https://doi.org/10.17576/apjitm-2015-0401-01

http://www.ftsm.ukm.my/apjitm
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 4 No. 1, June 2015: 1 - 10
e-ISSN: 2289-2192

A FRAMEWORK FOR CYBERSECURITY STRATEGY FOR DEVELOPING COUNTRIES: CASE STUDY OF AFGHANISTAN

KHOSRAW SALAMZADA
ZARINA SHUKUR
MARINI ABU BAKAR

ABSTRACT

Given the importance of cyber space for country development, many countries have invested large amount of money for cyber space application. Since, based on official documents, Afghanistan is in the process of integrating ICT into its critical information infrastructure, to this end, the country may face various challenges including cyber security. Due to various potential threats and risks to Afghanistan cyber security, a comprehensive cyber security strategy is necessary. Accordingly, Afghanistan has introduced an ICT security law. However, nowadays day by day internet is involving great portion of government and non-government sections. The country must introduce a comprehensive and appropriate cyber security strategy to tackle all of the issues and risks related to this arena. The aim of this study is to propose cyber security strategy based on developed countries experiences in cyber security, specifically Malaysia, because Malaysia and Afghanistan are both Islamic countries with cultural and religious values. Furthermore, Malaysia is considered as a developed country in terms of cyber security. Therefore, in this study, based on literature review and official documents, the current status of ICT as well as cyber threats were identified in Afghanistan context. In addition, to evaluate the current status of cyber security strategy in Afghanistan and Malaysia, some experts were interviewed and accordingly based on their suggestions and Malaysian experience in cyber security, a strategy framework was proposed for Afghanistan to address the ever-growing cyber threats. Then, the proposed cyber security strategy framework was evaluated by interviewing three experts in the field.

Keywords: *cyber space, cyber threat, cyber security, cyber security strategy*

INTRODUCTION

Cyber security strategy is regarded as an evolving task which caters to the entire spectrum of ICT users and providers such as home users and small, medium and large enterprises and government as well as non-government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. CSS framework allows the individual sectors and organizations to design appropriate cyber security techniques to satisfy their requirements in facing the cyber space challenges (Vernez, 2013). The strategy framework offers an overview of what is required to effectively protect critical national information infrastructure, information systems and networks, and also provides an insight into the government's approach for protection of cyber space in the country. In addition, it can be summarized that to some point, collaboration between public and private key players to safeguard the country's critical national information infrastructure, as well as information systems is allowed. Therefore, the strategy, aims to construct a cyber-security framework, leading to specific actions with programs to boost the cyber security of the country (Ten, Manimaran & Liu, 2010).

Given the importance of critical national information infrastructure for country development, different countries have cataloged and analyzed their relevant Critical national information including the protection of critical national information infrastructure (Fahad, 2010; OCED, 2012). Many national programs for the protection of critical infrastructure are

associated with critical information infrastructure protection (Hasim & Salman, 2011). Past studies highlight the relationships between protection of critical information infrastructure and ICT as a cross sectional matter, giving protection of critical national information infrastructure a special significance. However, to this end, there are some challenges specifically for the developing countries.

According to Walid (2013), there are four key challenges faced by the ICT sector in the Middle East that must be addressed in order to achieve the strategy goals:

1. Poor IT security infrastructure.
2. Minimal level of security procedures in corporations.
3. Gap between academia and industry.
4. Difficulty in attracting and retaining the ICT experts in the Middle East.

CASE STUDY OF AFGHANISTAN

Afghanistan as a developing Middle East country which in terms of cyber security is at its embryonic stage, needs cyber security strategy to survive in such competitive world. Correspondingly, MCIT Afghanistan (2011) quotes:

"*With the introduction of different ICT based technologies in the country, Afghanistan is moving towards embracing electronic culture in its day-to-day dealings. As these technologies are becoming popular and being widely used, it is important to put in place technological infrastructure and legal frameworks, which will safeguard the private and enterprise data flowing through these ICT based infrastructures. MCIT has already drafted an ICT law which has addressed broader cyber security related issues but in order to fully implement the Law there is need for further development of regulations in more focused areas*".

