Journal of Digital Convergence
Vol. 17. No. 5, pp. 23-31, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.5.023

The Model to Implement the Cyber Security Policy and Strategy for Azerbaijan Information System

Leyla Mehdi Aliyeva[1], Gee-Hyun, Hwang[2*]
[1]Researcher, Ministry of Communications and High Technologies, Azerbaijan,
[2]Professor, Office of International Affairs/Graduate School of Information Science, Soongsil University

아제르바이잔 정보시스템에 대한 사이버보안 정책과 전략의 실행모델 구축

Leyla Mehdi Aliyeva[1], 황기현[2*]
[1]아제르바이잔 정보통신고등기술부 전임연구원
[2]숭실대학교 국제처 / 정보과학대학원 교수

Abstract This study aims to build an AHP model that evaluates the priority of cyber security policies for the Azerbaijan information system. For this, 4 factors were constructed from components of ITU National Interest Model, whereas 5 alternatives were based on the best practices of the eight developed countries leading the cyber security field. Using the questionnaire, 24 security experts evaluated the strategic priority of such factors or alternatives. The analysis results using the AHP software showed that homeland defense and economic well-being were the dominant aspects of cyber security policy, whereas capacity building and infrastructure were the main concern of cyber security elements for Azerbaijan. This study presents the strategic priority of cyber security policies that can be adopted by Azerbaijan government. This study can contribute to developing the national cyber security guide of Azerbaijan.

Key Words : AHP, Cyber Security, Decision Making, Policy and strategy, Azerbaijan

요 약 본 논문은 아제르바이잔 정보 시스템에 대한 사이버보안 정책 및 전략의 우선순위를 평가하는 실행모델을 구축하는 것을 목적으로 한다. 이를 위하여 ITU 국가 이익 모델로부터 사이버보안 정책 및 전략의 4 개 요인을 구성하고, 사이버보안 분야를 선도하는 8 개 선진국의 우수사례를 바탕으로 5개 사이버보안 대안을 도출한 AHP 연구모델이 제안되었다. 연구모델을 바탕으로 작성된 설문지를 사용하여 24명의 정보보안 전문가들이 각 요인 및 대안의 전략적 우선순위를 평가하였다. AHP 분석용 소프트웨어를 통해 분석한 결과 아제르바이잔 정보시스템의 사이버보안 핵심요인은 국토방위와 경제복지이지만, 이들을 구현하는 중요한 대안은 역량개발과 기반시설 분야로 판명되었다. 본 연구는 각 요인 및 대안의 중요도 분석을 통하여 아제르바이잔 정부가 채택할 수 있는 사이버보안 정책 및 전략적 우선순위를 제시하였다. 본 연구는 아제르바이잔이 국가 사이버보안을 강화할 수 있는 실행 가이드를 수립하는데 기여할 수 있다.

주제어 : AHP, 사이버보안, 의사결정, 정책 및 전략, 아제르바이잔

*This paper was prepared based on the first author's master thesis in Soongsil University.
*Corresponding Author : Gee-Hyun, Hwang(mike2030@ssu.ac.kr)
Received February 28, 2019 Revised March 25, 2019
Accepted May 20, 2019 Published May 28, 2019

1. Introduction

Internet is getting more important in our lives. This world has become global village. Internet is becoming necessity of life. Cyberspace brings us a significant opportunity for social development and economic growth. Increasing our reliance on cyberspace brings new opportunities but also new threats[1].

Recently, the number of the cyber-security threats has increased rapidly around the world. As a result of digitalization of society, Azerbaijan is also facing growing cyber-security threats[2]. The 2016 Azerbaijan first semiannual report shows that the general internet traffic, and also information infrastructures, networks, servers and internet resources of other public and private organizations have been attacked. As a result, attackers achieved to stop activity of resources, access to administration panel passwords, send spam emails from domain addresses, get access to the system as an administrator, access passwords of users of systems, steal confidential data, deface web sites and replace actual content with provocative content and publish confidential data on the web[3-5].

