Science Arena Publications
Specialty Journal of Politics and Law
Available online at www.sciarena.com
2017, Vol, 2 (4): 70-76

Future Studies of Cyber Attacks on National Security of the Islamic Republic of Iran

Sanam, Yeganeh Azad*
MA, Department of International Law, Faculty of Law and Political Science, University of Shiraz, Shiraz, Iran

Abstract: *One of the most important developments in today's world, especially in the national security domain, is the comprehensive definition of the concept of security, which not only includes its classical dimension, i.e. the military dimension, but also other dimensions, including political, cultural, economic and cyber. Nowadays, due to the significant expansion of technology, cyberspace has been considered as one of the important dimensions of states' security. Since cyberattacks are occurred in cyberspace, it is considered as a new way of directing combat operations. On the other hand, the capability of these attacks to cause widespread damage has transformed the traditional concept of forceful use. Since one of the most important features of cyberattacks is the extent of disruption in the identification of the incident, this paper is written due to the importance of the result of the attacks on national security following the projection of the future of cyberspace and the role of this space as one of the major sources of government power. So, securing cyber space and dealing with these attacks should be done in a thorough manner. The present study seeks to investigate the future of cyberattacking in Iran's national security and provide appropriate solutions in different sectors in different fields against cyberattacks.*

Keywords: *Future Studies, Cyber Space, Cyber Attacks, Iranian National Security*

INTRODUCTION

Right is a factor in organizing social relations. Therefore, due to the dynamic political and social movements, the rights of armed conflicts are not excluded from it, and have been changed due to the changes that occurred in the type of agents involved in armed conflict and the means and methods of warfare. One of these changes is the use of cyber space and sabotage by computer malwares. Therefore, countries that draw their future prospects in all aspects of security, especially political security, have more capability to confront cybercrime. One of the important issues in the future perspective of governments that must be considered is the issue of cybercrime attacks. Considering the importance of this issue at the international community level, this paper investigates the future studies in cyber space. So, the Future Studies Method (Delphi method) is used which is one of the most practical methods in futuristic studies. In this paper, the nature of cyber-attacks and the impact of these attacks on national security are investigated. What is important in this research is the new approach (future studies) that has been introduced.

The nature of cyber-attacks:

Cyber-attacks are a new phenomenon that has emerged with the advent of information technology and the expansion of global communications through Internet. Cyber-attacks have unique characteristics compared to the classical mode of government in attacking each other. On the one hand, these threats cover a wide range of legal, cultural, technical, and organizational barriers, and, on the other hand, low cost, dramatic impact and

lack of public transparency in cyberspace have led many actors to enter this field. These actors can include individuals from organized criminal groups of terrorist groups, private companies and nation-states.

In fact, the low cost of entry, low time-consuming, and high performance in cyber space has provided conditions in which dangerous actions can be done in a short time and high speed. Active Internet users can target the major digital aims around the world without warning and in a few seconds (Bashari Rad, 2012).

On the other hand, without the possibility of punishment and accountability for hostile acts in cyberspace, this space has been safer than non-cyber alternative options. Cybercrime is actually a disturbance in data quality and accuracy, which usually occurs through malicious code and a change in the logic program and the control of the data that results in the wrong exit.

Cyber-attacks include four domains:0

1- Loss of integrity

2. Loss of ability

3. Loss of confidential information

4. Physical degradation

Water, electricity, banking, and air transportation are just a few examples of services provided by information and communication infrastructure. These infrastructures are increasingly interdependent. And any online attack like Domino games disturbs them. Disturbance in a system is equal to the disruption of other systems and the continuation of this trend leads to the potential impact of Internet attacks (Abdullah Khani, 2007).

In cyber-attacks, the computers and their relative systems are used to distract, affect, or harass the purpose. There are usually political and ideological reasons behind these attacks, and governments use an instrument that is illegal. So much data may be stolen or changed during cyber-attacks. The target networks may be damaged materially, but the main purpose of the cyberattacks is to damage.

Definitions and Features of National Security:

With the emergence of the nation state and the expansion of its specialty, national security was considered as the most important feature of the states-nations, and some national security theorists are equated it with the vital values of the country, as Arnold Wolfers equals it as the lack of threat to acquired values.

