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

계층적 사이버전 훈련 시나리오 저작

Layered Authoring of Cyber Warfare Training Scenario

송 의 현[1] 김 동 화[1] 안 명 길[1*]
Uihyeon Song Donghwa Kim Myung Kil Ahn

요 약

사이버전 훈련은 사이버전 역량 제고를 위한 핵심 수단이다. 일반적으로 사이버전 훈련은 시나리오에 의해 진행되며, 훈련의 질을 높여줄 수 있는 다양한 요소를 시나리오에 포함시킴으로써 훈련의 효과를 배가시킬 수 있다. 본 논문에서는 훈련 시나리오에 포함시킬 요소로 식별된 훈련 정보, 네트워크 맵, 트래픽 발생 정책, 위협/방어 행위를 소개하고, 이를 계층화하여 조합하는 방식으로 다양한 훈련 시나리오를 저작하는 방법을 제시한다. 그리고 각 시나리오 계층을 통합적으로 관리하기 위한 데이터베이스 설계를 제안한다. 계층적 훈련 시나리오 저작 방법은 기 저작된 계층들의 재사용을 통한 저작 편의성의 증대와, 계층 간의 다양한 조합을 바탕으로 훈련 시나리오를 확장시킬 수 있다는 장점을 가진다.

☞ 주제어 : 사이버전 훈련, 시나리오 저작, 시나리오 계층, 데이터베이스

ABSTRACT

Cyber warfare training is a key factor for boosting cyber warfare competence. In general, cyber warfare training is conducted by scenarios, and the effects of training can be enhanced by including various elements in the scenarios that can improve the quality of training. In this paper, we introduce the training information, network map, traffic generation policy, threat/defense behavior identified as elements to be included in training scenarios, and propose a method of authoring training scenarios by layering and combining them. We also propose a database design for integrated management of each scenario layer. The layered training scenario authoring method has the advantage of increasing convenience of authoring by reusing existing layers and extending training scenarios based on various combinations between the layers.

☞ keyword : cyber warfare training, scenario authoring, scenario layer, database

1. 서 론

사이버공간은 물리적인 실체를 갖지 않는 특수한 전장이다. 세계 각국은 보이지 않는 제 5의 전장인 사이버공간에서의 우위를 확보하기 위해 다양한 노력을 기울이고 있다. 육, 해, 공, 우주 등 전력이 무기체계에 의해 결정되는 타 전장과 달리 사이버공간의 전력은 사람에 의해 결정되며, 사이버전 역량은 곧 사이버 인력과 그들을 운용하는 전략 및 전술이다. 미국, 중국, 이스라엘 등 사이버 강국으로 일컬어지는 국가들은 이러한 사이버전 역량 확보를 목적으로 공격적인 투자를 이어가고 있다.

사이버전 훈련은 사이버전 역량 제고를 위한 핵심 수단으로서 다양한 목적의 사이버전 훈련 설계 및 시행을 통해 사이버 인력의 실력을 배양하고 실전 감각을 유지시켜야 하며, 이 과정에서 사이버 공간에서의 전술, 기법 및 절차(Tactics, Techniques, and Procedures, TTP)를 수립, 보완해 나가야 한다.

효과적인 사이버전 훈련을 위해서는 실전적 훈련 환경과 다양한 훈련 콘텐츠를 제공하는 훈련 시스템이 필요하다. 현재 세계적으로 많은 훈련 시스템이 운용 중에 있으나, 대부분은 단순 공격 모듈의 나열로 시나리오를 구성하고 있다는 한계가 있다. 또한 군이 사용할 훈련 시나리오의 저작을 위탁하기 위해서는 국방망, 전장망 등의 훈련 환경 정보와 시나리오를 구성할 TTP 정보의 제공이 필요한데, 이는 보안상 불가능하기에 군의 훈련에 기성 훈련 시스템을 도입하는 것은 적절치 않다. 이러한 이유로 군이 사용할 독자적인 훈련 시스템을 갖출 필요가 있다.

본 논문은 계층적인 훈련 시나리오 저작 방법을 다룬

1 The 2nd R&D Institute, Agency for Defense Development, Seoul, 05661, Korea
* Corresponding author (happyahn@add.re.kr)
[Received 14 November 2019, Reviewed 21 November 2019, Accepted 8 December 2019]

다. 일반적으로 훈련 시나리오에는 훈련에 참여하는 객체의 시간에 따른 행위 시퀀스가 담기게 된다[1]. 그러나 모의전투 개념의 전술 훈련을 실시하기 위해서는 훈련의 다양성과 질을 높여줄 수 있는 여러 요소를 포함하는 훈련 시나리오가 필요하다. 훈련 시나리오의 '계층적' 저작은 이러한 요소들을 입체적으로 포함시키기 위한 개념이다.