In this vulnerable cyber security environment, there is a urgent need for the existence of national policy and strategy to specifically guide the cyber security approaches within Azerbaijan. However, although Azerbaijan government currently has national strategies on developing information society, there is no any national cyber security strategy or policy document in legislation basis of Azerbaijan. In Azerbaijan, national cyber policy decisions were made without objective policy evaluation by stakeholders and cyber security experts. But, difficulties arise when many aspects need to be considered equally at the same time when making the best decisions to satisfy all stakeholders[6]. Therefore, different aspects of research should be considered properly for developing effective cyber security policy and strategy in Azerbaijan.

This research aimed to build an evaluation model for developing an effective cyber security policy and strategy in Azerbaijan. We identify elements of cyber security policy for Azerbaijan and develop an effective plan based on literature review in the field of cyber security. This study is focused on applying Analytic Hierarchy Process (AHP) tool to support cyber security policy decision making in relation to Azerbaijan information systems.

2. Cyber Security Policy

In this chapter, our research briefly describe important criteria and alternatives of national cyber security policy. The cyber security is defined as information technology security focused primarily on securing machines, networks, software and information from unauthorized access, manipulation, damage or destruction[7]. The role of cyber security is becoming increasingly important since many individuals, business organizations, and government agencies store, process and maintain their information and data in digital format which are shared by them using different types of information and communication technology(ICT) [8-11].

Statistics show that 22 percent of computers were infected by malware and used in different attacks in 2015,. During the last three years, some computers were infected by the critical threats which aim to steal bank account information of different countries. In 2017, more than 500 web sites were attacked by malicious users in Azerbaijan[3]. Therefore, cyber security plays a important role and should be considered the top priority in any country. There are many bodies in the cyber-security architecture of Azerbaijan. It is argued by Filipek[12] that cyber security policy should play an important role in

securing trust in the digital age and should be a national priority.

Cyber security policy must be strongly adhered so that each country and organization can recognize and prepare for different forms of growing cyber security threats in the future. Cyber security related literature describes various issues associated with cyber security policy, but any study has not been performed on evaluating cyber security policy and strategy for Azerbaijan information system especially using AHP method.

2.1 Cyber Security Aspects

The National Strategy for Development of Information Society in Azerbaijan between 2014 and 2020 considers all experiences and recommendations which have been made by ITU and the EU. The main aim of the Strategy is "to build an information society and efficient use of its capabilities by citizens, community and the state for the sustainable socio-economic, cultural and economic development of the country, including the development of ICT"[13,14]. The ITU model of National Interests describes four main national interests. Nations may justify the threat or use of military force to protect one of the following four national interests[15,16]. These four main interests have been chosen as the criteria of our research model.

Defense of homeland. Defense of homeland aspect of cyber security is the most important because countries must resist threats to their existence and territorial integrity at any cost. Cyber security is no longer a computer security rather it is a national security policy matter. Abnormal behavior of cyberspace can negatively affect public health, economic, safety and national security activities.

Economic well-being. Technology and cyberspace support the transition to economic measures. As online attacks increase the number of serious problems and economic damages in many countries, the economic welfare situation for action plans should be considered in cyber security policy.

Promotion of values. Cyber security policies may arise out the desire by nations to tackle cyber threats without losing attention on national values. Some of these factors are universal. For instance, the ITU Child Online Protection is prosperity because majority of stakeholders agree that there is need to provide children protection from injurious material and information to their well-being. Other values are country specific. For example, some governments may use cyberspace as the tool of encouraging national values such as democracy and other world rights.

Favorable world order. Favorable world order is a macro-national interest category. The case for a favorable world order covers the economic, social and diplomatic policies that a nation may establish to ensure that cyberspace and ICT promote their objectives and protect its interests in the group of states. Apart from developing national cyber security capabilities, Azerbaijan also works with other countries bilaterally, participates in intergovernmental organizations, and cooperates with global firms which specialize in cyber security.

2.2 Cyber Security Components

This study selected eight countries that have demonstrated a steady leadership when dealing with cyber crime. National cyber security policies of these eight countries have been researched and five key elements have been identified after combination and mapping procedure. They are capacity building, legislation, management, awareness and infrastructure [18]. Therefore, it was assumed that Azerbaijan should properly fulfill five components to achieve cyber security objectives across the country.

