J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

사이버 공간과 물리 공간이 연계된 사이버 무기체계의 효과성 분석 프레임워크 연구☆

A Study on the Framework for Analyzing the Effectiveness of Cyber Weapon Systems Associated with Cyberspace and Physical Space

장 지 수[1,2] 김 국 진[1,2] 윤 석 준[3] 박 민 서[4] 안 명 길[4] 신 동 규[1,2,3*]
Ji-su Jang Kook-jin Kim Suk-joon Yoon Min-seo Park Myung-Kil Ahn Dong-kyoo Shin*

요 약

과거 물리적 공간에서만 수행되던 작전이 사이버 공간을 포함하는 작전으로 바뀌면서 사이버 공격이 사이버 시스템을 활용한 무기체계에 어떤 영향을 미치는지 분석할 필요가 있다. 이를 위해 사이버와 연계한 물리적 무기체계의 영향을 분석하는 도구를 분석하는 것은 의미가 있을 것이다. 한국군은 물리 무기체계의 영향을 분석한 결과가 담긴 미군 JMEM을 확보해 운용하고 있다. JMEM은 재래식 무기체계에만 적용되어 사이버 무기체계의 영향을 분석하는 것은 불가능하다. 이를 위해 물리전의 MOE와 MOP를 기반으로 사이버 무기체계 효율성 분석을 위한 사이버지수를 산출하였다. 또한, 물리 작전에서 무기체계 효과 매뉴얼로 활용되고 있는 JMEM과 연계하여 사이버 공간에서의 전투 결과와 물리 작전의 효과를 비교 분석하여 임무 영향을 판단할 수 있는 프레임워크를 설계 및 시험하였다. 제안된 프레임워크를 입증하기 위해 국내외 군사 매뉴얼과 선행연구를 통해 작전 시나리오를 분석 및 설계하고 자산을 정의하고 실험을 수행하였다. 실험 결과 사이버 임무 효과 값의 감소가 클수록 물리적 작전에 미치는 영향이 커졌다. 다양한 작전에서 사이버 공격으로 인한 물리적 작전의 영향을 예측하는 데 사용할 수 있으며, 전장의 지휘관이 빠른 결정을 내리는 데 도움이 될 것이다.

☞ 주제어 : 사이버전, 사이버 공간, 사이버 작전, 사이버 무기체계, 임무 영향 분석

ABSTRACT

As operations that were only conducted in physical space in the past change to operations that include cyberspace, it is necessary to analyze how cyber attacks affect weapon systems using cyber systems. For this purpose, it would be meaningful to analyze a tool that analyzes the effects of physical weapon systems in connection with cyber. The ROK military has secured and is operating the US JMEM, which contains the results of analyzing the effects of physical weapon systems. JMEM is applied only to conventional weapon systems, so it is impossible to analyze the impact of cyber weapon systems. In this study, based on the previously conducted cyber attack damage assessment framework, a framework for analyzing the impact of cyber attacks on physical missions was presented. To this end, based on the MOE and MOP of physical warfare, a cyber index for the analysis of cyber weapon system effectiveness was calculated. In addition, in conjunction with JMEM, which is used as a weapon system effect manual in physical operations, a framework was designed and tested to determine the mission impact by comparing and analyzing the results of the battle in cyberspace with the effects of physical operations. In order to prove the proposed framework, we analyzed and designed operational scenarios through domestic and foreign military manuals and previous studies, defined assets, and conducted experiments. As a result of the experiment, the larger the decrease in the cyber mission effect value, the greater the effect on physical operations. It can be used to predict the impact of physical operations caused by cyber attacks in various operations, and it will help the battlefield commander to make quick decisions.

☞ keyword : Cyber warfare, Cyber space, Cyber operation, Cyber weapon system, Mission Impact Analysis

1 Department of Computer Engineering, Sejong University, Seoul, 05006, Korea.
2 Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul, 05006, Korea.
3 Department of Cyber Warfare Research Center, Sejong University, Seoul, 05006, Korea.
4 Cyber Technology Center, Agency for Defense Development, Seoul, 05771, Rep. of Korea.
* Corresponding author (shindk@sejong.ac.kr)
[Received 30 August 2022, Reviewed 17 September 2022(R2 11 October 2022), Accepted 14 October 2022]
☆ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UI210010XD).

1. 서 론

시간이 지남에 따라 인터넷은 점점 발전해가고 있다. 인터넷의 발전은 사이버 공간의 확장으로 이뤄지며 이는 [1]에서 논의된 바와 같이 삶의 질이 향상되었고, 전쟁 양상까지 변화되고 있다. 따라서 군사적 관점으로 과거 대화력전, 공습 작전 등의 작전은 물리 공간에서만 진행되어 졌으나, 점차 물리 공간과 사이버 공간을 포함한 작전의 형태로 변화했다.

기존 물리 작전에서는 물리 무기체계 효과분석 결과가 포함되어 있는 합동 탄약 효과 교범인 JMEM(Joint Munitions Effectiveness Manual)을 개발하여 운영하고 있다. JMEM은 공대공, 공대지, 지대공, 지대지, 특수무기와 같은 분야의 탄약들에 대해 각 탄약이 가지는 효과도를 체계적으로 연구한 자료로 다양한 전장환경 및 상황에 따라 효과를 측정하여 실제상황과 유사한 효과를 도출하고 있다. 하지만 JMEM은 사이버 무기체계의 효과를 분석하는 것은 불가능하다 [2].

사이버 공간에서 진행하는 작전은 사이버 공격으로 인해 정상적인 작전이 이루어지지 못할 가능성이 있음에도 불구하고 사이버 공격을 인지하지 못한다면 공격에 의한 효과를 파악하기 어렵다. 이를 위해 사이버 공격으로 인한 피해를 측정하기 위하여 다양한 연구들이 진행되고 있다 [3-5].

본 연구에서는 사이버 무기체계의 효과성 검증을 위하여 물리 작전의 MOE(Measures of Effectiveness), MOP (Measures of Performance) 기반 사이버 MOE, MOP를 설계한다. 설계한 MOE, MOP로 사이버 무기체계 효과성을 정량화하여 물리 작전과 사이버 작전의 효과를 연계하여 측정한다. 이는 추후 진행하는 작전을 위한 지휘관에 판단에 도움이 될 것으로 예상한다.

본 논문은 연구를 진행하기 위해 2장에서 수집된 자료를 기반으로 3장에서는 물리 작전을 선정하고 물리 작전의 시나리오 설계한다. 4장에서는 다양한 작전의 효과 분석을 위해 확장성을 고려한 MOE, MOP 설계방안과 적용방안을 설명한다. 5장은 효과성 분석을 위한 프레임워크를 제시하며 6장에서 제시한 프레임워크를 적용하여 분석한다. 마지막으로 7장은 제시한 프레임워크의 기대효과 및 향후 연구 방향을 다룬다.

2. 관련연구

2.1 작전환경과 위협

작전은 어떤 목표를 달성하기 위해 전략 계획에 따라 실행되는 전투행동으로써 ADP 3-0(Army Doctrine Publication, 2019) [6]의 1장 에서는 군사작전과 작전환경과의 관계 및 위협에 대해 설명한다. 작전환경에는 전쟁의 전략적, 작전적, 전술적 수준에서의 고려 사항이 포함되며 작전 수준은 작전 기술을 사용하여 작전의 설계, 계획 및 수행에 중점을 두고 군대의 전술적 사용을 국가 및 군사 전략 목표와 연결한다. 작전환경은 미 합동교범인 JP 3-0(Joint Publication, 2018) [7]에 따르면 능력 사용에 영향을 미치고 지휘관의 결정에 영향을 미치는 조건, 상황 및 영향의 집합체라고 정의한다. 모든 수준의 지휘관은 특정 작전을 위한 자체 작전환경을 가지고 있으며 각 지휘관의 작전환경은 상위 제대 지휘관의 작전환경의 일부이다. 작전환경은 공기, 육지, 해양 및 우주 영역의 물리적 영역과 정보 환경이 포함된다. 작전 환경은 상호 관련된 변수 간의 많은 관계와 상호작용으로 작전환경이 구성되기 때문에 지속적으로 변화하는 특징을 가지고 있다. 이 때문에 지휘관은 작전환경을 지속적으로 평가하고 가정을 재평가해야 한다.

또한, JP 3-0에서는 공중, 육상, 해상, 우주 및 사이버 공간 영역에서 합동군의 행동 자유를 방해하려고 시도하는 것을 위협이라 정의했으며 위협을 이해하는 것은 작전에서 중요하다고 말한다.

현대 정보 기술은 사이버 공간과 전자기 스펙트럼을 포함하는 정보 환경을 군사작전에 없어서는 안 될 요소로 만들고 있으며 정보 환경의 모든 행위자는 적이든 우호적이든 중립적이든 물리적, 심리적, 사이버 또는 전자적 수단에 의한 공격에 취약하다.

