CYBER SECURITY STRATEGY FOR DEVELOPING COUNTRIES

REFERENCE TO AFGHANISTAN

Mohammad Salem Hamidi

Prof. (Dr.) Baldev Singh

Abstract

Growing and development of country is related to the cyber space, most of country invested large amount of budget on cyber space software. According of formal documents and information, Afghanistan is in the process of integrating ICT into its important information structure and technology. For executing the integration country may face to different challenges that involving in cyber security. Due to various potential threats and risk on cyber security in Afghanistan, there is need for an extensive and comprehensive strategy.

Based on official documents Afghanistan has introduced an ICT security law in 2011. However the fast growth of internet in private sector and governmental sector in the last five years, cause to Afghanistan must introduce a comprehensive and appropriate cyber security strategy to cover all risk and issue that is related to this arena.

The aim of this research is to propose a comprehensive and complete cyber security strategy based on developed countries experiences in the field of cyber security, specifically India, because India has good situation in technology and has common benefits, furthermore India is considered as developed country in term of technology and cyber security.

Therefor, based on literature review and official documents, the current position of Afghanistan ICT as well as cyber threat were identified and detected in context to Afghanistan. To evaluate the situation of Afghanistan cyber security and India cyber security, some cyber security experts were interviewed and according their suggestion, and literature reviewed on developed country, a comprehensive strategy framework was suggested for Afghanistan to address ever growing cyber-attacks and treats.

Keywords: cyber security, cyber space, cyber-attack, cyber security strategy.

INTRODUCTION

Cyber security is the process of securing data and services. its evolving task to the entire ICT users and providers, such as home users, small offices, enterprises and governmental as well as non-government entities. Its like umbrella framework for clarifying and guideline for action related to security of cyber space.

CSs framework allow allows organization and individual sector to design proper cyber security techniques to satisfy their requirements in facing cyber security issue and challenges(Vernex,2013).

The framework offers an general survey of what is require to efficiently protect information infrastructure, data center and network, and also increase the defense of government in cyber space in the country.

Therefore, the strategy, objective to build a cyber-security framework, leading to specific action with program to raise the cyber space of country. (Ten, Manimaran and Liu, 2010).

In addition, we can summary that, cooperation between private key and public key players to safeguard the country's critical information infrastructure, also allowed information system.

Previous research emphasize the relation between of protection of critical ICT and information infrastructure as across sectional matter , given protection of critical information foundation and infrastructure special significance.

Most the time there are issue and challenges for developing countries specially in Afghanistan. According to Walid (2913) there for four main challenges faced by ICT sector in Middle East that must be addressed in order to gain the strategy goals:

1. Minimal level of cyber security, procedure in government offices and corporations.
2. Gap between industry and academia.
3. Poor it security infrastructure.
4. Difficulty in finding ICT experts in the middle East.

CASE STUDY OF AFGHANISTAN

According to MCIT Afghanistan(2011),Afghanistan is a developing country, which in term of cyber security is at the initial step, need strategy to survive in such competition world. by the introduction of different ICT based technology in the country, Afghanistan is moving in the direction of electronic culture in its day to days dealings. As the growing and become popularity of these technologies, it is important to put it in technological infrastructure and legal frameworks.

That will safeguard the enterprise and private data flowing through information and communication technology based infrastructure. MCIT Afghanistan already drafted an ICT law, which has addressed broader security related issue. But in order to completely implementing the law, there is require more development of regulation in focused area. Also emphasizes that, data privacy cause entrepreneurs for e-commerce, the government to run different services like e-services, e-administration and so on, and public to share their personal data with government and enterprises, by use of electrical service delivery channels.

According to ITU (2012) Afghanistan has two important challenging issues regarding of cyber security. First, no appropriate and proper mechanism to identify the threats and risk within private sectors and government sectors. Similarly most governmental offices computer and network devices are not equipped with reliable security software. There aren't anti-spam, antiviruses for blocking malware and viruses. Furthermore, some governmental offices state they haven't experienced any kind of attacks. This can be have to reason, first: they don't want to share the attacking information, secondly; they aren't aware of the attacks.

Also the country computer network structure is much scatter and spread. This can cause difficulty in detection of cyber-attack and increase the complexity of attack detection and control.

So Afghanistan require a comprehensive CSS to cover all the cyber secure issue. Since Afghanistan is in the initial process of integrating ICT into its critical information foundation, the country may face different challenges and issue in cyber security arena. Due to various potential threat and risks a comprehensive cyber security strategy is required in Afghanistan. However Afghanistan introduced an ICT security law in (2012), since internet has penetrated both governmental offices and non-governmental offices sectors with various cyber

security software. Thus the country should introduce a comprehensive and appropriate cyber security strategy to cover all of the issue and risks related to cyber security. So in this research we propose a cyber-security framework to defend and protect the country critical information infrastructure in the process of merging ICT in providing social and economic services.

