Journal of Defense Acquisition and Technology, Vol. 2, No. 2, Dec. 2020, pp. 39-43
https://doi.org/10.33530/jdaat.2020.2.2.39
eISSN : 2671-9401

An Assessment Model for Defense Cybersecurity Capability

Sungrim Cho

Abstract

As cyber threats increase around the world, many countries are focusing on increasing their cybersecurity while expanding their investments in cybersecurity. Recently, the pattern of war is changing in the direction of linking military operations and cyberattacks, and North Korea is also strengthening its cyber warfare capabilities as one of the asymmetric forces. North Korea's cybersecurity threat, along with nuclear and missile provocations, is rapidly emerging as a serious security threat on the Korean Peninsula. In order to effectively respond to North Korea's cybersecurity threat, this paper examines the trends in cybersecurity competency assessment at domestic and foreign countries, and presents a defense cybersecurity competency assessment model as a way to strengthen the cybersecurity competency level. The model will contribute to establishing cyber warfare preparedness by diagnosing the level of cybersecurity capabilities of the military and supporting decision-making so that cybersecurity forces can be efficiently equipped.

Key Words: Defense Cybersecurity, Evaluation System, Capability Maturity Model

I. INTRODUCTION

Recently, warfare has been changing in the direction of linking physical military operations and cyber operations. Cyber operations play a role of creating an environment favorable for wartime or attacking national infrastructure to paralyze or neutralize it.

A Russia's cyberattack, triggered by the Estonian government's plan to demolish the Soviet war memorial statue in 2007, was a distributed denial-of-service (DDoS) attack against major sites such as Estonian government agencies, parliament, banks and the media [1]. A Russia's cyberattack on Estonia was the first full-scale cyber warfare to attack the entire country for political purposes. Estonia suffered great social chaos due to this attack. A Russia's another cyberattack, which unfolded after the territorial dispute between Georgia and Russia in 2008, is regarded as the first example of a cyber operation linked to a physical military operation. Russia conducted DDoS attacks and tampering attacks on the Georgian president's homepage, government homepages, and media outlets, causing social confusion and disrupting communications. In addition, Operation Orchard, in which Israel attacked Syrian nuclear facilities, hacked into the Syrian radar network and neutralized the air defense system, creating conditions for Israeli fighters to infiltrate Syrian airspace and carry out an attack successfully.

North Korea recognized the importance of cyber warfare as one of the asymmetric forces, and established bureau for a cyber warfare leadership (named as Bureau 121) in the reconnaissance headquarter that leads cyberattacks to reinforce the cyber organization and cultivate more than 1,700 hackers. As North Korea strengthens her capabilities in the cybersecurity field, cyber terrors against Republic of Korea (ROK) were performed over 10 times for 2009-2016. It continues to increase, and its scope is gradually expanding [2].

Despite the reduction in defense budgets in countries around the world, the budgets of organizations related cybersecurity are increasing. In the U.S., the overall budget and IT budget for fiscal 2017 were $4.2 trillion and $89.9 billion, respectively, and the cybersecurity sector budget increased by 35% year-on-year to $19.9 billion. The cybersecurity budget accounts for 0.45% of the total national budget and 21% of the IT budget. According to the national informatization implementation plan, Korea's cybersecurity budget in 2017 was $350.8 million, an increase of 3.8% compared to the previous year, accounting for 0.088% of the national budget and 6.7% of the IT budget, which is still not large [3].

However, the ROK military also proposed to establish an all-round defense posture in preparation for North Korea's

Manuscript received December 23, 2020; Revised December 29, 2020; Accepted December 30, 2020. (ID No. jdaat-2020-00003)

*Corresponding Author: Sungrim Cho, Department of Computer Science and Engineering, Graduate School of Korea University, Seoul Korea.
E-mail: srcho@korea.ac.kr, Tel. +82-10-3292-334
Department of Computer Science and Engineering, Korea University, 145 Anam-ro, Seongbuk-gu, 02841, Seoul, Korea

military threats as a future vision of our military, and for this purpose, it is proclaiming to strengthen cyber warfare response capabilities and to create practical education and training conditions. Therefore, the proportion of the cybersecurity sector budget in defense expenditure is expected to increase.

The prerequisite for preparing for these changes in internal and external conditions and related trends is to accurately evaluate the cybersecurity capabilities we have and should have. Nevertheless, an evaluation model for diagnosing the level of ROK military's cybersecurity capabilities compared to those of neighboring countries on the Korean Peninsula has not yet been established. This paper diagnoses the cybersecurity capabilities of the ROK military and proposes a defense cybersecurity capability assessment model as a way to support decision-making in order to effectively strengthen it. The defense cybersecurity competency evaluation model is an evaluation method for objectively evaluating the ability of all forces including cyber weapons to ensure cybersecurity and reinforcing competencies in insufficient fields. This competency evaluation model can be compared with the ROK military by evaluating not only the level of cybersecurity capability of the ROK military, but also the level of cybersecurity capability of neighboring countries on the Korean Peninsula.

