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

사이버공격에 의한 임무영향 분석 도구를 이용한 통합시나리오 저작 방법☆

Integrated Scenario Authoring Method using Mission Impact Analysis Tool due to Cyber Attacks

김 용 현[1*] 김 동 화[1] 이 동 환[1] 김 주 엽[1] 안 명 길[1]
Yonghyun Kim Donghwa Kim Donghwan Lee Juyoub Kim Myung Kil Ahn

요 약

사이버 공간에서 이루어지는 전투 행위가 군의 주요 임무체계 및 무기체계에 어떠한 영향을 미치는지를 평가할 수 있어야 한다. 사이버공격에 의한 임무영향을 사이버 M&S로 분석하기 위해서는 대상이 되는 임무체계와 사이버전 요소를 모델로 구축하고, 시뮬레이션을 위한 시나리오를 저작하여야 한다. 사이버전에 의한 임무영향 분석 관련 연구는 미국을 중심으로 많은 연구가 수행되었으며, 기존의 연구에서는 물리전장과 사이버전장에 대해 별개로 시나리오를 저작하였다. 임무영향 분석의 정확도를 높이기 위해서는 물리전장 모델과 사이버전장 모델을 결합한 시뮬레이션 환경을 구축하고, 임무 시나리오와 사이버공격/방어 시나리오를 통합해서 저작할 수 있어야 한다. 또한 물리전장과 사이버전장은 업무영역이 상이함을 고려하여 시나리오를 효율적으로 저작할 수 있는 방법이 필요하다. 본 논문에서는 임무체계 정보를 이용하여 시나리오 저작에 필요한 자료를 사전에 작성하고, 선작업된 자료를 이용하여 통합시나리오를 저작하는 방법을 제안한다. 제안한 방법은 시나리오 저작도구의 설계에 반영하여 개발하고 있으며, 제안 방법을 입증하기 위해 대화력전 분야의 통합시나리오 저작을 수행하였다. 향후, 제안한 방법을 반영한 시나리오 저작도구를 활용하면 임무영향 분석을 위한 통합시나리오를 짧은 시간에 쉽게 저작할 수 있게 될 것이다.

☞ 주제어 : 사이버 임무 영향 분석, 사이버 M&S, CyMIA, 시나리오

ABSTRACT

It must be possible to assess how combat actions taking place in cyberspace affect the military's major mission systems and weapon systems. In order to analyze the mission impact caused by a cyber attack through cyber M&S, the target mission system and cyber warfare elements must be built as a model and a scenario for simulation must be authored. Many studies related to mission impact analysis due to cyber warfare have been conducted focusing on the United States, and existing studies have authored separate scenarios for physical battlefields and cyber battlefields. It is necessary to build a simulation environment that combines a physical battlefield model and a cyber battlefield model, and be able to integrate and author mission scenarios and cyber attack/defense scenarios. In addition, the physical battlefield and cyber battlefield are different work areas, so authoring two types of scenarios for simulation is very complicated and time-consuming. In this paper, we propose a method of using mission system information to prepare the data needed for scenario authoring in advance and using the pre-worked data to author an integrated scenario. The proposed method is being developed by reflecting it in the design of the scenario authoring tool, and an integrated scenario authoring in the field of counter-fire warfare is being performed to prove the proposed method. In the future, by using a scenario authoring tool that reflects the proposed method, it will be possible to easily author an integrated scenario for mission impact analysis in a short period of time.

☞ keyword : Cyber Mission Impact Analysis, cyber M&S, CyMIA, Scenario

1. 서 론

컴퓨터와 정보통신기술(ICT)의 전투 과정 통합이 증가함에 따라 ICT 자산의 손상 또는 손실로 인해 임무 실패가 발생할 수 있는 환경이 조성되고 있다. 따라서 사이버 공격을 받는 임무의 성공 여부는 사이버 공격이 물리

1 Cyber Technology Center, Agency for Defense Development, Seoul, 05771, Rep. of Korea.
* Corresponding author (yonghyunkim@add.or.kr)
[Received 10 October 2023, Reviewed 24 October 2023(R2 9 November 2023), Accepted 15 November 2023]
☆ 본 연구는 국방과학연구소 과제(912921301)의 지원을 받아 수행한 논문임

공간의 기능을 어떻게 저하시키는지 이해하는 것에 크게 좌우된다. 사이버 공격의 임무영향에 대한 지식이 향상되면 시스템 설계가 개선되고, 사이버 위협 관리가 개선되며, 사이버 공격 중에도 운영될 수 있는 보다 탄력적인 임무체계를 만들 수 있다.

미국방부는 지·해·공·우주 전력과 사이버 군사력의 운용을 합동 작전의 관점에서 분석 및 평가하고 있으며, 특히 미공군은 CAAJED(Cyber and Air Joint Effects Demonstration) 사이버 레인지를 구축하여 사이버전과 연계되는 물리전 공간에서의 사이버전 피해 효과 분석 등을 실시하고 주기적인 훈련을 실시하고 있다. 또한 이러한 배경에서 미국은 사이버 전술/전략을 지·해·공·우주 공간에 걸친 모든 물리적 작전과의 사이버 작전 동기화에 초점을 두고 있다. MITRE는 사이버전에 대한 임무효과를 분석하기 위하여 임무수행과정을 모델링하고, 사이버 위협이 발생했을 때 임무수행과정에 어떠한 영향이 미치는지를 분석하고, 복구대책을 강구할 수 있는 도구를 개발하여 운용 중에 있다. NATO는 임무수행하는 프로세스를 모델링하고 이산이벤트 시뮬레이션과 그래프 기반 사이버 자산과 임무간의 의존관계를 모델링, 동적인 가시화를 통하여 다양한 위협 시나리오에 대하여 임무에 대한 영향을 정량화하고 분석하는 연구를 진행중에 있다 [1].

