Developments in Iranian Cyber Warfare 2013-2014

Gabi Siboni and Sami Kronenfeld

In the course of 2013, Iran became one of the key players in the international cyber warfare theater. This development is a result of both defensive and offensive cyber force buildup processes and a measured relaxation of restraints on the part of Iranian decision makers with respect to offensive activity in cyberspace. Indeed, the Iranian activity points to major qualitative advances in Iran's technological and operational cyber capabilities. This article examines the activity and progress in Iran's cyber defense system, and the regime's use of this capability to restrain internal opposition. In addition, it looks at the offensive dimension, particularly cyber-attacks traced to Iranian agencies, agents, and allies.

Keywords: cyber, Iran, cyber security, cyber defense, networks isolation

Introduction

In an interview to the Atlantic Council, an American research institute, a senior source in the CrowdStrike Cyber Security Company rated Iran as a "third tier" country in regards to its cyberspace capabilities, stating that its cyber warfare capabilities were substantially inferior to those of "first tier" countries, such as the US, Russia, and the UK, as well as "second tier" countries such as China. This conception is in line with many Western intelligence specialists and administration officials. Iran is perceived as capable of harassing Western security systems and damaging "soft" targets, while lacking the knowledge and means to execute strategic cyber-attacks.[1] Nevertheless, during 2013, Iran became one of the key players in the international cyber warfare theater. It appears that this development is

Dr. Gabi Siboni is a senior research fellow and head of the INSS Cyber Warfare Program. Sami Kronenfeld is an intern in the Cyber Warfare Program at INSS.

a result of a combination of a measured relaxation of restraints on the part of Iranian decision makers with respect to offensive activity in cyberspace, and a major qualitative advance in the Iranian cyber warfare apparatus, which has surprised many Western experts in the extent of its activity, its professional sophistication, and its ambitious selection of targets.

Events such as the Stuxnet attack, severely damaging Iran's centrifuges, and the widespread protest that accompanied the 2009 elections in Iran – in which social networks and the internet played a major role in organizing protests and escalating events – have turned cyberspace into an important theater for the Iranian regime. These events and other cyber-attacks against Iran have led the regime to establish a ramified cyber apparatus, including operational frameworks with a command structure and professional echelon specializing in a variety of areas. Iran has invested over $1 billion in developing technologies, setting up infrastructure, and training defensive and offensive personnel.[2] Iranian cyber strategy is devised and overseen at the highest levels, among them the President, commander of the Revolutionary Guards, and senior ministers serving on the Iranian Supreme Cyberspace Council – the senior agency coordinating the country's cyber activity.[3]

This article seeks to present an up-to-date analysis of Iranian activity in cyberspace. The article is divided into two parts; the first examines Iran's cyber defense system's progress and activity, and the use of these capabilities to restrain its internal opposition. The second examines the offensive dimension, mainly through cyber-attacks traced to Iranian agencies, agents, and allies. Concluding insights are provided at the end of the article.

The Defensive Concept

Iran is aiming to create a multi-level defense system combining security, monitoring, and supervising technologies with physical enforcement mechanisms for the aggressive pursuit of operatives operating against the regime in cyberspace. To this extent, Iran is taking action through three main channels: first, it is creating a protective envelope against attacks on its essential infrastructure and sensitive information, such as the Stuxnet attack that damaged its uranium enrichment program. Second, it is striving to neutralize cyber activity executed by opposition groups and opponents of the regime, for whom cyberspace constitutes a key platform for communications, information distribution, and organized actions against the regime. Third, it aims to prevent harmful Western content and ideas from infiltrating Iran's internal cyberspace – ideas that could contribute to the development of a "soft revolution," undermining the regime's stability.

The targets and operational principles of the Iranian cyber defense apparatus, dictated by Iran's Supreme Council of Cyberspace, are implemented by central government agencies, such as the Passive Defensive Organization (belonging to the army), the Supreme Council of the Cultural Revolution (subject to the Supreme Leader), the Iranian Police, and Ministry of Communications.[4] Some of the technological and organizational infrastructure established by Iran has matured during the past year into operational agencies significantly contributing to strengthening Iranian defensive operations in cyberspace.

The Networks Isolation Project – Disengagement from the World

The Networks Isolation Program is one of the Iranian regime's main strategies in cyberspace. The project began materializing as early as 2009, when Iran's objective was to transfer the cyber activity in the country to an internal communications network, dubbed Halal Internet, isolated from the World Wide Web. The Iranian network was designed to operate in the spirit of the Shiite Muslim norms encouraged by the regime, and to enable the government to completely control and supervise the network's content, information, and users. From the regime's perspective, the establishment of an intranet network and the separation of Iranian cyberspace from global cyberspace is a key measure in strengthening its defense against cyber-attacks and espionage, preventing penetration by Western elements that do not coincide with those of the regime, and neutralizing its internal opposition.[5]

The first evidence of the Iranian network's operation was discovered in October 2012, when American cyber researchers, in cooperation with Iranian sources, noticed that Iranian Internet providers have begun allocating two IP addresses to every computer connected to the Internet – an ordinary internet address and an internal Iranian address, which could be accessed only from inside the country. The researchers estimated that the internal Iranian network was capable of managing 17 million IP addresses and that more than 10,000 home, commercial, and government computers were connected to it during 2012. In 2013, Halal Internet began to accumulate content (censored and supervised, of course), with a strong emphasis on development of local versions of popular internet services, such as e-mail, social networks, video and audio communications, map websites, and video websites.[6]

