

Received 7 April 2023, accepted 28 April 2023, date of publication 8 May 2023, date of current version 11 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3273612

## RESEARCH ARTICLE

# Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated With Cyber Asset Damage

JISOO JANG<sup>1,2</sup>, KOOKJIN KIM<sup>1,2</sup>, SUKJOON YOON<sup>3</sup>, SEONGKEE LEE<sup>4</sup>,  
MYUNGKIL AHN<sup>4</sup>, AND DONGKYOO SHIN<sup>1,2,3</sup>, (Member, IEEE)

<sup>1</sup>Department of Computer Engineering, Sejong University, Seoul 05006, South Korea

<sup>2</sup>Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, South Korea

<sup>3</sup>Cyber Warfare Institute, Sejong University, Seoul 05006, South Korea

<sup>4</sup>Cyber Technology Center, Agency for Defense Development, Seoul 05771, Republic of Korea

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


This work was supported by the Defense Acquisition Program Administration and Agency for Defense Development under Contract U1210010XD.

**ABSTRACT** As operations previously undertaken only in physical space in the past have changed to operations that include cyberspace, it is crucial to define the concept of “cyber missions” clearly. In this study, “cyber mission” refers to any military operation or process that utilizes cyber systems to perform actions in accordance with orders delivered to them. Because a weapon system that utilizes a cyber system executes actions based on the commands transmitted to the cyber system, it is necessary to analyze how attacks from cyberspace affects such a weapon system. To this end, it would be meaningful to analyze the tools used to analyze the mission impact of physical weapon systems linked to cyber-attacks. The US military’s Joint Munitions Effectiveness Manual (JMEM), which contains the results of analyzing the effects of weapon systems, does not include analysis results for the effects of weapon systems on cyber-attacks. In this study, based on the analysis of the effectiveness of physical warfare, the damage to cyber assets was quantified and associated to calculate the cyber index for the analysis of operational efficiency. In connection with JMEM, the results of combat in cyberspace and the effects of physical operations were compared and analyzed to propose a framework to judge the impact of missions, and the performance was tested. To verify the effectiveness of the proposed framework, domestic and foreign operational scenarios were analyzed and designed, assets were defined, and experiments were conducted. These experiments showed that a greater decrease in the cyber mission effect value was related to a greater effect on physical operations. This framework could be used in a variety of operations to predict the physical impact of a cyber-attack and will help determine the next step in an operation.

**INDEX TERMS** Cyber warfare, cyberspace, cyber operation, cyber weapon system, mission impact analysis.

## I. INTRODUCTION

As time goes by, cyberspace is becoming increasingly important in society. In the past, cash was mainly used, which made it necessary to go in person to purchase goods or enjoy cultural life. However, as the Internet evolves, all of these things happen more online than in the past, which makes cyberspace

The associate editor coordinating the review of this manuscript and approving it for publication was Sathish Kumar .

security increasingly important [1]. Likewise, from a military point of view, operations performed only in physical space are changing to operations that include cyberspace according to these technological advances. In addition, physical weapon systems such as physically guided missiles and unmanned drones are also changing to use cyber systems. These weapon systems executes actions in physical space according to commands transmitted to the cyber system. This means that damage in cyberspace affects their behavior in physical space.

For example, an unmanned drone system could be directed to a different destination than the user intended due to a cyber-attack. A car's self-driving system could also drive to a different location than its destination or fail to recognize a wall, putting occupants at risk.

The United States of America developed the Joint Munitions Effectiveness Manual (JMEM) to assess the effects of physical weapon systems, including the results of analyzing such effects, which is now being developed and utilized for existing physical operations. The JMEM contains data from the systematic study of the effectiveness of each type of ammunition in fields such as Air to Air, Air to Surface, Surface to Surface, and special weapons. This helps to predict the effect in real situations by measuring the effectiveness of ammunition according to various battlefield environments and situations. However, the JMEM is applied only to physical weapon systems, and it is impossible to measure its effectiveness in cyberspace [2]. Measuring damage in physical space does not tell you what damage has occurred in cyberspace. Therefore, when a cyber-attack causes physical damage to targets other than the original target, it is possible to measure damage in physical space, but this may not be what commanders and staff want. Because of these issues, many researchers have been working on measuring damage in cyberspace [4], [5], [6], [20], [21], [22], [23]. However, because these studies measure damage only in cyberspace, it is not possible to know the direct change in physical space following cyber-attacks. This means that various accidents due to errors occurring in physical space cannot be prevented. Therefore, this study analyzed the effects in physical space of damage in cyberspace.

In this study, the damage in cyberspace and damage in physical space are linked and analyzed. We identified the interface between cyberspace and physical space to connect the two different spaces. After quantifying the identified contact elements, they were used to measure and analyze the effects of cyberspace missions and physical space missions in association with each other. This is expected to help operational commanders make judgments when conducting operations in the operational planning stage, and is expected to contribute as follows.

a) From a military point of view, we expect damage from various cyber-attacks in the operational preparation stage. Commanders can use our proposed framework to assist them in devising countermeasures based on this damage.

b) Various companies can utilize this framework. Based on the description in Section V, it can be used in private companies by identifying and utilizing contact points.

According to the above contributions, this paper consists of nine sections. In Section II, describes the background of this study. Since it is very important to assess and analyze the impact of cyber operations, we define cyber operations and define the threats that occur in cyberspace. In addition, to understand the concept of cyber operations, we defined cyberspace, distinguished between cyber operations and physical operations in operations based on The U.S.

Joint Operation Planning Process (JOPP) [11], and identified the scope of cyber operations. In Section III, operations and cyberspace are defined to conduct research. In addition, to associate physical space and cyberspace, methods for measuring the effectiveness of physical weapon systems were selected, and cyber mission-based damage assessment techniques were investigated. After that, cyber-attack was defined to define attack behavior in cyberspace. Based on the data referenced in Section III, Section IV shows how an operation to conduct both physical and cyber operations was selected and a scenario was designed. In Section V, explains how to identify interface elements between physical space and cyberspace and how to apply them to analyze the effectiveness of various operations. In Section VI, presents a framework for conducting effectiveness analysis using the scenario designed in Section IV and the interface elements identified in Section V, Section VII shows how experiments using the framework were conducted. In Section VIII, we compared the framework we proposed with previously published cyber damage assessment cases. Finally, In Section IX, deals with the expected effects of the proposed framework and future research directions. The proposed framework was found to be more applicable to various environments than previous research, due to its utilization of a damage calculation method based on the Common Vulnerability Scoring System (CVSS). Furthermore, by being associated with physical space, it is possible to more accurately predict damage in real-world situations. deals with the expected effects of the proposed framework and future research directions.

## II. BACKGROUND

### A. DEFINITION OF OPERATION ENVIRONMENT AND CYBER THREATS

#### 1) DEFINITION OF CYBERSPACE OPERATIONS

An operation is a combat action executed according to a strategic plan to achieve a certain goal. Chapter 1 of US Army Doctrine Publication 3-0 (ADP 3-0) [7] describes military operations, the operational environment in which they are conducted, and threats. The operational environment includes considerations at the strategic, operational, and tactical levels of warfare. The operational level focuses on the design, planning, and conduct of operations using operational technologies, linking the tactical use of forces with national and military strategic objectives. According to the US Joint Publication (JP 3-0) [8], the operational environment is defined as the collection of conditions, circumstances, and influences that affect the use of capabilities and influence a commander's decisions. The operational environment includes physical domains and information environments in the air, land, sea, and space domains. The operating environment has the characteristic of constantly changing because the operating environment is composed of many relationships and interactions among interrelated variables. Because of this, commanders must continually evaluate the operating environment and re-evaluate assumptions.

## 2) DEFINITION OF CYBER THREATS

JP 3-0 [8] defines a threat as any attempt to disrupt the joint force's freedom of action in the air, land, sea, space, and cyberspace domains, and understanding that threat is critical to operations. Modern information technology is making the information environment, including cyberspace and the electromagnetic spectrum, an indispensable environment for military operations. All actors in the information environment, whether hostile, friendly, or neutral, are vulnerable to attack through physical, psychological, cyber, or electronic means. In this study, the operational environment was defined as the conditions and situations that affect operations, such as the commander's ability, enemy confrontation situation in physical space, and data possession list in cyberspace. Threats were defined as actions such as malicious code infection, document theft, data destruction, and data tampering through cyber-attacks.

## B. DEFINITION OF CYBERSPACE AND CYBERSPACE OPERATION RANGE

The US National Institute of Standards and Technology (NIST) defined cyberspace as a global domain within the information environment consisting of interdependent networks of information system infrastructure in CNSSI 4009 [9], which was prepared by the Committee on National Security Systems (CNSS). This includes the Internet, communication networks, computer systems, and embedded processors and controllers.

US Joint Publication 3-12 (JP 3-12) [10], which was prepared by order of the Chairperson of the Joint Chiefs of Staff (CJCS), deals with cyberspace operations (COs). A CO is used to achieve a goal within or through cyberspace and uses the capabilities of cyberspace for this purpose. Cyberspace is part of the information environment, but is dependent on the physical air, land, sea, and space realms. COs use links and nodes located in the physical realm, perform logical functions to create effects in cyberspace, and affect the physical realm as needed. Cyberspace is described by three interrelated hierarchical models: physical networks, logical networks, and cyber personas. The physical network layer consists of IT devices and infrastructure in the physical domain that provide for the storage, transmission, and processing of information within cyberspace, including data storage and connectivity that transfers data between network components. A logical network layer consists of network elements related to each other in a way that is abstracted from the physical network, based on the logic programming (code) that drives the network elements. A cyber persona layer is a cyberspace perspective created by abstracting data from a logical network layer using rules applied to the logical network layer to develop a description of a digital representation of an actor or entity identity in cyberspace (cyber persona). It consists of network or IT user accounts (whether human or automated) and the relationships between them.

