ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

사이버 레인지 운용 방안 연구☆

A Study of Administration of Cyber Range

김 대 식1* 김 용 현1
Daesik Kim Yonghyun Kim

요 약

전 세계를 활동영역으로 하는 현대 사회의 사이버전의 공격 기술은 날로 보다 정교해지고 새로운 공격의 출현 주기가 점점 짧아지고 있으며 이를 해결할 방어 기술 및 전문 인력은 매우 부족한 실정이다. 이러한 문제를 해결하기 위한 노력 중의 하나로 세계 각국은 사이버전을 대비하는 테스트 베드로써 사이버 레인지를 고려하고 있다. 본 논문은 사이버 레인지의 해외사례 및 유사 체계를 조사하면서 각종 요소를 수집 및 분석하였으며 시스템 엔지니어링 과정을 통하여 이를 체계적으로 분류하였다. 그 과정 중에 유도되는 임무 및 운영 개념을 아키텍처 프레임워크에 맞게 설정하였으며 사이버 레인지의 논리적 아키텍처를 작성하였다. 작성된 아키텍처를 활용하여 방어 기술 및 전문 인력 확보란 두 가지 목표를 달성하는 동시에 효율성 및 지속성을 확보하는 운용 방안을 제시하였다.

☞ 주제어 : 사이버 레인지, 테스트 베드, 시스템 엔지니어링

ABSTRACT

In the whole world the Attack Technologies of cyber warfare in modern society are growing faster and complicated. The frequency of the new attacks is shorter than before day by day. The defense technologies and experts against these attacks are very few. One of answers to solve these problems is the cyber range as a test-bed to prepare the cyber warfare considered by many countries. This paper examines the foreign cases and similar systems, collects and analyzes various attributes for cyber range. Finally it refines them through system engineering processes. In these processes missions and concepts for administration are set with architecture framework. The logical architecture is designed. Based on designed architecture two goals, defense technologies and procurement of experts, are established. And it shows effective and persistent administration of cyber range.

☞ keyword : Cyber Range, Test-bed, System Engineering

1. 서 론

미국을 비롯한 세계 여러 나라는 기하급수적으로 늘어나는 사이버 공격에 대응하기 위해 새로이 인터넷 및 관련 통신 망, 내장(embedded) 및 기반 환경 전반에 걸쳐 사이버 전장을 규정하고 사이버 작전을 수립하는 등 여러 가지 대책을 세우고 있다. 그 중의 하나로 실전에 배치할 수 있는 능력을 갖춘 사이버 인력의 양성을 위한 테스트 베드를 준비하고 있다[1,2].

사이버 레인지는 좁은 의미로는 사이버 레인지를 구성하는 하드웨어 및 소프트웨어 환경을 의미한다. 넓은 의미로는 운영 및 관리 체계를 포함하고 교육 훈련 체계까지를 의미한다. 미국 DARPA의 NCR(National Cyber Range)[2-4], 영국이나 유럽의 사이버 레인지[5]는 넓은 의미의 개념이며 미 USC-ISI의 연구용 테스트베드인 Deterlab[6]이나 IXIA사의 BreakingPoint[7] 및 Spirent사의 Avalanche[8] 등의 상용 도구는 좁은 의미의 사이버 레인지이다.

대표적인 사이버 레인지로는 미국에서 2009년부터 2012년 동안 개발한 NCR이 있다. 민, 군, 관의 사이버 레인지를 통합한 광대한 개념으로 국방 훈련 뿐 만 아니라 상용 제품의 시험 및 대학이나 연구소에서 개발한 기술의 실험에도 활용되고 있다. NCR은 보안 시설을 갖추고 혁신 기술을 수용하며 재현 가능한 프로세스를 제공하고 사이버 레인지의 숙련된 요원을 지원한다.

사이버 레인지의 개념은 군에서만 활용될 뿐 아니라 오히려 미국의 사이버 방어 대회(CDC: Cyber Defense Competition)에서도 공정한 시합의 운영과 평가를 위해 활용되고 있다.

