Journal of Digital Convergence
Vol. 17. No. 10, pp. 93-102, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.10.093

Analysis of Strategic Priorities for Strengthening Cybersecurity Capability of Cambodia

Mara Heng[1], Gee-Hyun, Hwang[2*]
[1]Ministry of Information, Communications and Technology, Cambodia,
[2]Office of International Affairs/Graduate School of Information Science, Soongsil University

캄보디아의 사이버보안 역량강화를 위한 전략적 우선순위 분석

Mara Heng[1], 황기현[2*]
[1]캄보디아 정보통신기술부 사무관
[2]숭실대학교 국제처 / 정보과학대학원 부교수

Abstract This paper aims to set the priorities for the cybersecurity strategy of Cambodian government. To this end, we built a AHP research model by adopting 4 factors from the ITU national interests model and selecting 7 strategies from best practices of 8 countries leading the cyber security. Using a questionnaire, 19 experts evaluated Cambodia's cybersecurity strategy priorities. The key policy factors were evaluated in the order of homeland defense, economic welfare, value promotion and favorable world order. Their strategic alternatives were identified in the order of legislation, capacity building, and cyber attack prevention for critical infrastructure. This study will contribute to setting the strategic priorities and feasible action plans to strengthen Cambodia's cybersecurity capabilities.

Key Words : AHP, Cyber Security, Capability, Strategic Priority, Cambodia

요 약 본 논문은 캄보디아 정부의 사이버보안 전략의 우선순위를 결정하는 것을 목적으로 한다. 이를 위해 ITU 국가 이익 모델에서 사이버보안의 4개 정책요인을 채택하고, 그 다음에는 사이버보안 분야를 리드하는 8개 선진국의 우수사례를 벤치마킹하여 도출한 7개 실행전략 대안으로 AHP 연구모델을 수립하였다. AHP 연구모델을 바탕으로 설문지를 작성하고 19명의 전문가들이 캄보디아의 사이버보안 전략의 우선순위를 평가하였다. 데이터 분석 결과 캄보디아 정부의 사이버보안 핵심 정책요인은 국토방어, 경제복지, 가치증진 및 유리한 세계질서 순으로 평가되었으며, 이들을 구현하는 주요 대안은 사이버보안 법제화, 역량개발, 중요 정보 인프라에 대한 사이버 공격 방지 순으로 판명되었다. 본 연구는 캄보디아 정부의 사이버보안 역량을 강화할 수 있는 전략적 우선순위와 실행계획을 수립하는데 기여할 수 있다.

주제어 : AHP, 사이버보안, 역량, 전략적 우선순위, 캄보디아

1. Introduction

Since the Information revolution, Information Communication and Technology(ICT) has been acknowledged as an important driving force in all areas of development for the decades. ICT is

*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 September 9, 2019 Revised September 26, 2018
Accepted October 20, 2019 Published October 28, 2019

an engine of growth of the major economic sectors and an enabler to increase the competitiveness of other industries[1]. In all areas, ICT changed the way individuals, companies and countries work around the world. Moreover, ICT has played an essential role in human society as well. At the same time, we can expect to see the emergence and growth of cybercrime and other information security concerns. Therefore, ICT security or cyber-security has become a critical factor for using ICT.

Today cyber-attacks are becoming more sophisticated and more difficult to detect and defend against them. Therefore, many countries prioritize cyber security as part of national security. In Cambodia, cyber attacks are growing rapidly and do a lot of damage nationwide. For example, some Cambodian government websites are under attack by anonymous groups. The hacktivist does its work using methods such as distributed denial of service(DDoS) attacks, website corruptions, redirects, information theft, website parodies, and so on.

Among them, Cambodia is mainly suffering from DDoS attacks and website defacement attacks. Moreover, there were several reports on spam mail, malicious viruses spreading, spyware, phishing, scam mail from the internet users, and also the efforts of young geek showing their attacking skill. Therefore, cybersecurity issues should be the most important point[2,3].

Although a number of cybercriminal have occurred in the recent years, there isn't any law and regulation or official national cybersecurity strategy for combatting cybercrime in Cambodia[4]. Any study on the cyber security strategy has not been undertaken in Cambodia. This study aims to identify and prioritize the elements necessary for developing the desired national cybersecurity strategy for Cambodia.