국내에서는 국방과학연구소를 중심으로 대규모 네트워크에 미치는 사이버전의 효과분석을 위한 구성모의 방식의 테스트베드를 일부 구축하였으며, 실가상 기술 기반의 사이버전 훈련을 수행하기 위한 모의전투 환경을 구축하였다. 또한 군은 다양한 임무체계 및 무기체계의 운용개념을 분석하고 평하기 위한 체계 모델을 개발하여 운용하고 있다. 그러나 군이 운용 중인 다양한 임무체계 및 무기체계에 대한 사이버공격 및 방어 행위가 어떠한 영향을 미치는지에 대해서는 단순 입력에 의한 초보적인 분석만이 이루어지고 있어 사이버전에 의한 임무 영향 분석 기술의 조속한 확보가 요구되는 실정이다. 국방과학연구소에서는 정보체계나 무기체계에 사이버공격이 가해졌을 때 체계에 부여된 임무가 받게 되는 피해를 분석하는 도구를 개발하고 있다 [2].

사이버공격에 의한 임무영향을 분석하기 위해서는 대상이 되는 임무체계와 사이버전 요소를 모델로 구축하고, 시뮬레이션을 위한 시나리오를 저작하여야 한다. 시나리오를 저작하기 위해서는 임무에 대한 운용개념도, 업무절차도, 부대/장비 배치도, 자산 상세정보, 체계 구성도/기능도, 데이터 흐름도 등을 이용한다. 또한 사이버공격/방어 시나리오를 저작하기 위해서는 네트워크 토폴로지, 취약점 정보 등을 파악하여야 한다. 물리전장과 사이버전장은 업무영역이 상이하여 시뮬레이션을 위한 임무 시나리오와 사이버공격/방어 시나리오를 저작하는 것은 매우 복잡하고, 많은 시간이 소요된다. 따라서 목적에 맞게 시뮬레이션을 수행하기 위해서는 물리전장 모델과 사이버전장 모델을 결합한 시뮬레이션 환경을 구축하고, 시나리오 저작 과정을 절차화한 임무 시나리오와 사이버공격/방어 시나리오를 통합해서 저작할 수 있어야 한다.

본 논문에서는 임무체계 정보를 이용하여 시나리오 저작에 필요한 자료를 사전에 작성하고, 선작업된 자료를 이용하여 통합시나리오를 저작하는 방법을 제안한다. 시나리오 저작도구의 설계에 반영하여 개발하고 있는 제안 방법을 입증하기 위해 대화력전 분야의 통합시나리오 저작 과정을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 사이버전에 의한 임무영향 분석 관련 국외 연구동향과 본 연구와 연관된 임무영향 도구를 소개한다. 3장에서는 사이버공격에 의한 임무영향 분석을 위한 통합시나리오 저작 방법을 제안한다. 4장에서는 실사례로 제안한 방법을 대화력전 분야에 적용하여 통합시나리오를 저작하는 과정을 설명하고, 5장에서 결론을 맺는다.

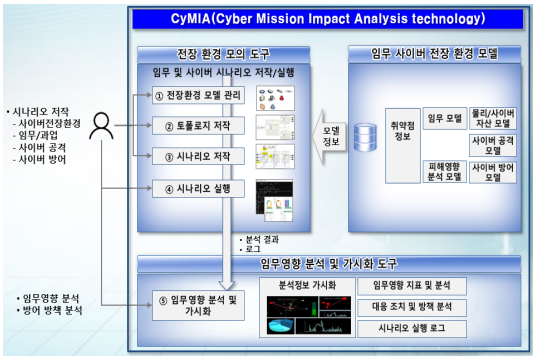
2. 관련연구

군사 작전에서 임무 수행에 활용되는 사이버 영역이 점차 확장됨에 따라 사이버 공간에서 수행되는 활동이 전통적인 영역인 지상, 해양, 항공 임무에 어떠한 영향을 미치는지 평가할 수 있어야 한다.

사이버 영역과 물리적 영역간의 영향을 분석하는 연구는 미국을 중심으로 다양하게 진행되었다. 영향성 분석을 위한 아키텍처 연구는 MITRE에서 수행한 AMICA[3]와 Cyber Argus[4]가 대표적이다. 영향성 분석을 위한 지표와 척도에 관한 연구로는 MITRE의 CMIA(Cyber Mission Impact Assessment)[5-6]와 JMEM(Joint Mission Impact Assessment)[2, 7]가 있다. 프로토타입을 위한 사이버 보안 적대적 활동 모델링 기법에 대한 연구도 수행이 되었다 [8-11]. 기존의 연구는 대부분 시나리오 저작에 대한 언급은 제한적이다. CMIA 도구는 BPMN(Business Process Modeling Notation)을 이용하여 임무 모델에 영향을 미치는 사이버 공격 행위를 공격의 효과 기반으로 모의하는 시나리오를 구성하여 임무 영향 분석을 지원하고 있다. AMICA는 임무 시나리오와 사이버공격/방어 시나

리오를 저작하는 도구로 기 개발된 도구를 각각 사용하고 있다.

