IJBPAS, September, 2015, 4(9), Special Issue: 391-402

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

NATIONAL SECURITY CHALLENGES AGAINST CYBER THREATS

[1]MOHAMMAD KHALIL SALEHI, [1]ADEL SARIKHANI, [1]DAVOOD KARAMI GOLBAGHI

[1]Qom University

mohamad.salehy@gmail.com; adelsari@yahoo.com; karami.law@gmail.com

ABSTRACT

Cyber world had faced governments and their citizens with new security challenges. Low cost entrance, anonymity, uncertainty of threatening territory, profound influence and lack of public transparency of cyberspace all caused that strong and weal players including governments, organized terrorism groups and even individuals entering this space to create threats such as cyber war, cybercrimes, cyber terrorism, and cyber espionage. This point distinguishes cyber threats from traditional national security threats (that are to a large extent clear with a specific geographical territory) and caused conflict of traditional concept of national security. In this article, it is tried to discuss how nature of new cyber threats affect national security of governments.

Keywords: Cyber Threats, National Security, Cyberspace, Cyber War, Cyber Terrorism

INTRODUCTION

Societies are facing with the second industrial revolution, ea. information revolution; the revolution that replaces machine with human thought and has more ability to change than industrial revolution of 19th century that replaced machine with manual work. Global advances of personal and commercial computers, increase in abilities of data storage and data processing, computer microchips installed on industrial products, integration of data process with new telecommunications technologies with research of artificial intelligence(AI) all express the current development that is often

called 'information age'. This victorious use of computer not only has benefits but also it caused significant importance of computerized systems, providing their security and its account great influence in trade, bureaucratic and social affairs. For example in trade dimension, the effect of financial operation performs by computer and in form of payment by bank account; balance sheets are provided by help of computer, and returns of a company often depend on ability of data processing system. Furthermore, many companies keep their most important secrets in computer's memory. Advances in bureaucratic systems also depend on computer technology and databases. Marine and aerospace control systems, medical supervision and defense system of most countries of the world are highly depended on advanced computer technology. It is because of this dependency that increase of crimes against data process systems during last decade in west European developed countries, US and Japan is considered as a danger for several levels of national security.

Therefore, we discuss impact of nature of modern cyber threats on national security. In this regard, we first study nature of threat and essence of cyber threats, and then we discuss about national security and its common concepts. Finally, we consider the influence of new cyber threats on national security.

Different theoretical approaches to national security

Field of national security considers different approaches of international relations. Each of these approaches consider issues such as power, national interests, and structure of international system based on their specific viewpoint. We discuss about concept of national security in the below. Realists believe that there is not an issue called 'security' in level of domestic policy, and security is only meaningful at international level. In other words, for them national security is nothing but international security and in this regard insecurity is characteristic of international system. From realists' point of view, insecurity, power, government and war are the main issue, the main tool, the most important actor and the most obvious view of insecurity in the international arena, respectively. Therefore, the focus of realism is on military security.

As Stephen Walt says, security studies are about threat, use and control of military force. Apart from military issues, other factors are also important in discussion of security, but realists and neo realists consider

their importance to the extent that helps development of military abilities. From realists' viewpoint, anything can influence on security; but the issue of security itself could not be everything. Realists believe because governments are main players of international system, thus they will be security reference.

In contrast, the classic liberalism accepts international anarchy, besides it believes that 'peace' is possible not by power balance and the more arming of countries, but trough developing democratic governments in the world. Like realism, institutional neo liberalism as one of the important attitudes of liberalism also accepts that international arena is arena of anarchy and such an environment endangers national and international security; but it has a different solution for security. Experts of this theory believe that for providing security and keeping peace, the behavior of governments must be controlled; and this is possible by establishing international organizations and regimes.