2. Research Background

2.1 Cyber Security Strategy in Cambodia

Cybersecurity is information technology security that focuses primarily on protecting machines, networks, software and information from unauthorized access, manipulation, damage or destruction [5,6]. The role of cybersecurity is getting more and more important. The reason is that many individuals, businesses, and government organizations store, process and keep information and data arranged in digital format that are shared by them[6-9].

On the other hand, Cambodia's economy keeps growing at a fast pace and more financial institutions are expanding into the digital space, it is time for companies to tighten their IT security to prevent their data from being stolen by hackers. For example, it is warned that the DDoS attack in early November, 2018 where several major Internet service providers (ISPs) were victims and overall, the internet speed in Cambodia was also impacted could recur if steps are not taken to improve network and IT security in the nation[2].

In Cambodia, as the urgency is mounting, plans are being laid to strengthen national cybersecurity as well as protect against cyberattacks, with the government identifying cybersecurity as one of five priority areas to develop. However, there are some major concerns or obstacles for Cambodia's future cybersecurity development. The most serious obstacle is the lack of necessary budget, laws and regulations and ICT systems and services. Another barrier is the lack of essential physical and social infrastructure, ICT security professionals, and human resources development.

The Cambodia's ICT Masterplan 2020 aims to address her capacity for dealing with cybercrime and seeks to develop cybersecurity measures across all sectors and organisations in order to better counter the ever-evolving threats. It will call upon businesses, institutions and governmental agencies to apply best practices so as to avoid disaster.

According to Cambodia's government, in 2018 alone, the nation witnessed 4,590,076 online cyberattacks that affected 30.5 percent of internet users, an increase of 2,835,938 from 2017's attacks. This is in line with regional and global trends, but as the prevalence of cybercrime grows, many fear that governments, businesses and individuals are unprepared for the impact of these attacks. So, cyber security plays a significant role and should be considered as a top priority in all countries[2].

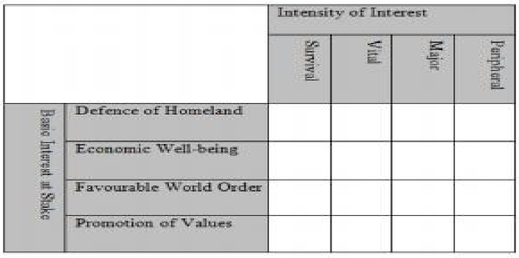
Noting that phishing scams, malware and DDoS attacks were all on the rise in Cambodia, the Cambodian Government is trying to push for greater co-operation between Asia-Pacific nations to enhance capacity, co-ordination and capabilities to deal with new cyber challenges as they arise. In spite of her effort, Cambodia is ranked 125th in the world and 15th in Asia Pacific region. This means that Cambodia is vulnerable to cybersecurity due to weaknesses in technical, human, organizational and regulatory factors [4].

On the other hand, Cambodia has not built national government roadmap for cybersecurity. There is no any officially recognized national cybersecurity strategy. If cyber attacks continue, it could also stifle Cambodia's digital transformation ambition which she hopes to achieve by 2030 - to empower society with more digital tools. It is therefore necessary to build a flawless cybersecurity roadmap for Cambodia. Cyber security policy must be strongly adhered so that Cambodia's government can recognize and get ready for different forms of cybersecurity threats in the future.

2.2 ITU National Interest Model

National interests of each country come from their national values, guiding their political decisions. It is very important to realize the interests of the nations, which leads to the achievement of such goals as security and stability of the nation, economic prosperity, superior international order and securing of individual freedom[6,10]. The nations protect their national interests by mobilizing all the tools and machinery of their national powers. The failure of this approach to secure national interests threatens national values.

The ITU model of national interests specifies four national basic interests such as homeland defense, economic well-being, promotion of values and favorable world order Fig. 1. Their reliance is main duty of government as well as all national security bodies[10]. The countries possibly will justify the threat or usage of military power to secure one of four national interests[10,11].



		Intensity of Interest			
		Survival	Vital	Major	Peripheral
Basic Interest at Stake	Defence of Homeland				
	Economic Well-being				
	Favourable World Order				
	Promotion of Values				

Fig. 1. ITU Model of National Interests.

Among four national interests, homeland defense is of the utmost importance because at any cost, the country must resist any threats to their presence and territorial integrity. Cyber security is no more computer security, but a matter of national security policy. For example, Canada referred to the secure government system, the first pillar of domestic cyber policy, as "the government will act to protect Canada's cyber sovereignty and protect and develop our national security and economic interests"[12]. As a result, normal behavior in cyberspace can have a positive influence on public health, financial safety and national security activities.