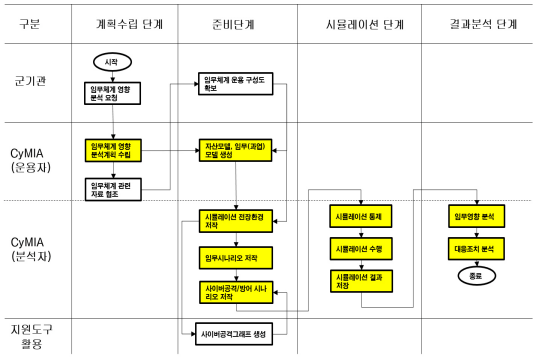
국방과학연구소에서는 정보체계나 무기체계에 사이버공격이 가해졌을 때 체계에 부여된 임무가 받게 되는 피해를 M&S(Modeling & Simulation) 기술을 이용하여 분석하는 도구(CyMIA)를 개발하고 있다 [12]. CyMIA는 그림 1에서와 같이 모델, 도구, 분석 파트로 구성되며, 모델 파트는 사이버 자산 및 물리 자산 모델, 사이버 공격 및 방어 모델, 피해영향 분석 모델로 구성된다. 도구 파트는 사이버 전장 환경을 구성하고, 임무를 수행하는 시나리오 및 사이버공격/방어 시나리오를 저작하는 기능을 제공한다. 임무영향 분석 파트는 사이버공격에 의한 자산의 영향이 최종적으로 임무에 미치는 영향을 분석하는 기능을 제공한다. CyMIA는 물리전장 모델과 사이버전장 모델을 결합한 시뮬레이션 환경을 구축하고, 임무 시나리오와 사이버공격/방어 시나리오를 통합해서 저작할 수 있다.



(그림 1) CyMIA 구성도
(Figure 1) CyMIA ConFigureuration Diagram

CyMIA의 운용절차는 다음과 같다. 군기관으로부터 사이버전에 의한 임무체계의 영향을 분석해 달라는 요청이 오면, CyMIA 운용자는 분석계획을 수립하고, 필요시 관련 군기관에 임무체계 관련자료를 협조한다. 운용자는 임무체계 자료를 이용하여 필요한 임무/사이버 자산모델, 임무(과업)모델을 구축하고, 분석자는 전장 환경 모의 도구를 사용하여 시뮬레이션을 위한 전장환경을 구축한다. 이후 전장환경에서 구동할 임무 시나리오와 사이버공격/방어 시나리오를 저작한다.

시뮬레이션 단계에서는 전장 환경 도구를 통해 시나리오를 선택하여 시뮬레이션을 수행하고, 시뮬레이션 과정과 결과를 저장한다. 모의결과분석 단계에서는 저장된 데이터베이스를 활용하여 시뮬레이션을 재현하고, 다양한 임무분석 기능을 통해 시뮬레이션 결과를 분석한다. 또한 사이버공격에 대한 대응조치 및 방책을 분석한다.



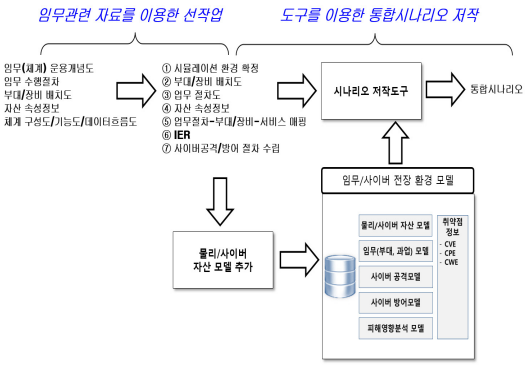
(그림 2) CyMIA 운용절차
(Figure 2) CyMIA Operating Procedures

3. 시뮬레이션을 위한 통합시나리오 저작 방법

본 장에서는 임무체계 정보를 이용하여 시나리오 저작에 필요한 자료를 사전에 작성하고, 선작업한 자료를 이용하여 통합시나리오를 저작하는 방법을 설명한다. 제안하는 통합시나리오 저작방법은 시나리오 저작 도구 기능에 반영되었으며, 제안하는 저작 방법은 사용자가 도구를 이용하여 시나리오를 저작하는 관점에서 기술한다.

시뮬레이션을 위한 시나리오는 개요, 전장환경, 임무, 사이버공격, 사이버방어로 구성된다. 각각 개별 시나리오로 저작 되지만 시나리오를 묶어서 관리하게 되며 이를 통합시나리오라고 한다. 사이버전의 임무영향 분석을 위한 통합시나리오를 저작하기 위해서 먼저 임무관련 정보를 이용하여 시뮬레이션 환경을 확정하고, 환경에 맞추어 사전에 시나리오 저작에 필요한 자료를 작성해야 한다. 다음으로 작성된 자료를 활용하여 시나리오 저작도구를 통한 통합시나리오를 저작한다.

그림 3은 통합시나리오를 저작하는 절차도이다. 통합시나리오를 저작하기 위해서는 임무체계에 대한 운용개념도, 임무 수행절차, 부대/장비 배치도, 자산 상세정보, 체계 구성도/기능도, 데이터 흐름도가 필요하다. 임무체계 관련 자료를 분석하여 시뮬레이션 환경을 선정하고, 선정된 시뮬레이션 환경에 맞게 임무체계 관련 자료를 이용하여 통합시나리오를 위한 선작업을 진행한다.



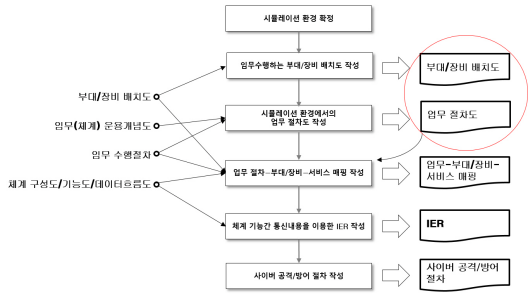
(그림 3) 통합시나리오 저작 절차도
(Figure 3) Integrated Scenario Authoring Process

선작업을 통해 시뮬레이션 환경에 맞춰 부대/장비 배치도, 업무 절차도, 자산 속성정보, 임무-부대/장비 매핑, 과업-서비스 매핑, IER(Information Exchange Requirement)을 작성한다. 또한 임무환경을 고려한 사이버공격과 사이버방어 절차를 수립한다.

