IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 20, 2020, accepted June 5, 2020, date of publication June 10, 2020, date of current version June 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3001286

Operation Framework Including Cyber Warfare Execution Process and Operational Concepts

SUNGJOONG KIM[1], JIWON KANG[1], HAENGROK OH[2], DONGIL SHIN[1], AND DONGKYOO SHIN[1], (Member, IEEE)

[1]Department of Computer Engineering, Sejong University, Seoul 05006, South Korea
[2]Agency for Defense Development, Daejeon 305600, South Korea

Corresponding author: Dongkyoo Shin (shindk@sejong.ac.kr)

This work was supported in part by the Defense Acquisition Program Administration, and in part by the Agency for Defense Development under Contract UD190016ED.

ABSTRACT Cyberspace has expanded due to the rapid spread of the Internet. This expansion of cyberspace has resulted in a change in war patterns from conventional warfare to cyberwarfare. Especially in the defense field, cyberspace was established as the fifth battlefield, following land, sea, air, and space. Cyberwarfare in cyberspace is caused by numerous cyberattacks. However, the current defense system to effectively defend against cyber threats is not sufficient. A new cyberwarfare framework is needed to complement current defense system. In this paper, we will construct the required concepts according to the cyber operation execution process into an integrated framework, conduct experiments on evaluating cyber battle damage assessment among the frameworks, and propose a cyberwarfare operation framework.

INDEX TERMS Cyberwarfare, battle damage assessment, cyber kill chain.

I. INTRODUCTION

With the rapid spread of the Internet, cyberspace has expanded. This expansion of cyberspace is exerting a great deal of change and influence on communication behavior. Especially in the defense sector, cyberspace has established itself as the fifth battlefield, following land, sea, air, and space. Cyberwarfare occurs in cyberspace and is being progressed and generated through various cyber attacks [1], such as hacking military information systems of other countries and paralyzing military and defense information systems to achieve military objectives.

In order to effectively defend against attacks in such a cyber threat environment, it is important to quickly identify and identify detailed attack information. However, the existing cyber defense system focuses on recovering when damage occurs. The defense system that is only focused on recovery has the disadvantage since it is difficult to respond immediately between actual operations. The defense system of the recovery point has the disadvantage that it is difficult to respond immediately between actual operations. To complement this, a new cyberwarfare operation framework is needed.

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq.

In this paper, we study the concept of cyber information surveillance reconnaissance, active defense and response, battle damage assessment, and command and control concepts required for defense-oriented cyber operations to develop an integrated operation concept for effective cyber operation. We present a cyberwarfare framework that can achieve a sustained strategic advantage in the cyber battlefield.

II. RELATED WORKS

In related research, cyberwarfare and the cyber kill chain, which are the basis of the cyberwarfare framework, will be described.

A. CYBERWARFARE

To define cyberwarfare, we need to first define cyberspace, which is the background of cyberwarfare [2]. Cyberspace is an environment in which information is transmitted through a computer network. The Department of Defense (DoD) has defined it as a global domain within the information environment [3]. The global domain consists of interdependent networks of information and communication technologies, including the Internet, communication networks, computer systems, and embedded processors and controllers. It is used to store, modify, and exchange data to achieve

cyberspace goals. Various studies have been conducted to define the cyberwarfare occurring in the cyberspace defined above. Hildreth raised concerns about countries' growing interest in cyberwarfare [4].

In the Stuxnet incident in June 2010, Jon R. Lindsay claimed that the impact of cyberwarfare was the greatest threat to the country to the extent that it could destroy the economy and civilization [5]. In order to defend against such cyberwarfare, a cyber operation was proposed in which all military systems were integrated, and it was emphasized that cyberwarfare should be concerned not only with national and military systems, but also with civilian systems.

Jeffrey described various examples of cyberwarfare by country in the 20th to 21st centuries [6]. The specific components used in the cyberwarfare case were described, and it was emphasized that it was a non-physical act of violence against an enemy without physical damage through a battle-free war.

Andrew described modern military operations that collect, disseminate, and utilize information in a variety of environments due to technological advances [7]. The study emphasized that even in military operations, the communications and information infrastructure has become a top priority for the military, and that actual cyberwarfare can cause physical damage to a country.

B. CYBER KILL CHAIN

Cyber kill chain is a term that originated from the military term kill chain [8] and is an active defense strategy for defending against cyber attacks. Its purpose is to neutralize or delay some of the various attack stages to reduce the effectiveness of the attack and minimize damage. Cyber kill chain was defined by Lockheed Martin [9]. The key concept used here is Kill Chain, which is the concept of detecting the origin and hitting the enemy first before firing nuclear or missiles. It consists of 6 stages: detection, verification, tracking, aiming, engagement, and evaluation. This refers to an offensive defense system. Further, it is the Cyber Kill Chain that applies this concept to the cyber security field. The Cyber Kill Chain model has various models for each defense industry and country and is composed of different stage models. Table 1 is an attack procedure model defined by Lockheed Martin and classified into 7 categories [9]. The concept of attack procedures defined by Lockheed Martin as above is used similarly in most companies and countries.