The JOPP [11] is a process consisting of a series of logical steps to investigate a mission. The JOPP is a proven process for organizing the work of commanders, staffs, subordinate commanders, and other partners to develop plans for problems to be addressed. It also enables commanders and staffs to organize planning activities, share a common understanding of the mission and commander's intentions, and develop effective plans and orders. The JOPP is not a formalized procedure that must be followed, but as JOPP procedures are followed, commanders modify the plan as needed during the operation and execution, helping to keep the broadest possible perspective to question the continuing relevance and suitability of the mission.

Just as general users cannot use a manager's data, the accessible data and actions differ depending on the owner of the network equipment. This study included cyberspace because the operation behavior differs depending on the owner of the network equipment. Therefore, in this paper, cyberspace is defined as a network space where users perform actions such as information browsing, transmission, and document preparation in order to create and distribute operational command documents as part of the information environment. In addition, the scope of operations in cyberspace is identified as the joint operation planning process and operation evaluation procedure, as shown in Figure 1. Based on the identified information, the cyber operation scope and physical operation scope were divided for the main purpose of this study, linking cyber and physical spaces. Changes in cyberspace that affect physical space can be identified as changes in planning orders and preparation stages that exist within the scope of cyber operations. Thus, in this study, stages 3 to 7, the scope of cyber operations, were set as the research scope.

## C. WEAPON SYSTEM EFFECTIVENESS ANALYSIS

The JMEM is a manual that specifies weapon system effects such as the killing probability and killing effect, or armaments, based on information on the battlefield environment (target error range, number of armaments to be loaded, armament effects such as fragmentation and storming, etc.). In the JMEM, calculating any probability (e.g., the kill probability) refers to the probability of success out of the total number of trials, rather than expressing success and failure as yes/no, as well as the percentage of successful results among multiple trials. In other words, it is explained by the killing effect (proportion) and killing probability, which is the probability that the result of one attempt will be successful [2]. In this study, a cyber behavior that damages a network is defined as cyber weapon system based on a calculation of the effect of the physical weapon system using the open version of JWS (JMEM Weaponneering System), a tool based on the JMEM.

## III. RELATED WORK

### A. CYBER MISSION-BASED DAMAGE ASSESSMENT

The MITRE Corporation's NOEL modeled three layers: Mission Process (Mission Model), Mission System

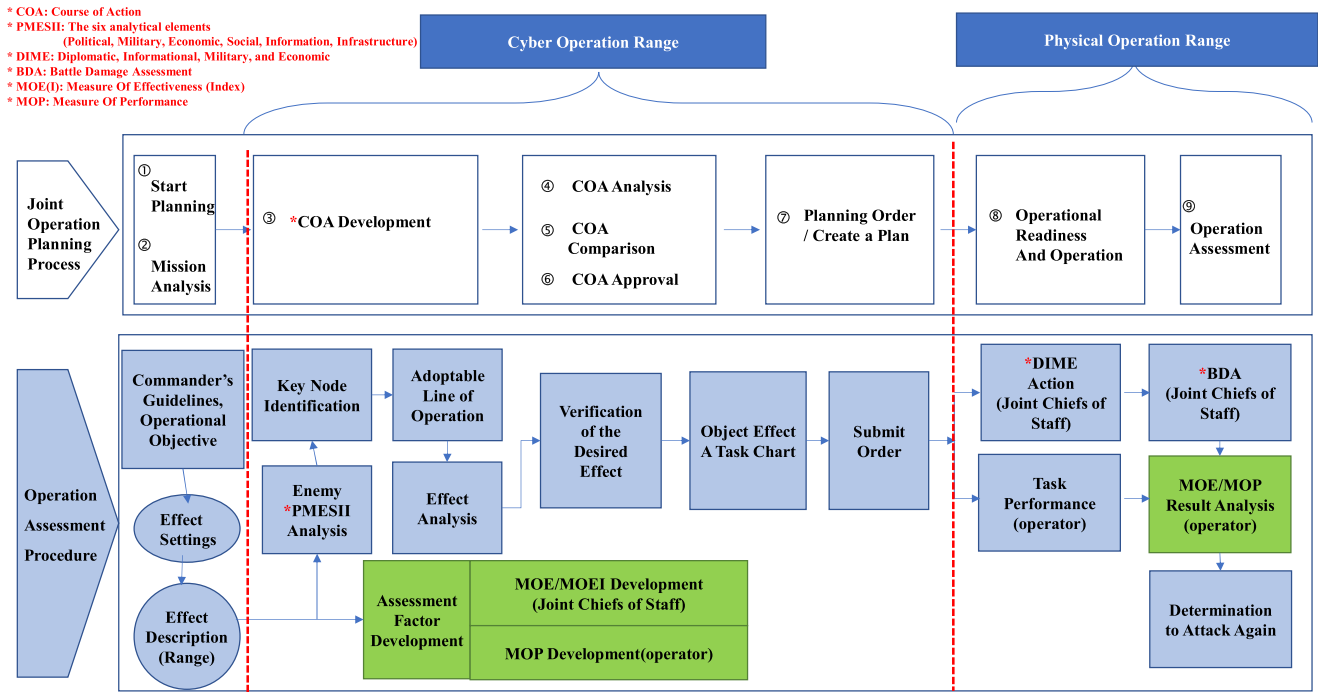


FIGURE 1. Identifying the scope of cyber operation in joint operation planning process.

(Infrastructure Model), and Cyber Attacker/Defender's Tactics, Techniques, and Procedures (TTPs). Based on the mission dependency structure presented by Jakobson et al. [3], AMICA (Analyzing Mission Impacts of Cyber Actions) modeling was presented as a concept in which assets entered in cyberspace ultimately affect missions. The mission dependency structure is shown in Figure 2. AMICA conducted simulations for each model for various mission and threat scenarios and quantified the impact in terms of mission-based measures. As shown in Figure 3, the model has a hierarchical structure and is managed independently. The model consists of a total of four models: attack, defense, infrastructure, and mission. AMICA's process creates one mission scenario as a mission model. If attackable methods exist in the created mission scenario, the attack methods are modeled and processed, and a defense model to defend against the attack is created. These exist as physical parameters and are applied to the infrastructure model. Then, the performance of the mission is analyzed by simulation, and a battle damage assessment (BDA) is calculated [4].

In order to overcome the limitations of existing commercial off-the-shelf (COTS) tools for process modeling, CMIA (a cyber mission impact assessment tool) was developed to analyze, monitor, and manage cyber resources in mission situations according to mission goals and the results and understanding of cyber resources. CMIA is used as a metric for cyber mission risk assessment and supports system assessment by simulating the application of potential security and resilience methods to systems within a mission context. CMIA evaluates the impact of missions by considering

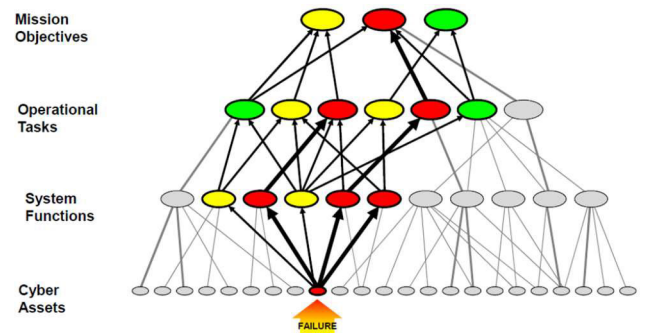


FIGURE 2. Mission dependency structure.

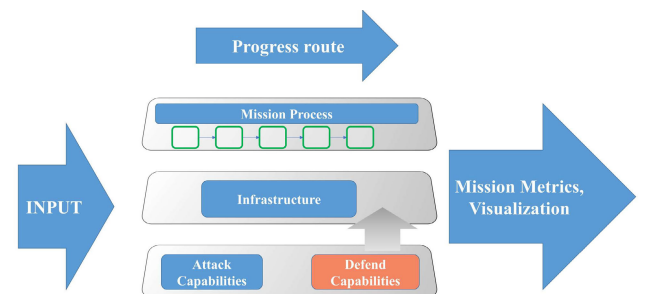


FIGURE 3. AMICA framework process.

six attack instances: degradation, interruption, interception, modification, fabrication, and unauthorized use attacks [6].

A previous study by this research team [12] presented a cyber combat damage assessment framework to evaluate the

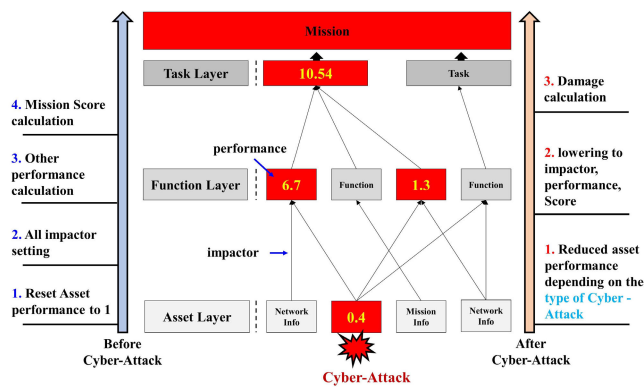


FIGURE 4. Cyber battle damage assessment framework workflow.