본 논문의 구성은 다음과 같다. 2장에서는 국내와 해외의 사이버전 훈련 시스템들을 소개하고 각각의 훈련 시나리오를 분석한다. 3장에서는 훈련 시나리오에 포함시킬 요소로 식별된 훈련 정보, 네트워크 맵, 트래픽 발생 정책, 위협/방어 행위를 소개하고 각 항목의 저작 방안을 제안한다. 4장에서는 3장에서 다룬 요소를 바탕으로 훈련 시나리오를 계층적으로 저작해나가는 방법을 제시한다. 그리고 5장에서 향후 연구 방향의 제안과 함께 결론을 맺는다.

2. 관련 연구

세계적으로 많은 사이버전 훈련 시스템이 운용 중에 있다. 여러 업체가 훈련 시스템을 개발해 서비스 중이며, 국방력 증대를 위해 자체적인 훈련 시스템을 운용하는 국가도 많을 것으로 사료된다. 그러나 보유하고 있는 훈련 시스템의 설계 정보를 공개하는 경우는 매우 드물다. 설계 정보는 업체의 입장에서 영업비밀이며, 국가에게는 무기의 설계도면처럼 대외비로서 관리해야 할 정보이다. 이러한 이유로 현존 훈련 시스템의 구체적인 훈련 시나리오 저작 방법에 대해 얻을 수 있는 정보는 제한적이다.

본 장에서는 사이버 훈련에 대한 이해를 돕기 위해 대표적인 사이버 훈련 및 훈련 시스템을 간략히 소개한다. 또한 그들이 훈련에 사용하는 시나리오는 어떻게 구성되는지 살펴보고 제약사항을 도출한다.

2.1 Locked Shields

현존하는 사이버 훈련 중 가장 규모가 크고 복잡한 훈련으로 알려져 있는 NATO(North Atlantic Treaty Organization)의 Locked Shields는 NATO CCDCOE (Cooperative Cyber Defense Center of Excellence)에 의해 2010년부터 매해 개최되는 훈련이다[2]. Locked Shields는 사이버 위협으로부터 IT 시스템 및 기반시설을 보호하는 훈련을 진행함으로써 사이버 보안 전문가들의 역량을 향상시키는 것을 목표로 한다. Locked Shields 2019에서는 4000개 이상의 가상화된 시스템과 약 2500개의 공격이 사용되었으며, 세계 각국에서 1200명 이상의 사이버 보안 전문가가 참여했다. 훈련 시나리오는 최신 해킹 기술들을 반영해 실제 사이버 공격 수준으로 구성되는 것으로 알려져 있다.

Locked Shields 2019에서는 참여하는 훈련자들이 팀을 이루어 Berylia라는 가상의 국가에 발생한 대규모 사이버 공격에 대응하도록 하는 훈련 시나리오를 사용했으며, 훈련자들에게는 다음과 같은 임무가 주어졌다.

- Main Scenario Challenge

  ISP(Internet Service Provider), 군 기지 등 가상 국가의 중요 시설에 사이버 위협이 발생하여 국가기반시설의 작동이 심각한 수준으로 저해된다. 참가자들은 해당 상황에서 시스템의 가용성이 유지되도록 해야 하며, 의사 결정 등의 정책적 임무도 수행해야 한다.

- Forensic Challenge

  사이버 공격을 분석해 위협의 근원을 찾고, 보고서를 작성하는 임무이다. 이를 위해 훈련자들은 네트워크 트래픽, 메모리 덤프, 레지스트리, 메일 등을 조사해 공격에 사용된 악성코드가 어떠한 조직에 의해 제작되었고 어떠한 취약점을 사용하는지 파악하게 된다.

- Media Challenge

  위기 대응을 위한 언론과의 소통을 평가하기 위한 챌린지로, 팀의 대변인이 언론에 대응하는 속도, 정확성, 논리성 등을 평가한다.

- Legal Challenge

  사이버 공격을 법적으로 분석하고 대응하는데 초점을 둔 챌린지로, 팀의 법적 고문을 필두로 법적 측면의 다양한 질문에 답변하는 임무를 수행한다.

2.2 CyberShield TnS

Cybershield TnS(Training and Simulation)는 이스라엘의 Cyberbit사에서 발표한 종합적인 사이버 방어 솔루션인 Cybershield의 구성 요소 중 하나로, 사이버전 훈련과 시뮬레이션을 위한 시스템이다. Cybershield TnS는 모든 형태의 사이버 공격에 대응해 조직체 및 군사적 목적의 네트워크를 보호할 수 있도록 사이버 보안 전문가 및 의사결정자의 훈련을 지원하는 가상 사이버 환경을 제공한다[3]. 이스라엘군은 Cybershield TnS를 이용해 사이버전 훈련을 실시하고 있는 것으로 알려져 있다.

Cybershield TnS는 현실 세계의 다양한 사이버 위협을 훈련 시나리오로 제공하며, SCADA(Supervisory Control

And Data Acquisition) 공격 시나리오 등의 특수한 훈련 시나리오를 보유하고 있다. 시스템의 공격 시나리오는 단위 위협의 시간 별 열거로 이루어지며, 이에 따라 시스템에서 위협을 발생시키고 훈련자는 방어 행위를 수행하게 된다.