According to the Institute for Defense Analysis's data in the "Cyber Security Test Evaluation Guidebook", the US Department of Defense can view the cyber security kill chain (CSKC) data that shows the main activities and objectives of attack and defense [10]. CSKC's attack process did not include the installation step from Lockheed Martin's seven steps, but it did add a step to maintain after achieving the objective.

As shown in Fig. 1, Hewlett-Packard's Attack Life Cycle consists of 10 stages: reconnaissance, attack delivery, exploitation, installation, command and control, regional seizure, internal exploration, elevation of privilege, channel creation, and information theft [11].

TABLE 1. Lockheed Martin cyber kill chain attack procedure.

step	Info
Reconnaissance	Harvesting email address, conference info, etc.
Weaponization	Coupling exploit with backdoor into deliverable payload
Delivery	Delivering weaponized bundle to the victim via email, web, etc.
Exploitation	Exploiting a vulnerability to execute code on victim`s system
Installation	Installing malware on the asset
Command and Control	Command channel for remote manipulation of victim
Actions on Objective	With 'Hands on Keyboard' access, intruders accomplish their original goals

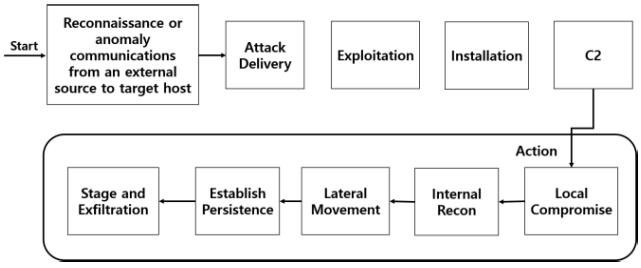


FIGURE 1. Attack life cycle of Hewlett packard.

Hewlett Packard's cycle is differentiated from Lockheed Martin's cyber kill chain model in that the stage after the attacker has penetrated the system is subdivided into internal search, elevation of privilege, and information theft processes and does not include the weaponization stage.

Lockheed Martin's Cyber Kill Chain model accounts for incidents where the network has already been intruded, and it has limitations that can only defend the defenders. Domestic research suggests that a cyber kill chain strategy is needed to counter this limitation [12]. This domestic research [12] proposes to fit the Cyber Kill Chain model of the same system as the "Kill Chain" phase in Korea, which consists of 4 steps, as shown in Table 2.

In this study, we propose a way to build a cyberwarfare framework based on active defense of the Cyber Kill Chain concept.

III. WAYS TO BUILD A CYBERWARFARE OPERATIONAL FRAMEWORK

According to the U.S. Army Cyber Command, cyber operation means the act of planning and synchronizing activities through cyberspace to promote freedom of movement and achieving goals. Operation in cyberspace includes Cyberspace ISR (Cyberspace Intelligence, Surveillance, Reconnaissance), Cyberspace Operational Preparation of the Environment (OPE), Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO), which are largely composed of four activities, each of which is performed under the concept of cyberspace activity [13].

TABLE 2. Proposed inland cyber kill chain.

Section	Contents
Sensor	A cyberspace surveillance system that can monitor an attacker's network or system and a surveillance system that integrates a real-world surveillance system
Decision	Analytical technology that can provide the basis for the strike based on the results of the surveillance system to prevent it from expanding into additional disputes after the Cyber Kill Chain is launched
Cyber Strike	A striking system consisting of hitting the origin of the attack, expanding the support force, and hitting the commander
System of Systems	The above three systems (Sensor, Decision, Cyber Strike) are operating systems to operate organically, not separately.

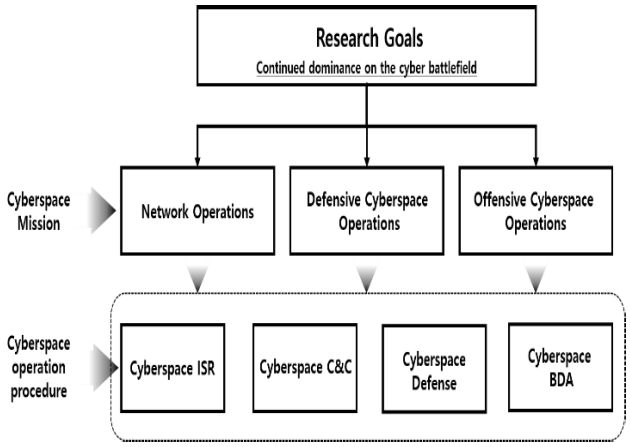


FIGURE 2. Cyberwarfare framework concept.

Cyber ISR is an activity that actively collects information on target targets and malicious attackers or enemy systems necessary to support cyber operations and responses. It provides information to cyber command and control decisions by discovering new threats and understanding the situation based on the results of all actions.

Cyber OPE is an activity to prepare and support Cyber ISR, DCO, OCO, and oversees all operational activities to prepare for cyber attacks and conducts information fusion and sharing.

DCO is an active and passive method to utilize cyberspace, guarantees the Freedom of Manoeuvre in cyberspace, and is performed within the information security framework. It consists of Active Defense, Passive Defense, Security, and Resilience.