1 Agency for Defense Development, Seoul, 05661, Korea.
* Corresponding author (dkim@add.re.kr)
[Received 5 March 2017, Reviewed 23 June 2017(R2 14 August 2017), Accepted 1 September 2017]
☆ 본 논문은 2017년도 한국인터넷정보학회 추계학술발표대회 우수 논문 추천에 따라 확장 및 수정된 논문임

미국은 각종 사이버 레인지를 통합하려는 노력을 하여 왔다. NCR은 서로의 입장이 다른 민·군·관의 사이버 레인지를 통합한 개념이다. 훈련과 교육을 같은 테스트 베드의 영역에 포함하며 제품 시험 및 훈련 교과 과정 선정의 임무들까지도 포함하는 매우 광범위한 체계이다. 미 MITRE 연구소는 사이버 훈련의 목적, 시나리오, 보고 및 평가 절차, 네트워크 아키텍처, 도구, 강평 등 전 수명 주기를 연구하고 있다[9]. 또한 미 DISA 연구소의 Information Assurance Range[10]와 같은 다양한 레인지 분야와 공조를 하고 있다.

본 논문의 구성은 다음과 같다. 제 2장에서는 다양한 사이버 레인지들을 조사하여 공통점 및 특징을 찾아내어 사이버 레인지 구조를 제시하고 구축 방향을 설정하였다. 제 3장에서는 사이버 레인지의 구성요소를 식별하였다. 제 4장에서는 사이버 레인지의 여러 요소들을 고려한 운용 방안을 제시하였다.

2. 사이버 레인지의 개요

2.1 사이버 레인지의 공통점

사이버 레인지와 관련된 해외 정부 및 군 조직이나 일반 회사들의 사이버 레인지를 언급한 자료들을 조사해 보았다. 연구 기관은 사이버 기술을 검증하기 위한 테스트 베드이며 군부대 및 관련 기관은 사이버 인력을 훈련하고 양성하기 위한 테스트 베드로 사이버 레인지를 인식한다. 반면에 일반 회사들은 사이버 관련 제품을 테스트하기 위한 테스트 베드로 인식한다. 또한 보안 제품 솔루션의 하나로 사이버 레인지를 언급한다.

그러나 전 세계의 사이버 레인지는 하나의 공통점을 가진다. 사이버전을 위한 테스트 베드라는 것이다.

사이버 레인지를 이용하는 사용자들은 첫 번째로 공격을 담당하여 사이버 레인지의 훈련 대상 시스템을 공략하려는 레드 팀이 있다. 두 번째로 침입, 파괴 및 탈취에 대항하여 훈련 대상 시스템을 유지시키려는 블루 팀이 있다. 마지막으로 사이버 레인지의 안정적인 운용과 훈련 대상 시스템 및 사용자 관리를 담당하는 화이트 팀으로 구분된다[11].

2.2 사이버 레인지 특징

사이버 레인지는 다른 과학 및 기술 분야의 실험실과는 진행 방법, 실험 종류 및 분석 등 여러 측면에서 구별되는 고유의 특징들이 있다.

실험은 먼저 분석 종류 및 항목을 구체적으로 설정한 후 진행한다. 그렇지만 사이버전은 이미 알고 있는 공격보다도 모르는 공격(Zero-Day Attack)을 더 많이 시도하는 전쟁이다. 또한 주력으로 사용하는 무기(주로 공격 위주의 해킹 도구)의 교체시기도 매우 빠르며 랜섬웨어(Ransom ware)와 같이 전에는 없었던 새로운 개념의 공격이 생겨난다.

실험실은 각각 실험 종류가 분명하게 정해져 있으며 해당 실험 장비들이나 실험 방법이 비교적 명확하다. 사이버전에서는 프로토콜 분석 도구, 빅 데이터 분석 도구 등과 같이 공격 장비와 방어 장비에 모두 포함되는 경우도 있다.