METHOD

Some previous research works have been used the qualitative approach that is interview to develop and improve cyber security strategy framework or have suggestions for the development of existing cyber security strategy framework (Reyes et al,2011; ITU,2014) as shown in the bellow table.

Table 1: Past Studies Qualitative Method in Literature

Researchers	Methods	Finding
Kulikova(2012)	Interview and literature review	Proposed a cyber-security framework
ENISA(2012)	Survey and interview	The interview experience, cause to recommend for practices in developing, implementing and marinating cyber security policy/ strategy
OCED(2012)	Open-ended questionnaire	Comparing ten countries cyber security strategy between (2005-2012) and recommend promotion of their policy/ strategy
PWC: Research UK cyber security (2013)	Online survey and interview	Survey and identification the current cyber security in UK, and motivate the other organization to do so.
Reyes et al (2011)	Interview and review of documents	Security of documents
Sommestad(2012)	Interview and literature review	Used framework to build a qualitative theory on cyber security to build and validate framework

Table 2: Proposed cyber security strategy framework for Afghanistan

Literature Review and Documents Analysis			
A: Body of knowledge on cyber space	**B:** cyber security strategy	**C:** Lesson from other countries	**D:** case study of ICT in Afghanistan
Cyber space	Review of global CSS	Developed countries CSS	Current status of ICT in Afghanistan
Threat in cyberspace	EU and non Eu countries CSS	India experience in cyber security	Internet, internet service providers
Cyber attack	Common themes	Common value of India and Afghanistan	Cyber space threats in Afghanistan
Cyber security			ICT law in Afghanistan

Thus, in this research we also used qualitative approach by using of half structure interview to suggest strategy framework according to cyber security experiences of developed and developing countries include India and Malaysia.

In addition Afghanistan information and communication technology current status are analyzed and recognize. Also Indian experience in cyber security is highlighted. For better understanding and identifying the current status of ICT and cyber security in Afghanistan, the responsible people in MCIT and cyber security department were interviewed.

Then, the threats and risk of Afghanistan cyber space are highlighted. Then the analyze process is done, and cyber security strategy framework is proposed for Afghanistan ICT, that is certified by interviewing experts in the field of cyber security. In the current research, experts and officials from Afghanistan were interviewed. the main goal of selecting these professional were to check the validity of the study methods and design.

Another in charge who have involve in the information and communication technology and cyber security research were obtain to answer the interviewed questions.

The reasons of selecting them is that, they have the latest information about cyber security, cyber security policy and strategy in Afghanistan. So these people are the famous figure and policy maker in cyber security filed. The make the proper sample for the current CSS framework.

RESULTS AND DISCUSSION

According of the developing and developed countries experiences (India, Malaysia and US), based on cyber security strategy and based on the finding of both interview and document contents analysis, it is discovered that Afghanistan has rapid development in the term of information and communication technology services in the economic and social aspects during the last decade. According of instance and record events the country experiences cyber security problems; there is no cyber security strategy framework in place.

Thus, Afghanistan as an ICT appears country, which is increasingly providing cyber based services. So there is need of cyber security strategy framework to address the challenges of cyber threats. Afghanistan ICT Minister, and ICTI director confirmed that priority should be given to defense the government investment and data. Therefore, in this research the main proposed on cyber security strategy structure is to protect governmental data, increasing foreign investment and increasing online shopping and services.

REFERENCES

1. Benzel, T. 2014. The science of cyber-security experimentation. Proceedings of the 27th Annual Computer Security Applications Conference. Florida
2. Dlamini, I. Z., Radebe, & Taute, B, J. 2012. Framework for an African policy towards creating cyber security awareness. Paper offer at the 21st (IFIP) TC9/TC11 South African Cyber-Security Awareness Workshop (SACSAW), May 12th, Garborone, Botswana.
3. Chander, M. 2016. (NCIIPC). National Critical Information Infrastructure Protection Centre . Role, Responsibilities & Charter http://www.indiasmartgrid.org/en/Lists/Members/Attachments/19/ISGD%20Plenay%20III%20 Muktesh%20Chander%20NCIIPC.pdf [May 9, 2014].
4. Dogrul, M., A, Aslan, & Celik, E. 201.1 Developing an international cooperation on cyber defense and deterrence against Cyber terrorism. Paper have been presented at the Cyber-Conflict (ICCC), 3rd International Conference on Cyber Conflict (ICCC), June 7-10, Tallinn-Estonia.
5. Science, 6(7): 808.., Gurkaynak, Yilmaz, I G & Taskiran, N. P. 2013. Governmental Efforts and Strategies to Reinforce Security in Cyberspace. International Law Research, 2(1):185
6. European Network and Information Security Agency (ENISA). 2014. National Cyber Security Strategies: Setting the course for national efforts to make strong security in cyberspace. Greece, He raklion: ENISA.
7. Ten, C. W., Manimaran, G., & Liu, C. C. 2010. Cyber-security for critical infrastructures: attack and protection modeling. Systems, Man and Cybernetics, Part A: Systems and Humans. IEEE Transactions, 40(4): 853-865.