TABLE 1. Asset performance formula description.

parameter	definition
$A$	Asset performance value
$V$	Vulnerability factor (1-5)
$F$	Number of assets used in the function
$\alpha$	Expert assessment score (1-5)

mission damage caused by cyber-attacks in military operations. The cyber battle damage assessment framework was composed of a hierarchical structure in the order of assets, functions, tasks, and missions based on the mission subordination structure of the US MITRE. It was assumed that cyber-attacks occurred in assets, and damages from assets to missions were measured, showing that damages to cyber assets also affected the upper layers. Quantitatively calculating the damage incurred during a mission and delivering it to the commander helped the commander to make a quick judgment in a wartime situation. The cyber battle damage assessment framework is performed on two scales: performance and impact. The performance is the degree to which a component is used to perform its mission, and the impact refers to the extent to which the relevant layer affects the mission. In order of hierarchy, the task performance capability is calculated in four steps through the initialization of asset performance, setting of impact, and calculation of the performance of functions and tasks. Figure 4 is a picture explaining this mechanism. The final calculated mission capability is measured before and after the cyber-attack to measure the cyber mission impact caused by the cyber-attack. In Figure 4, the Infra Layer includes the asset layer and connection information between assets.

a) Measuring asset performance and impact: Asset performance (Equation 1) describes the value of an asset in its mission. It is a modified calculation formula based on value engineering, and the parameters are shown in Table 1.  $V$  is a vulnerability coefficient that measures cyber-attacks in relation to confidentiality, availability, and integrity by classifying them as high, medium, or low. In the event of a cyber-attack, asset performance deteriorates as  $V$  fluctuates.

TABLE 2. Function performance formula description.

Parameter	Definition
$F(P)$	Function's Performance
$F_w$	Function weight, Number of branches connected to the Function
$A_n(P)$	Performance of $n$ th asset connected to Function
$A_n(I)$	Impactor of $n$ th asset connected to Function

The asset's impact was judged to be the one that has a greater impact on the mission, as the asset is used for multiple functions. The degree of influence was calculated by the number of branches connected to the functional layer. This cited the notion that the more branches connected to a node in the network, the more important the node is [23].

$$A = (F\alpha)/V \quad (1)$$

b) Measuring functional performance and impact: Functional performance refers to the extent to which a function is used in its mission. Function performance is calculated based on asset performance and impact, with more associated assets having a greater impact on function performance. It is calculated as shown in Equation 2, and the parameters are shown in Table 2.

$$F(P) = \left( \sum_{n=1}^{F_w} A_n(P) \times A_n(I) \right) \times F_w \quad (2)$$

If the function has an impact on the mission, the function influence is calculated by multiplying the function execution time influence, when the function is not performed within the set time, and the accuracy impact, when the performance result is not accurate. The effect of the function execution time is calculated as the function execution time compared to the task execution time. If there is a delay in function execution due to an attack, it is calculated through the product of the delayed function time compared to the delayed task time and the influence of the initial function execution time, as shown in Equation 3.

$$Func\ Time\ Impactor = \frac{InitTime_{func}}{InitTime_{task}} \times \frac{DelayTime_{func}}{DelayTime_{task}} \quad (3)$$

The accuracy impact has an initial value of one because there are no assets initially compromised. If they are compromised by a cyber-attack, the initial accuracy impact is calculated by subtracting the number of assets being compromised from the number of assets functioning, as shown in Equation 4.

$$Func\ Acc\ Impactor = 1 - \frac{Numberofattackedassets}{Funcweight} \quad (4)$$

c) Job performance measurements: Reduced work only deals with the performance and does not separately measure the impact on the job. Because task performance is calculated as the sum of the product of the functional performance and influence, the task performance differs depending on the

**TABLE 3. Function performance formula description.**

parameter	definition
$T(P)$	Task's Performance
$T_w$	Task weight, Number of branches connected to the Task
$F_n(I)$	Performance of $n$ th Function connected to the Task
$F_n(P)$	Impactor of $n$ th function connected to the Task

function. Equation 5 describes the performance of this task, and the parameters are shown in Table 3.

$$T(P) = \left( \sum_{n=1}^{T_w} F_n(I) \times F_n(P) \right) \times T_w \quad (5)$$

d) Measurement of mission performance capability: Mission performance capability is the sum of all the mission performance levels, and the final mission performance capability is measured according to the mission performance capability.

As discussed above, all the studies were conducted in a hierarchical structure with the concept that damage to assets affects missions. Similarly, in this study, it is composed of a 4-tier structure of asset-function-task-mission, and the research was conducted based on the framework presented in the previous research [12] of this research team.

## B. CYBER ATTACK

A cyber-attack causes effects such as degradation, disruption, and destruction in cyberspace or causes effects in the physical realm. In JP 3-12, cyber-attacks are divided into two types of attacks: denial and manipulation. A denial attack is defined as a form of deterioration in performance by denying access or work to a target, or delaying, i.e., interfering through a temporary denial, or destroying access to a target by making it unrecoverable. Manipulation is the control or alteration of information, information systems, networks, etc. in cyberspace through the use of deception, conditioning, spoofing, counterfeiting, and other similar techniques. At this time, the target network may appear to operate normally with secondary or tertiary effects, including physical effects, until the effects of the primary attack are revealed [10].

In September 1999, the National Cybersecurity FFRDC (NCF), a federally funded cybersecurity research organization operated by the MITRE Corporation, studied common vulnerabilities and exposure (CVE) systems for the general public. CVE is a vulnerability enumeration system that gives each publicly known vulnerability a different name, allowing users to talk about a particular vulnerability using that name. All the vulnerability data of CVE are managed by CVE identifiers, with these identifiers assigned by CNA, the CVE numbering authority. There are over 100 CNAs representing security companies, research institutes, and major IT vendors. Key information in a CVE includes reference information, which may include a brief description of the security vul-

nerability or exposure, links to vulnerability reports, and recommendations [13].

CVSS was introduced by the National Infrastructure Advisory Council (NIAC) and is currently managed by the Incident Response and Security Teams Forum (FIRST). CVSS helps security managers prioritize vulnerabilities by providing metrics of relative severity. CVSS assigns each vulnerability a quantitative value from 0 to 10, with higher values indicating higher severity. CVSS was designed as an open framework consisting of three groups of metrics: 1) a primary metric that describes the general nature of the vulnerability, 2) an optional temporal metric that indicates the change in severity over time, and 3) an optional environment metric that is unique to a particular user, organization, or business environment. The primary metric can be used alone or in combination with the two other optional metrics [14].

In this study, a cyber-attack was defined as an act of destroying, falsifying, or stealing data used for the operation of an asset through a CVE that exists in the designed asset.

## IV. SCENARIO DESIGN

This study was conducted based on a mission. In order to carry out a mission, an execution procedure is required, and a systematic mission execution procedure can be viewed as an operation. There are various types operations such as ground operations, sea operations, air operations, and cyber operations, and the Army Publishing Directorate (APD) documents and discloses various operational information that can be disclosed.

According to Army Techniques Publication (ATP) 3-09.12 [15] and Field Manual (FM) 3-09 [16], counter-fire warfare involves enemy weapons, target acquisition (TA) assets, surveillance and reconnaissance equipment, C2 installations, and communication and logistic sites. It is a ground-to-ground operation that protects allies, combat functions, and facilities from indirect enemy fire. Because counter-fire warfare identifies the location of a target through network communication between batteries and then concentrates fire-power on it, if smooth communication is not possible due to unstable network communication, the operation may not proceed and may be changed to a CAS (Close Air Support) operation. In JP 3-09.3 [17], a CAS operation is an operation that supports fire from the air at the request of a ground unit, and is an operation that includes two domains, air and ground. In CAS operations, cyberspace plays a role in connecting the two domains, terrestrial and airborne. Therefore, a CAS operation was suitable for analyzing the mission effects caused by cyber-attacks in various operations and environments, which was the goal of this study.

Therefore, this study designed the following scenario based on a CAS operation.

- Battalion units detect targets in friendly contact areas.
- The contact area commander decides to request a CAS.
- The unit notifies Tactical Air Control Party (TACP).
- Allied commanders go through higher echelons and request a CAS from the Air Force.

- e) Enemy cyber forces infiltrate our internal network.
- f) Enemy cyber forces stealthily attack (tamper/steal/destroy) Air Tasking Order (ATO) document creation elements to minimize the effectiveness of friendly operations.
- g) There is decreased operational effectiveness of friendly forces in response to enemy cyber-attacks (delayed CAS attack, failure to connect ground forces, failure to recognize targets).
- h) The content and effectiveness of enemy cyber-attacks are analyzed.
- i) A determination is made about whether to re-execute the CAS-requested operation based on the analyzed content.

## V. METHOD TO COMBINE CYBER AND PHYSICAL ELEMENTS

### A. DEFINITIONS OF MOE AND MOP

These terms refer to a course of action for evaluating cyberspace operations as the joint force progresses toward mission completion. This evaluation includes carefully comparing predicted outcomes with operational physical elements that determine the overall unit operational effectiveness to help establish a commander's determination to achieve a desired end state, objective, or task performance. These are defined in JP 3-12. The measure of effectiveness (MOE) evaluates changes in the system's behavior, capabilities, or operational environment and measures task efficiency, performance direction, quality of action, and appropriateness of action. An example in CAS operations is ATO information. When a part is modulated, the corresponding elements can be viewed as the MOE. The measure of performance (MOP) is a criterion for measuring task performance or completion, and is an objective standard for task achievement, the amount of performance in operations, and the amount of action. The reduced success rate of a CAS operation on the next day due to the modulated CAS ATO can be viewed as the MOP.

