INSS Insight No. 1328, June 3, 2020

A New Level in the Cyber War between Israel and Iran

David Siman-Tov and Shmuel Even

In cyber warfare, an attack on essential civilian infrastructure is considered a serious attack. According to media reports, Iran attacked Israel's water infrastructure, and Israel responded with a cyberattack against infrastructure at the Iranian port in Bandar Abbas. While these were not the first attacks between the two countries, they illustrate that the conflict theater includes essential civilian infrastructure. Israel has so far managed to deal with cyberattacks against civilian infrastructure without suffering much damage, but it may become more vulnerable as the cyber arms race accelerates and Iran gains more sophisticated capabilities. Israel must assume that in the cyber realm, there will be further and more sophisticated attempts to attack than those that have been seen thus far.

Cyber warfare is conducted secretly and anonymously, unless one of the sides in the confrontation has an interest in exposing it. The attacks are generally launched without claiming responsibility or with denying responsibility, if at all ascribed. In the vast majority of cases, identifying the source of the attack is difficult. Attacks in cyberspace are considered to suit a "campaign between wars," since they enable the attacker to operate from afar, secretly, and avoid human casualties on both sides in order to avoid escalation. Cyberattacks allow information collection to enable cognitive warfare, send deterrent messages, increase pressure on military and civilian systems in order to achieve defense and political goals, and launch preventive actions. The Stuxnet attack against Iran's nuclear facilities, which was revealed in 2010, was a formative event regarding military cyberattacks on infrastructure. The attack on the command and control systems of essential civilian infrastructure is considered to be at a high level on the scale of seriousness of cyberattacks. The most serious attacks of this sort are those that endanger large civilian populations, for instance due to water pollution or accidents that result from attacks on transportation systems.

According to reports in the American media, Iran and Israel have exchanged blows in cyberspace, attacking each other's civilian targets. Israel reportedly launched a cyberattack on May 9, 2020 against the Iranian port at the Shahid Raja'i port in Bandar Abbas in southern Iran, in response to an Iranian cyberattack against water and sewage infrastructure ("the water system") in Israel.

The attack against the Israeli water system attributed to Iran was carried out at a number of points throughout the country on April 24 and 25, 2020 (before Israel's Independence Day and at the start of the first stage of the exit from the coronavirus lockdown). At one facility, there were unusual data and "irregularities." At another, a pump was disconnected from automatic mode (controlled) and put into continual operation, and at another water source, the operating system was taken over (*Ynet*, May 19). In one of the cases, the water pump stopped operating for a short time. The concern, presented by the National Cyber Directorate, was that during the coronavirus crisis, Israel would be forced to deal with a temporary lack of water, or with a mixture of chlorine or other chemicals at the incorrect balance, which could have caused damage to the point of a disaster.

According to elements close to the investigation of the incident, the assessment is that the source of the attack software is in the cyber offense units of the Iranian Revolutionary Guards (as reported in the *New York Times* on May 19). Due to the attack, a notice was published by the Water Authority and the National Cyber Directorate in Israel, stating that "an attempted cyberattack was recently identified targeting the command and control systems in the water sector. The attempted attack was handled by the Water Authority and the National Cyber Directorate. We emphasize that there was no damage to the water supply, which was and is operating in an orderly manner." On May 28, Yigal Unna, the head of Israel's National Cyber Directorate, defined the attack as a "turning point" in the history of Israel's cyber warfare: "The attempted attack on Israel was coordinated and organized with the aim of harming our humanitarian water system, and had it succeeded, we would have been forced to deal with damage to the civilian population, and even with a temporary water shortage that could have caused extensive damage and disaster." Arik Barbing, formerly the head of the Cyber Directorate in the Israel Security Agency, provided an assessment that the attack shows state-level ability that is based on precise intelligence. Maj. Gen. (ret.) Prof. Isaac Ben-Israel, head of the Cyber Center at Tel Aviv University, noted that this was at least the third attempt to attack water systems in Israel, none of which succeeded.

