THREATS

Although the Internet has opened the gate for threats from all over the world, the threats targeting the Arab Gulf Cooperation Council countries often come from the regional neighboring countries or from other nongovernmental parties which are associated with the regional tension and conflicts. Similar to North America, Europe and Asia, there is quite a good number of organizations in the Middle East which are able to commit destructive acts in the electronic space. Reports state that Syria, Turkey and Israel have invested huge amounts of money to develop their capabilities to launch electronic attacks. Despite lack of data about such programs, the Iranian program of space electronic war has attracted a special attention. In the light of the available data in general, this research paper has concentrated on Iranian electronic activities.

The news program "Frontline" transmitted by the American channel "PBS" reported that in 2005, the Iranian Revolutionary Guards established a division specializing in space electronic war. The said division got its staff from three pirate groups or hackers in Iran; Ashiana, Shabguard and Semorg. This electronic army heavily depends on external expertise. It established special recruitment and training companies for application of high technology. 1

In May 2010 a big officer of the Iranian Revolutionary Guards stated that "the electronic army of the Iranian Revolutionary Guards have are at present the second most powerful electronic army in the world." 2. Although the basis of this claim is vague, the American Research Company Devin's Tech believes that the Electronic Division has recently got 2400 employer in addition to 1200 internet pirates (hackers) from the private sector. It is believed that it annual budget is more than 75 million dollars. 3. So far Iran's space wars

have been tasked to attack against electronic sites just for destruction and blocking the websites of media companies that cover the news of Iranian opposition groups. On 19 December Twitter Blogging website was exposed to blockage in various areas in the world. Those who wanted to visit that website were given a message that read:

"The USA thinks that it has full control over the Internet, but it is mistaken. Thanks to our power we control the Internet. Don't try to outrage the Iranian person … which of the two parties is at risk; Iran or the USA? We are now putting them at risk, beware!"

A month later after that incident the main webpage of the Chinese Search Drive was exposed to a similar deformation of its website with a phrase that meant "The Iranian Electronic Army was set up to obstruct the interference of foreign and Zionist websites into the internal affairs of our country. They are publishing incorrect and misleading news." It was unclear why the Chinese Search Drive was hacked this way, however the answer came soon from the Chinese hackers. The Chinese Association of Electronic Hackers - a group of hackers who targeted American websites before – took revenge on a set of Iranian websites chosen at random which were attacked in retaliation. The group of hackers published messages on that website in retaliation against the messages published on the Chinese Search Drive.

The deformation of electronic websites is usually made by amateur users; and it is more a sort of juvenile play or destruction than being a sort of professional war. It is wrong to believe that such patterns of attack unveil all the capabilities of the Iranian régime. The open and public statements available show that Iran recognizes that it is the

target of more sophisticated and more complicated equipments and with more professional techniques. Consequently Iran spares no effort to develop certain technologies to cope with such sophisticated attacks. The Iranian Minister of Defense Ahmadi Fahihdi commented openly declaring that Iran is ready to go to war into the electronic space. He was also quoted as saying "Information technology and telecommunications are currently considered to be of greater importance for all nations. We have to be ready and be prepared to protect ourselves against all sorts of electronic wars.

Defense Tech puts Iran high on the list among the most powerful nations of the world in terms of electronic attack as suggested by the list of cyber space weaponry that compromise the Iranian arsenal. It includes electromagnetic pulse weapons and wireless data jamming and interference instruments as well as Back Troy Horses, viruses and electronic worms.

In July 2009 the Israeli expert Aloun Bin David in his statement to the ABC news channel, announced that "Israel - through a campaign launched against the Iranian military networks – took to destroying and damaging data related to the Iranian nuclear research program." The ABC reported that Israel and the USA have initiated a program for destroying software and equipments bought by Iran from abroad to be utilized for its nuclear program. 9. Some Iranian officers have recently stated that some networks of eavesdropping instruments implanted in the Iranian cyber space were destroyed. They were meant to collect data about its nuclear program.10. This happened within the context of the ever mounting tension between Iran and Israel; such cyber attacks between the two countries may probably continue to be intensified.

