Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.5, Oct. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.5.805

사이버위기 경보 기반 사이버 방어 훈련장 설계 및 구축 연구

최 영 한,[1†] 장 인 숙,[2] 황 인 택,[2] 김 태 균,[2] 홍 순 좌,[2]
박 인 성,[3] 양 진 석,[3] 권 영 재,[4] 강 정 민[5‡]
[1,2,3,4,5]사이버안전훈련센터(실장, 책임연구원, 선임연구원, 선임기술원, 센터장)

Design and Implementation of Cyber Range for Cyber Defense Exercise Based on Cyber Crisis Alert

Younghan Choi,[1†] Insook Jang,[2] Inteck Whoang,[2] Taeghyoon Kim,[2] Soonjwa Hong,[2]
Insung Park,[3] Jinsoek Yang,[3] Yeongjae Kwon,[4] Jungmin Kang[5‡]
[1,2,3,4,5]Cyber Security Training and Exercise Center (Manager, Principal Researcher, Senior Researcher, Senior Engineer, General Manager)

요 약

사이버 방어 훈련은 최신 사이버공격을 고려한 훈련을 수행해야 할 뿐만 아니라 사이버공격 대응 과정이 실전과 유사해야 그 효과가 크다고 할 수 있다. 또한 최근에는 사이버공격에 관계없이 정상업무를 수행하거나 그에 준하는 업무를 지원할 수 있는 사이버 회복력에 대한 훈련 역시 중요하다. 이에 본 논문에서는 국내에서 사이버공격 발생 시 발령되는 사이버위기 경보를 기반으로 실시간 사이버훈련을 수행함으로 사이버 회복력의 요소들을 강화시킬 수 있는 사이버 방어 훈련장을 제안한다. 사이버위기 경보 수준에 따라 관심·주의·경계·심각 경보 발령 시, 사이버 방어 훈련장은 해당 경보에 따라, 보안 요소를 점검하는 예방보안, 실시간으로 사이버공격 방어를 수행하는 실시간대응, 피해 시스템의 사고조사를 수행하는 사후대응 훈련을 수행할 수 있는 환경을 지원한다. 본 논문에서 제안하는 사이버 방어 훈련장은 사이버위기 환경에서 국내 실정에 맞는 사이버 방어 훈련을 수행함으로써 훈련생들이 사이버위협에 대한 실질적인 대응 역량을 제고 할 수 있다.

ABSTRACT

Cyber defense exercise should require training on the latest cyber attacks and have a similar process to defense cyber attacks. In addition, it is also important to train on cyber resilience that can perform normal tasks or support equivalent tasks regardless of cyber attacks. In this paper, we proposed and developed a cyber range that can strengthen the elements of cyber resilience by performing cyber defense exercise in real time based on the cyber crisis alert issued when a cyber attack occurs in Korea. When BLUE, YELLOW, ORANGE, and RED warnings are issued according to the cyber crisis, our system performs proactive response, real time response, and post response according to the alarm. It can improve trainee's capability to respond to cyber threats by performing cyber defense exercise in a cyber crisis environment similar to the actual situation of Korea.

Keywords: Cyber defense exercise, Cyber security training

Received(05. 14. 2020), Modified(07. 20. 2020), Accepted(08. 25. 2020)

† 주저자, yhch@nsr.re.kr
‡ 교신저자, jmkang@nsr.re.kr(Corresponding author)

I. 서 론

사이버위협이 증가하고 그 피해가 막대해짐에 따라, 사이버공격 대비에 대한 수요가 점점 증가하고 있다. 이에 보안 전문 인력의 사이버보안 역량을 강화할 수 있는 사이버훈련이 요구되었으며, 세계 각국에서 사이버훈련이 활발하게 수행되고 있다[1,2,3,4]. 사이버보안의 선제적 조치로써 사이버 방어 훈련(Cyber Defense Exercise, CDX)을 실시간으로 수행함으로써 보안 역량을 제고 할 수 있다[5,6]. 사이버 방어 훈련 참가자는 각각 주어진 역할에 따라 Green Team에서 사이버 훈련장 환경을 구축하고, 방어를 수행하는 Blue Team을 대상으로 Red Team이 사이버공격을 수행한다.

사이버 방어는 예방·탐지·분석·대응이 순환적으로 수행되는 일련의 과정으로 사이버훈련은 이들 과정을 종합적으로 포함해야 한다. 특히 나라별로 사이버위협에 대한 대응체계가 달라 해당 나라 체계에 맞는 훈련을 수행해야 한다. 국내의 경우는 사이버위기 경보인 정상·관심·주의·경계·심각 단계에 따라 사이버 방어를 수행하도록 되어 있다[7]. 따라서 국내에서 수행되는 사이버훈련인 경우는 사이버위기 경보에 따른 단계적 과정이 반영되어야 한다.

또한, 최근에는 사이버공격에 관계없이 정상 업무를 수행하거나 그에 준하는 업무를 지원할 수 있는 사이버 회복력(Cyber resilience)이 강조되고 있다[8]. 사이버 회복력은 5개의 요소인 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Response), 복구(Recover)로 구성된다[9]. 사이버 회복력은 업무를 지속할 수 있는 능력으로 사이버공격의 정도와 관계없이 사이버 방어를 수행할 수 있도록 평시에 사이버훈련을 통해 그 역량을 유지하고 있어야 한다.

본 논문은 국내의 사이버위기 상황을 반영하여 사이버훈련을 수행할 수 있는 사이버위기 경보 기반 사이버 방어 훈련장을 제안하고 이를 기반으로 구축한 사이버 훈련장에 대해 기술한다. 본 논문의 사이버훈련은 사이버위기 경보에 따라 3개의 과정으로 구성되어 있다. I 과정에서는 사이버공격 발생 전의 정상 단계로 보안 취약 요소를 점검하는 예방보안 훈련을 수행한다. II 과정에서는 실시간으로 사이버공격이 이루어지며 관심·주의·경계·심각 단계가 차례로 발령이 된다. 경보 수준에 따라 실시간으로 방어를 수행하는 실시간대응 훈련이 이루어진다. III 과정에서는 상시로 이루어지는 사고조사로 피해 시스템을 분석하는 사후대응 훈련을 수행한다. 세 개의 과정을 차례로 수행함으로써 본 논문의 사이버 방어 훈련장은 사이버위기 환경에서 국내 실정에 맞는 사이버 방어 훈련을 수행할 수 있는 환경을 제공한다. 이를 통해 사이버 회복력의 5개 요소를 모두 훈련받을 수 있다.

사이버 방어 훈련장을 구축 및 운영하기 위해선 사이버공간을 모사할 수 있는 시스템이 요구되며 본 논문은 가상화 환경을 기반으로 개발하였다. 이를 통해 개별 시스템을 모사하는 가상머신을 수천개 구축할 수 있었다.

본 논문의 구성은 2장에서 사이버 훈련장과 관련된 기술 동향을 소개하고, 3장은 기존 사이버 훈련장을 분석하여 도출한 사이버 훈련장 구성하는 요소들에 대해 기술한다. 4장은 사이버 훈련장에 대한 문제 제기 및 이를 해결하기 위해 본 논문에서 제안한 방향을 제안한다. 5장에서는 사이버위기 경보 기반 사이버 방어 훈련장의 구조 및 훈련 과정에 대해, 6장은 사이버 방어 훈련장의 구축에 대해 설명한다. 7장에서는 결론을 맺는다.

II. 관련연구

사이버 훈련장은 사이버공격 및 방어를 실전처럼 수행할 수 있는 플랫폼으로 지속적으로 연구와 개발이 되고 있다. 초창기에는 네트워크를 테스트하기 위한 테스트베드로 주로 개발이 되었다가 사이버보안 요소가 더해지면서 점점 사이버 훈련장으로 확장되었다.