In July 2013, the Iranian regime inaugurated an e-mail service, @post.ir, requiring civilians to register and designed to constitute the main channel of communication between private citizens and the various governmental agencies. This service, which supports Farsi, English, French, and Arabic, is capable of providing e-mail addresses to about 100 million users. Each user is allocated a 50-megabyte mailbox, which can be expanded to up to two gigabytes. Opening the mailbox requires a person to give his name and address, and it appears that the email addresses provided are not encrypted – therefore enabling the regime to closely supervise the users and traffic in these addresses.[7] In December 2012, the Iranian State Broadcasting Authority launched a YouTube-like website under the name of "Mehr," displaying supervised content and enabling surfers to upload their own content under strict censorship rules.[8] The Iranian authorities also banned the use of foreign Information Security software, as they developed a local anti-virus system called "Padvish." According to Iranian sources, this system can protect networks and prevent malware penetration.[9]

In order to increase the number of Halal Internet and Iranian Internet services' users, the regime expanded its use of technological and legislative measures restricting Iranian citizens' possibilities for accessing the World Wide Web. The Iranian authorities blocked the use of Voice-over-IP software, such as Skype and Google Talk. Use of many VPN and TOR networks as well as filtering evasion software, important tools in bypassing government supervision and censorship of cyberspace, was also banned.[10] In addition, the Iranian cyber authorities began to deliberately slow external websites and Internet services (mainly services by Google, which are very popular in Iran), at times reaching 6 percent of the ordinary speed. The authorities are also carrying out websites and services migrating blocks, and are greatly restricting traffic on the encrypted Internet. These actions pose technical, legal, and psychological difficulties for Iranian citizens seeking to surf the World Wide Web, and are, in effect, forcing them to use the supervised and censored Halal Internet.[11]

Development of Defense and Supervision Technologies

As a supplementary measure to isolating the networks, Iran is investing in the development of its own cyber technologies and defense tools in order to reduce its dependence on foreign products that may prove to be Trojan Horses. A well-publicized ceremony attended by senior Iranian defense officials, including Minister of Defense General Hossein Dehqan and Civil Defense Unit Commander Gholam Reza Jalali in December 2013 unveiled 12 technological developments by Iranian industry, including a secure cellular telephone designed to provide users with a communication line impenetrable by electronic surveillance, a secure operating system designed to eliminate Iranian dependence on American operating systems, a GPS device, an optical communications system, software and systems against malware and a firewall. A system for identifying a cyber-attack, and equipment for information security centers were also unveiled at the conference.[12] Furthermore, the Iranian news agency ISNA reported that Iran had begun using a national cyber protection system called "Shahpad." According to Mohammed Naderi, head of the project, the system facilitates fusing information from a variety of user stations and sensors, and generates an overall nationwide cybernetic picture. In case of an attack, Shahpad immediately informs the data security centers in the country, enabling them to respond quickly, and to take action to block the attack.[13]

Iran is not relying solely on local development in order to reinforce its cyber security capability. In September 2012, it signed an extensive technology cooperation agreement with North Korea including information technology. According to experts, it is very likely that the two countries that have both been targets of cyber-attacks, and both regard this field as strategically important, will combine forces under this agreement to develop information security, monitoring, and even offensive technologies.[14]

Iran is also cooperating with China in the cyber field, and previously purchased a surveillance system from a Chinese company named ZTE Corp., making it possible to monitor voice communications, text messages, and Internet browsing.[15] Cooperation with these and other countries, such as Russia, is of great assistance in strengthening Iran's cyber defense and ability to conduct surveillance of the Internet and its own citizens' usage.

Strengthening Defensive Deployments

Beyond the technological aspects, Iran is placing special emphasis on reinforcing various state agencies' ability to face and thwart cyber-attacks. The Iranian cyber apparatus had conducted a number of comprehensive cyber defense drills training civilian and military units. In addition, a cyber-war exercise was conducted as part of naval maneuvers by the Revolutionary Guards in the Strait of Hormuz in December 2012. As part of this exercise, a cyber-attack was launched against the fleet's computer network in order to retrieve information and insert malware. The commanders of the exercise declared that the attack had been detected and foiled by the fleet's cyber defense system.[16]

In February 2013, the Iranian Fars News Agency, which is close to the regime, reported a comprehensive drill by the Revolutionary Guards' ground forces, examining and assessing the organization's cyber defense systems.[17] Another drill took place in October 2013 as part of the Passive Defense Organization's general defense maneuvers. As part of this drill, key government agencies' cyber defense apparatuses were examined, including nuclear installations, the Tehran metro subway network, the Iranian Broadcasting Authority, ports, the Iranian Central Bank, and the cellular communications' providers. According to the Passive Defense Organization commander, many security breaches in these organizations' cyber defense systems were found and managed. Following the drill, it was decided to establish a cyber-defense center at the Natanz nuclear facility.[18]

Restraining Regime Opponents

Iran is supplementing the technological measures it is taking in order to protect its cyberspace with aggressive physical enforcement action against its opponents at home, who use cyberspace extensively for subversive purposes. A key player in the Iranian regime's efforts to control its cyberspace is FATA, the Cyber Police, founded in 2011 under the command of the Iranian Police. Over the past year, FATA has become more aggressive in its efforts to enforce censorship restrictions and prevent subversive activity in cyberspace. The agency is engaged in locating and apprehending bloggers, online journalists, and opposition members supporting and voicing ideas and views that run contrary to the regime's positions.

The intense aggression against the regime's opponents exhibited by the Iranian Cyber Police gained global attention in November 2012, following reports of the death of Iranian blogger Sattar Beheshti in a prison near Tehran. Beheshti, who was arrested by FATA after he published a blog voicing criticism of the Iranian legal system (which he called "Khamenei's Slaughterhouse"), died as a result of torture and severe beating by the Cyber Police.[19] Reports of his death aroused a wave of criticism both within and outside Iran. As a result, the European Union imposed sanctions on FATA and other parties involved in his death, including judges and officials responsible for censorship in Iran.[20] International pressure led to the dismissal of the Cyber Police commander in Tehran,[21] but according to international human rights organizations, FATA is persisting in its strategy of widespread arrests and aggressive action to locate and punish Iranians expressing opposition to the regime on social networks and in blogs.[22] In recent months, the Iranian Cyber Police tightened its supervision of the popular Internet Cafes, closing dozens for violating the state's stringent registration laws and restrictions.[23]

The regime's supervision and enforcement became particularly intensive and thorough in the months leading up to the presidential elections on June 14, 2013. Two days prior to the elections, Google reported that it had detected and thwarted a phishing attack launched by parties inside Iran aimed at tens of thousands of e-mail accounts belonging to Iranian citizens. The attack included sending an e-mail disguised as a maintenance message from the Gmail system asking the user to type in his e-mail user name and password. The information typed was then transferred directly to the attackers, providing them with untrammeled access to the user's e-mailboxes.[24] An analysis of the attack raised the suspicion that the attackers were the same Iranians who attacked the Dutch DigiNotar company's servers in 2011.[25] The attackers' targets were unclear, though it appears there is a close connection between the attack and the election campaign, and that the attackers wanted to enable the Iranian authorities to collect information about the actions and opinions of Iranian citizens, and to take action against "problematic" elements.[26] In addition, in the weeks leading up to the elections, a broad cyber-attack took place against Iranian opposition and communications websites. A group of hackers calling itself "The Unknown Cyber Jihad," and, claiming affiliation to Hizbollah, broke into a number of Iranian opposition websites and replaced their content with a message aimed against the regime's opponents. Key opposition websites, such as the Communist Movement in Iran, the Green Movement, and human rights websites, were blocked by the regime for many hours, and dozens of online activists and journalists were arrested and imprisoned by the Iranian security forces.[27]

Following the events that accompanied Ahmadinejad's re-election in 2009, Iranian activity against the opposition and opponents of the regime has developed and become more advanced. At the time, the opposition used cyberspace with relative ease to organize demonstrations, distribute ideas, and transmit information about events in Iran to a target audience outside of the country (mainly through the use of VPN networks). In the

2013 elections, however, the Iranian cyber apparatus was technologically and operationally prepared and ready to control the dialogue that took place on the internet, and monitor subversive activity and the outwards flow of information from within Iran.

It appears that to date, the Iranian cyber defense system still has a long way to go before it is able to deal effectively and consistently with highly sophisticated cyber-attacks, such as Stuxnet and Flame, and to prevent any penetration by external content or ideas. Some describe this apparatus as no more than an improvised and less organized version of the Chinese "Cyber Wall."[28] Nevertheless, the great technological and organizational strides that Iran has made over the past year indicate a steep learning curve, and that it is likely to devise an effective and comprehensive defense system earlier than expected.

The Offensive Aspect – The Search for "High-Quality" Attacks

The Islamic Republic of Iran regards cyber warfare as an effective platform enabling it to inflict damage on enemies in possession of clear military superiority, while at the same time maintaining room for denial in order to avoid international condemnation, or even sanctions and counterattacks. This conception had led Iran to use cyber warfare as an important tool for attacking Western targets in response to sanctions, and as a means of deterrence against escalating sanctions actions against Iran by Western countries. The scope, targets, and relative success of cyber-attacks conducted over the past year and their attribution to Iranian groups indicate increased Iranian capabilities. Intelligence and administration officials in Israel and the US have also expressed concern regarding the speed of Iranian cyber warfare capabilities' development.[29]

Western sources attribute the progress in Iran's cyber warfare program to its success in integrating its capabilities, know-how, and trained personnel from Iranian computer science faculties[30] with the Iranian hacker community's extensive experience and highly developed abilities, many of whose members identify with the regime and its goals. The Iranian hacker community is one of the most dominant and active communities worldwide, and evidence suggests connections between its various groups and the Revolutionary Guards. The use of hackers, whose connections to the Iranian regime are vague, provides room for ambiguity and deniability when facing accusations of involvement in malicious and illegal cyber activity.

One of the leading Iranian hacker groups is the Ashiyane Digital Security Team, which is believed to have connections with the Revolutionary Guards, and whose members are ideologically motivated to support the Iranian regime and the revolution.[31] The Zone-H website, specializing in analyzing hacker activity in cyberspace, rates Ashiyane as second in the world in the number of websites into which its members have succeeded in breaking and corrupting, usually by replacing the content with the group's icon, or with pro-Iranian propaganda. The websites broken into by Ashiyane members include 26 Brazilian government websites, among them the Military Police website, and government websites in the UK and Pakistan.[32] According to Zone-H, besides Ashiyane, there are seven other Iranian hacker groups among the world's 40 most active hacker groups involved in corrupting websites. Such attacks are considered relatively minor, but they indicate a high level of technological capabilities, and in many cases serve as cover for information theft or introduction of malware and Trojan Horses.

Another factor contributing to the Iranian cyber warfare program's rapid progress is the Iranian cyber system's close relations with cyber criminals, hackers, and information security experts, primarily Russian, who are willing to hire out their capabilities for money. American sources regard these connections as a key element in Iran's rapid progress, and Congressman Michael Rogers, Chairman of the House of Representatives Select Committee on Intelligence, also stated that the wave of cyber-attacks against American banks' websites, which was attributed to Iranian groups, showed signs of involvement by Russian groups.[33] In addition to "importing" personnel, Iran can also purchase a powerful and technologically sophisticated cyber weapon which is available on the black market to the highest bidder. This Cyber Weapon enables the Iranians to rapidly enhance their capabilities and the threat posed by them.[34]