선작업 과정을 거쳐 작성된 자료를 기반으로 물리/사이버 자산 모델을 필요시 개발하여 임무/사이버 전장 환경 모델에 추가한다. 또한, 시나리오 저작도구를 활용하여 통합시나리오를 저작하게 된다. 시나리오 저작도구는 데이터베이스에 저장되어 있는 임무/사이버 전장 환경 모델을 이용한다.

3.1 임무관련 자료를 이용한 선작업

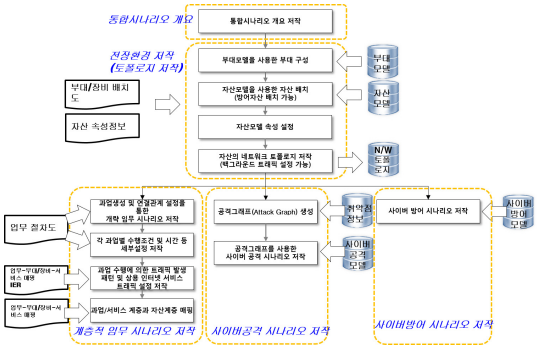
그림 4는 임무관련 자료를 이용한 선작업 순서도 및 자료 활용 및 재생산되는 관계도이다. 선작업의 첫 번째는 부대/장비 배치도를 활용하여 시나리오 저작에 맞게 임무를 수행하는 부대/장비 배치도를 작성한다. 다음으로 임무체계 운용개념도와 임무 수행절차를 활용하여 시뮬레이션 환경에 적합한 업무 절차도를 작성한다. 앞단계에서 작성된 부대/장비 배치도, 업무 절차, 데이터 흐름도를 이용하여 업무절차, 부대/장비, 서비스를 매핑한다. 다음으로 체계 구성도/기능도/데이터흐름도를 활용하여 체계 기능간 통신내용을 IER로 작성한다. 마지막으로 시뮬레이션 환경에서의 사이버 공격과 방어 절차를 작성한다. 이 과정을 통해서 임무관련 자료는 통합시나리오 저작에 필요한 자료로 재생산된다.



(그림 4) 임무관련 자료를 이용한 선작업 순서도
(Figure 4) Priority Task Flowchart using Mission-related Data

3.2 도구를 이용한 통합시나리오 저작

그림 5는 시나리오 저작 도구를 이용한 통합시나리오를 저작하는 순서도이다. 통합시나리오는 개요, 전장환경, 임무, 사이버공격, 사이버방어로 구성된다. 개요, 전장환경은 순차적으로 저작하면 되고, 임무, 사이버공격, 사이버방어는 주어진 전장환경에 맞춰 병렬로 저작하면 된다.



(그림 5) 시나리오 저작 도구를 이용한 통합시나리오 저작 순서도
(Figure 5) Integrated Scenario Authoring Flowchart using Scenario Authoring Tool

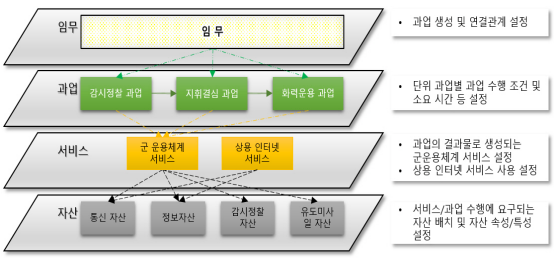
3.2.1 전장환경 저작

전장환경 부분은 임무영향 분석을 위한 전장환경을 구성하는 단계로 사전에 작성해 놓은 부대/장비 배치도와 자산 속성정보를 활용한다. 먼저 부대는 기 구축되어 있는 부대모델을 사용하여 관련 부대를 구성하고, 각 부대에서 사용하는 자산은 기 구축되어 있는 자산모델을

사용하여 자산을 배치한다. 자산별 구체적인 속성은 기 작성된 자산 속성정보를 활용하여 설정한 후, 자산간 연결을 통해 통신 네트워크 토폴로지를 저작한다. 이때 자산간 통신내용도 서비스 형식으로 저작할 수 있다. 네트워크 토폴로지는 임무, 사이버 공격, 사이버 방어 시나리오를 저작할 때 공통적으로 사용된다.

3.2.2 임무 시나리오 저작

임무 시나리오는 그림 6과 같이 임무를 자산, 서비스, 과업, 임무로 4개의 계층적 구조로 나눠서 저작한다. 임무는 어떠한 목적을 달성하기 위한 전술적 행동의 절차로 임무를 수행하기 위한 하부 구성요소는 과업으로 구성되어 있다. 과업은 수행 주체 단위별로 어떠한 결과를 도출하기 위해서 해야 할 일이며, 과업 수행 과정에는 정보의 입력과 생성이 발생하며 처리과정에서 저장되어 있는 정보를 활용한다. 이러한 정보 활용과정은 자산에서 제공되는 서비스로 표현할 수 있으며 서비스는 자산에서 제공하는 정보, 데이터 등을 보관, 처리 전달하는 행위이다. 서비스와 과업은 자산에서 수행되며, 자산은 임무 자산, 정보 자산, 통신 자산 등으로 구성된다. 임무는 임무를 수행하는 과업을 생성하고 과업간 연결을 설정하여 저작한다. 과업은 단위 과업별 과업 수행 조건 및 소요 시간 등을 설정하여 저작한다. 서비스는 과업의 결과물로 생성되는 군운용체계 서비스와 정보통신 자산의 상용 인터넷 서비스를 설정하여 저작한다. 서비스는 자산간의 유통되는 모든 메시지이며 메시지의 목록과 발생패턴을 정의한 IER을 활용하면 된다. 자산은 그림 5에서 설명한 전장환경 저작 부분에서 이미 저작된 상태이다. 임무 시나리오는 자산, 서비스, 과업, 임무 레이어에 저작된 내용을 모두 포함한 것이다.