Davis는 네트워크 테스트베드 관점에서 모델링, 시뮬레이션, 오버레이(overlay), 에뮬레이션으로 분류하여 군, 학계, 기업에서의 사이버 훈련장을 분석하였다[10]. Tsai는 네트워크 에뮬레이션 테스트베드로서 하드웨어와 상위 소프트웨어를 연결하는 컨트롤 프레임워크(control framework)의 다양한 기술을 소개하고 있다[11]. 네트워크 테스트베드는 사이버 훈련장을 구성하는 가장 기본적인 요소로 가상으로 구성된 네트워크 환경에서 사이버공격과 방어에 대한 훈련을 수행할 수 있다. Fox는 사이버공간에서의 공격과 방어를 수행하는 Cyber wargaming에 대한 기술 관련 요소와 적용되는 분야에 대해 분석을 하였다[12]. Priyadarshini는 사이버 훈련장을 인프라 스트럭쳐, 클라우드, 훈련을 수행하는 팀 역할 등에 따라 분류하였다[13]. Chaskos는 사이버 훈련장을 Cyber-threat intelligence, threat

forecasting, visualization, Gamification, Risk analysis, Forensic, interaction with external platform의 7개의 모듈을 기준으로 분석을 하였다[14]. Yamin은 사이버 훈련장과 관련된 용어들을 체계적 문헌고찰(systematic review) 방법을 이용하여 사이버 훈련장의 최근 동향을 분석하였다[15].

다음은 사이버 훈련장을 구축한 기관을 기준으로 학계, 정부, 기업으로 나누어 상세히 설명한다.

2.1 학계(Academia)

학계의 경우 사이버 훈련장은 사이버보안 교육 실습 운영을 위해 구축을 하거나 사이버 훈련장과 관련된 기반 기술 향상을 위한 연구 주제로 활용된다.

학교에서는 사이버 교육 실습을 위해 사이버 훈련장을 운영하고 있다. 대표적인 대학교로 Virginia Cyber Range[16], Regent Cyber Range[17], Wayne Cyber Range Hub[18], Arkansas Cyber Range[19] 등이 있다. Virginia Cyber Range는 버지니아의 고등학생과 대학생을 대상으로 수행되는 사이버교육을 지원하기 위한 사이버 훈련장이다. 200개 이상의 고등학교와 대학교를 지원하고 있으며, 5만개 이상의 가상머신이 구축되어 있다[16]. Georgia Cyber Range는 Georgia Cyber Center에서 운영하는 사이버 훈련장으로 오픈소스로 공개된 kinetic 시스템을 기반으로 사이버 훈련장이 구축되어 있다[20]. kinetic은 조지아의 US Army Cyber School에서 개발된 사이버 훈련장 개발 및 관리 툴이다[21].

또한 학계에서는 사이버 훈련장 관련 기술을 향상시키기 위한 연구도 수행한다. ICSrange는 SCADA를 기반으로 기업의 네트워크와 ICS(Industrial Control System) 에뮬레이션 환경을 제공한다. 공격 도구로 nmap, wireshark, metasploit, metepreter, kali linux 등을 사용한다[22]. CyTrONE은 Cybersecurity Training Framework로 사이버 훈련장을 구축하는 CyRIS[23], LMS(Learning Management System)을 위한 CyLMS, 웹 인터페이스를 위한 CyTrONE-UI-WEB, 시나리오 관리를 위한 CyPROM으로 이루어져 있다[24,25]. CloudWhip은 퍼블릭 클라우드인 AWS 상에 Brute Force Attack 등의 훈련 시나리오를 구현하였다[26]. RIO(Resource Orchestration Infrastructure)는 DoS 관련된 네트워크 공격 상황을 훈련할 수 있는 환경을 제공한다[27]. HTCR은 훈련 진행에 영향을 주지 않고 모니터링하기 위해 가상머신 외부에서 메모리를 분석하는 방법을 제안하였다[28]. DECIDE는 NUARI(Norwich University Applied Research Institutes)에서 개발한 사이버공격 훈련을 수행할 수 있는 플랫폼이다[29]. KYPO Cyber Range는 체코의 가장 큰 학교 대상 사이버 훈련장이다[30,31].

2.2 정부(Government)

NCR(National Cyber Range)은 DARPA에 의해 추진된 프로젝트이지만 지금은 록히드마틴과 관련된 DoD TRMC(Test Resource Management Center)에 의해 관리되고 있다. NCR은 네트워크 인프라, 도구 등과 같은 통합적인 사이버 환경으로 사이버훈련을 위한 기본적인 네트워크를 제공한다[32,33].

CRATE(Cyber Range And Training Environment)는 Swedish Defense Research Agency(FOI)에 의해 운영되는 사이버 훈련장으로 2008년에 개발되기 시작했으며 800개 정도의 물리 서버로 구성되어 있다[34,35]. CRATE 내에는 사용자 행위를 모사하는 트래픽 생성기와 CRATE를 모니터링하고 로깅을 하는 도구들이 설치되어 있다.

CaSTLE(Cyber Security Training and Learning Environment)은 AIT(Austrian Institute of Technology)에서 개발한 사이버 훈련장으로 IT와 OT(Operational Technology)의 환경을 제공한다[36,37].

2.3 기업(Industry)

사이버 훈련장을 활발하게 개발 및 운영하는 곳은 기업이다.

Cybexer은 운영자인 사람에 의해 발생될 수 있는 위험을 식별할 수 있는 Cyber-hygiene 모듈을 개발하였다[38]. 이를 이용하여 사이버훈련을 통해 운영 중 발생될 수 있는 위험 요소를 분석하며, 결과를 활용하여 대상 기관에 적합한 교육을 시킨다. Silensec Cyber Range는 클라우드를 기반으로 수천명의 동시 사용자가 훈련할 수 있는 수백개의 시

나리오가 지원되는 사이버 훈련장이다[39]. Cyberium Arena는 이스라엘의 ThinkCyber에서 개발한 사이버 훈련장으로 40개 이상의 훈련 프로그램을 제공한다[40]. IBM의 Cyber Tactical Operations Center(C-TOC)는 23톤의 트레일러에 구축되어 있으며 이동이 가능한 사이버 훈련장이다[41]. Michigan Cyber Range는 Merit Network이 운영을 하고 있으며 Merit Secure Sand box을 기반으로 사이버보안 관련 교육과 훈련을 수행한다[42]. Cybergym은 people, processes & policies, technology & tools 기반의 사이버위협 모델을 이용하여 훈련 대상 조직에 적합한 훈련을 수행한다[43]. Baltimore Cyber's Range는 통합된 Training Management System(TMS)에서 Setup, Execution, Review의 단계로 훈련이 수행된다[44]. Florida Cyber Range는 사이버보안과 관련된 West Florida Center와 사이버훈련 플랫폼을 위해 Metova CyberCENTS[45]가 함께 만들었다[46]. Circadence Cyber Range는 게임화를 지원하는 Cyber learning platform인 Project Ares가 Microsoft Azure 클라우드 상에 구축되어 있으며, 사용자 접속은 인터페이스인 CyberBridge를 통해 이루어진다[47]. Cyber warfare range는 Arizona Cyber Warfare Range에서 이름이 변경된 live-fire 형식의 사이버 훈련장이다[48]. CYBERIUM는는 Fujitsu사에서 개발한 사이버 훈련장으로 VDI(Virtual Desktop Infrastructure)를 이용하여 원격으로 사이버훈련을 수행한다[49]. Airbus CyberRange는 1,200개의 VM과 40,000개의 도커를 지원한다[50]. AWS Cyber Range는 AWS 환경에서 오픈소스 도구를 활용하여 훈련 시스템을 구축하였다[51].

네트워크 장비 업체는 자사의 네트워크 분석 기술 및 장비를 활용한 사이버 훈련장을 운영하고 있다. Cisco Cyber Range는 네트워크 관련 Infrastructure, 사이버공격 관련 Attacks, 어플리케이션 레벨의 사이버훈련인 Visibility & Control의 사이버훈련 서비스를 제공한다[52]. IXIA Cyber Range는 악성 네트워크 트래픽을 캡처한 후 훈련 시나리오에 따라 재생을 함으로써 다양한 사이버위협을 제공한다[53]. 네트워크 테스트베드를 제공하는 업체는 자사의 네트워크 구축 기술을 활용하여 사이버 훈련장을 구축하고 있다. SimSpace는 미리 정의된 네트워크 환경을 제공한다[54]. 15개의 호스트를 사용하는 mini-network에서부터 280개의 호스트를 사용하는 Generic Financial 네트워크 등 다양한 네트워크 환경을 제공한다. CyberVAN은 네트워크 시뮬레이션과 가상화 기술로 구현된 사이버훈련을 위해 제공되는 테스트베드이다[55]. 시나리오 작성시 OPNET, QualNet, ns2, ns3 등과 같은 네트워크 시뮬레이터를 사용할 수 있다.

방산업체는 군과 관련된 제품을 생산하는 기업으로 사이버 훈련장 또한 개발하여 운영하고 있다. Raytheon Cyber Range Capability는 하드웨어, 소프트웨어, 네트워크 등에 대한 사이버 회복력을 테스팅 하거나 공격·방어 임무에 맞추어 사이버훈련을 수행할 수 있다[56]. 이 훈련장은 Raytheon Cyber Operations, Development & Evaluation (CODE)와 연계하여 훈련 참가자의 기관 네트워크의 복사를 통해 대상 기관과 유사한 환경을 사이버훈련에 제공한다. Cyberbit는 사이버훈련을 위한 OT와 기업 환경을 가상적으로 제공하며, OT 하드웨어를 물리적으로 통합하여 훈련을 수행할 수도 있다[57]. 이 회사는 Baltimore's Cyber Range와 Regent Cyber Range 등과 같은 대학교의 사이버 훈련장도 구축하였다.

III. 사이버 방어 훈련장 구성 요소

사이버 훈련장은 훈련 대상 네트워크 환경을 모사한 시스템에 사이버 공격이나 방어를 수행할 수 있는 시나리오를 주입하여 사이버훈련 참가자가 훈련을 수행할 수 서비스를 제공한다. 본 논문에서는 기존 사이버 훈련장을 분석을 통해 사이버 훈련장을 기본적으로 구성하는 3가지 요소인 환경(Environment), 시나리오(Scenario), 운영(Operation)을 도출하였다(Fig.1.). 사이버 훈련장은 이들 3가지 요소를 기본적으로 가지고 있다.

- **사이버 훈련장 환경(Environment)**: 사이버 훈련장의 훈련 대상이 되는 네트워크 및 시스템이다. 사이버 훈련장은 기관 네트워크, SCADA, IoT, 모바일 등 다양한 환경을 모사한다. 가상화 기술의 발달로 최근에는 가상머신을 이용하여 훈련 환경을 많이 구축하고 있으며, 물리 시스템과 병행하여 구축함으로 훈련 대상 환경을 확장하고

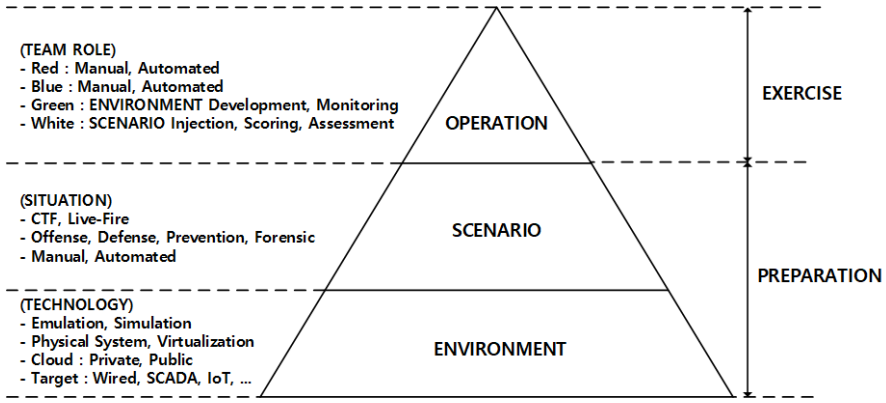

Fig. 1. Elements of cyber range

있다. 환경의 경우, 네트워크 환경을 잘 모사해야 하기 때문에 기술(Technology) 요소가 강조된다.

- **훈련 시나리오(Scenario)**: 사이버 훈련장 환경 위에 사이버 공격이나 방어를 수행할 수 있는 훈련 내용을 주입한다. 시나리오는 문제 풀이 형식이나 실전을 위한 이야기 흐름이 될 수 있으며, 주어진 임무를 수행함으로써 사이버 보안에 대한 역량을 강화 시킬 수 있다. 시나리오는 사이버위협에 대한 상황(Situation)을 잘 정의하고 표현할 수 있어야 한다.
- **훈련 운영(Operation)**: 훈련 수행 시 참가자는 각각의 역할이 주어진다. 사이버공격을 수행하는 Red Team, 사이버 방어를 수행하는 Blue Team, 사이버 훈련장 환경을 구축하는 Green Team, 훈련 시나리오를 개발 및 운영하는 White Team이 있다. 이와 같이 운영의 경우는 각각 주어진 팀 역할을 잘 수행할 수 있어야 한다.

사이버훈련 과정은 두 개의 단계로 분류될 수 있다. 준비(Preparation)는 훈련을 수행하기 전의 단계로 사이버 훈련장 환경 구축과 훈련 시나리오 개발과 관련 있다. 훈련 실시(Exercise)는 시나리오가 주입된 사이버 훈련장 환경에서 참가자들이 각자의 역할에 맞게 훈련을 수행하는 단계이다. 해당 단계에서는 훈련 수행시 발생하는 점수 취합과 평가를 포함한다.

3.1 사이버 훈련장 환경(Environment)

사이버 훈련장 환경은 훈련 대상이 되는 사이버 공간을 지칭한다. 그래서 사이버 훈련장은 네트워크 테스트베드에서 확장하여 사이버위협 시나리오를 적용한 경우가 많다[15]. SCADA[58, 59], 네트워크[55, 60]와 같이 다양한 사이버 공간이 사이버 훈련장을 위한 모사 대상이 된다.

사이버 훈련장 환경은 공간과 비용 문제로 인해 점점 물리 시스템보다 가상화 기술을 이용하여 구축한다. 이와는 별개로 Cyber-Physical System (CPS)의 경우는 사이버 공간과 접속하는 물리 시스템이 필요하기 때문에 물리 시스템을 병행하여 운영한다[61]. 가상화를 제공하는 플랫폼은 OpenStack[62], vSphere[63], KVM[64] 등과 같이 다양하다. KYPO Cyber Range, CaSTLE은 OpenStack을 기반으로 개발이 되었다. NATO Cyber Range는 vSphere를 사용하며, HTCR은 KVM 이용하여 개발되었다. 이들 가상화 시스템은 프라이빗 클라우드를 구성하는데 이런 경우는 시스템 및 데이터를 직접 관리할 수 있는 장점이 있으나, 시스템 유지 보수 및 용량 확대를 위해 지속적으로 확장을 해야 하는 단점이 있다. 이를 해결하기 위해 AWS[65], Azure[66]와 같은 퍼블릭 클라우드를 사용하는 사이버 훈련장이 늘어나고 있다. CloudWhip과 AWS Cyber Range는 AWS를, Circadence cyber range는 Azure를 이용하여 개발되었다.

3.2 훈련 시나리오(Scenario)

시나리오는 훈련을 참가하는 훈련생이 수행해야 하는 임무이다. 시나리오를 통해 사이버훈련 참가자들은 사이버 공격이나 방어를 실전처럼 경험할 수 있

다. 그래서 사이버 훈련장의 세 가지 구성 요소 중 가장 중요한 요소라 할 수 있다.

시나리오는 사이버 훈련장 환경 기반 위에 취약한 시스템을 통해 구축될 수 있다. 따라서 사이버 훈련장 환경이 훈련 대상 네트워크와 유사하면 할수록 시나리오는 현실을 잘 반영하게 된다.

시나리오 진행 방식은 이미 설치된 취약한 시스템의 접근을 하여 문제를 푸는 Capture The Flag(CTF) 방식과 실시간으로 사이버 공격이나 방어를 수행하는 Live-fire 방식이 있다. CTF의 경우는 다양한 분야의 보안 관련 문제들을 푸는 Jeopardy style 방식과 취약한 서비스를 가지는 가상머신에서 보안 문제를 찾고 고치는 Attack-defence 방식의 두 가지가 있다[67]. CTF 방식은 사이버 해킹 대회에서 많이 적용되는 방식이다[68]. Live-fire 방식은 사이버 공격이나 방어가 실시간으로 이루어지는 방식으로 실전과 같은 상황에서 사이버훈련을 수행할 수 있는 장점이 있다[69]. 에스토니아에서 개최하는 Locked Shield가 대표적이다[2].

시나리오 내용은 공격(Offense), 방어(Defense), 사고조사(Forensic), 예방(Prevention) 등과 같이 다양한 분야로 구성될 수 있다[70]. 공격 시나리오는 일정한 대상에 대한 사이버공격이며, 방어 시나리오는 사이버공격이 이루어지는 상황에서 방어를 수행하고, 사고조사는 사이버공격이 일어난 시스템에 대해 사고 원인과 피해를 분석한다. 예방은 사이버공격이 일어날 수 있는 시스템의 취약 요소를 제거하는 과정으로 직접적인 사이버공격과 관련된 훈련은 수행하지 않지만 사이버공격 피해를 최소화 시킬 수 있는 시나리오로 중요한 훈련 중 하나로 차지하고 있다.

3.3 훈련 운영(Operation)

훈련 운영은 훈련 시나리오가 사이버 훈련장 환경 위에 주입된 후 이루어지는 실제 훈련 수행과 관련이 있다. 훈련 참가자는 수행하는 역할에 따라 다음과 같이 분류된다[5].

- Red Team(RT)은 사이버공격을 수행하는 역할을 한다. 시나리오가 사이버공격인 경우는 RT가 훈련생이 된다. 사이버방어인 경우는 훈련을 운영하는 White Team에서 해당 역할을 수행할 수 있다.
- Blue Team(BT)은 RT에서 이루어지는 사이버공격의 방어를 수행하는 역할을 한다. 사이버방어를 수행함으로써 사이버위협에 대응하는 훈련생의 역량을 강화시킬 수 있다. 본 논문에서의 사이버 방어 훈련장에서는 훈련생은 BT로 참가하여 훈련을 수행한다.
- Green Team(GT)은 훈련 대상이 되는 사이버공간을 잘 모사하여 사이버 훈련장 환경을 구축하는 역할을 한다. 훈련시 직접 참가를 하지 않지만 시나리오가 주입되는 훈련 환경을 구축하는 중요한 역할을 수행한다.
- White Team(WT)은 훈련 시나리오를 사이버 훈련장에 주입하고 사이버훈련을 운영하는 역할을 한다.

훈련생은 훈련의 목적에 따라 사이버공격을 하는 RT나 사이버 방어를 하는 BT의 역할을 수행한다. CTF는 대상 시스템의 취약 요소를 찾는 경우가 많아 RT가 훈련생들의 주요 역할이며[71], CDX는 방어에 초점을 맞추기 때문에 BT가 주요 역할이 된다[5]. BT의 역량 향상을 위해 실제 사이버공격과 유사한 상황에서 훈련을 수행할 수 있도록 RT에서는 자동화된 공격 방법도 필요하다[72,73].

GT는 사이버 훈련장 환경을 구축하고 구축된 시스템의 상태를 모니터링 하는 역할을 수행한다. 가능한 훈련 대상이 되는 사이버 공간의 네트워크 환경과 시스템을 모사해야 한다. 따라서 네트워크 테스트베드를 구축하는 기술이 GT가 보유해야 할 기본 기술이 된다[15].

WT는 시나리오 실행을 통해 훈련을 진행하며 훈련생들의 점수를 스코어링 한다. 스코어링은 훈련생의 훈련 수행 정도를 파악하는데 중요한 정보로 활용된다[74,75]. 또한 사이버훈련을 수행하면서 해결하는 문제들을 통해 훈련생의 사이버보안 역량을 평가할 수 있다. NIST NICE(National Initiative for Cybersecurity Education)는 역량 평가를 위한 직무를 분류하고 요구되는 기술적 역량을 정의하고 있다[76].

IV. 문제 제기 및 접근 방향

4.1 문제 제기

기존 사이버 훈련장들은 대부분 임무 위주의 사이버훈련을 수행하기 때문에 사이버 공격과 방어에 대한 기술 습득에 초점을 맞추고 있다. 그러나 사이버 보안 활동은 예방, 탐지, 분석, 대응이 순환적으로 수행되는 일련의 과정으로 사이버훈련은 이들 과정을 종합적으로 포함해야 한다. 특히 각 나라별로 사이버 위협에 대한 대응 체계가 있으며, 국내 역시 사이버 위기 경보를 통해 사이버공격 정도에 따라 대응을 수행할 수 있는 체계가 존재한다. 그러나 국내에는 사이버위기 경보를 이용하여 시나리오를 구성하고 훈련을 실시하는 사이버 훈련장은 미비한 사항이다.

최근에는 사이버공격이 이루어지더라도 신속하게 복구와 업무를 수행할 수 있는 사이버 회복력(Cyber resilience)이 점점 중요해지고 있다[8, 77]. 사이버 회복력은 사이버위협에 대해 업무를 지속할 수 있는 능력을 의미하며, 구성하는 요소로 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)의 5가지를 정의하였다[9](Table.1.). 사이버훈련에서는 이들 요소들이 시나리오에 반영되어 훈련생들의 역량을 강화시킬 수 있어야 한다.

Table 1. Elements of cyber resilience

Definition	Explanation
Identify	Critical asset and process mapping, risk and readiness assessment, and so forth
Protect	Traditional first line of defense security mechanisms
Detect	Security analytics
Respond	Response to security breaches or failure
Recover	Coordinated recovery mechanisms

4.2 접근 방향

본 절에서는 앞 절에서 제기한 문제를 해결할 수 있는 사이버위기 경보를 기반으로 훈련을 수행하는 사이버 훈련장을 제안한다. 제안한 사이버 훈련장은 사이버위기 경보 단계를 기준으로 세 개의 과정이 순차적으로 이루어지며, 단계별 훈련을 통해 사이버 회복력의 5가지 요소를 훈련 받을 수 있다.

- **I 과정**: 사이버위협 관련 사이버위기 경보가 발령되기 전의 정상 단계에 해당된다. 사이버공격 발생 전 시스템의 보안 설정 및 취약요소를 점검하여 제거하는 훈련을 수행한다. 본 논문에서는 예방보안 훈련으로 지칭한다. 사이버 회복력에서 식별과 탐지의 요소를 훈련한다.
- **II 과정**: 사이버위기 경보가 관심·주의·경계·심각 단계가 차례대로 발령된다. 실시간으로 일어나는 사이버공격을 방어하여 공격의 피해를 최소화하거나 제거하는 훈련을 수행한다. 본 논문에서는 실시간대응 훈련으로 지칭한다. 사이버 회복력에서 탐지, 보호, 대응, 복구의 요소를 훈련한다.
- **III 과정**: 사이버위기 경보와 관련 없이 상시로 수행하는 사고조사 단계이다. 사이버공격이 일어난 피해 시스템에 대해 사고 원인을 분석하거나 제거하는 임무를 수행한다. 본 논문에서는 사후대응 훈련으로 지칭한다. 사이버 회복력에서 탐지의 요소를 훈련한다.

V. 사이버위기 경보 기반 사이버 방어 훈련장 설계

본 장에서는 본 논문에서 제안한 사이버위기 경보 기반 사이버 방어 훈련장을 설계한다. 3장에서 기술한 사이버 훈련장 구성 요소인 사이버 훈련장 환경, 훈련 시나리오, 훈련 운영을 기준으로 설명한다.

5.1 사이버 훈련장 환경

본 연구의 사이버 훈련장은 전체적으로 총 4개의 영역으로 구성되어 있으며 가상화 환경에 구축된다(Fig.2.).