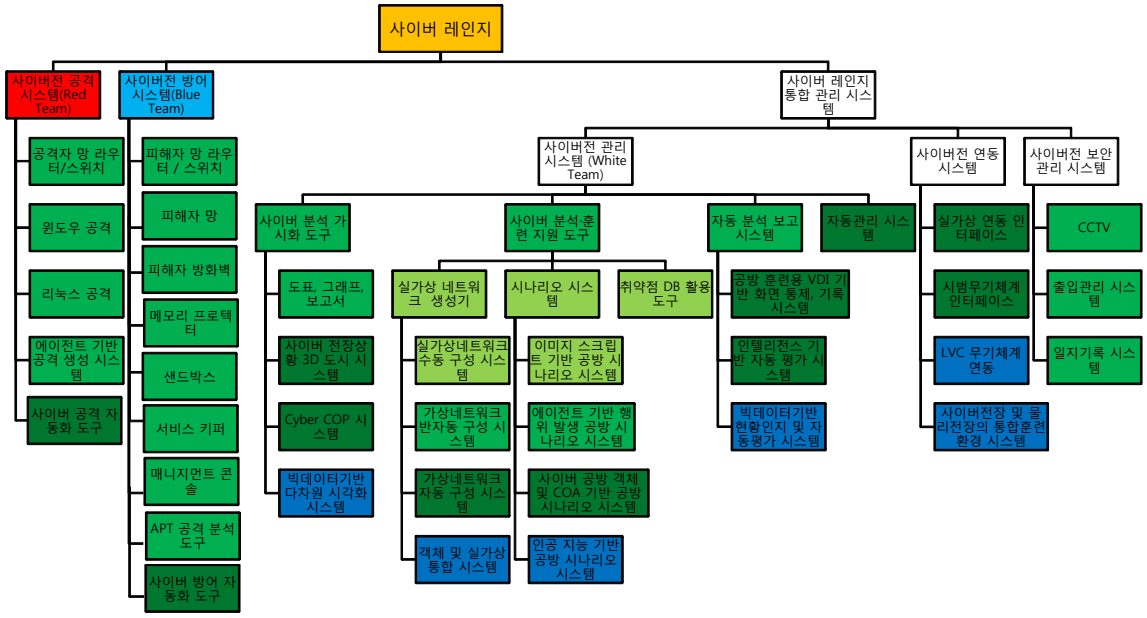
실험은 실험 의뢰자의 의뢰를 받아 실험 전에 실험계획서를 만들고 실험이 끝나면 비교적 명확한 실험결과서 및 실험결과 보고서가 나온다. 사이버전은 사건이 벌어진 원인과 경과를 규명하기 어려운 경우가 많다. 사이버 레인지를 통한 시뮬레이션으로 그 사건을 재현하여 반복적으로 여러 다양한 원인을 찾고 분석하고 최적이 아니더라도 타당한 대책을 마련해야 한다. 실험 결과의 해석이 명쾌하지 않는 경우도 다수 존재한다. 이런 경우의 시험결과 처리를 위한 논의 및 평가가 사이버 레인지의 운영 과정 중에 필요하다.

따라서 아직까지는 사이버 레인지는 일반인을 대상으로 하기보다는 전문가 혹은 관련 사업 종사자가 직접 수행해야 할 것이며 그 결과도 관련 당사자가 해석을 하고 받아들여야 할 것이다.

사이버 레인지는 훈련에도 사용된다. 레드 팀이나 블루 팀 같은 용어도 그 기원은 미군 훈련에서 사용되는 용어이다. 미군은 사이버 레인지 이전에도 레인지를 훈련장 개념으로 사용해 왔으며 사이버 레인지도 그 연장선상에서 보는 성격이 강하다. 우리나라의 사이버 전장 상황은 전장 운영 규모 및 비용에서 미국과 많은 차이가 나기 때문에 그 개념을 그대로 적용할 수 없다.

