Structure of Iran's Cyber Warfare

"Source: the BBC Persian"

A complex and multi-layered structure is in charge of cyber operations in the Islamic Republic of Iran. This structure is tasked to confront the enemies and critics of the Islamic regime on the Internet and has different units to pursue this goal.

Hereafter we will have a look the various elements of this structure and the responsibilities of each.

High Council of Cyberspace

In Iran, the highest government body that deals with the cyberspace is a newly-established organization named the High Council of Cyberspace (Shoray-e Aali-e Fazaye Majazi). In March of 2012 this new structure was set up on the orders of Ayatollah Khamenei with the mission of instituting high-level policies on the cyberspace. After the foundation of the High Council of Cyberspace, all other Iranian organizations in charge of cyber operations are committed to implement the policies instituted by this new government body.

This council comprises the highest-level Iranian authorities such as the president, the heads of the judicial power and the parliament, the head of the state-run radio-television, the commander-in-chiefs of the IRGC [1] and the police, the ministers of Intelligence, Telecommunication, Culture, Science, etc.

Cyber Defense Command

Since November 2010 an organization called "The Cyber Defense Command" (Gharargah-e Defa-e Saiberi) has been operating in Iran under the supervision of the country's Passive Civil Defense Organization (Sazeman-e Padafand-e Gheyr-e Amel) which is itself a subdivision of the Joint Staff of the Armed Forces (Setad-e Kol-e Niruhay-e Mosalah).

The Passive Civil Defense Organization which began its work in 2003 on orders of Ayatollah Khamenei, is responsible for the "Permanent Committee of Passive Civil Defense" on which sit representatives from the armed forces, and various government ministries and organizations. The secretariat of this permanent committee until August 2011 was in the Presidency compound after which it was transferred to the High Command of the Armed Forces, as agreed by Ali Khamenei and Mahmoud Ahmadinejad. The secretariat of the committee is charged with coordinating numerous government organizations and agencies to non-militarily respond to a military attack on the country with the goal of minimizing damage to the country's infrastructure and facilities in the event of a probable war.

[1] The Islamic Revolution Guards Corps.

The head of Passive Civil Defense Organization, who is also the head of the permanent passive civil defense committee, is General Gholam-Reza Jalali who was appointed to this position by Hassan Firouzabadi, the head of the High Command of the Armed Forces. According to Jalali, the Cyber Defense Command is responsible for providing security to the country and its infrastructure against cyber threats. From the way officials have defined this command, its work is "defense" against cyber attacks. It appears that at least in the beginning of its formation, the task of the command was indeed confined to defense (and not attack) and till today it has not (unlike the "Cyber Army") conducted attacks against internet activists and sites. But despite this, it is not unlikely that in future this group may engage in cyber attack operations of its own. In addition to the Passive Civil Defense Organization, the Cyber Defense Command also has other members such as the ministries of Telecommunications, Defense, Intelligence, and Industries.

The idea of creating a cyber defense command was launched by some officials of the Passive Civil Defense Organization some time ago but they only managed to convince senior authorities of the regime to approve the creation of such an organization after some Iranian nuclear sites came under attack of the Stuxnet computer malware.

Iran's Cyber Army

Iran's Cyber Army is a group comprising highly skilled specialists in information technology and professional hackers who avoid revealing their identity. This group is not officially registered and till today no agency or government organization has assumed responsibility for it. Still, incontestable evidence suggests that the group is affiliated with the IRGC.

The technical capabilities of Iran's Cyber Army are such that it has till now managed to hack a lot of foreign-based media outlets as well as Twitter and some government sites in the West.

In December 2011 Eric Schmidt, the executive chairman of Google commented in an interview with CNN on Iran's activities on the cyberspace and said that the Iranians had succeeded in taking over the information traffic on the Internet through intelligent hacking. According to him, Iranian hackers had succeeded in diverting the flow of information in Denmark towards Iran and then return it back to Denmark. He concluded that, "Iranians are unusually talented in cyber war for some reason we don't fully understand."

In September 2011, it was revealed that Iranians had hacked into 500 Internet security certificates to hit some 300,000 Iranian internet users. The Dutch government said that attackers hacked into DigiNotar, a Dutch Web security firm. The Dutch Justice Ministry published a list of the users of fake certificates that were sent to sites operated by Yahoo, Facebook, Microsoft, Skype, AOL, the Tor Project, WordPress, and by intelligence agencies like Israel's Mossad and Britain's MI6.

