Iran and Cyberspace Warfare

Gabi Siboni and Sami Kronenfeld

Introduction

Throughout the world decision makers and the general public have undoubtedly realized in recent years that cyberspace must be treated as a genuine realm of warfare. As such, it allows considerable room for maneuvering and has vulnerabilities that can be breached by hostile elements seeking to derail information systems or even inflict physical damage on critical infrastructures controlled by industrial control systems. In the wake of this new understanding, many countries are investing increasingly in safeguarding their cyber resources (particularly in the fields of defense, intelligence gathering, and offense capabilities). Since the Stuxnet attack – one of the most destructive cyber attacks to date – Iran has been working hard to improve its cyberspace defenses on the one hand, while building up cyberspace intelligence gathering and offensive capabilities on the other.

The Iranian cyberspace defense program has a dual objective: first, it hopes to prevent another attack like Stuxnet and intelligence-directed penetration of Iranian computers by viruses such as Duqu and Flame. In this sense, the goal of the Iranian program is similar to that of many other nations seeking to protect their critical infrastructures. The second objective is the regime's desire to ensure its survival by means of surveillance and blocking of information and services originating with the Iranian public. In many cases the two goals are achieved with the same tools, e.g., the Iranian effort to create a separate Iranian web or the disabling of Google services in that country.[1]

Dr. Gabi Siboni is the head of the Military and Strategic Affairs Program and the Cyber Warfare program at INSS. Sami Kronenfeld is an intern in the Cyber Warfare Program at INSS.

At the same time, Iran is also in the midst of a concerted effort to construct offensive capabilities, on the assumption that in any future confrontation the use of cyberspace will have a critical impact on achieving success against the enemy. Gathering information openly about Iranian cyberspace capabilities, especially offensive ones, is by definition extremely difficult. But the country's cyberspace activities have recently been in the spotlight because of suspicions of Iranian involvement in some serious cyberspace incidents, including the theft of internet security permissions, an attack on the Saudi Arabian oil company's organizational network, and not least, the penetration of computers at some leading American banks.

This article examines the current situation regarding various elements of Iran's cyberspace development process. The first section analyzes the country's cyberspace strategy, while the second section describes the organizational and operational response to the formulated strategy. This comprises three components: infrastructures for training and developing technological manpower for work in cyberspace; technological developments that have already been introduced; and the overall processes of cyberspace force construction. Finally, the article focuses on a number of cyberspace incidents attributed to Iran, attempts to gain some insight into the way Iran conducts its cyberspace activities, and examines implications for Israel and other Western nations.

Iran's Cyberspace Strategy

The role of the communications and information networks in the outbreaks that followed the 2009 Iranian presidential election and those that erupted as part of the "Arab Spring," as well as the cyber attacks on Iran made the cyberspace arena tremendously important to the Iranian regime's overall security doctrine. Evidence of the subject's significance in the minds of Iran's decision makers was proffered by none other than the Supreme Leader himself, Khamenei, in a direct reference to the opportunities and dangers of cyberspace when, in March 2012, he announced the establishment of a Supreme Cyberspace Council composed of senior government representatives charged with planning and implementing a single integrated cyberspace strategy.[2] While the work of this Council began only quite recently, an analysis of Iranian cyberspace activity in recent years indicates the existence of an Iranian cyberspace strategy with clear goals and objectives.

Two fundamental assumptions underlie Iran's approach to its modus operandi in cyberspace. The first concerns the development of defensive capabilities to withstand attacks by hostile nations and entities, alongside the development of operational capabilities against opponents of the regime on the home front; the second concerns the development of offensive capabilities to enable Iran to combat what it sees as American superiority and control of global internet capabilities and infrastructures.

In the defense arena, Iran is working to accomplish two main goals in cyberspace.[3] First, it aims at an effective, comprehensive, advanced technological protective system to defend critical infrastructures and sensitive data against cyber attacks such as Stuxnet, which compromised the Iranian uranium enrichment program and shut down more than 1,000 centrifuges at the enrichment facility in Natanz.[4] Second, Iran is trying to curb and foil the cyberspace activities of domestic opposition parties and opponents of the regime, for whom cyberspace is an important communications platform for disseminating information and organizing anti-government activities. In addition, the regime hopes to prevent the cyberspace penetration of Western ideas and information that conflict with its interests, thereby blocking "soft revolution" processes that are liable to damage the regime's stability and hold on the state. In the context of defensive capabilities, the news about Iranian plans to develop a separate, independent communications network is noteworthy.[5] Although this has at times been denied by Iranian officials,[6] as time goes by it seems to take on more validity.[7]

On the offensive front, Iran's cyberspace strategy sees this arena first and foremost as central in the asymmetrical doctrine of warfare, a key principle in Iran's perception of the use of force. Iran sees cyberspace warfare, in a similar way to more obvious asymmetrical tactics such as terrorism and guerilla warfare, as an effective tool to inflict significant damage on the enemy's home front with military or geostrategic superiority. Experts estimate that in the event of an escalation in the confrontation between Iran and the West over the Iranian military nuclear program, Iran would attempt a cyber attack against major infrastructures – such as power plants, financial institutions, and transportation systems – on American soil.[8] An article published in July 2011 in the Iranian newspaper *Kayhan* (which is closely identified with Khamenei) hinted at such a possibility by warning that the United States must take care lest "an unknown player somewhere in the world" carry out an attack on its most vital infrastructures.[9]

Beyond the military-strategic aspect, the Iranian regime and its supporters also use offensive cyberspace warfare to impair the cyber activities of Western countries and opponents to the regime in Iran. Iranian hackers, who usually have no official affiliation with the establishment but are linked to it nonetheless, consistently engage in cyber attacks causing internet crashes, inserting pro-Iranian material, stealing information, committing credit card fraud, damaging service providers, and rerouting internet traffic.[10] Propaganda is another part of the cyberspace warfare strategy. The Iranian regime understands well the importance of cyberspace in shaping the points of view and attitudes of large groups of people inside Iran and abroad, and invests major efforts in creating a sizable and effective propaganda machine extolling the regime and maligning its enemies. To realize these strategic goals, Iran is investing considerable resources in creating a tight, skilled, multi-layered structure that includes impeding, monitoring, controlling, and offensive capabilities in cyberspace.