- 관리영역(Management Area): 사이버 방어 훈련장, 훈련생 접속 웹 인터페이스(포털), 훈련 시나리오 등 사이버훈련을 수행하기 위해 훈련장을 전반적으로 관리하는 영역이다.
- 인터넷영역(Internet Area): 방어영역 내의 시스템이 정상 인터넷 활동을 할 수 있도록 웹사이트와 사용자를 모사한 영역이다. 방어영역에서는

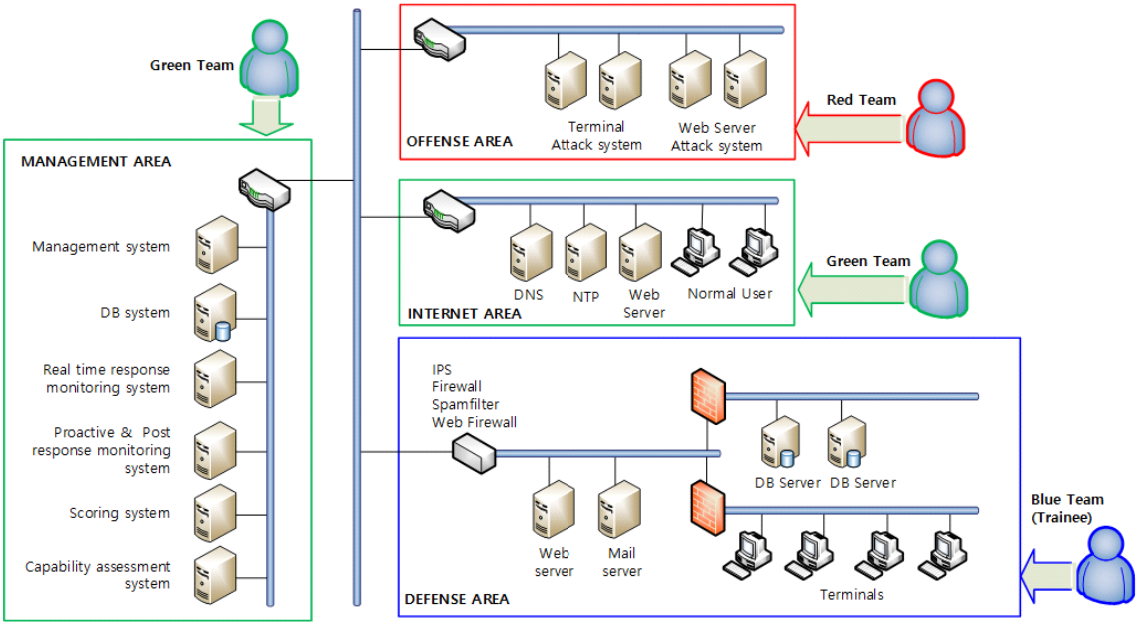

Fig. 2. Cyber range for cyber defense exercise based on cyber crisis alert

인터넷 공간으로 간주된다.

- 공격영역(Offense Area): RT가 사용하는 영역으로 방어영역 내의 시스템을 공격한다.
- 방어영역(Defense Area): BT인 훈련생들이 참가하여 방어를 수행하는 영역이다. 훈련생들은 훈련 시나리오가 진행될 때 방어영역 내의 시스템을 방어함으로써 사이버보안 역량을 강화한다.

5.1.1 관리영역(Management Area under GT)

관리영역에서는 훈련장의 운영을 위한 시스템, 참가 훈련생, 접속 웹 인터페이스(포털), 훈련 시나리오 등을 관리한다.

- 관리시스템(Management system): 전반적인 사이버 방어 훈련장을 관리한다. 본 연구의 사이버 훈련장은 가상화 기반 사이버 훈련장으로 훈련 시나리오를 위해 설치된 가상머신(VM)을 관리한다. 관리영역에서 제공하는 포털 웹 인터페이스를 통해 훈련생이 방어영역의 시스템에 접근한다. 모든 포털을 통해 이루어진다.
- DB 시스템(DB system): 훈련장 운영을 위한 데이터와 훈련 수행시 생성되는 모든 데이터를 저장 및 관리한다.
- 실시간대응 모니터링 시스템(Real time response monitoring system): 실시간대응 훈련 시 방어영역 내 시스템의 상태를 모니터링 한다.
- 예방보안 & 사후대응 모니터링 시스템(Proactive & Post response monitoring system): 예방보안과 사후대응 훈련 시 훈련생이 접속하는 시스템에 대한 상태를 모니터링 한다.
- 훈련 점수 시스템(Scoring system): 예방보안, 실시간대응, 사후대응 훈련 시나리오를 해결하는 과정에서 채점되는 훈련생들의 점수를 수집하여 처리한다.
- 역량평가 시스템(Capability assessment system): 훈련 점수 및 수행한 훈련 미션을 기반으로 훈련생들의 사이버보안 역량을 평가한다.

5.1.2 인터넷영역(Internet Area under GT)

방어영역 내 시스템이 정상 인터넷 활동을 할 수 있도록 인터넷 내 웹사이트와 사용자를 모사한다. 이는 방어영역으로 정상 트래픽을 발생시켜 실제 사이버 사고 분석 환경을 제공하는 역할을 한다.

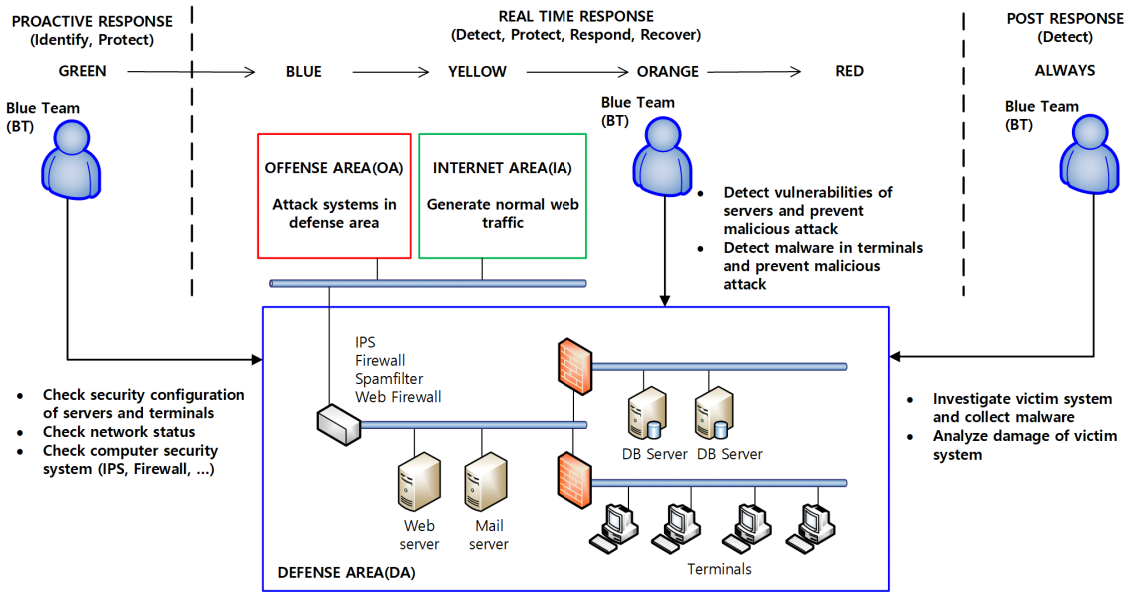

Fig. 3. Process of cyber defense exercise based on cyber crisis alert

- 정상 웹사이트 모사 시스템: 방어영역 내 사용자들이 접속하는 인터넷 환경을 모사하기 위한 웹사이트의 집합이다. 다양한 웹사이트와 이들 웹사이트의 도메인을 관리하기 위한 DNS 서버가 있다. 실시간대응 훈련시 말웨어와 C&C 통신 사이에 정상 트래픽을 발생시킴으로써 실제 환경과 유사하게 만든다.
- 정상 사용자 모사 시스템: 방어영역 내 웹서버에 접속하는 사용자를 모사하기 위한 웹서버 접속 트래픽을 생성한다. 이렇게 함으로써 웹서버에 다양한 사용자들의 접속 로그가 남게 된다. 실시간대응 훈련시 사이버공격을 받는 웹서버의 실제 환경과 유사하게 만든다.

5.1.3 공격영역(Offense Area under RT)

실시간대응 훈련 시 방어영역 내에 있는 웹서버와 단말을 공격한다. 사이버위기 경보의 단계에 따라 공격의 수위가 달라진다.

- 웹서버 공격시스템: 훈련 시나리오 별로 방어영역 내 웹서버의 취약점을 악용하는 공격을 동시에 혹은 순차적으로 수행한다.
- 단말 공격시스템: 공격은 취약점을 이용한 설치 단계와 설치 후 동작 단계로 나누어진다. 설치 단계는 단말에 설치된 어플리케이션의 취약점을 이용하여 악성코드를 설치한다. 동작 단계는 단말 내에서 은밀히 설치된 악성코드가 C&C의 명령을 받음으로 공격이 이루어진다.