Capacity building. As emerging trends continue to evolve, security professionals will need to be

able to protect against threats that might exploit enterprises. So, it is important to continue to develop programs to help inspire a culture of security[18,19]. Training at all levels of the organization on security appropriate to their responsibility should be focused on both human and technical factors.

Legislation. Each country has a role to take some measures in the regulatory or legal field in order to clarify, improve, and enforce domestic laws related cyber crime. In this context, governments also have the responsibility to promote the interoperability over the legal frameworks developed by other countries [20].

Management. The challenges which are efficiently and globally spreading information related to exploits and threats are increased. Therefore, management aspect of cyber security are critical in ensuring information processing of a country or organization. Filipek [12] decribes that it includes data classification, access control, and so on.

Awareness. Awareness is a learning procedure that sets the ground for training by changing personal and organizational attitudes to accomplish the importance of security and the unfortunate consequences of its failure. This is explicitly required in all aspects of life. Enhancing cyber security awareness is a major goal for many governments or organizations, whereby greater awareness of the state of environments enables improved decision-making [21,22].

Infrastructure. Nowadays, the monitoring capabilities of information technologies and their providers are provoking a global crisis of confidence in both these technologies and the key players in the sector. Modern economies rely on the newly developed cyber infrastructures and assuring their security has become the top priority of many actors like governments, companies, etc.

3. Research Model

For implementing and evaluating cyber security policy and strategy, this study propose a conceptual research model in Fig. 1. This research model was constructed using 4 criteria and 5 alternatives introduced in Section 2. On top level, this study specifies the objective of our research which is Azerbaijan national cyber security policy and strategy(NCSPS) evaluation with respect to information system. The four main criteria of national cyber security policy and the five alternatives are prepared on the second and third stages. Four main criteria are taken from ITU National Interests Model, whereas 5 alternatives are identified by analysing different reports of 8 countries leading cyber security in the world. In order to evaluate priority of four criteria and five alternatives, this study use Analytic Hierarchy Process(AHP) developed by Saaty in 1977[23], which is well known as an excellent tool to find the solution of multi-criteria decision making problems.

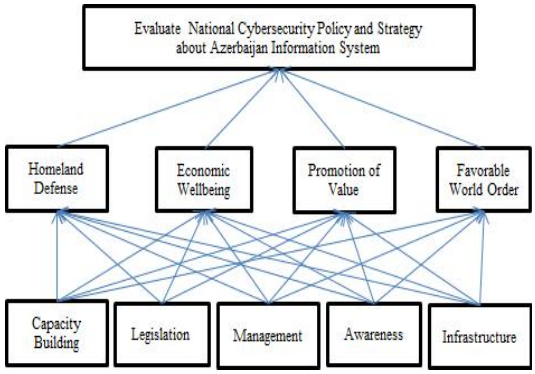

Fig. 1. Proposed NCSPS evaluation model.

3.1 Analytic Hierarchy Process

AHP is a hierarchically layered structure which is widely used, especially in military analysis[23]. It has attracted the interest of many researchers due to the nice mathematical properties of this method and the fact that the required

input data are rather easy to obtain. In particular, a complex decision questions with tangible and intangible factors are properly solved using AHP. In addition, decision makers enable to carry out both qualitative and quantitative analysis with AHP.

In general, AHP analysis process can be easily accomplished in four simple steps[24-26]. First of all, the problem is structured into hierarchy. This consists of decomposition into elements based on the nature and configuration of the problem. The AHP model comprises three levels such as goal, criteria and alternatives(see Fig 1). Second, a comparison is made between the elements of a specific level for a particular element in the immediate upper stage. The resulting weight of each element is named the local weight. Third, local weight of each element and consistency of comparison are calculated from the decision matrices by applying the eigenvector method. Last, the local weights across various levels are aggregated to get final weights of the decision-making alternatives.