Iran's Organizational and Operative Response

With its cyberspace strategy goals in mind, Iran set about applying itself vigorously to strengthening its cyberspace capabilities. There are reports of investments amounting to some $1 billion in the development and acquisition of technologies and in recruitment and training of experts to advance and strengthen both defensive and offensive cyberspace capabilities.[11] There are various interconnected components in the processes of building an operative and organizational cyberspace response: first, building up a training and development manpower base at research institutes and institutions of higher education; second, efforts towards large scale technological development; and third, processes of force buildup, including development of a doctrine, establishment of organizations, and formulation of a hierarchy of authority to implement the doctrine.

Manpower Training and Development

The infrastructures for the technological training and development of Iranian cyberspace are found primarily in the country's universities and technological institutes. Iran has many institutions of higher education and academic research engaged in research and training in the fields of

IT, computer engineering, and communications.[12] Leading universities in this area include: Sharif University of Technology in Tehran, offering advanced degrees in computer engineering, electronic engineering, and mathematics,[13] and which is also the site of two advanced research institutes in communications and information technologies (the Advanced Information and Communication Technology Center[14] and the Advanced Communication Research Institute[15]); and Amikabir University of Technology, also in Tehran, with large departments of mathematics, computer sciences, computer engineering, and information technology. It seems that Amikabir specializes in data security; the computer engineering department offers several advanced courses in security information,[16] and also operates a research lab specializing in data security[17] and a separate research lab specializing in secure systems analysis.[18]

In addition to academic research and training, the Iranian regime invests significant sums in the promotion and support of IT and computer communications companies. Such investments are made directly by government organizations such as the Science Ministry, and indirectly via the financing and establishment of greenhouses for hi-tech companies in which the government has an interest.[19] The Iran Telecommunications Research Center is a key government body in the IT field; it specializes in research in information and communications technology and is the research and professional arm of the Information and Communications Ministry. The center operates and trains advanced research teams in many fields, including data security.[20] Another government body promoting research in IT is the Technology Cooperation Office, which belongs to the Presidential Bureau. Its stated objective is to improve technological cooperation with other nations. It directs and initiates research projects in many areas, including information technologies.[21] The EU and other Western sources have singled it out as being involved in the nuclear program.[22]

Apart from direct investments by government bodies, the Iranian regime also operates hi-tech greenhouses engaged in data security research. Prominent among such hi-tech centers is the Pardis Technology Park, also known as the Iranian Silicon Valley. Established in 2001 by the Presidential Bureau and the Technology Cooperation Office, it houses more than 400 companies involved in communications and IT.[23] Another hi-tech greenhouse is Guilan Science and Technology Park, a support center for startups and home to a number of companies working on information security.[24]

Technological Empowerment

Beyond developing and training a strong cyberspace workforce, Iran has also been focusing on technology to promote its strategic goals in cyberspace. One target of major investment is intra-state cyberspace and information flow. In recent years, the Iranian regime has bought and developed advanced technological systems allowing it to conduct surveillance and monitor information traffic on computer and mobile networks in the country. The largest government controlled telecom corporation (the Telecommunications Company of Iran) bought a surveillance system from the Chinese ZTE Corp. The system, capable of monitoring information on telephone lines, computer networks, and cellular lines, was acquired as part of a comprehensive deal between the two companies estimated at $130 million. The deal covered products of the ZMXT system, which the Chinese company describes as an integrated monitoring system. The products purchased enable voice communications eavesdropping, text message surveillance, and monitoring of web surfing.[25]

In addition to surveillance and monitoring, the Iranian government is also developing website blocking and filtering technologies, since international sanctions prevent Iran from buying Western-manufactured data filters. Amnafzar Ltd., an IT company with links to the regime, developed a data filter called Separ, which is updated constantly and frequently changes its filtering strategy so as to evade efforts to circumvent it.[26] Using this technology, the regime has succeeded in significantly limiting the flow of information into and within the country. Research published in March 2009 by the OpenNet Initiative (a joint project by a number of institutions, including Harvard University and the University of Toronto) identified Iran as one of the leading nations in website filtering and blocking, alongside nations such as China, North Korea, Syria, and Myanmar.[27]

These technologies allow Iran relatively close control of the state's cyberspace, but the regime nonetheless strives for outright control of information, ideas, and access to Iranian cyberspace. To this end Iran embarked on a project of establishing an independent and separate national network, isolated from the World Wide Web. The idea is that the establishment of this national web, named Halal, will allow the regime full control of contents for public exposure and will also cause serious damage to opponents of the regime conducting widespread activities on the internet. It will also make virus attacks and other cyber attacks on Iranian infrastructures much more difficult. The national network project first came into being in 2009, when the Iranian authorities instructed domestic companies to move their network activities to servers and data centers on Iranian soil. During 2012 it was reported that Iran is developing an internal email service, an independent operating system, a search engine, and other tools for use on the new network.[28] In August 2012 Iranian Communications Minister Reza Taghipour announced that Iran would disconnect from the World Wide Web within 18 months.[29] However, Western experts believe it will be difficult for the regime to sever all connections with the global network.[30]

