What went wrong with Israel's cybersecurity agency

More than three years after it was established, former key officials and other sources describe a government body has lost its focus

Amitai Ziv | Aug. 29, 2018 | 1:07 AM

When Israel's cabinet approved a plan, strongly backed by Prime Minister Benjamin Netanyahu, to form a Nation Cyber Defense Authority in 2015, the idea was first and foremost to help businesses that didn't have the financial and human resources to protect themselves.

But now, more than three years later, the authority – this year merged with another government body called the Cyber Bureau and renamed the Israel National Cyber Directorate – has lost its focus. The directorate is increasingly staffed by ex-employees of security agencies and functions more and more as if it were an arm of the Shin Bet security service.

The result has been a wave of resignations and a failure to perform the job it was tasked to do, say former key officials and other sources close to the operation. They say salaries and budgets have grown inflated.

"The Shin Bet isn't interested in cybercrime or in threats that don't come from Iran and other enemy states," said one former senior official at the directorate who asked not to be named. "But these kinds of threats are happening all the time."

The source cited as an example a wave of ransom attacks on small businesses that don't know how to deal with the problem and need outside help.

"With all these people [from the security agencies] coming on board, all the idea of 'we're here for you' has disappeared," the source said. "They don't jump into incidents like we used to, if at all."

The heart of the directorate, inherited from the cybersecurity authority, is the Cyber Emergency Response Team, which was largely set up to help private-

sector companies that couldn't cope with cyberwarfare on their own. CERT would cooperate with counterparts overseas and investigate attacks with its own analysts.

In many cases, businesses are so unprepared, they aren't aware they've been hacked, and part of CERT's job was to notify them of the problem. But with the reorientation of the directorate, many of the team have departed in recent months, including CERT's head, Alberto Hasson.

"They took out all the analysts from CERT. Have you heard of anything like this – CERT without analysts? All the incidents now are handled by the Shin Bet," said a former directorate staffer. "Yigal Unna has turned the directorate into a puppet of the Shin Bet because the Shin Bet has difficulties talking to private business."

Director general Unna is part of the change that has come to the directorate. Appointed in December to replace Buki Carmeli, he headed the Shin Bet's signal intelligence cybersecurity division between 2014 and 2017.

"You sit at a meeting [of the directorate] and next to you is sitting someone from the Shin Bet, someone from the Mossad, someone from the Defense Ministry's security arm and someone from the army – there aren't any civilians," the ex-senior official said.

Israel was a pioneer in developing a government-coordinated response to the growing problem of cybersecurity. Back in 2002 the government assigned the task to the Shin Bet, but its brief was limited to what was designated as critical infrastructure like the Israel Electric Corporation and the water company Mekorot.

But the great majority of businesses and organizations were left to their own devices. By 2010, however, the government realized that it couldn't leave so much of the civilian sector unprotected. The Shin Bet chief at the time, Yossi Cohen, wasn't interested, so the Cyber Defense Authority was created.

In turn, the authority and later the directorate took over all civilian cyber-defenses, and the Shin Bet unit that had been responsible for protecting critical infrastructure was disbanded. But over time the Shin Bet and officials from other security agencies came to fill key roles at the directorate and changed its priorities, including a downgrade of CERT.

“Go to Be’er Sheva, where CERT is based – it’s empty there,” the senior ex-official said. “There’s a room with a TV and a few students employed there through a center operated by Rafael and EMC, but it’s mainly for show, a visitors’ center. There are no professionals.”

To be sure, not everyone shares the criticism of how the directorate has changed, including Hasson, who told TheMarker he quit because he didn’t relish the long commute to Be’er Sheva.

“There’s a natural turnover of key personnel and changes that have come with the merger of the two bodies [the Cyber Bureau and authority], which is a natural and healthy process,” he said.

Carmeli said that during his tenure he insisted that ex-security officials adopt to the directorate’s business-focused mission. “I recruited people from the Shin Bet and the Mossad because I wanted the best for the long term,” he said.

“But the first thing I told them was ‘forget your security perspective – you’re working with civilian businesses that, apart from good will, don’t owe you anything. They’re only responsible to shareholders.’”

Meanwhile, the directorate’s budget and payroll have been growing fast. The state budget has set spending for it at 115 million shekels ($32 million) for 2019, but sources said this is just a baseline budget and the real figure would be twice as much. The Finance Ministry told TheMarker that the directorate’s 2017 budget was 215 million shekels, up from 120 million the year before.

Meanwhile, staffing levels are growing from 220 in 2017 to a projected 250, according to the 2019 budget.

Sources said the budget is inflated by high salaries. Deputy directors earn 35,000 shekels a month on average, about three and a half times the average salary nationwide, and section heads take in between 25,000 and 27,000 shekels. Each section has two heads, one in Be’er Sheva and one in Tel Aviv.

The Prime Minister’s Office, which oversees the directorate, did not issue a response.