### B. MOE AND MOP OF PHYSICAL OPERATIONS AND CYBERSPACE ASSESSMENT

As mentioned in 3-A, the MOE and MOP can be part of the ATO information in CAS operations, which refers to the type of weapon system, operation request time, operational unit, target, and operational location from the perspective of physical operations. The MOP is from the point of view of physical operations, and includes effects such as the range of destruction and number of people killed, as well as the probabilities of destruction and killing. Both the MOE and MOP of physical operations are included in the JMEM.

If the factors to be applied to the JMEM are modulated due to a cyber-attack before measuring the effect of the physical weapon system using the JMEM, the resulting MOP will lead to a different direction from the original purpose. However, since the result is derived according to the elements applied to the JMEM, it proceeds regardless of information about the change or destruction of elements. Therefore, it is necessary

to know the damage caused by cyber-attacks in connection with cyberspace.

In this study, JWS, which is programmed with the JMEM, was used, and because JWS input elements can be subject to tampering and destruction, the corresponding elements were identified as target elements.

### C. CONTACT ELEMENT QUANTIFICATION

Because the effect in physical operations differs depending on the identified target element, this study defined it as a physical operation impact score, and the initial value was defined as one.

#### 1) METHOD OF QUANTIFICATION

In order to quantitatively calculate the physical motion impact score, this study used a complicated method that obtained accurate measurements based on expert experience and a simple method that measured in a simple form such as zone classification.

There are various elements that can be input to the JWS, such as the error range of the target and number of equipped weapons. All of these elements can be changed according to the actual operational time and battlefield environment. That is, it is impossible to generalize and measure all the factors. Therefore, the two measurement methods used in this study are explained using the target position as an example.

a) Complicated method: The complicated method is a method based on the judgments of the operational commander and experts. The commander must analyze the battlefield environment in detail to proceed with the operation and prepare a plan to measure all the factors individually. For example, if the target location is a location that affects the enemy, even if it is different from the actual mission goal, it can cause damage to the enemy. Thus, the effect of a cyber-attack can be considered insignificant. However, if the location of the target is changed close to the position of the allies, damage to the allies occurs, and cyber-attacks are highly effective. If you are in a position where you cannot inflict damage on the enemy and change to a target position similar to the existing target, the operation of the allies will fail. This can be expressed as a concave function and is shown in Equation 6. When expressed as a graph, it is shown in Figure 5, where X and Y are the coordinates of the battlefield, and Z is the physical operation impact score. However, As previously mentioned, similar targets that cannot cause damage to the enemy will result in a failed ally's mission, so the physical mission impact score will be measured at 0.3 or lower.

$$Z = 1 - \sqrt{(X^2 + Y^2)} \quad (6)$$

However, it is important to note that if the physical operation impact score (Z) is based on factors other than just the target location, the score may not necessarily fall within the range of 0 to 1. In such cases, it is necessary to normalize the score to ensure that it falls within the appropriate range. This can be achieved through a process of rescaling or standardization,

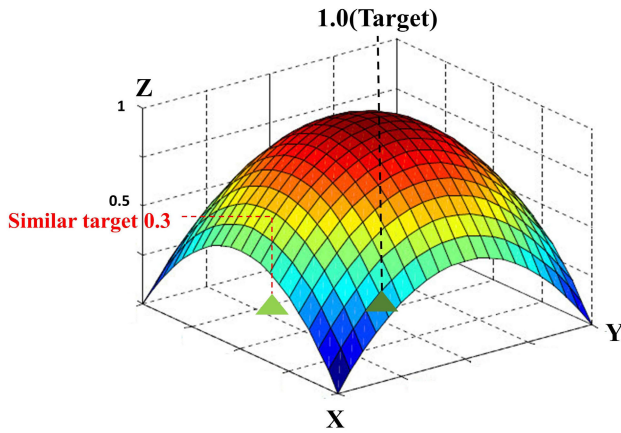


FIGURE 5. Example graph of calculating target location using complicated method.

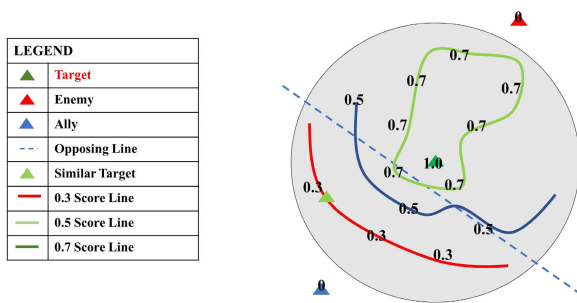


FIGURE 6. Target location calculated by simple method.

which would enable the score to be expressed as a value between 0 and 1, where 0 represents the lowest possible impact and 1 represents the highest. Therefore, in cases where the physical operation impact score is based on multiple factors, it is important to consider the normalization of the score to ensure a consistent and accurate comparison. The calculation method may vary depending on the operational environment and commander’s experience.

b) Simple method: The simple method is a method of simply measuring the contact elements in the form of top, middle, bottom, or 0 and 1. This method is simple, but has the advantage of being able to intuitively check the effect of a cyber-attack. However, it has the disadvantage of being less accurate than the complicated method. For example, when the type of armament is changed, 0 and 1 can be used to distinguish the change in armament type. The target location can be set to a similar target, cyber-attack effect in the case of a location close to friendly forces, under effect if close to the enemy group, or no effect if there is no significant damage to the enemy or friendly group. However, in the case of the target location, as mentioned above, the measurement method may vary depending on the operational environment. Thus, when establishing the measurement method, the score according to the location must be defined in advance. Figure 6 is a pictorial representation of the target position using a simple measurement method, and the section setting for each line

should be set by the commander and experts according to the target position measurement method mentioned in C-a of section IV. In this study, if you are utilizing a Complicated method, ensure that you have knowledge of all the specific details pertaining to what you are measuring. However, from a military perspective, the expected damage rate of a target point as a function of target coordinate variation, the expected damage rate as a function of armament variation, or the mission success rate are not publicly available information and are not suitable for experimentation in this study. Similarly, information such as the sewing error margin of a doll manufacturing factory and the credit score error margin of a bank loan are also not publicly available and not suitable for experimentation in this study. As a result, this study uses a simple method of measurement, which involves inferring using simple analogies such as 0 and 1, or high, medium, and low.

## 2) HOW TO APPLY

The physical operation impact score is a score that measures factors that affect physical operations in cyberspace. Because the physical operation impact score will change due to cyber-attacks, the physical operation impact score becomes an index of cyber mission effectiveness. It is also identified as a data element in the asset hierarchy and affects asset performance. Therefore, it can be applied to other studies or frameworks that quantify the performance of assets other than the framework proposed in this study.

## VI. MISSION IMPACT ANALYSIS FRAMEWORK

The framework of this study was designed by reinforcing the previous study [12], which was based on the four layers of asset-function-task-mission of AMICA [4] proposed by the MITER Corporation.

### A. CYBER ASSET IDENTIFICATION

The North American Electricity Reliability Corporation (NERC), a power company in North America, defines cyber assets as hardware, software, and data, including programmable electronic devices and communication networks [18]. In the previous study [12], equipment that performed cyber activities such as PCs and servers existing on the network were defined as assets. However, when measuring the damage to cyber assets, it is difficult to apply cyber resilience, which has recently been considered important, because there is no detailed information on how the damaged equipment was damaged. In addition, in order to utilize the physical operation impact score mentioned above, this study defined cyber assets as all network assets along the path through which data moves to carry out cyber mission activities. However, each network asset was identified as shown in Tables 4, including the available data and available application information.

As mentioned above, a data asset that measures the physical operation impact score was composed of elements input to the operation order and JWS. Data can also be viewed as an



**TABLE 4. Identify data assets and CVEs in network asset.**

Network Asset	Operation Staff's PC in Regimental	
Application	Data CVE	CVSS
Window Defender	CVE-2020-0835	7.2
Office 2010	CVE-2016-4290	7.8
Outlook 2010	CVE-2017-0204	5.5
Windows 10 release 19044.1889	CVE-2022-30205	6
Available Data		
	Ally attack target	
	Enemy attack path	
	Target location	
	Allied position	
	allied forces	

asset because it can be modified and moved in cyberspace. Data may be used differently for each operation, and the data used by assets for each operation may also be different. Therefore, each asset can be an indicator for determining the importance of data assets used during mission execution, which means that a decrease in the physical operation impact score influences the importance of the asset.

**B. FRAMEWORK STRUCTURE**

As shown in Figure 7, the framework of this study had four hierarchical structures: assets, functions, tasks, and missions. The asset layer included physical network assets and data assets required for mission execution. In addition, the physical operation impact score measured in the asset class was applied to the JWS to measure the impact of the physical operation. The functional layer included functions for performing operational procedures. A task can be seen as one small mission, but in this study, the entire cyber mission to perform physical operations was considered as one mission. Thus, the task hierarchy contained the operational procedures of the mission. Finally, the damage caused by cyber-attacks was compared and analyzed with the numerical values at the mission layer in cyberspace and the JWS result values. These comparisons demonstrate that even if the physical damage statistics appear to match the intended outcome, they can actually result from a completely different situation as indicated by the damage in cyberspace.

**C. MEASURE OF FRAMEWORK**

All the calculations were made based on two factors: impact and performance. In the previous study [12], the vulnerability coefficient was calculated based on the confidentiality, integrity, and availability (CIA) in the performance of the asset, and the expert evaluation score was used. However, in this study, the CVSS present in cyber assets other than the CIA was calculated as a vulnerability coefficient based on the  $Vul_{sp}$  value proposed by Kim et al. [19], which is shown in Equation 7, with the parameters listed in Table 5.

$$A = (Fd)/V \tag{7}$$

All the vulnerabilities and CVSSs must be identified during asset identification to compute the transformed asset

**TABLE 5. Defining transformed asset performance formulas.**

parameter	definition
$A$	Asset performance value
$V$	Assets CVSS total score
$F$	Number of assets used in the function
$d$	Physical operations impact score

performance. In addition, network assets identify data assets that can be used or accessed to measure the damage caused by cyber-attacks.