Iran is also seeking to isolate networks in the security establishment and construct a national intelligence communications network separate from the global web.[31] The first indication of this effort is Basir, the intra-organizational network of the Revolutionary Guards, whose existence became public knowledge in March 2012. Reports describe it as a closed cellular network, possibly operated by designated relay stations. The network supposedly affords the organization efficient, encrypted lines of communication, even in a scenario of a comprehensive cyber attack on the country's communications and information infrastructures. Thus far it is unclear if it is also an information network or a voice system only.[32]

Force Buildup

As for cyberspace force buildup processes, the many training and development facilities available to Iran have allowed the Islamic Republic to establish a large cyberspace configuration with multiple capabilities, both defensive and offensive. In the last decade, Iran embarked on a strategic expansion of its national cyber constellation, with cyberspace agencies and organizations established for almost every relevant government ministry. The goal is to create a hierarchical and diverse organizational alignment with a clear plan of action, well thought out resource allocations, distribution of responsibility and the ability to preserve and disseminate information, know-how, and data.

The crowning glory in the construction of Iran's cyberspace force is the establishment of the Supreme Cyberspace Council. The Council was set up in March 2012 at the behest of Supreme Leader Ayatollah Khamenei and serves as the ultimate authority on all of the nation's cyberspace issues.[33] The Iranian President heads the Council and its members comprise senior government representatives and others, including the senior commander of the Revolutionary Guards, the head of the Majlis, the Ministers of Science, Communications and Culture, the chief of police, and the president of the Islamic propaganda organization. The Council has the authority to determine national cyber policy and its directives are binding on all Iranian institutions operating in the field. The Council plans to establish a National Cyber Center under its auspices, to integrate all Iranian cyberspace activity, gather and disseminate information and instructions, and oversee the enforcement of the Council's directives by all relevant bodies.

Iran's cyberspace structure comprises many cyberspace organizations working in various fields and officially affiliated with establishment organizations. One central organization with a defensive orientation is the Cyberspace Defense Command, which operates in the context of the Passive Defense Organization belonging to the general staff of the armed forces.[34] Alongside military personnel, this cyberspace organization also comprises government ministry representatives (the Communications, Defense, Intelligence, and Industry ministries). Its main objective is to develop a comprehensive defensive doctrine for state institutions and infrastructures against cyber threats.[35] The organization is primarily defensive, and currently does not seem to be involved in offensive cyber activity.

Another defensive cyberspace entity is the Center for Information Security, known as MAHER, established and operated as part of the Communications and Information Technologies Ministry. This center is primarily responsible for activating computer security incident response teams in the event of emergencies and cyber attacks. In addition, the center trains skilled manpower, develops response mechanisms to cyber crises, and stores and disseminates data security know-how. It is responsible for defending all government websites, as well as those of private companies operating officially and listed with the Communications Ministry. The center's teams were called on to impede and foil the work of the Flame and Stuxnet viruses that attacked Iran.[36]

Other cyberspace organizations focus on enforcement and control of intra-Iranian cyber activities that run counter to the regime's interests. In July 2009, the Supreme Council of the Cultural Revolution, which is subject to the supreme leader, founded the Committee to Identify Unauthorized Websites. Among its members are the Attorney General, the chief of police, the supervisor of government media, and various government ministers (from the Intelligence, Communications, Culture, and Science ministries, among others). The committee's purpose is to identify websites whose contents and activities are incompatible with the regime's requirements and wishes, and it is authorized to block access to such sites.[37] In 2011, the police established its own cyberspace unit, FETA,[38] to combat cybercrime – fraud, data theft, threats, and so on – but it is also authorized to take action against political and security criminals in cyberspace, and it is actually this latter task that primarily occupies it.[39] In addition, FETA is further charged with monitoring and controlling internet users in Iran, especially those in internet cafes around the country, where web surfing can be relatively anonymous.[40]

As for the offensive capabilities of Iran's cyberspace resources, the picture is less clear. Naturally, the Revolutionary Guards are crucial in the establishment and operation of offensive cyberspace warfare. Western experts place Revolutionary Guards capabilities in the top tier of cyberspace warfare worldwide.[41] A 2008 analysis by the research institute Defense Tech[42] estimated that the Revolutionary Guards cyberspace warfare program employed some 2,400 professionals and at that time had a budget of $76 million. Among capabilities that Defense Tech attributed to the Revolutionary Guards were: developing infected software by inserting malicious codes into counterfeit computer software; developing capabilities to block communications and WiFi networks; developing malicious codes (viruses and worms) capable of reproducing in networks and attacking target computers; developing tools for penetrating computers and networks to gather intelligence and pass it on to remote servers; and developing delay mechanisms installed in target computers to be operated by a predetermined schedule or by command from control servers.