As part of the theorists of Copenhagen School, Barry Buzan defines security as a threat and the ability of states and communities to maintain their independent identity and functional integrity against changing forces. In one of his writings, the new model of security studies in the 21st century, Bozen considers a new model of security studies based on five political, military, economic, social and environmental components. According to him, the field of security studies is widespread and deep-seated. Regardless of the Copenhagen School, although governments have a central role in security studies, this field covers every individual and international audience (Buzzan et al., 2001). With the information and communication revolution, the concepts of cyberspace and the cyber-attacks on the relationship between governments were growing dramatically, and the same for the government of Iran. And they have been cyberattacked frequently. Although this has had many challenges for the country, it eventually awakens cyberspace and some aims are considered to develop this sector in the country's developmental policies. What has been discussed in this paper is the national security issue in the Islamic Republic of Iran. With a new approach to futures research, it is planning to formulate effective and practical strategies to deal with such attacks by mapping possible scenarios.

Soft War, Cyber Attack, and National Security Threat:

The soft warfare follows the upsurge of the thinking and thought of the community to weaken the cultural and intellectual circles, and leads to the instability of the political-social system. Cyber-attacks are one of the most important forms of the soft war (Nye, 2004). The international system came to the conclusion that it is not possible to hurt Iranian national security of the hardware thirty years after the Islamic revolution, so soft warfare, especially cyberattacks, can be an important factor in fulfilling their demands, especially that cyberattacks are low-cost and destructive. For example, the attack on nuclear power plants by Stux net malware and Flame is one of those attacks. The launch of Internet sites and the provision of spywares to their agents in Iran has been one of the hostile attitudes of the enemies in the international system to undermine Iran's national security.

Reviewing the Future Studies steps in this article by Delphi method:

Future Studies Background:

The Future Studies were proposed for the urgent of the Political System in 1948 in Rand institute and sought to identify the possible events of war, it was used on civilian and economic issues. The concept of future studies was used in Policymaking in 1980s and later, and for the first time, the Japanese used it as a tool for policy-making. For decades, prospective programs have been planned in public-private institutions in regional and national levels, and in different areas of science, technology, culture, environment and so on. Fifty years ago, a French future studies researcher named Bertrand de Jouvenel, who named the father of the modernism future studies, founded the Futurebille institute, which is considered as one of the most important futuristic poles in Europe. After the Cold War and the history of nuclear weapons, the important concern for military officials was the anticipation of events that could occur after a possible nuclear confrontation, so the very first game of war was created.

With regard to futuristic studies, one of the most effective methods according to researchers and experts view was Delphi method which was first used by Rand Institute. Political officials had suggested that companies determine and explain the priorities and necessities of the security system (Marry et al., 1996).

The Delphi method is used as a method of discussion and is a suitable way to outline an overview of current events in the field of practice. In this method, which is often a two-step process, the researcher began his work with the aim of knowing a wide range of scholars and then integrated them (Coping & alignment) and sent feedback to the contestant for review. The Delphi method is in fact the establishment of a national storm, which is often used in the national future studies. The basic premise of the standard Delphi methods is that the consensus between the respondents group is more intrusive than the personal opinions, and the main advantage of this method is the work done by a network of experts (Pey, 2005).

The Delphi method involves a communication and research process that involves at least 8 steps, which include:

1- Determining some goals and issues that can be considered in the possible future direction as a probable reference.

2- Making a questionnaire as a tool for collecting data.

3. Selection of Responsible Individuals (Experts on the Future Studies subjects).

4. Main review of respondents' opinions.

5. Initial organization and summary of the data resulting from the preliminary studies.

6- Relationship between the results of primary review with opinions as a feedback of all respondents.

7. Reviewing the respondents' comments as they are informed, and their ideas may change under the influence of other inquirers.

8. Provide an evaluation and interpretation of the data and the final reports. However, it is necessary to take into account this point in the application of the Delphi method that the process of collecting expert opinions will continue as long as there is a relative and acceptable consensus on the issues and a clear outcome of the phenomena (Khazaee et al., 2008).