OCO refers to the act of creating denial and destruction effects through cyberspace. In the concept of cyberspace, the physical layer, logical layer, persona layer, etc. can occur in a complex manner. In a comprehensive security strategy, offensive cyber operations are expected to collaborate with information operations and predict the damage that occurs in cyberspace.

The cyberwarfare framework proposed in this paper is composed of Cyber Information Surveillance Reconnaissance (ISR), Cyber Command and Control (C&C), Cyber Defense, and Cyber Battle Damage Assessment (BDA) and organizes these four stages in an organic relationship.

The cyberwarfare framework construction plan proposed in this paper is a process of sharing information collected, measured, and managed through four stages: Cyber ISR, Cyber C&C, cyber defense, and Cyber BDA. Based on this, we would like to present an integrated operation plan of the cyberspace operation system and further propose the concept of cyber command and control that can achieve an advantage in cyberspace.

Fig. 3 shows the cyberwarfare framework operation plan. Cyber ISR proceeds with ISR for the target identified and delivers the collected information to the cyber threat information database at Cyber C&C. Cyber Defense studies software-based malware detection technology and threat detection technology, firmware-level malware detection technology, and embedded hardware-based threat detection & response technology based on active defense. The vulnerabilities collected through the research are delivered to the Cyber C&C cyber threat information database. Cyber BDA develops the indicators for cyber assets and damage assessment methods in connection with cyberwarfare and physical wars. The measured and predicted indicators are delivered to the decision support system of the Cyber C&C.

The Cyber C&C prepares a decision support system based on cyber situational awareness by integrating and managing the information delivered at each stage. In addition, scenarios based on the Advanced Persistent Threat (APT) attack were established, as shown in Fig. 4, in order to materialize the concept of integrated operation at each stage. Looking at the scenarios step by step, the Cyber ISR stage is a collection of information about the enemy environment. Tasks were given to detect the signs of attack by an enemy or an attacker that caused cyber threats, collect the attack patterns of the enemy, and analyze the enemy network environment to inform them. In the Cyber BDA stage, the system is responsible for the analysis of the APT attack route and allied assets to be attacked. It analyzes the importance of friendly cyber assets, analyzes the relationship between assets and missions, and predicts damage from enemy attacks. In the Cyber Defense stage, it analyzes allied assets that are targeted for attack and performs the act of detecting vulnerabilities or malicious behavior. The final Cyber C&C stage serves to derive risk by collecting and analyzing information collected from each stage and asset analysis data. Looking at the flow of the scenario, Cyber ISR delivers information about the target of attack, such as the predicted attack method and threat information, to the Cyber BDA and delivers threats such as

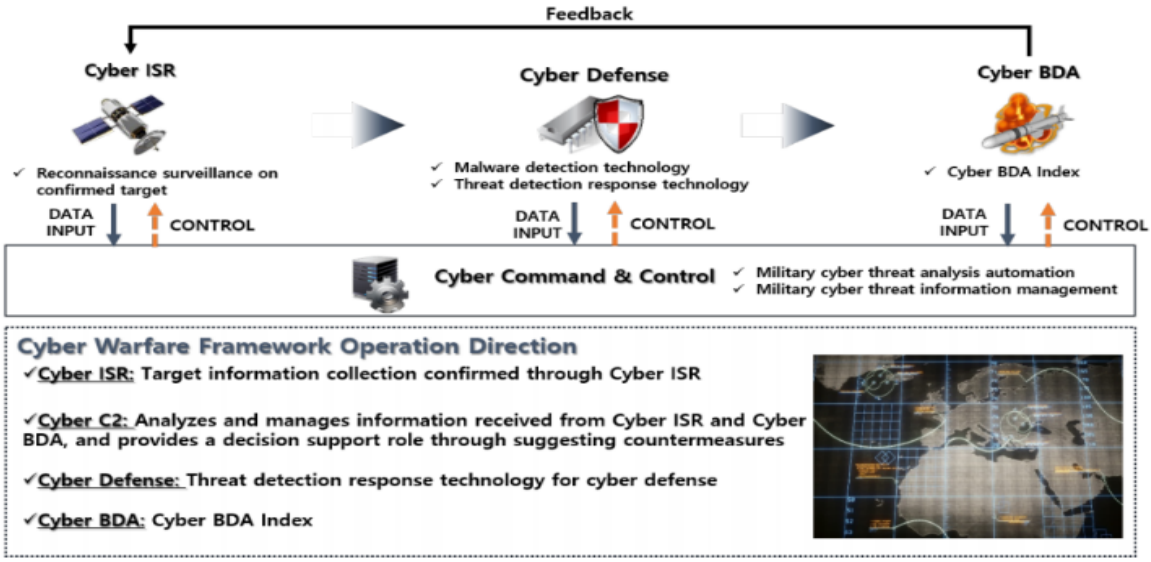


FIGURE 3. Cyberwarfare framework operation plan.