훈련관리자는 Cybershield TnS의 훈련 관리 시스템을 통해 훈련 세션을 위한 훈련 방법과 훈련 시나리오를 정의, 구축, 배치, 실행시킬 수 있다. 이후 훈련 설정 시 네트워크 수정, 훈련 팀 할당, 훈련 시나리오 선택 및 훈련 목적 정의 등을 수행하게 된다.

Cybershield TnS는 다양한 사용 옵션을 제공한다. 훈련 방법을 포함하는 완전한 턴키(turnkey) 솔루션을 제공받거나, 사용자가 원하는 서비스를 선택해 그에 상응하는 값을 지불하고 사용할 수 있다. 업체에서 훈련 시나리오를 저작해 제공한다는 점은 타 훈련시스템과 유사하다.

2.3 CMT

국방과학연구소(Agency for Defense Development)는 사이버 위협이 대규모 네트워크에 미치는 영향을 분석하기 위해 LVC(Live, Virtual and Constructive) 환경에서 시나리오를 통한 사이버전 효과분석과 사이버전 위협/방어 기술의 검증 및 훈련을 지원하는 사이버전 모의분석 도구인 CMT(Cyber Warfare Modelling Technology using LVC)를 개발해 운용 중이다. 사이버전 모의분석 기술은 사이버전 위협/방어 기술에 대한 각종 시험평가와 향후 사이버전 전투실험 및 훈련체계 구축 시 적용 가능한 기술로 평가된다[4][5].

(그림 1) CMT 운용 개념 및 시스템 구성
(Figure 1) CMT operational concept and system architecture

CMT는 그림 1과 같이 사이버전 효과분석 및 기술 검증을 위한 구성모의(constructive) 모델과 사이버전 훈련을 지원하기 위한 가상운용환경, 그리고 시나리오 저작 도구 및 효과분석기를 포함한다. 시나리오 저작은 시스템 및 네트워크 배치와 사이버 위협/방어 시나리오 구성이라는 두 항목으로 이루어진다[6].

2.4 제약사항

Locked Shields 훈련은 공격 시나리오에 따라 훈련자가 블루팀의 일원으로서 방어 임무를 수행하는 방식으로 진행되며, 훈련자의 공격 훈련은 다루지 않는다. Cybershield TnS 또한 시스템이 제공하는 공격 시나리오에 따라 훈련자가 방어 역할을 수행하도록 하는 방식을 채택하고 있으며, 공격 훈련에 대한 구체적인 언급은 없다. 이를 비롯한 대부분의 상용 훈련 시스템들은 서비스의 대상인 민간 기업의 네트워크 인프라 및 비즈니스 연속성 보호를 목적으로 하며, 이에 따라 방어 훈련에 초점을 두고 설계된다. 그러나 사이버 안보의 관점에서는 방어 훈련만큼이나 공격 훈련도 중요하게 고려해야 하고, 군은 사이버 공격과 방어 훈련 시나리오 저작을 모두 지원하는 훈련 시스템을 확보할 필요가 있다. 이러한 필요성에 따라 3장에서는 위협 행위를 비롯해 훈련 시나리오에 포함시킬 요소로 식별한 항목들을 소개한다.

CMT는 훈련 시나리오의 범위에 네트워크 배치와 사이버 위협/방어 시나리오 구성이라는 항목을 포함시켰다. 이러한 요소를 통해 사용자는 원하는 환경을 구성할 수 있고, 사용할 위협/방어 행위를 저작할 수 있다. 그러나 CMT의 경우 훈련자의 훈련 행위를 정의하기 위한 시나리오 저작이라기보다는 위협과 방어 행위에 의한 결과 분석에 중점을 두는 시나리오 저작이기 때문에 실질적인 훈련에 적용하기에는 부족하다. 또한 사용자가 저작할 수 있는 항목의 증가는 세부적인 훈련 설계를 가능하게 한다는 점에서 긍정적이지만, 동시에 훈련 시나리오 저작의 난이도를 상승시킬 수 있다는 문제를 지니고 있다. 이에 사용자의 저작 편의성 확보를 위한 고민이 필요하다. 이러한 문제점을 해결하기 위해 4장에서는 계층적 훈련 시나리오 저작 방법을 소개한다.