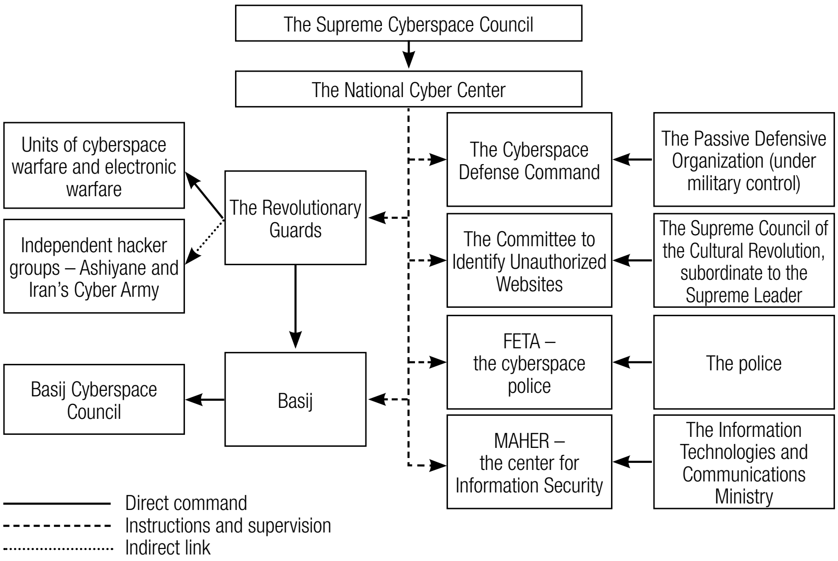
In addition to information warfare capabilities, the Revolutionary Guards are also creating an electronic warfare system capable of blocking radar and communications. The organization is investing large sums in the acquisition of electronic warfare systems[43] that, in conjunction with existing cyberspace warfare capabilities, will serve as an effective tool for compromising the electronic systems of the United States and its allies during a military confrontation.[44] According to declarations by the Revolutionary Guards, Iran has exhibited its prowess in the realm of cyberspace warfare with the capture of an unmanned aerial espionage vehicle in December 2011.[45]

Other than the Revolutionary Guards cyberspace warfare units, there is evidence linking the Revolutionary Guards and groups of Iranian hackers active against domestic and global enemies of the regime. The use of outsourcing allows the Revolutionary Guards and Iran to maintain distance and refute any allegations of Iranian involvement in cyberspace warfare and cybercrime. Experts have identified one group of Iranian hackers involved with the Revolutionary Guards as the Ashiyane Digital Security Team,[46] whose members are motivated by an ideology supporting the Iranian regime and the revolution, and who aim their attacks at the regime's enemies. The Ashiyane Team trains hackers and gives them significant capabilities,[47] which are then used for political activities (including the insertion of pro-Iranian propaganda into Western and Israeli websites and causing them to crash), as well as criminal enterprises (credit fraud, identity theft, and infiltration of databases and financial institutions). Furthermore, the group hosts a forum called War Games, which holds hacker competitions whose targets include American infrastructures companies.[48]

Another hacker group believed to be linked to the Revolutionary Guards is Iran's Cyber Army,[49] which consists of hackers and computer experts using fictitious identities and declaring themselves part of an organization. The group's main activities include breaking into Western websites with the aim of inserting pro-Iranian contents, seizing control of and redirecting information traffic, infiltrating Western data security companies, and damaging websites of the regime's opponents.

The Basij organization, which is subordinate to the Revolutionary Guards, has also become active in cyberspace and in 2010 established the Basij Cyberspace Council. Basij focuses primarily on creating pro-Iranian propaganda in cyberspace. It recruits and trains thousands of Iranians to write contents, afterwards deploying organized computer groups for tens of thousands of pro-regime bloggers. They also write talkbacks and other materials supporting the regime in the new media, on major forums, and on websites in Iran and abroad.[50] Nevertheless, Basij plans to further advance its cyberspace capabilities and is using experts from the Revolutionary Guards' cyberspace units to train hackers with high offensive capabilities.[51]

All of this clearly illustrates that in recent years Iran has established an extensive cyberspace structure encompassing many areas of activity, and has a wide range of capabilities at its disposal. The organizational flowchart below demonstrates the hierarchical configuration of the state's cyber establishment, as described above.


The Supreme Cyberspace Council
The National Cyber Center
Units of cyberspace warfare and electronic warfare
Independent hacker groups – Ashiyane and Iran's Cyber Army
The Revolutionary Guards
Basij Cyberspace Council
Basij
The Cyberspace Defense Command
The Committee to Identify Unauthorized Websites
FETA – the cyberspace police
MAHER – the center for Information Security
The Passive Defensive Organization (under military control)
The Supreme Council of the Cultural Revolution, subordinate to the Supreme Leader
The police
The Information Technologies and Communications Ministry
Direct command
Instructions and supervision
Indirect link

Clearly there have been significant advances in Iran's cyber activities. On the defense front all energies are focused on creating a defensive and isolation capability adequate for coping with any attempts at infiltrating the country's vital networks and infrastructures. Although it is hard to gain an entirely reliable picture of the development of offensive cyber capabilities, the following section of this article looks at several such activities.

Cyberspace Activities Attributed to Iran

In December 2011, an expose broadcast in an investigative program on the Univision television network led to an American inquiry into the involvement of official Iranian personnel in a cyber plot against the United States. The network's investigative reporters managed to infiltrate a group of Mexican hackers operating against US targets and secretly videotaped a meeting between their representatives and the Iranian Ambassador to Mexico. At the meeting, held at the Iranian Embassy, the hackers asked about the possibility of receiving support and financing from the Iranian government in order to carry out cyberspace attacks on American targets, such as the Pentagon, the CIA, the FBI, and various American nuclear installations. The video shows then-Iranian Ambassador to Mexico Muhammad Hassan Ghadari asking questions and proposing additional courses of action. The Ambassador stressed that Iran wants information on the possibility of an American attack on Iran. At the end of the conversation, he expressed his desire to stay in touch with the hackers and promised to forward the proposal to his superiors.[52] It may be assumed that this attempt was not an isolated one and that Iran is actively recruiting hackers and others around the world to further its offensive cyberspace goals.

A decisive determination of the identity of cyberspace attackers is complex and requires resources and international cooperation. Therefore, it is hard to say with absolute certainty who is behind many cyberspace actions. Nonetheless, it is often possible, using circumstantial diagnostics, to identify those responsible with a high degree of certainty. This article highlights three incidents: an attack on two data security companies aimed at stealing security permissions; an attack on large financial institutions in the United States; and an attack on the Saudi Arabian oil company Aramco.