2.3 사이버 레인지 체계 구조

사이버 레인지 체계는 단기간에 구성되는 것이 아니라 장기적인 안목으로 구성이 되어야 한다. 장기적으로 운영되고 개선되는 체계는 해마다 달라지는 기술 성숙도로 인하여 추진하려는 기술과 적용해야 하는 기술이 달라지는 경우가 많이 발생한다. 하지만 사이버 레인지의 도입이 시급한 현실에서 현재 기술로도 충분히 구현 가능한 것들을 먼저 즉시 반영하여 진행하는 것이 원칙이



(그림 1) 사이버 레인지 구조
(Figure 1) Cyber Range Structure

다. 인공지능을 이용한 퍼징, 스캐닝 등의 공격기술, 3D 기술을 이용한 다차원 토폴로지 화면 도시나 화면 조작 기술, 심지어는 심층 분석을 위한 홀로그래피까지 장래 기술 성숙이 예측되는 기술들의 도입을 사전에 미리 고려한다. 또한 분석을 위해 방대한 데이터를 다루기 위한 특별한 기술이 필요하다면 사이버 레인지에 적용하는 것이 타당할 것이다.

신기술을 도입함으로 빠르고 정확한 판단력이 가능하고 적보다 일분일초라도 빠른 선제공격으로 타격을 입힌다면 사이버 레인지 구축에 드는 비용이 아깝지 않을 것이다. 물론 미래 기술만 바라보며 현존하는 기술을 쓰지 않는 것은 시스템이 완성이 된 후에야 사이버 레인지를 사용할 수 있다는 점에서 매우 비효율적이다.

현존하는 기술을 사용하여 빠른 적용이 가능하게 함과 동시에 미래지향적인 설계를 통해 신기술로 빠르게 대치할 수 있는 시스템 공학 기법, 즉 모듈방식의 설계라든지 콤포넌트 방식의 조립식 설계방식을 적용시킨다. 현재에도 사용가능한 동시에 향후 미래기술로 대치할 수 있는 열려있는 시스템 아키텍처를 설계하고 적용하여 구축하는 것이 바람직 할 것이다[12]. 이를 위하여 사이버 레인지를 위한 기술들을 식별하여 계층적으로 분류하였다. 그림 1에서는 사이버 레인지의 운용에 필요한 시스템을 구성한 구조를 제시하였다[11].

2.4 사이버 레인지 구축 방향

사이버 레인지는 가상, 실, 구성 환경을 모의할 수 있는 LVC(Live-Virtual and Constructive, 실가상) 연구 환경의 구축을 시작한다. 중간 단계로 무기체계가 결합한 복합 환경을 구축한다. 최종적으로 민·군 통신망 및 무기체계와 연동까지 실험을 할 수 있는 운용환경을 구축하는 것으로 방향을 설정하였다. 이에 따라 시나리오도 스크립트 기반에서 에이전트 기반으로, 반자동(semi-automatic)에서 COA(Course-of-Action)기반 자동생성 시나리오로 점차적으로 개발한다. 최종적으로는 가상 네트워크가 자동으로 생성이 되며 실 환경과 연동되는 통합 시나리오를 저작하는 단계까지 구축이 될 것이다.

정보 수집 분석도 기술검증에서 좀 더 인텔리전스 기반 인지가 가능할 것이고 각 팀이나 개개인의 평가가 인텔리전스를 기반으로 자동으로 이루어질 것이다. 시각화도 마찬가지로 시험결과가 이차원 그래프 및 텍스트 보고서로 보여 진다. 점차 3D로 인식가능하고 다층구조로 상황판단이 가능하며 데이터를 필요에 따라 분류하고 분석하고 제시하는 빅데이터 기반 다차원 시각화 환경을 갖추는 것을 기본으로 하고 있다[13].