3.2 AHP Evaluation model in Expert Choice

AHP analysis was performed using Expert Choice which plays a role of a multicriteria decision support system[24]. Except for various methods of decision analysis, Expert Choice is also free to use online. This makes the program more widely available. Expert Choice also performs AHP group decision analysis to ensure the sum of multiple decision-makers in a single decision-making process. Our AHP evaluation model is developed in Expert Choice as seen in Fig. 2.

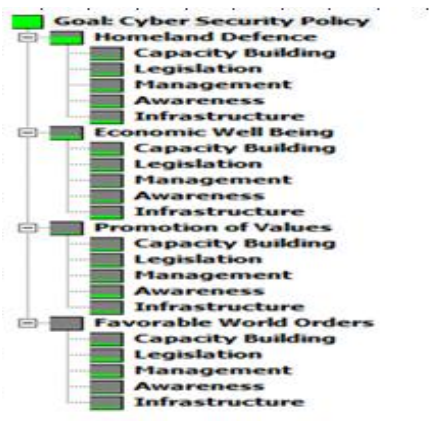

Fig. 2. AHP evaluation model in in Expert Choice

4. Data Analysis and Discussion

Data collected from professionals was analyzed using Expert Choice software which is digital interface for AHP. Considering data analys results and current status of information security in Azerbaijan, the researcher suggested action plans for development and implementation of national cyber security strategy which can be used by local government and other states by ensuring national cyber security policy priority.

4.1 Data Collection

The authors followed Delphi method which was formulated in order to get the most reliable opinion agreement of a group of experts by engaging them to a series of questionnaires in depth scatter with controlled opinion feedback. Therefore, the prepared questionnaire was sent to approximately 50 experts and 24 of them responded with their relevant feedbacks.

Given two options with respect to 'Homeland', the respondents can judge their relative importance as shown in Fig. 3. If the respondents think the option 'Capacity Building' in left column is moderately more important than the option 'Legislation' in right column, then they mark 3 with (x) on the left hand side. If they think the option 'Awareness' in right column is moderately more important than the option 'Capacity Building' in left column, then they mark 3 with (x) on the right hand side. The collected data was imported into Expert Choice software following the research model structure. Structure of questionnaire in Expert Choice is shown in Fig. 3.

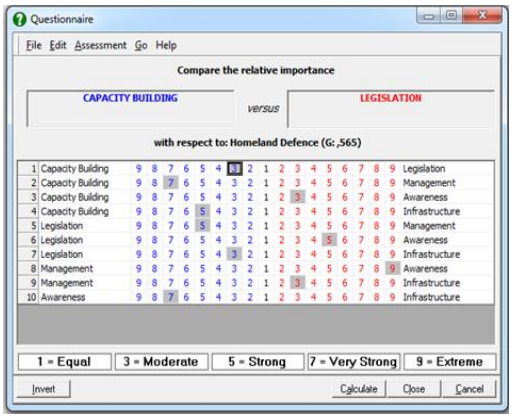

Fig. 3. The Questionnaire in Expert Choice

4.2 Data Analysis

4.2.1 Prioritization of Criteria.

As mentioned before, 'Homeland Defense' is the most important factor for developing an effective national cyber security strategy for Azerbaijan in terms of security. The data analysis result also shows that 'Homeland Defense' aspect has the highest value of 56.5% in Fig. 4. 'Economic Well Being' criteria value is 26.2%, followed by 'Promotion of Values' with 11.8% and 'Favorable World Order' by 5.5%. The overall cumulative inconsistency index is 0.04, showing that final results are reliable. Basically, inconsistency ratio should be less than 0.1 to be considered reliable[27,28].