The Attack on DigiNotar and Comodo

In 2011 two attacks took place on companies providing SSL (secure sockets layer)[53] permissions. The first, in March 2011, targeted the American company Comodo Ltd. Several permissions were stolen, among them domain permissions of internet mail services such as Google, but these were withdrawn before being used by the attacker. In fact, someone with authority in the mail.google.com domain can steal Gmail passwords and hijack users' accounts. Someone with a stolen authorization for the Microsoft.com domain can install malicious software in victims' computers. According to the company, the following findings came to light about this incident:[54]

a. The attack lacked features typical of cybercrime.
b. The attackers were organized and knew precisely what they were seeking before the attack, indicating the involvement of a state organization in the attack.

c. The source of the attack was primarily Iran (based on identification of the IP address).
d. The website where the stolen permissions were checked is located in Iran and was immediately removed from the web after Comodo discovered the attack.

The attack on Comodo failed to achieve its goal: it was identified and neutralized before the stolen permissions could be used. However, this was not the case with DigiNotar, the major Dutch SSL permissions provider. The company's databases came under attack from June through August 2011. During the attack, which came to be known by the name Black Tulip, certifications for website verification were stolen, including the certification serving to verify the google.com domain, thus allowing the attacker to assume this identity and reroute Gmail servers.[55]

An analysis ordered by DigiNotar (which went bankrupt and shut down operations after the attack) showed that 531 certificates were stolen and fabricated and that most stolen permissions were used to penetrate users' email accounts, especially in Iran. The analysis further revealed that the attack managed to penetrate more than 300,000 computers, which were overwhelmingly Iranian (more than 99 percent).[56] It is hard to determine the source of the attack with absolute certainty, but experts believe that it was Iran and that it was apparently intended for internal security purposes.[57] What led to this conclusion were the targets and extensive scope of users attacked and messages left on the company's website indicating Iranian involvement in the attack.

The Attack on American Financial Institutions

A report issued in the United States in September 2012 shows that at around the same time, several US financial institutions also came under attack, including sites belonging to the Bank of America, Morgan Chase, and Citigroup. Assessments by American sources concluded that the cyber attacks against the American financial institutions did not originate from random hackers, but were most likely financed by Iran and carried out by way of retaliation against sanctions imposed on Iran by the United States.[58]

As a result, the Financial Services Information Sharing and Analysis Center[59] issued an alert to banks in the United States about cyber attacks designed to steal identities via email, Trojan horses, and malicious tools for registering keystrokes and to retrieve user and employee names and passwords. Although large banks were also attacked, most of the victims were small and medium businesses, small banks, and credit companies. A group called the Izz ad-Din al-Qassam Cyberspace Fighters announced that it had attacked the Bank of America and the New York Stock Exchange in retaliation for a September 2012 movie expressing disrespect for the prophet Muhammad. These attacks, as described in the warning, indicate that the attackers succeeded in obtaining a great deal of information from the banks' networks, at least in some cases, and also accessed employees' entry permissions, thereby circumventing defensive mechanisms.[60]

The Attack against Aramco

In August 2012, apparently with insider help from someone with a high level of access to company computers, some 30,000 computers belonging to the Saudi Arabian oil company Aramco and the Qatari natural gas company ResGas were attacked by a computer virus called Shamoon. According to experts, this was one of the most devastating attacks carried out against any single company. The virus spread through the company's servers and attacked information stored in them. In-house computer experts say that the damage was limited to office computers and did not affect the company's operational and control systems.[61]

Symantec identified the virus for the first time in August 2012. An analysis by their experts and other security companies reveals the following findings:[62]

a. The Shamoon virus was designed to attack computers of an organizational computerized system (IT) rather than a control system. The virus is not in the same category of sophisticated cyberspace warfare tools such as Stuxnet, which attacked the Iranian nuclear program in 2010.

b. The purpose of the viral attack was not espionage or intelligence gathering but rather the complete and total destruction of data and target computers.

c. The writers of the malicious code do not seem to belong to the top tiers (such as the writers of Stuxnet and Flame), and there are indications that those behind it do not have a very high professional profile, since it was riddled with coding errors. They were, on the other hand, skilled enough to create a particularly destructive code.

d. The virus penetrated the company's computers with the help of a collaborator inside the company with direct access to the system and who seems to have used a USB device for the purpose.
e. The writers of the code used a section of a picture of a burning American flag to hide the contents of the files in the infected computers, indicating a political and/or religious (Islamic) affiliation.
f. The code of Shamoon's deletion mechanism contained the word Wiper. A similar name was used in the virus code of Flame, which attacked the Iranian oil company. This parallel raises a suspicion that the attack on Aramco was an Iranian retaliation to the Flame attack.

A group called The Cutting Sword of Justice claimed responsibility for the Aramco attack, declaring it was aimed at the main source of income in Saudi Arabia, a country accused of committing crimes against Syria and Bahrain. The group further claimed that the virus allowed it to access many secrets, but to date no relevant information on the issue has been reported. Reports on similar attacks on oil and gas companies in the Persian Gulf raised suspicions that the attacks were part of a concerted national effort. US Secretary of Defense Leon Panetta recently hinted at Iranian involvement in the attack. A former senior member of the American administration spoke out more directly when he claimed the administration believes Iran was behind the attacks in the Gulf.[63]

An analysis carried out by American cyberspace security expert Jeffrey Carr[64] raises a number of allegations linking Iran to the attack. It is the only country with access to the original Wiper code, which seems to have formed the basis for the Shamoon virus. According to a report issued by Kaspersky,[65] the Wiper code used in the attack on the Iranian Energy Ministry in April 2012 was also used by Shamoon's creators. Iran is highly motivated to attack the Saudi Arabian oil company because of harsh sanctions in place against Iran in the energy field. Furthermore, a suspicion of Hizbollah involvement in the attack was also investigated, and several Lebanese employees of Aramco were arrested and interrogated.