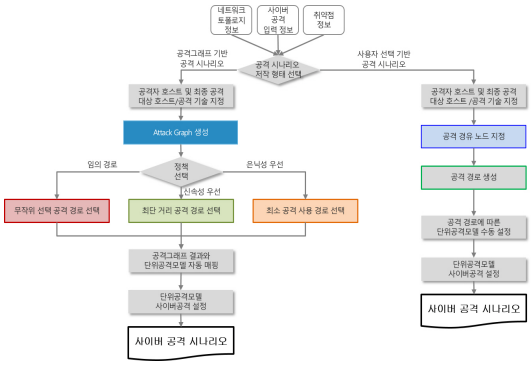


(그림 6) 임무 시나리오 저작을 위한 계층적 구조 및 레이어별 설정
(Figure 6) Hierarchical Structure and Layer-specific Settings for Mission Scenario Authoring

3.2.3 사이버공격 시나리오 저작

사이버공격 시나리오는 전장환경 저작 과정에서 도출된 네트워크 토폴로지와 취약점정보, 단위공격모델을 활용하여 저작한다. 그림 7은 사이버공격 시나리오 저작 순서도이다. 네트워크 토폴로지, 사이버공격 입력 정보, 취약점 정보를 입력한 후, 공격시나리오 저작형태를 선택한다. 공격시나리오 저작형태는 공격그래프 기반과 사용자 선택기반이 있다.

공격그래프 결과를 이용하여 공격경로를 선택하는 방법은 공격자 노드에서 공격대상 노드까지의 경로를 신속성을 우선으로 할 것인지, 은닉성을 우선으로 할 것인지, 임의의로 할 것인지를 결정하는 것이다. 사용자 선택 기반은 공격자 노드에서 공격대상자 노드까지의 경로를 사용자가 선택하는 방법이다.



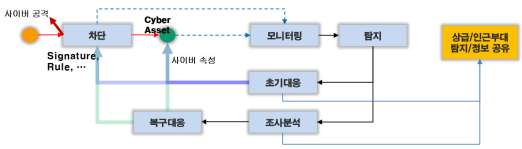
(그림 7) 사이버공격 시나리오 저작 순서도
(Figure 7) Cyber Attack Scenario Authoring Flowchart

공격경로 선택에 따라 4가지의 공격경로가 결정되면 공격그래프 결과를 이용할 경우는 공격그래프 결과와 단위공격모델이 자동으로 매핑됨으로써 사이버 공격 시나리오가 저작된다. 사용자 선택 기반으로 공격경로를 선택할 경우는 공격경로에 따른 단위공격모델을 수동으로 설정함으로써 사이버 공격 시나리오가 저작된다.

3.2.4 사이버방어 시나리오 저작

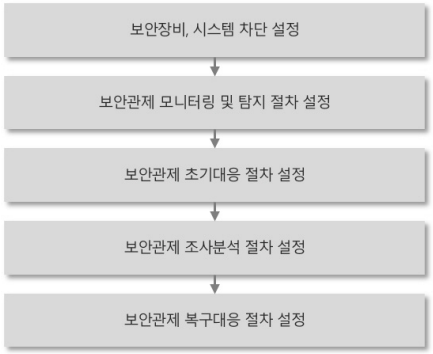
사이버방어 시나리오는 전장환경 저작 과정에서 도출된 네트워크 토폴로지와 방어행위 절차 모델, 방어자산 모델을 활용하여 저작한다. 사이버방어 시나리오는 사이버 방어 작전을 모델화한 사이버 방어행위 절차 모델을 기반으로 저작한다. 그림 8은 사이버 방어행위 절차를 모

델링한 것이다. 사이버 방어행위는 탐지하기 전과 탐지한 후의 대응으로 구분할 수 있으며, 탐지하기 전에는 사이버 공격을 최대한 막고, 지속적으로 모니터링을 하면서 공격을 탐지하기 위한 노력을 수행한다. 탐지 후에는 빠른 초기대응으로 공격의 확산을 차단하고, 정확한 조사분석을 통해 피해를 최소화하기 위해 복구대응 행위를 수행한다. 사이버 방어 시나리오는 모니터링, 탐지, 초기대응, 조사분석, 복귀대응과 같은 5개의 방어행위 절차 모델을 설정하는 형태로 저작된다.



(그림 8) 사이버 방어행위 절차 모델링
(Figure 8) Cyber Defense Procesure Modeling

그림 9는 사이버방어 시나리오 저작 순서도이다. 보안장비와 호스트 기능을 이용하여 차단을 설정하고, 다음으로 모니터링 대상이 되는 보안관제 대상과 탐지규칙을 설정한다. 이후 초기대응 절차, 조사분석 절차, 복구대응 절차를 순서로 설정한다.



(그림 9) 사이버방어 시나리오 저작 순서도
(Figure 9) Cyber Defense Scenario Authoring Flowchart

4. 대화력전 분야 통합시나리오 저작

본 장에서는 제안한 통합시나리오 저작방법의 실 적용사례로 대화력전 분야의 통합시나리오 저작과정을 기술한다. 대화력전을 수행하는 개념은 기동주대의 기동여건을 보장하고 상대적 화력우세를 달성하여 전장의 주도권을 획득하는 것이며, 이는 제대별 탐지 및 타격 자산의 능력을 고려하여 통상 사단급 이상 부대에서 실시한다. 이를 효과적으로 운용하기 위해 합동화력운용체계(JFOS-K)를 활용하여 합참을 중심으로 육해공군의 가용한 탐지 자산과 타격 수단을 통합 운용한다.