With regard to economic well-being, ICT should be of great importance to all participants in the modern economy. If information is not properly distributed, the entire economic sector, such as finance, wholesale and retail, transportation, manufacturing, and many service industries, is vulnerable. Without computers, crawling will be slow or impossible[13]. Therefore, economic well-being is essential as modern cyber attacks incur serious economic damage that cannot be quantified. Many countries, such as Cambodia, Australia, Estonia and New Zealand, believe that cyber threats greatly threaten economic growth and national competitiveness [10].

Third, every country has its own social value. The promotion of value is considered so that the outcome can be adjusted according to the social values of the country. Some of these factors are universal. A good example is ITU Child Online Protection. This is because most stakeholder agree to protect children from harmful information and materials. Other values vary by country. South Korea and Hong Kong, for example, use cyberspace as a tool to promote national values such as democracy and civil rights[6].

Last, the favorable world order is a macro national interest category. It deals with the economic, social and foreign policies that nations can ensure that cyberspace protects its benefits in the national community. In addition to developing national cyber security capabilities, Cambodia also works with other nations, participating in intergovernmental organizations, and with global companies specializing in cybersecurity.

2.3 Benchmarking Cyber Security Strategy

This study benchmarked eight countries that showed consistent leadership in dealing with cybercrime. The national cybersecurity strategy in these countries was studied and compared through a combination and mapping procedure, and 15 elements were identified. In a more in-depth analysis, seven of them were selected, which share the same view in eight countries[2]. The seven key elements in Table 1 are considered the basis of Cambodia's cybersecurity strategy.

First of all, the top priority is to develop an appropriate legal framework to ensure information security. The eight countries serve to take some action in the field of regulation or law to clarify, improve and enforce domestic cybercrime laws. In this aspect, governments are responsible for promoting interoperability with legal frameworks introduced by other countries[14].

Table 1. Seven Selected Key Factors

Key factors	Code
To develop an appropriate legal framework to ensure information security	DLF
To enhance cybersecurity awareness and capacity building	EAC
To enhance organizational structure	EOS
To ensure cybersecurity through cooperative effort	ECE
To guarantee public safety and improve public-private partnership	PPP
To prevent cyber-attacks against critical information infrastructure	CII
To tackle cybercrime	TTC

The second priority is to enhance cybersecurity awareness and capacity building. As new trends continue to evolve, security professionals will need to protect their businesses from threats that could exploit them. Therefore, it is important to keep developing programs that help inspire a culture of security[15-17]. Training on security that is appropriate for accountability at all levels of the organization should focus on human and technical factors. Increasing awareness of cybersecurity is a major goal for many governments or organizations, and raising awareness of environmental conditions improves decision making [18,19].

The third priority is to enhance organizational structure and capacity. Cybersecurity is everyone's responsibility[15,20]. The board and senior management should set the priorities and form the culture, but even the lowest level employees must play their part in keeping the organization safe. However, it is also important for the organization to appoint someone responsible for these efforts. In most organizations, this person is the Chief Security Officer (CSO) or Chief Information Security Officer (CISO). This person should closely run the General Counsel (GC) to insure that the organization's cybersecurity protocols satisfy its legal requirements[21].

The forth priority is to ensure cyber security through both international and national cooperation. Eight developed countries work bilaterally with other countries, participates in inter-governmental organizations, and work with global companies that specialize in cyber-security. Each country also works with computer emergency response teams in other countries.

The fifth priority is to guarantee public safety and improve public-private partnership. To achieve public-private partnership in each developed country, the cyber security center acts as a coordinating body in the area of cyber security. This center should serve as a bridge connecting businesses, internet providers, law-enforcement institutes and the general public. The center should work with national internet providers to investigate cybersecurity law violations in order to maintain a safe digital space in the country[21,22].

The six priority is to prevent cyber-attacks against critical information. Security greatly contribute to protecting the economies or businesses as an infrastructure of the modern economy, so that security is a top priority for many actors such as governments, companies, etc[13,22]. The reason is that the difficulty lies in prohibiting cyber abuse and excesses, and also in managing incidents and even crises that may occur. The other difficulty lies not only in protecting citizens, children, consumers, digital heritage, and secrets, but also in expressing our requirements for cyber security and building the rights and obligations of actors, and assuring that they are respected[10].