Conclusion

Iran's developed and developing cyberspace warfare capabilities should be a source of concern to Israel and, of course, the United States, as well as other Western nations. Because of the audacity demonstrated by the attempt on the life of the Saudi Arabian Ambassador to the United States, American experts feel that Iran's intentions and capabilities in daring to attack critical infrastructures in the United States should not be dismissed. Like the rest of the world, one may assume that Iran too – victim of one of the most destructive cyberspace attacks ever – has learned the lessons of Stuxnet and understands the destructive potential inherent in the development of an offensive tool that could damage industrial control systems, thereby causing physical destruction.

The development of the Iranian strategy and the subsequent force buildup processes indicates systematic preparations and organization with a view to becoming a major cyberspace warfare player. Experts report constant progress in Iran's cyberspace capabilities and operations. Following reports of the cyber attack on the American financial institutions attributed to Iran, one such expert stated, "[Iran's cyberspace program] is similar to the nuclear program: it isn't particularly sophisticated but it moves forward every year."[66] It would be a mistake not to take Iranian technological capabilities seriously. The country's science infrastructure is highly developed and there is a great deal of skilled manpower. One must therefore assume that before too long Iran will represent a significant threat in this area on the global level.

This assessment was further reinforced by the attack on Aramco, after which James A. Lewis, a specialist on cyberspace security, said that Iran was quicker in developing offensive capabilities and more daring in their use than anyone expected.[67] Usually, any activity that is exposed is no more than the tip of the iceberg of concealed activity. Furthermore, Iran's growing defensive sophistication requires interested parties to prepare to operate in an environment of isolated networks or an Iranian network isolated from the World Wide Web. Although the challenge of establishing such a network and achieving total isolation is enormous, such activity is also discernible. This defensive doctrine will represent a very tough challenge indeed for anyone interested in conducting activity in Iranian cyberspace.

The actions attributed to Iran as described above lead to several insights. Iran's attempts to secure SSL permissions indicate work against large groups of citizens rather than focused targets, such as nations or companies and organizations; they are apparently aimed at identifying and monitoring domestic targets. Nevertheless, the cumulative experience gained from such actions will also enable activity against more focused targets, such as nations and organizations. At the same time, although the detected activity indicates a certain degree of organization and systematic planning, it seems that Iran has yet to cross the threshold into the most sophisticated technological and organizational level. Nevertheless, the country's motivation, force buildup, and technological capabilities will enable it to make very rapid strides in that direction.

The attack on Aramco elicits further conclusions, the first being the fact that conventional defenses against internet threats are not enough. Most experts assume that the company had invested in protection against internet threats. The destructive virus was not discovered by virus protection systems and seems to have been inserted by a company insider possessing the appropriate permission. Current standard protective systems are not built to supply protection against focused threats (APT) and unknown malicious codes (Zero Date and others). Therefore, there is a growing need to develop tools capable of offering better protection against such threats. One such direction lies in developing tools based on the identification, blocking, and neutralization of anomalous and undesirable behavior in the computers under attack. Such tools can neutralize threats even after the malicious code has managed to enter the target computer. A second insight concerns the targets of the attack, which was aimed primarily at the mass and indiscriminate destruction of data in the tens of thousands of computers belonging to the Saudi Arabian oil company, rather than at intelligence gathering. If intelligence gathering in cyberspace may be considered legitimate in some cases, Iranian mass destruction of a civilian target is a sign that Iran is transitioning to retaliation. This should worry those in charge of defense in many nations. Leon Panetta's statement about the need to settle accounts with those behind the attack is one such illustration.[68] But of course actions will speak louder than words.

As the victim of one of the world's most destructive cyberspace attacks, one may assume that Iran fully understands the potential inherent in this realm, and accordingly will work to develop similar capabilities of its own. In that case, the systematic force construction described in this article will very quickly turn Iran into a significant player on the cyberspace battlefield; this will include attacking critical infrastructures in hostile nations, such as the United States and Israel, while creating maximum separation in the event of exposure of such activity. Iran uses so-called civilian hacker communities to try to create a distance between cyber activities and the regime and official Iranian organizations. A similar approach is adopted elsewhere in the world, e.g. China and Russia, allowing those nations to deny responsibility and lay the blame at civilian doors. Therefore the major challenge of connecting Iran to cyberspace offensives will continue.

Iran's focus of cyberspace activity on Israel and other Western countries requires designated defensive responses. All the countries in question need an updated doctrine on cyberspace defense and protection. The attackers' sophistication necessitates intelligence-based defense activity in addition to generic protections. Therefore, and in light of Iran's development processes, Israel must place Iranian cyberspace high on its list of intelligence priorities, preempting and foiling offenses before they can be carried out. In a way comparable to the Iranian nuclear program, the challenge is not Israel's alone but faces many nations in the West, as well as the Gulf states, as evidenced by the attack on Aramco. Hence, international cooperation of the widest scope possible should be initiated toward intelligence and preemption of Iranian cyberspace activity.

At the same time, Israel must continue to build an effective defensive response focused on three relevant national layers of cyberspace. The first is security organizations, which constantly need to test exposure to Iranian cyberspace capabilities and ensure they are not succeeding in damaging the critical capabilities of the defense establishment. The second concerns the network of critical infrastructures guided by the Information Security Authority by virtue of an Israeli government decision. Here too, the challenge requires constant activity, especially in terms of understanding the threat, adapting the response to it, and sharing information among the various institutions. Finally, one must not dismiss Iran's capabilities and possible attempts to damage non-governmental commerce and industry. Private sector commercial and industrial corporations usually take steps primarily to safeguard their data assets. It is hard to demand that they protect themselves against the possibility of a cyberspace attack from a foreign nation such as Iran. Hence the critical role of the recently established National Cyberspace Staff as an integrating entity capable of promoting processes of regulation, information sharing, and intelligence on the basis of the evolving map of threats.