The Iranian cyber warfare capabilities' progress is reflected in a series of attacks that occurred in the second half of 2012 and in 2013, utilizing more sophisticated techniques, attacking high quality targets, and on a larger scale than earlier attacks attributed to Iran. One attack attributed to Iranian groups began in September 2012 and continued into 2013, including a large-scale attack on the websites of key banks and financial institutions in the US. Information security experts described this attack as "unprecedented in scope and effectiveness." Its uniqueness and quality lay in the method employed by the attackers: instead of attacking through breaches in individual computers, they routed their attacks through data centers' computer networks. These data centers, operated by companies like Google and Amazon.com, are composed of giant computer networks connecting hundreds, sometimes thousands, of servers and computers, providing cloud computing services to a large number of companies and businesses throughout the world. The attackers succeeded in taking over part of these computing "clouds," utilizing their enormous computer power as a platform for attacks on the websites of US-based banks and financial companies. Security specialists described this maneuver as the "cybernetic equivalent of turning a Chihuahua into a fire-spitting Godzilla."[35]

A group of hackers calling itself Izz a-Din al-Qassam Cyber Fighters assumed responsibility for the service-denying attack against the websites of important banks in the US, which included Bank of America, Citigroup, and HSBC. Members of the group exploited the data centers' computer platform to channel enormous volumes of traffic to the banks' websites, causing them to crash and denying their customers access to their accounts. In addition to using traffic, the attackers employed a technique called Encrypted DDos (distributed denial of service). This method exploits the banks' own information encryption mechanisms, whose operation requires major system resources. The attackers flooded the banks' websites with transactions requiring encryption, thereby substantially slowing and hindering their activity. Nevertheless, the bank accounts were not broken into during the attacks, and customers' money was not stolen.[36]

Information security experts state that the high level of capabilities required to carry out an attack on such a large scale and with such great technological sophistication indicates that a country must be involved. An attack against a country's financial infrastructure, especially an economic power like the US, has serious consequences, and is liable to cause severe economic damage as it disrupts many commercial companies and households' regular financial activity.

Despite Iranian denials and the absence of physical proof, senior US administration and intelligence officials are convinced that Iran is behind the attacks as a response to the international sanctions against it and the cyber-attacks that damaged its infrastructure, for which it holds the US and Israel responsible. The US Secretary of Defense at the time, Leon Panetta, commented on the attacks against the banks, saying that they constituted a "significant escalation," without mentioning Iran by name.[37]

Another wave of attacks attributed to Iranian groups focused on American infrastructure and energy companies. It began to gather steam in early 2013, until the US Department of Homeland Security decided in May 2013 to issue an exceptional warning to energy and infrastructure companies regarding the escalating cyber threat to their computer networks. This warning stated that these were not routine attacks for the purpose of stealing information, industrial espionage, or inflicting damage on administrative systems; they were attacks seeking to gain control of their systems and damage their physical operations or the safety equipment of critical infrastructure, such as oil and gas pipelines and electrical systems. The American administration did not officially declare Iranian involvement, but experts and administration officials said that there was operational evidence indicating that the attacks had originated on Iranian soil, and that carrying them out required at least some support from the agencies in charge of Iranian cyberspace.[38] Any future sanctions escalation against the Iranian energy market is likely to cause Iran to take strategic measures against the international energy market, both as a deterrent measure and in order to increase the demand for its oil. [39]

Experts describe the attacks on the American energy companies' computer networks as a large-scale information collection operation, learning and assessing the systems in order to create knowledge infrastructure and gain experience in preparation for a future attack on the control systems that operate and regulate critical infrastructures' activity. Harming these systems is liable to cause significant damage and even loss of life on a large scale. Indeed, in the course of the attack, the attackers succeeded in bypassing some of the security systems and collecting information about their structure, capabilities, and their security breaches.[40] A senior source in Mandiant, an Information Security company, said that in at least one case, its investigators had succeeded in tracing the attack to a group of Iranian hackers whose connections with the regime were unclear. He added that the attackers' goal, moving within the American computer systems and studying their detection and security array, was to accumulate experience with "live" networks, and to explore their weak points.[41] Senior American officials stated that the attacks against the energy companies and the hackers' relative success indicated that the cyber offensive capabilities at the Iranians' disposal were improving and developing rapidly.[42] If Iran obtains effective offensive capabilities against essential infrastructure systems' control, this is likely to constitute a strategic threat to its enemies.

Another significant attack attributed to Iran occurred in September 2013, when official US sources reported that an unclassified US Naval computer network had been compromised. The sources said that the attack had been committed by a group of hackers operating in the service of the Iranian regime, or at least with its consent and support. The network affected was the fleet's internal network, which, while unclassified, is used for correspondence and communications, among other things, and contains sensitive information, such as e-mail addresses of the fleet commanders and of senior officials. Administration sources reported that the attackers had succeeded in penetrating the network management systems, but claimed that no significantly valuable information had been stolen, and that e-mailboxes had not been broken into. Particularly alarming was the fact that the hackers continued operating in the fleet's computer network even after American security agencies had reported their successful removal from the network. The Iranian sophistication revealed in this attack is another sign of the development and progress in Iran's infiltration capabilities, and of Iran's readiness to target military cyber systems.[43]

In addition to the series of attacks against American institutions, groups affiliated with Iran assumed responsibility during the past year for cyber-attacks against Israeli institutions. In June 2013, Prime Minister Benjamin Netanyahu announced that there has been a steep rise in the Iranian cyber-attacks against important computer infrastructure in Israel.[44] In December 2013 and January 2014, a group of Islamic hackers calling itself The Islamic Cyber Resistance Group (ICRG) claimed that it had conducted a number of high-quality attacks against targets in Israel and the Middle East in revenge for the killing of senior Hezbollah leader Hassan al-Laqqis. The group, extensively publicized by the Iranian Fars News Agency, claims that it managed to penetrate the Israeli Civil Aviation Authority control systems, and was able to remain undetected within the system for months. In addition, the group claimed that it had succeeded in stealing sensitive information, and could, had it chosen to do so, take over the Authority's navigation and communications systems causing an air disaster.[45] ICRG also proclaimed that it had succeeded in penetrating the IDF computer servers, stealing secret information, such as the personal files of IDF soldiers, lists of officers, passwords, residential addresses and e-mail addresses, and military codes. Aside from the attacks against Israel, ICRG announced that it had managed to break into the Saudi Arabian army database and the computers of companies owned by the Bin Laden family.[46] At the same time, sources in Israel stated that the rumored attacks boasted by the group were false, and were no more than propaganda and psychological warfare on the part of Iran.

