정 보 보 호 학 회 지
제 33 권 제6호, 2023. 12

차세대 IT·OT 융복합 사이버훈련장 구축 연구

최 영 한*, 남 택 준*, 전 동 호*, 양 현 철*, 조 수 현*, 강 정 민*

요 약

사이버위협의 증가로 사이버보안 역량을 강화할 수 있는 사이버훈련에 대한 요구가 점점 증가하고 있다. 사이버훈련이란 개인의 사이버보안 역량 강화 및 사이버공격에 대한 조직적 대응을 단련하는 일련의 행위를 가리킨다. 최근 IT 영역에서 실생활과 밀접한 관계가 있는 OT 영역으로 사이버공격 범위가 늘어나 그 피해는 증가하고 있다. 이로 인해 이들 사이버공격에 대비한 사이버훈련이 필요하며, IT 위주에서 OT를 포함한 사이버훈련으로 확장할 필요가 있다. 본고에서는 IT와 함께 OT 영역까지 사이버훈련을 수행할 수 있는 사이버훈련장 구축 연구를 소개한다. 본고에서는 OT 영역을 11개의 국가기반시설로 분류하였고, OT 사이버환경을 SW 기반으로 구축할 수 있는 방안을 제안한다. 제안된 사이버훈련장을 통해 IT와 OT 대상 사이버공격에 대한 사이버훈련을 수행할 수 있으며 사이버보안 역량을 강화할 수 있다.

Ⅰ. 서 론

최근 국가 내 주요 시설을 대상으로 하는 사이버공격은 실생활과 밀접한 관계가 있어 큰 피해를 준다. 특히 러시아-우크라이나 전쟁에서 볼 수 있듯이 국가의 주요 시설에 대한 사이버공격은 국가적 혼란을 야기시켰다[1]. IT(Information Technology)에 이어 주요 시설인 OT(Operational Technology) 영역까지 사이버공격의 범위가 넓어지고 있다. OT는 물리시스템을 제어하기 위한 소프트웨어와 하드웨어를 지칭하며, 산업, 에너지, 빌딩 등 사회 전반적으로 일반 사람들과 함께 밀접하게 사용되고 있다[2]. 콜로니얼 파이프라인 사건에서 보듯이 OT에 대한 사이버공격이 성공한 경우 그 피해는 매우 크다[3].

이로 인해 IT 영역과 함께 OT 영역을 포함한 사이버훈련이 전세계적으로 수행되고 있다[4,5]. 이들 사이버훈련들은 OT 모사 환경을 대상으로 하고 있어 실제 환경에서 수행한 것과 같은 효과를 가지며, 이를 통해 사이버보안 역량을 강화하고 있다. Cyber Storm은 CISA에서 분류한 16개의 섹터 내 OT 시설들을 대상으로 사이버훈련을 수행하고 있다[6].

현재 우리나라는 IT 위주의 사이버훈련이 많이 수행되고 있어 OT 대상 사이버훈련으로 확장이 필요한 상황이다. OT 대상 사이버훈련의 경우, 가장 적절한 방향은 실제 운영되는 시스템이나 테스트베드에서 수행하는 것이지만 구축·유지 비용 및 확장성에 한계가 있다. 이를 극복하기 위해 OT 환경을 모사한 시스템에서 사이버훈련을 수행하고 있다.

본고에서는 IT와 OT 영역을 대상으로 사이버훈련을 수행할 수 있는 사이버훈련장 구축 연구를 기술한다. 우선 OT와 관련된 국내법 및 외국의 사례를 분석하여 국가기반시설을 11개 섹터로 분류하였다. 2023 사이버공격방어대회(Cyber Conflict Exercise, CCE)에서는 11개 섹터 내 15개 시설을 대상으로 사이버공격에 대한 방어를 수행하는 사이버훈련을 수행하였다[7]. 다음으로 OT 환경을 SW 기반으로 모사하기 위한 방법을 제시하였다. 현재 11개 섹터 중 7개 섹터에 대해서 연구 중에 있으며, 전 섹터로 확장할 예정이다. SW 기반이기 때문에 가상머신에 구축 가능하며, 수정·확장·유지가 용이하다.

본고의 구성은 2장에서 사이버훈련 동향을 소개하고, 3장에서 사이버훈련과 사이버훈련장에 대해 설명한다. 4장에서 IT·OT 사이버훈련장 전체 구조를 제안하고, 5장에서 국가기반시설 분류 및 SW 기반 사이버훈련 환경을 구축하는 방법을 기술한다. 6장에서는 결론을 맺는다.