본 연구에서는 지휘관의 역량, 물리 공간에서의 적/아 대치상황, 사이버 공간에서의 데이터 보유 목록 등 작전에 영향을 미치는 조건, 상황을 작전환경이라 정의하며 사이버 공격을 통한 악성코드 감염, 문서 탈취, 데이터 파괴, 데이터 변조 등의 행위를 위협이라 정의한다.

2.2 사이버 공간의 정의

미국 국립표준기술연구소(NIST)에서는 사이버 공간을 인터넷, 통신 네트워크, 컴퓨터 시스템, 임베디드 프로세서 및 컨트롤러를 포함한 정보 시스템 인프라의 상호 의존적인 네트워크로 구성된 정보 환경 내의 전역 도메인이라고

국가보안시스템위원회(CNSS)에서 작성한 CNSSI 4009에 정의하였다 [8].

합참의장(CJCS)의 지시에 작성된 JP 3-12(2018) [9]에는 사이버 공간 작전(CO)을 다루고 있다. CO(Cyberspace Operation)는 사이버 공간 내 또는 사이버 공간을 통해 목표를 달성하는 것이며 이를 위해서 사이버 공간의 기능을 사용한다. 사이버 공간은 정보환경의 일부이나 공기, 육지, 해양 및 우주의 물리적 영역에 의존하고 있다. CO는 물리적 영역에 위치한 링크 및 노드를 사용하고, 논리적 기능을 수행하여 사이버 공간에서 효과를 생성하며 필요에 따라 물리적 영역에까지 영향이 끼친다. 사이버 공간은 물리적 네트워크, 논리적 네트워크, 사이버 페르소나의 3가지의 상호 연관된 계층 모델로 설명된다. 물리적 네트워크 계층은 데이터 저장소 및 네트워크 구성 요소 간에 데이터를 전송하는 연결을 포함하여 사이버 공간 내에서 정보의 저장, 전송 및 처리를 제공하는 물리적 도메인의 IT 장치 및 인프라로 구성된다. 논리 네트워크 계층은 네트워크 구성 요소를 구동하는 논리 프로그래밍(코드)을 기반으로 물리적 네트워크에서 추상화된 방식으로 서로 관련된 네트워크 요소로 구성된다. 사이버 페르소나 계층은 사이버 공간(사이버 페르소나)에서 행위자 또는 엔터티 ID의 디지털 표현에 대한 설명을 개발하기 위해 논리 네트워크 계층에 적용되는 규칙을 사용하여 논리 네트워크 계층에서 데이터를 추상화하여 생성된 사이버 공간의 관점으로 사람이든 자동화되었든 네트워크 또는 IT 사용자 계정과 서로 간의 관계로 구성된다.

네트워크 장비의 소유자에 따라 접근할 수 있는 데이터와 행위가 다르다. 본 연구는 네트워크 장비 소유자에 따라 작전에서 행위가 다르므로 사이버 공간을 포함하고 있다. 따라서 본 논문에서는 사이버 공간을 정보 환경 일부로써 작전명령문서를 작성 및 배포하기 위해 사용자가 정보 열람, 전송, 문서 작성 등의 행위를 행하는 네트워크 공간으로 정의한다.

2.3 지표 및 척도

황진하 [10]는 Modeling and Simulation을 활용하여 문제제기, 개념모델, 시뮬레이션, 실험결과의 과정을 통한 임무수행에 효율적인 무기체계 획득을 위한 임무 요구에 따라 물리 작전에서의 효과척도(Measure of Effectiveness)를 정의했다. 대한민국 국방에서 정의한 무기체계 분류기준에 따라 단위/통합으로 운용 환경에서 무기체계 성능을 발휘하여 운용목표를 달성하는 정도를 정량적으로 표시하였으며 계획, 준비, 실시, 결과분석 4단계의 과정으로 구성했다. 무기체계의 효과척도는 분석 대상, 의사결정자의 수준과 분석 목적에 따라 다양하게 정의되어 사용될 수 있으며 일반적인 효과척도는 전장에서 무기체계의 성능으로 나타난 임무 달성율으로, 아군 손실, 손실비율, 전진율, 소요/지연시간, 탄약 소모량 등을 예로 하여 탐지율과 식별률로 정의하여 평가하였다.

본 연구는 사이버 공간에서 발생한 공격이 물리 공간에 미치는 영향을 파악하고, 효과성을 분석하기 위함이므로 물리 작전의 요소를 활용하여 지표를 작성한다. 효과 척도는 물리 작전의 경우 무기체계의 효과를 측정하는 도구인 JWS를 사용하여 측정하고, 사이버 공간에서 진행하는 임무의 수행능력으로 척도를 정의한다.

2.4 무기체계 효과 분석

1963년, Close Air Support Board로 알려진 위원회의 육군-공군 패널들은, 현재 보유하고 있는 air-to-surface nonnuclear munitions에 관한 데이터들이 총체적으로 부정확하고 현실과 격차가 너무 크다는 문제를 제기했다. 미 합동참모본부는 데이터를 수집하고, 공대지 폭탄에 대한 JMEM을 제작하도록 지시하였다. JMEM은 전장 환경 정보(타겟 오차범위, 적재할 무장의 개수, 파편화, 폭풍화 등의 무장효과 등)를 바탕으로 살상 확률, 살상 효과 등의 무기체계의 효과 혹은 무장의 추천을 해주는 교범이다. JMEM에서는 어떠한 확률을 계산 할 경우(예: 살상확률) 성공 및 실패를 예/아니오로 표현하는 것이 아닌 전체 시행 횟수 중 성공 가능성을 의미하며 여러 번의 시도 중 결과가 성공으로 나타날 비율. 즉, 살상효과(proportion)와 한 번의 시도 결과가 성공으로 나타날 확률 즉, 살상확률 (probability)로 설명하고 있다. 모델은 몬테카를로 시뮬레이션 등의 절차를 이용해 값을 얻어내는 계산과정과 그 방법론들을 적용해 놓은 결과물로 단순모델, 공학적 모델, 법칙모델로 3가지의 모델로 구분된다 [2].

본 연구에서는 JMEM을 기반으로 제작된 도구인 JWS(JMEM Weaponeering System)의 공개버전을 활용하여 물리 무기체계 효과를 산출하며 네트워크 망에 피해를 입히는 사이버 행위를 사이버 무기체계라고 정의한다.

2.5 사이버 임무기반 피해평가

NOEL은 임무 프로세스, 임무 시스템, 사이버 공격자/방어자 TTPs의 3계층을 모델링 하였으며 사이버 공간에서 입력된 자산이 최종적으로 임무에 영향을 미치는 개념으로 AMICA(Analyzing Mission Impacts of Cyber Actions)프

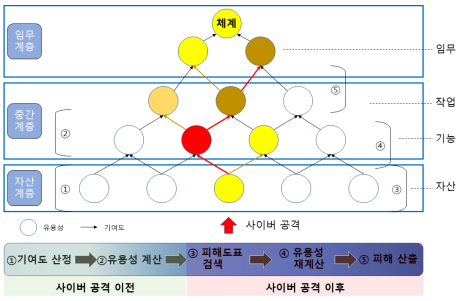
레임워크를 제시하였다 [3].

프로세스 모델링을 위한 기존의 상업용 기성품(COTS) 도구의 한계를 극복하기 위해 미션 목표와 결과가 사이버 자원의 이해도에 따라 미션 상황에서 사이버 리소스를 분석, 모니터링 및 관리가 가능한 CMIA(A cyber mission impact assessment tool)도구를 개발했다. CMIA는 사이버 임무 위험 평가의 척도로 사용하며 미션 컨텍스트 내 시스템에 잠재적 보안 및 복원력 방법의 적용을 시뮬레이션하여 시스템 평가를 수행할 수 있도록 지원한다. CMIA는 Degradation, Interruption, Interception, Modification, Fabrication, Unauthorized Use Attacks의 6가지 공격 인스턴스를 고려하여 임무의 영향을 평가하였다 [4].

유성근 [5]은 국방 임무 수행체계에서 사이버 공격에 대한 피해평가는 객관적인 시스템의 특정 부분이 아닌 전체 시스템에 대한 손상을 임무 수준에서 평가한다고 하였다. 또한, 임무 수행능력은 전장에서 의도한 효과를 달성하기 위한 능력으로 사이버 공격에대한 피해평가의 척도로 활용했으며 사이버 공격으로 인한 국방 임무 수행체계의 임무 수행 능력이 감소하며, 사이버 공격이 일어난 전후의 임무 수행능력의 변화를 식 1과 같이 도출하여 피해평가를 진행했다.

$$damage_{cyberattack} = 1 - \frac{Mcapability_{post_{cyberattack}}}{Mcapability_{pre_{cyberattack}}} \quad (1)$$

국방 임무 수행체계 피해평가 프레임워크는 미션(Mission), 작업(Task), 기능(Function), 자산(Asset)의 4계층 구조로, 기여도 산정, 유용성 계산, 피해도표 검색, 유용성 재계산, 피해 산출의 순서로 피해평가를 진행되는 것으로 그림 1과 같다.