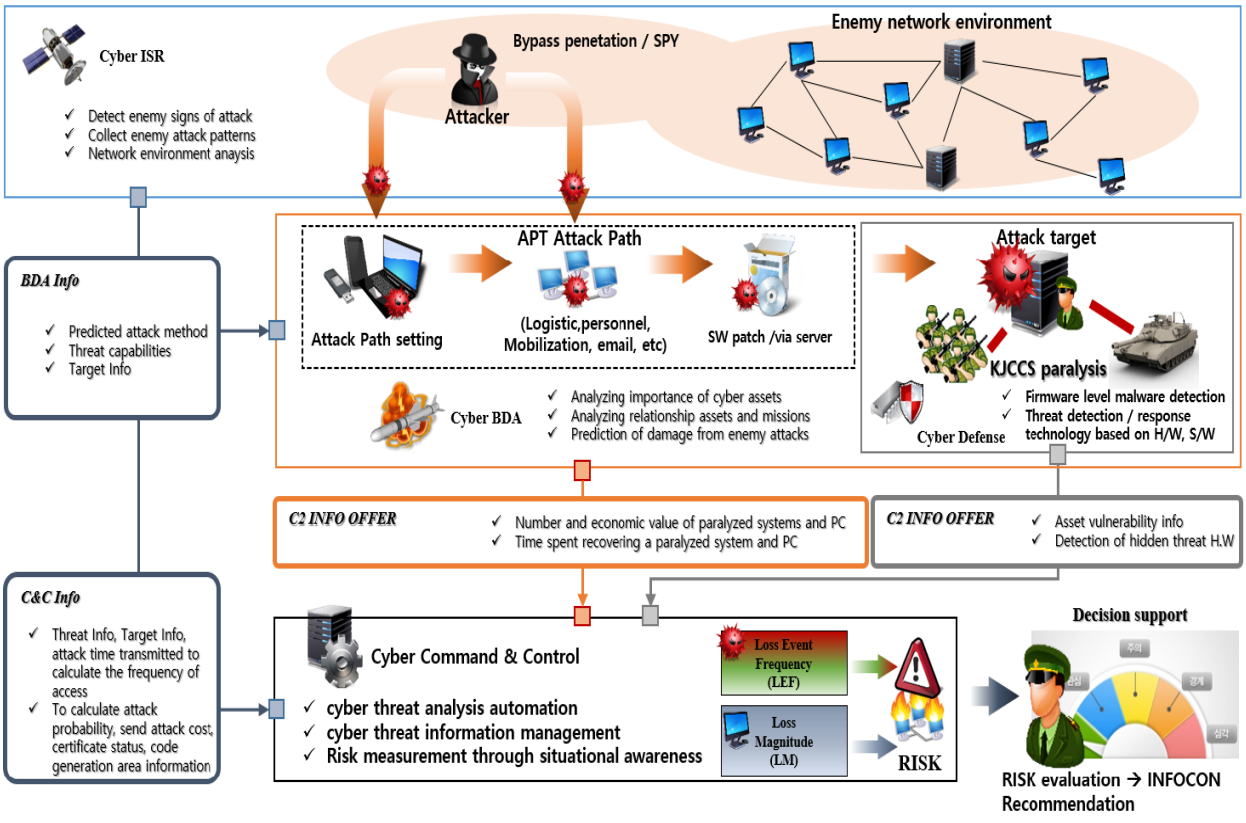


FIGURE 4. Cyberwarfare framework operation plan scenario.

the frequency of attackers to Cyber C&C. Cyber BDA then delivers the damage assessment results to Cyber C&C. The collected information provides information to help decision makers in Cyber C&C.

IV. RATING SCALE

Among the four stages of the cyberwarfare framework proposed in this paper, the evaluation indicators of Cyber BDA are described.

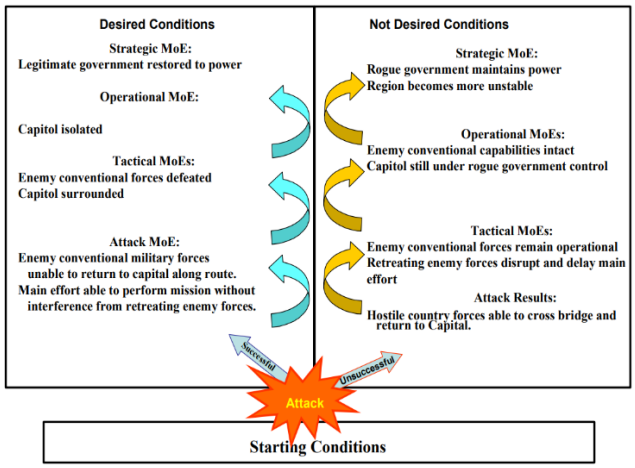


FIGURE 5. MOE and MOP relationship.

