INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

INSS Insight No. 536, April 3, 2014

Developments in Iranian Cyber Warfare, 2013-2014

Gabi Siboni and Sam Kronenfeld

In early 2013, a senior official from the cyber security company CrowdStrike described Iran as a "third tier" country in terms of its cyber capabilities, and estimated that they lagged significantly behind the capabilities of leading countries such as the United States, Russia, Great Britain, and China. The perception was that Iran had the ability to be a nuisance to Western information security systems, but that it lacked the knowledge and means to carry out a strategic cyber attack. These assumptions largely dissolved over the course of 2013, when Iran became one of the most active players in the international cyber arena. Iran's progress can be attributed to a combination of two elements: a certain easing of the restraints on offensive activity in cyberspace by Iranian decision makers, and a qualitative leap by the Iranian cyber warfare system. This major advance by Iran has surprised many Western experts in terms of its scope, its professional sophistication, and the ambitious choice of targets.

The Defense Concept: Cutting Iran Off from the World

From its past experience with events such as the Stuxnet virus and the post-election riots in June 2009, Iran learned the importance of an effective cyber defense system and effective control of the internet. To this end, Iran has worked on three main tracks to create a multi-dimensional cyber defense system: (1) creating a defense envelope against cyber attacks on critical infrastructures and sensitive information; (2) neutralizing cyber operations by opposition elements and regime opponents; 3) keeping Western ideas and content, which could contribute to the development of a "soft revolution" that would harm the stability of the regime, out of Iranian cyberspace.

Each of these three tracks in the Iranian cyber defense system underwent a significant upgrade during 2013, mainly as a result of the maturation of organizational technologies and systems. First, Iran has introduced an isolated domestic intranet that gives it close control over content in cyberspace within the country. Second, Iran has invested in developing technologies and cyber defense mechanisms locally in order to reduce its dependence on foreign products that could be Trojan horses. In addition, the Iranian regime has increased physical enforcement against regime opponents who are active online, mainly through aggressive use of the cyber police. Furthermore, the Iranian cyber authorities have instituted a routine of training, exercises, and inspections among the country's security and civilian institutions. The impact of these measures was reflected during the elections in June 2013, when the Iranian cyber system worked efficiently and largely succeeded in controlling the discourse on the domestic internet and monitoring subversive activity.

It appears that as of today, the Iranian cyber defense system still has a long way to go in coping effectively and consistently with highly sophisticated cyber attacks such as Stuxnet. But Iran's technological and organizational leap in the past year indicates that the Iranians could formulate a comprehensive and effective defense system sooner than anticipated.

The Offense Dimension: Seeking "High Quality" Attacks

The Islamic Republic sees the cyber arena as an effective offensive platform enabling it to cause harm to adversaries with clear military superiority, and at the same time, maintain a margin of denial that will prevent international censure or even sanctions and a counter attack. During 2013, cyber warfare became a key tool used by Iran to attack Western targets in response to the sanctions and as a means of deterring escalation by Western countries against Iran. The scope, targets, and relative success of those cyber attacks of the past year ascribed to Iran show its improved capabilities. Western sources attribute the progress in Iran's cyber warfare program to its success in combining the capabilities, knowledge, and manpower in Iranian computer science departments with the experience and capabilities of the Iranian hacker community, much of which identifies with the regime and its goals. Furthermore, the increasingly close ties between the Iranian cyber system and cyber criminals, hackers, and information security experts, mainly Russians, who are prepared to sell their services for money, contribute to the rapid progress in Iran's cyber warfare program. In addition to reinforcing its own cyber system, Iran is working to expand and strengthen the cyber warfare capabilities of its allies. It appears that the Iranians are seeking to create an effective system of proxies that work for them in cyberspace. One of the centers of this Iranian activity is in Syria, where Iran is supporting the Syrian Electronic Army (SEA), a hackers organization that is an increasingly important player in cyberspace.

The progress in Iranian cyber warfare capabilities can be seen in a number of attacks that occurred in the second half of 2012 and during 2013. These attacks made use of sophisticated techniques, had high quality targets, and were wider in scope than previous Iranian attacks. Among the most prominent of these was the large scale attack on websites of major banks and financial institutions in the United States, which one information security expert described as unprecedented in scope and effectiveness.

Another wave of attacks blamed on Iran focused on US energy and infrastructure companies and involved attacks on control systems that could have harmed their physical operation or the safety measures for critical infrastructures such as gas and oil conducting systems and electrical systems. In the past year, Iranian-affiliated elements have also taken responsibility for cyber attacks against Israeli institutions, and in June 2013 Prime Minister Benjamin Netanyahu announced that there had been a significant increase in Iranian cyber attacks against important computer infrastructures in Israel.

The rapid development of Iran’s cyber warfare capability and that of its proxies and allies means that Israel and other Western countries must work decisively and systematically to maintain qualitative and operational superiority in cyberspace. The importance of cyberspace for Israel’s security concept and the urgency of creating a “digital Iron Dome” were well expressed by IDF Chief of Staff Lt. Gen. Benny Gantz: “Israel must be on a superpower level in cyberspace…we must not wait with this.”

iNSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב