Study on Cyber Attack Damage Assessment Framework

Sungjoong Kim¹, Jisoo Jang¹,², Oh-jin Kwon³ Ju-youb Kim⁴, Dongkyoo Shin¹,²

¹Department of Computer Engineering, Sejong University, Seoul 05006, Korea
²Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Korea
³Department of Electrical Engineering, Sejong University, Seoul 05006, Korea
⁴Cyber/Network Technology Center, Agency for Defense Development, Seoul 05661, Korea

Corresponding author: Dongkyoo Shin (shindk@sejong.ac.kr)
This work was supported by Agency for Defense Development under the contract. (UI210010XD)

ABSTRACT Cyberspace has expanded as a result of the rapid spread of the Internet. This expansion has led to a change from conventional warfare to a form that includes cyber warfare. Cyber warfare, which occurs in cyberspace, consists of numerous cyberattacks using the vulnerabilities of cyber assets. Cyberattacks have increased with increases in the number of assets connected to the network and the information held by these assets; information can control the outcome of a war. Therefore, it is very important to assess the damage from cyberattacks between physical operations because such cyberattacks may be directly linked to the failure of an operation. This paper presents a cyber damage assessment framework for assessing the damage from cyberattacks between physical operations.

INDEX TERMS Cyber warfare, Cyber Battle Damage Assessment, cyberattack, mission

I. INTRODUCTION
Cyberspace has expanded as a result of the development of information and communication technology. This expansion has brought about changes in the war environment represented by cyber warfare. In the past, conventional warfare with physical strikes such as from tanks and missiles was changed to Network Centric Warfare (NCW), in which all elements of the battlefield environment were linked, making it possible to paralyze or destroy the warfare system through cyberattacks. This brought about changes in the war environment, as discussed in [1]. Cyberattacks have increased with increases in number of assets connected to the network and the information possessed by these assets. Information can dominate a war [2]. Therefore, if a cyberattack occurs between physical operations, it may be directly linked to the failure of an operation. Thus, it is very important to assess the damage from cyberattacks between physical operations.

This paper presents a cyber damage assessment framework for assessing the damage from cyberattacks between physical operations. Section 2 describes studies related to damage assessment, section 3 describes the cyber damage assessment framework presented in this paper, and section 4 reviews a case study that was conducted of the cyber damage assessment framework presented in this paper. Conclusions are drawn in section 5.

II. Related Work
Most cyber damage assessment methods utilize the common vulnerability scoring system (CVSS) [3] to determine the damage to assets. However, the CVSS only uses standardized vulnerability scores, rather than quantitative measures for the damage. Therefore, studies on the assessment of the quantitative cyber damage from cyberattacks are still being conducted in various ways.

Kim et al. developed a formula called the measure of cyber effectiveness (MOCE) and proposed a cyber asset damage assessment framework based on three types of damage: interruption, interception, modification [4].

Wagner et al. proposed a damage assessment method that used the operational delay as a measure to evaluate the operational damage caused by a cyberattack on the network side [5].

Hong et al. proposed a method for calculating the damage caused by a cyberattack using Gorden-Lobe model and the security scoring method to evaluate the impact of a cyberattack [6].
Kotenko et al. proposed a framework for cyberattack impact assessment that used an attack graph to model a cyberattack and security variables [7]. Jakobson and Gabriel presented the dependency between cyberspace and a mission using an impact dependency graph and proposed a method for evaluating the possible impact on cyber assets, service, and missions [8].

III. CYBER BATTLE DAMAGE ASSESSMENT FRAMEWORK

A. Cyber Battle Damage Assessment Framework Architecture

The mission dependency structure of the US company MITRE [9] is shown in Fig. 1. It is structured hierarchically in the order of assets, system functions, operational tasks, and mission objectives.

In addition, Snyder et al. [10] believed that cyberattacks will have a cascading effect, as shown in Fig. 2. This effect shows that if the lowest level asset in the hierarchical structure is damaged, the mission itself will be damaged because it will not perform its proper role at the upper level.