In the midst of these events is the mysterious death of Revolutionary Guardsman Mojtaba Ahmadi, found dead in early October 2013. Reports in the West indicated that he had served as commander of the Revolutionary Guards' Cyber War Headquarters. His death was attributed to Israel at first, but the Revolutionary Guards strongly denied this allegation, stating that his death had resulted from a "strange accident."[47] Despite the great obfuscation surrounding this event, the possibility that Ahmadi's death had consequences for the organization's activity in the cyber sphere cannot be ruled out.

The Cyber Warfare Agents

Along with Iran's government cyber apparatus and its cooperation with the hacker community, Iran is redoubling its attempts to expand and strengthen its allies' cyber capabilities. It appears that Iran is seeking to create an effective system of agents acting in cyberspace on its behalf. One of its main foci in this area is Syria, which has strategic importance for Iran. At the beginning of the conflict between the Assad regime and the rebel forces, the Iranians began to finance, equip, and train the Syrian security forces in methods of monitoring and controlling cyberspace, used by the rebels as a an important platform for organizing activity against the regime. Iranian advisers and specialists trained and reinforced the Syrian cyber police, and helped conduct surveillance of the computer and cellular networks in the country, thereby damaging the rebel's ability to transmit messages and information, both within and outside the country.[48]

A key player in this context is the Syrian Electronic Army (SEA). This group of Assad-supporting hackers began operating in 2011. During its first year of activity, it conducted mainly relatively amateurish vandalizing attacks against low-security websites that did not require significant technical ability: spam attacks, flooding talkback systems of various forums and news websites, etc.[49] In 2012, SEA began executing more complex operations against websites with a higher level of security, requiring greater technical knowledge and capabilities. Western cyber experts and administration officials attribute this major improvement to the involvement and instruction of Iranian cyber warfare experts, training and equipping SEA's operatives. Former CIA Director and NSA Director Michael Hayden also stated that the Syrian group of hackers was for all intents and purposes, an agent of Iran.[50]

The development of SEA was reflected over the past year in a wave of attacks against communications agencies and human rights organizations' websites, perceived as hostile to the Assad regime. Among other things, SEA members attacked leading news websites, including the *New York Times*, BBC, al-Jazeera, the *Washington Post*, and the *Huffington Post*. The organization also attacked the Human Rights Watch website, which provides information about the number of civilians killed in battles in Syria. In addition, members of the organization succeeded in causing substantial damage when they took over the AP news agency's Twitter account, and published a false report about a supposed attack on the White House that injured President Obama. The report generated immediate panic on Wall Street, causing a nosedive in share prices and damage estimated at $136 billion. In April 2013, SEA assumed responsibility for crashing the Twitter Social Network, and for channeling surfers from the US Marines' recruitment website to a propaganda website against the rebels.[51]

Recently, it appeared that SEA had exhibited another major advance in its capabilities, and was beginning to use more sophisticated techniques and tools, such as phishing, malware, and Trojan Horses. Such tools have enabled the organization to carry out high-quality attacks against Internet communications companies' servers, such as TrueCaller which is the world's largest telephone index; the messaging and video service company Tango, and the communications applications company Viber. In the course of these attacks, the attackers succeeded in stealing huge quantities of information, such as personal information and e-mail addresses, which may very well have been handed over to Syrian intelligence and used to target the regime's opponents as well as for espionage.[52] The Iranian Fars News Agency also reported that the organization had attacked the water system of the city of Haifa,[53] but pictures attached to the report showed that SEA had merely penetrated the irrigation control system of a community in northern Israel.[54] Nevertheless, the attack on and penetration of the control system of Israeli infrastructure indicates an attempt by SEA to utilize and target more advanced cyber warfare methods.

These advanced capabilities, which many experts regard as the result of Iranian training, guidance, and assistance, have turned SEA into significant actor in the cyberspace arena, and have made cyber warfare in general a crucial element in Syria's deterrence strategy. When Syria sought to deter an American attack in response to the use of chemical weapons by Assad's forces, SEA operatives sent a message to the Reuters news agency saying that in the event of an American attack in Syria, the organization would escalate its attacks, and take action against more significant targets. Richard Clarke, Former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism and Special Advisor to the President on Cyber Security said that if the US attacks Syria, every response by Syrian agencies in cyberspace would be facilitated by Iranian groups.[55]

In addition to its support of the Assad regime's cyber capabilities, Iran continues its traditional support for its satellite and closest ally, Hizbollah's cyber deployment, which has become an active player in attacking Israel.[56] A report by the Meir Amit Center indicates intensive involvement and support by Iran for the Hizbollah's array of websites. These sites constitute a platform for propaganda and indoctrination in the ideas of the Islamic Revolution, including pro-Iranian propaganda, the glorification of Supreme Leader Khamenei and Hizbollah leader Hassan Nasrallah, and anti-Israel and anti-Semitic propaganda. The content of these websites was determined in cooperation with Iran, subject to the Iranian propaganda strategy. Part of the content is even operated from Iranian territory by parties close to the regime.[57]

Concluding Insights

Iran's cyber warfare capabilities are continuously progressing. Iran already constitutes a significant factor whose intentions should not be held lightly. It can be stated that the Iranian decision to operate in cyberspace on a large scale is due to two main considerations; the first is its experience as the target of serious cyber-attacks. As a country that had experienced the power and capabilities of a cybernetic attack, Iran recognizes the importance of establishing defensive capabilities and building and using attack capabilities. Iran's other motive concerns global technological development, allowing the expansion of its range of actions into cyberspace, in addition to the physical world. This development optimally fits in with Iran's asymmetric strategy concept.