On the other hand, doctrine of Kopenhague is also disagreed with the approach that perceives war and force as core of security studies. Buzan (1989) believes that according to realists' viewpoint, complex concept of security is reduced with power. According to doctrine of kopenhague, although personal security shows a specified and important level of analysis, but people can't could not be identified as security reference, since it is basically subordinate of higher national and international political structures. Therefore, Kopenhague doctrine also rejects individual orientation of security reference, and emphasizes on government as center of security. In one of his writings named' new pattern of security study in 21 century', Buzan knows the new pattern based on political ,military ,economic ,social and environmental components.

Constructivism approach rejects anarchic nature of international system, besides it involves identity in security studies and foreign policy as a procedure.in this framework, governments perceive the identity, enemies and competitors based on their identity and define and redefine their identity in this process. Security does not indicate outside material situation, but it is a social, intersubjective and semantic concept that is constructed in social process. Attention to human security and orientation towards ideological concepts in global security are features of constructivism approach. Of course it must be noted that

some authors like Jessica Tuchman emphasized on issues such as environmental threats, economic welfare and population growth.

With this brief study, we achieve the result same as Buzan in his security studies. He explains that 'national security is weak in terms of concept; it is ambiguous in terms of definition but politically strong'. As a result, none of the relative definitions and approaches could analyze issue of national security well; during last decades, this complexity of security concept is doubled due to entering issues relative to cyberspace and its threats.

Nature of cyber threats

Cyber threats are new phenomena that had emerged during last decades simultaneously with information technology (IT) and development of global communications through extensive network of internet all around the world; so that today the challenge of cyber threats seems important and complicated both. This importance and complexity is due to new nature of cyber threats and its unique features and trends. In a conference that was held in March, 2010 by CACI international institute and US institute of marine research titled 'national security cyber threats and dealing with global challenges' , cyber threats were defined as ' events that are influential on virtual space naturally and/or by human (intentional or unintentional) ,and incidents performed by virtual space or related to it'. Also cyberspace is defined by some experts as 'impact of space and society formed by computers, information, electronic devices, digital networks and/or its users'.

Types of cyber threats

Public and non-public actors use cyber power to archive their social, ideological, social, military and financial goals in cyberspace and real world. These goals are achieved in cyber space by several methods including: cyber war, cyber terrorism, cybercrimes, cyber espionage and cyber agitation.

Cyber war

If we are agree with Clausewitz that war is not just a political action, but it is a political tool achieving political goals, then we can say that war in cyber space is performed by actors who are seeking to use this space to achieve their political goals. In order to understand whether hostile act in cyber space is considered as 'war' or not, we need to perceive purpose of actor. For example, if purpose of an internet attack is financial or personal income by criminal method such as theft, fraud and extortion, then it must be

treated as criminal act; but if purpose of attacker is greater ambitions such as imposing serious damage to government or its citizens, weakening and inactivating military and non-military infrastructures, then such a behavior is in fact something close to traditional concept of beginning war. In 2007, Estonia as a small modern country was under internet attacks in large scale. High technology of this country was a suitable field for cyber-attacks with political motives. As Richard Clarke states, cyber war is a new form of battle that we are not able to understand yet. Yet, it is clear that battlefield of modern world expands its domain to cyberspace and we must consider it as the 5th field of war beside traditional fields of earth, air, marine and space.

Cyber attacks

Cyber-attack is different from cyber war. It is disorder in accuracy of data usually performed by destructive codes and change in logic programming and data control led to wrong output. Cyber-attacks include 4 categories: 1. Loss of integrity, 2. Loss of ability, 3. Loss of secret information and 4.physical destruction. Water, electricity, banking and aerial transportation are just a few example of services that are running by information and communication infrastructures. These infrastructures are increasingly interdependent and any cyber-attack can disrupt them like domino game; as disorder in a system equals to disorder in other ones, and continuity of this process is of potential impacts of cyber-attacks.