* 사이버안전훈련센터 (실장, yhch@nsr.re.kr, 책임연구원, tjnam@nsr.re,kr, 선임연구원, plutonic@nsr.re.kr, 선임연구원, hcyang06@nsr.re.kr, 선임연구원, soohyunjo@nsr.re.kr, 센터장, jmkang@nsr.re.kr)

Ⅱ. 사이버훈련 동향

본 장에서는 대표적인 OT 대상 사이버훈련인 미국 CISA(Cybersecurity and Infrastructure Security Agency)의 Cyber Storm과 NATO CCDCOE (Cooperative Cyber Defense Centre of Excellence)의 Locked Shields에 대해 알아본다.

2.1. Cyber Storm(사이버 스톰)

Cyber Storm은 CISA에서 2006년부터 2년마다 미국 내 주요 기반 시설을 대상으로 수행되는 사이버훈련이다[4]. 정부와 민간 조직의 사이버 사고에 대한 대응, 주요 인프라 보호, 사이버 위협 완화 및 효율적 복구 능력을 향상 시키는 것을 목표로 하고 있다. 2022년 2,000여명의 참가들이 IT와 CISA에서 분류한 16개 주요 기반 시설(Critical Infrastructure Sector) 중 10개 섹터에 대해 사이버훈련을 수행하였다.

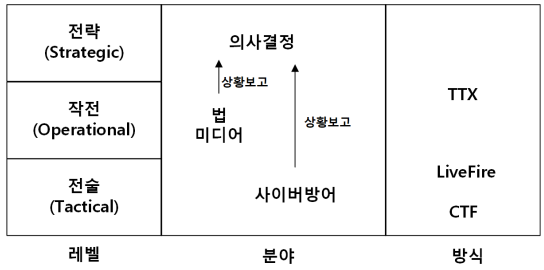
2.2. Locked Shields(락드쉴즈)

Locked Shields(LS)는 NATO CCDCOE 에서 개최하는 사이버 방어 훈련이다[5]. LS는 2010년에 처음 개최가 되었으며 NATO에 속한 국가들을 대상으로 매년 열리고 있다. 우리나라는 2021년 방어팀(Blue Team)으로 처음 참가 하였다[8]. 2021년에는 22개의 방어팀이 참가 하였으며, 4,000개의 사이버공격이 5,000여개의 가상머신을 대상으로 이루어졌다. 가상머신에 IT 및 OT 대상 사이버훈련 환경이 구축되어 있다.

Ⅲ. 사이버훈련과 사이버훈련장

3.1. 사이버훈련

사이버훈련이란 사이버위협에 대한 방어를 반복적으로 수행하여 사이버보안 역량을 강화시키는 일련의 행위를 가르킨다. 사이버훈련으로 해석될 수 있는 영어의 단어는 Training과 Exercise이다. Training은 개인의 사이버보안 능력을 향상시키기 위해 교육을 받거나 실습을 하는 훈련이라고 한다면, Exercise는 두 명 이상이 체계를 이루어 조직적인 대응을 하는 훈련으로 볼 수 있다. 본고에서는 IT 및 OT 환경에 대한 사이버공격을 조직적으로 방어하는 사이버훈련에 초점을 맞추고 있으며, Exercise을 가리킨다.



〔그림 1〕 사이버훈련의 레벨, 방식, 분야

사이버훈련은 사이버전에서 사이버공격에 대해 방어를 한다는 점에서 3가지 단계인 전략(Strategic Level), 작전(Operational Level), 전술(Tactical Level)로 나누어 볼 수 있다[9]. 전략은 사이버전에서 승리하기 위해 국가차원에서 자원을 투입하는 단계라고 하면, 작전 단계는 일련의 전투를 묶은 개념으로 사회 차원에서 혼란을 일으키는데 목적이 있다. 전술은 실제 사이버전이 일어나는 단계로 사이버훈련에서 기술적인 요소를 많이 고려해야 하는 단계이다.

전술은 사이버공격에 대한 방어가 수행되는 단계로 기술적 요소가 많이 들어간다. 사이버훈련생에게는 방어에 대해 기술적으로 대처할 수 있는 사이버훈련 능력이 요구된다. 사이버훈련 방식으로 실시간으로 발생하는 사이버공격에 대해 방어를 수행하는 실시간(LiveFire) 방식과 사고조사와 포렌식을 수행하는 CTF(Capture the Flag) 방식이 있다. 실시간 방식 모델 중 대표적으로 Cyber Defense eXercise (CDX)가 있다[10]. CDX에서는 사이버훈련 역할별로 팀을 색으로 표현한다. 그린팀(Green Team)은 IT와 OT 사이버훈련 환경을 구축하고, 훈련 시나리오를 개발한다. 블루팀(Blue Team)은 그린팀이 구축한 사이버환경을 방어하고, 레드팀(Red Team)은 블루팀을 공격한다. 기술적인 요소 못지않게 상황보고는 전략·작전·전술 단계를 수행하기 위한 중요한 요소이다. 전략 단계에서 기술적으로 대처한 내용들이 상부로 보고되어야지 정확한 의사결정을 할 수 있다. 따라서 전술 단계에서는 기술적 대처와 상황보고를 할 수 있는 사이버훈련 콘텐츠가 개발되어야 한다.

