A Domestic Model to Counter the Cyberspace Threats in Iran

Seyed Vahid Aghili, PhD.
Faculty member
Social Communication Department of Science and Research Branch
Islamic Azad University
Tehran, Iran.

Farahnaz Mostafavi Kahnegi
PhD candidate
Social Communication Sciences
Faculty of Humanities
Science and Research Branch
Islamic Azad University
Tehran, Iran.

Abstract

This study seeks to offer a domestic model to counter the factors affecting cyber threats. From this perspective, with a review of the concept, considering the research questions and given the characteristics of the population under study, it is aimed to identify the factors affecting cyber threats.

With a combined approach of exploring method and using interview techniques (qualitative approach) along with questionnaire techniques (quantitative approach), over 154 professors, professionals and experts in cyber activist in Tehran through purposive sampling (in the cyber elite domains) and simple random sampling (among professors, scholars and activists in the field) with an error level of 0.05 and confidence level of 95% were chosen. The required data was collected, in order to calculate the validity of the indicators, the method of content and numeric Sigma ranging from zero and one, and also in order to calculate the reliability of the indicators, the Cronbach alpha was used to determine the reliability coefficient.

Research findings show that making decisions in controlling all aspects of cyberspace and its systems calls for awareness and understanding of the situation.

Keywords: cyberspace, cyber threats, internet, information technology

1. Introduction

In the past few decades there has been a revolution in computing and communications, and all indications are that technological progress and use of information technology will continue at a rapid pace (Lee).Threats to the cyber and telecommunications infrastructure are constantly increasing (Eisler, 2009) and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests. Activities producing undesirable results include unauthorized intrusion to gain access and view protected data, stealing or manipulating information contained in various databases, and attacks on telecommunications devices to corrupt data or cause infrastructure components to operate in an irregular manner. Of paramount concern to the national and homeland security communities is the threat of a cyber-related attack against the nation's critical government infrastructures — "systems and assets, physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters." In the past year, much has changed in cyber security. Attackers aligned with national agendas have focused on targeting businesses and governments in attacks that have resulted in the leakage of sensitive and critical data.

Employees bringing consumer technology into the workplace most notably, smart phones and tablets—have led to increased productivity, but at the same time have undermined the security practices at companies which had, in the past, focused on securing their perimeter. The movement of business and consumer data to the cloud has often led to the increase of the overall security of such information but created large stores of important data that will lure attackers. If we are going to prevent motivated adversaries from attacking our systems, stealing our data and harming our critical infrastructure, the broader community of security researchers—including academia, the private sector, and government—must work together to understand emerging threats and to develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it (Emerging Cyber Threats Report, 2013).

2. Types of Cyber Threats

Cyber threats generally fall within six categories:

- **Traditional threats** typically arise from state employing recognized military capabilities and forces in well-understood forms of military conflict. Within cyberspace, these threats may be less understood due to the continuing evolution of technologies and methods. Traditional threats are generally focused against the cyberspace capabilities that enable our air, land, maritime, and space forces and are focused to deny the US military freedom of action and use of cyberspace.
- **Irregular threats** can use cyberspace as an unconventional asymmetric means to counter traditional advantages. These threats could also manifest through an adversary's selective targeting of US cyberspace capabilities and infrastructure. For example, terrorists could use cyberspace to conduct operations against our financial and industrial sectors while simultaneously launching other physical attacks. Terrorist also use cyberspace to communicate anonymously, asynchronously, and without being tied to set physical locations. They attempt to shield themselves from US law enforcement, intelligence and military operations through use of commercial security products and services readily available in cyberspace. Irregular threats from criminal elements and advocates of radical political agendas seek to use cyberspace for their own ends to challenge government, corporate, or societal interests.
- **Catastrophic threats** involve the acquisition, possession, and use of weapons of mass destruction (WMD) or methods producing WMD-like effects. Such catastrophic effects are possible in cyberspace because of the existing linkage of cyberspace to critical infrastructure SCADA systems. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructure locally, nationally, or possibly globally. For example, electromagnetic pulse events could cause widespread degradation and outright destruction of the electronic components that comprise cyberspace leading to the debilitating destruction of segments of the cyberspace domain in which operations must occur.
- **Disruptive threats** are breakthrough technologies that may negate or reduce current US advantages in warfighting domains. Global research investment, development, and industrial processes provide an environmental conductive to the creation of technological advances. DOD must be prepared for the increased possibility of adversary breakthroughs due to the continuing diffusion of cyberspace technologies.
- **Natural threats** that can damage and disrupt cyberspace include acts of nature, such as floods, hurricanes, solar flares, lightning, and tornados. These types of events often produce highly destructive effects requiring DOD to support the continuity of operations in cyberspace, conduct consequent management, and restore cyberspace capability. These events also provide adversaries the opportunity to capitalize on infrastructure degradation and diversion of attention and resources.

Accidental Threats are unpredictable and can take many forms. From a backhoe cutting a fiber optic cable of a key cyberspace node, to inadvertent introduction of viruses, accidental threats unintentionally disrupt the operation of cyberspace. Although post-accident investigations show that the large majority of accidents can be prevented and measures put in place to reduce accidents, accidents must be anticipated (National Military Strategy for Cyberspace Operations, at C-1, C-2).

3. Research objectives

Main Goal: To specify the effective factors in political, economic, social, military and technological cyberspace threats in Iran and to offer a domestic model for counter the threats.