First step of the questionnaire:

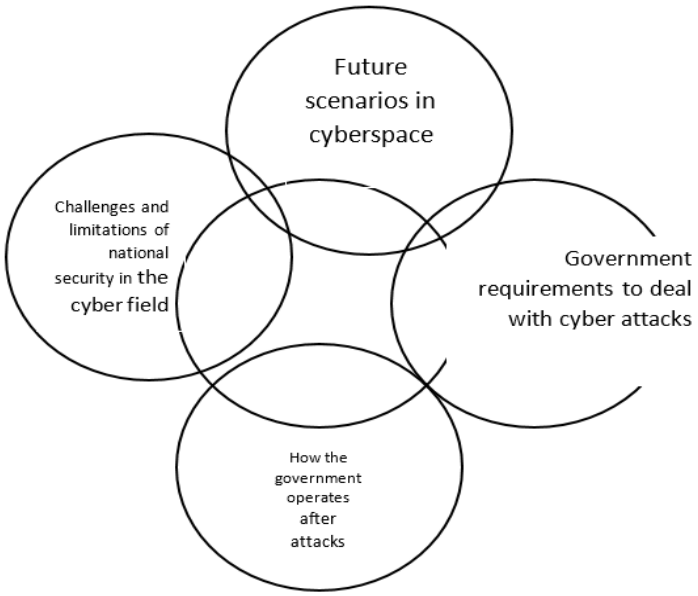
Based on the general framework of the Delphi methodology, a scientific questionnaire was developed using expert opinions related to the subject. In this regard, considering the importance of cyberspace, future cyber-attacks and awareness of the actions of cyberattack, the initial and probable trends of the actions can be estimated, thus the control over cybercrime attacks can be managed (Eftekhari, 2003).

1. Given the current trend of the international community and the virtual struggle for virtual cyberattacks and cybercrime, as compared to its classical form (military attacks), how will be the probabilities and scenarios in the future?

2- Given that cyberspace is considered as an appropriate place to hurt the security of the state from enemies due to its unique features (availability of cyber space, the uncertainty of attackers, the cost-effectiveness of this method compared to Classical methods such as military conflict and high speed finding the desired outcome) are considered as the most important soft warfare tool in the future. What challenges and limitations may be made to national security by experts and cyberspace specialists?

3. What are the government's measures to protect cyberspace, especially the protection of its vital and fundamental infrastructure during cybercrime?

4. What are the plans and actions that the government can do after a cyber-attack within the framework of international law and the UN Charter?



Step 2: Setting up a questionnaire

This step is developed in collaboration with a group of experts in the field of cybersecurity. After collecting the views, common areas were identified in their views. According to the Delphi methodology, the questionnaire was somewhat consensual which was contributed between members for the second time (Paknazar, 2001).

1. The probability of exacerbating cyber-attacks in the future, given the increasing concentration of hostile governments on cyberspace.

2. Deep development of security in the technology environment and the deployment of active defenses to cover cyber-attacks and their testing attachments.

3. Cybersecurity accelerates digitization. In this scenario, the activities of the private and public sectors restrict the spread of cybercrime tools, resulting in institutionalized capabilities and also motivate the innovation. In fact, a resilient vital cyber system that facilitates business connectivity and technology activation, and the technology innovation will be activated.

4. Attackers are stronger than defenders, although they continue to deal with threats, and the level of threats has increased.

5. The frequency and severity of attacks have increased dramatically, and international cooperation in dealing with attacking means is useless, the pre-emptive strikes have been posted to dismantle sub-bases and services sectors (such as national payment networks).

6. In the near future, with cyber-security assistance, a stunning order will be appeared in the ground-sea-air operation units, provided that military and civilian infrastructure is deployed.

Among the six raised scenarios, 3 more likely scenarios in response to the questions are as the following:

1. The probability of exacerbating cyber-attacks in the future due to the increasing concentration of hostile governments on cyberspace.

2. Deep development of security in the technology environment and the deployment of active defenses to cover cybercrime attacks, along with their continuous testing.

3. Cybersecurity accelerates digitization. In this scenario, the private and public activities restrict the spread of cyberattack tools, which leads to the creation of institutional capabilities and also drives innovation. An essential ecosystem of cyber facilities the connection of business operations, and technological innovation is activated.

According to the studies, it can be stated that cyberspace and the ability to use this space is considered as one of the most important sources of power in the 21st century, so state and non-state actors use this power to be able to achieve social, Political, military and ideological goals in cyberspace and real world. Therefore, information power plays an important role in world equations in the current era (Pour Roustai, 2010). Thus, considering the importance of the issue of cyberspace and the increase of cyber-attacks by governments, Iranian government should also develop an effective and principled program that has the following strategic components considering the dependencies in the public and private sectors in today's meta-communicate world:

1. Institutional preparation:

A) Prioritizing information based on business risks and cyber resilience integration.