작전 및 전략은 전술의 상위 단계로 비기술적인 요소로 사이버공격에 대한 대처를 하는 단계라 할 수 있다. 대표적으로 법과 미디어 분야가 있다. 법 분야는 사이버공격에 대해 국내·국제법을 근거로 하여 법률적

으로 대응한다. 미디어 분야는 SNS 등을 이용하여 사회를 불안하게 하는 심리전에 대한 대응이다. 해당 단계를 수행하는 방식으로 도상훈련(Table Top eXercise, TTX)이 많이 활용된다. 도상훈련은 실제 발생할 가능성이 있는 사이버위협 상황을 설정하면 이를 토론식으로 해결한다[11]. 해당 단계 역시 상부에서 의사결정을 하기 위해 수행한 사이버훈련에 대한 결과를 정리하여 보고하는 사이버훈련이 요구된다.

전략·작전·전술 단계의 사이버훈련은 각 단계에서의 적절한 대처와 의사결정을 위한 상황보고가 유기적으로 운영되어야 한다. 사이버훈련(Exercise)은 조직적인 대응으로 전략·작전·전술 단계에서 각자 맡은 역할을 충실히 수행함으로 사이버전에서 승리할 수 있다.

3.2. 사이버훈련장

사이버훈련장(Cyber Range)은 사이버훈련을 관리·수행·평가를 할 수 있는 플랫폼이다[12]. 실시간, CTF, TTX 등의 방식을 지원한다. 실시간 방식의 사이버훈련 콘텐츠는 사이버훈련 환경을 구축한 후 사이버공격이 이루어지고 이를 방어하는 사이버훈련 시나리오로 구성된다[10]. CTF 방식의 사이버훈련 콘텐츠는 예방 단계인 웹 해킹, 포너블 등이 있으며, 탐지·분석·대응 단계인 리버싱, 포렌식, 암호 등이 있다[13]. TTX의 사이버훈련 콘텐츠는 사이버공격에 대한 실제 상황을 가정하여 시나리오가 개발되어 운영된다[14]. 각각의 사이버훈련 방식은 장단점이 있기 때문에 목적에 맞추어 방식을 선택하면 된다[14].

국내 사이버훈련장은 한국인터넷진흥원(KISA), 사이버작전사령부, 사이버안전훈련센터에서 대표적으로 운영하고 있다[15]. KISA의 시큐리티짐은 사이버 공격 및 방어가 가능한 실전형 사이버훈련장이다. 사이버작전사령부의 사이버훈련장은 방어시 탐지·대응·분석·예방의 순환적 과정을 종합적으로 수행할 수 있다. 사이버안전훈련센터의 사이버훈련장은 관심·주의·경계·심각의 사이버위기 경보를 기반으로 사이버 방어 훈련을 수행할 수 있다[16].

대규모의 사이버훈련생 지원 및 사이버훈련 콘텐츠의 설치 및 운영의 유연성을 위해 사이버훈련장은 클라우드 기술을 활용한다. 프라이빗이나 퍼블릭 클라우드 내에 구축된 가상머신을 자동으로 생성·배포·설정하며 사이버훈련 콘텐츠를 운영한다. 사이버훈련장의 규모가 커지면 커질수록 그린팀의 역할이 점점 중요해진다. 그린팀에서 클라우드 기반 사이버훈련장 내 사이버훈련을 자동으로 구축하는 기술이 사이버훈련장의 핵심이라 할 수 있다.

