INSS Insight No. 375, October 15, 2012

Iran's Cyber Warfare

Gabi Siboni and Kronenfeld

The recent statement by US Secretary of Defense Leon Panetta about the need to confront Iranian cyber warfare waged against American targets highlights developments of the last two years regarding Iran's extended activity to construct defensive and offensive cyber capabilities. Apparently underway is a large cyber campaign by Iran, both to attack various targets in retaliation for the sanctions imposed against it and to repel the cyber attacks directed at it.

Iran is working to develop and implement a strategy to operate in cyberspace. The approach by Supreme Leader Khamenei to opportunities and risks inherent in cyberspace, reflected in his March 2012 announcement on the establishment of the Supreme Cyber Council, shows how central the issue is in Iran. Defensively, Iran is working to realize two main goals: first, to create a "technological envelope" that will protect critical infrastructures and sensitive information against cyberspace attacks such as the Stuxnet virus, which damaged the Iranian uranium enrichment program, and second, to stop and foil cyberspace activity by opposition elements and opponents to the regime, for whom cyberspace is a key platform for communicating, distributing information, and organizing anti-regime activities. The Iranian program to create a separate, independent communications network is particularly important in this context.

Offensively, the cyberspace strategy is part of the doctrine of asymmetrical warfare, a central principle in the Iranian concept of the use of force. Cyberspace warfare, like other classical asymmetrical tactics such as terrorism and guerilla warfare, is viewed by Iran as an effective tool to inflict serious damage on an enemy with military and technological superiority. In a case of escalation between Iran and the West, Iran will likely aim to

---

Dr. Gabi Siboni is the head of the Cyber Warfare Program at INSS. Sami Kronenfeld is an intern in the program. This essay is shortened version of a forthcoming article on Iran's cyberspace capabilities, to be published in the December issue of *Military and Strategic Affairs*.

launch a cyber attack against critical infrastructures in the United States and its allies, including energy infrastructures, financial institutions, transportation systems, and others.

In order to realize the goals of its strategy, Iran has allocated about $1 billion to develop and acquire technology and recruit and train experts. The country has an extensive network of educational and academic research institutions dealing with information technology, computer engineering, electronic engineering, and math. In addition, the government operates its own institute – the Iran Telecommunications Research Center, the research and professional branch of the Information and Communications Ministry. The institute trains and operates advanced research teams in various fields, including information security. Another government body is the Technology Cooperation Officer, which belongs to the president's bureau, and initiates information technology research projects. This body has been identified by the European Union and others in the West as involved in the Iranian nuclear program.

The Iranian cyberspace system comprises a large number of cyber organizations, formally related to various establishment institutions and involved in numerous fields. One central organization with a primarily defensive orientation is the Cyber Defense Command, operating under Iran's Passive Defensive Organization, affiliated with the General Staff of the Armed Forces. Alongside military personnel, this cyberspace organization includes representatives of government ministries, such as the ministries of communications, defense, intelligence, and industry, and its main goal is to develop a defensive doctrine against cyberspace threats. Another cyberspace body of a defensive nature is the MAHER Information Security Center, operating under the aegis of the communications and information technology ministry. The center is in charge of operating rapid response teams in case of emergencies and cyber attacks. Iran also has a Committee for Identifying Unauthorized Sites and FETA, the police cyberspace unit, which in addition to dealing with internet crime also monitors and controls Iranian internet usage, with emphasis on internet cafés throughout the country that allow relatively anonymous web surfing.

The picture is less clear regarding Iran's offensive cyberspace capabilities. Clearly the capabilities of the Revolutionary Guards make Iran one of the most advanced nations in the field of cyberspace warfare, with capabilities, inter alia, to install malicious code in counterfeit computer software, develop capabilities to block computer communications networks, develop viruses and tools for penetrating computers to gather intelligence, and develop tools with delayed action mechanisms or mechanisms connected to control servers. There is also evidence of links between the Revolutionary Guards and hacker groups in Iran and abroad that operate against the enemies of the regime at home and around the world. The use of outsourcing allows the Revolutionary Guards and Iran to maintain distance and deniability about Iran's involvement in cyberspace warfare and

cyber crime. A prominent hacker group linked to the Revolutionary Guards is the Ashiyane Digital Security Team, whose members are motivated by an ideology supporting the Iranian regime and the Islamic Revolution and who target the enemies of the regime for attack. The Basij, subordinate to the Revolutionary Guards, also became active in cyberspace when in 2010 established the Basij Cyberspace Council. The activities of the Basij focus primarily on creating pro-Iranian propaganda in cyberspace, and the organization works on developing more advanced cyberspace capabilities and using Revolutionary Guards cyberspace operatives to train hackers in high offensive capabilities.

Iran is already active offensively, as evidenced by several events in recent years. In 2011 there were two attacks on companies providing security permissions; most prominent was the attack from June to August 2011 on DigiNotar in the Netherlands, whose databases – the major source of SSL permissions in Holland – were attacked. During those months, certificates for authenticating websites, including the certificate authenticating the google.com domain, were stolen; the latter item allowed attackers to pose as Google and redirect Gmail servers. In fact, the attack allowed Iran to penetrate more than 300,000 computers, primarily in Iran, and seems to have been designed to monitor users at home for internal security purposes.

In September 2012, a number of financial institutions in the United States came under attack, including sites belonging to the Bank of America, Morgan Chase, and CitiGroup. According to American analysts, the most destructive attack occurred in August 2012 on the computers of the Saudi Arabian oil company Aramco and the Qatari gas company RasGas. The attack was carried out by means of a computer virus called Shamoo, which spread through company servers and destroyed information stored in them. A group called the Cutting Sword of Justice took responsibility for the attack and claimed it was aimed at the main source of income of Saudi Arabia, which was accused of committing crimes in Syria and Bahrain.

The development of Iran’s cyberspace capabilities and the most recent attacks should concern the United States as well as Israel. The success of the attack on Aramco computers is of concern because the standard defensive systems proved insufficient against the focused and anonymous attacks. It is therefore necessary to develop tools that can deal with such threats. One of the directions being developed involves identification, blocking, and neutralization of unusual behavior in computers under attack. Such tools could neutralize threats even after the malicious code managed to penetrate the targeted computer. The attack on Aramco was designed more to destroy information indiscriminately in tens of thousands of company computers and less (if at all) to gather intelligence. If intelligence gathering in cyberspace can be considered legitimate in some cases, a large scale attack such as the one by Iran against a civilian target marks a

transition by Iran to retaliatory action. Secretary Panetta's recent statement on the need to close accounts with those responsible for this attack demonstrates this, but what ultimately counts is the test of action and not of words.

The focus of Iran's cyberspace activity directed against Israel and other countries in the West requires appropriate defensive arrangements, beginning with an up-to-date doctrine of cyberspace defense. The attackers' sophistication requires intelligence-based defenses as well as the generic ones. In light of developments in Iran, the State of Israel must place the issue of Iranian cyberspace activity among its highest intelligence priorities, in order to identify advance preparations and foil attacks before they are underway. Similar to the Iranian nuclear program, the challenge is not Israel's alone, rather that of many other states in the West as well as the Gulf states. It is therefore necessary to initiate broad interstate cooperation to gather intelligence and foil Iranian cyber activity.