The seventh priority is to tackle cybercrime. Our society is increasingly dependent on electronic networks and information systems. Advances in ICT have resulted in criminal activity that threatens citizens, businesses, governments, and major infrastructure. Cybercrime consists of criminal acts committed online using electronic communication networks and information systems. It's a borderless issue that can be categorized into three broad definitions: Internet-specific crime, online fraud and counterfeit and illegal online content. For example, to combat cybercrime, the EU has enforced legislation and supported operational cooperation as part of its EU cybersecurity strategy[10].

3. AHP Research Model Design

Analytic Hierarchy Process(AHP) developed by Saaty in 1977[23], is a multi-layered structure which is widely used in determining priority and weight of strategic issues[23]. AHP properly solves complex decision-making issues about tangible and intangible factors by performing a set of pairwise comparison. In particular, AHP contributes to subdividing and stratifying the atypical and multi-layer complex problem into sub-criteria. In addition, AHP enables to measure information about decision making process on a ratio scale through qualitative and quantitative criteria[6].

As a means of guiding cyber security roadmap, this research propose a AHP research model in Fig. 1. This study model was suggested using four criteria and seven alternatives described in Section two. On top level, this research states final objective of our study which is focusing on determining priority of Cambodian national cyber security strategy for information system. The four key criteria of national cyber security strategy and the seven alternatives are suggested on the second and third layers.

Four key criteria such as defense of homeland, economic well-being, promotion of values and favorable world order are chosen from the ITU National Interests Model. On the other hand, seven alternatives are selected by analysing various reports of 8 countries that are leading cyber security in the world. They are legal framework, cybersecurity awareness and capacity building, organizational structure, cooperative effort, public-private partnership, information infrastructure and cyber crime resolution[16,24]. In order to assess priority of four criteria and seven alternatives, this research uses AHP as an excellent tool to solve multi-criteria issues.

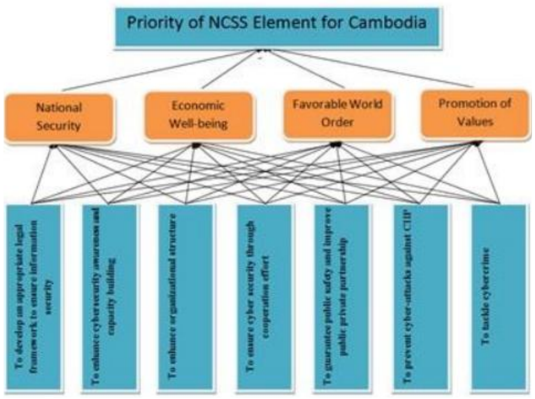

Priority of NCSS Element for Cambodia
National Security
Economic Well-being
Favorable World Order
Promotion of Values
To develop an appropriate legal framework to ensure information security
To enhance cybersecurity awareness and capacity building
To enhance organizational structure
To ensure cyber security through cooperation effort
To guarantee public safety and improve public private partnership
To prevent cyber-attacks against CIIP
To tackle cybercrime

Fig. 2. Proposed NCSS evaluation model.

4. Data Analysis Results

Data collected from nineteen experts was analyzed using Expert Choice 2000. Based on data analysis results and current status of information security in Cambodia, this study guides action plans for developing and implementing national cyber security strategy. This can be applied to local government and other states by assuring national cyber security strategy priority.

4.1 Data Collection

In order to assess the relative importance of the AHP model for strengthening Cambodia's cybersecurity capabilities, this study followed Delphi method which was formulated in order to get the most reliable opinion agreement of a group of cybersecurity experts by engaging them to a series of questionnaires in depth scatter with controlled opinion feedback.

The prepared questionnaire was sent to forty cybersecurity experts working for Cambodia's finance, education and IT organizations in both private and public sectors. The number of respondents was determined in a larger scale, assuming that approximately 50% of them would successfully participate in multiple surveys over a long period of time. The surveys were conducted several times via email and facebook between July 20 and August 30, 2017. Finally, nineteen cybersecurity experts responded with their relevant feedbacks.

This study inserted all response data into Expert Choice for AHP analysis. The nineteen experts consist of 76% of the men and 24% of the women. 74% of respondents are working in the government sector with 26% of them in the private. Their positions include 5 experts, 4 heads, 3 managers, 3 lawyers in the cybersecurity field and 4 others from information technologies. The respondent's experiences are distributed as 32% of respondents for 5 to 10 years, 21% for 10 to 15 years, 21% for 3 to 5 years, 5% for 15 to 20 years, 5% for more than 20 years, and 16% for others.