(그림 1) 국방 임무체계 피해평가 프레임워크

(Fig 1) Defense Mission System Damage Assessment Framework

이전의 본 연구팀의 연구 [11]는 군사작전에서 사이버 공격으로 인한 임무의 피해를 평가하는 사이버 전투피해평가 프레임워크를 제시했다. 사이버 전투피해평가 프레임워크는 미 MITRE 사의 임무 종속 구조를 기반으로 자산, 기능, 과업, 임무 순의 계층 구조로 구성했다. 사이버 공격은 자산에서 발생한다고 가정하였으며 사이버 자산에서 발생한 피해가 상위계층에도 영향이 미친다는 것으로 자산부터 임무까지의 피해를 측정했다. 임무에 발생한 피해를 정량적으로 산출하여 지휘관에게 전달함으로써 지휘관이 전시상황에 신속한 판단을 할 수 있도록 도움을 주었다. 사이버 전투피해평가 프레임워크는 수행도와 영향도 2가지 척도로 수행하며 수행도는 구성요소가 임무를 수행하는데 있어 사용되는 정도, 영향도는 해당 계층이 임무에 영향을 미치는 정도로 정의하여 계층의 순서대로 측정했다.

1) 자산 수행도 및 영향도 측정: 자산의 수행도(A)는 임무 수행에 있어 자산의 가치 정도를 나타내는 것으로 식 2와 같이 계산되며 매개변수는 표 1과 같다.

$$A = \frac{F \bullet \alpha}{V} \quad (2)$$

(표 1) 자산 수행도 매개변수 정의

(Table 1) Asset Perform parameter definitions

매개변수	설명
A	자산 수행도(Asset Performance)
V	자산 취약점 계수
F	자산이 기능에 사용되는 수
α	전문가 평가점수

자산의 영향도는 여러 기능에 사용되는 자산일수록 임무에 더 큰 영향을 끼치는 자산으로 판단하여 기능계층에 연결된 가지 수로 영향도를 산출했다.

2) 기능 수행도 및 영향도 측정: 기능 수행도는 기능이 미션에 사용되는 정도를 나타내며 식 3과 같이 계산되고, 매개변수는 표 2와 같다.

$$\text{기능수행도} = \left(\sum_{n=1}^{\text{기능가중치}} \text{자산}_n\text{수행도} \times \text{자산}_n\text{영향도}\right) \times \text{기능가중치} \quad (3)$$

(표 2) 기능 수행도 매개변수 정의
(Table 2) Function Perform parameter definitions

매개변수	설명
기능가중치	기능에 연결된 가지 수
자산$_n$수행도	기능에 연결된 자산 수행도
자산$_n$영향도	자산$_n$영향도

기능이 미션에 있어서 영향을 미치는 경우는 기능이 정해진 시간 내에 수행하지 못했을 경우인 기능 수행 시간 영향도와 수행결과가 정확하지 않은 경우의 정확도 영향도의 곱으로 기능 영향도를 산출한다. 기능 수행 시간 영향도는 과업 수행 시간 대비 기능 수행 시간으로 산출하며 과업 수행에 지연이 발생할 경우 초기 기능 수행 시간 영향도에 지연된 과업 시간 대비 지연된 기능 시간의 곱 연산을 통해 산출하며 식 4와 같다.

$$\text{기능수행시간영향도} = \frac{\text{초기시간}_{\text{기능}}}{\text{초기시간}_{\text{과업}}} \times \frac{\text{지연시간}_{\text{기능}}}{\text{지연시간}_{\text{과업}}} \quad (4)$$

정확도 영향도는 초기에는 피해를 받은 자산이 없으므로 1로 초기화되며, 사이버 공격에의해 피해를 받았을 경우 초기 정확도 영향도에서 기능 수행되는 자산 수 대비 피해를 받은 자산 수를 차감하여 산출했으며 식 5와 같다.

$$\text{기능정확도영향도} = 1 - \frac{\text{피해입은자산수}}{\text{기능가중치}} \quad (5)$$

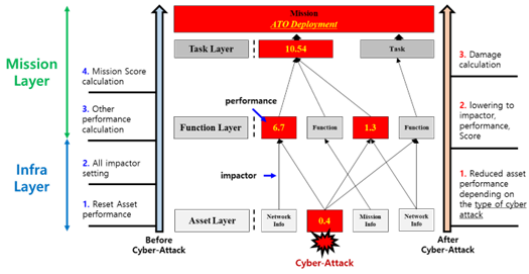
3) 과업 수행도 측정: 과업에서의 척도는 수행도만 다루고 있으며 임무에 대한 영향도는 따로 측정하지 않는다. 과업 수행도는 기능 수행도와 영향도의 곱의 합으로 산출되며 식 6과 같고, 매개변수는 표 3과 같다.

$$\text{과업수행도} = \left(\sum_{n=1}^{\text{과업가중치}} \text{기능}_n\text{영향도} \times \text{기능}_n\text{수행도}\right) \times \text{과업가중치} \quad (6)$$

(표 3) 과업 수행도 매개변수
(Table 3) Task Perform parameter definitions

매개변수	설명
과업가중치	과업에 연결된 가지 수
기능$_n$수행도	과업에 연결된 기능 수행도
기능$_n$영향도	기능$_n$영향도

위와 같은 척도를 활용하여 그림 2와 같이 프레임워크가 동작한다.



(그림 2) 사이버 전투피해평가 프레임워크 동작 방식
(Fig 2) Cyber Battle Damage Assessment Framework Process

위와 같이 모든 연구가 계층적 구조로 자산의 피해가 임무에 영향을 미친다는 개념으로 진행했다. 본 연구에서도 이와 마찬가지로 자산-기능-과업-임무의 4계층 구조로 진행하며 이전의 본 연구팀의 연구 [11]에서 제시한 프레임워크를 기반으로 연구를 진행한다.

2.6 사이버 공격

사이버 공격은 사이버 공간에서 성능 저하, 중단 및 파괴 등의 효과를 발생시키거나 물리적 영역으로 이어지는 효과를 발생시킨다. JP 3-12에서는 사이버 공격을 거부, 조작의 두 가지 공격 형태로 나누었다. 거부 공격은 대상에 대한 액세스 또는 작업을 거부함으로써 성능 저하를 일으키거나 일시적으로 거부함으로써 지연 즉, 방해하거나, 대상에 대한 액세스를 복구 불가능하게 하여 파괴 하는 형태라고 정의한다. 조작은 속임수, 기만, 컨디셔닝, 스푸핑, 위조 및 기타 유사한 기술을 사용하여 사이버 공간에서 정보, 정보 시스템, 네트워크 등을 제어하거나 변경하는데, 표적 네트워크는 1차 공격의 효과가 드러날 때까지 물리적 효과를 포함한 2차 또는 3차 효과가 정상적으로 작동하는 것처럼 보일 수 있다 [9].

Mitre 社에 의해 운영되고 연방정부의 자금을 지원받아 사이버 보안 연구를 진행하는 NCF(National Cybersecurity FFRDC)는 1999년 9월에 일반인들을 위한 CVE(Common Vulnerabilities and Exposure) 시스템을 연구했다. CVE는 공개적으로 알려진 각 취약성에 서로 다른 이름을 부여하여 사용자는 자신의 이름을 사용하여 특정 취약성에 대해 이야기할 수 있도록 하는 취약점 열거 시스템이다. CVE의 모든 취약성 데이터는 CVE 식별자로 관리하며 식별자는 CVA 넘버링 기

관인 CNA에서 할당한다. 보안 기업 및 리서치 조직과 주요 IT 벤더를 대표하는 CNA는 100여개 이상 존재한다. CVE의 주요 정보는 보안 취약점 또는 노출에 대한 간략한 설명, 취약점 보고서 및 권고 사항 링크가 포함될 수 있는 참조 정보가 포함된다 [12].

CVSS는 NIAC(National Infrastructure Advisory Council)에서 도입했으며 현재 FIRST(사고 대응 및 보안 팀 포럼)에서 관리합니다. CVSS는 상대적 심각도에 대한 메트릭을 제공하여 보안 관리자가 취약점의 우선 순위를 지정할 수 있도록 지원한다. CVSS는 각 취약성을 0에서 10까지의 정량적 수치로 나타내며 값이 높을수록 심각도가 높음을 나타낸다. CVSS는 3가지 다른 메트릭 그룹으로 구성된 개방형 프레임워크로 설계되었다. 1) 취약점의 일반적인 특성을 설명하는 기본 메트릭 2) 시간 경과에 따른 심각도의 변화를 나타내는 선택적 시간적 메트릭 및 3) 특정 사용자, 조직 또는 비즈니스 환경에 고유한 선택적 환경 메트릭. 기본 메트릭은 단독으로 사용하거나 다른 두 가지 선택적 메트릭과 함께 사용할 수 있다 [13].

본 연구에서는 사이버 공격을 설계된 자산에 존재하는 CVE를 통해 자산에서 작전에 사용하는 데이터를 파괴, 변조, 탈취하는 행위로 정의한다.