Ⅳ. 차세대 IT·OT 융복합 사이버훈련장

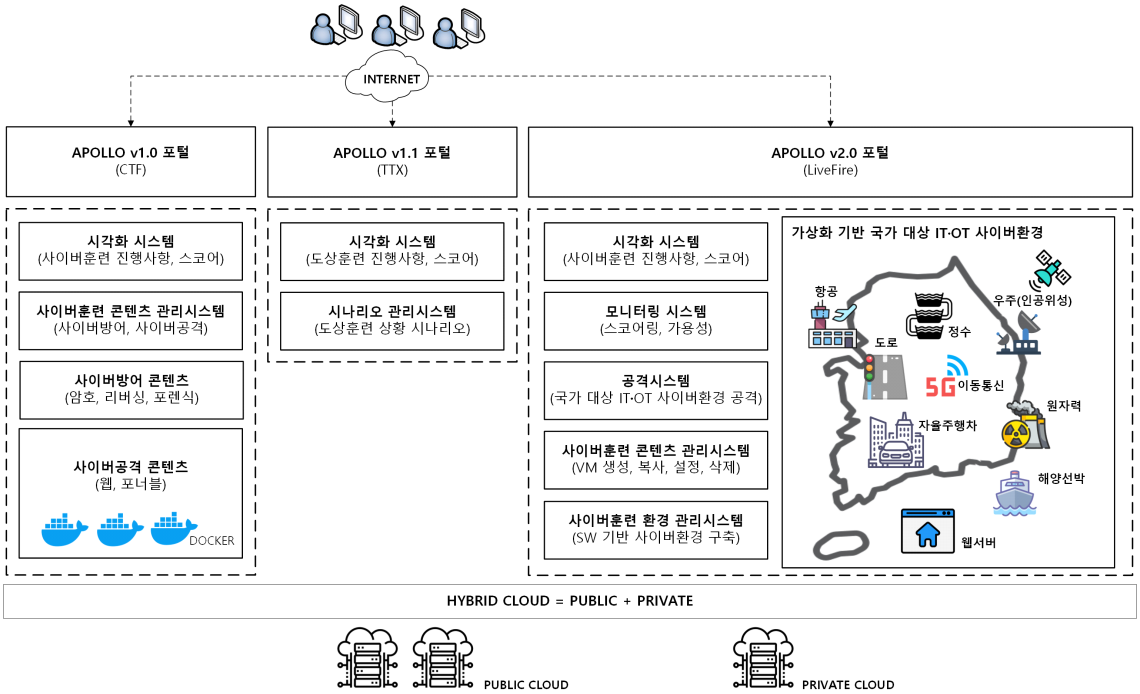
본 장에서는 IT 및 OT 대상 사이버훈련을 수행할 수 있는 차세대 IT·OT 융복합 사이버훈련장을 제안한다. 사이버안전훈련센터에서는 현재 CTF와 TTX를 지원하는 사이버훈련장(온라인 사이버보안 훈련장, APOLLO)을 개발하였으며, 이를 확장하여 OT 사이버훈련을 할 수 있는 사이버훈련장으로 연구 중이다.

- APOLLO v1.0: CTF 방식을 지원하며, 사이버공격방어대회(CCE) 예선·본선 출제 문제를 포함하여 다양한 문제를 보유하고 있다[그림 2]. 2021년부터 CCE 예선 개최 전에 모의체험으로 대국민 사이버훈련을 수행하고 있다.
- APOLLO v1.1: 도상훈련 기능을 제공한다.
- APOLLO v2.0: IT·OT 융복합 사이버훈련장으로 클라우드 상에서 다량의 가상머신을 생성·복사·설정·삭제가 가능하고 SW 기반으로 OT 사이버환경이 구축된다.

IT·OT 융복합 사이버훈련장은 크게 세 부분으로 나누어진다[그림 3].

- 포털: 사이버훈련장 UI
- 사이버훈련장 관리 부분: 사이버훈련을 준비·운영·

〔그림 2〕 APOLLO v1.0 로그인 화면



〔그림 3〕 IT·OT 융복합 사이버훈련장 전체 구조

평가 한다. 사이버훈련 환경 관리시스템, 사이버훈련 콘텐츠 관리시스템, 공격시스템, 모니터링 시스템, 시각화 시스템으로 구성된다.

- IT·OT 사이버훈련 환경 부분: 가상머신 상에서 SW 기반으로 구축된다.

포털은 사이버훈련생이 사이버훈련을 수행할 때 접하는 UI이다. 웹으로 구현되며 CTF 혹은 실시간 방식으로 임무가 할당되면 사이버훈련생은 사이버훈련을 수행한다. 사이버훈련 중에는 진행 상황 및 결과를 확인할 수 있다.

사이버훈련은 준비·운영·평가의 과정이 순환적으로 반복된다. 대규모의 사이버훈련생 지원 및 운영의 효율성을 높이기 위해서는 여러 시스템이 요구된다.