It also emphasizes that data privacy will support: Entrepreneurs for e-commerce; the government to run e-administration and e-services and the public in order to share their personal data with government as well as enterprises through e-service delivery channels. Correspondingly, according to The International Telecommunication Union (ITU) (2012) reports, Afghanistan has two challenging issues regarding cyber security. First, there is no appropriate mechanism in order to detect, identify and deter cyber threats and risks within government sectors. Similarly, some government agency computers are not equipped with suitable and reliable protection software, that is, antivirus, for blocking malware and viruses.

Furthermore, some government agencies state that they have never experienced any kind of cyber-attack, this can be associated to two possible issues, either they are not eager to share the information regarding attack, or they are unaware of the attacks. In addition, the country cyber network is much dispersed and spread, and this makes the detection of cyber-attack incidents is very complicated and difficult. In addition, no government agency appears to have any related information concerning cyber security policies or procedures which are in place. Also, no Government agencies are fully have any knowledge about numerous cyber security standards available that can be adopted to surge security, including COBIT, FISMA, ISO/IEC 27001, and ITIL.

Afghanistan needs a comprehensive CSS to tackle the cyber space security issues. Since, Afghanistan is in the process of integrating ICT into its critical information infrastructure, the country may face various challenges including cyber security. Due to various potential threats and risks, a comprehensive cyber security strategy is required for Afghanistan. However, Afghanistan has introduced an ICT security law, since internet has penetrated both the

government and non-government sectors with various cyber applications. Thus, the country must introduce a comprehensive and appropriate cyber security strategy to tackle all the issues and risks related to this arena. Therefore, the purpose of this research is to propose a cybersecurity strategy framework for Afghanistan to protect the country's critical national information infrastructure in the process of integrating ICT and cyber services in providing social and economic services.

METHOD

Some previous works have used qualitative approach including interview to develop a cybersecurity framework or provide suggestions for the improvement of the existing cyber security frameworks (ITU, 2012; Kulikova et al., 2012; Sommestad, 2012; OCED, 2012; ENISA, 2012; Lindau, K. 2012; Reyes et al., 2011) as shown in table 1.

TABLE 1. Research framework

Past Studies Qualitative Method in Literature

Researchers	Methods	Findings
Kulikova (2012)	Interview &Literature review	Proposed a cyber-security framework &validated testing, defining two security incident scenarios and interview
Sommestad (2012)	Interview &literature review	Framework used to develop a qualitative theory over cyber security to develop and validate framework
OCED (2012)	Open-ended questionnaire	Comparing the CSP/Strategy of ten countries and edification from 2005 to 2012 recommendation for promotion of their policy/ strategy
PWC: Research UK cyber security (2013)	Online survey &interview	Identifications of the current trends in UK cyber security adoption; the motivation for organization to do so; and constraints that inhibits investment in this area
ENISA(2012)	Survey& interview	The interview experience, recommendation for practices in developing , implementing evaluating and marinating cyber security policy/ strategy
Reyes et al (2011)	Interview and review of documents	Security of document

Research Framework of Cyber Security Strategy for Afghanistan

Literature Review and Documents Analysis

A: Body of knowledge on cyber space	B: Cyber security strategy	C: Case study of ICT in Afghanistan	D: Lesson From other countries
* Cyber space * Threat in cyberspace * Cyber Attack *Cybersecurity	* Review of global CSS * EU and non-EU Countries CSS *Common Themes	* Current Status of ICT in Afghanistan * Internet, Internet Service Provider * Cyber Space Threats in Afghanistan * ICT Law in Afghanistan	* Developed countries CSS * Malaysia Experience in cyber Security * Common Values of Malaysia & Afghanistan

Interview

A: Interview with Experts for Validating Research framework and Methodology	B: Interview with Afghan and Malaysian Experts to collect the research primary data	C: Interview With Malaysian Experts to validate the proposed CSS framework

Proposed Cyber security Strategy Framework for Afghanistan

Thus, this study also employs a qualitative approach using semi-structured interview to propose a cybersecurity strategy framework based on the cyber security experiences of the developed and developing countries including Malaysia. As a result of conducting a comprehensive literature review, cyber threats, cyber security, and global cyber security strategy are discussed. In addition, Afghanistan ICT status as well as cyber security are identified. The Malaysian experience in cyber security has also been highlighted. To identify the status of ICT and cyber security in Afghanistan and Malaysia, the people in charge were interviewed. Then, the threats to Afghanistan cyber space are highlighted. The Afghanistan cyber security strategy is then analyzed (but the country has only general ICT law). Finally, a cyber-security strategy framework is proposed for Afghanistan ICT context whose validity is corroborated by interviewing the experts in the field.