II. CYBERSECURITY COMPETENCY ASSESSMENT TRENDS AND IMPLICATIONS

The assessment model for evaluating the level of cybersecurity competency is divided into a comparative evaluation model and a maturity evaluation model. The comparative evaluation model is an evaluation model that identifies evaluation items corresponding to cybersecurity capabilities and determines the relative comparative advantage between evaluation items. On the other hand, the maturity evaluation model is an evaluation model that divides the cybersecurity competency level into maturity levels, and determines the competency level according to whether the maturity level is satisfied.

2.1. Comparative evaluation model

There are Technolytics Model [4], Defense Tech Model [5-7], and Richard Clark Model in the comparative evaluation model released in the late 2000s. It is a method of evaluating cybersecurity capabilities between countries by comparing cybersecurity elements such as cyberattack experience, the size of cyber personnel, and cyber budget.

Since the comparative evaluation model is composed of broad evaluation items, it is difficult to identify the details for developing cybersecurity capabilities. It is also difficult to trust the evaluation results because the method of calculating the evaluation results for each item is not disclosed. The results of each country's cybersecurity competency evaluation based on the comparative evaluation model announced during specific period have been converted to private, or the evaluation results have not been published after that. Since most of the cybersecurity capabilities of neighboring countries on the Korean peninsula such as North Korea and China, which have been cited by the media recently, are mostly based on evaluation results published, it is unknown how much has changed since then.

2.2. Maturity assessment model

Maturity assessment models include Robert Lenz's model [8], BAH model, ETRI-affiliated institute model [9], milCyberCAP model developed by RAND Europe research center [10], Cyber Security CMM model developed by Oxford University [11]. The Robert Lenz model and the BAH model presented only the maturity level that defined the cybersecurity competency level, and the other models included the maturity level and the evaluation items to measure the maturity level.

The Robert Lenz model defines cybersecurity capabilities in five stages, from A to E, and the final stage E defines the organization as the stage with resilience from cyberattacks. This model has been criticized for being a model that focuses on resilience, or defense, and fails to assess overall cybersecurity capabilities. The BAH model divided the cybersecurity competency level into five stages: confusion, definition, management, measurement, and innovation, and was referenced to define the maturity level of other maturity assessment models. The Cyber Security CMM model defines the maturity level by referring to the maturity level of the CMM model, which is Carnegie Mellon University's software process maturity model.

The ETRI-affiliated institute model and milCyberCAP model include combat development factors (doctrine, organization, training, materials, leadership, manpower, and facilities) as evaluation items, but the ETRI-affiliated institute model is evaluated as national level and the mil CyberCAP model is to assess the average cybersecurity capabilities of the NATO member states.

The milCyberCAP model adds evaluation items in consideration of interoperability among NATO member states in addition to combat development factors. The milCyberCAP model presents evaluation items to NATO member states, and evaluates the maturity level with the average value of the results of self-assessment by NATO member states. The Cyber Security CMM model defines cyber policy and strategy development, responsible cyber culture creation, cyber education and training, cyber manpower and technology acquisition, cyber legal system framework development, and risk management based on standards and technology as evaluation items.

2.3. Implication

When evaluating the military's defense and cybersecurity capabilities and performing comparative analysis with neighboring countries, the comparative evaluation model is limited in the use of evaluation models and evaluation results due to the composition of comprehensive evaluation items and the non-disclosure of evaluation methods. In addition, the maturity assessment model defines the maturity level of cybersecurity capabilities and is composed of detailed assessment items. However, since evaluation targets are countries such as the ETRI affiliated research institute model and Cybersecurity CMM model, or NATO member countries such as the milCyberCAP model, the evaluation results of these maturity evaluation models are also limited. Therefore, it is needed to evaluate the level of defense cybersecurity in consideration of Korea's internal and external cybersecurity environment, identify and improve the areas that are lacking, and thus need a new standard to strengthen the defense cybersecurity capabilities.

III. DEFENSE CYBERSECURITY CAPABILITY ASSESSMENT MODEL

In order to strengthen the cybersecurity capabilities of the ROK military, this paper diagnoses the current level of cybersecurity capabilities and proposes a Defense Cybersecurity Capability Assessment Model to support decision-making in the future cybersecurity field. This model has the following characteristics.

First, the model focuses on evaluating the maturity level of cybersecurity as shown in Table 1. Among the two models described above, the model adopted a maturity evaluation model that allows both individual and relative evaluation rather than a comparative evaluation model that allows only relative evaluation. The model can be used as a tool to identify the current level of the Korean military and set the direction of progress to reach the target level, and can perform a relative comparative evaluation on the cybersecurity capability level of neighboring countries on the Korean Peninsula.

Second, evaluation items were set by analyzing existing domestic and international cybersecurity competency evaluation models. As shown in Table 2, the evaluation items consist of two major categories, ten dimensions, and 22 measures. The major classification is divided into infrastructure competencies required to build a cybersecurity environment and core competencies required to conduct

Table 1. Maturity level of defense cybersecurity capability assessment model

Level	Stage	Explanation
5	Innovation	The concepts and procedures are defined, and rapid and flexible innovation in response to environmental changes are performed.
4	Measurement	The concepts and procedures are defined, well evaluated, and improved.
3	Definition	The concepts and procedures are defined, and the tasks are performed according to the defined concepts and procedures.
2	Practice	The concepts and procedures are not defined, but as a practice, tasks are repeated to produce the same results.
1	Early	The concepts and procedures are not defined, so the tasks are performed according to individual capability.