Cyber terrorism

Federal emergency management agency defines terrorism as:' illegal threat and attack against computers, networks and information saved in, when it is performed to force or terrorize government or people for further social or political goals'. With loss of key physical bases (like Afghanistan), terrorist became a key threat for action in cyberspace. These actions could include increase in resources to support their operations, operations programming (use of accessible tools such as Goggle earth), control of operations, intrusive operations and training their members (establishing explosive devices).

Cyber crimes

Cybercrimes can be infringement of spiritual property rights, patent infringement, or abduction of trade secrets. These crimes include designed attack to computers in order to misadjust them or to copy classified information. Analysts had estimated that cost of cybercrimes is more than 1000 milliard

dollars for global industry in case of infringement of intellectual property and loss of information. For example, in 2009 a person stole several terabytes of data related to electronic system and information design of the Pentagon's program joint fighter program valuing 300 million dollars. Furthermore, most of internets criminals have escaped punishment. It is obvious this profitable activity and often without punishment is in fact a treat for national security.

Cyber espionage

Cyber espionage use computers and related systems to gather confidential information. In contrast to cybercrimes in which financial and economic issues are main motives of criminals, cyber espionage has mostly political effects and threatens the society. Premium motives of cyber espionage are different, but include military, industrial, political and technical interests. Cyber spies use data stolen with several purposes including threats, extortion and disrupting the activities of political rivals.

Cyber agitation

Cyber agitation use computers and related systems to mutilate its desired goal, to influence it and/or to annoy it. There are political and ideological goals behind these actions and individuals use illegal tools. Nihilistic and anarchic hacker groups use cyber agitation; for example, a group called 'unknown' performed vast cyber-attacks in response to arrest of Julian Assange , the manager of controversial site 'Wikileaks'. In contrast to cybercrimes and cyber espionage aimed at stealing or changing information, cyber agitation tries to punish or influence on beliefs and behavior of its goals. During this process, lots of information might be stolen and/or changed; but main purpose of cyber agitation is to damage. Public and non-public actors can use this tool, but till now cyber agitation is performed by individuals who are known as 'hackers'.

Cyber threats have a diverse, vast and unique nature; it is diverse since these threats affected all aspects of human life and as a result, insecurity of cyberspace is high. It is vast since not only public actors but also private firms, groups and individuals are involved in it. Its uniqueness is because nature of these threats is different from traditional and common threats; of course, this feature mostly had affected governments and their understanding of threat.

National security: common perceptions

Simultaneous with creation of government-nation and developing its specific functions,

the national security was placed on the agenda of governments as one of the most important functions; so that most of analysts believe that essence of governments is linked with providing domestic and foreign security by them and how to define, extend and improve concept of national security. In this regard, there are different approaches among governments and academic environments about discussion of national security and how to provide it. In this section, we present the most important common theoretical approaches.

Impact of cyber threats on national security

Most of experts and analysts of security domain believe that end of cold war not only had not led to safer world, but also creating non-military security challenges such as environmental degradation, economic welfare, international terrorism organizations and massive migration of people – had faced national security with more serious challenges than in the past. Analysts believe that importance of these 'new' issues not only necessitates review of national threats but it also requires review of security concept itself.

Yet, what is significant about these new threats is that nowadays these viruses ,worms ,crimes, hackers and internet attacks are certain and routine realities. The important destructive attacks with vast effects had portrayed cyber threats as one of the worth threats to national interests; to the extent that America had announced it treat these threats as war and will respond physically. On the other hand, discussion of these threats is influenced by continual information revolution and its penetration to all aspects of human life. Thus, we first consider information revolution and wonderful impact on its power and resources, then we will study the relative cyber threats and its impact on national security.

Security of modern age

Today, national security faces with several threats, but in between cyber threats are new phenomena with information technology and open communications. This phenomenon is so new that study of its consequences for national l security of governments has largely neglected. During two last decades, an attitude had developed toward strategic studies of cold war. This trend emphasize on a criteria beyond most of trends that are considered as excessive military interpretation. According to this group, today security threats are not just military, but environmental issues, global poverty,

migration and recently cyber threats endanger security of governments more than military threats.