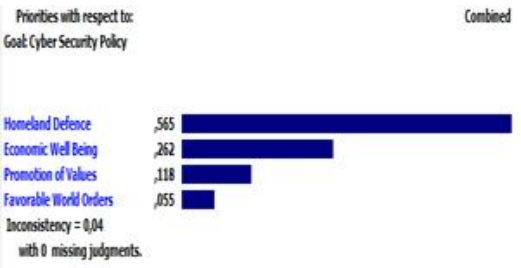

Fig. 4. Four main criteria in Expert Choice

4.2.2 Prioritization of Alternatives

The authors inserted all the response data into Expert Choice to analyze them on the AHP method. For prioritizing the key elements which are alternatives of our research model, we analyzed data based on four national interests like economic well-being, homeland defense, promotion of values and favorable world order. The analysis results are given with respect to each of four main criteria. As seen in Fig. 5 and Fig. 6, infrastructure constitutes 22.0% of all factors in homeland defense and its value is 25.8% on economy well-being aspect. infrastructure is the most important factor in terms of homeland defense and economic well-being.

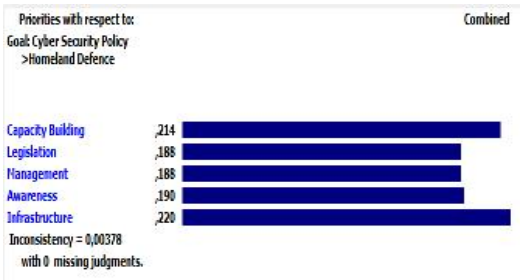

Fig. 5. Prioritization of alternatives w.r.t. Homeland Defense

In similar, awareness is the most important factor for promotion of values with value 28.3%. On the other hand, considering experts' feedback, legislation is very important with respect to favorable world orders with value 23.1%. Inconsistency for homeland defense is 0.004, economic well-being 0.003, promotion of values 0.009 and favorable world orders 0.002. As a consequence, we can consider these results reliable because all inconsistency indices are under 0.1.

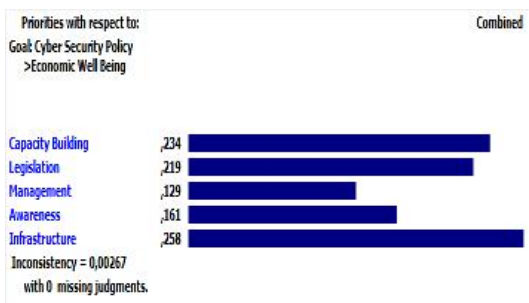

Fig. 6. Prioritization of alternatives w.r.t. Economic Well Being

4.2.3 Final Result

The final analysis was then performed in order to obtain composite overall priorities or global weight value as the final weight of alternatives. Such final analysis result is described in Table 1.

Table 1. Global weight Value

Goal	HD	EW	PV	FW	Overall
CB	0.121	0.061	0.019	0.012	0.214
LE	0.106	0.057	0.023	0.013	0.199
MA	0.106	0.034	0.017	0.012	0.169
AW	0.107	0.042	0.033	0.007	0.189
IN	0.125	0.068	0.025	0.011	0.230
Overalll	0.565	0.263	0.117	0.055	

Based on these analysis results, the authors discuss the key findings as follows. With respect to cyber security alternatives, infrastructure is considered to be the highest priority by Azerbaijan decision maker compared to capacity building, legislation, management, and awareness. It is found that infrastructure has accounted for 0.230, whereas capacity building, legislation and awareness, management have accounted for 0.214, 0.199, 0.189 and 0169 respectively.

In similar, it is found that homeland defense and economic well-being are regarded to be more important than promotion of values and favorable world order aspects. Azerbaijan government seems to put more weight on homeland defense and economic well-being aspects of cyber security which accounted for 0.565 and 0.263 respectively compared to promotion of values and favorable world order which only 0.117 and 0.055 respectively.

5. Conclusion and Discussions

This research applied AHP method to evaluate national cyber security policy and strategy in Azerbaijan. AHP provides a powerful and comprehensive approach for cyber security policymakers in both qualitative and quantitative methods as proven in this research.

This study have proved how AHP model can be applied to support cyber security policy maker evaluate cyber security policy and strategy implementation. From the viewpoint of cyber security aspect, homeland defense and economic well-being aspects are evaluated to be the most important factors compared to promotion of values and favorable world order aspects. In similar, from the perspective of cyber security component, infrastructure shows the highest priority in cyber security policy implementation followed by capacity building, legislation, awareness, and management.