Due to the fact that more than one hundred or more have actually developed or trying to develop their electronic offensive capabilities, it is expected the]t cyber space war will constitute an important part of future conflicts. Virtual electronic weaponry will play an important role that might be definitive in actual wars. Victory will be for the country which is able to protect its cyber space and block the enemy's cyber space and able to acquire the ability to use information technology efficiently and skillfully and develop its ability to launch campaigns on the virtual cyber space of the enemy. In this respect an electronic war is capable of changing the scale of traditional conflicts. However a more latent fatal hazard may be the electronic assaults used for criminal purposes. In spite of the strict law enforcement measures in the Gulf Countries, this has not protected them from electronic crimes.

The security specialist Trend Micro Establishment stated that throught 2009 the internet hackers were able to cripple around 800000 electronic systems in the Kingdom of Saudi Arabia. The motivation behind those offensives was financial in most cases. In the United Arab Emirates hackers were able to cripple around 250000 electronic systems. Those crimes were tracked and trailed in both countries, and it was found that most of them were launched from websites out of cyber borders of the victimized attacked countries. In the year 2008 the UAE Ministry of Education and Ministry of Labor were victimized in chase offensives that aimed mainly at collecting personal information. The hackers who launched the attacks made very similar websites to the official website www.moe.gov.ae and the other website www.mol.gov.ae under the names www.moe.gov.tk and www.mol.gov.tk and both websites are registered in the Region Tokelau, New Zealand 12.

In March 2010 Abu Dhabi Police warned people against the increasing number of virtual crimes targeting individuals in order to get the details of their bank accounts. 13. Virtual attacks on establishments operating in the Gulf Region and people residing there might have cost them milliards, a matter that might reduce the ability of the region to attract potential foreign investors and expatriates Therefore, counteracts need to made in retaliation for such offensives in order to reduce and relieve the threats caused by electronic criminal assaults and block their channels and minimize their negative consequences.

Points of Weakness

There are a fairly good number of weak points in most local networks which make them liable for virtual assault. The weakest of all points is in the engineering structure of the networks and in protocols which control communication among these networks. The research in hand concentrates mainly on the common points of weakness due to absence of the DDOS service and on assaults against the official military networks.

Service Barring Offenses

On three different occasions Russia launched assaults to bar some East European and Mid Asian countries that once were part of the Soviet Union - from DDOS service. In 2007 Estonia was exposed to service barring offensives after Estonians had removed the statue of a Soviet soldier from one of the central public squares. It was a memorial set up the Russians when the Russians occupied Estonia after the World War 2. In that incident the ‘nationalist” Russian internet hackers dumped the Estonian virtual space with millions of

instructions transmitted to Estonian electronic web pages. Offensives targeted the internet protocols of telephone and banking systems.

After one and half years when violence broke out in Russia and the Republic of Georgia, the Russian Hackers Division was set to service again. This time the electronic assaults coincided with the actual physical air and land military attacks. The Russians used the "Putt" nets to topple the government of Georgia and damage its media electronic websites. They were able to dump the electronic space of the country with choking masses of instructions that made it impossible for the other cyber packs to get into or out of the country.

Moreover, the hackers had full control over the receiving orienteer to control any leaking traffic. After six months the Russians resorted to that technique again, and the target this time was the Republic of Kirghizstan in Mid Asia. The internet was crippled for more than a week.

Offenses against Government and Military Operations

Government and military systems are exposed to daily attacks targeting espionage operations. A number of countries launch these attacks to rob weaponry systems and plans and get important useful data by robbing military plans and decoding the intelligence messages of the enemy or by incapacitating the enemy's networks and barring the enemy arms against using them in war time. Any system connected to the Internet is exposed to assault. Any system connected to any other system connected to the Internet is also exposed to offensives. Moreover, we may notice that governments and armies whose systems are dependent on such systems may be unable to function when they are in dire need of their own systems. Consequently even an army equipped with high technology and an

excelling and highly proficient military network may fade down and collapse under electronic assaults.