5.1.4 방어영역(Defense Area under BT)

방어영역은 훈련생들이 사이버공격으로부터 보호를 해야 하는 영역이다. 시스템 구성은 훈련 시나리오에 따라 다양하다. 기본적으로 정보보호시스템, 웹서버, DB서버와 단말로 구성된다. 예방보안, 실시간대응, 사후대응 훈련 시나리오 별로 사이버위협에 취약한 단말 및 서버가 설치된다.

5.2 훈련 시나리오

훈련 시나리오는 사이버위기 경보 단계를 기반으로 개발된다. 전체 과정을 세 개(예방보안, 실시간대응, 사후대응)로 나누어져 사이버위협에 따라 순차적으로 진행된다(Fig.3.).

- **예방보안(정상 단계)** 사이버위협 발생 전 단계로 방어영역 내의 시스템에 대해 일상적인 점검을 수행한다. 서버, 단말, 정보보호시스템 등 방어영역 내 구축된 시스템에 대한 보안 설정 및

취약요소를 점검하여 수정한다. 해당 훈련을 통해 사이버 회복력에서 식별과 보호와 관련된 사이버보안 역량이 강화된다.

- **실시간대응(사이버위기 경보 발령 단계)** RT에 의해 실시간으로 공격이 이루어지며, BT는 이를 방어하기 위한 훈련을 수행한다. 사이버위기 경보 단계에 따라 공격영역의 사이버공격의 정도는 강해진다. 참가자는 서버와 단말의 취약요소를 제거하여 사이버공격을 막는 임무를 수행한다. 해당 과정에서는 방어영역 내의 웹서버, 단말 등의 다양한 시스템을 보호해야 한다. 사이버 회복력에서 보호, 탐지, 대응, 복구와 관련된 사이버보안 역량을 강화시킬 수 있다.
- **사후대응(상시)** 해당 과정은 피해를 입은 시스템에 대해 사고조사를 수행한다. 분석 도구를 사용하여 피해 시스템 내의 악성 행위 및 피해 정도를 분석한다. 해당 과정을 훈련받게 되면 사이버 회복력에서 탐지와 관련된 역량을 강화 시킬 수 있다.

5.3 훈련 운영

본 논문의 사이버위기 경보 기반 훈련의 참가자들은 다음과 같은 3개의 역할을 각각 맡아 훈련을 진행한다.

- Blue Team(BT): 훈련생이 수행하는 역할이며, 관리영역에서 제공하는 포털을 통해 방어영역에 접속한다. 사이버위기 경보 단계에 따라 예방보안, 실시간대응, 사후대응 훈련을 순차적으로 수행한다.
- Red Team(RT): 실시간대응 훈련시 공격영역에서 방어영역에 대한 사이버공격을 수행한다. 공격의 진행 상황에 맞추어 사이버위기 경보가 발령된다. RT는 항상 BT의 상황을 모니터링하고 있으며, BT의 대응 정도에 따라 공격의 수준을 조절한다.
- Green Team(GT): BT와 RT를 제외한 훈련장을 구축 및 운영하기 위한 일을 수행한다. 본 사이버 훈련장에서 GT는 시스템 구축을 하는 Green Team, 훈련을 구성하고 훈련 수행을 점검하는 White Team의 역할을 모두 수행한다.

VI. 사이버위기 경보 기반 사이버 방어 훈련장 구축

본 논문에서는 사이버위기 경보 기반 사이버 방어 훈련장을 VMware vSphere 6.7 기반으로 프로토타입을 개발하였다. 가상머신의 상당수가 방어영역 네트워크 구성에 사용되었으며 각각의 방어영역은 격리가 되어 다른 참가자들의 시스템에 접근을 할 수 없도록 하였다. 물리서버들은 SAN을 통해 공통의 스토리지에 접근을 할 수 있다.

훈련 시나리오는 예방보안 3개, 실시간대응(웹) 4개, 실시간대응(단말) 4개, 사후대응 3개가 개발되었다.

- 예방보안의 훈련 시나리오는 Windows 10, 2016과 CentOS 7에 대한 보안 설정 및 취약요소를 점검 사항을 제공한다.
- 웹서버 대상 실시간대응의 훈련 시나리오는 SQL 취약점 공격 등 웹페이지에 대한 실시간 공격으로 이루어진다.
- 단말인 PC 대상 실시간대응의 훈련 시나리오는 Windows 10을 공격하는 악성코드에 대해 C&C 서버 공격을 막고 악성코드를 제거하는 훈련 시나리오를 제공한다.
- 사후대응의 훈련 시나리오는 사이비공격 피해를 받은 Windows 10에 대해 사고의 원인을 분석한다.

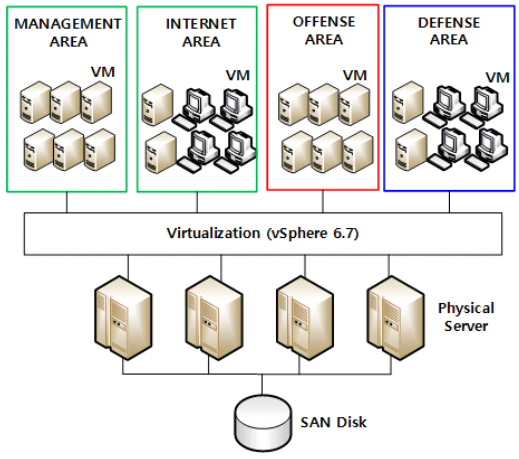

Fig. 4. Implementation of cyber range

훈련생들이 접근하는 포털은 웹으로 구현이 되었다. 훈련이 시작되면 사이버위기 경보가 발령되고 훈련생들에게는 시간별로 설정된 보안권고문이 발송된다. 보안권고문의 내용은 사이버위기 경보 단계와 관련이 있다. 사이버훈련은 각 시나리오별 힌트가 있는 보안권고문을 참고하여 수행된다. 시나리오별로 미리 설정된 취약한 가상머신에 콘솔로 접근을 하여 주어진 임무를 수행한다. 콘솔은 Windows의 UI 화면을 제공하여 웹에서 가상머신에 설치된 PC를 제어할 수 있다.

15여개 팀들이 사이버위기 경보 기반 사이버 방어 훈련에 동시 참가 하였다. 이를 지원하기 위해 훈련 시나리오가 주입된 300여개의 가상머신이 생성되었다. 사이버위기 경보 단계에 맞추어 예방보안 5시간, 실시간대응 7시간, 사후대응 3시간 동안 훈련을 수행하였으며 사이버보안 역량을 강화하였다(Table 2.).

Table 2. Specification of scenarios of cyber defense exercise

	I	II	III
# of scenario	2	4	2
Time(hour)	5	7	3
Target OS	Win10 Win2016	Win10 CentOS7	Win10
Cyber resilience			
Identify	O		
Protect	O	O	
Detect		O	O
Respond		O	
Recover		O	

I : Proactive response
II : Real time response
III : Post response

VII. 결론 및 향후 연구

7.1 결론

본 논문에서는 국내에서 사이버공격을 대응하기 위한 체계로 구축된 사이버위기 경보 단계를 훈련 받을 수 있는 사이버 방어 훈련장을 제안 및 구축하였다. 본 사이버 방어 훈련장은 사이버위기 경보에 따라 예방보안, 실시간대응, 사후대응의 3단계로 나누어 훈련이 진행된다. 각 단계에 주어진 임무를 수행함으로써 훈련생들은 국내 실정에 맞는 사이버공격 대응 능력을 향상시킬 수 있다. 각 과정을 거치면서 사이버 회복력의 5가지 요소를 모두 훈련받을 수 있다. 향후, 본 연구의 사이버 방어 훈련장은 사이버위협에 대한 실전 훈련 수행을 통해 국가 · 공공기관의 사이버위협 대응 능력 향상에 큰 역할을 할 것으로 기대된다.