An analysis of the cyber-attacks attributed to Iran and its satellites shows a broad range of targets, goals, and methods. One of the conclusions arising from this article is that Iran's cyber capabilities have recently matured on both offensive and defensive levels. Although it is likely that these capabilities are still inferior to those of the leading technological powers, it appears that the Iranians are bridging the gaps quickly and effectively.

One of the most dangerous trends in Iran's offensive cyber activity is its ability to target organizations and countries' core operational systems. These systems, controlling and overseeing manufacturing processes, supplies and essential services, are liable to be targets of Iranian attacks. Exploratory, scanning and learning actions discovered in the American energy companies' computer systems and traced to Iranian groups can be interpreted in only one way: Iran is trying to attain the capability and accessibility needed for an attack on critical infrastructure. This accessibility may avoid detection altogether, and can be utilized in the future for offensive purposes if Iran so decides. A successful attack on the energy, gas, and water facilities' control systems is liable to cause substantial damage. In the framework of the rules of the game, espionage and information theft in cyberspace is seemingly tolerable, but attempts to penetrate civilian infrastructure control systems cannot and should not be accepted. These attempts require a decisive response.

It appears that the realization that Iran poses a significant threat to its enemies in cyberspace is already inspiring close cooperation between the countries threatened by these capabilities. Upgrading intelligence and producing better defensive capabilities are not enough, however; they will never suffice against a determined enemy with operational, intelligence, and technological capabilities. Cyberspace makes possible a range of channels through which one can transmit messages below the threshold of physical warfare. These actions will require demonstration of the damage that Iran may suffer should it continue to act without restraint against sensitive targets. Particular information was recently published regarding a large-scale cyber offensive operation in Syria prepared by NSA in the spring of 2011, immediately following the outbreak of the Syrian civil war.[58] If this report is correct, the preparation of a cybernetic strike against Iran, combined with the occasional demonstration of qualitative capabilities, can help restrain its actions in the area of critical infrastructure.

Until a magic technological formula is found for identifying the source of cyberspace attacks at a level of certainty that can be legally proven, circumstantial evidence of the source of the attack can suffice in quite a few cases, and strong action in cyberspace below the physical warfare threshold can be taken against this source.

Above all, closer cooperation between the democratic countries is a cornerstone in facing Iran and its satellites. Better operational, intelligence, and technological connections are essential, as well as improvement in information sharing regarding the methods and tools used by Iran and its satellites. In addition, Israel is also likely to find allies against Iranian cyber warfare among the Sunni regimes in the Persian Gulf, headed by Saudi Arabia, which is under continual threat, and which has been damaged in the past by Iranian agencies. The cyber defense realm, in which Israel is a leader, is likely to serve as a basis for a fruitful strategic dialogue on broader regional issues, such as the Iranian threat in its general sense, the crisis in Syria, and the Palestinian issue.

The Iranian cyber deployment's aggressive behavior highlights the totalitarian character of the Iranian regime. Tight and intrusive supervision that violates the freedom of speech and expression of Iranian citizens, combined with the violence and aggression typical of agencies such as the Cyber Police, refute the image that the Rouhani regime is seeking to promote in order to break the international sanctions regime against Iran. Israel and other countries can use Iran's activities in cyberspace as an explanatory platform for highlighting the totalitarian and aggressive nature of the Islamic Republic.

This reality of Iran's rapid cyber warfare capabilities' development, its satellites, and its allies require Israel and other Western countries to act methodically and with determination to maintain their qualitative and operational edge in cyberspace. The importance of this space for Israel's security concept and the urgency of creating a "digital Iron Dome" were strongly emphasized by IDF Chief of Staff Lt. General Benny Gantz, who said he believed that Israel needed to do a lot more in the cyber realm: "We must not wait with this story."[59]

Notes

[1] Barbara Slavin and Jason Healey, "Iran: How a Third Tier Cyber Power Can Still Threaten the United States," The Atlantic Council, 2013, http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf.

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

[3] Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (2012): 77-99.

[4] Ibid.

[5] Majid Rafizadeh, "Iran's 'Halal' Version of the Internet," *al-Arabiya News*, July 12, 2013, http://english.alarabiya.net/view-renderer?mgnlUuid=cb92c5e3-f973-45ce-8d46-12b8fb4dfe17.

[6] Sara Reardon, "First Evidence for Iran's Parallel Halal Internet," *New Scientist*, October 10, 2012, http://www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html#.UnZubT4UHVI.

[7] Saeed Kamali Dehghan, "Iran Launches 'National Email Service,'" *The Guardian*, July 9, 2013, http://www.theguardian.com/world/2013/jul/09/iran-launches-national-email-service.

[8] "Iran launches Own 'YouTube' Website," *AFP*, December 9, 2012, http://en-maktoob.news.yahoo.com/iran-launches-own-youtube-website-121634740.html.

[9] F. Karimov, "Iran Introduces Domestically-Made Antivirus Padvish," *Trend News Agency*, June 30, 2013, http://en.trend.az/capital/it/2166121.html.

[10] This blocking was accomplished, among other ways, by deliberately distributing malware disguised as filtering evasion software, which enabled the regime to trace illegal networks.

[11] Urt Hopkins, "Why Iranians might Actually Use the Censored Halal Internet, " *The Daily Dot*, April 25, 2013, http://www.dailydot.com/society/iran-halal-private-internet-blocked-censorship; "Iranian Internet Infrastructure and Policy Report," *Small Media*, February-March 2013, http://smallmedia.org.uk/InfoFlowReportMARCH.pdf.

[12] "Iran Unveils 12 Cyber Products," *Fars News*, December 14, 2013, http://english.farsnews.com/newstext.aspx?nn=13920923001322.