This result shows the unbalanced approach of cyber security policy development in Azerbaijan government sector. The analysis results suggest that homeland defense and economic well-being aspects should be considered as more important issues in building a sound and effective cyber security policy implementations. Therefore, we confirm that these research findings are supporting the guide recommended by the ITU model of National Interests[12,15], which pointed out cyber security as one of the challenging decision-making issues to develop effective cyber security policy and strategy in Azerbaijan.

This study shows that the application of AHP resulted in clearly evaluating the performance of cyber security policy in Azerbaijan. Furthermore, the research findings enables us to suggest several implications for more improved implementation of Azerbaijan cyber security policy in the future.

Our study show that cyber security have the most influence on home defence and then economic welfare. Therefore, Azerbajan government need to enhance cyber security awareness among citizens and government officials. Some education and training programs associated with cyber security are required to advertise the contribution of cyber to home defence and economic welfare as well as to create sound security culture nationwide.

The close relationship between home defence and cyber security are very clear and well understandable. However, economic welfare aspect of cyber security need to be emphasized as one of critical factors for Azerbaijan government or citizens in recent information age.

Capacity building and infrastructure should be balanced with legislation, awareness, and management, particularly in the area of information exchange or business transaction between government agencies and private businesses. Therefore, the latter three factors should be improved in Azerbaijan cyber security policy and strategy planning and implementation. Last, Azerbaijan government should periodically review the performance of cyber security policy and strategy implementations using AHP evaluation model proposed in this research[28].

This study recommends that Azerbaijan would strength both infrastructure and capacity building in order to efficiently implement national cyber security policy and strategy. With respect to infrastructure, it is recommended that Azerbaijan might make more improvement in the background information management on major incidents, the cyber security architecture of the country, the financing on information security, the information sharing mechanisms, etc. Then, it is required to enhance security awareness through cyber security education and training of citizens as well as trust and working culture.

For future study, one of the major ramifications of this convergent study is that the research method, approach and its results can serve as a framework for other countries, especially CIS(Commonwealth of Independent States) countries. For example, Uzbekistan and Kazakhstan are trying to introduce smart cities and cyber security systems, whereas Azerbaijan is operating government data centers. Azerbaijan started international cooperation with computer emergency response teams of more than 20 countries, such as Georgia, Czech Republic, Lithuania, Latvia, Russia, Ukraine, Kazakhstan, and so on. In this case, comparative studies of such countries can identify similarities or differences between different countries or groups.

Finally, the research procedures and methods used to derive 4 factors and 5 alternatives of our research model and their reliability and validity are also required to be described more in detail in the follow-up study.

REFERENCES

[1] S. T. K. Myo & G. H. Hwang. (2017). Effect of Mobile Devices on the Use Intention and Use of Mobile Banking Service in Myanmar. *Journal of Digital Convergence, 15(6),* 71-82.

[2] K. Makili-Aliyev & Rehman. (2013). A. Cyber-Security Objective: Azerbaijan in the Digitalized World. *SAM Review,* 5-27.

[3] CERT.az(2017). *About us. Retrieved from Cyber Security Center.*
DOI : https://www.cert.az/en/about-us

[4] H. J. Mun, Y. C. Hwang, & H. Y Kim. (2015). Countermeasure for Prevention and Detection against Attacks to SMB Information System - A Survey. *Journal of IT Convergence Society for SMB, 5(2),* 1-6.

[5] K. B. Kim & J. Y. Yun(2015). Comparison and Analysis on Mobile Payment in terms of Security : Survey. *Journal of IT Convergence Society for SMB, 5(3),* 15-20.

[6] I. Syamsuddin & J. Hwang. (2008). The Application of AHP to Evaluate Information Security Policy Decision Making. *IJSSST, 10(4),* 46-50.

[7] UMUC. (n.d.). *Cyber Security Primer.*
DOI : http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm#

[8] K. K. Seo(2016). Analysis of use intention of mobile cloud service using a convergence technology acceptance model. *Journal of Digital Convergence, 14(12),* 105-110.