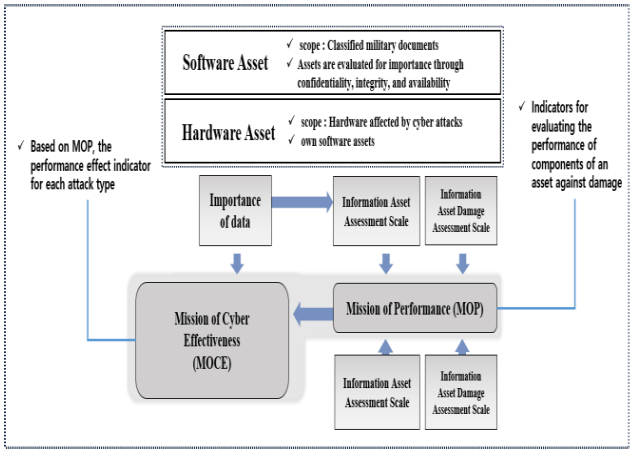


FIGURE 6. MOCE generation process.

A. MEASURE OF EFFECTIVENESS, MEASURE OF PERFORMANCE

Mission analysis packages tasks to achieve a measurement of the mission results. The progress of the mission is measured using a process called Measure Of Performance(MOP) to allocate the capability packages to the operations. MOP is defined as a measure of the performance of a system that can be quantified. The mission analysis process is measured using a process called MOE [14] to determine whether assigned MOPs meet mission requirements and enable job execution. MOE is defined as an indicator of the achievement of a mission. Fig. 5 shows the relationship between Measure Of Effectiveness(MOE) and MOP. In this paper, MOE is used as a modified Measure Of Cyber Effectiveness(MOCE) [15] for cyberwarfare MOCE generation process is shown in Fig. 6.

B. CYBERWARFARE INDICATOR

We designed cyberwarfare indicators for Cyber BDA. The cyberwarfare index consists of MOCE, MOP, and information asset evaluation scales.

TABLE 3. Information asset evaluation scale.

Information asset evaluation scale	unit	Formula
Total PC	number	-
Total Server	number	-
Total Data	MB	-
PC recovery time	Sec	-
Reproduction time by file	Sec	-
SW reinstall time	Sec	-
Network dependence	%	Network connection time / PC uptime
Data importance	Dot	C I A score
Network connection time	Sec	-
Recovery personnel	number	-

TABLE 4. MOP scale.

MOP	unit	Formula
Damaged server ratio	%	(Damaged server / total server) * 100%
Damaged PC ratio	%	(Damaged PC / total pc) * 100%
Recoverable PC Ratio	%	(Recoverable PC / damaged pc) * 100%
Ratio of non-recoverable PC	%	100% - Recoverable PC
Percentage of corrupted data	%	(corrupted data / total data) *100%
Recoverable data rate	%	(recoverable data / corrupted data) * 100%
Ratio of non-recoverable data	%	100% - recoverable data
Average reproduction by file Time	sec	$\left(\sum_{i=1}^{n} i\right) \div n$ (i = reproduction time by file, n = number of file)
SW damage rate	%	Damaged SW / total SW
Total PC recovery time	sec	(PC recovery time * recoverable PC) / recovery personnel
Average recovery time per PC	sec	Total PC recovery time / recoverable PC

The elements of MOP can be divided into human factors and physical factors. In this paper, only the physical or functional damage assessments of the physical factors are the scope of the research. The indicator for the MOP element is basically set as a fixed indicator based on the absence of the introduction of new information assets. The information asset evaluation scale was set to reflect the normal operation status of the information asset.

TABLE 5. MOCE interruption EXP INFO.

DT_i	i-th PC (server) damage time
DS_i	Available memory size(KB) of the damaged file on the i-th PC(server)
R_i	Whether the i-th PC(server) is damaged by the network {1(True), 0(False)}

TABLE 6. MOCE interruption.

NUM	Mission performance indicator	unit
01	Privilege theft attack?	Yes/No
02	Is it related to the mission?	Yes/No
03	Number of systems stopped	number
04	Number of degraded systems	number
05	Estimated system delay time	sec
06	Suspended system recovery time	sec
07	Amount of system memory available	KB

TABLE 7. MOCE Interception EXP INFO.

W_i	Importance of i-th Data
D_i	i-th data size
R_i	Whether the i data is captured {1(True), 0(False)}

MOCE, which is a Measure of Cyber Effectiveness, is a type of cyber attack that is used to calculate damage by making Interruption, Interception, and Modification indicators [16]–[18]. A MOCE makes it possible to measure cyber damage. Through MOCE, you can check the damage level of the attacked user. For the evaluation scale of the interruption, the evaluation index is prepared based on how much the performance deteriorates and how much the work speed is delayed. The damage rate of the MOCE Interruption is as shown in EXP. 1 and includes the information in Table 6.

$$\left\{\left(\sum_{i=1}^{n} DT_i \times DS_i \times R_i\right) \div \left(\sum_{j=1}^{n} DT_j \times DS_j\right)\right\} \times 100 \quad (1)$$

Based on the interception's evaluation scale, an evaluation index is prepared based on how well the allied information has been captured. The damage rate of MOCE Interception is shown in EXP. 2 and includes the information in Table 8.

$$\left\{\left(\sum_{i=1}^{n} W_i \times D_i \times R_i\right) \div \left(\sum_{j=1}^{n} W_j \times D_j\right)\right\} \times 100 \quad (2)$$

Based on the modification's evaluation scale, an evaluation index is prepared based on how much the allied data has been modified from the previous data. The damage rate of the MOCE Modification is as shown in EXP. 3 and includes the information in Table 10.

$$\left\{\left(\sum_{i=1}^{n} (W_i \times D_i + S_i) \times R_i\right) \div \left(\sum_{j=1}^{n} W_j \times D_j + S_j\right)\right\} \times 100 \quad (3)$$

When a cyber attack occurs, the amount of damage is determined by calculating the MOP and MOCE using the corresponding indicators.