4.1 임무관련 자료를 이용한 선작업

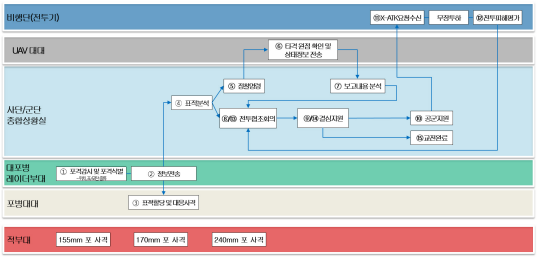
대화력전 임무 모의는 적의 장사정포 공격상황을 모의하고, 발사지점을 식별하여 자주포, 전술지대지 유도탄, 공대지 유도탄의 타격체계로 무력화시키는 것이다. 임무 모의와 사이버 공격에 대한 대화력전 임무의 영향분석을 포함한 시뮬레이션의 개요를 표 1에 정리하였다.

(표 1) 시뮬레이션 환경
(Table 1) Simulation Environment

임무	대화력전
주요 내용	• TPQ-36/37, Arthur-K 대포병레이더가 사격중인 적 포병부대 원점을 식별하여 아군이 대포병사격 실시
적용 제대 및 작전범주	• 사/군단 포병대대 • 사/군단급 대화력전
표적 특성	• 고정표적
작전 공간	• 지상, 사이버
통신망	• 지상망(ATCIS, B2CS, BTCS, AFCCS)
참여 모델	• 아군 - 감시정찰: 대포병 레이더 (TPQ-36/37/74, Arthur-K), UAV - 지휘통제 : ATCIS, AFCCS - 타격체계: K9, MLRS, X-ATK • 적군 - 타격체계: 자주포(170mm), 방사포(240mm)
시뮬레이션 목적	지상군 포병전에 대한 적 사이버 공격시 작전영향 분석 → 적 피해율 00% 이상
업무(Task)	• 적 장사정포 발사 • 적 장사정포 발사위치 파악 • 표적정보송신/수신 및 표적할당 • 최단 시간내 대응 포사격 • 합동화력운용(K-9, MLRS, 천무, ATCMS, X-ATK)
사이버공간	• 사이버 공격

임무	대화력전
공격, 방어 방안	- ATCIS, BTCS, AFCCS유통정보 변조/누락(표적위치, 표적할당등) - ATCIS, BTCS, AFCCS 전산장비 동작 방해 (정보 전달시간증가) • 사이버 방어(추천 방어조치수행)
평가지표	• 적 피해율 • 체계 반응 시간 • 노출시간내 표적타격 비율 • 사격명령 착오율 • 중복표적 발생률

대화력전의 상황 전계를 기반으로 대화력전의 제대별 업무 절차를 작성하면 그림 10과 같다. 설명의 편의를 위해 그림 10에는 사단과 군단의 대화력 업무를 같이 표시하였다. 실제로는 사단과 군단의 업무는 개별적으로 수행되며, 상하부대의 구조에 따라 협조요청하는 업무절차가 추가되어야 한다. 그림에서와 같이 대화력전 기본업무는 적부대의 공격을 탐지하고 대응하는 절차를 연결시킨 것으로, 이 자료와 시간정보를 이용하면 임무(과업) 시나리오를 작성할 수 있게 된다.



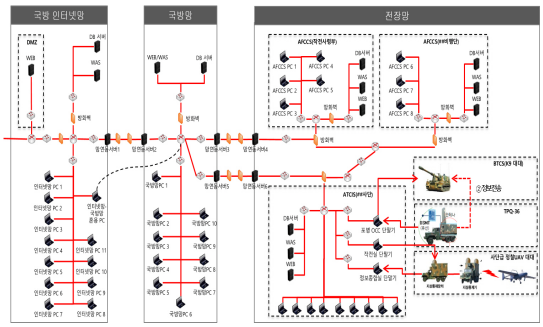
(그림 10) 대화력전 업무 절차도
(Figure 10) Counterfire Business Procedures

대화력전 임무에 가하는 사이버공격은 외부 공격자가 국방 인터넷망, 국방망, 전장망에 잠입해 표적정보를 변조하는 것으로 한다. 국방 인터넷망에 있는 공개 웹 서버의 게시판에 문서형 악성코드를 업로드 해서 침투를 하고, 인터넷망/국방망 혼용 PC를 통해 국방망에 접근한다. 이후 망연동장비를 통해 전장망에 침투한다. 전장망에서 유통되는 패킷을 후킹해서 표적정보를 변조하는 공격을 수행한다.

4.2 도구를 이용한 통합시나리오 저작

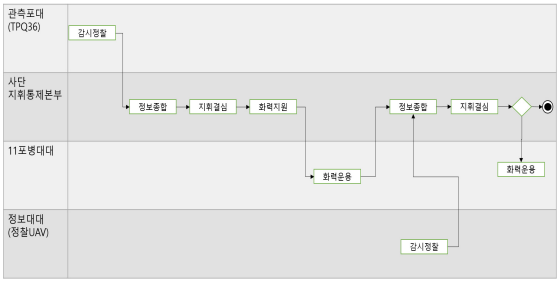
통합시나리오는 CyMIA를 이용하여 저작과정을 기술하여야 하지만 현재 도구가 개발이 진행되고 있어 본 절에서는 시나리오의 내용을 그림 위주로 설명한다. 또한 시뮬레이션 환경 중 사단급의 대화력전의 통합시나리오를 저작하는 과정을 기술한다. 통합시나리오는 통합시나리오 개요, 전장환경, 임무 시나리오, 사이버공격, 사이버방어로 구성된다.