During last decade, a number of general features of attacks designed by computer known as 'cyber attacks' are identified as one of the worth threats for national interests. According to what was said, we can define cyber security generally as 'protecting important information infrastructure and its processes and contents'. Thus, as one of the most important sectors of national power arises from information power, also one of the most important sectors of national security comes from data security and protection.

Size and scope of these threats is to the extent that America had confessed this is the first time during the history it cannot protect its infrastructures alone. Americans had confessed they cannot employ large enough army or police force to protect all phone lines and/or US citizens' computer networks, especially when 95% of these infrastructures belong to private sector. Of course this itself is subject to the fact that employing army and police force could be helpful against these threats; with respect to specific features cyber threats, efficiency of these forces against threats is doubtful. It seems there are some issues that not only USA but also all countries are facing with in relation to cyber security efforts:

- Unreliability about geographical location of internet attackers;
- Developing integration of mobile technology devices with sensitive information infrastructures;
- New damages to country's infrastructures through complex and increasing threats;
- Lack of coordination between public and private sectors due to emerging threats; and
- Legal uncertainties to respond such threats

These issues have at least four important consequences for national governments: first, change in perception of governments about how to define their interests, power and security bases; second, arising challenges against ability of governments to control and manage release of information; third, relation of security issue with global networks and fourth, reduction in capacity of governments to ensure security of their citizens.

Therefore, the concept of traditional national security which means lack of threat against country's vital values is also changing. The damage of manipulating information infrastructures might be more than financial and physical effects of some wars. Today, invaders to a country might be governments,

groups, individuals and/or combination of them. For example, in 1998 Washington complained to Russia government due to Moscow's seven internet addresses involved in stealing secrets of Pentagon and NASA. The Russian responded that phone numbers involved in the mentioned attack are not valid. Therefore, US government had no way to understand whether Russia had participated in this attack or not?

According to traditional approach, governments pay much attention to their survival and providing military security. Yet, it must be noted that nowadays governments are forced to consider new dimensions of security. For example, Canadians do not worry about American soldiers to attack Toronto again like 1813, but they fear that a computer in Texas faces up Toronto with a main problem. The traditional concepts of war based on attack and defense are rapidly changing; they have been challenged by complexities of cyberspace, and this threat had changed traditional concepts of war to some extent. Cyber threat is asymmetric and hence, there is no need to great investment for its application and/or attack by it. In contrast, defense must consider all aspects against cyber threat with increasing costs.

Other problem of cyber threats is caused by its legal uncertainties; it means that there is no law of cyber subversive activity, especially cyber war. In traditional rules of war, there are agreements and commitments such as Genève convention and UN charter that explicitly state 'no nation can use its force against integrity or political independence of other countries'; while it is difficult to define cyber war in this framework.

CONCLUSIONS

At last, we can conclude that cyber security is important and complicated both. To achieve effective settings, the government needs comprehensive strategy including coordinated action by government, private sector and citizens. Global society also has explicit joint interests in support of cyber systems security and immediate cooperation and action in this field. In line with such an importance, in 29 May 2009 US president announces that cyber space is an important national property that government will defend it by all means.

Thus, cyber security is indirect relation with national security of the country. Today, it is no longer possible to define national security in relation with foreign borders and to protect citizens by military forces. Now, enemy has

infiltrated our homes with help of internet and a computer, while we do not realize its physical presence. Such penetrating risk had undermined all common and traditional perceptions of national security concept.