3. 시나리오 설계

임무기반 사이버 무기체계 효과성 분석을 위해서는 작전이 필요하다.

ATP(Army Techniques Publication) 3-09.12 [14]와 FM(Field Manuals) 3-09 [15]에 따르면 대화력전은 지대지 작전으로써 적의 무기, TA(target acquisition) 자산, 감시정찰 장비, C2 시설, 통신 및 물류 현장을 무력화하거나 파괴함으로써 적의 간접 사격으로부터 아군, 전투 기능 및 시설을 보호하는 작전이다. 대화력전은 각 포대 간의 네트워크 통신으로 표적의 위치를 식별 후 화력을 집중하여 타격하기 때문에 네트워크 통신 불안정하여 원활한 소통이 되지 않는 경우 작전이 진행되지 않고 CAS(Close Air Support) 작전으로 변경될 수 있다. JP 3-09.3 [16]에 따르면 CAS 작전은 지상 부대의 요청에 따라 공중에서 지원사격을 하는 작전으로써 공중과 지상 2개의 도메인을 포함하는 작전이다. CAS 작전에서의 사이버 공간은 지상과 공중 2개의 도메인을 연결하는 역할을 한다. 따라서 CAS 작전은 본 연구의 목표인 다양한 작전에서, 다양한 환경에서 사이버 공격으로 인한 임무 효과를 분석하기에 적합하다고 판단하였다.

CAS 작전을 기반으로 아래와 같이 시나리오를 설계하였으며 설계된 임무 시나리오 프로세스는 다음과 같다.

1) 아군 접점지역 대대단위 부대가 목표물을 탐지
2) 접점지역의 지휘관이 CAS 요청하기로 결심
3) 유닛이 TACP에 알림
4) 아군 지휘관은 상위 제대를 거쳐 공군에 CAS 요청
5) 적 사이버부대는 아군의 내부망에 침투
6) 적 사이버부대는 아군 작전의 효과를 최소화하기 위해 ATO 문서 작성 요소를 들키지 않게 공격(변조/탈취/파괴)
7) 적의 사이버 공격에 따라 아군의 작전 효과 감소(CAS 공격 지연, 지상군 연결 실패, 표적인지 실패)
8) 적의 사이버 공격 내용 및 효과 분석
9) 분석된 내용을 기반으로 CAS 요청 작전 재실행 여부 판단

4. MOE, MOP 설계와 분석

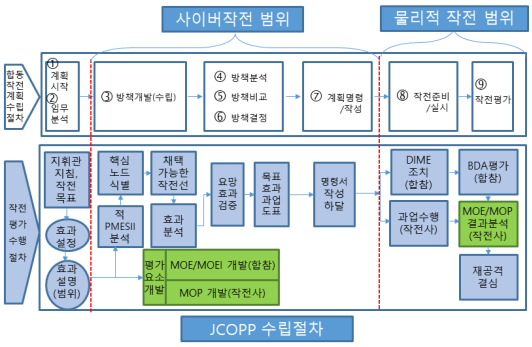
MOE와 MOP를 정의하기에 앞서 본 연구의 사이버 공간의 범위를 식별할 필요가 있다.

합동작전계획수립절차(Joint Operation Planning Process, JOPP)는 임무를 조사하기 위한 일련의 논리적 단계로 구성된 질서있고 분석적인 프로세스이다. JOPP는 해결해야 할 문제에 대한 계획을 개발하기 위해 지휘관, 참모, 예하 지휘관 및 기타 파트너의 작업을 조직하는 입증된 프로세스를 제공한다. 또한, 지휘관과 참모들이 계획 활동을 조직하고, 임무와 지휘관의 의도에 대한 공통된 이해를 공유하고, 효과적인 계획과 명령을 개발하도록 한다. JOPP는 반드시 준수해야 하는 정형화된 절차는 아니지만, JOPP의 절차에 따라 진행함에 따라 지휘관은 작전 진행 중 필요에 따라 계획을 수정하고, 실행하며 임무의 지속적인 관련성과 적합성에 의문을 제기할 수 있도록 가능한 한 넓은 시야를 유지하도록 돕는다 [17].

작전평가 수행 절차와 사이버 작전 범위를 그림 3과 같이 식별하였고, 식별된 사이버 작전 범위를 기반으로 MOE와 MOP를 설계했다.

4.1 MOE, MOP 정의

사이버공간작전 평가는 합동부대가 임무완수를 향해 진행하는 조치과정으로 정의하고 있다. MOE는 과업의 효율, 수행 방향, 행동의 질, 행동의 적절성으로, MOP는 과업달성의 객관적 기준, 작전의 수행 성과량, 행동의 양으로 정의하고 있다 [9].



(그림 3) JOPP 수립절차 內 사이버작전 범위 식별
(Fig 3) Identify the scope of cyber operation in Joint Operation Planing Process

본 연구에서는 사이버 공격 시 작전의 효과를 감소 시키기 위하여 ATO(Air Tasking Order) 문서 일부를 변조한다고 가정했다. ATO 문서는 장착 무장, 표적 위치, 작전 실행 시간 등의 작전에 큰 영향력을 가지고 있는 요소들로 작성되어 해당 요소들이 공격으로 인해 변조, 파괴 등의 피해를 입을 시 작전에 가장 큰 영향을 끼칠 것으로 판단했다. 따라서 ATO 문서의 요소(무장 정보, 표적 정보, 시간 정보 등의 사이버 공격이 가해질 요소)들을 MOE로 정의하고 변조된 CAS ATO에 의해 수행될 CAS 작전의 감소된 성공률을 MOP로 정의한다.

4.2 MOE, MOP 설계 방안

3 장에서 설계한 CAS 임무 시나리오를 기반으로 물리 작전과 연계하여 효과성 분석을 위한 MOE를 설계했다. 작전환경에 따라 MOE와 MOP는 달라질 수 있으나 작전에서 사용되는 명령문서의 요소로 MOE를 설계하였기 때문에 본 연구에서 다루는 CAS 작전 외에도 다양한 작전에서 사용할 수 있도록 설계했다.

적의 사이버 공격 효과는 사이버공격 형태(기만/위조/변조/약화/와해/파괴 등)에 의해 ATO문서를 변조하고 최종적으로 물리적 작전에 영향을 준다. 그러므로 MOE는 ATO 문서에서 변조될 가능성이 있는 요소로 선정하되 물리작전과 연계하기 위하여 JMEM 입력 요소로 선정한다. 그림 4는 선정된 MOE의 예시이며 표적의 경우 요청한 표적 위치와 전혀 상관이 없는 위치(좌표 변조로 인해 다리가 아닌 위병소의 위치가 되는 경우)의 경우 요청한 바와 전혀 다르므로 실제 임무 중 사이버 공격에 당했음을 감지할 수 있다. 사이버 공격을 인지했다는 것은 아군의 정상적인 임무 진행이 어렵다는 것을 예측 할 수 있으므로 적은 공격을 들키지 않기 위해 변조 범위에 따라 위치를 변조해야 한다. 다른 요소들도 위와 같은 요령으로 MOE를 설계할 수 있다. MOP의 경우 설계된 MOE를 적용하며 물리작전에서는 JWS(JMEM Weaponeering System) 실행 결과로, 사이버 공간에서의 효과성은 사이버 공격 전/후 비교로 산출되는 수치로 산출한다.

- 표적

표적종류	이동유무	표적 위치	변조 미 인식 지리적 범위	요망효과	대공화기	물리작전 영향점수
다리	고정	좌표(정의)	10Km	무력화	-	0.43

- 작전 시간

표적	시간	임무시간	물리작전 영향점수
다리	최소 30분	30분~1시간	0.56

- 주파수

주체	주파수	기만확률	변조 미 인식 수치 범위	예비주파수	물리작전 영향점수
ASOC	INT	10%	∓ 100이내	있음	0.13

- 장착 무장

폭탄	무게	장착 항공기	파괴 효과	물리작전 영향점수
Mk 82	500 파운드	F-5/FA-50/F-4/F-16/F-15	30×10 ft(Small)	0.23

(그림 4) 물리작전 영향점수(MOE) 설계 예시
(Fig 4) Physical Operation Impact Score Design Example

그림 4와 같이 설계하였을 때 각 데이터는 1의 초기 값을 가지고 있으며 사이버 공격으로 인해 데이터에 피해가 생겼을 경우 각 데이터 피해를 측정한다. 각 데이터는 물리작전에 영향이 가는 요소이므로 이를 물리작전 영향점수라 정의한다.

각 데아터의 피해는 작전의 종류가 같더라도 작전상황에 따라 환경이 달라질 수 있으므로 전문가의 판단에 따라 공격에 대한 피해를 산출한다. 물리작전 영향점수는 사이버 공격 전 물리작전 영향점수에서 사이버 공격으로 인한 피해 수치를 전문가의 측정 하에 차감하는 것으로 식 7과 같이 산출한다.