3. 사이버 레인지 구성 요소

3.1 사용자 유형

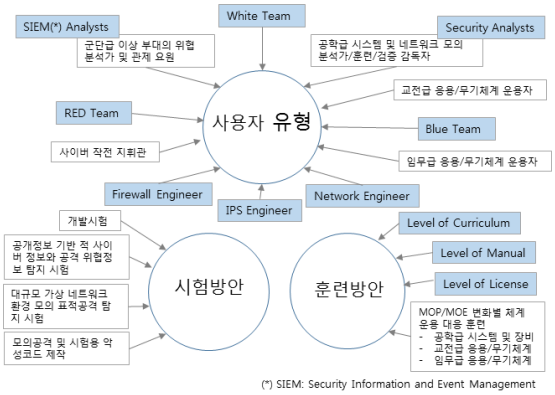
사용자 유형은 취약점을 파악하여 침투하기 위해 다양한 공격을 시도하는 레드 팀, 방어 환경을 구축하고 공격 대응을 탐지하여 대응을 하려는 블루 팀, 양측의 공방을 평가, 운영 및 관리를 위한 화이트 팀으로 나누며, 경우에 따라 블루 팀의 서비스를 제공받는 일반 사용자의 역할을 하는 그린 팀이 추가되기도 한다. 그 외에도 사용자 유형은 그림 2와 같이 각 분야에 따라서 또는 원하는 수준에 따라서 세 가지 범주에 들어가는 경우라도 별도로 세분화하여 분류할 수 있다. 이 구분은 규모나 목적에 따라서 방어 실험 또는 방어 훈련을 목적으로 할 경우에는 특별히 레드 팀에 모의 침투(Penetration Test) 전문가가 참여하여 블루 팀의 역량을 점검할 수 있다. 이러한 경우에는 화이트 팀의 참여자를 동시에 겸하여 사이버 전장을 관리할 수 있다. 그림 3에서는 다양한 목적의 사용자 유형들이 사이버 레인지에 참여하는 것을 보여준다.

3.2 훈련 방안

사이버 레인지는 각각의 훈련 대상에 맞추어 수준을 조절할 수 있다. 사이버 훈련 수준은 초보자에서 숙련자까지를 고려함은 물론 집단 훈련뿐만 아니라 개인의 실력향상을 위한 자발적 훈련 개념을 갖추고 있다. 또한 사이버 레인지는 여러 훈련을 동시에 치러낼 수 있다. 비교적 단순하다고 여겨지는 컴퓨터 바이러스 대처 훈련에서부터 실 환경에서는 매우 오랜 시간이 소요되는 APT 공격 및 대응 방안을 상대적으로 짧은 시간 안에 훈련을 할 수 있다. 그림 2에서는 수준별 훈련 방안을 보여준다. 사이버 레인지 각 팀 내부의 참여자는 사이버 레인지에서 제공되는 것 이외의 공격 혹은 방어의 개별 장비 및 소프트웨어를 가지고 실험에 임할 수도 있다. 화이트 팀은 각 팀 및 개개인을 관리하기 위한 통합 관리 시스템도 함께 갖추기도 한다. 이때 사이버 레인지는 테스트 사전에 이를 수용할 수 있는 준비 기간이 필요하다.

3.3 시험 방안

또한 사이버 레인지는 사이버 관련 장비나 기술을 시험하기 위해서 쓰인다. 사이버 관련 인터넷 기술이 빠른 속도로 발전하고 있는 만큼 그 소프트웨어의 설계 결함, 비의도적 오류, 취약점 등을 이용한 공격이 물리적 환경



(그림 2) 사이버 레인지 구성 요소
(Figure 2) Cyber Range Components

에도 영향을 미친다[14]. 사이버 레인지는 이에 적절하게 대응하여 신기술을 신속히 적용하고 사용할 수 있는 유연함을 갖추어야 한다. 그림 2에서는 사이버 레인지를 통하여 할 수 있는 다양한 시험을 제시한다.