[13] "Iran Launches Home-Made Defence Shield," *ISNA*, December 9, 2013, http://isna.ir/en/news/92091812343/Iran-launches-home-made-defense-shield.

[14] Alastair Stevenson, "Iran and North Korea Sign Technology Treaty to Combat Hostile Malware," V3, September 3, 2012, http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware#.

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

16 "Iran for the First Time Stages Cyber Warfare Drill," *al-Arabiya*, December 31, 2012, http://www.alarabiya.net/articles/2012/12/31/257960.html.

17 "Drones, Cyber-Defence Feature in Iran Guards Drill," *Jerusalem Post*, February 23, 2013, http://www.jpost.com/Iranian-Threat/News/Drones-cyber-defense-feature-in-Iran-Guards-drill.

18 N. Umid, "Iran Holds Defence Exercises," *Trend News Agency*, October 22, 2013, http://en.trend.az/news/politics/2203465.html; "Iran Carries out Drills to Detect Cyber Vulnerabilities," *Tasnim News Agency*, October 22, 2013, http://www.tasnimnews.com/english/Home/Single/172473.

19 "Iranian Blogger who Told Supreme Leader Khamenei 'Your Judicial System… is nothing but a Slaughterhouse' Tortured to Death in Prison," *MEMRI*, November 19, 2012, http://www.memri.org/report/en/0/0/0/0/0/0/6819.htm.

20 European Parliament, *Resolution of November 22, 2012 on the Human Rights Situation in Iran, Particularly Mass Executions and the Recent Death of the Blogger Sattar Beheshti*, November 22, 2012, http://www.europarl.europa.eu/document/activities/cont/201301/20130109ATT58696/20130109ATT58696EN.pdf.

21 Thomas Erdbrink, "Head of Tehran's Cybercrimes Unit is Fired over Death of Blogger," *The New York Times*, December 1, 2012, http://www.nytimes.com/2012/12/02/world/middleeast/after-death-of-sattar-beheshti-iranian-blogger-head-of-tehrans-cybercrimes-unit-is-fired.html.

22 "Intelligence Ministry Admits Arresting News Providers, Blames Foreign Media," *Reporters Without Borders*, February 20, 2013, http://en.rsf.org/iran-intelligence-ministry-admits-20-02-2013,44099.html ; "Iran: Two Arrested for 'Insulting Regime Officials' on their Facebook Page, "*National Council of Resistance of Iran*, July 10, 2013, http://www.ncr-iran.org/en/news/human-rights/14138-iran-two-arrested-for-insulting-regime-officials-on-their-facebook-pa.

23 "Tehran Closes Dozens of Internet Cafes," *Mohabat News*, July 27, 2013, http://www.mohabatnews.com/index.php?option=com_content&view=article&id=7222:tehran-closes-dozens-of-internet-cafes&catid=35:inside-iran&Itemid=278.

24 Eric Grosse, "Iranian Phishing on the Rise as Elections Approach," *Google Blog*, June 12, 2013, http://googleonlinesecurity.blogspot.co.il/2013/06/iranian-phishing-on-rise-as-elections.html.

25 Siboni and Kronenfeld, "Iran and Cyberspace Warfare."

26 Betsy Isaacson, "Iran's Pre-Election Phishing Scheme Detected, Disrupted by Google," *Huffington Post*, June 13, 2013, http://www.huffingtonpost.com/2013/06/13/iran-phishing-google_n_3435811.html.

27 "Iranian Authorities Target Internet, Media before Elections," *CPJ*, June 13, 2013, http://www.cpj.org/2013/06/iranian-authorities-target-internet-media-

before-e.php; Helle Dale, "Iran Clamps down on Dissidents before Election," *The Foundry*, June 12, 2013, http://blog.heritage.org/2013/06/12/iran-clamps-down-on-dissidents-before-election.

28 Neal Ungerleider, "Iran's 'Halal Internet' is really a 'Filternet,'" *Fast Company*, 2013, http://www.fastcompany.com/3009714/irans-halal-internet-is-really-a-filternet.

29 Thom Shanker & David E. Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers," *New York Times*, June 8, 2013, http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?nl=todaysheadlines&emc=edit_th_20130609&_r=4&pagewanted=all&.

30 Siboni and Kronenfeld, "Iran and Cyberspace Warfare."

31 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 Cybersecurity, Infrastructure, Protection and Security Technologies*, April 26, 2012, p. 5.

32 "Brazilian Military Police & 26 Govt Websites Hacked by Ashiyane Digital Security Team," *Hackread*, January 28, 2013, http://hackread.com/brazilian-military-police-26-govt-websites-hacked-by-ashiyane-digital-security-team.

33 Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers ," *The Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB1000142405270230452620457910160235675177 2; Adam Kredo, Mike Rogers, "China, Iran and Russia Launching Cyber Attacks Against U.S. ," *The Washington Free Beacon*, July 22, 2013, http://freebeacon.com/mike-rogers-china-iran-and-russia-launching-cyber-attacks-against-u-s.

34 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers."

35 Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=1&ref=iran&&version=meter+at+6&region=FixedCenter&pgtype=Article&priority=true&module=RegiWall-Regi&action=click.

36 Ibid.

37 Julian E. Barnes and Siobhan Gorman, "Iran Blamed for Cyberattacks," *The Wall Street Journal*, September 27, 2013, http://news.walla.co.il/?w=/15/2569449, "Iran Launches Powerful Cyber Attack against Banks in US," Walla!, January 9, 2013, http://news.walla.co.il/?w=//2605254.

38 Ellen Nakashima, "U.S. Warns Industry of Heightened Risk of Cyber Attack," *The Washington Post*, May 10, 2013, http://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html; see also an analysis of the capabilities required to carry out a high level

cyber-attack: Gabi Siboni, Daniel Cohen, and Aviv Rotbart, “The Threat of Terrorist Organizations in Cyberspace,” *Military and Strategic Affairs*, Volume 5, No. 3, Institute for National Security Studies, December 2013, http://d26e8pvoto2x3r.cloudfront.net/uploadImages/systemFiles/The%20Threat%20of%20Terrorist%20Organizations%20in%20Cyberspace.pdf; Nicole Perlroth and David E. Sanger, “New Computer Attacks Traced to Iran, Officials Say,” *The New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html?_r=1&.