Notes

1 Art Keller, "The Great Persian Firewall, "*Foreign Policy,* September 2012, p.28, http://www.foreignpolicy.com/articles/2012/09/28/Iran_firewall_google?page=full.

2 Khamenei's statement announcing the establishment of the council on his official website, http://farsi.khamenei.ir/message-content?id=19225.

3 Ilan Berman, "The Iranian Cyber Threat to the U.S. Homeland," Statement before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Subcommittee on Counterterrorism and Intelligence, April 26, 2012, pp. 1-3, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Berman.pdf.

4 CBS News, "Iran Confirms Stuxnet Worm Halted Centrifuges," November 29, 2010, http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml.

5 Kevin McCaney, "Iran Building a Private, Isolated Internet, but Can it Shut out the World?" *GCN*, April 10, 2012, http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx.

6 Agence France Presse, "Iran Denies has Plan to Cut Internet Access," *AFP*, April 10, 2012, http://www.google.com/hostednews/afp/article/ALeqM5h4e57x6CYbsavza1PeDuQP7Bf9Vg.

7 Amir Taheri, "Iran will Launch its National Internet Next Week but not for the Reasons you Might Think," September 20, 2012, http://www.opednews.com/articles/Iran-will-launch-its-natio-by-Amir-Taheri-120919-83.html.

8 Brian Ross, "What Will Happen to the US If Israel Attacks Iran?" *ABC News*, March 5, 2012, http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id1584852.

9 Berman, "The Iranian Cyber Threat to the U.S. Homeland," p. 4.

10 Reza Marashi, "The Islamic Republic's Emerging Cyber War," National Iranian American Council, April 30, 2011, http://www.niacouncil.org/site/News2?page=NewsArticle&id=7318.

11 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

12 J. P. Patterson and M. N. Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, Master's Thesis (Monterey, CA: Naval Postgraduate School, 2005), pp. 17-22, www.fas.org/irp/eprint/cno-iran.pdf.

13 Sharif University website: http://www.sharif.ir/web/en.

14 Institute website: http://www.aictc.com/web/content/main.

15 Institute website: http://acri.sharif.ir/en/Default.asp.

16 Advanced course descriptions: http://ceit.aut.ac.ir/autcms/courses/courseOfferingView.htm?level=M.Sc&depurl=computer-engineering&lang=en&cid=70317.

17 The data security lab website: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3350532&depurl=computer-engineering&lang=en&cid=147776.

18 The secure systems analysis lab website: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3369580&depurl=computer-engineering&lang=en&cid=147732.

19 Patterson and Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, pp. 29-35.

20 For more on the center's activity in information security, see http://www.itrc.ac.ir/itrc-secure-en.php.

21 Reference to investments in information technologies at the Technological Cooperation Office website, http://citc.ir/newpages/page27.aspx?lang=Fa.

22 Iran Watch, "The Wisconsin Project on Nuclear Arms Control," January 3, 2011, http://www.iranwatch.org/suspect/records/technology-cooperation-office.htm.

23 The list of companies at Pardis Technology Park is available at http://www.techpark.ir/?/content/142.

24 Guilan Science and Technology Park website: http://www.gstp.ir/modules.php?name=Content&pa=showpage&pid=16.

25 Steve Stecklow, "Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf.

26 Marashi, "The Islamic Republic's Emerging Cyber War." Informational literature presenting the Separ technology and indicating the link between the regime and the technology's development may be found at http://www.iranascience.com/1-home/newsletters/21-Web%20Filters.pdf.

27 OpenNet Initiative, *Internet Filtering in Iran*, June 16, 2009, http://opennet.net/research/profiles/iran.

28 McCaney, "Iran Building a Private, Isolated Internet."

29 Robert Tait, "Iranian State Goes Offline to Dodge Cyber-Attacks," *The Telegraph*, August 5, 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-goes-offline-to-dodge-cyber-attacks.html.

30 Cyrus Farivar, "Security Researcher Unearths Plans for Iran's Halal Internet," *Ars Technica*, April 17, 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/.

31 Tait, "Iranian State Goes Offline to Dodge Cyber-Attacks."

32 Ali Akbar Dareini and Brian Murphy, "Iran Internet Control: Tehran Tightens Grip on Web," *Huffington Post*, April 16, 2012, http://www.huffingtonpost.com/2012/04/16/iran-internet-control_n_1429092.html?ref=world.

33 Emily Alpert and Ramin Mostaghim, "Iran's Supreme Leader Calls for New Internet Oversight Council," *Los Angeles Times,* March 7, 2012, http://

latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html.

34 "Structure of Iran's Cyber Warfare," *BBC Persian*, p. 1, http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf.

35 "Iran is Formulating Strategic Cyber Defense Plan: Official," *Tehran Times*, June 15, 2012, http://tehrantimes.com/politics/98761-iran-is-formulating-strategic-cyber-defense-plan-official.

36 The center's structure and functions are described on its official website: http://www.certcc.ir/index.php?newlang=eng.

37 "Structure of Iran's Cyber Warfare", pp. 4-5.

38 "Iran to Crack Down on Web Censor-Beating Software," *Hürriyet Daily News*, September 22, 2012. http://www.hurriyetdailynews.com/iran-to-crack-down-on-web-censor-beating-software.aspx?pageID=238&nID=22789&NewsCatID=374.

39 "Structure of Iran's Cyber Warfare," p. 4.