사이버공격 前물리작전영향점수
− 전문가가측정한피해수치
= 사이버 공격 後물리작전 영향점수 (7)

4.3 MOE, MOP 적용

본 연구는 사이버 공격으로 인한 물리 작전의 영향과 사이버 무기체계 효과성을 분석하기 위한 연구로써 사이버 공격 효과성 점수를 활용하여 사이버 무기체계의 효과성을 분석하고, 물리작전 영향점수를 활용하여 분석한 뒤 비교하여 사이버에서 일어난 공격의 효과가 물리 작전에도 영향을 끼치는지 분석한다.

사이버 공격 효과성 점수는 자산계층에서 산출되는 점수로써 이전의 본 연구팀의 연구 [11]에서 제시했던 사이버 공격 피해평가 프레임워크의 자산 산출식의 전문가 평가점수를 대체하여 적용한 뒤 계산한다. 변형된 산출식은 5.3장의

수식 8와 같으며 각 매개변수는 표4와 같다. 물리작전 영향점수는 사이버 공격으로 인한 물리작전의 영향을 비교 및 분석하기 위하여 아래의 순서로 진행된다.

1) 물리작전 영향점수를 반영하여 사이버 공격으로 인한 변조된 데이터(물리작전 MOE)를 산출한다.
2) 사이버 무기체계 효과성과 물리작전의 영향을 파악하기 위하여 JWS에 변조된 데이터를 입력한다.
3) 사이버 공격 후 JWS 결과(물리작전 MOP)와 사이버 공격이 진행되지 않았을 때의 JWS 결과를 분석한다.

5. 사이버 무기체계 효과성 분석 프레임워크

본 연구의 시나리오는 CAS 작전 시나리오이며 목표는 사이버 무기체계의 효과성 분석으로써 사이버 무기체계로인한 사이버 공간에서 진행되는 작전의 효과를 분석하는 것이다. 기존 사이버 공간에서의 피해평가는 사이버 공격 이전의 수치와 이후의 수치만을 비교함으로써 사이버 효과를 분석하였으나 물리작전과의 연계를 통하여 작전의 최종 결과를 분석함으로써 사이버 공간에서 일어난 공격으로 인해 물리작전에 끼치는 영향까지 파악 한다.

5 장에서는 사이버 무기체계 효과성 분석을 하기 위한 자산을 식별하고, 프레임워크 구조를 설계한 후 마지막으로 프레임워크가 적용된 후의 작전 결과를 예측한다.

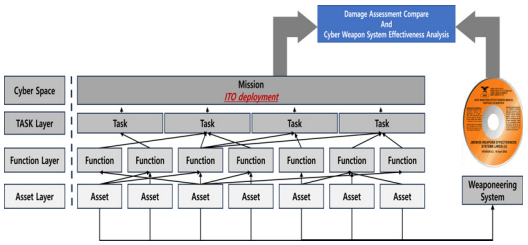
5.1 사이버 자산 식별 및 정의

북미지역의 전력 업체인 NERC(North American Electricity Reliability Corporation)는 사이버 자산을 프로그램 가능한 전자 장치 및 통신 네트워크로써 하드웨어, 소프트웨어 및 데이터로 정의하고 있다 [18].

본 연구의 작전 시나리오(CAS 작전)에서 자산은 요청서 작성(CAS요청서), 명령 문서(ATO 문서) 작성, 아군 전력 확인 등 시나리오 진행 중 데이터 작성, 열람, 전달 등을 위한 정보자산이다. 따라서 본 연구에서는 사이버 자산을 작전 시나리오에서 사용하는 정보 데이터가 이동하는 경로에 있는 모든 정보자산(PC, Switch, Server)이라고 정의하며 해당 정보자산에는 정보 데이터가 포함된다.

5.2 프레임워크 구조

본 연구에서 사이버 공간에서의 무기체계 효과도 평가를 위한 프레임워크는 자산, 기능, 작업, 임무의 4계층으로 구성된 절차 구조이며 그림 5와 같다.



(그림 5) 사이버 무기체계 효과성 분석 프레임워크 구조
(Fig 5) Cyber Weapon System Effectiveness Analysis Framework Structure

사이버 공격은 데이터를 공격하여 변조, 탈취, 파괴 등의 활동을 한다. 모든 데이터는 자산계층에서 작성, 열람, 전달 등을 하므로 사이버 공격은 자산계층에서 발생하며 자산이 가지고 있는 데이터를 대상으로 공격을 진행한다. 공격으로 인한 자산 가치의 변화가 상위계층에 영향을 미치고, 최종적으로는 임무에 영향을 미치게 된다.

자산계층은 임무 실행에 필요한 정보자산(PC, Switch, Server)이 있으며 정보자산 內 가용 가능한 데이터에 따라 그 가치가 달라진다. 기능계층은 임무 수행에 필요한 절차를 위한 기능(작전 환경 분석, 표적 식별, ITO 문서 작성 등)이며, 과업계층은 임무 수행 절차를 포함하고 있다. 마지막으로 임무계층은 수행할 작전을 의미한다.

자산계층에서는 사이버 무기체계의 효과성을 분석하기 위한 계산뿐만 아니라 물리작전에서의 무기체계 효과성 분석을 위한 계산을 위해 물리작전 영향점수를 산출하고 JMEM을 프로그램화하여 제공되고 있는 JWS에 적용하여 사이버 공격으로 인한 물리 무기체계의 효과를 분석한다.

기능계층에서는 기능 수행에 소요되는 시간과 수행하는 기능에 포함된 자산의 피해 정도에 따라 정확도를 산출하여 임무에 영향을 끼친다. 하위계층에서 산출된 수치에 따라 각 과업의 수치가 산출되고, 모든 과업의 합으로 임무의 값을 산출한다. 최종적으로 임무계층에서 산출되는 값과 JWS를 활용한 물리 무기체계의 효과를 비교하여 사이버 무기체계 효과성을 검증한다.

5.3 사이버 무기체계 효과성 분석 프레임워크 척도

사이버 무기체계 효과성 분석 프레임워크는 피해평가 프레임워크 [11]의 척도를 기반으로 사이버 공격의 임무 영향을 분석한다. 피해평가 프레임워크의 전문가 평가점수는 실제 임무를 수행하는 전문가가 부여하는 값으로, 1부터 5까지의 값을 부여한다. 그러나 이는 전적으로 전문가의 판단으로

만 측정되므로 전문가마다 판단의 근거가 크게 다를 수 있다. 본 연구에서는 이를 보완하여 자산에서 사용되는 데이터로 자산의 중요도를 측정하며 이는 식 8과 같고, 매개변수는 표 4와 같다.

$$A = \frac{F \bullet d}{V} \tag{8}$$

(표 4) 자산 수행도 매개변수 정의
(Table 4) Asset perform parameter definitions

매개변수	설명
A	자산 수행도
V	취약점 계수, Vul_{SP}
F	자산이 기능에 사용되는 수
d	데이터 점수 합

데이터 점수 합(d)의 데이터는 표적 정보, 장착 무장 정보, 항공기 정보 등으로써 4.2에서 설계한 지표와 같다. 자산마다 사용 가능한 데이터가 다르고, 하나의 데이터라도 없거나, 정상적이지 않다면 임무에 많은 영향을 끼치므로 모든 데이터는 중요함에 정도를 가리기 어렵다. 따라서 자산의 사용 가능 데이터 개수에 따라 자산의 중요도가 달라진다. 취약점 계수(V)는 이전의 본 연구팀의 연구 [19]의 수식으로 식 9와 같으며 이는 해당하는 자산에 할당된 애플리케이션 취약점, OS 취약점 등 모든 취약점에 해당하는 CVSS 점수를 합산하여 도출한 값이다.

$$Vul_{SP} = \Sigma_{k=1}^{n} CVSS_k \tag{9}$$

6. 실 험

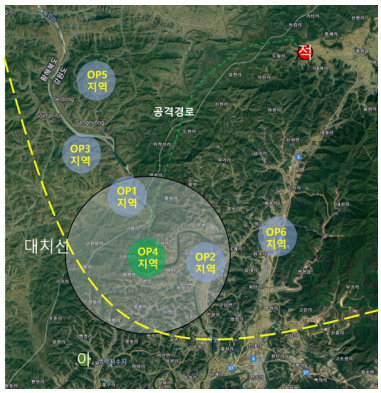
본 논문에서 제안하는 프레임워크의 적용성을 입증하기 위하여 실험을 진행한다. 실험은 임무 설정, 작전 시나리오 설계, 인프라 구성, 공격시나리오 설계, 효과분석의 5단계로 진행되며 3장에서 설계한 CAS 시나리오를 기반으로 실험을 진행했다. 또한, 사이버 공격 중 탈취의 경우 데이터에 직접적인 영향을 끼치지 않을뿐더러 어떠한 정보가 탈취되어 적의 행동이 바뀌었는지 알 수 없으므로 임무가 종료되어도 사이버 공격으로 임무에 영향이 미쳤는지 확인하기 어렵다. 따라서 본 논문에서는 변조, 파괴의 두 가지 사이버 공격으로 실험을 진행한다.