REFERENCES

1. Hare, Forrest, 2010, The Cyber Threat to National Security: Why Can't We Agree? CCD COE publications.
2. Markoff, Jaud & Shanker, T. 2009, Halted Plan Illustrate U.S Fear of Cymerwar Risk, the New York Times, p:13
3. Chertoff, Michael, 2008, the Cyber Security Challenge, Regulation & Governance, p: 484
4. Tabasco, Lior,' Basic Concepts in Cyber Warfare', Military and Strategic Affairs, p88,2011.
5. Vatis, Michael, 2002, Cyber Attacks: Protecting American's Security against Digital Threats, John F. Kennedy School of Government, Harvard University, p:2
6. Theohary, Catherine A, & Rollins, Johan, 2009, Cyber Security: Current Legislation, 7.Executive Branch Initiative, and Options for Congress, Congressional Research Service, p:45
7. Klarke, Y.' Globalization and theory of international relations', translated by Faramarz Taghilu, office of political and international studies, Tehran, p.236, 2008.
8. Nay, J, 'Cyber Power, Belfour Center for Science and International Affairs, p:4, 2010.
9. Nay, J.' Power in information age: from realism to globalization', translated by Saied Torabi, strategic research center, p.98, 2009.
10. Mir Mohamadi,M, et al.' Politics and information: case study of America', institute of cultural studies and international research, Tehran, p.52, 2009.
11. Rozena,J,et al.' Information revolution: security and new technologies', translated by Alireza Tayeb, strategic research center, Tehran, p.362, 2012.
12. Tuchman, Jessica, 1989, Redefining Security, Foreign Affairs, vol 68, No 2, p:162-177
13. Buzan,B.' People ,governments and fear', strategic research center, Tehran, p 8, 2000.

14. Darvishi, F.' A theoretical approach to national security: threats and strategies', Tehran, p 23, 1998.

15. Roshandel,J.' National security and international system', Samt publications, p 14, 1994.

16. Abdolahkhani,A.'Theories of security', institute of cultural studies and international research, Tehran, vol 1, p 70, 2004.

17. Yazdan fam,M.' Change in theories and concepts of international security', journal of strategic studies', vol 38, p 731, 2008.

18. Mandel, R.' Changing face of national security', strategic research center, Tehran, p 44, 2001.

19. Wolfers, Arnold, 1962, Discord and Collaboration, Baltimore: Johns Hopkins University press, p:120

20. Buzan, Barry, 1991, New Pattern of Global Security in the first-twenty century, International Affaire, p:432

21. Terrify,T, et al.' studies of modern security', translated by Alireza Tayeb & Vahid Bozorgi, strategic research center, Tehran, p 49, 2005.

22. Nagre, Dhanashree & Warade, Priyanka, 2008, Cyber Terrorism Vulnerabilities and Policy Issues, Facts Behind the Myth, www. Andrew.cmu,edu/user/danger. p:5

23. Peritz, Akij & Sechrist, Michael, 010, Protecting Cyberspace and the U.S National Interest, Belfer Center for Science and International Affairs, p:5-7

24. Starr, Stuart H, 2009, Toward an Evolving Theory of Cyber Power, National Defense University, Center for Technology and National Security Policy, p:18

25. Islam Qasem, Teun van Dongen, Marjolein de Ridder, 2011, Dealing with Cyber Security: accept Vulnerability, World foresight forum is an initiative of www. Worldforesigh forum.org, p:5-6

26. Army, U, 2005, Cyber Operations and Cyber Terrorism, in U, Army Trainin, p:1-3 .

27. Rodrigues, Carlos A, 006, Cyber terrorism, Inter-American Defense College as a Prerequisite for the Diploma approved, p:9-10.

28. Cornish Paul & Livingstone, David & Clemente, Dave & York, Claire, 2010, on Cyber 30.Warfare, A chatham House Report, www, chathamHouse.org.uk, p:12-13

29. Tiirma-Klaar, Heli, 2011, Cyber Security Threats and Responses: At Global, Nations State, www. Ceri-scienes-po.org, p:34 .

30. Lord Kristin M, and Sharp, Travis,' America's Cyber future Security and Prosperity in the Information Age, Center for a New American Security, Volume I, p: 10 .