hooked up online, accessible with cellphones, with feeds easily diverted by hackers.

Many are installed with minimal security by unsophisticated users who fail to set up passwords or install security patches.

Securing cameras takes constant vigilance, but hacking them takes identifying just one exposed vulnerability, such as an outdated system or a generic password like "1234."

Even surveillance systems set up by

governments on networks sealed off from the internet are vulnerable: It takes just one insider turncoat to compromise such systems.

“Humans are kind of the weakest link,” Marrapese said. “There’s really only so much you can do.”

> Advances in AI have allowed militaries to overcome a critical hurdle in weaponizing hacked footage

Eyal Hulata, Israel’s former national security adviser and a senior fellow at the Foundation for the Defense of Democracies, said Israel is under constant cyberattacks from Iran but has so far been able to defend against it.

“There is high alert on all cyber fronts,” he said.

For years, hacking cameras for war remained theoretical. But in 2023, Hamas hacked surveillance cameras in southern Israel ahead of its Oct. 7 attack, allowing the group to monitor Israeli army patrols and assisting the attack, according to Israeli media.

That same year, a Ukrainian official told reporters that Russia attempted to hijack cameras near missile targets, a trend that continued in 2024 when Russians hacked cameras in Kyiv and last year, when they hacked cameras at border crossings.

Experts say advances in AI have allowed militaries to overcome a critical hurdle in weaponizing hacked footage: sifting through huge amounts of video to identify people, vehicles, and other targets, a task that once took teams of analysts weeks or months but can now be done in real time.

With a simple keyword search, AI can scan feeds and return results almost immediately.

“It used to be that you could hack the cameras, but humans had to do the real work of figuring out where the person was,” said cryptographer and security expert Bruce Schneier. “With AI systems ... you can do a lot more automatically.”

The despot's dilemma

Iran’s cameras have been repeatedly hacked over the past few years.

In 2021, an Iranian exile group leaked footage of abuses at Tehran’s notorious Evin prison. In 2022, another group claimed it hacked over 5,000 cameras around Tehran, dumping gigabytes of surveillance footage and internal data on a Telegram channel.

Then, during a 12-day war last summer, Israel used Tehran’s cameras to track and bomb the location of a meeting of Iran’s Supreme National Security Council, injuring Iranian President Masoud Pezeshkian, according to Iranian lawmakers and an Israeli documentary.

“All the cameras at our intersections are in the hands of Israel,” Mahmoud Nabavian, deputy chairman of the Iranian parliament’s national security committee, told Iranian media in September. “Everything on the internet is in their hands ... if we move, they will find out.”

The vulnerabilities have come amid Iran’s stepped-up use of surveillance cameras after a series of protests roiled the country.

Subway cameras, for example, are used to detect when women don’t don the country’s mandatory hijab, or headscarf, using facial recognition to identify violators.

But data collected to consolidate control creates a ripe target for hackers, said researcher Michael Caster, who investigated China's sales of surveillance technology to Iran.

“Malicious parties can more easily gain access," Caster said.

All the cameras at our intersections are in the hands of Israel - Mahmoud Nabavian

Iran in particular, long sanctioned by the West, faces difficulties in getting up-to-date hardware and software, often relying on Chinese-manufactured electronics or older systems. Pirated versions of Windows and other software are common. That makes it easier for potential hackers to target the country.

The Financial Times earlier reported on the use of cameras in Khamenei's killing.

The person briefed on the operation who spoke to the AP said that for years almost all the traffic cameras in Tehran had been hacked and the information transferred to servers in Israel.

At least one camera was at an angle that allowed Israel to track daily movements of people, such as where they parked their cars near Iran's leadership compound, the two people said.

Algorithms helped provide information including people's addresses, routes they took to work and who protected them, according to the person briefed on the operation.

That same person said the attack had been planned for months, but the operation was expedited once it was determined that Khamenei and his top officials would be in the leadership compound that morning.

Israel's prime minister's office didn't respond to request for comment.

Col. Amit Assa, a former official with Israel's Shin Bet domestic security service, said that such operations are powered by many sources of intelligence, such as undercover agents and bugged conversations.

However, Assa says cameras play a key role because they allow intelligence officers to identify people, providing key confirmation in deciding on whether to strike.

When you see a person's face on a screen in the command center, it helps in making the decision to put your "finger on the yellow button, as we say," he said.

More cameras, more coverage

Check Point Research, a cyber threat intelligence group, says Iranian hacking attacks on cameras have spiked since the beginning of the war, with surges of activity in Israel and Gulf countries such as Bahrain and the United Arab Emirates.

Such hacks could help Iran monitor targets and assess damage after missile strikes, according to Gil Messing, Check Point Research's chief of staff.

"The more people are installing cameras ... the more area is being covered by these cameras," Messing said. "It is very easy to use in order to get extra eyes into different places."

Analysts estimate there are more than one billion security cameras installed worldwide, triple the number a decade ago. Hundreds of millions more are installed every year.

Muhanad Seloom, assistant professor in security studies at the Doha Institute for Graduate Studies, said that oil-rich Gulf countries like Qatar have long known their petroleum facilities could be targeted in a war and had their systems tightly secured. But only recently have officials in the region realized that street cameras, too, could be weaponized.

"I don't think anyone anticipated that these traffic cameras would become targeting tools

... there is alarm all over," Seloom said. "How come Iran's whole leadership has been decapitated on the first day? ... It is a topic that is being talked about."

> Gulf monarchies have barred residents from filming or livestreaming footage of Iranian strikes

Across the region, governments are on high alert.

Gulf monarchies have barred residents from filming or livestreaming footage of Iranian strikes, with the UAE arresting dozens of people for sharing video of the conflict online.

Though aimed in part to protect the country's reputation, the bans are also motivated by concerns that such footage could be exploited by the Iranian military, Seloom said.

Earlier this month, Israel's National Cyber Directorate said that it had warned hundreds of camera owners targeted by Iran and urged the public to change passwords and update software to starve off attacks.

Ali Vaez, Iran project director at the International Crisis Group, said though hacking has long been a concern in the Middle East, its increasing use since the war began was "a wake-up call".

Still, he said there's only so much that can be done to patch up vulnerabilities.

"It's a whack-a-mole," Vaez said.