**VII. EXPERIMENT**

The experiment conducted in this study consisted of five steps: mission setting, operation scenario design, infrastructure setting, attack scenario design, analysis, and results. The operation was based on the CAS scenario designed in Section IV. In Section IV, only the design of the overall flow of the operation was carried out. Therefore, the design had to be carried out in detail. However, because military information is confidential, everything described in the experiment was based on known information and may differ from reality. The experiment proceeded with two types of cyber-attacks: modification and destruction. In the case of stealing information, it does not directly affect the data and does not proceed because the information of the stolen data is unknown.

**A. MISSION SETTING**

The operation selection and desired effect to be used in the scenario were set, which became the basis for the assets, functions, and tasks to be designed later. In this study, the operation was set as the pre-planned CAS operation; the battlefield location was around Yeoncheon-gun, Gangwon-do, Korea; and the desired effect was the destruction of the bridge in the OP4 area, which was along the enemy's path. In addition, the size, location, ammunition, and armament of the allies were set as shown in Table 6, and based on this, the battlefield situation was mapped as shown in Figure 8 to easily compare before and after the cyber tampering attack. The map expresses information from OP1 to OP6, including the location of friendly forces (A) and location of enemies (E), and cyber attackers could attack friendly systems and tamper with friendly target locations. In addition, when the target perceived by the allies was modulated, the range in which the allies could immediately recognize the target modulation was also expressed.

**B. OPERATIONAL SCENARIO DESIGN**

The scenario design stage is a stage in which the mission, task, function, asset, and data used in the asset are designed in order based on the operation set in the mission setting. The mission was set based on the desired effect set in the previous step, and the task was set as an operational procedure to be performed for the mission. The function was set as an action to perform a task, such as creating or delivering a document.

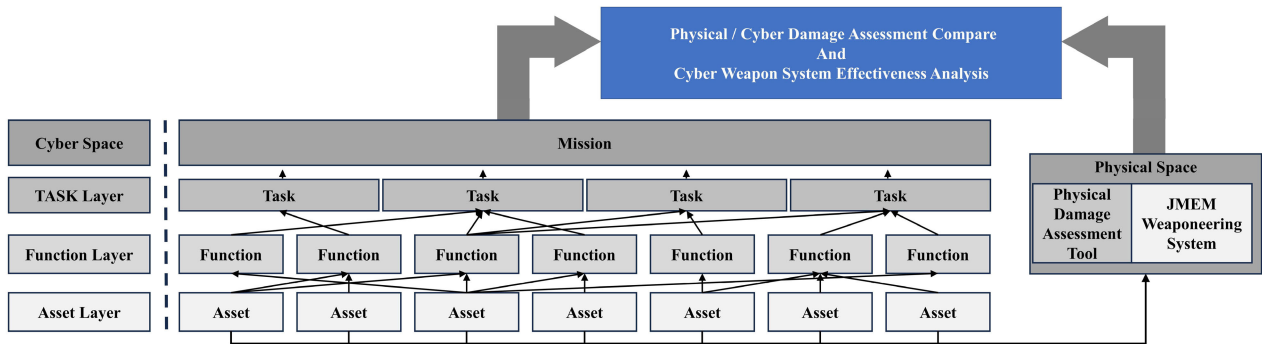


FIGURE 7. Framework structure.

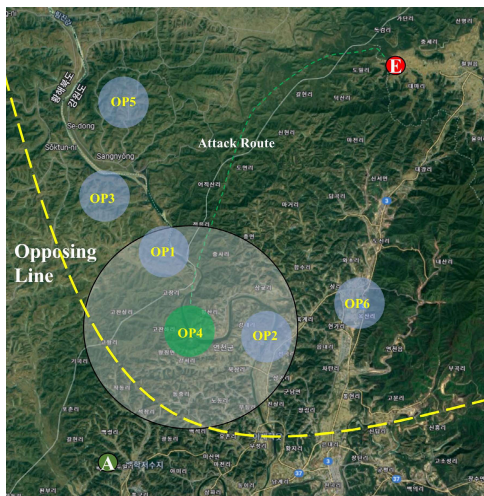


FIGURE 8. Battlefield map to check for modification in OP areas.

TABLE 6. Task performance formula description.

Operation Info	Descriptions
Operation	Scheduled CAS
Request effort	Destroy the OP4 area bridge that exists in the enemy's path
Ally's location	5 km south of OP4 area
Ally's armament	Fighter 001 (2 units), Fighter 002 (1 units), Fighter 003 (under maintenance)
Ally's ammo	Missile 001 (8 pieces), Missile 002 (2 pieces), Missile 003 (6 pieces)
Allies in the confrontation area	2 Regiments, 2 Tanks
Target Type	1st priority bridge, 2nd priority enemy tank destruction, 3rd priority enemy troop killing
Enemy power	1 regiment with 4 tanks
Enemy location	30 km north of OP4 area

Finally, network devices such as PCs and routers used and owned by performers for these actions and all the data used to perform functions were identified as assets.

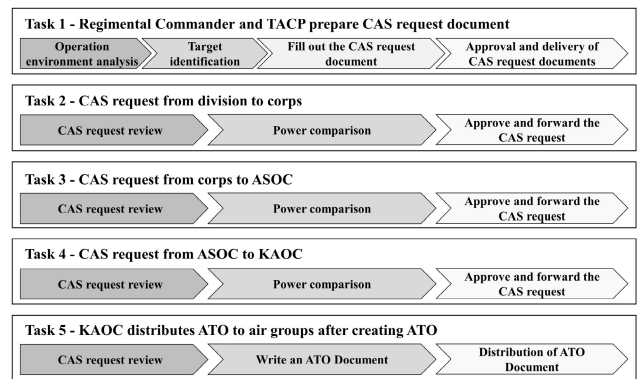
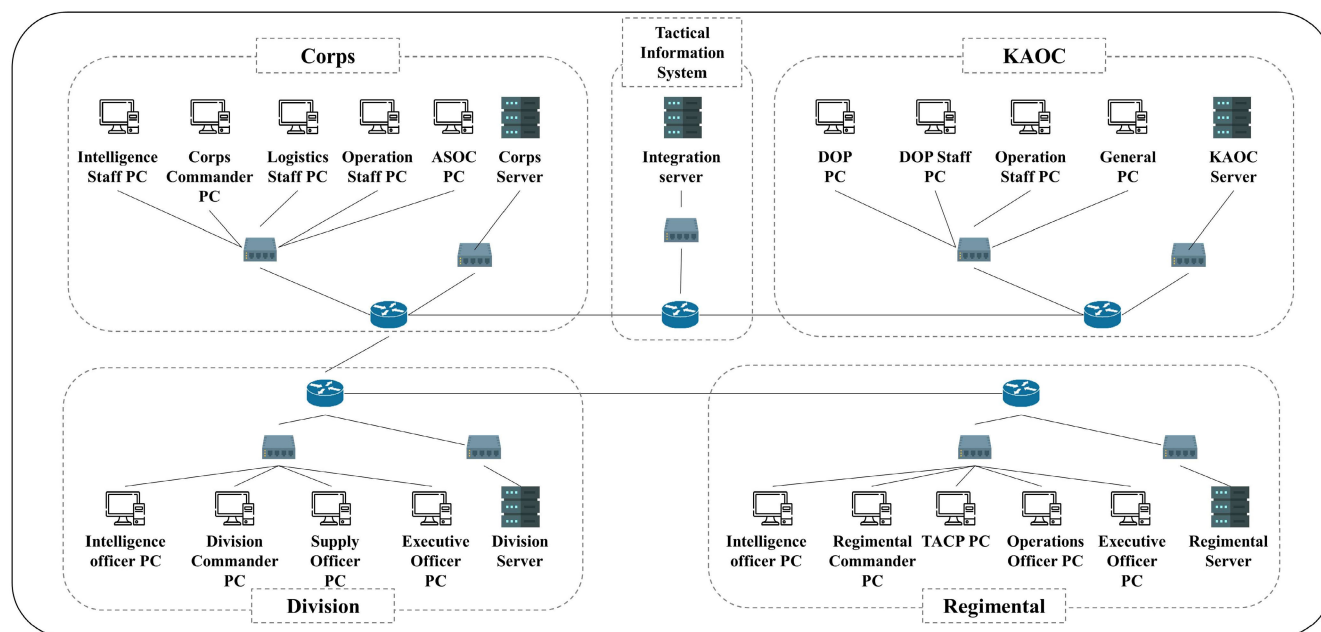


FIGURE 9. Designed task and function layer.