The asset layer contains information assets necessary for mission execution. The function layer is a function for performing an execution procedure, and the task layer contains the mission execution procedure. Finally, the mission layer contains the operation to be performed.

| TABLE I | CYBER BATTLE DAMAGE ASSESSMENT FRAMEWORK LAYER INFO |
|---------|----------------------------------------------------|
| Layer   | INFORMATION                                         |
| Asset   | Assets needed to perform the mission               |
| Function| Detailed functions for performing mission procedures|
| Task    | Mission procedure to accomplish the mission        |
| Mission | Task to be performed                                |

B. Cyber Battle Damage Assessment Framework Measure

The measures of the cyber battle damage assessment framework proposed in this paper primarily consist of the ‘Performance’ and ‘Impactor’.

Performance is the degree to which a component is used to perform a mission, and all hierarchical components have a performance value. Impactor is assigned to the relationship between the components of the upper-lower hierarchy based on the extent that the corresponding hierarchy affects the mission. The performance and impactor are different in how they are calculated for each layer.

1) ASSET LAYER

The method used to obtain the Asset Performance and Asset Impactor, which are the measures of the asset layer, is as follows.

![Mission Layer Diagram](image_url)  
**FIGURE 1. MITRE mission dependency structure**

![Task Layer Diagram](image_url)  
**FIGURE 2. Chain effects from cyberattacks**

![Function Layer Diagram](image_url)  
**FIGURE 3. Cyber Battle Damage Assessment Framework structure**

![Asset Layer Diagram](image_url)  
**FIGURE 4. Cyber Battle Damage assessment framework measure**
In this paper, the asset performance is constructed based on value engineering (VE). VE is a design engineering technique that critically examines and analyzes the design of components with reference to their functional value, and plays an important role in asset management [11]. Equation (1) is used to calculate the existing VE.

\[
V = \frac{F}{C}
\]  

(1)

In other words, VE considers the value of the ratio of the cost to achieve the desired function as value. In this paper, the VE is modified from the perspective that ‘the more assets used for various functions compared to the number of vulnerabilities an asset has, the more valuable it is for missions.’ Thus, asset performance has the meaning of the value of the asset to the mission performance, and the method of finding it is the same as Equation (2).

\[
A = \frac{F \times \alpha}{V}
\]  

(2)

The method used to obtain the Function Performance and Function Impactor, which are measures of the function layer, is as follows. The Function Performance is the degree to which a function is used for its mission. As in Equation (3), the calculation method is calculated as the sum of the product of the Asset Performance and Asset Impactor of the lower layer, the asset layer.

\[
Function\ performance = (\sum_{n=1}^{N} Asset_n perform \times Asset_n impactor)
\]  

(3)

The Function Impactor indicates the extent that the function affects the mission if the function cannot be performed within the specified time, or when the result of the function execution is an error due to inaccurate information required to perform the function. Therefore, the Function Impactor has two cases that affect the mission as a measure. The Function Time Impactor is the scale for the case of a failure to perform within the specified time, and the Function Accuracy Impactor is used for the case where an error occurs as a result of execution. The method to obtain the Function Impactor is as in Equation (4).

\[
Function\ Impactor = Function\ Time\ Impactor \times Function\ Accuracy\ Impactor
\]  

(4)

The Function Time Impactor calculation method calculates the execution time of the function compared to the execution time of the task, as in Equation (5). If there is a delay in task execution, it is calculated by multiplying the delayed function time by the delayed task time in the Function Time Impactor. Fig. 5 shows an example of the Function Time Impactor.

\[
Function\ Time\ Impactor = \frac{init time\ function}{init time\ task} \times \frac{delay time\ function}{delay time\ task}
\]  

(5)

2) FUNCTION LAYER
The method used to obtain the Function Performance and Function Impactor, which are measures of the function layer, is as follows. The Function Performance is the degree to which a function is used for its mission. As in Equation (3),