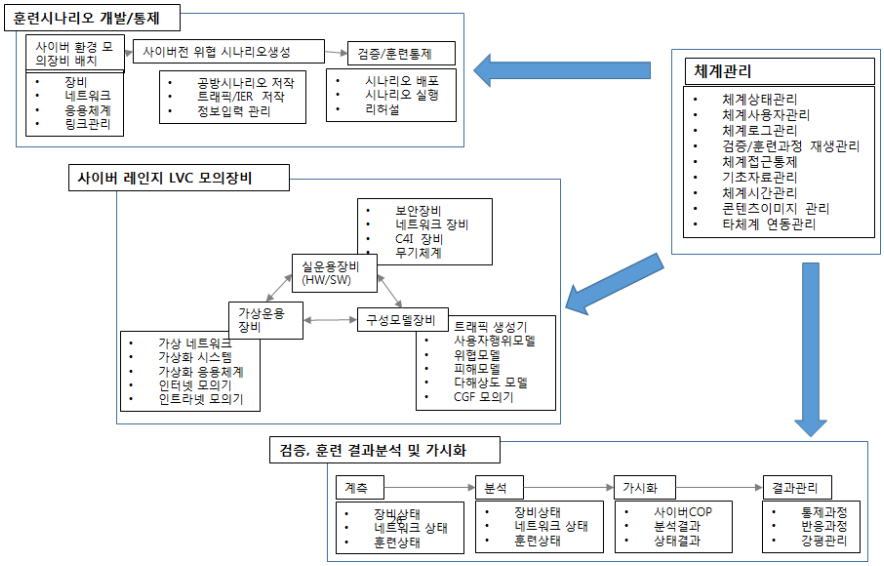
3.4 HW/SW 구성환경

사이버 레인지는 실제 사이버전 환경과 매우 유사한 인터넷 환경을 제공하며, 지능형 지속 공격(APT), 서비스 거부 공격(DDOS) 등을 포함한 다양한 사이버전 공격 시나리오 및 도구를 지원하며, 사이버 레인지 내부의 행위가 외부로 누출될 가능성을 사전에 봉쇄하며, 여러 훈련 및 시험 대상이 동시에 이용할 수 있으며, 시험 및 훈련 중 발생한 모든 행위에 대한 모니터링 및 기록 기능을 제공한다. 그중 일례로 Jason [9]이 언급하였던 사이버 훈련의 전 주기에 걸쳐 필요한 기능을 식별한 후, 시스템의 기능 식별 및 아키텍처 생성에 필요한 태스크 목록(UJTL: Universal Joint Task Lists)[11]을 작성한 다음 운영개념에 필요한 기능을 통합 및 세분화하여 정리한 환경을 그림 3에 제시하였다.

4. 사이버 레인지 운용 방안

4.1 운용 방안 형성 과정

사이버 레인지의 운용 방안 도출을 위하여 각종 해외 자료 및 필요 요구사항을 수집 및 분석하여 최적의 태스크 목록을 뽑아내고 각 요소의 기능을 개념에 맞게 고려한 아키텍처를 작성하고 향후 기술 발전 요소를 프레임



(그림 3) 사이버 레인지 HW/SW 구성 환경
(Figure 3) Cyber Range HW/SW Configurations

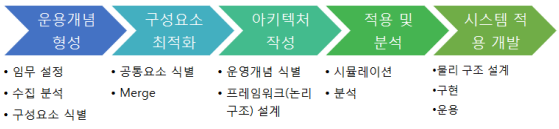
워크 고려 요소에 포함하여 유연성을 가지도록 만든다 [11]. 시뮬레이션을 통한 아키텍처의 적용 시험을 통하여 요소 중복, 데드락, 고립 등의 논리적 문제점을 해결한 후 시스템 개발에 적용하며 이때의 운용 방안을 그림 4로 도식화하여 제시하였다.

4.2 필요 운용 기능 구조 식별

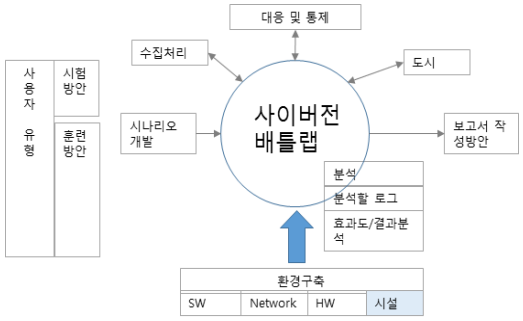
각 요구사항을 분석하여 사이버 레인지에 필요한 기능을 식별한다. 최상위 레벨에서 사용자 유형, 시험방안, 훈련방안에 따른 시나리오 개발, 수집처리, 대응 및 통제, 도시, 분석, 보고서 기능이 식별되었으며 이를 구현하기 위한 환경도 식별이 되었다. 그림 5는 최상위 레벨의 논리적 사이버 레인지 운용 기능 구조로 이 다이어그램 외에도 세분화된 기능도 식별되어 있다.