The Iranian hackers left behind a Persian signature embedded in the hacking code, similar to the one found in March 2011 against the Comodo, the United States security firm that was hacked by Iranian individuals too. The signature was: "Janam Faday-e rahbar", which means: "I sacrifice my life for the Leader [Ayatollah Khamenei]."

In May 2009, Defense Tech, an American company which deals with the Internet security, named Iran among five countries with the most powerful cyber capabilities in the world. This

is despite the fact that the capabilities of the Cyber Army after the 2009 elections are greater and its operations more complex than the pre-election days.

The IRGC has not yet officially assumed responsibility for Iran's Cyber Army. Yet, some IRGC authorities have made references to the activities of the Cyber Army and its connections to this military force. For example, in April 2011 Mojtaba Zolnoor, the former deputy representative of the Supreme Leader in the IRGC said that by using the "Cyber Army" Iran had succeeded to hack "enemy sites." Just a few weeks prior to that, Yadollah Javani, the former head of IRGC's political office, said that this military force possessed the world's fifth largest Cyber Army. Last November, Hossein Hamedani, the former IRGC commander of the province of Tehran claimed that there were "two cyber war centers" in Tehran under the IRGC. Even Mohammad Ali Jaafari, the commander-in-chief of the IRGC in March 2012 announced that this force had struck devastating blows to Internet networks of regime opponents by recognizing and then confronting them.

Basij Paramilitary Force

In addition to Iran's Cyber Army and the Cyber Defense Command there are other - less professional - units in the institutions of the Iranian regime for Internet operations.

One such institution is the Basij which has made large investments for such operations. It should be mentioned that after its reorganization in 2007, the armed units of the Basij have now become members of the ground forces of the IRGC while its non-military units - which constitute the majority of the Basij units - have the responsibility for "soft war" and are particularly in charge of cyber war with enemies of the Iranian regime.

Of course since the majority of Basij members are non-expert individuals (and mostly belong to the lower social classes) the most important cyber activities that already have taken place in this paramilitary force are to provide computer, Internet and blog writing skills among the members. As part of this project, tens of thousands of Basijis have been provided free classes and thousands of web blogs have been created for them to work at. The key expectation that Basij officials have from these trained Basijis is to write material in support of the regime and the leader of the Islamic Republic on their own blogs and write up comments on the interactive spaces of other sites. In this light, Basijis post countless comments on numerous sites - including sites that are critical of the regime - and social networks whose content is the same: defending the regime and attacking the regime critics.

But aside these general activities, a Basij "Cyber Council" has been created too in the organization among whose tasks is to utilize hackers under the supervision of IRGC specialists. Hossein Hamedani, the former IRGC commander of Tehran province has recently spoken of having trained 1500 "cyber war commandoes" in the Basij Cyber Council in a report on the activities of the council.

It appears that despite the extensive planning of the Basij and the IRGC to expand the activities of the Cyber Council, this body is still made up of mostly inexperienced individuals who engage in less complex hacking or infiltration operations on sites and emails, while the more sophisticated operations rest with the Iran Cyber Army of the IRGC.

The Police

The Iranian police too, have been paying growing attention to Internet operations. While this force has generally been involved in this for years, but its engagement has increased significantly and more organizationally since the 2009 presidential election.

In September 2009, Ismail Ahmadi-Moghadam, the chief police commander announced the creation of the Cyber Police. This special police unit was named "FETA Police" in January of 2011 (which stands in Persian for "the Police of the Space of Creating and Exchanging Information"). FETA police's main task is to confront Internet crimes. One responsibility of FETA Police is similar to what is done with Internet crimes in other countries and includes combating fraud, personal information theft, threats, etc.

But this police unit also has the responsibility to combat so-called "political and security crimes" as well, which is in fact its principal activity. In November 2011 an official of Tehran police announced that this force was going to use a group of hackers to battle Internet crimes. He described the duties of these hackers to provide assistance to the police to better understand the technical weaknesses of government sites and ways to remove these. But the duties of these police hackers do not remain limited to these spheres and they have responsibilities to infiltrate "distasteful" sites and "criminal" email accounts (i.e., regular crimes, in addition to political and security crimes) as well. Still, the police units that engage in infiltrating sites and email accounts of regime opponents are apparently much smaller in scale than similar units of the Cyber Army in the IRGC.

In fact the most important activity of the police on the cyberspace is "controlling" Internet users. One way they do this is to apply pressure on Internet Service Providers and force them to provide information on Internet users.

Another important activity of the police – which is growing – is to control cyber cafés. Owners of cyber cafés in Iran are under pressure from the police to pass them information on Internet users. In this light, FETA police recently issued a directive ordering cyber café owners to accept only those Internet users who provide them personal identity information – preferably the national ID cards.