TABLE 8. MOCE interception.

NUM	Mission performance indicator	unit
01	Privilege theft attack?	Yes/No
02	Is it related to the mission?	Yes/No
03	Number of systems stopped	number
04	Number of degraded systems	number
05	Estimated system delay time	sec
06	Suspended system recovery time	sec
07	Amount of system memory available	KB

TABLE 9. MOCE modification EXP INFO.

W_i	Importance of i-th Data(SW)
D_i	i-th data size
S_i	i-th SW size
R_i	Whether the i-th data (SW) is modified or deleted {1(True), 0(False)}

TABLE 10. MOCE modification.

NUM	Mission performance indicator	unit
01	Privilege theft attack?	Yes/No
02	Is it related to the mission?	Yes/No
03	Amount of data changed	Mb
04	Importance of changed data	dot
05	Whether damaged data can be recovered	Yes/No
06	Time to recover corrupted data	Sec

V. EXPERIMENT

In this paper, we propose a Cyber BDA in a cyberwarfare framework. Since the damage cannot be directly identified, a simulation for a cyber damage assessment was conducted using DEVSim++.

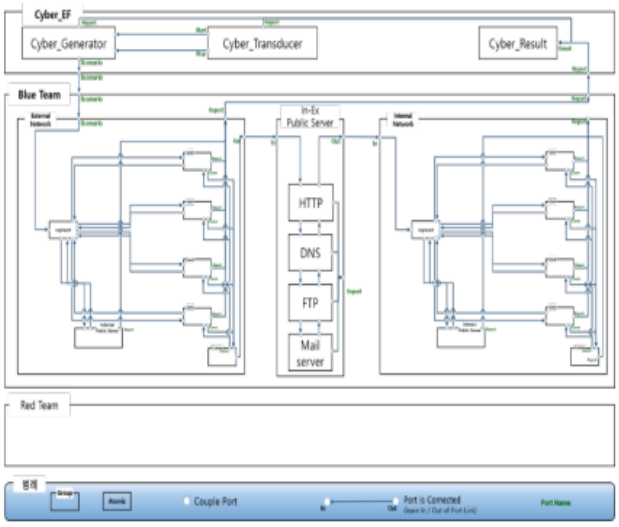


FIGURE 7. Virtual network system structure.

A. SIMULATION NETWORK STRUCTURE

The virtual network structure first consists of Cyber_EF for the execution and operation of the simulation, and Blue Team, the part of the network where cyber attacks and damage occur. In addition, Cyber_EF and Blue Team are composed of modules. First, Cyber_EF is divided into Cyber_Generator, which generates cyber attacks, Cyber_Transducer, which is responsible for running and terminating simulations, and Cyber_Result, which stores the cyber damage of the Blue Team. The Blue Team is divided into external networks, internal networks, internal and external public servers, and the Regiment constituting it.

B. SIMULATION EXECUTION ORDER

The simulation scenario is as follows.

1. Attacker conducts cyber attack and propagation activities on friendly network through elevation of privilege vulnerability
2. Cyber Interruption, Interception, and Modification attacks against multiple randomly selected units (pc, server) among allied cyber network networks
3. Promote damage damage by applying the damage result for the unit of the friendly network to the MOCE formula

The flow of the simulation is shown in Fig. 8.

The initial input values are as follows. For the simulation, we input a file containing the importance of the cyber assets of the unit, PC, and server in the virtually configured network, along with the number of cyber assets. Fig. 9 shows the simulator's input data. In addition, a simulation process is performed to perform cyber attacks according to the virtual network structure. When the attack is over, the damage value for each unit is displayed as a text file, as shown in Fig. 10. The text file consists of the module's existing attribute values and the damaged attribute values. Then, the output text file is

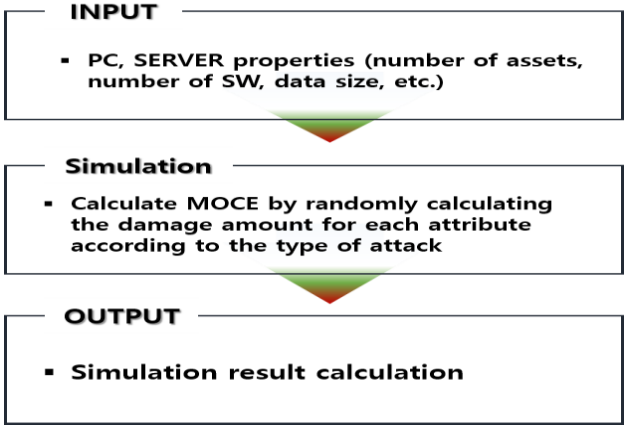


FIGURE 8. Simulation execution flow.