In qualitative studies where interview is the main method of data collection, the selection of the interviewee is of paramount importance (Creswell, 2012). The rationale is that the person who participates in the interview should have the necessary information to enable the researcher to explore the phenomenon deeply (Macky & Gass, 2005). In the current

research, eight experts and officials (four from Afghanistan and four from Malaysia) were interviewed. The respondents from Malaysia consist of the ICT and law experts. The purpose for selecting these experts was to check the validity of the study design and method. As there is a close relationship between cyber security strategy and law, their selection for validating the study design and mehod is rationalized. Another respondents who have involved in the ICT and cyber security research were recruited to answer the interview questions. The rational for their selection is that they have the latest information regarding cyber security policy/strategy in Malaysia. In addition, they are in charge of cyber security policy making and execution. Last but not least, four Afghan officials were interviewed to explore their knowledge and views concerning the latest status of ICT, cyber threat, cyber security, and cyber security Strategy. Since these people are the key figures and policy makers in cyber security, they make the appropriate sample for the current study.

RESULTS AND DISCUSSION

Based on the experiences of some developing and developed countries (Malaysia, India and the US), in terms of cyber security strategy, and also based on the findings of both document content analysis and interview, it is discovered that Afghanistan has a drastic development in terms of ICT services in the social and economic aspects during the last decade. However, it was found that although the country experienced cyber security problems, there is no cyber security strategy framework in place. Thus, Afghanistan, as an ICT emerging country, which is increasingly providing cyber-based services, needs a cyber-security strategy framework to address the challenges of cyber threats. Correspondingly, Afghanistan ICT Minister, Deputy ICT Minister and ICTI director confirmed that priority should be given to protect the government data and investment. Therefore, in this research, the main focus of the proposed cyber security strategy framework is to protect government data, foreign investment and Afghan citizen. Thus, the current research proposes the following pillars with their corresponding objectives illustrated as follow:

EFFECTIVE GOVERNANCE

According to ITU (2012), "Lack of problem scrutiny, misunderstanding as well as overlapping of resources accordingly losing sight of the all-encompassing national needs". "No government agency or department has any relation to information regarding cybersecurity related strategies or procedures that are in place". According to SATRC Report (2012), the focus of ICT law in Afghanistan is "Its mandate is to ensure information security in the country including all governmental data networks, transactions, cyber space, PKI, ECA, and to name a few". ICTI director declares that "*Afghanistan is at the beginning of the ICT journey and slowly the issues (including cybersecurity) are arising. There is a lack of strategy as the Ministry of Telecommunication has not given sufficient attention"*. According to the vice president of Cyber Security Malaysia it is important to have effective governance because without strategy and action plan, it is impossible to address this issue.

CULTURE OF SECURITY AND CAPACITY BUILDING

There is no awareness of common cyber security standards or regulatory frameworks in Afghanistan (ITU, 2012). According to Dlamini, Taute and Radebe (2011), "With respect to cyber security awareness programs, increased public awareness on cyber security issues, and fostering and funding cyber security research are included in the US national cyber security policy". In the contrary, according to the Minister of ICT of Afghanistan, "*Low literacy rate among population, especially in rural areas contributes to digital divide in the country… With*

the introduction of different ICT based technologies, Afghanistan is moving towards embracing electronic culture in its day-to-day dealings" Likewise, ICT Institute Director in Afghanistan claims that "… *regarding cyber security, it is a present challenge as well as a long term challenge, and it can be a big concern for government, people and the Ministry of Telecommunication"*.

SECURING E-GOVERNANCE SERVICES

Government agencies along with departments in Afghanistan are not aware of numerous cybersecurity standards and strategies, including ISO/IEC 27001, COBIT, FISMA and ITIL that can be adopted to upsurge security (ITU, 2012). This was confirmed by the Afghanistan ICT Minister, Deputy ICT Minister and ICTI director which then suggested that priority should be given to protect the government data and investment.