Based on what was set in 6-A, the mission was set as the mission of the planned CAS operation and the destruction of the bridge in the OP4 area. Each unit, regiment, division, corps, Air Support Operations Center (ASOC), and Korean Air Operations Center (KAOC) was in charge of one task. Task 1 was a sub-mission carried out by the regiment, where the information manager, operation officer, and operations manager analyzed the operational environment by checking the size of the friendly force and enemy attack routes. Based on the analyzed operational environment, the head of the information and operation department identified target information and delivered it to TACP, which requested enemy and friendly information from the server, collected it, and prepared a CAS request. The TACP delivered the prepared CAS request to the regiment commander, who approved the CAS request, stored the request in the server, and submitted a re-request to the upper unit. Task 2 was completed through the process of reviewing the request received by the division, comparing forces, approving the request, and forwarding it to the upper unit. Tasks 3 and 4 followed the same process as task 2. Finally, the KAOC in task 5 reviewed the CAS request, prepared the ATO, and distributed it to the wing and sub-units. The designed tasks and functions are shown in Figure 9, and in the case of Task 1, network assets and data assets were divided and identified as shown in Table 7, with the time

**TABLE 7. Identify available data assets by network asset.**

Data Asset	Intelligence Officer PC	Regimental Commander PC	TACP PC	Regimental Server	Operation officer PC	Executive officer PC
Ally size	available	available	available	available	available	
Ally location	available		available			
Enemy attack route	available	available		available		available
Ally’s armament		available	available		available	
Ally’s ammo		available	available		available	
Target information	available		available	available		available
Key target			available		available	
Sub attack target				available		



**FIGURE 10. Network infrastructure design.**

**TABLE 8. Identify available data assets by network asset.**

Function	Runtime(min)	Network Assets
Operation environment analysis	10	Intelligence officer PC, Operation officer PC, Executive officer PC
Target identification	8	Intelligence officer PC, Executive officer PC
Fill out the CAS request document	10	TACP PC
Approve and forward the CAS request	15	Regimental Commander PC, Regimental Server

required for each function and used network assets identified as shown in Table 8.

**C. INFRASTRUCTURE CONFIGURATION**

This is the stage of designing the network infrastructure configuration and asset applications and vulnerabilities suitable for the designed scenario. A well-designed network is

**TABLE 9. Damaged data assets (modification).**

Data	Normal	Range	Modified Data	Physical Score
Equipped ammunition	Missile001 8 pieces	Even number	Missile001 4 pieces	0.5
Target position	OP4	OP1, OP2	Tunnel next to the bridge	0.7
Key target	Bridge	Similar target		0.7
Equipped armament	Fighter001	Armament Available	Fighter002	0.3
Ally attack target	Destroy the bridge	Possible to Inflict damage on enemies	Troop killing	0.3

essential for accurately predicting and modeling the effects of cyber-attacks on the network. By providing a solid foundation for developing and testing various cyber-attack scenarios,

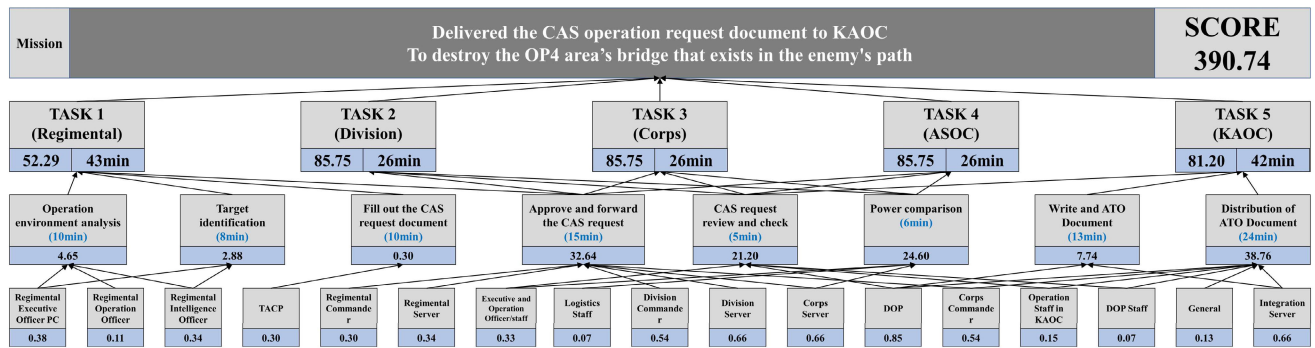


FIGURE 11. Cyber mission score before cyber-attack.

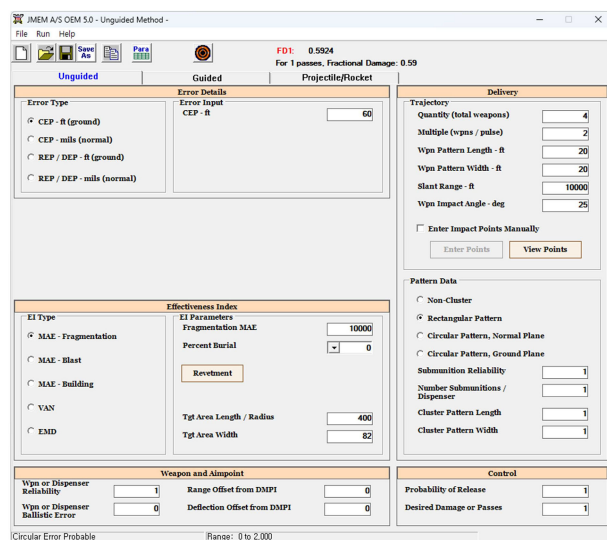


FIGURE 12. JWS FD1 score before cyber-attack.

a carefully planned and structured infrastructure network can help organizations identify potential vulnerabilities and enhance their preparedness against cyber threats. Therefore, designing an infrastructure network is crucial in creating effective cyber-attack scenarios. As shown in Figure 10, the configured infrastructure consisted of four units, regiment, division, ASOC, and KAOC, and included an integrated server where the final ATO was stored.

### D. ATTACK SCENARIO DESIGN

The attack scenario was written for two types of attacks: data modification and destruction. The destruction and modification attack scenarios attacked the same data to analyze their effectiveness in a similar environment and proceeded in the following order.

a) The attacker sent an e-mail with an attachment inserted in the malicious code to the executive officer, operations officer, and intelligence officer with the e-mail subject “Instructions of the Regimental Commander.”

b) The victim downloaded and opened the attachment and at the same time was infected with malicious code.

c) The aggressor’s objective was to reduce the effectiveness of our operations.

d) The attacker established the target of the attack by checking operational data accessible to the victims.

e) Attackers modified and destroyed the target information and armament intelligence data.

### E. EFFECT ANALYSIS AND RESULT

All the items established in the previous step were applied to the framework proposed in this study. After that, the effects of the mission conducted in cyberspace and physical effect using JWS were compared and analyzed. Furthermore, this provided an interpretation method for the results based on the analyzed contents. As shown in Figure 11, the effect value of a normal mission without a cyber-attack was calculated to be 390.74, and as a result of the calculation after inputting it into the JWS, a weapon system effectiveness manual program, the Fractional damage of 1(FD1) was calculated to be 0.59, as shown in Figure 12.

When an attacker falsified data as shown in Table 9 through a cyber-attack, the effect of the cyber mission according to the falsified data is shown in Figure 13. The attacker falsified the unit ammunition information, target location, key target information, unit armed information, and attack target data, and it was confirmed that the physical operation impact score of each data was changed accordingly. Because of the change in the physical operation impact score, the cyber mission effect was reduced by 67.89% to 125.45.

Among the modulated data, the data directly input into the JWS were information on the ammunition possessed by the unit and the location of the target. As the key target and armament information were changed, changes in the target error range, number of fragmentation, and probability occurred. The battlefield situation map changed by the attack is shown in Figure 14, and the JWS result is shown in Figure 15.

The JWS result could be identified as only a small change of 0.05, from the existing 0.59 to 0.54. However, because this was the result of the modulated target position, not the original target position, it cannot be seen as a physical effect for

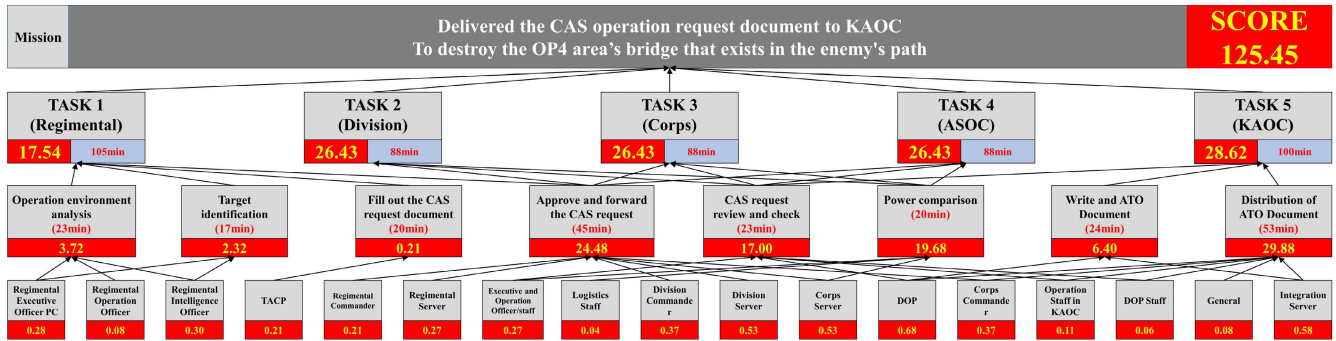


FIGURE 13. Cyber mission score after cyber-attack (modification).

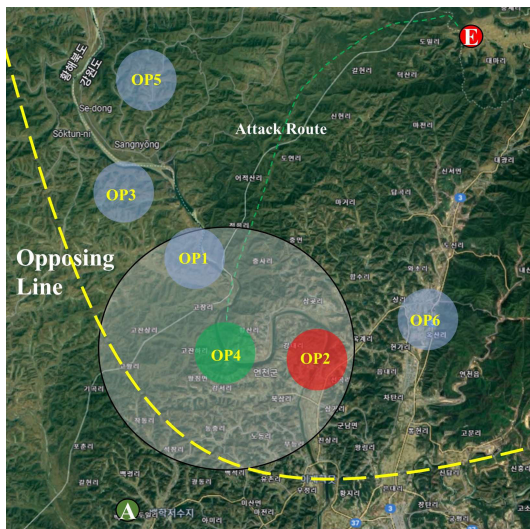


FIGURE 14. Modified target location (from OP4 to OP2).

the target mission. Thus, the commander needed to prepare for the operation again.