6.1 임무 설정

시나리오에서 사용될 작전 선택 및 요망효과, 사이버 공격을 받지 않을 경우의 정상 작전명령문서를 설정하는 것으로 시나리오에서 설계될 자산, 기능, 과업의 기반이 된다. 작전은 기계획 CAS 작전, 요망효과는 적 진행경로에 존재하는 OP4 지역 다리 파괴로 설정하였으며, 아군의 규모, 위치, 보유 탄약, 보유 무장 등을 설정하고 마찬가지로 적의 규모, 위치, 전력, 공격 경로 등의 전장 상황을 표 5와 같이 설정했으며 이를 기반으로 그림 6과 같이 전장 상황도를 지도에 표현하였다. 설정한 내용을 기반으로 작성되는 정상 작전 명령서는 표 6과 같이 작성된다.

(표 5) 전장 상황 설정
(Table 5) Battlefield Situation Settings

작전	기계획 CAS
요망 효과	적 진행경로에 존재하는 OP4 지역 다리 파괴
아군 위치	대치선 기준 남쪽 30Km 밖
아군 규모	연대 수준의 4부대 규모
대치중인 아군의 보유 무장	연대별 전차 2대, 포 1대
대치중인 아군의 보유 탄약	전차 포탄 7개, 소총 탄환 3000발
적군 규모	연대 수준의 2부대 규모
적군 위치	대치선 기준 60Km 밖
적 전력	전차 3대 이상
예상 공격 경로	산악지형을 좌측으로 우회하여 다리 통과(40Km)
다리 통과 예상 시간	13:20 I



(그림 6) 전장 상황도
(Fig 6) Battlefield Situation

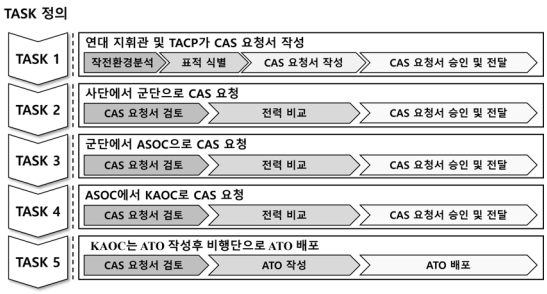
(표 6) ATO 작성 정보 일부 및 설명
(Table 6) ATO creation information and description

필드명	작성 정보	설명
MSN NO	1021	임무 번호
UNIT	8th wing	수행 부대명
TYPE/ NUMBER OF	4/FA-50	무장 명
CALL SIGN	Nani 23	콜사인
MSN AREA	OP4	임무 지역
IP TIME	1300I	최초 진입 시간
ToT	1320I	목표물 상공 도착시간
TGT Coordinate	CB2345341	표적 위치 좌표
Ordnance	each 4 Mk.82	장착 무장
Prime Frequency	TD 122	주 주파수
Back up Frequency	TD 238	보조 주파수
IFF Mode	2346	적/아 식별 코드
Play Time	30	수행 시간

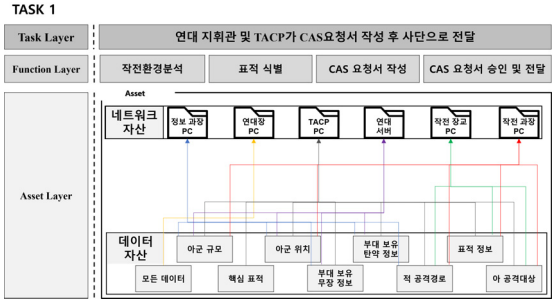
6.2 작전 시나리오 설계

시나리오 설계단계는 임무 설정에서 설정된 작전을 기반으로 임무, 과업, 기능, 자산, 자산에서 사용하는 데이터 순서로 설계하는 단계이다. 임무는 이전 단계에서 설정한 요망효과를 기준으로 설정되며 과업은 임무를 위해 수행하는 작전 하위단계의 임무 집합을 말한다. 기능은 과업을 수행하기 위한 행위로써 문서의 작성, 전달 등의 행동이다. 이러한 행동을 위해 수행자가 사용 및 소유하는 PC, Router와 같은 네트워크 장치와 기능을 수행하기 위해 사용되는 데이터를 자산이라 한다.

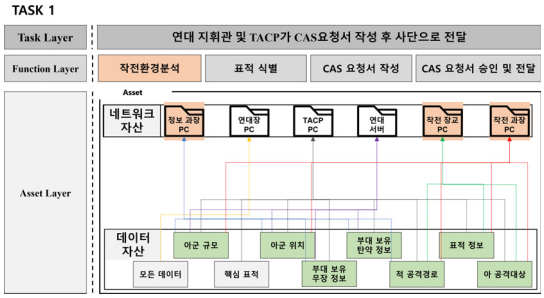
임무 설정 단계에서 설정된 작전은 기계획 CAS 작전이며 요망효과는 OP4 지역 위치에 있는 다리 파괴이므로 임무는 OP4 지역 다리 파괴를 위한 CAS 요청서를 KAOC로 전달하여 ATO를 배포하는 것으로 1부터 5까지의 총 5단계로 설계했다. 과업 1은 연대에서 진행되는 하위 임무로써 정보과장, 작전장교, 작전과장이 아군 규모 및 적 공격경로 등을 확인하여 작전환경을 분석한다. 분석된 작전환경을 기반으로 정보과장과 작전과장이 표적정보를 식별 후 TACP에게 전달하며 TACP는 서버에 적 정보 및 아군 정보를 요청 후 취합하여 CAS 요청서를 작성한다. TACP는 작성된 CAS 요청서를 연대장에게 전달하게 되며 연대장은 CAS 요청을 승인 후 서버에 요청서를 자정하고 상위제대로 재요청을 하게 된다. 마찬가지로 과업 2에서는 사단이 군단으로, 과업 3에서는 군단에서 ASOC으로 과업 4에서는 ASOC에서 KAOC로 요청서 검토, 전력 비교, 요청서 승인 및 전달의 과정을 거친다. 마지막으로 과업 5의 KAOC는 CAS요청서를 검토 후 ATO를 작성하며 비행단 및 하위 제대로 배포한다. 설계된 과업 및 기능은 그림 7과 같으며 자산은 그림 8과 같이 네트워크 자산과 데이터 자산을 나누어 식별하였고, 그림 9와 같이 기능마다 사용되는 자산을 식별했다.



(그림 7) 설계된 과업 및 기능
(Fig 7) Designed tasks and functions



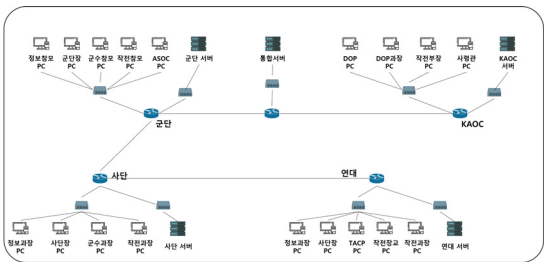
(그림 8) 과업1에서 식별한 자산
(Fig 8) Assets identified in Task 1



(그림 9) 기능에 사용되는 자산 식별
(Fig 9) Identify the assets used in the function

6.3 인프라 구성

설계된 시나리오에 적합한 네트워크 인프라 구성 및 자산의 애플리케이션과 취약점을 설계하는 단계이다. 사이버 공격자는 구성된 인프라를 통해 공격을 진행한다. 구성된 인프라는 그림 10과 같다.



(그림 10) 네트워크 인프라 구성
(Fig 10) Network Infrastructure Configuration

6.4 공격시나리오 설계

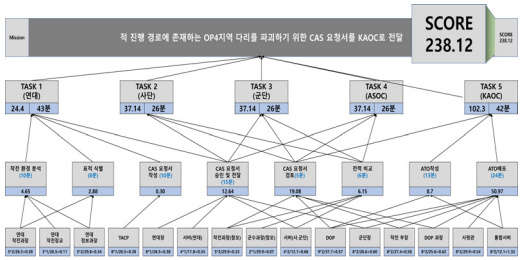
공격시나리오는 데이터 변조와 파괴 두 가지의 공격 형태로 저작했다. 파괴 및 변조 공격시나리오는 유사한 환경에서의 효과를 분석하기 위해 동일한 데이터를 공격하며 다음 순서에 따라 진행된다.

