GlobalResearch
Center for Research on Globalization

Iran and Modern Cyber Warfare

By Vladimir Platov
Global Research, December 24, 2014

Region: Middle East & North Africa
Theme: History
In-depth Report: IRAN: THE NEXT WAR?

Today US intelligence services seem to finally have become aware of the potential damage a cyber-attack can inflict, therefore Washington is placing particular stress on enhancing its "combat capabilities" in virtual space. Therefore, not only the CIA, but the NSA and the Pentagon have started getting substantial resources on an annual basis in order to be able to create the most advanced cyber-weapons conceivable.

In 2013 alone Washington has allocated one billion dollars to the NSA and 685 million dollars for the CIA for them to carry out offensive cyber-operations and develop spyware like Flame and Duqu and malware like Stuxnet, which had previously been used against countries "that are unfriendly to the United States", specifically against Iran, Syria, North Korea, and China.

Additionally, Washington has been busy with the creation of a 5000 men strong specialized unit that goes under the name of United States Cyber Command, which is headquartered, according to Bloomberg, at Fort Meade military base in Maryland. This unit alone has been provided with a hefty 3.94 billion dollars in 2013, while in 2014 this sum increased to 4.65 billion dollars, forcing countries that are being targeted by the United States' offensive cyber-operations to increase their own defensive capabilities as well as creating similar units.

It's no coincidence then, that Iran has started developing a new cybersecurity strategy, which will make cyber-operations top priority for both the army and national intelligence agencies. According to Western analysts, should the conflict between Iran and the West turn from bad to worse, Tehran could use cyber-attacks to inflict substantial damage on critical infrastructure in the United States and its allies, including power plants and financial networks.

Additionally, the new cybersecurity strategy of Iran specifies the two critical goals that the national agencies are to achieve. First – is the creation of technological capabilities that would allow the protection of critical infrastructure and top-secret information from various forms of intrusion (including malicious viruses such as Stuxnet, which had caused a considerable amount of damage to Iran's uranium enrichment program), and opposition to anti-Iranian activities in cyberspace, since it has been been a key tool for the spread of disinformation and the organization of anti-government rallies.

To attain these goals Iran has recently created an elaborate network of educational and research institutions. In addition, the Ministry of Communications and Information Technologies has established the Iran Telecommunications Research Center which is playing a key role in advanced research in various high-tech fields, including information security. On top of this, there's been created the position of Technology Cooperation Officer in the President's office, since the control on research projects in across the field of information

technology is established at the highest level of the Iranian government. As for the emergency response to cyberattacks and other challenges there's the MAHER Information Security Center which is working under the authority of the Ministry of Communications and Information Technologies.

There is also an operation under the supervision of the High Council of Cyberspace (Shoray-e Aali-e Fazaye Majazi) which is formed by high-profile Iranian authorities, including the President. Once the High Council was created back in 2012, all other Iranian organizations and groups responsible for cyber operations were placed under this new government body. The most active part in today's Iranian cyber operations is played by Cyber Defense Command (Gharargah-e Defa-e Saiberi), established in November 2010, which operates under the supervision of the Passive Civil Defense Organization, an independent unit of the Joint Staff.

The better part of offensive cyber operations is being carried out by the Iranian cyber army, that employs highly qualified specialists in the field of information technology. One of the most active well-known units of this army is the Ashiyane Digital Security Team, which has become known for its ideological commitment to the Iranian government. The technical capabilities of Iranian cyber troops is apparent in the fact that they were able to repeatedly infiltrate Western government and intelligence networks, despite all the security measure that were taken. In December 2011, Google's CEO Eric Schmidt in an interview with CNN noted that Iranians are unusually talented in cyberwarfare, for reasons that the US fails to fully understand.

In May 2009, an American cybersecurity company Defense Tech has named Iran among the five countries with the strongest cyber capabilities in the world.

Additionally, Iran is using supplementary units that are somewhat less proficient than central Iranian cyber units, among them is Basij – Iran's paramilitary volunteer militia formed by Ayatollah Khomeini in November 1979, which according to various estimates, has more than 11 million members.

Iranian police has been paying an increasing amount of attention to cyberspace operations as well. It has been involved in them for many years, while its involvement has only grown since 2009, when the presidential elections in Iran were held. In September 2009, Iranian police commander Ismail Ahmadi-Moghadam announced the creation of the Iranian cyber police. This unit was labeled FETA, which in Persian stands for "the Police of the Space of Creating and Exchanging Information". Its chief task is to confront Internet crime (fraud, identity theft, etc.), as well as "crimes of a political nature and related to national security."

To establish its control over local cyberspace Iran has established the Committee to Identify Unauthorized Internet Sites on July 2009. The committee is composed of the Attorney General, Minister of Culture, the head of the national police, intelligence and telecommunication experts along with radio and television professionals. To date the Committee has effectively banned a number of anti-Iranian websites for local users.

In September 2012 numerous financial institutions in the United States (in particular, Bank of America, Citigroup, and others) were subjected to Iranian cyber-attacks. According to American analysts, the most destructive attack occurred in August 2012 on the computers of the Saudi Arabian oil company Aramco and the Qatari gas company RasGas. The attack

was carried out by a virus called Shamoo, which spread across all corporate servers and destroyed all data stored within. A group that goes under the name the “Cutting Sword of Justice” has assumed responsibility for this attack, by stating that it was aimed at the main source of income for Saudi Arabia. According to this group, Saudi Arabia has been committing crimes in Syria and Bahrain.

Despite a number of calls made by international leaders to end wars of all kinds, some of them were awarded with peace prizes (like Barack Obama with his Nobel Peace Prize), and these very same leaders are taking military operations to cyberspace, carrying out acts of cyber-terrorism and full-scale information warfare, involving, unfortunately, the rest of the world in a new cyber arms race.

Vladimir Platov, Middle East expert, exclusively for the online magazine “New Eastern Outlook”

Articles by: Vladimir Platov