3. 훈련 시나리오 구성 요소

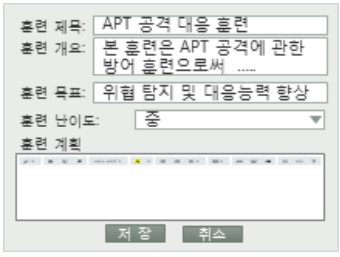
사이버전의 양상이 복잡해질수록 그 훈련의 수준도 고도화 되어야 하며, 특히 국방 영역에서는 모의전투 개

념의 전술 훈련을 실시할 필요가 있다. 훈련 시나리오는 본질적으로 훈련을 설계하고 이를 훈련 시스템에 탑재시키기 위한 사용자 인터페이스(interface)의 역할을 가지며, 이러한 관점에서 훈련 시나리오에 훈련의 다양성과 질을 높여줄 수 있는 여러 요소를 포함시킬 수 있어야 한다[7]. 이에 국방과학연구소의 사이버전 모의전투 도구를 비롯한 신생 훈련시스템들은 다양한 요소를 훈련 시나리오의 범주에 포함시키는 추세이다.

본 장에서는 훈련 시나리오의 범주에 포함시켜야 할 요소로서 식별한 네 가지 항목의 내용과 저작 방안을 살펴본다.

3.1 훈련 정보

훈련 정보는 훈련을 정의하기 위한 항목이다. 훈련 정보 항목을 통해 사용자는 그림 2와 같이 훈련의 제목, 개요 및 목적 등 훈련에 대한 일반적인 정보를 서술할 수 있어야 한다[8]. 훈련 정보의 범위에는 훈련을 수행하기 위해 필요한 팀 구성 계획과 팀 내 훈련자의 역할 할당이 포함되며, 이에 대한 자원 및 권한 분배 계획 정보를 함께 입력해 향후 저작된 시나리오를 운용할 때 가이드라인으로 활용할 수 있도록 한다.

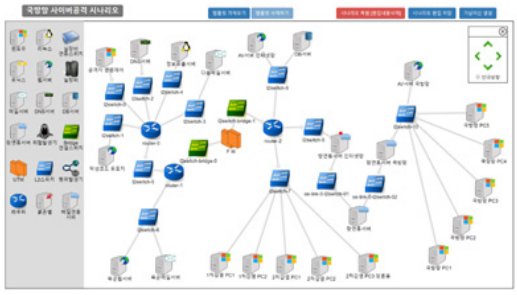


(그림 2) 훈련 정보 저작 예
(Figure 2) Training information authoring example

3.2 네트워크 맵

네트워크 맵은 훈련을 수행할 환경을 구축하기 위한 항목이다. 훈련을 수행할 가상환경 모의 과정에서 네트워크 토폴로지 정보를 사용자가 직접 입력해 원하는 훈련 환경을 구성할 수 있도록 한다.

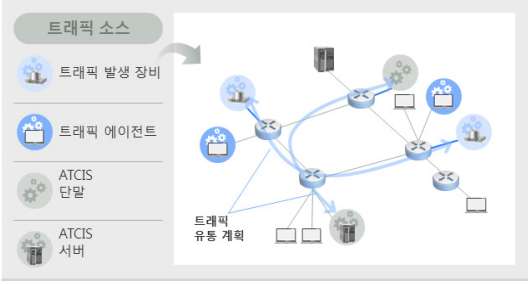
그림 3과 같이 가용한 시스템 및 네트워크 장비를 GUI(Graphical User Interface) 상에 아이콘 형태로 나타내며, 이를 배치하고 링크(link)를 연결하는 방식으로 네트워크 맵을 저작할 수 있어야 한다[8]. 장비의 속성은 네트워크 맵 상에서 아이콘 클릭 시 확인 가능한 창을 통해 설정할 수 있도록 한다.



(그림 3) 네트워크 맵 저작 예
(Figure 3) Network map authoring example

3.3 트래픽 발생 정책

트래픽 발생 정책은 훈련 환경에 현실감을 더하기 위한 항목으로, 네트워크 맵에 트래픽을 공급하기 위한 정책을 사용자가 직접 저작할 수 있도록 한다. 트래픽 발생을 위해 트래픽 발생 장비를 도입하거나 자체 트래픽 에이전트를 개발해 활용하는 등 여러 트래픽 소스를 복합적으로 사용할 수 있어야 한다[8]. 예를 들어 일반적인 배경 트래픽은 트래픽 발생 장비로, 국방망이나 전장망 등 특수한 환경의 트래픽은 자체 트래픽 에이전트를 통해 모의할 수 있을 것이다. 이러한 경우를 고려해서 트래픽 발생 정책의 범위는 훈련에 사용되는 트래픽 소스 별 트래픽 발생 정책과 발생시킨 트래픽을 훈련 환경에 적절히 공급하기 위한 트래픽 유통 계획을 포함한다.



(그림 4) 트래픽 유통계획 저작 예
(Figure 4) Traffic distribution plan authoring example

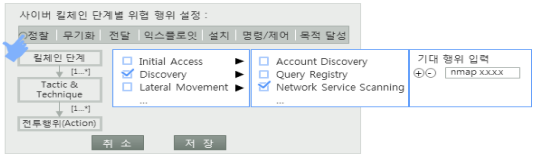
그림 4의 예는 육군전술지휘정보체계(ATCIS, Army

Tactical Command Information System)의 트래픽 모의를 표현한 것이다. 트래픽 발생 장비와 트래픽 에이전트를 함께 사용해 트래픽을 발생시키며, 네트워크 맵 상에 ATCIS 단말 및 서버를 가상화시켜 배치함으로써 전장망과 유사한 실전적 훈련 환경을 구성하는 모습을 확인할 수 있다.