부대별 자산배치도는 부대간 망을 연결하면 그림 11과 같은 네트워크 토폴로지가 구성된다. 본 네트워크 구성도는 외부 인터넷망을 이용하여 사이버공격을 수행하는 시나리오를 위해 인터넷, 국방망을 포함하였다.



(그림 11) 네트워크 토폴로지 구성
(Figure 11) Network Topology ConFigureuration

임무 시나리오는 임무를 수행하는 과업을 생성하고, 과업의 순서에 맞춰 과업을 연결해서 저작한다. 그림 12는 사단급 대화력전에 대한 과업을 생성한 것이다.



(그림 12) 대화력전 과업 생성
(Figure 12) Creating Tasks for Counterfire

과업이 생성되면 과업모델 속성을 입력한다. 과업모델 속성은 과업의 시작조건, 소요시간, 종료조건, 운용자산, 과업수행 과정에서의 송수신되는 서비스가 있다. 표 2는 임무 시나리오에서 설정할 서비스를 나타낸 것이다.

(표 2) 임무 시나리오에서 설정할 서비스
(Table 2) Services in Mission Scenario

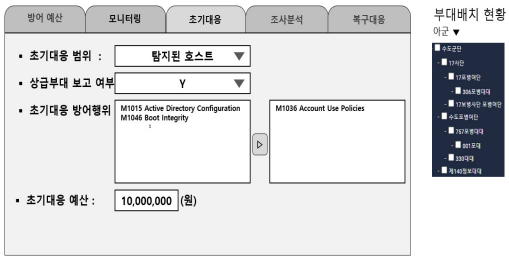
서비스	송신 부대	송신 자산	수신 부대	수신 자산
감시정찰보고	관측포대	ATCIS 클라이언트	사단 지휘소	ATCIS 클라이언트
정보종합보고	사단 지휘소	ATCIS 클라이언트	사단 지휘소	ATCIS 클라이언트
사격명령	사단 지휘소	ATCIS 클라이언트	사단 지휘소	ATCIS 클라이언트
사격명령	사단 지휘소	ATCIS 클라이언트	155mm 포병대대	ATCIS 클라이언트
사격결과보고	155mm 포병대대	ATCIS 클라이언트	사단지휘소	ATCIS 클라이언트

사이버공격은 국방 인터넷망에 있는 공개 웹 서버의 게시판에 문서형 악성코드를 업로드 해서 침투를 하고, 인터넷망/국방망 혼용 PC를 통해 국방망에 접근한다. 이후 망연동장비를 통해 전장망에 침투하고, 전장망에서 유통되는 패킷을 후킹해서 표적정보를 변조하는 공격을 수행한다. 표 3은 사이버공격 순서와 각 단계별 수행할 단위공격을 나타낸 것이다. 본 사이버공격 시나리오는 사용자 선택 기반 시나리오이며, 식별된 MITRE TTP의 단위공격모델을 매핑시켜서 사이버공격 시나리오를 저작한다.

(표 3) 사이버공격 순서 및 단위공격
(Table 3) Cyber Attack Sequence and Unit Attack

순서	망	공격 대상	수행 항목	단위공격
1	국방 인터넷망 (DMZ 구간)	DMZ 구간 공개웹 서버	취약점 스캔 진행	Active Scanning (T1595)
2			취약점 공격 수행	Exploit Public-Facing Application (T1190)
3			문서형악성코드 업로드	Stage Capabilities (T1608)
4	국방 인터넷망	인터넷 망PC2	DMZ 구간 공개 웹 서버 방문 후 문서형 악성코드 다운로드 및 실행	User Execution (T1204)
5			문서형악성코드는	Explit (T1190)
			Exploit을 하여 악성 프로세스 생성	
6			악성코드는 공격자 단말로 Reverse Shell 연결 수행 (공격자는 PC2의 제어권획득)	Command and Scripting Interpreter (T1059)
7		국방 인터넷망 네트워크	추가 내부접근확장을 위해 내부망스캐닝 (인터넷망/국방망혼용 PC에 RDP 포트 활성화 확인)	Active Scanning (T1595)
8		인터넷망/국방망혼용 PC	크리덴셜획득	Brute Force (T1110)
9			제어권획득	Remote Services (T1021)
10	국방망	국방망 네트워크	추가 내부접근 확장을 위해 내부망 스캐닝 (망연동 서버 발견 및 취약점 스캔)	Active Scanning (T1595)
11		망연계 서버1,2	망연동서버 취약점을 이용해 제어권획득	Exploit Public-Facing Application (T1190)
12	전장망	전장망 네트워크	ATCIS 서버 내 WAS, WEB, DB 서버 취약점 스캔 (WEB 서버 대시보드 취약점 발견)	Active Scanning (T1595)
13		WEB 서버	취약점 공격 수행	Exploit Public-Facing Application (T1190)
14			웹 쉘 생성	Server Software Component (T1505)
15			웹 쉘을 통해 데이터 수집 (추가 악성 프로그램 생성을 위한 데이터 수집용도)	Automated Collection (T1119)
16			분석 패킷을 토대로 내부에 Hooking 코드 설치	Hijack Execution Flow (T1574)
17			표적 대상 변조 및 누락 수행	Data Manipulation (T1565)

방어행위 절차는 모니터링 및 탐지, 초기대응, 조사분석, 복구대응으로 나눠져 있으며, 각각의 단계마다 화면에서 설정하는 형태로 저작하게 된다. 그림 13은 초기대응 화면을 나타낸 것으로 초기대응 방어행위를 선택하고, 주어진 초기대응예산을 입력함으로써 시뮬레이션 과정에서 주어진 예산범위내에서 초기대응 방어행위를 수행하게 된다.



