INSS Insight No. 598, August 26, 2014

The Iranian Cyber Offensive during Operation Protective Edge

Gabi Siboni and Sami Kronenfeld

Although the IDF's abilities to handle the rocket and attack tunnel threats have garnered most of the attention during the latest campaign in the Gaza Strip, it is now clear that Israel was also forced to confront cyber challenges during Operation Protective Edge. A senior officer in the C^4I Corps noted that in the course of the campaign Iranian elements launched a widespread cyber offensive against Israeli targets, including attempts to damage security and financial networks. While these attempts were neutralized relatively easily and quickly by Israeli cyber defenses, it seems that Iran is investing heavily in the development of effective offensive capabilities against infrastructure systems, and might present a serious challenge to Israeli defenses within the foreseeable future. In 2013, a series of attacks on the websites of major US banks and financial institutions was attributed to Iran. An information security expert described these attacks, which included sophisticated techniques and demonstrated an ability to act in significant scope against high quality targets, as unprecedented in degree and effectiveness.

Attacks on a nation's financial infrastructures have serious repercussions, liable to result in heavy financial damage as they disrupt routine financial activity of commercial enterprises and households alike. However, the focus of the cyber offensive during Operation Protective Edge was the civilian internet. Iranian elements participated in what the C^4I officer described as an attack unprecedented in its proportions and the quality of its targets. The attack targeted IDF websites such as the Home Front Command and the IDF Spokesperson's Unit, as well as civilian internet infrastructures. The attackers had some success when they managed to spread a false message via the IDF's official Twitter account saying that the Dimona nuclear reactor had been hit by rocket fire and that there was a risk of a radioactive leak. Some of the attacks against Israel were attributed to the Syrian Electronic Army (SEA), a group of Assad-supporting hackers that in recent years has developed significant attack capabilities and described by Michael Hayden, former Director of the CIA and the NSA, as a veritable Iranian proxy.

Cyber attacks on Israeli targets accelerated as the military operation expanded on the ground. If, during the early part of the operation, there was marginal, unorganized attack activity by pro-Palestinian elements, the ground incursion in the Gaza Strip prompted,

according to the IDF's chief of cyber defense, a significant leap in the scope of attacks on Israel and often in their sophistication as well. The attacks peaked on July 25, 2014 – the last Friday of Ramadan, observed in Iran as "Jerusalem Day" and dedicated to resistance against Israel and Zionism – when Iranian elements, together with hackers from all over the world, launched a widespread attack against many Israeli websites in order to block access for a long period of time. Joint efforts of the IDF and the General Security Service (GSS) were prepared for the cyber onslaught in advance and successfully thwarted the attack.

An analysis of Iran's cyber activity during Operation Protective Edge indicates growing maturity in the Islamic Republic's operational capabilities and shows that it is capable of conducting an extensive military cyber operation against a range of targets using a wide spectrum of methods. Moreover, Iran's focus on cyberspace during Operation Protective Edge may indicate the start of a process in which cyberwar replaces classical terrorism as the main tool in Iran's doctrine of asymmetrical warfare. Cyberwar, which offers the attacker distance and deniability, two features the Iranians consider extremely valuable, enables serious damage to the civilian front of an enemy enjoying military and geostrategic superiority. Thus far Iran's cyberspace capabilities remain inferior to Israel's and to those of the leading technological powerhouses, but it is rapidly and efficiently closing the gap.

Israeli cyber defenders succeeded in foiling the Iranian attack, but there is no certainty they can repeat the feat in the future. Israel has yet to establish a comprehensive preparedness approach or name the agency that will take command of the defense against extensive cyber attacks. Israeli cyberspace has a host of institutional players: the IDF, the GSS, the Mossad, telecommunications companies and providers, the Bank of Israel and commercial banks, government ministries, the Israeli Police, civilian security companies, and others. The absence of a ranking of authority in defensive and preventive efforts is liable to create holes in the digital Iron Dome defending the country and allow enemies to cause severe damage.

The success scored in preventing the recent attack is more indicative of cooperation and coordinated work at the professional level rather than a mapping of authority among the various organizations, and Israel cannot rest on these laurels. Iran's cyber force buildup and attacks are progressing apace, and Iran is liable to challenge Israel's defensive capabilities to a larger extent than ever before. It is therefore imperative that Israel sees to the organizational aspect of the nation's cyber defense as soon as possible, and determines the interrelationships among the various institutions operating in the field. Furthermore, defensive measures are not enough, and therefore Israel must launch preemptive and retaliatory strikes as well. There is no reason that Israel's long arm should not reach the hands of those who are intent on injuring Israel in cyberspace.