According to this directive, in the cyber cafés, no more than one person should use the Internet on the same PC at the same time. Furthermore, closed circuit TVs will be installed on all Internet cafés and all such places must have the capability to video record 24 x 7 and keep the videos for six months. In addition, cyber cafés must also record other information of their Internet users and keep the users' IP addresses, their log files, the days and hours of Internet usage, the list of websites visited by users, the specific pages that were visited by them, etc.

Committee to Identify Unauthorized Sites

Iranian government's plans to filter the Internet sites intensified after the formation of a committee named "The Committee to Identify Unauthorized Internet Sites" in July 2009. The responsibility of this body is to identify websites whose operations were not approved by the regime for different reasons.

This committee is formed by the Supreme Council on the Cultural Revolution which is under the control of Iran's Supreme Leader. This committee comprises of the members such as the Attorney General, the commander-in-chief of the Police, the head of the state-run radio-television, the ministers of Culture, Intelligence, Telecommunications, Science, etc. A lot of websites have already been blocked from user access based on the ruling of this committee.

To have a better understanding of the level of the intervention of The Committee to Identify Unauthorized Internet Sites in the activities of Iranian websites, it is worth mentioning that recently, even the official website of Akbar Hashemi Rafsanjani was filtered (for a few days) by this committee, to put pressure on Rafsanjani to omit some of his personal memories that were published in the website.

National Internet Project

A number of Iranian officials have in recent months spoken of efforts by the regime to launch a "National Internet." The Iranian government's official website has announced one of this project's aims to be to provide "security" on the Internet, protection against Internet attacks and "battle the US in the soft war".

In this regard, Reza Taghipour, the minister of Telecommunications and Information Technology has said that the regular Internet shall continue to exist side by side with the National Internet but the latter shall have a much higher speed (the normal Internet is extremely slow in Iran). Some other officials however have said that once the national Internet project is launched and operational, the regular Internet will be shut denying access to it from Iran.

Another measure to be undertaken by the Iranian regime to control the cyberspace is launching of a "National Internet Search Engine". Iranian officials have talked about replacing global search engines such as Google or Yahoo by this new search engine. According to Iranian officials the name of the national search engine will be "Ya Hagh," (an expression meaning: Oh God!).

The minister of Telecommunications has stressed that after the national search engine is launched, all data centers and hosting shall take place inside Iran (many of these hosting sites are currently in the US).

Soon after these remarks, Ismail Ahmadi-Moghadam, the police chief declared that "Our computer information centers should not be outside the country," and added that "Google was not a search engine but a spying tool."

In another statement in this regard, in February of 2012 Iran's minister of Intelligence Heidar Moslehi said that the Internet and social media had played a key role in the post-2009 presidential elections and added that this experience demonstrated that "new threats required new means of dealing with them." Mr. Moslehi also accused Internet providers around the world of espionage and said Western intelligence agencies used the Internet to provide its users with information that they wanted to pass on to them.

In view of the measures that the Iranian regime has been carrying out regarding the cyberspace, it appears that it intends to make it impossible, in the not-too distant future, for the people of Iran, particularly its youth, to interact with the world through cyberspace.

A group of experts however believe that the cyberspace plans of the regime e (such as "the National Internet") are not easy to implement and that many statements that Iranian authorities make in this regard are exaggerations. At the same time, there are many other experts who have a completely different view and warn that the measures of the Iranian regime regarding the Internet should not be underestimated.

They say that the progress that the regime has made since the 2009 elections in preventing Iranians from accessing the free world through the Internet, show that the continuation of this progress can significantly restrict access levels of Iranians to information to unprecedented levels.

The defenders of free exchange of information warn that if the Iranian regime succeed in its plans for the cyberspace, not only will the level of access of Iranians with the world diminish significantly, the volume of information that the international community will have of developments in Iran (ranging from human rights violations to the regime's political and security activities) will also be greatly reduced. Should something like this happen, the regime in Tehran will have less fears that its human rights violations and breaches of international obligations will be exposed and as a consequence will continue to crackdown on human rights activists, and social and political critics with greater comfort. At the same time, Iranian victims of human rights violations, dissidents and activists will drastically lose their options in disseminating the developments in the country to the outside world.

Ultimately, in view of these realities, it is not an exaggeration to say that the future of the pro-democracy and human rights movement in Iran will suffer proportionately as the Iranian regime makes headway in implementing its anti-Internet projects. Projects which if successful, will make Iran more and more similar into a model that already exists in another part of the world: North Korea.