RESEARCH AND DEVELOPMENT TOWARDS SELF-RELIANCE

"*There is a gain in research and development (R&D) in cybersecurity experimentation methodology, infrastructure, tools, resource expansion, utilization innovations, and other new methods"* (Benzel, 2011). Strodl, Petrov and Rauber (2011) expound: *"the challenges related to the preservation of digital resources of increasing volume and heterogeneity by developing tools allowing for more efficiency and self-reliance of preservation processes".* Vice president of Cyber security Malaysia suggests "*research and development (R&D). You have to develop to research. Probably put under technology innovation... because you have to anticipate, to know the plan to address the issue*". In this vein, Minister of ICT *Afghanistan states "Active participation in forums, workshops, conferences and exchange of best practices would enable us in tackling these problems*".

CYBER SECURITY EMERGENCY READINESS

The boost of education and awareness is useful. The existing incident response center needs to be strengthened in order to be able to give the appropriate response (Hasim & Salman, 2011). Effective cybersecurity monitoring is not widespread across the critical national information infrastructures. Nevertheless, vigilant monitoring as well as correlation of data at the national level are critical elements to ensure that security incidents are being identified and managed appropriately. According to ITU (2012), "… w*ith the establishment of a crime investigation research team, knowledge of the available best practices with regards to cybersecurity standards could be implemented*". Deputy IT Minister claims that "…w*e are already facing problem because the cyber incidents since we looked at in 2010, 2011, 2012 are increasing. There are more cases that the ministry needs to look at. When more people are connected to the internet, there will be more privacy issues... The data center is specifically designed and it hosts the government digital data. All the websites that we have must be protected. We are working on the national cyber security strategic documents as well, but still at the beginning stage".*

INTERNATIONAL COOPERATION

The cyber environment is not limited to the physical boundaries of the countries. Therefore, successful cybersecurity initiatives require international cooperation (Hasim & Salman, 2011). Sharing research, best practice, intelligence, discussing challenges and learning from others' mistakes as well as assisting in formulating and driving international strategy direction along with initiative would help Afghanistan secure the critical national information infrastructures.

Dogrul, Aslan and Celik (2013) assert that it is rather hard to cope with the threat by means of merely 'national' cyber defence policies and strategies, since the cyberspace spans worldwide and attack's origin can even be overseas. ICTI director acknowledges that "… *we need a great team with international experienced in cyber security strategy to help us in crating strategy and strategy of cyber security".* The implication is that Afghanistan has no cybersecurity strategy which deal with international cooperation. Minister of ICT Afghanistan claims "… *Afghanistan is a landlocked country, providing international traffic and internet services to its residents through terrestrial connectivity of neighboring countries".* Afghanistan ICT director confirms by saying *"... of course some countries need to create strategy for cyber security. So strategies for national, regional and international cooperation are necessary".* Similarly Cyber security Director in Afghanistan asserts that "… w*hen it comes to international strategy, there is no such strategy or policy. What we have what you call it. Best practices are coming from other countries".* Vice president of Cyber security of Malaysia, states that one of the trust in our policy is international cooperation. That is very important because the cyber space is wireless.

TECHNOLOGY INNOVATION

Due to the dynamic nature of cyber threats and attacks, the governments are required to take appropriate measures to get along with the latest technologies useful for detecting and addressing cyber threats (Lynn, 2010). In order to keep updated with the latest findings in this field, research is mandatory (Hasim & Salman, 2011). The Minister of ICT, Afghanistan states that one of the objectives is to promote competitive protection measures for eliminating treats in cyber and delivery of quality services. Director of Cyber Security says that the public infrastructure specifically for the security purpose is paramount to secure their electronic ID card system. But since it is huge, so, we finally decided to not only work on the national ID project, but also provide a secure mechanism for e-mail exchange for the government, electronic certification authority, and digital certificates. Hence, it is recommended that Afghanistan adopst technology innovation to explore new cybersecurity initiatives and to stay ahead of cybersecurity threats.

PROTECTING PUBLIC HEALTH

According to EPHA (Endurance Public HealthAlliance), Europe (2013), the European Union (EU) and, in particular, the Commission's Directorate General for Health and Consumers (DG SANCO), works extensively in the area of health threats, seeking to protect European citizens from a range of risks and hazard, which cyber security concerns play a significant role". According to Afghanistan ICT Deputy Minister, "… *this office is looking from A to Z of whole frequency of what the ICT should be catching upon to the ICT in education, ICT in health, ICT for economic development, ICT for social benefits and all those in public services delivery , so that's what my office is looking after*".