[9] S. H. Kim & J. S. Han. (2014). Smart Cold-Chain Monitoring Automation System Architecture based on Internet of Things. *Journal of digital convergence, 12(12),* 351-356.

[10] J. H. Cho &, H. J. Lee(2018). A Study on the Real-time Cyber Attack Intrusion Detection Method. *Journal of the Korea Convergence Society, 9(7),* 55-62.

[11] S. H. Hong & J. A. Yu(2018). Ransomware attack analysis and countermeasures of defensive aspects. *Journal of Convergence for Information Technology, 8(1),* 139-145.

[12] R. Filipek. (2007). Information security becomes a business priority. *Internal Auditor, 64(1),* 18.

[13] N. Orujova. (2014). *Information Society Strategy to be implemented in two stages..* DOI : https://www.azernews.az/business/65843.html

[14] C. H. Yoon & G. D. Choi. (2014). The Effects of National Culture on Ethical Decision-Making in the Internet Context : An Exploratory Analysis. *Journal of digital convergence, 12(12),* 23-36.

[15] F. Wamala. (2011). *The ITU National Cybersecurity Strategy Guide.* ITU.

[16] S. H. Lee & D. W. Lee. (2014). A Study on Internet of Things in IT Convergence Period. *Journal of digital convergence. 12(7),* 267-272.

[17] L. Aliyeva. (2018). *Developing An Effective National Cyber Security Strategy For The Republic of Azerbaijan.* Master Thesis, Soongsil University, Seoul.

[18] ISACA. (2015). State of Cybersecurity : Implications for 2015. *CyberSecurity Nexus, 22.*

[19] L. S Kim. (2015). Convergence of Information Technology and Corporate Strategy. *Journal of the Korea Convergence Society, 6(6),* 17-26.

[20] OECD(2012). Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies. *OECD Digital Econmy Papers, 212.*

[21] L. S. Kim. (2015). Convergence of Information Technology and Corporate Strategy. *Journal of the Korea Convergence Society, 6(6),* 17-26.

[22] Z. Yunos, R. S. A. Hamid & M. Ahmad. (2016). Development of a cyber security awareness strategy using focus group discussion. *SAI Computing Conference (SAI),* 1063-1067.

[23] L. Saaty. (1990). *The Analytic Hierarchy Process.* RWS Publications, Pittsburgh, PA.

[24] F. Zahedi. (1986). The analytic hierarchy process—a survey of the method and its applications. *Interfaces, 16(4),* 96-108.

[25] H. T. Choi. (2018). Analysis of policy priorities for strengthening the capacity of local public officials. *Journal of the Korea Convergence Society, 9(11),* 345-351.

[26] C. J. Yoon, C. G. Hwang, H. G. Kwon & M. Y. Won. (2018). Study on Political Factors for Innovating Textile and Fashion Industry in Northern Gyeonggi Province. *Journal of Convergence for Information Technology, 8(1),* 253-263.

[27] H. F. Ernest, T. L. Saaty, A. Mary & W Rozann. (1983). *Expert Choice – Decision Support Software.* McLean, VA,

[28] B.C. Kim. (2015). A Internet of Things(IoT) based exploration robot design for remote control and monitoring. *Journal of digital convergence, 13(1),* 185-190.

Leyla Mehdi Aliyeva [정회원]

· 2018년 2월 : 숭실대학교 정보과학대학원 글로벌ICT융합학과 졸업(공학석사)
· 2018년 3월 ~ 현재 : 아제르바이잔 정보통신부 사이버보안센터 연구원 근무
· 관심분야 : 사이버보안, 전자정부 등
· E-Mail : eyla.aliyeva@cert.az

황 기 현(Hwang, Gee-Hyun) [정회원]

· 1987년 2월 : 한국과학기술원 산업공학과 졸업(공학석사)
· 1997년 12월 : 영국 버밍험대에서 공학박사 취득(TQM and SCM)
· 2010년 9월 ~ 현재 : 숭실대 국제처 / 정보과학대학원 교수 재직 중
· 관심분야 : 국제개발협력, TQM, SCM, ICT융합 등
· E-Mail : mike2030@ssu.ac.kr