Iran cyberattack on Israel’s water supply could have sickened hundreds – report

June 1, 2020

The Times of Israel

<https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/>

Iran tried to increase chlorine levels in the water flowing to residential areas during April’s cyberattack against Israel’s water systems, a Western intelligence official has told the Financial Times.

The official told the British newspaper [in a report published Monday](https://on.ft.com/3eAuBif) that hundreds of people would have been at risk of getting sick and that the attack was close to being successful.

The head of Israel’s National Cyber Directorate [hinted](https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/) last week that the attack may have aimed to mix chlorine or other chemicals into the water supply.

Additionally there was a chance that [the attack](https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/) would have triggered a fail-safe, shutting down the pumps and leaving thousands without water during during the recent deadly heatwave in Israel.

“It was more sophisticated than they [Israel] initially thought,” the Western official said. “It was close to successful, and it’s not fully clear why it didn’t succeed.”

An unnamed Israeli official told the Financial Times that the attack created “an unpredictable risk scenario” by starting a tit-for-tat wave of attacks on civilian infrastructure, something both countries had so far avoided.

The Western official and four Israeli officials, who were all briefed on the attack and all remained anonymous, told the newspaper that the Iranians hacked into the software that runs the pumps after routing through American and European servers to hide the source.

An Iranian regime insider dismissed the allegations to the newspaper, saying: “Iran cannot politically afford to try to poison Israeli civilians. And even if Iran did so, where is the Israelis’ appropriate response?”

The report also discussed Israel’s alleged reprisal on May 9 against the Shahid Rajaee port, with two of the Israeli officials saying the attack on the port came at the request of then-defense minister Naftali Bennett, who was coming to the end of his brief tenure with the forming of a new government.

“It was small, very small — like a knock on the door,” said one official. “Think of it [as] a gentle reminder. ‘We know where you live.’”

Neither Israel nor Iran have officially acknowledged targeting each other’s civilian infrastructure, nor have they publicly described the severity of the cyberattacks. The Iranian regime insider said: “Iranian ports are usually chaotic and disruptions happen.”

It was unclear how successful the alleged retaliation was, but the Western official said there was evidence of lines of trucks as Iranian officials tried to fix the damage.

Shahid Rajaee port was “roughly in the middle of the page of options,” an Israeli official said. “Any disruption would be economic, nobody’s safety would be placed at risk, they would be reminded we are here, we are watching.”

The Western official said that although the damage appeared to have been limited in the recent round, it was probably not the end.

“So Iran may have caused a temporary water shortage, and Israel may have caused a temporary traffic jam,” the official said. “In the grand scheme of things, it’s nothing. But it never stops at that.”

Last week, Israel’s national cyber chief described the hack as a “synchronized and organized attack” aimed at disrupting key national infrastructure.

Yigal Unna, who heads the National Cyber Directorate, did not mention Iran directly, nor did he comment on the alleged Israeli retaliation two weeks later, but he said recent developments have ushered in a new era of covert warfare, ominously warning that “cyber winter is coming.”

“If the bad guys had succeeded in their plot we would now be facing, in the middle of the corona crisis, very big damage to the civilian population and a lack of water and even worse than that,” he added.

Israel and Iran are bitter foes and have engaged in years of covert battles that have included high-tech hacking and cyber attacks. Iran’s leaders routinely [call](https://www.timesofisrael.com/khamenei-explains-final-solution-poster-i-favor-destroying-israel-not-jews/) for the elimination of Israel, and Israel alleges that Iran is seeking nuclear weapons in order to carry out that goal. Most famously, US and Israeli intelligence agencies are suspected of unleashing a computer worm called Stuxnet years ago in an attempt to disrupt Iran’s nuclear program.

But Unna said the attempted hacking into Israel’s water systems marked the first time in modern history that “we can see something like this aiming to cause damage to real life and not to IT or data.”

Had Israel’s National Cyber Directorate not detected the attack in real time, he said chlorine or other chemicals could have been mixed into the water source in the wrong proportions and resulted in a “harmful and disastrous” outcome. His office released a brief statement after the attempt, acknowledging it had been thwarted and saying no damage had been caused. But Unna’s comments marked the first official detailed account of what happened.

“It is a part of some attack over Israel and over the national security of Israel and not for financial benefit,” he said. “The attack happened but the damage was prevented and that is our goal and our mission. And now we are in the middle of preparing for the next phase to come because it will come eventually.”

Iran hasn’t commented on the attempted hacking and has played down the [alleged reprisal](https://www.timesofisrael.com/cyberattack-on-port-suggests-israeli-tit-for-tat-strategy-shows-iran-vulnerable/) on May 9 against the Shahid Rajaee port. Mohammad Rastad, head of Iran’s port and marine agency, told the semiofficial ILNA news agency that the attack failed to infiltrate into the agency’s systems and only damaged “several private sector systems.”

Israel has not officially commented on the attack against Iran.

Without discussing the attack directly, Unna said the past month marked a historic turning point in cyber warfare.

“Cyber winter is coming and coming even faster than I suspected,” he said. “We are just seeing the beginning.”

A television report last month said Israeli leadership viewed the attack on water systems as a significant escalation by Iran and a crossing of a red line because it targeted civil infrastructure.

“This is an attack that goes against all the codes of war. Even from the Iranians we didn’t expect something like this,” Channel 13 news quoted an official saying.