7.2 향후 연구

본 연구의 사이버위기 경보 기반 사이버 방어 훈련장은 대규모의 훈련생을 지원하기 위해 사이버 훈련장 환경의 확충과 다양한 훈련 시나리오가 필요하다.

60개 이상의 팀이 동시 접속하여 훈련을 수행하기 위해 3,000개 이상의 가상머신이 생성되어 운영되어야 한다. 이를 위해 우선 물리적인 시스템 확장이 필요하며 이들 가상머신을 자동 배포하고 네트워크 구성을 자동으로 관리하는 시스템이 필요하다. 이와 함께 훈련시 발생하는 대용량의 네트워크 트래픽을 처리하기 위한 효율적인 네트워크 구성이 필요하다. 또한 대규모의 팀인 200개 이상의 팀을 동시 지원하기 위해서는 현재 구축되어 있는 프라이빗 클라우드에서 퍼블릭 클라우드에서 동작하는 사이버 훈련장을 개발해야 한다.

다양한 사이버위협에 대한 사이버훈련을 수행하기 위해 100개 이상의 훈련 시나리오가 필요하다. 현재 보유하고 있는 14개의 훈련 시나리오를 늘려 다양한 사이버위협을 경험할 수 있는 실전 위주의 훈련 시나리오를 개발해야 한다. 훈련 대상 OS 플랫폼의 확장과 다양한 상황을 표현하기 위한 네트워크 환경도 지원할 계획이다.

References

[1] Cybersecurity & Infrastructure Security Agency, "Cyber Storm: Securing cyber space," https://www.cisa.gov/cyber-storm-securing-cyber-space

[2] The NATO Cooperative Cyber Defence Centre of Excellence, "Locked Shields," https://ccdcoe.org/exercises/locked-shields/

[3] European Union Agency For Cybersecurity, "Cyber Europe 2020," https://w

ww.enisa.europa.eu/topics/cyberexercises/cyber-europe-programme/cyber-europe-2020

[4] National Security Agency, "Cyber Defense Exercise (CDX)," https://apps.nsa.gov/iaarchive/programs/cyber-defense-exercise/index.cfm

[5] E. Seker and H.H. Ozbenli, "The concept of Cyber Defense Exercise (CDX): Planning, execution, evaluation," Proceedings of 2018 International Conference on Cyber Security and Protection of Digital Services, June 2018.

[6] W.M. Petullo, K. Moses, B. Klimkowski, R. Hand and K. Olson, "The use of Cyber-Defense Exercises in undergraduate computing education," Proceedings of 2016 USENIX Workshop on Advances in Security Education, pp. 1-8, Aug. 2016.

[7] National Cyber Security Center, "Cyber Crisis Alert," https://www.nis.go.kr:4016/AF/1_7_1_1/list.do

[8] D. Bodeau and R. Graubart, "Cyber resiliency design principles," 17-0103, MITRE, 2017.

[9] F. Dickson and P. Goodwin, "Five key technologies for enabling a Cyber-resilience framework," US45455119, IBM, 2019.

[10] J. Davis and S. Magrath, "A survey of cyber ranges and testbeds", DSTO-GD-0771, Cyber Electronic Warfare Division, 2013.

[11] P.W. Tsai, F. Piccialli, C.W. Tsai, M.Y. Luo, and C.S. Yang, "Control framework in network emulation testbeds: A survey," Journal of Computer Science, vol. 22, pp. 148-161, Sep. 2017.

[12] D.B. Fox, C.D. McCollum, E.I. Arnoth, and D.J. Mak, "Cyber wargaming: Framework for enhancing cyber wargaming with realistic business context," 16-J-00184-04, HSSEDI, Aug. 2018.

[13] I. Priyadarshini, "Features and architecture of the modern cyber range: A qualitative analysis and survey," Master Thesis, University of Delaware, Sep. 2018.

[14] E.C. Chaskos, "Cyber-security training: A comparative analysis of cyber-ranges and emerging trends," Master Thesis, National and Kapodistrian University of Athens, Mar. 2019.

[15] M.M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," Computer & Security, vol. 88, pp. 1-26, Jan. 2020.

[16] Virginia Cyber Range, https://www.virginiacyberrange.org

[17] Regent University, "Science, technology, engineering & math," https://www.regent.edu/programs/academicdegrees/science-technology-engineering-math/

[18] Wayne State University, "Wayne cyber range hub," https://wayne.edu/educationaloutreach/cyber-range/

[19] University of Central Arkansas, "Cyber range," https://nicerc.org/arcybersecurity/

[20] Georgia Cyber Center, "Cyber range," https://www.gacybercenter.org/services/cyber-range/

[21] GeorgiaCyber, "kinetic system," https://github.com/GeorgiaCyber/kinetic

[22] V. Giuliano and V. Formicola, "ICSrange: A simulation-based cyber range platform for industrial control systems," Proceedings of the 15th European Dependable Computing Conference, 2019.

[23] C. Pham, D. Tang, K.I. Chinen, and R. Beuran, "CyRIS: A cyber range

instantiation system for facilitating security testing," Proceedings of the 7th International Symposium on Information and Communication Technology, pp. 251-258, Dec. 2016.
[24] CROND, https://www.jaist.ac.jp/misc/crond/achievements-en.html
[25] R. Beuran, D. Tang, C. Pham, K.I. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: CyTrONE," Computers and Security, vol. 78, pp. 43-59, Sep. 2018.
[26] A.K. Amorin, B. Shekar, and C.L. AlAufi, "CloudWhip: A tool for provisioning cyber security labs in the amazon cloud," Proceedings of 2014 International Conference on Security and Management, 2014.
[27] I.D. Alvarenga, M.B. Duarte, "RIO: A denial of service experimentation platform in a future internet testbed," Proceedings of 7th International Conference on the Network of the Future, Jan. 2016.
[28] Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin and X. Cui, "A real-time correlation of host-level events in cyber range service for smart campus," IEEE Access, vol. 6, 35355-35364, Jun. 2018.
[29] Norwich University Applied Research Institutes, "DECIDE Platform," https://nuari.net/
[30] P. Celeda, J. Cegan, J. Vykopal, and D. Tovarnak, "KYPO - A platform for cyber defense exercise," STO-MP-MSG-133, NATO Science and Technology Organization, 2015.
[31] J. Vykopal, R. Oslejsek, P. Celeda, M. Vizvary, and D. Tovarnak "KYPO cyber range: Design and use cases," Proceedings of 12th International Conference on Software Technologies, 2017.
[32] M. Rosenstein and F. Corvese, "A secure architecture for the range-level command and control system of a national cyber range testbed," Proceedings of the 5th USENIX Workshop on Cyber Security Experimentation and Test, pp. 1-9, Aug. 2012.
[33] B.C. Ferguson and A. Tall, "National cyber range overview," Proceedings of 2014 IEEE Military Communications Conference, Oct. 2014.
[34] Swedish Defence Research Agency, "CRATE, cyber range and training environment," https://www.foi.se/en/foi/resources/crate-cyber-range-andtraining-environment.html
[35] N. Hatty, "Representing attacks in a cyber range," Mater Thesis, Linkoping University, Jun. 2019.
[36] Austrian Institute of Technology, "Cyber range & training," https://www.ait.ac.at/en/research-topics/cyber-security/cyber-range-training/
[37] M. Frank, M. Leitner, and T. Pahi, "Design considerations for cyber security testbeds: A case study on a cyber security testbed for education," Proceedings of 15th International Symposium on Dependable, Automatic and Secure Computing, pp. 38-46, Nov. 2017.
[38] CybExer Technologies, "Cyber range platform," https://cybexer.com
[39] silensec, "Cyber ranges," https://www.silensec.com/cyber-range
[40] ThinkCyber, "Cyberium arena," https://www.thinkcyber.co.il/
[41] IBM, "X-force command cyber tactical operations center," https://www.ibm.com/security/services/managed-security-services/xforce-command-cyber-tactical-operations-center