3.4 위협/방어 행위

위협/방어 행위는 훈련에 참여하는 객체의 행위를 저작하기 위한 항목이다. 위협 행위는 레드팀 역할을 맡은 객체가 수행할 TTP를 의미하며, 방어 행위는 블루팀 역할을 맡은 객체가 수행할 TTP를 뜻한다. 훈련에 참여하는 객체는 훈련자 또는 위협/방어 행위를 모의하는 에이전트가 될 수 있다.

훈련자의 행위 수행 결과를 확인하기 위해 훈련자 기대 행위를 입력할 수 있다. 훈련자 기대 행위란 저작한 위협/방어 행위에 대한 훈련자의 예상 행위를 의미한다. 이는 훈련자 행위 모니터링 및 사후강평을 지원하기 위한 기능이다.



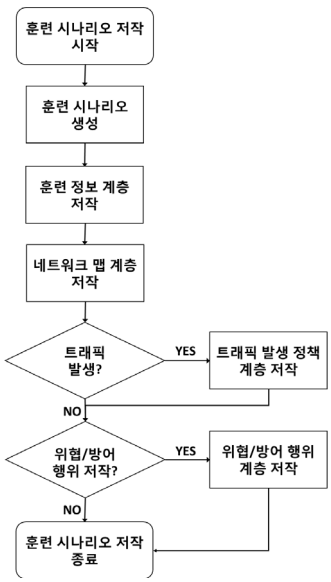
(그림 5) 위협/방어 행위 저작 예
(Figure 5) Threat/defense behavior authoring example

그림 5는 위협/방어 행위 저작의 예시로서, 대표적인 사이버 공격 분석 모델인 사이버 킬체인(Cyber Kill Chain) 단계 별로 위협/방어 행위를 설정할 수 있도록 한다. 각 사이버 킬체인 단계에서 사용할 수 있는 전술을 추천하고, 전술을 선택하면 해당 전술에 포함되는 기법들을 제시하는 형태이다. 기법 선택 후에는 해당 기법에 대한 훈련자의 기대 행위를 입력할 수 있다[8]. 예시에서 사용한 TTP는 MITRE사의 ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) 프레임워크를 바탕으로 구성했다. 사이버 킬체인의 단계 중 정찰을 선택하고, 추천되는 전술 중에서는 Discovery를, 기법 중에서는 Network Service Scanning을 설정한 모습이다. 이러한 방식으로 위협/방어 행위의 시퀀스를 구성해 훈련 시나리오에 포함시킬 수 있어야 한다.

4. 계층적 훈련 시나리오 저작 방법

4.1 저작 순서

3장에서 식별한 요소들은 훈련 시나리오를 구성하는 계층이 된다. 훈련 시나리오는 훈련 정보 계층, 네트워크 맵 계층, 트래픽 발생 정책 계층, 위협/방어 행위 계층 순으로 그림 6과 같이 순차적으로 저작할 수 있다. 이때 각 계층의 저작은 선행적으로 저작된 계층의 재사용 또는 수정을 포함한다.



(그림 6) 훈련 시나리오 저작 순서도
(Figure 6) Training scenario authoring flowchart

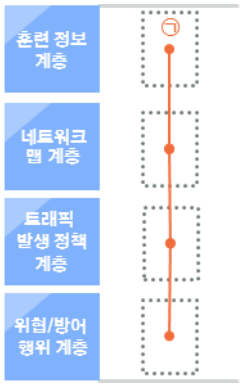
훈련 시나리오를 생성하고 훈련 정보 계층과 네트워크 맵 계층을 저작한다. 트래픽 발생 정책 계층과 위협/방어 행위 계층은 선택적으로 훈련 시나리오에 포함시킬 수 있다. 이는 훈련의 종류에 따라 배경 트래픽이 불필요할 수 있으며, 높은 수준의 훈련자들이 참여할 경우 위협/방어 행위를 저작하지 않고 훈련자들 간 자유롭게 공방 행위를 펼치도록 하는 방식의 훈련이 가능해야하기 때문이다[9].

4.2 저작 방법

각 계층은 독립적으로 저작이 가능하다. 훈련 정보 계층에서 목적에 따라 다양한 훈련을 정의할 수 있으며, 네

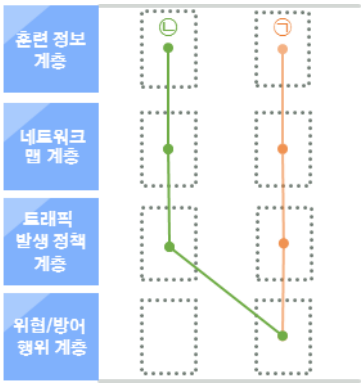
트워크 맵 계층에서는 국방망, 전장망, 인터넷망 등의 다양한 네트워크 맵을 저작해둘 수 있다. 이와 유사하게 트래픽 발생 정책 계층에서도 다양한 망에 대한 배경 트래픽이나 DDoS(Distributed Denial of Service)와 같은 특수한 형태의 트래픽 발생 정책을 저작할 수 있고, 위협/방어 행위 계층에서 현실의 위협/방어 행위를 모사하는 TTP를 선행적으로 저작할 수 있다.