PROTECTING CRITICAL INFORMATION INFRASTRUCTURE

According to the Ministry of Communication and Information Technology (MCIT) of Afghanistan, (2011), privacy of data would give confidence to:

1. entrepreneurs to do business in Afghanistan through e-commerce.
2. the government to rollout e-administration and e-services.
3. the public to share their personal data with both government and enterprises through electronic service delivery channels due to the importance of internationally recognized elements of critical national information infrastructure such as: Communication,

Emergency Services, Energy, Finance, Food, Government and Public Service, Public Safety, Health, Transport, Water and Defence.

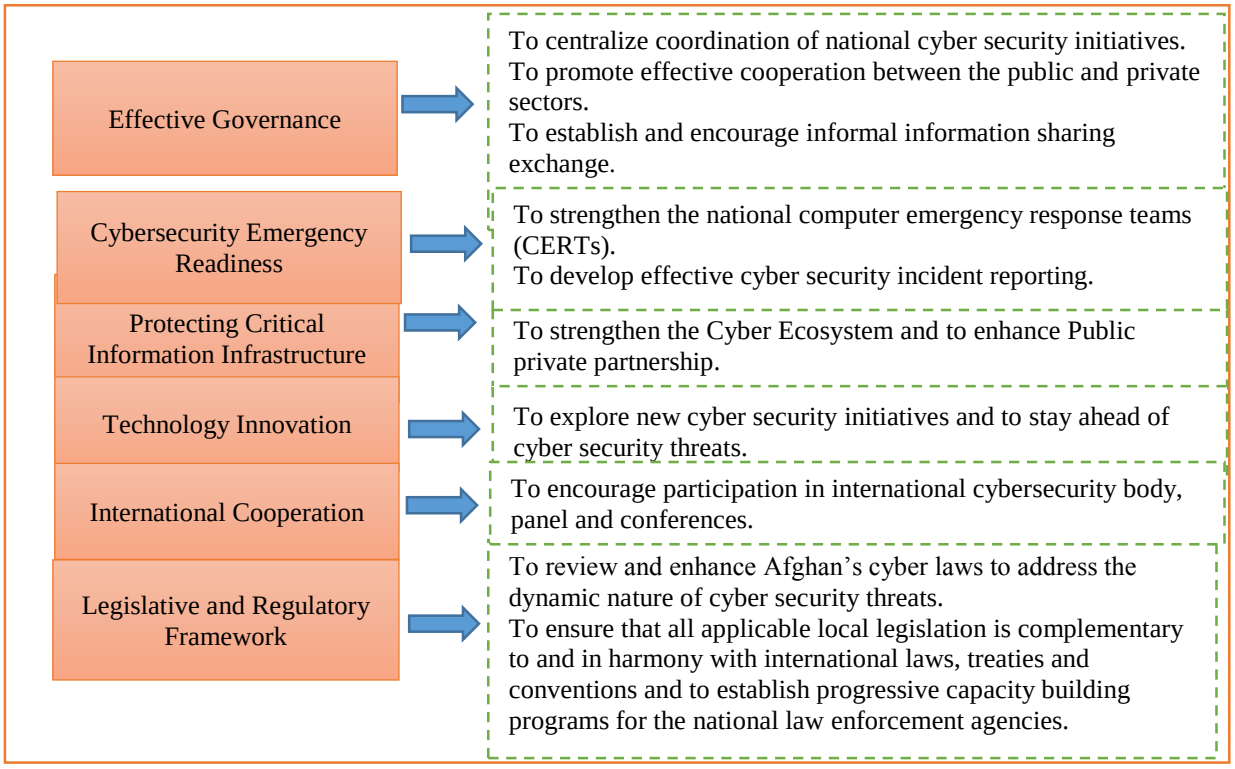
The Cyber Security Director states that private certification authority where all private banks or other entities will be willing to electronic transactions. They should be provided with security. These are the current infrastructures in place at the moment. The need is big since the ICT market is blooming day by day. In the era of technology, and e-government,it is crucial to protection the critical national information infrastructure (Luallen & Labruyere, 2013). Thus, it is inferred that Afghanistan needs to develop cybersecurity strategy to protect CNII, and accordingly to strengthen the cyber ecosystem and enhance public private partnerships.

