Israel Publicly Threatens Iran With F35s, But The Cyber War Is Already Underway

GETTY

“Iran has recently threatened the destruction of Israel,” Benjamin Netanyahu said on Tuesday (July 9), filmed in front of an F35 fighter jet at the Nevatim Air Force Base near Be’er Sheva. “But these planes,” he warned, “can reach anywhere in the Middle East—including Iran and Syria.”

Meanwhile, Israel’s cyber capabilities have not been held back. Almost all of the real action is taking place behind the scenes, as the integration of cyber and conventional warfare has developed this year as never before. And this has introduced a new media dynamic—what is being seen is one dimension, one slice, you see what those controlling the narrative want you to see.

In his F35 video, Netanyahu was responding publicly to the threat made a week earlier by Mojtaba Zolnour, head of Iran's National Security and Foreign Policy Commission, that "if the U.S. attacks Iran, Israel will have only half an hour left to live."

State media rhetoric apart, the real backdrop to this latest exchange is Iran's breach of the 2015 limits on uranium enrichment—the International Atomic Energy Agency (IAEA) verified Iran's "enriching uranium above 3.67% U-235," and Israel's warning that Iran faces (unilateral, if necessary) military action if it continues to break nuclear limits. Iran's breach remains well below weapons-grade enrichment, but the direction of travel is sending a message. And that message has been received.

And so the cyber conflict is now well underway. Although sometimes this will (deliberately) hit the headlines, as with last month's U.S. retaliatory cyberattack on Iran's command and control systems, mostly it won't. The message sent with that attack was that "we can reach into your most secure networks when needed," with execution requiring more than clever coding and cyber superiority. Behind such an attack is the implication of significant action on the ground, usually entailing the compromise of individuals or physical equipment or the placement of an infected storage device into a live system.

Headlines may pause between publicized incidents, activity does not.

Teheran has now responded with the hurried introduction of a command and control unit designed to withstand cyberattacks. Time will tell whether that is effective, but unless there has been a material collaboration with a foreign power—think Russia or China—I would have my doubts. And on that note, it is also interesting that Teheran has made its cyber relationship with Beijing headline news at the same time, with ICT Minister Mohammad Javad Azari Jahromi telling the media that "Iran and China are now standing in a united front to confront U.S. unilateralism and hegemony."

At a cyber conference in Israel last month, Netanyahu described the U.S. as Israel's "great and irreplaceable ally," with the two countries "cooperating on cybersecurity like never before." The prime minister openly said that the investments being made are necessitated by "national defense." And in the world of offensive cyber, Israel sits at the grown-up's table, with its Unit 8200 having

achieved legendary status and a cyber startup landscape near Be'er Sheva intended to replicate Maryland and Cheltenham.

And while offensive actions on foreign powers will remain—usually—under wraps, Israel has decided that as a proxy it can promote its cyber expertise in combatting terrorist activity in Israel as well as in "dozens of countries" around the world. It's a message to the world. This is an international effort, with a common focus and a common enemy, and it has an extensive reach.

In his cyber presentation, Netanyahu referenced the foiling of an attack on an A380, bound for Abu Dhabi from Sydney, and said that "if you multiply that fifty-times, it will give you an idea of the contribution Israel has made to prevent major terrorist activities—mainly by ISIS—in dozens of countries, and most were foiled by our cyber activities."

Netanyahu was not addressing his audience, he was addressing the media beyond the walls of the auditorium.

A documentary broadcast in Israel this week continued the theme. It again referenced the fifty-plus ISIS attacks that have been foiled by intelligence and cyber, even including a dozen such attacks in Turkey, despite the suspension of diplomatic ties between the countries under President Erdogan's stance over the issue of Palestine.

And there are parallels here with the level of collaboration taking place behind the scenes in the Middle East between Israel and surrounding Arab states, where the theory of "my enemy's enemy" has forged some fast collaborations (if not alliances, quite yet), most notably with Saudi Arabia.

Make no mistake, as the world sits and watches and waits to see what happens next in the Middle East, the cybersphere in its more usual non-public guise is running at full speed. Networks are being probed, weaknesses and vulnerabilities are being tested and exploited, offensive actions are being planned.

Meanwhile, Iran (following China's lesson) is more than happy to focus its cyber efforts on soft industrial and civilian targets rather than hardened military ones—seen by Teheran as the soft underbelly it can attack on a low-effort, high-impact basis. Last month, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS issued a warning about a "recent rise in malicious cyber

activity directed at United States industries and government agencies by Iranian regime actors and proxies.”

This year has seen the integration of conventional and cyber warfare as never before. That hybrid, mix and match approach has significantly increased the operational flexibility on both sides—but it has also increased the risks. And with Russia and China actively sitting on the sidelines, both carrying a cyber threat far beyond Iran’s wildest dreams, those risks can escalate as quickly as conventional ones, albeit much less visibly.

Follow me on Twitter

Zak Doffman Contributor
I am the Founder/CEO of Digital Barriers, providing surveillance solutions to defense, security and law enforcement agencies worldwide. Contact me at zakd@me.com.

Source:
https://www.forbes.com/sites/zakdoffman/2019/07/10/israel-threatens-iran-with-f-35s-but-behind-the-headlines-its-all-about-cyber/#6d1e362d4fa9

[Disclaimer]