4.2 Data Analysis

4.2.1 Overall Result

Homeland defense is the most critical factor to achieve the successful implementation of national cyber security strategy in Cambodia.

The data analysis results also show that the home defence aspect has the greatest value of 44.5%. ‘Economic Well Being’ aspect is 29.3%, followed by ‘Promotion of Values’ for 18.2% and ‘Favorable World Order’ by 8.1%. The total cumulative inconsistency ratio is 0.02, showing that this research results are reliable to be implemented in a real environment. Basically, inconsistency index should be lower than 0.1 to be reliable[23,25].

4.2.2 Prioritization of Alternatives

To prioritize key alternatives in this research model, we analyzed the data based on four national concerns: economic well-being, homeland defence, promotion of values and favorable world order. Both legal framework for information security and national security, and cybersecurity awareness and capacity building are the most important factors in four criteria.

The analysis were carried out for each of four main criteria. Firstly, with regard to homeland defense, the top priority factor is to develop an appropriate legal framework to ensure information security(DLF), which constitutes 21.7% of all factors as seen in Table 2. Second, to enhance cybersecurity awareness and capacity building(EAC) accounts for 15.7% of total. Third, to prevent cyber attack against critical information infrastructure(CII) represents 15.4% of total. The total cumulative inconsistency ratio 0.00452, showing that the analysis result is reliable.

Table 2. Prioritization of alternatives for each criteria

	Defense of Homeland	Economic Wellbeing	Promotion of Value	Favorable World Order
DLF	0.217	0.155	0.193	0.154
EAC	0.157	0.203	0.155	0.113
EOS	0.142	0.150	0.132	0.133
ECE	0.122	0.103	0.102	0.125
PPP	0.101	0.150	0.149	0.143
CII	0.156	0.141	0.151	0.182
TTC	0.104	0.098	0.118	0.151
Inconsistency	0.00452	0.00181	0.00354	0.00252

With respect to economic well-being aspect, the top three priority factors are to enhance cybersecurity awareness and capacity building factor(EAC) weighted by 20.3% of total, followed by developing an appropriate legal framework to ensure information security factor(DCF) and enhancing organizational structure factor(EOS) (16.1%). The perspective of the experts in economic well-being aspect is acceptable because inconsistency is 0.00181.

For the promotion of value aspect, the top priority is to develop an appropriate legal framework to ensure information security factor(DCF)(18.2% of total), followed by to enhance cybersecurity awareness and capacity building factor(EAC)(15.4%). To prevent cyber-attacks against critical information infrastructure(CII) is the third priority(15.3%). The perspective of the experts in Promotion of Value aspect is acceptable because inconsistency is 0.00354.

Last, with regard to favorable world orders, the top priority is to prevent cyber attack against critical information infrastructure represents(CII) which constitutes 18.2% of all factors as seen in Table 2. Second, to develop an appropriate legal framework to ensure information security(DLF) occupies 15.4% of total. Third, to tackle cybercrime(TTC) accounts for 15.1% of total. The total cumulative inconsistency ratio 0.00252, showing that the analysis result is reliable.

4.2.3 Final Analysis Results

The final analysis was then carried out in order to determine global priorities as the final weight of seven alternatives. The final analysis results are described in Table 3.

Table 3. Global weight Value

	Defense of Homeland	Economic Wellbeing	Promotion of Value	Favorable World Order	Global Priority
DLF	0.096	0.045	0.035	0.012	0.188
EAC	0.070	0.059	0.028	0.009	0.166
EOS	0.063	0.044	0.024	0.011	0.142

ECE	0.054	0.030	0.019	0.010	0.113
PPP	0.045	0.044	0.027	0.012	0.129
CII	0.069	0.041	0.027	0.015	0.153
TTC	0.046	0.029	0.021	0.012	0.109
Overall	0.443	0.293	0.182	0.081	

Based on our analysis results, this study describes the key outcomes as follows. With respect to Cambodia's cybersecurity alternatives, DLF is considered a top priority by Cambodian experts in comparison to EAC, EOS, ECE, PPP, CII and TTC(see code in Table 1). It is found that DLF represents 0.188, whereas EAC, EOS, ECE, PPP, CII and TTC account for 0.166, 0.142, 0.113, 0.129, 0.153 and 0.109 respectively.

In other words, the most important alternative is to develop a proper legal framework to assure information security. The next important priority is to strengthen cyber security awareness and capacity building, and then to prevent cyber-attacks against critical information infrastructure.