Framework changes due to data destruction attacks are shown in Figure 16, and the data changed by destruction are shown in Table 10. The cyber mission effect due to the destructive attack was 133.18, reducing the effect by about 65.91%.

As the ammunition loaded in the armament was changed to missile 002 as a result of the data destruction attack, the effect was changed to an explosion rather than fragmentation, and the physical operation effect was confirmed by inputting this into the JWS. As a result, as shown in Figure 17, it was reduced by about 47% to 0.31. This means that the success rate of the mission was greatly reduced.

In the case of an attack caused by data destruction, the destruction of the target location and armed information data had the greatest impact on the mission. Thus, it can be said that the cyber mission did not proceed normally. In addition, according to the results of the JWS, it was possible to see an effect that was reduced by about 47% compared to the desired effect during the physical operation, and it could be

TABLE 10. Damaged data assets (destroy).

Data	Normal	Input data after attack	Physical Score
Equipped ammunition	Missile 001 8 pieces	Missile 002 2 pieces	0.3
Target position	OP4	OP1	0.5
Equipped armament	Fighter 001	Fighter 002	0.3
Enemy attack route	Bridge in the OP4 area	Unknown	0.5

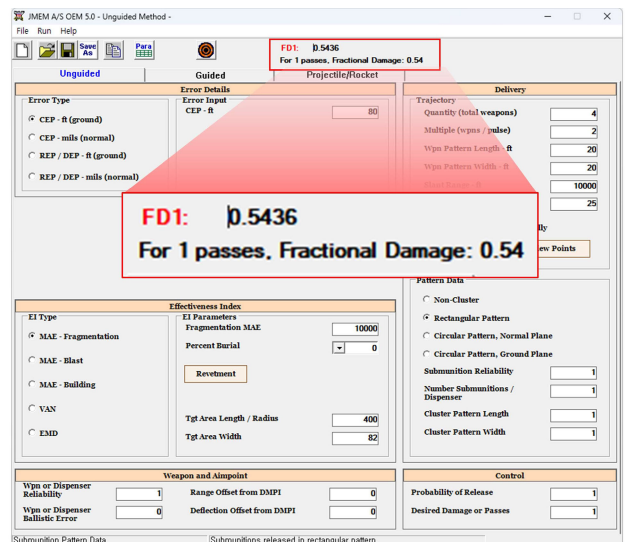


FIGURE 15. JWS FD1 score after cyber-attack (modification).

expected that the battlefield environment would not change significantly due to the small amount of damage from the enemy's point of view. In this study, various and detailed interpretations could be provided based on the decrease in the cyber effect and physical operation effect due to the cyber-attack in the analysis stage as above. This interpretation would help to improve the commander's capacity.

TABLE 11. Comparison of the proposed framework and previous studies.

Proposed method	General approach	Mission context	Cyber Asset Damage	vulnerability scoring	Multiformity
I.J. Kim et al. [20]	Mission centric	Yes	Yes	C(confidentiality), I(integrity), A(availability),	Yes
A. B. Barreto et al. [21]	Mission centric	Yes	Yes	CVSS	No
S. Musman et al. [6]	Cyber resource	Yes	No (Resource)	Degradation, Interruption, Modification, Fabrication, Interception, Unauthorized use	No
P. Radanliev et al. [22]	IoT digital data	No	No (Digital data)	Combined MicroMort (MM) and Value-at-Risk (VaR) unit-of-risk calculation metrics	Yes
Proposed Framework	Mission centric	Yes	Yes	CVSS	Yes

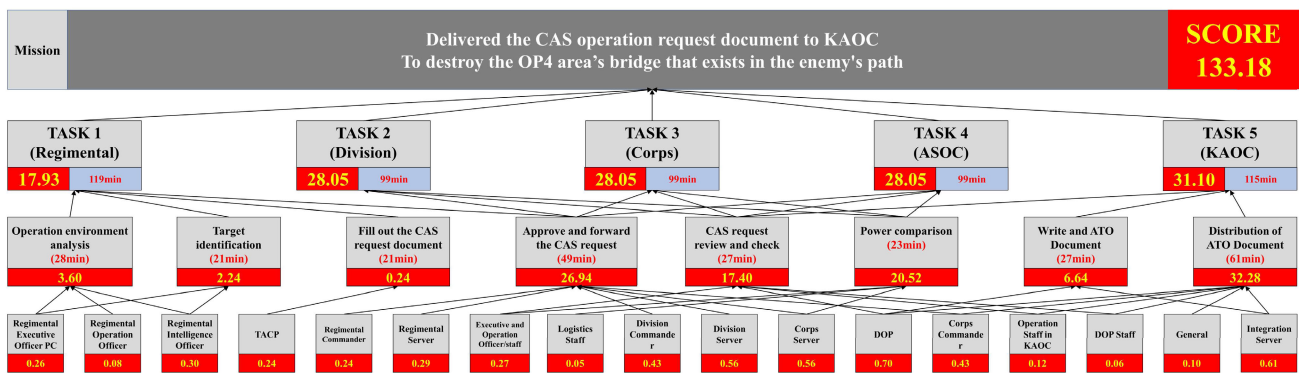


FIGURE 16. Cyber mission score after cyber-attack (destroy).

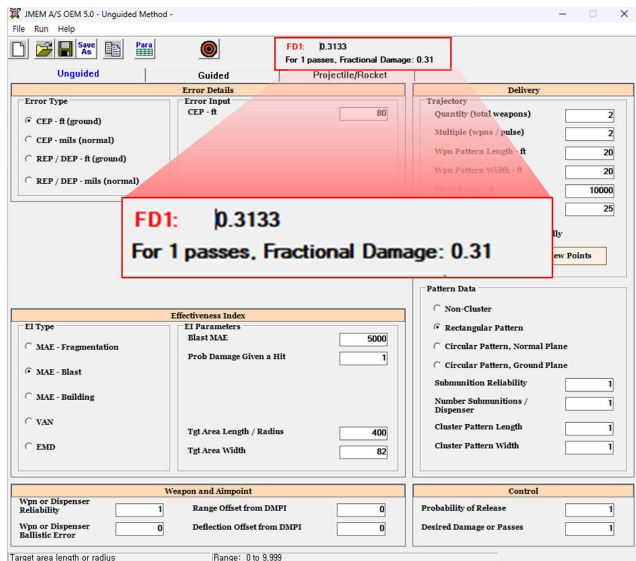


FIGURE 17. JWS FD1 score after cyber-attack (destroy).

VIII. COMPARISON

In this chapter, we compared the cyberspace effect analysis model proposed in this study with the cyber damage assessment cases that have been studied in the past. Table 11

summarizes the comparison between the model proposed in this study and existing cases.

Kim et al. [20] proposed a model for conducting as cyber security test evaluation (T&E) based on missions in connection with weapon systems and the risk management framework (RMF). It was said that the attack was initiated from the asset. Using simulation, the performance of each layer was calculated from the mission perspective, and the vulnerabilities and protection measures identified in the cyber security test and evaluation were quantified to evaluate and derive protective measures considering the performance of the mission. It had the same hierarchical structure as this study, but it had the disadvantage of not specifying how it could be linked with physical space.

The damage assessment study of Barreto et al. [21] proposed a methodology that provides a mapping between the cyber domain and operational domain. It generated an infrastructure capacity index using a unique index, different security perspectives for missions, and different perspectives. The infrastructure capacity index measured certain levels of quantity, quality, efficiency, and required resource and service costs, and used these to build a Bayesian network and create an inference model that predicted mission damage. The inference model was input into the simulation to conduct the mission impact assessment. Cyberspace and mission domains

were linked to understand the impact of actions in cyberspace on mission effectiveness. Cyber threats vary by performer, and threats start with cyber assets. Although cyber assets and physical assets are included in assets, it is difficult to identify direct damage to cyber assets because resources exist at a higher level, and the impact is evaluated using simulation. In addition, because all of the experiments used existing vulnerability modules, event modules, and simulators, their use is limited.

Musman et al. [6] conducted a study focusing on how to calculate the impact of cyber-attacks on IT processes and information. Mission impact was calculated based on modeling mission activity, cyber activities supporting mission activity, and cyber resources. Because the performance degradation was evaluated according to the resources, damage to cyber assets depended on the resources.

Radanliev et al. [22] assessed the economic impact of the Internet of Things (IoT) and related cyber risk vectors and peaks (reinterpreting the IoT vertical). We calculated the value of assets according to the ratio of digital assets in Internet of Things products and created cyber risk indicators through various methodologies. However, because cyber threats were only studied based on the IoT, their use is limited.

## IX. CONCLUSION

This study developed a framework for analyzing the impact of cyber-attacks on physical missions through associated physical operations. Based on the previous cyber battle damage assessment framework, it was linked with JMEM, which is being used as a weapon system effectiveness manual in physical operations. After that, a framework was proposed to identify the impact of the mission by comparing and analyzing the results of battles and defenses in cyberspace with the effects of physical operations. To prove this, we analyzed and designed operational scenarios using domestic and foreign military manuals and preliminary studies, defined assets, and conducted experiments. In the experiment, two types of cyber-attacks were conducted: modification and destruction. In the case of stealing, it did not directly affect the data, and the information of the stolen data was unknown. Thus, we did not proceed. The experiment showed that the greater the decrease in the cyber mission effect value, the greater the impact on the physical operation. When it was difficult to judge the cyber effect alone, the physical weapon system effect could also be compared and analyzed to help determine whether to proceed with the physical operation.