B) Deep development of security in the field of technology and the establishment of active defenses to cover active attacks along with their continuous testing.

C) Developing an expert network and better coordination with key actors to reduce risk.

2. Public and international policy

A) Creating a comprehensive and transparent cyber strategy that integrates approaches across all domains.

B) Establishing a national cyber strategy and identify their institutions and critical capabilities to coordinate policies.

3-community

A) Investing in research to better understand the cyber perspective and its threats.

B) Better upgrading to deploy information by developing more collaborative tools and resources.

4. Systematic:

A) Investing in the development of risky markets and value risks from cybercrime.

B) Efforts to better integrate the security in IT tools and systems.

Conclusion:

As this paper suggests, contemporary world security developments have provided a comprehensive definition of the security framework, and one of the most important areas for national security threats of each country is cyberattacks that occur in cyberspace. In fact, Internet has faced the countries with a new challenge. The low cost of entry was unknown, the uncertainty surrounding the threatened geographic area, the tremendous impact, and the lack of transparency in cyberspace caused that the strong and weak actors, including governments, organized and even terrorist groups would enter this space and create the threats like cyber-attacks, cybercrime and cyberwar, and this has caused national security to be challenged in this space.

Since the Islamic Republic of Iran is in the process of developing and enhancing its ability to deal with the strategic sphere of cybercrime, considering that there are two main trends in cyberattacks worldwide, which include the rapid increase in the severity of cyberattacks and the Speeding up of the quality of collision by the public and private sectors. Considering the explanations given in this article, while outlining the definition and the purpose of cyberattacks, it is seeking to look at the most important scenarios for cyberattacks in the future. The main purpose of this study is to recognize the ability of the cyberspace in the future regard to the importance of the increasing number of cyberattacks, both in the national security and international security area (Lord et al., 2011). Based on studies and scenarios in the future studies of cyber space and cyberattacks that have occurred in this area, and by reviewing the opinions of experts, we conclude: Given that some of the cyber-attacks are inevitable, so instead of spending a great deal of time and money on cyber security promising businesses that do not help in inevitable cyberattacking, you can invest in cyber flexibility. More addition, a set of different elements of this area state that the future of cyberattacks can be defined in terms of the severity of the threat of attack and its impact on the private and public sectors of the country in the form of 3 more likely scenarios that have been proposed by experts. And with the use of a comprehensive cybercrime strategy, it has enhanced the country's ability to cyber-attacks against enemies.

REFERENCES

1. Bashari Rad, Babak. (2012) Computer Viruses and Malwares. First Edition, Tehran: Noghos Publish. 2012.
2. Abdollah Khani, Ali. (2007) the battle in the age of information. Second edition. Tehran: Abrar Moaser Institute of Studies and Research.
3. Buzzan, Barry, and Weaver (2001), A Framework for Analysis of Security, Translated by Alireza Tayeb, Tehran: Strategic Studies Faculty Publication.
4. Nye, S. Joseph (2004), Soft Power; the means to success in World Politics, New York; Public Affairs.
5. Marry Jane and Grim, Terry (1996), A survey of future Research Methods; Using Future Research in Your Work, World Future Society Conference, July.
6. Pey, Sakol (2005). Methods of Future Studies Research, Translation of Saeed Khazaei, Center for the Future research of Science and Food Sciences, Vice-President of Informatics and Scientific Services.
7. Khazaee, Saeed and Abdolrahim, Pedram (2008). Guidance to the Future Strategic Research, Tehran: informing Central Future Studies Publish.
8. Eftekhari, Asghar, (2003) National Strategy for Security in Cyberspace. First Edition. Tehran: Research Institute for Strategic Studies.
9. Paknazar, soraya (2001) "A Review of the Forms of the New War in the Third Millennium: Virtual and Internet Wars." Number 18.
10. Pour Roustai, Mohammad Ali (2010) "The War with Information Technology Weapons. Electronic News Newsletter. No 1.
11. Lord, Kristin M. Sharp, Travis (2011); America Cyber Future security and Prosperity in the information age, center for a new American security, Volume I.