훈련 시나리오는 생성된 계층 정보를 바탕으로 저작할 수 있다. 훈련 시나리오의 다양한 저작 방법을 차례로 살펴본다.



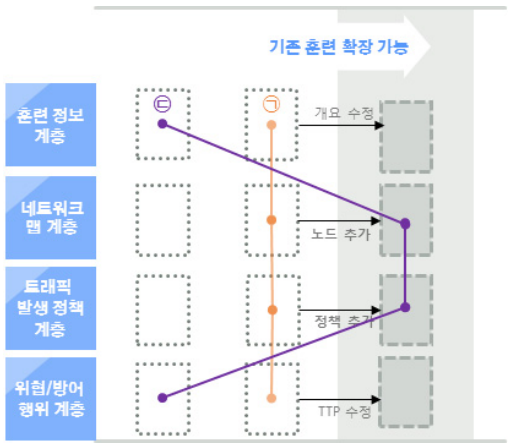
(그림 7) 훈련 시나리오 저작 방법 I
(Figure 7) Training scenario authoring method I

그림 7의 훈련 ㉠은 훈련 시나리오의 일반적인 저작 형태를 표현한 것이다. 훈련 시나리오 저작 과정에서 훈련 정보 계층, 네트워크 맵 계층, 트래픽 발생 정책 계층, 위협/방어 행위 계층을 순차적으로 저작해 나간다.



(그림 8) 훈련 시나리오 저작 방법 II
(Figure 8) Training scenario authoring method II

그림 8의 훈련 ㉡은 훈련 ㉠과 유사하지만, 훈련 ㉡에서 사용할 훈련 정보 계층, 네트워크 맵 계층, 트래픽 발생 정책 계층을 저작한 후, 앞서 훈련 ㉠에서 저작된 위협/방어 행위 정보를 재사용하는 형태이다. 기 저작된 계층 정보를 재사용하는 저작 방법에 대한 현실적인 예로서, 훈련 ㉠이 인터넷망에서의 APT(Advanced Persistent Threat) 대응 훈련이고 훈련 ㉡ 은 국방망에서의 APT 대응 훈련이라고 할 때 훈련 ㉡ 저작 과정에서 훈련 정보 및 네트워크 맵 정보와 트래픽 발생 정책 정보는 새로 저작해야하지만 훈련 ㉠의 위협/방어 행위 정보를 재사용함으로써 훈련 시나리오의 저작 편의성을 증대시킬 수 있다.



(그림 9) 훈련 시나리오 저작 방법 III
(Figure 9) Training scenario authoring method III

그림 9는 기 저작된 계층 정보를 수정해 타 훈련 시나리오에서 사용하는 형태를 나타낸 것이다. 앞선 예시를 이어 설명하면, 인터넷망에서의 APT 대응 훈련인 훈련 ㉠에서 사용한 네트워크 맵 정보에 노드를 추가해 더욱 복잡한 훈련 환경을 조성하고, 이에 따라 필요한 트래픽 발생 정책을 추가해 더욱 높은 수준의 훈련에 사용할 수 있을 것이다. 훈련 ㉢은 이러한 저작 방법을 채택한 것으로, 훈련 ㉠에서 확장된 훈련 환경 정보를 사용해 인터넷망에서의 새로운 훈련을 설계하는 상황을 표현한 것이다. 훈련 ㉢ 저작 과정에서 기 저작된 네트워크 맵 정보와 트래픽 발생 정책 정보를 수정해 사용하고, 훈련 목적에 맞는 새로운 위협/방어 행위를 저작해 훈련 시나리오를 완성시키는 모습을 확인할 수 있다. 이처럼 계층 정보의 자유로운 수정과 조합을 통해 다양한 훈련 시나리오

를 편리하게 저작해낼 수 있다.

4.3 저작 인터페이스

훈련 시나리오는 3장에서 살펴본 훈련 시나리오 구성 요소 저작 예와 같이 GUI를 기반으로 저작하거나 스크립트(script)를 기반으로 저작할 수 있다. GUI 기반의 저작 형태는 사용자 친화성의 관점에서 강점을 가지며, 스크립트 기반의 저작 형태는 시나리오 계층 정보를 수정하는 등의 세부적인 작업을 정교하게 수행할 수 있도록 한다.