Attacks on Highly Sensitive Infrastructure

Though service barring attacks may look comparatively few from the technical point of view, they are destructive at the national level. We should not at all underestimate the resulting economic losses which a country might suffer from for a week of paralysis when the Internet service is blocked. Countries that have highly sophisticated technological military systems depending on the Internet technology may lose their system preparedness as a result of such assaults. Quite often the impact of these attacks is limited to the cyber space. However, due to the increasing use of the Internet remote control systems for diagnosing and adjusting systems and carrying out the other administrative functions, electronic hackers and rogues have become capable of controlling and remote controlling gas pipelines, fuel production infrastructure, chemical plants and power stations. In any of these cases hacking may cause real damage, confusion and anarchy all over the world.

The USA national Lab of Idaho conducted an experiment in 2006 that demonstrated the destruction of a generator in a service company by launching an Internet attack against the company. The generator was connected to an electronic laboratory system in a way similar to actual technique adopted by electricity companies for connecting systems. The process was carried out through a remote control by giving instructions to the generator that developed vibrations and shakes causing automatic explosion from within. It is worthy of mentioning that such types of generators need around six months to be manufactured.

Consequences

The consequences of such attack and assaults are intuitive and self evident. Due to our heavy dependence on the Internet-connected technology service barring assaults targeting any national network, may paralyze a whole country within a few days. Nevertheless, the consequences of such offense might continue for a longer time. In the next decade, the virtual space will be the battlefield where nation will either be losing or gaining their sovereignty. Countries that cannot secure full control over their Internet websites will not be able to attract investors or become good havens for businesses or even become a safe home to live in.

The economy of the Gulf Region basically depends on oil and gas extraction and treatment. Electric generators which usually depend on petroleum and gas are considered essential for the continuity of oil extraction and treatment of hydrocarbons. Furthermore, living in this part of the world heavily depends on air conditioning in the long hot season and arid climate. Should air conditioners become out of order life in this region will be under threat. Water desalination stations also depend on the electric power stations which are usually set up close to them. Should such infrastructure building be exposed to an electronic assault, consequences would be fatal. Finally one can safely say that electronic wars against government and military systems are able to incapacitate the government. This would make governments unable to control discipline and order. They would be unable to render civil or military facilities to defend, safeguard or protect the national territories. Costs will be too high unless all points of weakness are addressed and resolved.

Action Plans

As a result of the frequent and continued connection of our essential operations to the Internet, and due to the escalating intense of the dirty hacking activities on the website, the safety of the virtual space of many countries will continue to be a strategic issue in any decision taken by firms and institutions with regard to the places where their businesses could be started. Consequently security and safety which were regarded as mere costs that could be reduced; will be the controlling factors and the main concerns of the market. Countries which fail to shield their websites will allow electronic hackers, criminals and infiltrators to launch their attacks. This will encourage them to continue with their aggression. The matter will not be limited to this, but it will impact the national economic growth and impede its development. Hence, the AGCC countries should take a positive action to change the Gulf Region into a safe secured electronic zone. The strategic national plan of 2003 for a secured electronic space of the USA was proposed for the entire North America, but the plan was not implemented at all.

The following proposals may be the most important component of a safe and secured cyber space.

- Improvement of Domain Names System in the AGCC counties
- Concentration on national networks' safety and security
- Strengthening cooperation to overcome electronic crimes
- Drawing cooperative plans to reduce the impacts of service barring assaults
- Reinforcement of government and military infrastructure
- Protection and shielding government and military systems

Conclusion

To reduce threats and overcome areas of weakness and control consequences in the virtual space, the AGCC countries should take a step forward and adopt a unified agenda for cyber security. To start adopting such an agenda these countries should form a high level commission including representatives of telecommunication authorities and computer emergency centers, police and military domain names specialists and Internet providers, smart infrastructure operators from all the AGCC countries. This commission in its turn should form subcommittees to address all the matters on the agenda - from improvement of Domain Names Systems to protection and shielding government and military systems. As far as matters like the infrastructure and government and military systems, the Commission should only lay more emphasis on exchange of the best practices adopted to address electronic space problems in each member country.

With regard to other matters like the safety of domain names system, improvement of networks, fighting electronic crime and reduction of service barring assaults, the subcommittees should be tasked to draw a five-year strategic plan to cooperatively improve security in a sensible way. Convenient investment in this field should start with electronic virtual space of the AGCC countries in the hope of making the Region a model to be copied by all countries worldwide.