Applicatory GOALS

1. To specify different dimensions of the effective factors in cyberspace threats

2. To specify different dimensions of the threats and methodological approaches of the threats

3. To define the cyberspace and explain the nature of the cyberspace threats

4. To identify the applicatory aspects of cyberspace threats

4. Research Questions

Main Question: Which are the most important political, economic, social, military and technological cyberspace threats in Iran?

Subsidiary Questions

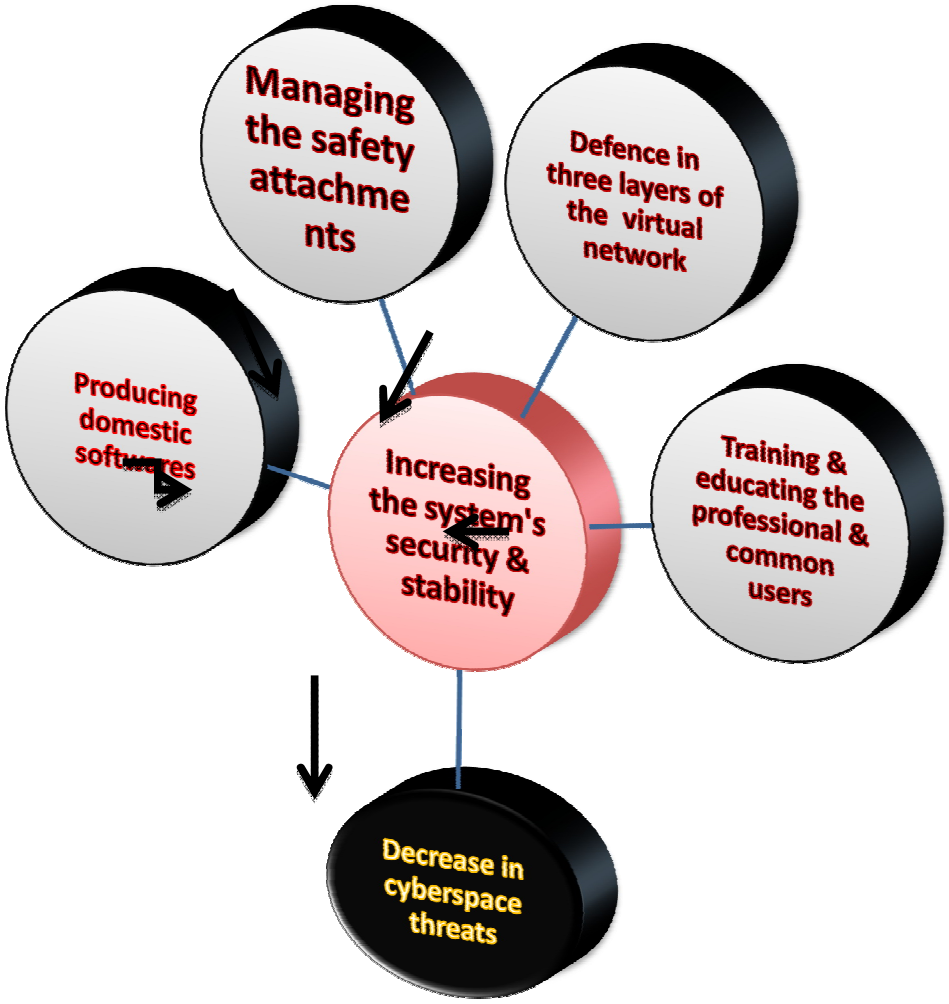
1. Is the cyberspace an opportunity or a threat for the country?
2. Which are the strengths of Iran in countering the cyberspace threats?
3. Which parts of the cyberspace in Iran are damageable by the threats from outside the country and why?
4. How can the strength and power in Iran be used to counter the cyberspace threats?
5. Which are the factors to set a domestic model for countering the cyberspace threats in Iran?
6. How successful has Iran been in countering the cyberspace threats?

5. *Factors and Motivations to Threaten*

Factors and motivations to threaten fall within four categories:

1. Ideological motivations
2. Benefit orientated motivations
3. Individual motivations
4. National motivations

6. Domestic Model for Countering Cyber Threats



7. Conclusion

Today, cyber is the fifth field after earth, sea, air and space. Given the cyberspace entering all aspects of life from scientific issues to work, entertainment, economy, education and communications, attackers can create challenges in the target society's people's daily affairs. Moreover, as most organizational or inter-organizational communications are made through internet, cutting the internet service itself could be a reason for challenges and inconvenience in countries. Hence, setting a harmonic and united strategy in cyberspace in local, national and international levels is a must. As a result, following offers look useful for the success of the country in application of the cyberspace and countering the threats in this field:

1. Cooperation of public and private organizations

2. Public awareness

3. Making use of international standards, strategies and experiences

4. Training the human resource

5. Considering individual sanctum

6. Assessing the damageability, reminding and reactions

7. International cooperation in cyberspace security

References

Eisler Peter, "Reported Raids on Federal Computer Data Soar," USA Today (Feb. 17, 2009) (full-text). Based on data reportedly provided to USA Today, the U.S. Computer Emergency Readiness Team (US-CERT), a Department of Homeland Security entity, found that known cyberattacks on U.S. government networks rose 40% in 2008 compared to 2007.

Emerging Cyber Threats Report, 2013: http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf

Lee, Konsbruck Robert, Route de Chavannes, 27C CH-1007 Lausanne-Vidy Switzerland.

National Military Strategy for Cyberspace Operations, at C-1, C-2.

Terrorist Capabilities for Cyberattack: Overview and Policy Issues.

42 U.S.C. §5195c(e). Critical Infrastructures: Background, Policy, and Implementation.