Iran: Be Afraid, Be Very Afraid (#4)

by Hugh Fitzgerald

Iran's intelligence forces have broken down in the face of a series of devastating explosions.

The story is [here](#):

What the world is witnessing right now is someone hitting Iranian nuclear and conventional weapons and IRGC facilities practically at will.

Iran is facing a total intelligence breakdown.

With another explosion on Thursday night, reportedly at an Iranian Islamic Revolutionary Guard Corps facility, the question is not only how anyone has pulled up to seven attacks off in around two weeks, but how has the Islamic Republic repeatedly failed to stop them….

In general, Iranian counterintelligence is known as performing at a much higher level than most Israeli adversaries. Sometimes they falsely announce arrests of Mossad agents who are just political opposition members, but sometimes they can flush out spies at a professional level closer to the world's top powers.

Until Israel's January 2018 operation seizing Iran's nuclear secrets, Iranian territory was thought of as much harder to penetrate than Syrian territory, where Israel has admitted to thousands of intelligence and airstrike operations.

In the days of Meir Dagan, a score of attacks on Iranian nuclear scientists were attributed to the Mossad….

To the extent that these are cyber-attacks, it might be more understandable that Tehran has caught no one and stopped nothing. Explosions perpetrated through a cyber-attack could have been pre-planted months or even years ago to be set off now.

But even in the cyber arena, US and Israeli officials have been warning that after the 2010 Stuxnet attack, the regime heavily improved as a cyber power.

However, what we appear to be witnessing are the limits of a second-tier counterintelligence force. Up against a premier intelligence or cyber power, Iran is apparently near defenseless…

Iran has been unable even to conclude which of the attacks on its facilities were the result of cyberattacks and which were caused by bombs placed inside military targets. It continues to insist that it does not know, a full two weeks after the most important attack, at Natanz, whether it was a Stuxnet-like cyberattack, as many Western experts now believe (or as they now say, it "was bigger than Stuxnet"), or a huge bomb placed near a gas pipe in the building by Iranian agents of Israel. Nor have the Iranians been able to satisfactorily explain the other six attacks that came in rapid and frightening succession. In every case they have at first minimized the attack's destructive force, misidentified the source of the explosion (lots of gas tanks were supposedly leaking), and misstated, or passed over in silence, the method used — that is, a kinetic or a cyber attack.

The Israelis are running rings around Iran's counterintelligence. Imagine the agents they must have deep within Iran's counterintelligence, to have known just how most devastatingly to attack the new centrifuge plant at Natanz, and the ballistic missile factory at Khojir, where top-secret work was going on which included the preparation of nuclear

warheads for intermediate-range ballistic missiles. And who helped the Israelis identify the other, seemingly innocuous civilian sites, some of which may in fact have been military facilities, that Israel struck with such devastating effect?

Think, too, of Iran's intelligence donnybrook when it failed to protect the records of its nuclear program. Iranian agents had to have identified for Mossad the nondescript warehouse where the records of Iran's nuclear project were hidden, information that led to the Israelis seizing 55,000 documents and 183 CDs detailing Iran's nuclear program, in the middle of the night, in the middle of Tehran, working furiously to open dozens of safes with blowtorches, knowing they had to be well out of there before 7 a.m., when Iranian employees arrived. Iran still has not figured out how the Israelis managed to carry off all that top secret cargo, or how they got themselves, and that enormous cache of material, safely out of Iran and back to Israel. But Iranian agents working with Israel— possibly anti-regime Iranians — were certainly involved. And not one has yet been caught.

Israel's spectacular cyberwarriors have proven themselves to be among the best in the business, fully the equal of those in the U.S., Russia, and China. Were I advising the Iranians, I would tell them to take their licks, not even think of trying to retaliate, and be afraid, very afraid.

First published in