![FIGURE 5. Function time impactor example](image)
The Function Accuracy Impactor is a metric for determining whether a function is correctly performed. When the assets required to perform the function can be fully utilized, the correct mission is performed, and the initial function accuracy impactor is initialized to 1. If an asset is damaged by a cyberattack, it is calculated as in Equation (6) by subtracting the number of damaged assets from the number of assets used in the function in the Function Accuracy Impactor.

\[
\text{Function Accuracy Impactor} = 1 - \frac{\text{number of attacked assets}}{\text{function weight}}
\] (6)

3) TASK AND MISSION LAYER
The task layer and mission layer have only performance values. The method of calculating the performance of each layer is as follows. The Task Performance is calculated as the degree to which the task is used for the mission, as follows. As in Equation (7), it is calculated as the sum of the product of the performance of the lower function layer and the impactor.

\[
\text{Task performance} = \left( \sum_{n=1}^{\text{Task weight}} \text{Func}_n\text{perform} \times \text{Func}_n\text{impactor} \right)
\] (7)

| TABLE 5 | TASK PERFORMANCE FORMULA DESCRIPTION |
|---------|---------------------------------------|
| SYMBOL  | INFORMATION                            |
| Task weight | Number of branches connected to the Task |
| Func_perform | Performance of Func, connected to the Task |
| Func_impactor | Impactor of Func, connected to the Task |

Lastly, Mission Performance refers to the ability to perform missions. It is calculated as the Task Performance sum.

C. Cyber Battle Damage Assessment Framework Workflow
The progress of the cyber battle damage assessment framework proposed in this paper is as follows. First, the mission performance is calculated before receiving a cyberattack. When a cyberattack occurs, the damaged asset is identified, and its performance is reduced as seen in the asset damage reduction table. The mission performance is calculated again by calculating the upper layer affected by the decrease in asset performance. Finally, as in Equation (8), the damage evaluation is performed by comparing the mission performance values before and after the cyberattack.

\[
\text{Damage assessment} = 1 - \frac{\text{Mission Performance}_{\text{after}}}{\text{Mission Performance}_{\text{before}}}
\] (8)

D. Asset damage reduction table
The asset damage reduction table is used as a means to reduce asset performance by identifying the degree of damage caused by cyberattacks. In the composition of the table, as assets are used in functions, the damage that can occur to the assets is identified based on the function and included in the table.

Fig. 7 is an example of the asset damage reduction table. For the table configuration, functions and assets are configured based on inquiries to the military expert who performs the mission. According to the degree of damage, the impact is classified into three levels: high, medium, and low, which are given scores of 3, 2, and 1 points, respectively.

The procedure for reducing the asset performance using the asset damage reduction table is shown in Fig. 8. First, find the assets that have been damaged by a cyberattack. Then, after checking the function that the damaged asset is used for, the impact of the damaged part is identified through the asset damage reduction table. Finally, the initial asset performance is reduced by the impact.
IV. EXPERIMENT

We conducted an experiment using the cyber battle damage assessment framework proposed in this paper. In this experiment, mission and attack scenarios were configured, and the results of a simulation using OMNeT++ were checked [14].

A. Mission scenario configuration

In the experiment, a mission scenario was set up to request a close air support (CAS) operation. A CAS operation is an operation to attack the enemy with an aircraft in close proximity to friendly forces [13], and the mission scenario was the process of properly requesting the CAS operation from the army regiment and finally distributing the air mission order (ATO).