In this study, an experiment was carried out by taking only one example of a CAS operation. However, it could be used in various operations with experts designing new MOEs and MOPs according to the MOE and MOP design methods covered in this study to create scenarios. In addition, as suggested in this study, if the interface elements of cyberspace and physical space could be identified, and the physical operation impact score for each interface element could be measured, the proposed framework could be applied

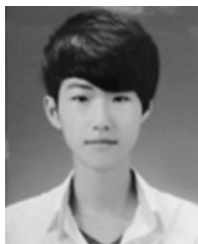
in civilian society. In other words, it could be applied to tasks that affect physical space according to procedures performed in cyberspace, such as automated factories, passport issuance, and credit loans. For example, coefficients such as the probability of defects and probability of producing normal products in a canning plant could substitute for FD, which is the result of JWS. In addition, the quantity information data of material A and status data of the manufacturing process steps could be identified as interface elements between cyberspace and physical space. Missions in cyberspace could be set, such as manufacturing 10,000 cans of food. By setting the tasks, functions, and assets to be performed for manufacturing 10,000 units, the impact of achieving the manufacturing goal could be measured in the event of a cyber-attack with the framework proposed in this study. This suggests that the proposed framework, compared to the combat damage assessment framework of the previous study [12], could be used to grasp the direct impact on the physical space and has evolved into a form that can be used in various operations and situations.

We plan to analyze elements of operation documents used in various operations in the future, classify common data and operation-specific data, and develop a framework or tool to perform integrated mission impact analysis. In addition, as mentioned in 6-E, as well as estimating the damage from cyber missions and damage from physical operations, the results of the analysis will be studied so that they can be used as commander judgment indicators through machine learning.

## REFERENCES

- [1] M. Hancock, "The influence of cybersecurity on modern society," EasyChair, Tech. Rep. 5882, Jun. 2021. [Online]. Available: <https://easychair.org/publications/preprint/PvXC>
- [2] M. R. Driels, *Weaponneering: Conventional Weapon System Effectiveness*. Reston, VA, USA: American Institute of Aeronautics and Astronautics, 2013.
- [3] G. Jakobson, "Mission cyber security situation assessment using impact dependency graphs," in *Proc. 14th Int. Conf. Inf. Fusion*, Chicago, IL, USA, 2011, pp. 1–8.
- [4] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. K. Thomas, J. McFarland, B. King, S. Webster, and B. Tello, "Analyzing mission impacts of cyber actions (AMICA)," in *Proc. NATO IST-128 Workshop Cyber Attack Detection, Forensics Attribution Assessment Mission Impact*, 2015.
- [5] 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, doi: [10.1109/THS.2015.7225283](https://doi.org/10.1109/THS.2015.7225283).
- [6] 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.*, Montreal, QC, Canada, Apr. 2011, pp. 46–51, doi: [10.1109/SYSCON.2011.5929055](https://doi.org/10.1109/SYSCON.2011.5929055).
- [7] K. S. Miller, "Army doctrine publication (ADP) 3–0 operations," Washington, DC, USA, Tech. Rep., Jul. 2019.
- [8] K. D. Scott, "Joint publication (JP) 3–0, joint operation," Washington, DC, USA, Tech. Rep., Oct. 2018.
- [9] E. J. Robert. (Mar. 2022). *Committee on National Security Systems (CNSS) Glossary*. [Online]. Available: <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>
- [10] K. D. Scott, "Joint publication (JP) 3–12, cyberspace operation," Washington, DC, USA, Tech. Rep., Jun. 2018. [Online]. Available: [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf)
- [11] M. G. Mullen, "Joint publication (JP) 5–0 joint operation planing," Washington, DC, USA, Tech. Rep., Aug. 2011. [Online]. Available: [https://grugq.github.io/resources/jp5\\_0.pdf](https://grugq.github.io/resources/jp5_0.pdf)

- [12] S. Kim, J. Jang, O.-J. Kwon, J.-Y. Kim, and D. Shin, "Study on cyber attack damage assessment framework," *IEEE Access*, vol. 10, pp. 59270–59276, 2022, doi: [10.1109/ACCESS.2022.3179977](https://doi.org/10.1109/ACCESS.2022.3179977).
- [13] D. E. Mann and S. M. Christey, "Towards a common enumeration of vulnerabilities," in *Proc. 2nd Workshop Res. Secur. Vulnerability Databases*, 1999, pp. 1–13.
- [14] M. Peter, K. Scarfone, and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," in *Proc. 1st Forum Incident Response Secur. Teams*, vol. 1, Jun. 2007, p. 23.
- [15] M. F. Averill, "Army techniques publication (ATP) 3–09.12 field artillery counterfire and weapons locating radar operation," Washington, DC, USA, Tech. Rep., Oct. 2021. [Online]. Available: [https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/ARN33999-ATP\\_3-09.12-000-WEB-1.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33999-ATP_3-09.12-000-WEB-1.pdf)
- [16] K. S. Miller, "Field manuals (FM) 3–09 fire support and field artillery operations," Washington, DC, USA, Tech. Rep., Apr. 2020. [Online]. Available: [https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/pdf/web/ARN21932\\_FM\\_3-09\\_FINAL\\_WEB.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN21932_FM_3-09_FINAL_WEB.pdf)
- [17] D. L. Goldfein, "Joint publication (JP) 3–09.3 close air support," Washington, DC, USA, Tech. Rep., Jul. 2009. [Online]. Available: [https://irp.fas.org/doddir/dod/jp3\\_09\\_3.pdf](https://irp.fas.org/doddir/dod/jp3_09_3.pdf)
- [18] NERC, Atlanta, GA, USA. (Jan. 2021). *Appendix 2 to the NERC Rules of Procedure*. [Online]. Available: [https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix\\_2\\_ROP\\_Definitions\\_20210119.pdf](https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_2_ROP_Definitions_20210119.pdf)
- [19] K. Kim, S. Yoon, D. Lee, J. Jang, H. Oh, and D. Shin, "Study on prioritization of actions by classifying and quantifying cyber operational elements using 5W1H method," *IEEE Access*, vol. 10, pp. 74765–74778, 2022, doi: [10.1109/ACCESS.2022.3190530](https://doi.org/10.1109/ACCESS.2022.3190530).
- [20] I. Kim, S. Kim, H. Kim, and D. Shin, "Mission-based cybersecurity test and evaluation of weapon systems in association with risk management framework," *Symmetry*, vol. 14, no. 11, p. 2361, Nov. 2022.
- [21] A. B. Barreto and P. C. G. Costa, "Cyber-ARGUS—A mission assurance framework," *J. Netw. Comput. Appl.*, vol. 133, pp. 86–108, May 2019.
- [22] P. Radanliev, D. C. De Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap, "Future developments in cyber risk assessment for the Internet of Things," *Comput. Ind.*, vol. 102, pp. 14–22, Nov. 2018.
- [23] W. Stanley and F. Katherine. (1994). *Social Network Analysis*. [Online]. Available: <https://www.cambridge.org/core/books/social-network-analysis/90030086891EB3491D096034684E9FB8>



**JISOO JANG** received the B.S. degree in computer science from the Seoul Hoseo Occupational Training College, Seoul, South Korea, in 2021. He is currently pursuing the M.S. degree with Sejong University, Seoul. From 2017 to 2019, he was an alternative to military service with a real estate bank in South Korea, where he was responsible for website development and maintenance. His research interests include machine learning, cyberspace, cyber warfare, and military science.



**KOOKJIN KIM** received the B.S. degree in computer science from the Seoul Hoseo Occupational Training College, Seoul, South Korea, in 2017. He is currently pursuing the Ph.D. degree with Sejong University, Seoul. From 2017 to 2019, he developed mobile applications and back-end software with M2Soft, South Korea. His research interests include machine learning, neural networks, cyberspace, cyber warfare, and cyber targeting.



**SUKJOON YOON** received the B.S. degree in aeronautical engineering from the Korea Air Force Academy, in 1984, the M.S. degree in weapon systems engineering from Korea National Defense University (KNDU), Yangchon-myeon, Nonsansi, Chungcheongnam-do, Republic of Korea, in 1992, and the M.S. degree from the Department of Military Science, Führungsakademie der Bundeswehr, Hamburg, Germany, in 1998. Since 2021, he has been a Joint Test Team Analyst with the Republic of Korea Joint Chiefs of Staff, Republic of Korea. Since 2021, he has been with the Department of Computer Engineering, Sejong University, South Korea, where he is currently a Professor. His research interests include cyberspace, force, weapons, and cyber warfare.



**SEONGKEE LEE** received the B.S. degree in mathematics from Dongguk University, South Korea, in 1984, the M.S. degree in computer science from Yonsei University, in 1989, and the Ph.D. degree in computer science from Korea University, in 2003. From 1984 to 1998, he was a Research Fellow with the Korea Institute of Defense Analyses. He was a Visiting Scholar with Syracuse University, USA, in 1994. Since 1999, he has been a Senior Principal Researcher with the Agency for Defense Development. His research interests include software engineering, modeling and simulation, project management, and cyber security. He was certified as a professional engineer in the information processing area, in 1991.



**MYUNGKIL AHN** received the B.S. degree in information and communication engineering from Chungnam National University, Republic of Korea, in 1997, the M.S. degree in computer science from Sogang University, Republic of Korea, in 2003, and the Ph.D. degree in electrical engineering from Chung-Ang University, Republic of Korea, in 2021. Since 2006, she has been with the Agency for Defense Development, South Korea, where she is currently a Principal Researcher. Her research interests include cyber warfare, cyber M&S, cyber training, and cyber impact analysis.



**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 machine learning, ubiquitous computing, bio-signal data processing, and information security.

...