1) 공격자가 악성코드에 삽입된 첨부파일이 있는 '연대장 지시사항'이라는 메일을 작전과장, 작전장교, 정보과장에게 발신
2) 피해자는 첨부파일을 다운로드하여 실행함과 동시에 악성코드에 감염
3) 공격자의 목적은 아군 작전의 효과를 감소 시키는것
4) 공격자는 피해자들이 접근 가능한 작전 데이터를 확인하여 공격 목표를 설정
5) 공격자는 표적 정보와 무장 정보 데이터를 공격

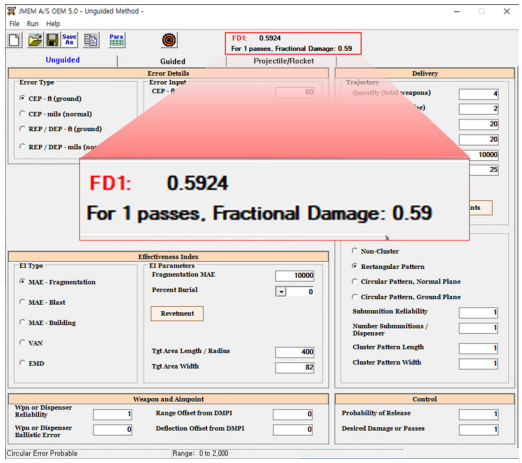
6.5 효과 분석

설계된 인프라와 작전/공격시나리오를 제시한 프레임워크에 적용하여 사이버 공간에서 진행된 임무 피해 효과와 JWS를 활용한 물리 효과를 비교하여 분석한다.

사이버 공격이 발생하지 않았을 때 프레임워크에 적용된 수치는 그림 11과같이 238.12로 산출되었으며 2.4장에서 언급한 무기체계 효과 교범을 기반으로 제작된 도구인 JWS에 입력 후 계산 결과 그림 12와 같이 FD1(부분 살상 확률) 0.59의 효과가 산출되었다.



(그림 11) 사이버 공격 발생 전 프레임워크 적용 결과
(Fig. 11) Results of applying the framework before cyber attacks

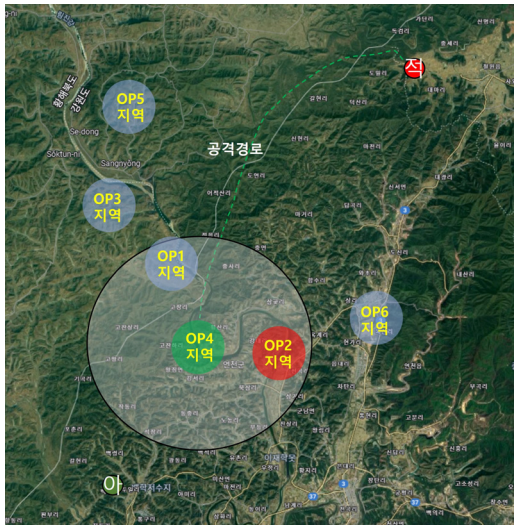


(그림 12) 사이버 공격 발생 전 JWS 적용 결과
(Fig. 12) Results of applying the JWS before cyber attacks

변조 공격시나리오에서 공격자로 인해 피해입은 데이터 자산은 표 7과 같으며 그림 13과 같이 OP4 지역에 인접하고 목표한 표적인 OP2 지역 다리로 변조하여 사이버 공격을 인지하기 어렵게 하였으므로 물리작전 영향점수가 0.34로 감소하였고, 장착무장의 개수를 4개에서 2개로 변조하여 물리작전 영향점수가 0.5점으로 감소했다. 또한, 표적 위치 및 무장 정보가 변조됨에 따라 표적 오차범위가 60ft에서 80ft로 변경되어 물리작전 영향점수가 0.34로 감소되었다. 데이터 변조로 인해 기능의 수행 시간 역시 변경되었으며 이는 표 8과 같다.

(표 7) 피해입은 데이터 자산 (변조)
(Table 7) Damaged Data Assets (Modification)

데이터명	정상 데이터	미인식 범위	변조된 데이터	물리작전 영향점수
표적 위치	OP4	OP1, OP2	OP2	0.34
표적 오차범위	60ft	±30ft	80ft	0.34
표적	다리	다리	다리	1
탄약 정보	KAOC/ Mk.82/4개	무장에 장착가능한, 짝수개	KAOC/ Mk.82/2개	0.5
무장 정보	FA-50	부대 內 보유한무장	FA-50	1

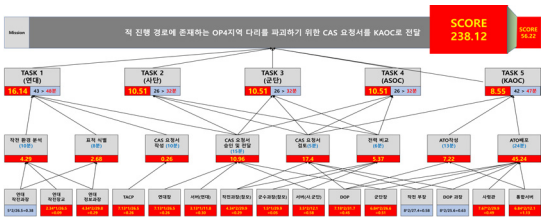


(그림 13) 변조된 표적 위치
(Fig 13) Modified target locaion

(표 8) 변경된 기능의 수행시간(변조)
(Table 8) Changed function execution time (Modification)

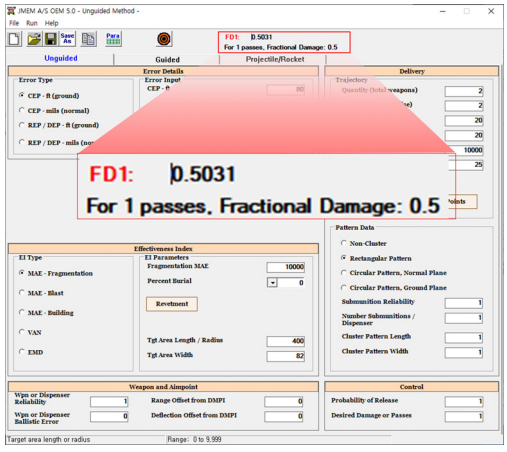
기능 명	정상 수행 시간 (분)	변경된 수행 시간 (분)
작전 환경분석	10	13
표적 식별	8	10
CAS 요청서 작성	10	10
CAS 요청서 승인 및 전달	15	15
CAS 요청서 검토	5	7
전력 비교	6	10
ATO 작성	13	15
ATO 배포	24	25

감소한 물리작전 영향점수를 프레임워크에 재적용하면 그림 14와 같이 56.22로 산출되며 공격으로 인한 사이버 작전의 효과는 76.4% 감소한 것을 확인할 수 있다.



(그림 14) 사이버 공격 발생 후 프레임워크 적용 결과(변조)
(Fig 14) Results of applying the framework after cyber attacks (Modification)

그림 15와 같이 물리적 효과는 0.5가 산출되었으며 이는 기존보다 약 15% 감소한 효과이다.



(그림 15) 사이버 공격 발생 후 JWS 적용 결과(변조)
(Fig 15) Results of applying the JWS after cyber attacks(Modification)

데이터 파괴 공격시나리오는 표적 위치 데이터가 파괴되면 임무 수행이 어려워지므로 사이버 공격이 발생하는 연대에서 공격을 인지하고 사이버 공간에서 진행하던 모든 임무를 물리 공간에서 진행하게 되어 효과측정이 되지 않는다. 공격자는 보유한 탄약과 무장 데이터 일부를 파괴하여 무장 및 탄약의 선정에 혼동을 일으켜 표 9와 같이 데이터가 변경되었고 표 10과 같이 기능 수행 시간이 변경되었다.

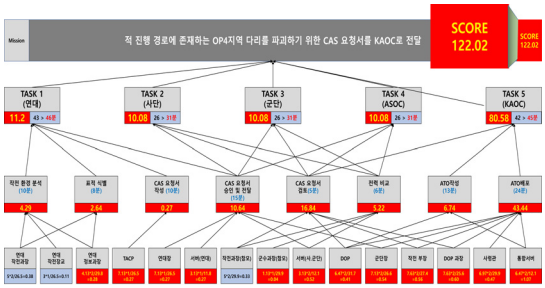
(표 9) 피해입은 데이터 자산(파괴)
(Table 9) Damaged Data Assets(Destroy)

데이터명	정상 데이터	변경된 데이터	물리작전 영향점수
표적 위치	OP4	OP4	1
표적 오차범위	60ft	75ft	0.43
표적	다리	다리	1
탄약 정보	KAOC/ Mk.82/4개	KAOC/ Mk.83/4개	0.77
무장 정보	FA-50	F-5	0.63

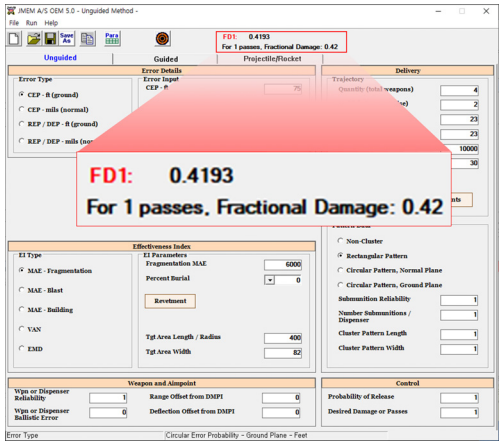
(표 10) 변경된 기능의 수행시간 (파괴)
(Table 10) Changed function execution time (Destroy)

기능 명	정상 수행 시간 (분)	변경된 수행 시간 (분)
작전 환경분석	10	10
표적 식별	8	8
CAS 요청서 작성	10	12
CAS 요청서 승인 및 전달	15	16
CAS 요청서 검토	5	7
전력 비교	6	8
ATO 작성	13	14
ATO 배포	24	24

프레임워크 적용 결과 최종 효과 수치는 그림 16과 같이 122.02로 사이버 공격 전보다 49% 감소하였으며 물리 효과 역시 그림 17과 같이 0.42.의 효과로 29% 감소한 것을 확인 했다.