[39] This article was written as nuclear negotiations were taking place between Iran and the great powers. One cannot rule out the possibility of escalating energy sanctions should the negotiations fail.

[40] Siobhan Gorman and Danny Yadron, “Iran Hacks Energy Firms, U.S. Says,” *The Wall Street Journal*, May 23, 2013, http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968.

[41] Chris Strohm, “Iran-Based Hackers Traced to Cyber Attack on U.S. Company,” *Bloomberg News*, May 14, 2013, http://www.businessweek.com/news/2013-05-14/iran-based-hackers-traced-to-cyber-attack-on-company-inside-u-dot-s-dot.

[42] Shanker and Sanger, “U.S. Helps Allies Trying to Battle Iranian Hackers.”

[43] Barnes and Gorman, “U.S. Says Iran Hacked Navy Computers.”

[44] Gili Cohen, “Netanyahu Confirms: U.S. is Working with Israel on Cyber Defence, Iranian Attacks Increasing,” *Ha’aretz*, June 9, 2013, http://www.haaretz.com/news/diplomacy-defense/.premium-1.528728.

[45] “Israel’s Aviation Agency under Muslim Hackers’ Control for Months,” *Fars News*, January 8, 2013, http://english.farsnews.com/newstext.aspx?nn=13921018001457.

[46] “Saudi Army, Al-Qaeda Company, Israeli Army Hacked in Revenge for Assassination of Hezbollah Leader,” *Fars News*, December 16, 2013, http://english.farsnews.com/newstext.aspx?nn=13920925001699.

[47] Damien McElroy and Ahmad Vahdat, “Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination,” *The Telegraph*, October 2, 2013, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html; Lisa Daftari, “Internal Plot, not Israel, Eyed in Latest Hit on Iranian Scientist,” *Fox News*, October 8, 2013, http://www.foxnews.com/world/2013/10/08/internal-intrigue-not-israel-eyed-in-latest-hit-on-iranian-scientist.

[48] Simon Tisdall, “Iran Helping Syrian Regime Crack Down on Protesters, Say Diplomats,” *The Guardian*, May 9, 2011, http://www.theguardian.com/world/2011/may/08/iran-helping-syrian-regime-protesters; Lisa Daftari, “Iranian General Admits ‘Fighting Every Aspect of a War’ in Defending Syria’s Assad,” *Fox News*, August 28, 2012, http://www.foxnews.com/world/2012/08/28/iranian-general-admits-fighting-every-aspect-war-in-

defending-syria-assad; Geneive Abdo, “How Iran Keeps Assad in Power in Syria, “*Foreign Affairs*, August 25, 2011, http://www.foreignaffairs.com/articles/68230/geneive-abdo/how-iran-keeps-assad-in-power-in-syria.

49 Ronald Deibert, “Waging the Cyber War in Syria,” *National Post*, May 21, 2013, http://fullcomment.nationalpost.com/2013/05/21/ronald-deibert-waging-the-cyber-war-in-syria.

50 Joseph Menn, “Syria, Aided by Iran, Could Strike Back at U.S. in Cyberspace,” *Reuters*, August 29, 2013, www.reuters.com/article/2013/08/29/us-syria-crisis-cyberspace-analysis-idUSBRE97S04Z20130829.

51 Sarah Hurtubise, “Syrian Hacker Army Could be Advancing with Iranian Help,” *The Daily Caller*, April 9, 2013, http://dailycaller.com/2013/09/04/syrian-hacker-army-could-be-advancing-with-iranian-help; Andrea Peterson, “The Post Just Got Hacked by the Syrian Electronic Army. Here’s who they are,” *The Washington Post*, August 15, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are.

52 Kenneth Geers and Ayed Alqartah, “Syrian Electronic Army Hacks Major Communications Websites,” *FireEye*, July 30, 2013, http://www.fireeye.com/blog/technical/cyber-exploits/2013/07/syrian-electronic-army-hacks-major-communications-websites.html.

53 “Syrian Electronic Army Reveals Documents of Haifa Hack,” *Fars News*, June 15, 2013, http://english2.farsnews.com/newstext.php?nn=9203180050.

54 Elad Salomons, “Did the Syrian Electronic Army Attack Haifa’s Water Supply SCADA System?” *Water Simulation*, June 5, 2013, http://www.water-simulation.com/wsp/2013/06/05/did-the-syrian-electronic-army-attack-haifas-water-supply-scada-system.

55 Menn, “Syria, Aided by Iran, could Strike back at U.S. in Cyberspace.”

56 Olivia Goldhill and Reuters, “Benjamin Netanyahu: Iranian Cyber Attacks on Israel ‘Non-Stop,’” *The Telegraph*, June 10, 2013, http://www.telegraph.co.uk/technology/10110381/Benjamin-Netanyahu-Iranian-cyber-attacks-on-Israel-non-stop.html.

57 “Terrorism in Cyberspace: Hezbollah’s Internet Network,” *The Meir Amit Intelligence and Terrorism Information Center*, March 4th, 2013, http://www.terrorism-info.org.il/en/article/20488.

58 David E. Sanger, “Syria War Stirs New U.S. Debate on Cyberattacks,” *The New York Times*, February 24, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?hp&_r=2.

59 Amos Harel and Gili Cohen, “2014: Iran out, Global Jihad in,” *Haaretz*, February 1, 2014, http://d26e8pvoto2x3r.cloudfront.net/uploadimages/systemfiles/iran%20out,%20global%20jihad%20in.pdf.