In order to construct the cyber damage assessment framework proposed in this paper, we analyzed the elements of the mission scenario. The tasks and functions were defined based on the analyzed elements, and the assets to be used in mission scenarios, and networks, were configured. Tables 6 and 7 define the tasks and functions of the mission scenarios, respectively.

| TABLE 6 | MISSION SCENARIO TASK DEFINITION |
| TASK | INFORMATION |
|---|---|
| 1 | The regimental commander and TACP fill out the CAS request form. |
| 2 | CAS request from regiment to division |
| 3 | CAS request from division to ASOC |
| 4 | CAS request from ASOC to KAOC |
| 5 | CAS operation planning at KAOC |
| 6 | CAS approval and ATO publish |

| TABLE 7 | MISSION SCENARIO FUNCTION DEFINITION |
| NO | TASK | Function |
|---|---|---|
| 1 | 1 | Operation Environment Analysis. |
| 2 | 1 | Target identification |
| 3 | 1 | CAS Operation determination |
| 4 | 1 | CAS Operation request form |
| 5 | 2,3,4 | Send CAS Operation request |
| 6 | 2,3,4 | CAS Operation request analysis |
| 7 | 2,3,4,5 | Available Power Analysis |
| 8 | 5 | Selection of fighter jets |

The assets used in the mission scenario were configured as shown in Fig. 9.

B. Cyberattack scenario configuration

In order to understand how much the mission was affected when a cyberattack occurred during the mission, the attack scenario was configured as shown in Fig. 11. The simulation was carried out with the configured scenario.
Scenario #1: The case of tampering with the CAS request by infecting a PC in a solidarity network using malicious code

Based on the simulation results, the damaged assets were identified and substituted into the cyber battle damage assessment framework. As a result, the mission performance after the cyberattack was 3697.4, which was about 86% of damage.

V. COMPARISON

In this section, the damage assessment model proposed in this paper is compared with the previously studied damage assessment case. Table 8 is a brief summary of the comparison between the previously studied damage assessment case and the model proposed in this paper.

| Proposed Method       | General approach | Mission context | Cyber asset damage |
|-----------------------|-------------------|-----------------|--------------------|
| Cho et al. [15]       | Threat centric    | No              | Yes                |
| Yoo et al. [16]       | Mission centric   | Yes             | No                 |
| Kim et al [4]         | Threat centric    | No              | Yes                |
| Hong et al [6]        | Threat centric    | No              | Yes                |
| Barreto et al [17]    | Mission centric   | Yes             | Yes                |
| Wagner et al [5]      | Threat centric    | No              | Yes                |

Cho et al. measures the effectiveness of cyberattacks using MoE and MoP. Damage analysis is carried out by identifying the threat success rate and host infection rate. The damage assessment only evaluates the damage to the network, not the impact of the task or mission. Therefore, the impact of the mission due to the cyber attack is unknown.

In Yoo et al.’s damage assessment study, it is a mission-based damage assessment method that has an asset-function-work-mission structure as in this paper, and damage assessment is carried out with a usefulness scale that has a meaning to the degree of usefulness of each component. Although the structure is similar to this paper, it is difficult to understand the actual damage suffered by cyber assets because the degree of damage is defined in advance. Although the impact of the mission can be confirmed, there is a disadvantage that direct cyber damage cannot be confirmed.

In Kim et al.’s damage assessment study, a formula was developed that can quantitatively determine the degree of damage according to the type of damage (modification,
interruption, interception) caused by a cyber attack. Although it is possible to directly check the degree of damage caused by a cyber attack, it has the disadvantage that the damage received by the mission cannot be confirmed.

In Hong et al.’s damage assessment study, using the Gorden-Lobe model, the expected damage was calculated through the investment and the loss function for the reaction to the actual threat. This is a practical response by defining the damage scale for the type and type of attack. As a method of calculating the scale and standards for the level, the study also cannot determine the impact of the mission.

In Wagner et al.’s damage assessment study, it is difficult to understand the impact of a task or mission because damage assessment is carried out with network delay.

In Barreto et al.’s damage assessment study, the infrastructure capacity index is generated using cyber asset information (vulnerability, etc.), and a Bayesian network is built with these values to create an inference model that predicts the damage the mission will take, and then conducts mission impact evaluation. By connecting cyberspace and mission area, it is possible to understand how actions in cyberspace affect mission efficiency.

On the other hand, the damage assessment proposed in this paper divides the mission performance system into asset - function - task - mission and proceeds with damage assessment. Because damage can be checked by layer, it is possible to not only check the degree of damage to the network and system, but also to quantitatively check how much the cyberattack has finally affected the mission.