40 In January 2012 the regime passed a set of laws for monitoring and surveillance of web surfers at internet cafes throughout the country. These laws allow FETA to create a user log of all temporary surfers in the country and monitor anti-regime activities in cyberspace. Farnaz Fassihi, "Iran Mounts New Web Crackdown," *Wall Street Journal*, January 6, 2012, http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html.

41 Berman, "The Iranian Cyber Threat to the U.S. Homeland," p. 4.

42 Kevin Coleman, "Iranian Cyber Warfare Threat Assessment," *Defense Tech*, September 23, 2008, http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment.

43 Stephen Trimble, "Avtobaza: Iran's Weapon in Alleged RQ-170 Affair?" *The DEW Line*, December 5, 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html.

44 Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," A Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies. April 26, 2012, p. 5, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo.pdf.

45 Scott Peterson, "Iran's Cyber Prowess: Could it Really have Cracked Drone Codes?" *Christian Science Monitor*, April 24, 2012, http://www.csmonitor.com/World/Middle-East/2012/0424/Iran-s-cyber-prowess-Could-it-really-have-cracked-drone-codes.

46 Cilluffo, "The Iranian Cyber Threat to the United States," p. 5.

47 Patterson and Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, pp. 44-49.

48 Iftach Ian Amit, "Cyber [Crime | War]," paper presented at DEFCON 18 Conference, July 31, 2010, http://www.defcon.org/images/defcon-18/dc-18-presentations/Amit/DEFCON-18-Amit-Cyber-Crime-WP.pdf.

49 Khashayar Nouri, "Cyber Wars in Iran," *Institute for War & Peace Reporting,* July 23, 2010, http://iwpr.net/report-news/cyber-wars-iran.

50 Golnaz Esfandiari, "Basij Members Trained to Conquer Virtual World," *Payvand Iran News*, August 21, 2010, http://www.payvand.com/news/10/aug/1206.html.

51 Jeffrey Carr, "Iran's Paramilitary Militia is Recruiting Hackers," *Forbes,* January 12, 2011, http://www.forbes.com/sites/jeffreycarr/2011/01/12/irans-paramilitary-militia-is-recruiting-hackers/.

52 Bob Beauprez, "Iranian Cyber-Attack Plot against U.S. Exposed in Mexico," *Townhall*, December 13, 2011, http://finance.townhall.com/columnists/bobbeauprez/2011/12/13/iranian_cyber attack_plot_against_us_exposed_in_mexico/page/full/.

53 SSL is a protocol for security communications on the internet, making sure that the server a client is contacting is in fact the right server, while encrypting the information between the browser and the server. SSL keys can be purchased from authorized providers. The theft of keys would allow the thief (with control of the network's infrastructure) to divert surfers to counterfeit websites masquerading as legal sites and thereby access confidential information about the user.

54 Report issued by Comodo Ltd., March 13, 2011, http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html.

55 Eva Galperin, Seth Schoen, and Peter Eckersley, "A Post Mortem on the Iranian DigiNotar Attack," *Electronic Frontier Foundation,* September 13, 2011, https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack.

56 Fox-It, Interim Report, "DigiNotar Certificate Authority Breach 'Operation Black Tulip,'" September 5, 2011.

57 Toby Sterling, "Iran Involvement Suspected in DigiNotar Security Firm Hacking," *HuffPost Tech*, September 5, 2011, http://www.huffingtonpost.com/2011/09/05/iran-diginotar-hack_n_949517.html.

58 Gerry Smith, "Cyber Attacks Against US Banks Sponsored by Iran, Lieberman Says," *Huffington Post,* September 9, 2012.

59 The FS-ISAC is an organization whose role is to analyze and share information among financial institutions about threats to critical financial services in the United States.

60 Jaikumar Vijayan, "U.S. Banks on High Alert against Cyber Attacks," *Computerworld*, September 20, 2012, http://www.computerworld.com/s/article/print/9231515/U.S._banks_on_high_alert_against_cyber ttacks.

61 Jim Finkle, "Exclusive: Insiders Suspected in Saudi Cyber-Attack," *Reuters*, September 7, 2012, http://in.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idINBRE8860CR20120907.

62 Kelly Jackson Higgins, "Shamoon Code 'Amateur' but Effective," *Dark Reading*, September 11, 2012, http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240007179/shamoon-code-amateur-but-effective.html; Nicole Perlroth, "Cyber Attack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyber attack-on-saudi-oil-firm-disquiets-us.html?_r=1&adxnnl=1&pagewanted=all&adxnnlx=1351084069-1i53F0BCczNEGcP8ut3n4A&.

63 Associated Press, "Panetta Hints Iran behind Gulf Cyber attacks," *CBS News*, October 12, 2012, http://www.cbsnews.com/8301-202_162-57531088/panetta-hints-iran-behind-gulf-cyber attacks.

64 Jeffrey Carr, "Who's Responsible for the Saudi Aramco Network Attack?" Blogspot, August 27, 2012, http://jeffreycarr.blogspot.co.uk/2012/08/whos-responsible-for-saudi-aramco.html.

65 Global Research & Analysis Team, "Shamoon the Wiper – Copycats at Work," *Kaspersky Lab Expert*, August 16, 2012, https://www.securelist.com/en/blog?print_mode=1&weblogid=208193786.

66 Reuters, "Iranian Hackers Attacked Three Largest U.S. Banks as Part of Cyber Campaign: Sources," September 21, 2012, http://news.nationalpost.com/2012/09/21/iranian-hackers-attacked-three-largest-u-s-banks-as-part-of-cyber-campaign-sources.

67 Perlroth, "Cyber Attack on Saudi Firm, U.S. Sees Iran Firing Back."

68 Associated Press, "Panetta Hints Iran behind Gulf Cyber Attacks."