4.3 운용 방안 고려 사항

각각의 사용자 유형에 따라 사이버 레인지를 제공하는 운용 방안을 달리한다. 예를 들어 그림 6와 같이 주로 관리차원에서는 화이트 팀의 개념을 위주로 운용 방안을 고려한다. 화이트 팀은 사이버 레인지 과정 중의 실습용 시스템과 네트워크를 구상하고 배치하며 실험 장비의 실습 환경을 준비하고 정해진 시나리오대로 네트워크 트래

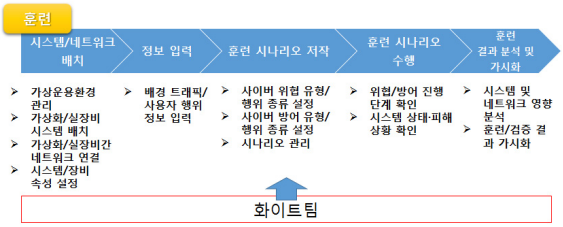


(그림 4) 사이버 레인지 구축 방안
(Figure 4) Cyber Range Building Methodology



(그림 5) 사이버 레인지 기능 구조
(Figure 5) Cyber Range Functional Architecture (Top Level)

픽이나 행위 정보를 발생시킨다. 또한 훈련 시나리오를 수행하면서 로그 정보를 수집하고 시각정보로 이를 표현하며 분석/검증 도구를 지원한다.



(그림 6) 훈련을 위한 화이트 팀의 운용 절차
(Figure 6) Administrative Procedures of White Team for Training

그 밖에도 사이버 레인지에는 고려해야 할 요소들이 많이 있다. 각각의 기능을 사용자 유형, 시험 방안, 훈련 방안에 맞추어 운용 방안을 고려해야 한다. 각 팀의 수준에 따라 차이는 있으나 일반적으로 블루 팀의 운용 절차는 다음과 같다.

1) 망의 상태를 파악한다.
2) IPS/IDS, 방화벽 등의 방어 시스템의 구성항목 상태를 파악한다.
3) 도시화면의 임계치를 조정하는 등의 준비 및 모니터링을 하면서 이상 징후를 탐지한다.

그 외에도 때로는 트래픽 소스를 추적하기도 해야 할 것이다. 다른 구성 요소들도 운용을 함에 있어서 표 1과 같이 각각의 유형을 고려한 사항을 파악하여야 할 것이다.

(표 1) 유형별 운용 고려 사항
(Table 1) Considerations for Each Type

유형	운용 고려 사항
공방 훈련	사용 가능한 사이버 도구의 확보 및 시범연동 등
개발기술 검증	검증용 시나리오를 제작, 사용자 편의성을 고려한 시나리오 저작 도구를 지원, 웹기반 관리 인터페이스 등
개발기술 시험평가	기존 연구 결과와 진행 중인 기술 시스템과의 연동, 시각화 등
관리	보안 취약점 점검 절차, 소프트웨어 개발 보안 절차, 소프트웨어 보안약점 진단 절차, 인터넷 주소 분쟁해결 절차, 분석 및 실험 지정 절차, 분석 절차, 관리체계 운영 절차, 개인정보의 기술적·관리적 보호 절차 등

5. 결 론

본 논문을 통하여 사이버 레인지의 운용 방안 개념을 제시하였다. 미국의 경우에도 처음부터 국가차원에서 모든 것을 만족하는 것을 만들지 않고 각 기관별로 사이버 레인지를 구성하였다. 통합 개념의 NCR도 역시 많은 시행착오를 거쳐서 모델링 과정을 구현하였다.