In similar, it is found that both homeland defence and economic well-being are considered to be more critical than promotion of values and favorable world order aspects. The Cambodian government seems to focus more on the national security and economic well-being of cyber security which accounts for 0.443 and 0.293 respectively, compared with the promotion of values of 0.182 and favorable world order of values of 0.081.

5. Conclusion and Discussions

This study used AHP to evaluate national cyber security strategy in Cambodia. AHP provides a powerful and comprehensive approach for cyber security policymakers in both qualitative and quantitative methods.

From cyber security aspect, homeland defense and economic well-being aspects are assessed to be the most critical factors compared to promotion of values and favorable world order. In similar, with respect to cyber security alternatives, legal framework for information security shows the top priority in cyber security strategy implementation and the second priority is awareness and capacity building, followed by organizational structure, international cooperation, public-private partnership, infrastructure and cybercrime prevention.

We suggest that homeland defense and economic well-being aspects must be considered as more critical issues for establishing a desirable cyber security strategy. On the other hand, this sturdy confirm that our findings are identical with the guide recommended by the ITU national interests model[10,20], which pointed out cyber security as one of the challenging decision-making issues to develop effective cyber security strategy in Cambodia.

Furthermore, the study findings reveals several implications for building Cambodian cyber security strategy in the future. Cyber security have the most influence on home defence and then economic welfare. Therefore, Cambodian government need to construct and improve legal framework for information security and national security as the most important factor in the area of homeland defense. The second priority should be focused on enhancing cybersecurity awareness and capacity building among citizens and government officials, whereas the third priority should be given to preventing cyber-attacks against critical information infrastructure such ICT network and facility.

With respect to economic well-being aspect, there is slight different priority. Cambodian government should enhance cybersecurity awareness and capacity building, followed by developing an appropriate legal framework to ensure information security factor and then enhancing organizational structure factor.

From the strategic step-by-step approach, Cambodian government need to pay much more attention to 3 urgent alternatives among seven strategic alternatives at the first phase. Among three, Cambodia should prepare the appropriate regulation or law, improve and enforce domestic cybercrime laws by benchmarking legal frameworks introduced by other advanced countries. Next, Cambodia should develop some programs that help inspire a culture of cybersecurity and increase awareness of it. Last, preventing cyber−attacks against critical information is required to protect the economies or businesses as an infrastructure of the modern economy.

After implementing the most urgent three alternatives, the second phase is to strengthen organization structure, and guarantee public safety and improve public−private partnership. The third phase that must be implemented in the future consists of two recommendations for ensuring cybersecurity through cooperative effort and tackling cybercrime.

Finally, this research analysed data collected from nineteen experts engaging in the cyber security fields. Most respondents came from the government sector, therefore we need more experts from the private sector or academic sector as well. The researchers should be careful about interpreting the results because ICT sector is changing rapidly, particularly new trends of cybersecurity incident are associated with the speedy development of ICT like AI, Big Data and Drone[13].

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] M. Heng. (2018). *A study on developing the Roadmap for Strengthening Cybersecurity Focused on Cambodia.* Master Thesis, Soongsil University, Seoul.

[3] M. Dara & D. de. Carteret. (2016). Slew of websites hacked. The Phnompenh Post, January 12.

[4] I. Peña−López.(2015). Global Cybersecurity Index & Cyberwellness Profiles Report. *WSIS Forum 2015 Geneva,* 1−37.

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

[6] L. M. Aliyeva & G. H. Hwang. (2019). The Model to Implement the Cyber Security Policy and Strategy for Azerbaijan Information System. *Journal of Digital Convergence, 17(5),* 23−31.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] Canada & Public Safety Canada. (2010). Canada's cyber security strategy: for a stronger and moreprosperous Canada. Ottawa, Ont.: Government of Canada.

[13] 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.

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

[15] S. Berman(2018). How to Structure Your Organization's Cybersecurity Management: Insights from Nutter's Seth Berman. Nutter,October 3,

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

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

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

[19] 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.

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

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

Mara Heng [정회원]

- 2018년 2월 : 숭실대학교 정보과학대학원 글로벌ICT융합학과 졸업(공학석사)
- 2018년 3월 ~ 현재 : 캄보디아 정보통신기술부 근무
- 관심분야 : 사이버보안, 전자정부 등
- E-Mail : mara-heng@gmail.com

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 부교수 재직 중
- 관심분야 : 국제개발협력, TQM, SCM, ICT융합 등
- E-Mail : mike2030@ssu.ac.kr