LEGISLATIVE AND REGULATORY FRAMEWORK

The initiatives within this strategy is to define, categorize and penalize cybercrimes in order to deter future wickedness and malice to provide a general CSS framework for the country to have a suitable level of agreement to protect the critical national information infrastructure (Hamdard, 2012). The laws and regulations are important to produce trust and confidence in the critical national information infrastructure. Governments have to develop strategies against cyber-attacks and cyber threats, including legislative measures to protect themselves (Gurkaynak, Yilmaz & Taskiran, 2013). ICT Institute Director declares that cyber security strategy is the most important thing of all. Judges who are familiar with cyber strategy and law are required. If a cyber-security strategy is not in place, it is impossible to establish up cyber courts. This is a challenge which is difficult for the Ministry of Telecommunication to address shortly.

After conducting interviews with some Malaysian experts in ICT, cyber security and cybercrime namely, Vice President of Cyber Security Malaysia, Policy Study experts and Cyber Law experts, based on their suggestions, the number of pillars was reduced to six whose explanations are provided below. Therefore, it is crucial for Afghanistan to pass Legislative and Regulatory Framework to review and enhance Afghan’s cyber laws to address the dynamic nature of cyber security threats. Figure 2 illustrates the strategies with their corresponding objectives. In this study, initially, ten pillars of cyber security strategy were proposed.

TABLE 2. Cyber Security Strategy Framework for Afghanistan



In this study, the current status of ICT including the internet in Afghanistan was investigated and the threats to internet and cyber space were highlighted. The Afghanistan cyber security strategy was also examined and was discovered that Afghanistan has no cyber security strategy framework in place. This had led to proposing a general cyber security strategy framework.

Cyber space, cyber threats, cyber security, and global cyber security strategy in general were discussed based on the literature review prior to identifying the Afghanistan ICT status, cyber space and cyber security. To identify the status of ICT and cyber security in Afghanistan and Malaysia, the people in charge were interviewed after which the issues of and threats to Afghanistan cyber space were highlighted followed by analyzing the Afghanistan cyber security strategy. Finally, a cyber-security strategy framework with six pillars was proposed for Afghanistan ICT context whose validity was corroborated by interviewing the experts in the field. The findings of the current study could help Afghanistan develops or modifies the comprehensive cyber security strategy based on the experiences of the developed countries, thereby the country can address the issues of cyber security. The implication of this study is that the results can be used for assessing the current situation and developing a framework to national cyber security. Although this research has proposed a general cyber security framework for Afghanistan, it has not been evaluated through case studies. In fact, the evaluation was limited only to the views of three experts in the fields of cyber security and cyber ethics and law. It is suggested that for future research the proposed cyber security framework be tested in real situation.

REFERENCES

Benzel, T. 2011. The science of cyber security experimentation: the DETER project. *Proceedings of the 27th Annual Computer Security Applications Conference*. Orlando, Florida: ACM

Bjegovic-Mikanovic, V., Czabanowska, K., Flahault, A., Otok, R., Shortell, S., Wisbaum, W., & Laaser, U. 2014. Addressing needs in the public health workforce in Europe. European Observatory on Health Systems and Policies. Copenhagen: WHO-EURO.

Chander, M. 2012. National Critical Information Infrastructure Protection Centre (NCIIPC). Role, Charter & Responsibilities (Unpublished presentation). http://www.indiasmartgrid.org/en/Lists/Member/Attachments/19/ISGD%20Plenay%20III%20Muktesh%20Chander%20NCIIPC.pdf [May 9, 2014].

Dlamini, I. Z., Taute, B., & Radebe, J. 2011. Framework for an African policy towards creating cyber security awareness. Paper presented at *the 21st IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW)*, May 12th, Garborone, Botswana.

Dogrul, M., Aslan, A., & Celik, E. 201.1 Developing an international cooperation on cyber defense and deterrence against Cyber terrorism. Paper presented at the *Cyber Conflict (ICCC), 3rd International Conference on Cyber Conflict (ICCC)*, June 7-10, Tallinn, Estonia.

European Network and Information Security Agency (ENISA). 2012. *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*. Heraklion, Greece: ENISA.