- 사이버훈련 환경 관리시스템: 가상머신 상에 네트워크를 구성하고 구축된 IT·OT 사이버훈련 환경을 관리한다.
- 사이버훈련 콘텐츠 관리시스템: IT·OT 사이버훈련 환경 내에 사이버위협을 삽입한 후 다수의 사이버훈련생을 위해 해당 사이버훈련 환경을 생성·복사·설정·삭제한다.
- 공격시스템: 사이버훈련 콘텐츠에 따라 사이버훈련생이 방어하는 IT·OT 사이버훈련 환경을 공격한다. 사이버훈련생별 공격 결과를 모니터링 시스템에 전송한다.
- 모니터링 시스템: 사이버훈련 진행사항을 모니터링한다. 주어진 임무의 완료 정도에 따라 스코어링을 하고 사이버훈련 환경 내에 시스템이 정상적으로 동작하는지 가용성 점검도 수행한다. 공격시스템에서 공격 결과를 받아 모니터링한 데이터와 병합한다.
- 시각화 시스템: 사이버훈련생 및 운영자가 사이버훈련의 전체 진행 상황을 파악하기 위해 모니터링한 데이터를 가공한 정보를 보여준다.

Ⅴ. IT·OT 사이버훈련 환경 구축

본 장에서는 SW 기반 IT·OT 사이버훈련 환경을 구축하는 방안을 제안한다. 이를 위해 우선 OT 환경을 11개의 국가기반시설로 분류하였고, 이들 시설에 대해 SW 기반으로 가상머신에 구축하는 방안을 기술한다.

5.1. 국가기반시설 분류

5.1.1. OT 분류

OT에 대한 분류는 국가별 및 국가 내에서 기관별로 다양하다. 이는 각각 기관에서의 OT에 대한 시각이 다르기 때문이다. 미국의 경우 CISA는 국가 주요 시설에 대해 16개의 섹터(Chemical, Commercial Facilities, Communications, Critical Manufacturing 등)로 나누었다. Cyber Storm은 이들 섹터에 대해 수행하는 사이버훈련이다[6].

국내는 OT와 관련된 주요 시설을 여러 법률에서 정의하고 있다. 재난안전법에서는 국가핵심기반으로, 정보통신기반보호법은 주요정보통신기반시설로, 통합방위법에는 국가중요시설로 정의되어 있다.

재난안전법 제3조 12호에서는 국가핵심기반을 에너지, 정보통신, 교통수송, 보건의료 등 국가경제, 국민의 안전·건강 및 정부의 핵심기능에 중대한 영향을 미칠 수 있는 시설, 정보기술시스템 및 자산 등으로 정의하고 있다[17]. 이를 근거로 행정안전부에서 11개 분야인 에너지, 정보통신, 교통수송, 금융, 보건의료, 원자력, 환경, 식용수, 정보중요시설, 공동구, 문화재로 분류하였다[18].

정보통신기반보호법 제7조에 주요정보통신기반시설을 정의하고 있다.[19]. 해당 법률에서는 주요 교통시설(도로·철도·지하철·공항·항만 등), 에너지·수자원 시설(전력, 가스, 석유 등), 방송중계·국가지도통신망 시설, 정부출연연구기관의 연구시설(원자력·국방과학·첨단방위산업 관련)이다.

통합방위법 제2조에 국가중요시설은 공공기관, 공항·항만, 주요 산업시설 등 적에 의하여 점령 또는 파괴되거나 기능이 마비될 경우 국가안보와 국민생활에 심각한 영향을 주게 되는 시설로 정의하고 있다[20].

5.1.2. OT 사이버훈련을 위한 국가기반시설 분류

사이버공격방어대회(Cyber Conflict Exercise, CCE)에서는 1회(2017년)부터 OT 관련 사이버훈련 콘텐츠를 개발 하였으며[표 1], 7회(2023년)에는 OT를 국가기반시설 11개 섹터로 분류하여 사이버훈련 콘텐츠를 개발하여 활용하였다[7].

CCE 2023은 CISA 16개 섹터, 국내 법률 및 신기술분야를 분석하여 우리나라 국가기반시설을 11개 섹터로 분류하였다. 11개의 섹터는 통신, 수력, 정부·공공기관, 금융, 에너지, 의료·보건, 교통, 원자력시설, 우주, 항만, 방송이다. CCE 본선에서는 11개 섹터에 속하는 15개 시설을 선택하여 사이버공격에 대한 방어훈련을 수행하였다. 특히 우주 분야를 대상으로 인공위성 5가지 취약점에 대한 실시간 사이버훈련 콘텐츠를 개발하였다.