효과적이고 적합한 운용 방안을 구현하기 위하여 사이버전에 관련된 사업들과 밀접한 관계를 가지고 협력을 해야 한다. 예를 들어 사이버전이라면 거의 공통적으로 활용되는 취약점 DB나 악성코드 DB를 공통 플랫폼으로 활용할 수 있을 것이고, 서로 다른 상이한 용어로 같은 개념을 설명하는 일이 없도록 용어의 표준화 작업도 필요할 것이다. 또한 지금 설정되어 있는 목표도 구현 단계에서 실험실의 수요가 확정지어질 때 활용범위나 소요량 등이 변동될 수 있다는 점을 명심한다. 또한 첨단 빅 데이터 기법 등 신규 기술 도입이 필요한 경우도 있다.

각 기관이나 조직의 환경에 적합한 고유의 사이버 레인지 운용 방안을 마련하는 것이 최적화 측면에서는 적합할 것으로 생각된다. 그렇지만 미국 NCR 경우와 같이 여러 조직의 사이버 레인지를 통합해야 하는 경우도 있을 수 있다. 그렇다면 초기 단계부터 시스템 공학 기법중의 하나인 시스템 아키텍처 프레임워크를 기반으로 논리 구조 및 아키텍처를 설계하여야 한다. 그리고 이러한 설계들을 바탕으로 한 개방적이고 상호 호환적인 시스템을 점진적으로 구현하는 것이 바람직할 것이다.

참 고 문 헌(Reference)

[1] Joint-Pub 3-12(R), Cyberspace Operations, U.S.-Military, National Information Security Strategy, 2013.
[2] https://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf, DARPA NCR Fact Sheet, 2012.
[3] https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf, National Cyber Range Overview, Feb. 24, 2015.
[4] DISA-JITC/JTG1, DoD Information Assurance Range: A Venue for Test and Evaluation In Cyberspace, Aug., 2011.
[5] M. P. Lindgreen, Roadmap for the MoD Cyber Test Range, Master Thesis, Defence Materiel Organisation, Delft TopTech, Sept 10, 2012

[6] Terry Benzel, The Science of Cyber Security Experimentation: The DETER Project, In Proceedings of the Annual Computer Security Applications Conference (ACSAC '11), Orlando, Florida, December 2011.
[7] Whitepaper, 915-6729-01 Rev. A, Cyber Range: Improving Network Defense and Security Readiness : Real-World Attack Scenarios for Cyber Security Training, IXIA co., Aug., 2014
[8] Whitepaper, Rev A. Operational Impact of Cyber Range Elements, Simulations and Realism, Spirent co., Aug., 2014.
[9] Jason Kick, Cyber Exercise Playbook, MITRE, Nov. 2014.
[10] David Robinson, DARPA Initiatives in the Cyber Experimentation Domain National Cyber Range, Experimental Security Panoramas Workshop, July 14, 2011.
[11] Daesik Kim, et al., "A Study of an Conceptual Architecture for Cyber Range", Proceedings of KIMST Fall Conference, pp. 791-792, 2015.
[12] DoD Architecture Framework Version 2.0, U.S. Department of Defense, 28 May 2009.
[13] Daesik Kim and Yonghyun Kim, "A Study of Operational Concept for Cyber Range", Proceedings of KIMST Spring Conference, pp. 1192-1193, 2016.
[14] William C. Liu and Kevin M. McNeill, Overview of Cyber Experimentation & Test Ranges, BAE Systems, ICOTE Sept. 25, 2012.

◐ 저 자 소 개 ◑

김 대 식(Daesik Kim)
1988년 서강대학교 전자계산학과(공학사)
1990년 연세대학교 대학원 전산과학과(이학석사)
1990년~1998년 국방정보체계연구소 연구원
1990년~현재 국방과학연구소 책임연구원
관심분야 : 사이버 레인지, 시스템 엔지니어링 etc.
E-mail : dkim@add.re.kr

김 용 현(Yonghyun Kim)
1993년 광운대학교 전자공학과(공학사)
1995년 광운대학교 대학원 전자공학과(공학석사)
2013년 광운대학교 대학원 전자통신공학과(공학박사)
1995년~현재 국방과학연구소, 책임연구원(팀장)
관심분야 : 사이버 시뮬라전, 배틀랩 구축, WSN, 사이버전 M&S, 훈련체계 etc.
E-mail : yonghyunkim@add.re.kr