(그림 16) 사이버 공격 발생 후 프레임워크 적용 결과(파괴)
(Fig 16) Results of applying the framework after cyber attacks (Destroy)



(그림 17) 사이버 공격 발생 후 JWS 적용 결과(파괴)
(Fig 17) Results of applying the JWS after cyber attacks(Destroy)

변조 및 파괴 공격의 결과 모두 사이버 임무 효과와 물리 무기체계 효과 수치가 감소했다. 변조 공격에서 지휘관은 사이버 작전 효과가 76.4% 감소하였으며, 표적의 위치가 변조되었으므로 정상적인 물리 작전을 수행할 수 없다고 판단할 수 있다. 또한, JWS에 입력하여 측정한 효과 역시 잘못된 위치정보로 입력된 정보로써 작전의 목표와 부합하지 않기 때문에 사이버 작전 재수행 여부를 결정한다. 그에 반해 파괴 공격에서 지휘관은 표적의 위치가 변조되지 않았기 때문에 물리 무기체계 효과의 감소로 인해 요망효과를 도출해 낼 수 있을지 판단하여 물리 작전 수행 여부를 결정한다.

7. 결 론

본 연구는 물리작전과의 연계를 통해 사이버 공격이 물리적 임무에 끼치는 영향을 분석하기 위한 프레임워크를 제시했다. 이전에 진행하였던 사이버 전투피해평가 프레임워크를 기반으로 물리작전에서 무기체계 효과교범으로 사용하고 있는 JMEM과 연계하여 사이버 공간에서의 공방 결과를 물리작전의 효과와 비교 및 분석하여 임무 영향을 파악하는 프레임워크를 설계했다. 이를 증명하기 위하여 국내외 군사교범 및 사전 연구들을 통해 작전 시나리오를 분석 및 설계하고 자산을 정의하여 실험을 진행했다. 실험 결과 사이버 임무 효과 수치의 감소폭이 클수록 물리 작전에 큰 영향을 미쳤으며 사이버 효과만으로 판단이 어려울 시 물리 무기체계 효과를 함께 비교 및 분석하여 물리 작전 진행 여부를 결정하는 데 도움이 되었다.

본 연구에서는 사이버 공격을 변조, 파괴의 두 가지 공격 형태로 진행하였으며 탈취의 경우 적 지휘관의 판단과 물리 전장 상황에 따라 적의 행동이 달라지기 때문에 이를 예측할 수 없다면 효과를 측정하기 어렵다고 판단하여 진행하지 않았다.

본 연구를 활용하여 다양한 작전에서 사이버 공격으로 인한 물리작전의 영향을 예측할 수 있으며, 전장 지휘관의 빠른 판단에 도움을 준다. 또한, 본 연구에서는 CAS 작전의 하나만 예시를 들어 실험을 진행하였으나 타 작전의 전문가들이 본 연구에서 다룬 MOE, MOP 설계 방법에 따라 새로운 MOE와 MOP를 설계하고 시나리오를 작성할 시 다양한 작전에서도 사용할 수 있을 것이다.

향후 연구는 다양한 작전에서 사용하고 있는 작전 문서들의 요소들을 분석하여 공통된 데이터와 작전별 데이터를 분류하여 하나의 프레임워크 혹은 도구로 통합 임무 영향 분석을 할 수 있도록 발전시킬 예정이다.

참고문헌(Reference)

[1] C. S. Park and Y. S. Park, "A study on the improvement of capability assessment and the plan for enhancing cyber warfare capability of Korea," Journal of the Korea Institute of Information and Communication Engineering, vol. 19, no. 5, pp. 1251 - 1258, 2015. https://doi.org/10.6109/jkiice.2015.19.5.1251

[2] M.R. Driels. Weaponeering : Conventional Weapon System Effectiveness. Reston, Va: American Institute of Aeronautics and Astronautics, Inc., 2013. Print.

[3] NOEL, Steven, et al. Analyzing mission impacts of cyber actions (AMICA). In: NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact. 2015.

[4] MUSMAN et al. "A cyber mission impact assessment tool", 2015 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE Access, p. 1-7, 2015. http://doi.org/10.1109/THS.2015.7225283

[5] Seung Keun Yoo et al. "Utilization of Defense Simulation Model in Warfighting Experimentations." The Korea Society for Simulation, pp. 117-122, May, 2005.

[6] Army, U. S., "Army Doctrine Publication (ADP) 3-0 Operations" Washington, DC, July, 2019.

[7] The Joint Staff, "Joint Publication (JP) 3-0, Joint Operation," Washington, DC, Oct, 2018.

[8] E.J. Robert, "Committee on national security systems (CNSS) glossary", Mar, 2022.

[9] The Joint Staff, "Joint Publication (JP) 3-12, Cyberspace Operation," Washington, DC, Jun, 2018.

[10] 진하 황, "M&S를 활용한 무기체계 효과분석에 관한 연구 감시장비 대안분석을 중심으로" 한성대학교 국방과학대학원, 국방M&S학과 석사학위논문, Aug. 2019.

[11] S.J. Kim et al., "Study on Cyber Attack Damage Assessment Framework," IEEE Access, Jun, 2022. https://doi.org/10.1109/ACCESS.2022.3179977

[12] D.E. Mann et al., "Towards a Common Enumeration of Vulnerabilities", 2nd Workshop Research with Security Vulnerability Databases, 1999.

[13] M. Peter, et al. "A complete guide to the common vulnerability scoring system version 2.0." Published by FIRST-forum of incident response and security teams. Vol. 1, Jun, 2007.

[14] Chief of Staff. "Army Techniques Publication (ATP) 3-09.12 Field Artillery Counterfire and Weapons Locating Radar Operation" Washington, DC, Oct, 2021.

[15] Chief of Staff. "Field Manuals (FM) 3-09 Fire Support and Field Artillery Operations" Washington, DC, Apr, 2020.

[16] Joint Chiefs of staff. "Joint Publication (JP) 3-09.3 Close Air Support." Washington, DC, Jul, 2009.

[17] The Joint Staff, "Joint Publication (JP) 5-0 Joint Operation Planing" Washington, DC, Aug, 2011.

[18] NERC, "Appendix 2 to the NERC Rules of Procedure", Atlanta, GA, Jan, 2021. https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_2_ROP_Definitions_20210119.pdf

[19] K.J. Kim et al. "Study on Prioritization of Actions by Classifying and Quantifying Cyber Operational Elements Using 5W1H Method." IEEE Access 10, 74765-74778, 2022. https://doi.org/10.1109/ACCESS.2022.3190530

◐ 저 자 소 개 ◑

장 지 수(Ji-su Jang)
2021년 호서전문학교 정보보호학과(학사)
2021년~현재 세종대학교 대학원 컴퓨터공학 지능형드론융합학과(공학석사)
관심분야 : 사이버전장, 소프트웨어 공학, 군사 공학, 기계학습, etc.
E-mail : wekki96@sju.ac.kr

김 국 진(Kook-jin Kim)
2017년 서울호서전문학교 정보보호학과(학사)
2019년 (주)엠투소프트 전자문서사업부 주임
2019년~현재 세종대학교 대학원 컴퓨터공학과(석박사통합과정)
관심분야 : 사이버전, 사이버 지휘통제, 정보보호, 인공지능, etc.
E-mail : kjkim@sju.ac.kr

윤 석 준(Suk-joon Yoon)
1980년 공군사관학교 항공공학과(학사)
1991년 국방대학교 무기체계공학(석사)
1996년 독일지휘관참모대학 군사학(석사)
2016년 합동군사대 교리부 연구교수
2020년~현재 세종대학교 사이버전연구소 교수
관심분야 : 사이버전, 사이버보안, 사이버 지휘통제, 사이버작전, etc.
E-mail : ysjoony@sejong.ac.kr

박 민 서(Min-seo Park)
2018년 고려대학교 사이버국방학과(학사)
2018년~현재 국방과학연구소 현역파견원
관심분야: 사이버전 사이버M&S 정보보호 사이버영향분석
Email : 19pms@korea.ac.kr

안 명 길(Myung-Kil Ahn)
1997년 충남대학교 정보통신공학과 (학사)
2003년 서강대학교 컴퓨터공학과 (석사)
2021년 중앙대학교 전기전자공학과 (박사)
2006년~현재 국방과학연구소 책임연구원
관심분야 : 사이버전, 사이버M&S, 사이버훈련, 사이버영향분석, etc.
E-mail : happyahn@add.re.kr

◐ 저 자 소 개 ◑

신 동 규(Dong-kyoo Shin)
1986년 서울대학교 컴퓨터과학과(학사)
1992년 Illinois Institute of Technology 대학원 컴퓨터과학과(석사)
1997년 Texas A&M University 대학원 컴퓨터과학과(박사)
1998년～현재 세종대학교 컴퓨터공학과 교수
관심분야 : 사이버전, 사이버보안, 사이버 지휘통제, 인공지능, 정보보호, etc.
E-mail : shindk@sejong.ac.kr