Table 2. Dimension of defense cybersecurity capability assessment model

Dimension	Measures
Infrastructure capability	
Legal system	Cybersecurity law Cybersecurity regulation Acquisition system for cyber weapon
Policy / strategy	Cybersecurity policy Cybersecurity strategy
Budget	Cybersecurity budget
Organization	Coordination control organization Operational organization
Personnel	Policy for personnel acquisition Policy for personnel management
Education	Professional education General education
External cooperation	National cooperation for cybersecurity Private cooperation for cybersecurity International cooperation for cybersecurity
Core capability	
Operation	Cyber operation Cyber doctrine
War power	Warrior for cybersecurity Defense technology for cybersecurity Core technology for cybersecurity Command and control for cybersecurity
Training	Training for cybersecurity

cyber warfare. In the dimension, infrastructure competencies and core competencies are subdivided into organization and function. Although the milCyber CAP model and the ETRI-affiliated institute model constituted evaluation items as elements of combat development, there was limitation that the task and the responsibility to develop the field were not well connected with the organization. In proposed model, it is subdivided into organizations and functions to facilitate the use of the evaluation results.

Third, the model sets the target level of cybersecurity in consideration of Korea's internal and external cybersecurity environment, and provides a framework for establishing an implementation plan by identifying vulnerable areas. In other words, this assessment model is applied to measure the level of cybersecurity in the ROK military, set targets based on the maturity level, and then establish and implement development plans for vulnerable areas, while evaluating the level of competency against the target every year to promote continuous development.

IV. CONCLUDING REMARKS

As the cybersecurity field becomes increasingly important as an asymmetric force in defense, the arms race in the cyber field is also accelerating. Systematic and effective improvement of a cybersecurity capability is an essential and obligatory task for the military as well. In order to effectively implement this, an evaluation tool is needed to diagnose the current level of a defense cybersecurity capability and to establish future development plans. Various models for evaluating the defense cybersecurity capability have been introduced, but the reliability of the evaluation results is low and unclear because the details of calculating the evaluation results have not been disclosed.

In this paper, the model for evaluating a defense cybersecurity capability in consideration of the defense environment was proposed. The proposed model will enable the establishment of a solid preparedness for cyber warfare by supporting the military's cybersecurity policy establishment, increasing budget, and decision-making on priorities.

In addition, it is necessary to establish an information system to continuously manage a cybersecurity capability evaluation and an evaluation history, and to establish cybersecurity-related information of neighboring countries on the Korean Peninsula as a database. Like other evaluations, the reliability of the evaluation results varies depending on the quality of the information input in the evaluation of a defense cybersecurity capability. It should be noted that the defense cybersecurity capability is not improved through a one-time assessment, but can be improved by continuously accumulating information in the cybersecurity database, conducting capability assessments, and reinforcing an insufficient cyber capability according to the results.

There are some limitations in this study. After proposing the model, its application cases are necessary to validate it. The application cases were not described due to classified information in the defense cybersecurity domain. If the classified information would be released to unclassified information, the application cases can be described in near future. Moreover, the specific weights among measures and assessment process are needed in the further studies.

REFERENCES

[1] J. I. Lim, "Cyber war status and future tasks," *in The 1st Korea Federation of Science and Technology Societies Policy Discussion*, 2011. (in Korean)

[2] S. R. Lee, "The increase in North Korean cyber terror threats and countermeasures," *Issue and Points*, no. 1127, National Assembly Legislative Research Office, 2016. (in Korean)

[3] Republic of Korea Ministry of National Defense, *2016 Defense Expenditure Brochure*, 2016. (in Korean)

[4] Technolytics, *Cyber Commander's eHand-book version* 2.0, 2011.

[5] Defense Tech, "China's Cyber Forces," 2008. http://defensetech.org/2008/05/08/chinas-cyber-forces.

[6] Defense Tech, "Russia's Cyber Forces," 2008. http://defensetech.org/2008/05/27/russias-cyberforces.

[7] Defense Tech, "Iranian Cyber Warfare Threat Assessment," 2008. http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment.

[8] R. Lentz, *Cyber Security Maturity Model*, 2011. http://dintel.org.

[9] www.boozallen.com

[10] N. Robinson, A. Walczak, S.-C. Brune, A. Esterle, and P. Rodriguez, "Stocktaking study of military cyber defence capabilities in the European Union (milCyber CAP): Unclassified Summary," *RAND Europe*, 2013.

[11] Global Cyber Security Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM)," Revised Edition, University of Oxford, 2016.

AUTHOR

Sungrim Cho received an M.S. in Computer Science from Seoul National University and is pursuing Ph.D. in computer science at Korea University. She is a research fellow at the Korea Institute for Defense Analyses who specializes in defense information policy, C4ISR, Cyber Warfare, Information system evaluation, and SW Engineering.