UNIT	Numerical value	Mean
Whole PC num	10	Total PC
Whole Asset num	100	Total Asset
Whole Data size (KB)	6924290048	Total Data size
Whole Software num	1931	Total SW
Whole RAM size (GB)	192	Total RAM SIZE
Recuperator num	2	Recovery number
Comm-Server		
Server bandwidth(Mhz)	15	Server bandwidth
Asset num	36	Asset num
Data size (KB)	1474297856	Data size

FIGURE 9. Simulation input example.

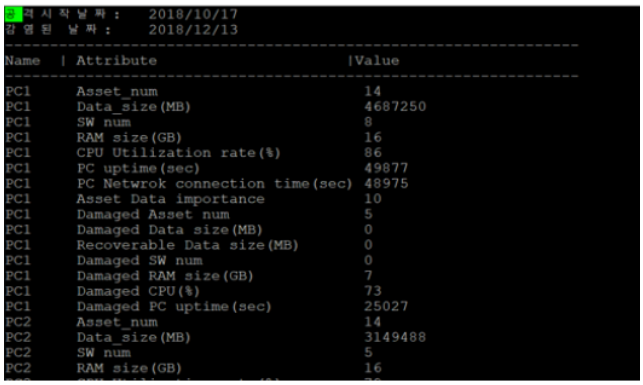


FIGURE 10. Simulation result.

substituted into the MOCE calculation formula to calculate the final damage rate.

C. SIMULATION RESULT VISUALIZATION

After calculating the final damage rate through MOCE, it is intuitively constructed and visualized. The visualization uses the attack classification for each unit. Also, since the damage to the server is more fatal than for a single PC, the damage rate of the PC and the server are divided and expressed by each attack classification. Fig. 11 shows that, in the scenario,

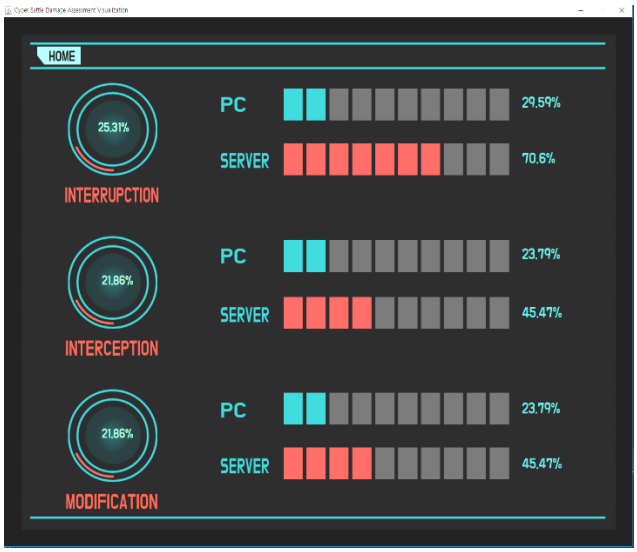


FIGURE 11. Visualization of MOCE damage rate.

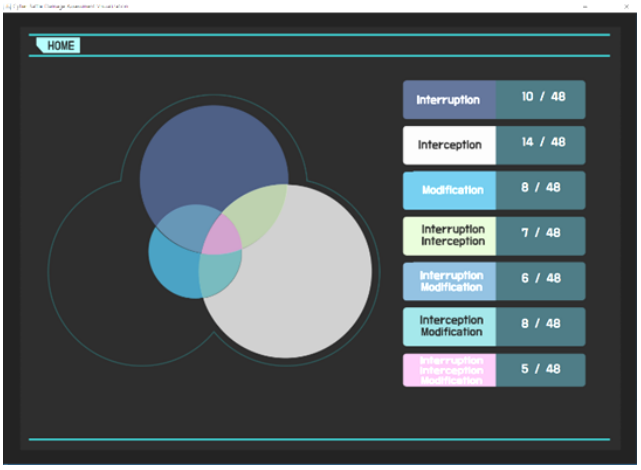


FIGURE 12. Visualization of damage ratio by MOCE.

the amount of server damage of the interruption due to system paralysis is high.

In addition, by knowing the number of PCs and servers for each attack that have been damaged in each unit, it is possible to deal with each damage category. Therefore, as shown in Fig. 12 the number of PCs and servers damaged by the classification of MOCE is expressed.

The intuitive visualization is easy to use as an indicator of judgment in Cyber C&C, so we believe that it can help decision makers.

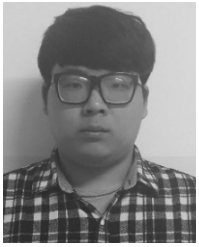
VI. CONCLUSION

In this paper, a cyberwarfare framework consisting of ISR, C&C, Cyber Defense, Cyber BDA was constructed and developed in the cyber battlefield. We presented a concept of cyber warfare that can achieve a sustained strategic advantage. The simulation system for combat damage evaluation was designed and implemented, and the damage evaluation result was visualized as a means to assist the commander's decisions during the command and control phase.