(그림 13) 초기대응 설정 GUI
(Figure 13) Initial Response Setting GUI

5. 결 론

사이버 공격에 의한 임무영향을 분석하기 위해서는 대상이 되는 임무체계 모델을 구축하고, 시뮬레이션을 위한 시나리오를 저작하여야 한다. 시나리오를 저작하기 위해서는 임무에 대한 운용개념도, 업무절차도, 부대/장비 배치도, 자산 상세정보, 체계 구성도/기능도, 데이터 흐름도 등이 필요하다. 또한 사이버 공격과 방어 시나리오를 저작하기 위해서는 네트워크 토폴로지, 취약점 정보 등이 필요하다. 본 논문에서는 사이버전에 의한 임무영향 분석을 위한 통합시나리오를 저작하는 방법을 제안하고, 실제 군작전 임무에 적용하여 통합시나리오를 저작하는 과정을 실사례로 제시하였다. 제안한 방법을 반영한 시나리오 저작도구를 활용하면 임무영향 분석을 위한 통합시나리오를 짧은 시간에 쉽게 저작할 수 있다.

본 논문과 관련하여 향후 개선할 사항은 다음과 같다. 먼저 시나리오 저작 대상이 되는 임무체계의 관련정보의 수준 차이로 인하여 임무관련 자료를 이용한 선작업이 제한되었다. 이를 개선하기 위해서는 임무체계의 특성을 분류할 필요가 있고, 특성에 맞게 확보할 자료를 정리할 필요가 있다. 다음으로 CyMIA가 현재 구현중으로 도구를 이용한 저작이 불가함으로 인해 본 논문에서 정립한 시나리오 저작방법에 대한 검증이 완전하지 못했다. 따라서 CyMIA 도구가 개발 완료된 이후 본 논문에서 수립한 시나리오 저작방법은 추가 검증이 필요하다.

참고문헌(Reference)

[1] Wansoo Cho, “The Analysis of Evaluation the Impact of Cyber Attacks on Mission Systems,” Research Report ADDR-412-220103, Agency for Defense Development, 2022.

[2] Ji-su Jang, Kook-jin Kim, Suk-joon Yoon, Min-seo Park, Myung-Kil Ahn, Dong-kyoo Shin, “A Study on the Framework for Analyzing the Effectiveness of Cyber Weapon Systems Associated with Cyberspace and Physical Space,” Journal of Internet Computing and Services, Vol. 23, No. 5, pp. 111-126, 2022. http://doi.org/10.7472/jksii.2022.23.5.111

[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] Alexandre, B. B., Paulo, C., Michael, H. “Cyber-Argus: Modeling C2 Impacts of Cyber Attacks,” 19th ICCRTS – C2 Agility: Lessons Learned from Research and Operations, 2014.

[5] S. Musman, A. Temin, M. Tanner, R. Fox, B. Pridemore, “Evaluating the Impact of Cyber Attacks on Missions,” in Proceeedings of the 5th International Conference on Information Warfare and Security, Dayton, Ohio, 2010, edited by E. Armistead and E. Cowan, pp. 446-456, 2010.

[6] 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

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

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

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

[10] E.J. Robert, Committee on national security systems (CNSS) glossary, Mar, 2022.
[11] The Joint Staff, Joint Publication (JP) 3-12, Cyberspace Operation, Washington, DC, Jun, 2018.
[12] Yonghyun Kim, Donghwa Kim, Donghwan Lee, Juyoub Kim, Myungkil Ahn, “Study on the Hierarchical Structure Model-based Scenario Authoring Method for Mission Impact Analysis by Cyber Warfare,” 2023 Korea Institute of Military Science and Technology Comprehensive Academic Symposium, pp. 1571-1572, 2023.

◐ 저 자 소 개 ◑

김 용 현(Yonghyun Kim)
1993년 광운대학교 전자공학과(공학사)
1995년 광운대학교 대학원 전자공학과(공학석사)
2013년 광운대학교 대학원 전자통신공학과(공학박사)
1995년~현재 국방과학연구소 책임연구원
관심분야 : 사이버보안, 무선센서네트워크 etc.
E-mail : yonghyunkim@add.re.kr

김 동 화(Donghwa Kim)
2004년 고려대학교 전기전자전파학과(공학사)
2007년 고려대학교 대학원 전기공학과(공학석사)
2007년~현재 국방과학연구소 선임연구원
관심분야 : 사이버보안, 사이버전 M&S etc.
E-mail : dhkim@add.re.kr

이 동 환(Donghwan Lee)
2006년 고려대학교 산업시스템정보공학과(공학사)
2008년 고려대학교 컴퓨터학과(이학석사)
2008년~현재 국방과학연구소 선임연구원
관심분야 : 무선네트워크 보안, 분산시스템 보안, 사이버전 M&S 등
E-mail : dlee@add.re.kr

◐ 저 자 소 개 ◑

김 주 엽(JuYoub Kim)
1992년 경기대학교 경영정보학과(경영학사)
1995년 서강대학교 대학원 경영학과(경영석사)
1995년~현재 국방과학연구소 책임연구원
관심분야 : 사이버보안, 센서네트워크 etc
E-mail : pluto@add.re.kr

안 명 길(Myung Kil Ahn)
1997년 충남대학교 정보통신공학과(공학사)
2003년 서강대학교 대학원 컴퓨터공학과(공학석사)
2021년 중앙대학교 대학원 전자전기공학과 컴퓨터전공(공학박사)
2006년~현재 국방과학연구소 책임연구원
관심분야 : 사이버보안, 사전위협분석 및 취약성검증
E-mail : happyahn@add.re.kr