[그림 4]는 CCE 2023 본선 시 국가기반시설 11개 섹터 15개 시설에 대한 사이버공격을 실시간으로 방어하는 진행사항을 보여주는 상황판이다. 우리나라 전역에 위치하는 국가기반시설에 대한 사이버공격이 이루

〔그림 4〕 2023 사이버공격방어대회 시 국가주요시설 11개 섹터 15개 시설에 대한 사이버공격에 대한 방어 상황판

〔표 1〕 사이버공격방어대회 역대 특징

연도	특징
2017년	기반시설 모사시스템 개발 및 적용
2018년	상황보고 및 미디어대응 게임요소 도입
2019년	방어목표시스템의 가용성 확보
2020년	사이버펜데믹 시대 사이버 회복력
2021년	사이버회복력을 위한 사이버 집단면역 형성
2022년	디지털 플랫폼 시대의 사이버안보
2023년	국민안전을 위한 사이버안보

어지고, 방어 상태에 따라 사이버위기 경보단계가 발령된다. 사이버공격은 국가기반시설에 떨어지는 미사일로 표현하였고, 방어정도에 따라 빨간색에서 연두색으로 점차 변하도록 시각화하였다. 본선 시작시에는 모든 시설이 공격을 받고 있기 때문에 심각 단계이지만 참가자들이 문제를 풀면서 방어를 하게 되면 경계, 주의, 관심 단계로 낮아진다.

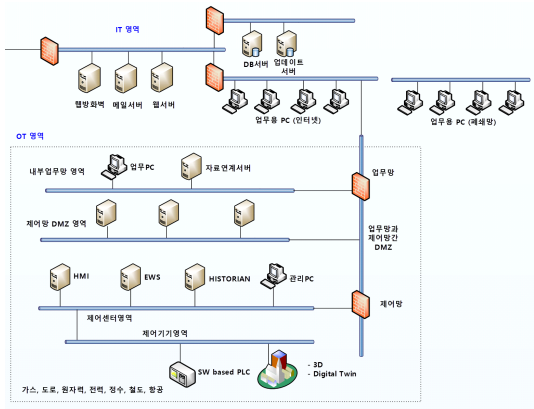
사이버훈련 분야는 사이버공격과 사이버방어 분야로 나누었다. 사이버공격 분야는 웹 공격, 시스템 공격이다. 사이버방어 분야는 암호 분석, 악성코드 분석, 사고조사이다.

방어 관련 측정 지표는 사이버회복력을 사용하였으며, MITRE에서 제시한 메트릭(Cyber Resilience Engineering Framework)을 활용하였다[21]. 사이버회복력 평가 항목으로 예측(anticipate)·지속(resist)·회복(recover)·진화(evolve)를 사용하였다. 사이버훈련 분야에서 예측은 전 분야와 관련이 있으며, 지속은 웹 공격과 시스템 공격, 회복은 암호 분석과 악성코드 분석, 진화는 사고조사와 관련 있다.

5.2. SW 기반 IT·OT 사이버훈련 환경 구축

국가기반시설 11개 섹터 내 시설을 구축하기 위해선 실제 물리시스템이 있어야 하지만 현실적으로 과도한 비용 및 확장성의 한계로 사이버훈련의 경우 가상머신 상에 SW 기반으로 구축한다[5].

정부·공공기관 섹터 내의 IT와 OT 영역으로 구성된 사이버훈련 환경을 고려하면 [그림 5]와 같이 구성할 수 있다. IT 영역인 경우 인터넷이 연결된 업무영역과 폐쇄된 업무영역이 구축 되어야 한다. DMZ에는 메일서버, 웹서버 등이 운영되어야 하며, 해당 시스템의 경우는 오픈소스로 충분히 구축 가능하다. 업무망이 OT 영역과 연결이 된다면 PLC, HMI, EWS 등 물리시스



〔그림 5〕 정부·공공기관 대상 IT·OT 네트워크 구성 예

템 관련 시스템이 구축되어 있어야 한다[22].

본고에서는 OT 사이버훈련 환경을 SW 기반으로 구축할 수 있는 연구를 소개한다[표2]. IT·OT 융복합 사이버훈련장은 11개 섹터 중 7개 섹터를 대상으로 연구하고 있으며, 4개 섹터(정부·공공기관, 금융, 의료·보건, 방송)는 추후 확장할 계획이다.

오픈소스인 에뮬레이터 혹은 시뮬레이터를 활용하는 방법이 있다. 해당 시스템의 경우는 각 분야의 전문가들이 SW로 개발하였기 때문에 상당 부분 실환경이 모사되어 있다고 할 수 있다. 사이버훈련의 경우 사이버위협에 대한 대처가 주요 목표이기 때문에 해당 OT 분야에 기 개발된 오픈소스를 충분히 활용하면 사이버훈련장 구축시 효율성을 높일 수 있다. 본고에서는 통신과 우주 섹터에 해당 방법을 적용하였다.