[42] Merit, "Cyber education training," https://www.merit.edu/security/training/
[43] Cybergym, https://www.cybergym.com
[44] Baltimore Cyber, "Baltimore cyber's range," https://www.baltimorecyberange.com/copy-of-about
[45] CyberCENTS, "CENTS," https://cybercents.com/
[46] Florida Cyber Range, https://floridacyberrange.org/
[47] Circadence Cyber Range, https://www.circadence.com/
[48] Cyber Warfare Range, https://www.azcwr.org/
[49] K. Hara, "Cyber range CYBERIUM for training security meisters to deal with cyber attacks," Fujitsu Scientific & Technical Journal, vol. 55, no. 5, pp. 59-63, 2019.
[50] Airbus, "CyberRange," https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/
[51] Medium, "AWS cyber range," https://medium.com/aws-cyber-range
[52] P. Qiu, "Cisco cyber range", 2016.
[53] Keysight, "Cyber-range services", https://www.keysight.com/us/en/products/services/network-security-services/cyber-range-services.html
[54] SimSpace, "SimSpace cyber range", 2015 Annual Computer Security Applications Conference, Dec. 2015.
[55] R. Chadha, T. Bowen, Y.J. C.J. Chiang, Y.M. Gottlieb, A.Poylisher, A. Sapello, C. Serban, S. Sugrim, G. Walther, L.M. Marvel, E.A. Newcomb, and J. Santos, "CyberVAN: A cyber security virtual assured network testbed", Proceedings of 2016 IEEE Military Communications Conference, Nov. 2016.
[56] Raytheon Technologies, "Cyber range," https://www.raytheon.com/cyber/capabilities/range
[57] Cyberbit, "Cyber range," https://www.cyberbit.com/solutions/cyber-range/
[58] A. Ashok, S. Krishnaswamy, and M. Govindarasu, "PowerCyber: A remotely accessible testbed for cyber physical security of the smart grid," Proceedings of 2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, Sep. 2016.
[59] A.F. Browne, S. Watson, and W.B. Williams, "Development of an architecture for a cyber-physical emulation test range for network security testing," IEEE Access, vol. 6, pp. 73273-73279, Nov. 2018.
[60] C. Javali and G. Revadigar, "Network web traffic generator for cyber range exercises," Proceedings of IEEE 44th Conference on Local Computer Networks, 2019.
[61] G. Kavallierators, S.K. Katsikas, and V. Katsikas, "Towards a cyber-physical range," Proceedings of the 5th on Cyber-Physical System Security Workshop, pp. 25-34, Jul. 2019.
[62] OpenStack, https://www.openstack.org
[63] VMware, "vSphere," https://www.vmware.com/products/vsphere.html
[64] KVM, https://www.linux-kvm.org/page/Main_Page
[65] Amazon Web Service, https://aws.amazon.com
[66] Azure, https://azure.microsoft.com
[67] A.S. Raj, B. Alangot, S. Prabhu, and K. Achuthan, "Scalable and lightweight CTF infrastructures using application containers," Proceedings of 2016 USENIX Workshop on Advances in Security Education, pp. 1-8, Aug. 2016.
[68] DEFCON, https://www.defcon.org
[69] J.S. Kim, Y.J. Maeng, and M.S. Jang, "Becoming invisible hands of national

live-fire attack-defense cyber exercise," Proceedings of 2019 IEEE European Symposium on Security and Privacy Workshops, pp. 77-84, Jun. 2019.

[70] R. Beuran, T. Inoue, Y. Tan, and Y. Shinoda, "Realistic cybersecurity training via scenario progression management," Proceedings of 2019 IEEE European Symposium on Security and Privacy Workshops, pp. 67-76, Jun. 2019.

[71] E. Trickel, F. Disperati, E. Gustafson, F. Kalantari, M. Mabey, N. Tiwari, Y. Safaei, A. Doupe, and G. Vigna, "Shall we play a game? CTF-as-a-service for security education," Proceedings of 2017 USENIX Workshop on Advances in Security Education, pp. 1-10, Aug. 2017.

[72] J. Yuen, "Automated cyber red teaming," DSTO-TN-1420, Australian Government Department of Defence, Apr. 2015.

[73] A. Applebaum, D. Miller, B. Strom, C. Korban, and R.Wolf, "Intelligent, automated red team emulation," Proceedings of the 32nd Annual Computer Security Applications Conference, pp. 363-373, Dec. 2016.

[74] M. Pihelgas, "Design and implementation of an availability scoring system for cyber defense exercises," Proceedings of the 14th International Conference on Cyber Warfare and Security, pp. 329-337, Feb. 2019.

[75] M. Andreolini, V.G. Colacino, M. Colajanni, and M. Marchetti, "A framework for the evaluation of trainee performance in cyber range exercises," Mobile Networks an Applications, vol. 25, no. 2, pp. 236-247, Dec. 2019.

[76] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National initiative for cybersecurity education (NICE) cybersecurity workforce framework," 800-181, NIST, Aug. 2017.

[77] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. Mcquaid, "Developing cyber resilient systems," 800-160, NIST, Nov. 2019.

〈저자소개〉

최 영 한 (Younghan Choi) 정회원
2002년 2월: 한양대학교 전자공학과 졸업(학사)
2004년 2월: KAIST 전자공학과 졸업(공학석사)
2015년 2월: 고려대학교 정보보호대학원 졸업(공학박사)
2019년 2월: 한국방송통신대학교 법학과 졸업(학사)
2004년 2월~현재: 한국전자통신연구원 부설연구소 책임연구원
2020년 2월~현재: 사이버안전훈련센터(실장)
〈관심분야〉 사이버보안, 사이버훈련, 사이버법률

장 인 숙 (Insook Jang) 정회원
1998년 2월: 경북대학교 문헌정보학과 졸업(학사)
2001년 2월: 경북대학교 컴퓨터과학과 졸업(이학석사)
2017년 2월: 충남대학교 컴퓨터공학과 박사 수료
2001년 3월~현재: 한국전자통신연구원 부설연구소 책임연구원
〈관심분야〉 사이버보안, 사이버훈련, 정보보안 교육

황 인 택 (Inteck Whoang) 정회원
2010년 8월: 중앙대학교 컴퓨터공학과대학원 졸업(공학박사)
2010년 12월: 한국전자통신연구원 부설연구소 입소
2019년 1월~현재: 사이버안전훈련센터 책임연구원
〈관심분야〉 사이버보안, 사이버훈련, 정보보안 체계

김 태 균 (Taeghyoon Kim) 정회원
1995년 2월: 충남대학교 전자공학과 졸업(학사)
1997년 2월: 충남대학교 전자공학과 졸업(석사)
1997년 3월~2004년 8월: 한국 마이크로소프트 연구원
2004년 8월~현재: 한국전자통신연구원 부설연구소 책임연구원
〈관심분야〉 사이버보안, 사이버훈련

홍 순 좌 (Soonjwa Hong) 정회원
1989년 2월: 숭실대학교 전산과 졸업
1991년 2월: 숭실대학교 전산과 석사
2005년 8월: 충남대학교 컴퓨터과학과 박사
1991년 2월~2000년 1월: 국방과학연구소(ADD) 선임연구원
2000년 2월~현재: 한국전자통신연구원 부설연구소 책임연구원
〈관심분야〉 사이버보안 인력양성 정책, 미래 IT・보안기술, 사이버보안 기술・위협 분석, 국내외 정보보호 법・정책

박 인 성 (Insung Park) 정회원
2004년 9월: 경북대학교 컴퓨터과학과 졸업(석사)
2003년 4월~현재: 한국전자통신연구원 부설연구소 선임연구원
〈관심분야〉 사이버보안, 사이버훈련

양 진 석 (Jinseok Yang) 정회원
2003년 2월: 성균관대학교 정보공학과 학사 졸업(학사)
2005년 2월: 성균관대학교 컴퓨터공학과 졸업(석사)
2012년 2월: 성균관대학교 컴퓨터공학과 수료(박사)
2016년 9월~2017년 2월: 고려대학교 사이버국방학과 겸임교수
2005년 2월~현재: 한국전자통신연구원 부설연구소 선임연구원
〈관심분야〉 사이버훈련, 네트워크보안

권 영 재 (Yeongjae Kwon) 정회원
2007년 2월: 영산대학교 컴퓨터공학과 졸업(학사)
2012년 3월~현재: 충남대학교 전자전파정보통신공학과 석박사통합과정
2015년 8월~현재: 한국전자통신연구원 부설연구소 선임기술원
〈관심분야〉 정보보호, 사이버훈련

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