In addition, Channel 12 News reported on May 25, 2020 that in recent weeks, cyberattacks intended to harm Israeli research institutes dealing partly with the development of medications and vaccines against the coronavirus have been disclosed. According to the report, the goal of the attacks was not information collection, but destruction. If this is another step connected with the cyber war between Israel and Iran, the scope of the Iranian attack was broader.

The Israeli media reported that the cyberattack on the water systems was discussed in the political-security cabinet on May 7, 2020. Presumably that is when the decision to

respond was made. The attack attributed to Israel by the US media was launched on May 9, 2020, and was aimed at infrastructure at the port in Bandar Abbas. The attack caused the collapse of the computers that direct the movement of ships, truck, and goods, which led to the shutdown of activity at the port for a number of days. *Israel Defense* (May 15, 2020) noted that from the Iranian standpoint, this was the third cyberattack since December 2019 that led to the shutdown of its ports. However, Israel is not the only country blamed for cyberattacks in Iran.

Presumably Israel viewed the attack on its civilian water infrastructure (particularly during the national coronavirus crisis) as a serious incident that could not be ignored, be it a stand-alone incident or one escalated incident in a chain of events. Perhaps the fact that the attack attributed to Iran was exposed by the media is what spurred Israel to respond. In any case, Israel was not strategically surprised by the attack. In June 2019, Unna said that "Iran and its proxies remain the main cyber threat in the Middle East. Israel is prepared for cyber threats. We have the ability to respond powerfully against cyberattackers, and not necessarily in the same space in which they attacked." According to data he presented, the Iranians are acting consistently over time along a broad attack path, including attacks for intelligence collection, attacks intended to have a psychological effect (such as attacks on Israeli sites), and attacks that aim to cause the destruction of systems (*Ynet*, June 26, 2019).

The attack on the Iranian port was apparently intended to send a deterrent message, as suggested by hints by senior Israeli defense officials. Defense Minister Naftali Bennett announced on May 18, 2020 at the ceremony marking the end of his term that "the Iranian octopus is sending its tentacles to grab onto us from all directions…We must increase political, economic, military, and technological pressure, and act in other dimensions as well. It can be done." IDF Chief of Staff Lt. Gen. Aviv Kochavi announced on May 19, 2020 that the IDF "will continue using a variety of military tools and unique combat methods to harm the enemy."

Iran's cyber combat is part of the strategic struggle it is waging on several fronts against a number of enemies, chiefly the United States, Israel, and Saudi Arabia. To Iran, cyberattacks are not an alternative to kinetic action, but an added capability. For instance, relatively high quality attacks against the Saudi Aramco oil company have been attributed to Iran. These facilities are part of the source of the kingdom's wealth as an important oil provider to the global economy that helped the United States cover the shortage of Iranian oil as a result of the sanctions imposed on Iran. In December 2012, Iran carried out a broad cyberattack against Aramco that damaged about 30,000 of the company's computers. In September 2019, Iran surprised the world with precision kinetic attacks on

the company's facilities using drones and cruise missiles. Tehran did not claim responsibility in either case.

The Iranian cyberattacks are part of the multi-front struggle with Israel, which is also reflected in calls to destroy Israel, military entrenchment in Syria, support for Hezbollah and Palestinian Islamic organizations, and the drive for nuclear weapons. While the reason for the timing of the attack on Israel's water facilities is not known, the event demonstrates that Iran has no hesitation in using the cyber weapon against civilian populations. It may be a concrete reaction to kinetic attacks attributed to Israel against Iranian targets in Syria, or it may be another Iranian attack taking advantage of the opportunity in an ongoing multi-front campaign between wars that includes cyber warfare.

In the cyber realm, Iran is technologically and economically inferior to Israel, and certainly to Israel's American ally. However, in a cyber war against Iran, Israel may also suffer damage, and will certainly incur additional costs to protect its cyberspace, particularly as its dependence on the digital dimension increases. Despite the fact that Iran has not yet succeeded in causing significant damage to Israel in cyberspace, there are likely to be continued efforts on its part and the development of higher quality attacks, as well as more Israeli responses.