VI. CONCLUSION

In this paper, we proposed a framework for evaluating the damage caused to a mission by a cyberattack. Assuming that a cyberattack occurs in an asset, when a cyber asset is damaged, it is part of a hierarchical structure and affects the upper layer. The damage assessment method compared the results before and after damage.

The damage assessment framework proposed in this paper can quickly and quantitatively derive the degree of damage that has occurred in a mission. This can quantitatively convey the damage caused to the mission to the commander, which will help the commander make a decision.

In the future, we plan to advance the BDA using the results of the cyber damage assessment framework presented in this paper.

REFERENCES

[1] C. Park, and Y. Park, “A study on the improvement of capability assessment and the plan for enhancing cyber warfare capability of Korea,” Journal of the Korea Institute of Information and Communication Engineering, vol. 19, no. 5, pp. 1251–1258, 2015
[2] S. Im, C. Lee, S. Hong, and S. Jeon, “A method of defense scoring on trainer in cyber mock battle,” in Proc. KICS, Jeju, Korea, 2019, pp. 833-834.
[3] Common Vulnerability Scoring System 3.1, https://www.first.org/cvss

[4] D. Kim, D. Kim, D. Shin, D. Shin, and Y. Kim, “Cyber Battle Damage Assessment Framework and Detection of Unauthorized Wireless Access Point Using Machine Learning,” in International Conference on Frontier Computing, Singapore: Springer, 2018, pp 510-519.

[5] N. Wagner, C. Ş. Şahin, M. Winterrose, J. Riordan, D. Hanson, J. Peña, and W. W. Streilein, “Quantifying the mission impact of network-level cyber defensive mitigations,” The Journal of Defense Modeling and Simulation, vol.14, no.3, pp.201–216, 2017.

[6] B. Hong, J. Lim, W. Kim, and J. Cho, “Definition of aggressive response scale through quantitative evaluation of cyberattack,” Convergence Security Journal, vol. 17, no. 4, pp. 17–29, 2017.

[7] I. Kotenko, and A. Chechulin, “A cyber attack modeling and impact assessment framework,” in Proc. 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, 2013, pp. 1–24.

[8] G. Jakobson, “Mission cyber security situation assessment using impact dependency graphs,” 14th International Conference on Information Fusion, Chicago, IL, USA, 2011, 1–8.

[9] W. Heinbockel, S. Noel, and J. Curbo, “Mission dependency modeling for cyber situational awareness,” in NATO IST-148 Symposium on Cyber Defense Situation Awareness, 2016, pp. 1-14.

[10] D. Snyder, G. E. Hart, K. F. Lynch, and J. G. Drew, “Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems: Guidance for Where to Focus Mitigation Efforts,” Rand Corp., Santa Monica, CA, USA, Jan, 2015.

[11] E. Sallis, “Total quality management in education,” vol. 3, London, 1996.

[12] S. Wasserman, and K. Faust, “Social network analysis: Methods and applications,” 1994.

[13] Joint Chiefs of staff, Joint Publication 3-09.3, “Close Air Support”, Jul, 2009.

[14] A. Varga, “A practical introduction to the OMNeT++ simulation framework,” in Recent advances in network simulation. Cham, Switzerland: Springer, 2019, pp.3-51.

[15] W. Cho, and T. Kim, “Modeling and Simulation of Cyber Damage Assessment for Cyber Warfare Effectiveness Analysis,” JKIIE-S 16, pp. 3119–3125, 2016.

[16] S. Yoo, and D. Baik, “Comprehensive Damage Assessment of Cyberattacks on Defense Mission Systems,” IEEE TRANSACTIONS on Information and Systems, vol. 102, no. 2, pp. 402-405, 2019.

[17] A. B. Barreto, and P. C. G. Costa, “Cyber-ARGUS-A mission assurance framework,” Journal of Network and Computer Applications, vol.133, 2019, pp.86-108.