5G는 단말, 무선망, 코어망, 인터넷망으로 구성된다[23]. 5G망의 핵심인 무선망과 코어망의 경우 이들을 모사한 오픈소스인 UERANSIM과 Open5GS를 활용하면 5G망을 SW 기반으로 구축할 수 있다[24,25]. 인

〔표 2〕 11개 섹터 중 7개 시설

섹터	시설	구축방안
통신	5G	오픈소스
우주	인공위성	오픈소스
수력	정수	SW PLC
에너지	전력, 가스	SW PLC
교통	도로, 철도, 항공	SW PLC
	자동차	수집한 실데이터
원자력시설	원자력발전	SW PLC
항만	해양선박	HILS

공위성은 다양한 오픈소스 SW가 있으나 NASA와 관련된 NOS3(NASA Operational Simulation for Small Satellite)를 이용하면 인공위성을 활용한 네트워크를 구성할 수 있다[26].

SW 기반으로 PLC를 개발하는 방안이다. OT 대상으로 사이버환경을 구축할 때 어려운 점은 하드웨어와 관련 있는 PLC와 물리시스템 때문이다. 물리시스템은 단순히 PLC에서 받은 입력에 대해 반응을 하는 부분으로 응답 값만 적절히 출력할 수 있다면 SW 기반 PLC로 OT 사이버훈련 환경을 충분히 가상머신 상에 구축될 수 있다. PLC를 모사하는 방법으로 3가지 방향으로 접근할 수 있다. PLC를 개발하는 방법으로 OpenPLC가 사용될 수 있다[27]. 본고에서는 수력, 에너지, 교통, 원자력 시설 섹터에 적용하였다.

다음으로 PLC가 동작하는 실제 네트워크에서 패킷을 수집하여 재생하여 PLC 동작을 모사하는 방법을 적용할 수 있다. 본고에서는 교통 섹터 중 자동차에 적용하였다.

하드웨어를 모사한 HILS (Hardware In the Loop Simulation) 방법이 있다. PLC를 시뮬레이션하여 HMI에서 수신한 데이터를 처리한다. 본고에서는 항만 섹터에 적용하였다.

Ⅵ. 결 론

OT 영역에 대한 사이버공격 피해 증가로 인해 사이버훈련의 필요성이 점점 증가하고 있다. 본고에서는 IT와 OT 영역에서 사이버훈련을 수행할 수 있는 IT·OT 융복합 사이버훈련장 연구를 소개하였다. OT와 관련된 국내법 및 외국의 사례를 분석하여 국가기반시설 11개 섹터로 분류하여, 사이버공격방어대회에서 사이버훈련을 수행하였다. 또한 이들 섹터에 사이버훈련을 수행할 수 있는 가상머신 상의 SW 기반 구축 방안을 제시하였다. 해당 사이버훈련장이 구축되면 사이버훈련생이 IT와 OT 사이버공격에 대한 방어를 수행할 수 있는 사이버보안 역량이 강화될 것으로 예상된다.

참 고 문 헌

[1] T. E. Song, "The Role of Cyber Warfare in a Full-Fledged Contemporary War: The Case of 2022 Russia-Ukraine War", *Journal of National Defense Studies*, 65(3),pp. 215-236, 2022.

[2] What is operational technology (OT)?, https://www.redhat.com/en/topics/edge/what-is-ot. (Accessed on 08/08/2023).

[3] 콜로니얼 파이프라인 랜섬웨어 사건, 파이프라인 OT 취약성 드러내, https://www.boannews.com/media/view.asp?idx=97355. (Accessed on 08/08/2023).

[4] Cyber Strom: Secure Cyber Space, https://www.cisa.gov/cyber-storm-securing-cyber-space. (Accessed on 08/08/2023).

[5] Locked Shields, https://ccdcoe.org/locked-shields/. (Accessed on 08/08/2023).

[6] Critical Infrastructure Sectors, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. (Accessed on 08/08/2023).

[7] 사이버공격방어대회, https://cce.cstec.kr. (Accessed on 08/22/2023).

[8] 국정원, 세계 최대 규모 사이버 방어훈련 '락드쉴즈' 첫 참가, https://www.boannews.com/media/view.asp?idx=96502. (Accessed on 08/22/2023).

[9] M. Schulze, "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operation", Cycon, 2020.

[10] Seker, "The Concept of Cyber Defence Exercise(CDX): Planning, Execution, Evaluation", International Conference on Cyber Security, 2018.

[11] Tim Grance, Tamara Nolan, et al., "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities", SP 800-84, NIST, 2006.

[12] ECSO, "Understanding Cyber Ranges: From Hype to Reality", 2020.

[13] CTFd, https://ctfd.io/. (Accessed on 08/22/2023).

[14] Markus Ilmar Münzer, "Productization of Strategic Decision-Making Exercise Software based on the STRATEX Platform", Bachelor's Thesis, 2022.

[15] J. H. Yu, et al. "Technological Trends in Intelligent Cyber Range", Electronics and Telecommunications Trends, 2022.