EPHA. 2013. Cyber Security and Health Technologies Rue de Trèves, 49-51, 1040 Brussels, Belgium.

Fahad M. T. 2010. Dominant factors in national information security policies. *Journal of Computer Science*, 6(7): 808.

Gurkaynak, G., Yilmaz, I., & Taskiran, N. P. 2013. Governmental Efforts and Strategies to Reinforce Security in Cyberspace. *International Law Research*, 2(1):185.

Hamdard, J. 2012. *The state of telecommunications and internet in Afghanistan six years later 2006-2012*. USAID Assessment Report.

Hasim, M. S., Salman, A. 2011. Internet usage in a Malaysian sub-urban community: A study of diffusion of ICT innovation. *The Innovation Journal: The Public Sector Innovation Journal*, 16(2): 1-15.

ITU. 2012. *Readiness assessment for establishing a national CIRT (Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal*). Telecommunication Development Sector.

Kulikova, O., Heil, R., van den Berg, J., & Pieters, W. 2012. Cyber Crisis Management: A decision-support framework for disclosing security incident information. Paper presented at the International Conference on Cyber Security (CyberSecurity), Dec. 14th-16th Washington, DC.

Lindau, K. 2012. Cyber Security in Estonia: Lessons from the Year 2007 Cyber-attack. Master thesis, Tallinn University Institute of Informatics, Estonia.

Luallen, M. E., & Labruyere, J. P. 2013, January. Developing a critical infrastructure and control systems cybersecurity curriculum. *Proceedings of the System Sciences (HICSS), 2013 46th Hawaii International Conference on* System Sciences. Wailen, Hawaii: IEEE.

Lynn, W. J. 2010. Defending a new domain: The Pentagon's cyber strategy. In Cyberwar Resources Guide, Item #121. http://www.projectcyw-d.org/resources/items/show/121.[3 March 2014]

Mackey, A., & Gass, S. M. 2005. *Second language research: methodology and design*. New Jersey: Lawrence Erlbaum Associates.

Ministry of Communication and IT. 2011. *Report of e-Afghanistan National Priority Program Proposal*.

Ministry of Communication and IT, Afghanistan. 2013. Request for expressions of Interest (REOI including TOR) (Individual consultancy services).

OCED. 2012. Cyber security policy making at a turning point: Analysing a new generation of national cyber security strategies for the internet economy and non-governmental perspective on a new generation of national cyber security strategies: contributions from BIAC, CSISAC and ITAC.

Reyes, A., Brittson, R., O'Shea, K., & Steele, J. 2007. *Cybercrime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*. Rockland, MA:Syngress Publishing Inc..

SATRC Working Group on Policy and Regulations. 2012. *SATRC Report on Critical Information Infrastructure Protection and Cyber Security*.

Sommestad, T. 2012. A framework and theory for cyber security assessments. PhD thesis. Industrial Information and Control Systems KTH, Royal Institute of Technology Stockholm, Sweden.
Strodl, S., Petrov, P., & Rauber, A. 2011. *Research on digital preservation within projects co-funded by the European Union in the ICT programme*. Tech. Report.Vienna University of Technology.
Ten, C. W., Manimaran, G., & Liu, C. C. 2010. Cybersecurity for critical infrastructures: attack and defense modeling. Systems, Man and Cybernetics, Part A: Systems and Humans. *IEEE Transactions*, 40(4): 853-865.
Walid, al-Ahmad. 2013. A Framework for a Corporation Cyber War Strategy. Paper presented at *the 2nd International Conference on Informatics Engineering & Information Science in Malaysia (ICIEIS2013)*, Nov. 12-14, Kuala Lumpur.
Vernez, G. 2013. The Development of the Swiss Cyber Security Strategy. *Information Warfare*, 178.

Khosraw Salamzada
ICT Specialist
Ministry of Telecommunication and IT
Kabul, Afghanistan
kh.salamzada@gmail.com & salamzada.kh@icti.edu.af
Phone: (+93) 786191213
(Corresponding author)

Prof. Dr. Zarina Shukur,
Marini Abu Bakar
Research Center for Software Technology and Management
Universiti Kebangsaan Malaysia
zarinashukur@ukm.edu.my, marini@ukm.edu.my

Received: 17 August 2014
Accepted: 27 October 2014
Published: 27 February 2015