훈련 시나리오는 최초 GUI를 기반으로 저작되어 데이터베이스(database)에 저장되며, 저장된 객체를 스크립트로 변환해 필요한 작업을 수행할 수 있다[10]. 그림 10은 이러한 스크립트 기반 저작의 예로, 사용자가 직관적으로 작성 또는 수정할 수 있는 XML(Extensible Markup Language) 문법을 사용했다. 또한 내용의 확인과 저작의 용이성을 위해 XML 엘리먼트(element)를 한글로 구성할 수 있도록 했다.

```
<?xml version="1.0"?>
    <function name="네트워크맵">
        <사용자>add_test</사용자>
        <식별자>add01</식별자>
        <네트워크맵명>국방망침투시나리오맵</네트워크맵명>
        <네트워크맵설명>국방망침투시나리오맵</네트워크맵설명>
        <리소스목록>
            <리소스 name="window7_1" 종류="윈도우" X좌표="100" Y좌표="100">
                <리소스명>공격서버</리소스명>
                <아이피>203.31.49.10</리소스아이피>
                <서브넷>24</서브넷>
                <DNS>8.8.8.8</DNS>
                <DOMAIN>N/A</DOMAIN>
            </리소스>
            <리소스 name="mailserver_1" 종류="메일서버" X좌표="100" Y좌표="100">
                <리소스명>메일서버</리소스명>
                <아이피>211.236.124.42</아이피>
                <서브넷>26</서브넷>
                <DNS>8.8.8.8</DNS>
                <DOMAIN>army.mil.kr</DOMAIN>
            </리소스>
        </리소스목록>
    </function>
```

(그림 10) 스크립트 기반 저작 예
(Figure 10) Script-based authoring example

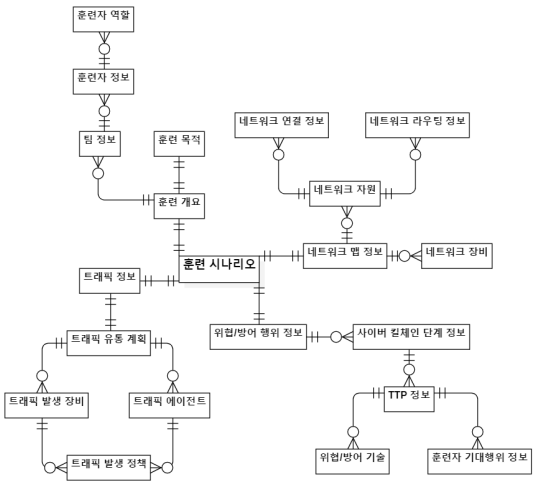
4.4 데이터베이스 설계

본고에서 제시하는 훈련 시나리오 저작 방법을 구현하기 위해서는 각 계층 정보의 통합적 관리가 요구된다. 이를 위한 설계 과정에서 표 1과 같이 데이터베이스에 포함되어야 할 테이블(table)들을 식별하였다.

(표 1) 테이블 목록
(Table 1) Table list

테이블 명	내 용
훈련 시나리오	훈련 정보, 네트워크 맵, 트래픽 발생 정책, 위협/방어 행위 계층의 조합으로 구성되는 훈련 시나리오
훈련 개요	훈련 정보 계층에서 저작되는 훈련의 개요
훈련 목적	훈련의 목적
팀 정보	훈련 수행에 필요한 팀 정보
훈련자 정보	팀 구성을 위한 훈련자 할당 계획 정보
훈련자 역할	훈련자의 역할 및 이에 대한 자원/권한 정보
네트워크 맵 정보	네트워크 맵 계층에서 저작되는 네트워크 맵 정보
네트워크 자원	네트워크 맵을 구성하는 가상머신 정보
네트워크 연결 정보	네트워크 자원 간 링크 정보
네트워크 라우팅 정보	네트워크 맵 내부의 라우팅 정보
네트워크 장비	네트워크 맵에 포함시킬 수 있는 장비 정보
트래픽 정보	트래픽 발생 정책 계층에서 저작되는 트래픽 정보
트래픽 유통 계획	발생된 트래픽을 훈련 환경에 공급하기 위한 계획
트래픽 발생 장비	가용한 트래픽 발생 장치
트래픽 에이전트	가용한 트래픽 에이전트
트래픽 발생 정책	트래픽 발생 장치 또는 트래픽 에이전트에서 트래픽을 발생시키기 위한 정책
위협/방어 행위 정보	위협/방어 행위 계층에서 저작되는 위협/방어 행위 정보
사이버 킬체인 단계 정보	훈련을 구성하는 사이버 킬체인 단계 정보
TTP 정보	사이버 킬체인 단계에 매핑되는 전술 및 기법 정보
위협/방어 기술	TTP에서 사용할 수 있는 위협/방어 기술
훈련자 기대행위 정보	TTP에서 훈련자에게 기대되는 행위 정보

식별된 테이블을 바탕으로 데이터베이스의 개념적 스키마를 생성해 그림 11의 ERD(Entity Relationship Diagram)로 표현했다. 그림 11에서 훈련 시나리오를 구성하는 네 계층과, 각 계층을 이루는 테이블 간의 관계를 확인할 수 있다.