[16] Y. H. Choi, et al. "Design and Implementation

of Cyber Range for Cyber Defense Exercise Based on Cyber Crisis Alert", JKIISC, 30(5), pp 805-821, 2020.
[17] 재난 및 안전관리 기본법, https://www.law.go.kr/법령/재난및안전관리기본법. (Accessed on 08/08/2023).
[18] 국가핵심기반 보호, https://www.mois.go.kr/frt/sub/a06/b13/protectNationCoreFoundation/screen.do. (Accessed on 08/08/2023).
[19] 정보통신기반 보호법, https://www.law.go.kr/법령/정보통신기반보호법. (Accessed on 08/08/2023).
[20] 통합방위법, https://www.law.go.kr/법령/통합방위법. (Accessed on 08/08/2023).
[21] D. Bodeau, R. Graubart et al., "Cyber Resiliency Engineering Framework", MITRE, 2011.
[22] T.J. Choi, et al. "An Analytics Framework for Heuristic Inference Attacks against Industrial Control Systems", 19th International Conference on TrustCom, 2020.
[23] Deploying 5G Core Network with Open5GS and UERANSIM, https://medium.com/rahasak/5g-core-network-setup-with-open5gs-and-ueransim-cd0e77025fd7. (Accessed on 08/08/2023).
[24] UERANSIM, https://github.com/aligungr/UERANSIM
[25] Open5GS, https://open5gs.org
[26] The NASA Operational Simulator for Small Satellites, http://www.stf1.com/NOS3Website/Nos3MainTab.php
[27] OpenPLC, https://openplcproject.com

〈저자소개〉

최 영 한 (Young Han Choi)
2002년 2월 : 한양대학교 전자공학과 졸업
2004년 2월 : KAIST 전자공학과 석사 졸업
2015년 2월 : 고려대학교 정보보호대학원 박사 졸업
2004년 2월 ~ 현재 : ETRI 부설연구소 책임연구원
2020년 2월~현재 : 사이버안전훈련센터 실장
<관심분야> 사이버보안, 사이버훈련, 사이버법률

남 택 준 (Taek Jun Nam)
2001년 2월 : 한국외국어대학교 컴퓨터공학과 학사 졸업
2003년 2월 : 한국외국어대학교 컴퓨터공학과 석사 졸업
2003. 11월~현재 : ETRI 부설연구소 책임연구원
<관심분야> 사이버보안, 사이버훈련

전 동 호 (DongHo Jeon)
2012년 2월 : 경희대학교 전자전파공학과 학사 졸업
2014년 2월 : 경희대학교 전자전파공학과 석사 졸업
2023년 : 고려대학교 정보보호대학원 박사 수료
2013년 12월~현재 : ETRI부설 국가보안기술연구소 선임연구원
2023년 1월~현재 : 사이버안전훈련센터
<관심분야> 정보보호, 사이버훈련, 인공지능

양 현 철 (Hyun Chul Yang)
2014년 2월 : 서울시립대학교 전자전기컴퓨터공학부 졸업
2016년 2월 : KAIST 로봇학제 석사 졸업
2015년 12월~현재 : ETRI 부설연구소 선임연구원
<관심분야> 사이버보안, 사이버훈련

조 수 현 (SooHyun Jo)
2009년 8월: 한남대학교 전자공학과 공학사
2011년 8월: 인하대학교 대학원 컴퓨터정보공학과 공학석사
2014년 8월: 중앙대학교 산업창업경영대학원 경영학석사
2018년 2월: 고려대학교 대학원 컴퓨터학과 박사 수료
2011년 7월~2017년 12월: 삼성전자 무선사업부 선임연구원
2018년 1월~현재: ETRI 부설연구소 선임연구원
2021년 7월~현재: Best of the Best 보안제품개발트랙 멘토
2022년 4월~현재: SW마에스트로 기술부문 멘토
2022년 4월~2022년 12월: 이노베이션 아카데미42서울 비상근 멘토
2023년 10월~현재: 대전광역시 데이터위원회 위촉위원
<관심분야> 사이버보안, 블록체인

강 정 민 (Jungmin Kang)

정회원

2003년 6월~현재 : 사이버안전훈련센터(센터장)

2015년 3월~2016년 2월 : UCSD QI (Qualcomm Institute) 방문연구원

2014년 4월 : 고려대학교 컴퓨터교육학과 졸업(박사)

2011년 7월 : NATO 국제회의 한국대표단

2005년~2011년 : UN GGE(정보보호 정부전문가그룹) 국제회의 한국대표단

2002년 2월~2003년 5월 : 삼성SDS 근무

2002년 2월 : 광주과학기술원(GIST) 정보통신공학과 졸업(석사)

<관심분야> 사이버교육훈련, 사이버보안 및 회복력, 기반시설보호, 국제동향과 사이버분쟁