As a future plan, it is expected that the proposed cyberwarfare framework will be developed to provide a framework for future cyber operations that can be used to develop related technologies and operational procedures.

REFERENCES

[1] M. T. Kwon, "A study on the defense cyber warfare exercise," *J. Inf. Secur.*, vol. 9, no. 4, pp. 43–53, 2009.
[2] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, vol. 49, pp. 70–94, Mar. 2015.
[3] *Secretary of Defense*, DoD Publications.
[4] S. A. Hildreth, "Cyberwarfare," Library of Congr. Washington DC Congressional Res. Service, Tech. Rep., 2001.
[5] J. R. Lindsay, "Stuxnet and the limits of cyber warfare," *Secur. Stud.*, vol. 22, no. 3, pp. 365–404, Jul. 2013.
[6] J. Carr, *Inside Cyber Warfare*, 2nd ed. Sebastropol, CA, USA: O'Reilly, 2012.
[7] A. Colarik and L. Janczewski, "Establishing cyber warfare doctrine," in *Current and Emerging Trends in Cyber Operations*. London, U.K.: Palgrave Macmillan, 2015, pp. 37–50.
[8] M. S. Khan, S. Siddiqui, and K. Ferens, "A cognitive and concurrent cyber kill chain model," in *Computer and Network Security Essentials*. Cham, Switzerland: Springer, 2018, pp. 585–602.
[9] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare & Security Research 1.1*, vol. 80. 2011.
[10] *Cybersecurity Test and Evaluation Guidebook. Version 2.0*, Dept. Defense, Richmond, VI, USA, 2018.
[11] *HPE Attack Life Cycle Use Case Methodology*, Hewlett Packard Enterprise, San Jose, CA, USA, 2016.
[12] J.-W. Yoo and D.-W. Park, "Cyber kill chain strategy for hitting attacker origin," *J. Korea Inst. Inf. Commun. Eng.*, vol. 21, no. 11, pp. 2199–2205, 2017.
[13] *ARCYBER The NEXT Battlefield*, Dept. Defense, Richmond, VI, USA, Dec. 2013.
[14] E. P. Blasch, R. Breton, and P. Valin, "Information fusion measures of effectiveness (MOE) for decision support," *Proc. SPIE*, vol. 8050, May 2011, Art. no. 805011.
[15] J. Park, D. Kim, D. Shin, and D. Shin, "Design and implementation of simulation tool for cyber battle damage assessment using MOCE (measure of cyber effectiveness)," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 29, no. 2, pp. 465–472, 2019.
[16] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, "Computing the impact of cyber attacks on complex missions," in *Proc. IEEE Int. Syst. Conf.*, Apr. 2011, pp. 46–51.
[17] S. Musman, A. Temin, M. Tanner, D. Fox, and B. Pridemore, "Evaluating the impact of cyber attacks on missions," in *Proc. MITRE Tech. Paper*, Jul. 2010, pp. 446–456.
[18] S. Musman and A. Temin, "A cyber mission impact assessment tool," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Apr. 2015, pp. 1–7.



SUNGJOONG KIM received the M.S. degree from Sejong University, in 2018. His research interests include cybersecurity and data mining.

JIWON KANG received the M.S. degree in computer science (information security) from Yonsei University, and the Ph.D. degree in information security from Kyonggi University, South Korea. He is currently a University-Industry Collaboration Professor with the Computer Engineering Department, Sejong University, South Korea. His research interests include cyber-space operations in defense and convergence security.

HAENGROK OH received the B.S. degree in computer science processing and the M.S. degree in computer science from Inha University, Incheon, South Korea, in 1987 and 1989, respectively, and the Ph.D. degree in computer science from Korea University, Seoul, South Korea, in 2004. Since 1989, he has been a Researcher with the Agency for Defense Development (ADD), South Korea. His research interests include cybersecurity and cyber C2 (command and control).

DONGIL SHIN received the B.S. degree in computer science from Yonsei University, Seoul, South Korea, in 1988, the M.S. degree in computer science from Washington State University, Pullman, WA, USA, in 1993, and the Ph.D. degree from the University of North Texas, Denton, TX, USA, in 1997. He was a Senior Researcher with the System Engineering Research Institute, Deajeon, South Korea, in 1997. Since 1998, he has been with the Department of Computer Engineering, Sejong University, South Korea, where he is currently a Professor. His research interests include information security, bio-signal data processing, data mining, and machine learning.

DONGKYOO SHIN (Member, IEEE) received the B.S. degree in computer science from Seoul National University, South Korea, in 1986, the M.S. degree in computer science from the Illinois Institute of Technology, Chicago, IL, USA, in 1992, and the Ph.D. degree in computer science from Texas A&M University, College Station, TX, USA, in 1997. From 1986 to 1991, he was with the Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he was a Principal Researcher with the Multimedia Research Institute, Hyundai Electronics Company, South Korea. He is currently a Professor with the Department of Computer Engineering, Sejong University, South Korea. His research interests include natural user interaction, information security, biosignal data processing, and ubiquitous computing.