(그림 11) 훈련 시나리오 ERD
(Figure 11) Training scenario ERD

5. 결 론

본 논문에서는 사이버전 훈련 시나리오 구성을 위한 계층으로서 식별된 훈련 정보, 네트워크 맵, 트래픽 발생 정책, 위협/방어 행위를 소개하고 각 항목의 저작 방안을 제안했다. 그리고 이들의 조합을 통해 훈련 시나리오를 계층적으로 저작해나가는 방법을 제시했다.

계층적 훈련 시나리오 저작 방법의 장점은 기 저작된 계층들의 재사용을 통한 저작 편의성 증대와, 계층 간 다양한 조합을 바탕으로 하는 훈련 시나리오의 확장 가능성이다. 이러한 방법이 훈련 시스템에 접목되어 군의 사이버전 역량 제고를 위한 재료로 사용될 수 있기를 기대한다.

추가 연구 사항으로서, 각 계층이 자유롭게 수정 및 조합되었을 때 계층 간 결합을 통해 생성되는 훈련 시나리오의 실행 가능성을 자동적으로 확보할 수 있는 기술을 갖춘다면 저작 편의성이 더욱 개선될 것이다. 또한 모의전투 시나리오 저작을 지원하는 훌륭한 훈련 시스템을 보유하게 되더라도, 이에 대한 콘텐츠를 저작하는 것은 훈련 시스템 운용자의 몫이다. 효과적인 훈련을 위해서 사이버전 교리 및 TTP의 정립을 위한 군 차원의 노력이 함께 이루어져야 할 것이다.

참고문헌(Reference)

[1] Uihyeon Song, Wansoo Cho, Changwon Lee, Myung Kil Ahn, “Cyber Warfare Training Scenario Authoring Method Using Integrated DB”, Proceedings of 2019 Korea Institute of Military Science and Technology Academic Conference, pp.1322-1323, 2019.

[2] Jonghee Chun, “A Result Report on Scenario Building for Cyberwarfare Training”, Agency for Defense Development, ADDR-412-190795, 2019.

[3] Wansoo Cho, “Analysis of Cyber Warfare Training Tools”, Agency for Defense Development, ADDR-412-160879, 2016.

[4] Myung Kil Ahn, Yong Hyun Kim, “Research on System Architecture and Simulation Environment for Cyber Warrior Training”, Journal of The Korea Institute of Information Security&Cryptology, pp.533-540, 2016.
https://doi.org/10.13089/JKIISC.2016.26.2.533

[5] Myung Kil Ahn, Donghwan Lee, Haeng Rok Oh, Wansoo Cho, Yong Hyun Kim, “Research on M&S System Architecture and Technology for Effect Analysis and Training/Test based Cyber warfare”, Proceedings of 2015 Korea Institute of Military Science and Technology Academic Conference, pp.1230-1231, 2015.

[6] Wansoo Cho, “Analysis of Cyber Range and Testbed”, Agency for Defense Development, ADDR-114-152051, 2015.

[7] Myung Kil Ahn, Donghwa Kim, Yong Hyun Kim, “Research on Multi-Level Scenario Authoring Method for Threat in Cyber Training Environment”, Proceedings of 2018 Korea Institute of Military Science and Technology Academic Conference, pp.835-836, 2018.

[8] Agency for Defense Development, “Software Requirement Specification for Advanced Cyberwar Trainer”, Agency for Defense Development, 2019.

[9] Agency for Defense Development, “Operational Concept Description for Advanced Cyberwar Trainer”, Agency for Defense Development, 2019.

[10] Agency for Defense Development, “Software Design Description for Advanced Cyberwar Trainer”, Agency for Defense Development, 2019.

◐ 저 자 소 개 ◑

송 의 현(Uihyeon Song)
2018년 고려대학교 사이버국방학과(공학사)
2018~현재 국방과학연구소 현역파견원 육군 중위
관심분야 : 사이버전, 정보보호
E-mail : uhs0317@add.re.kr

김 동 화(Donghwa Kim)
2004년 고려대학교 전기전자전파공학과(공학사)
2007년 고려대학교 대학원 전기공학과(공학석사)
2007년~현재 국방과학연구소 선임연구원
관심분야 : 정보보호, 사이버 훈련
E-mail : donghwa78@gmail.com

안 명 길(Myung Kil Ahn)
1997년 충남대학교 정보통신공학과(공학사)
2003년 서강대학교 대학원 컴퓨터공학과(공학석사)
2017년 중앙대학교 대학원 전자공학과 박사 수료
1997년~2006년 LG전자 정보통신 연구소
2006년~현재 국방과학연구소 책임연구원
관심분야 : 정보보호, 사이버전M&S, 사이버 시뮬라전, 효과분석, 훈련체계
E-mail : happyahn@add.re.kr