JKIICE

Short Paper

한국정보통신학회논문지 Vol. 25 No. 6: 857~860, Jun. 2021

국내외 사이버보안 훈련 동향

The Trends of Domestic and Overseas Cyber Security Training

Daesung Lee*

*Associate Professor, Department of Computer Engineering, Catholic University of Pusan, Busan, 46252 Korea

ABSTRACT

The 21st century society has entered the fourth industrial society of machine to machine from the information society of human to machine. Accordingly, countries around the world are always operating efficient crisis management systems that can quickly respond to disasters or crises. As cyber attacks such as cyber warfare are actually progressing, countries around the world are conducting defense training in response to cyber attacks, and reflecting the results of simulation attacks in improving or building security systems. In this paper, we would like to consider the future cyber training development guide by comparing and analyzing the trends of cyber training in domestic and foreign countries.

Keywords : Cyber crisis, Cyber security, Cyber warfare, Cyber training program

Ⅰ. 서 론

국가차원에서의 사이버 방어훈련은 실생활 환경과 매우 유사한 환경에서 사이버 방어기술을 습득하는 가장 효과적인 방법 중의 하나이며, 모의공격의 결과를 보안시스템 개선 혹은 구축에 즉각 반영할 수 있다는 측면에서 미국, NATO 등에서 매년 훈련테마를 설정하여 훈련을 실시하고 있다. 광의의 사이버 방어훈련에는 사이버안전 예방 훈련, 사이버위기 대응 훈련, 사이버위기 대응 종합훈련, 사이버공격 방어 대회, 사이버 안전/정보보호 교육 등을 포함시킬 수 있다. 현 시대에는 사이버전과 같은 사이버 공격이 실제적으로 진행되면서, 세계 각국은 사이버 공격 대응 능력을 고도화시키기 위해 사이버 훈련에 다양한 노력을 기울이고 있다[1].

사이버 훈련은 광의로는 사이버안전 예방 훈련, 사이버위기 대응 훈련, 사이버위기 대응 종합훈련, 사이버공격 방어 대회, 사이버 안전/정보보호 교육 등으로 구분한다.

사이버 훈련은 사이버전과 사이버기술개발을 위한 가상환경인 사이버레인지 환경을 구축하여 실시하고 있으며, 훈련의 궁극적인 목표는 모의공격의 결과를 보안시스템 개선 혹은 구축에 반영하여 방어능력을 고도화하는데 있다.

대표적인 사이버 훈련 개발 프로그램으로는 HSEEP (Homeland Security Exercise and Evaluation Program)을 활용한다[2].

본 논문에서는 세계 각국의 사이버 훈련을 비교 분석하고, 국내 사이버훈련 현황을 고찰함으로써, 향후 사이버 훈련 프로그램 가이드 개발 시에 고려해야할 주요 사항들과 훈련 프로그램 내용들에 대해 고찰해 보도록 한다.

Ⅱ. 세계 각국의 사이버 훈련

2.1. 미국 Cyber Storm[3]

미국 Cyber Storm은 2006년부터 2년 단위로 국토안보부 주관으로 사이버 공격 대응훈련을 실시하고 있으며, 그 주요내용은 아래 [표 1]과 같다.

Table. 1 US Cyber Storm main training themes

Date	Training Themes
Cyber Storm 1 (Feb. 2006)	Cyber incident response
Cyber Storm 2 (Mar. 2008)	Improving personal responsiveness and leadership

Received 9 April 2021, **Revised** 16 April 2021, **Accepted** 23 April 2021

*** Corresponding Author** Daesung Lee(E-mail:dslee@cup.ac.kr, Tel:+82-51-510-0653)
Associate Professor, Department of Computer Engineering, Catholic University of Pusan, Busan, 46252 Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.6.857 print ISSN: 2234-4772 online ISSN: 2288-4165

Date	Training Themes
Cyber Storm 3 (Sept. 2010)	Development of a federal response framework
Cyber Storm 4 (Mar. 2013)	Improving federal and state cyber responsiveness, Conducted separately in the U.S. independent training and international training
Cyber Storm 5 (Mar. 2016)	Adding medical health and distribution security
Cyber Storm 6 (Apr. 2018)	National Cyber Incident Response Plan (NCIRP) evaluation
Cyber Storm 2020 (Aug. 2020)	strengthen cyber security preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure.

2.2. NATO CCDCOE의 Locked Shield 훈련[4]

세계 최대 최첨단 사이버 방어 훈련인 Locked Shields는 NATO CCD COE(Cooperative Cyber Defence Centre of Excellence)가 2010년 5월에 최초로 스웨덴 국방대학교, 에스토니아 방위연맹과 공동으로 실제 공격을 방어하는데 필요한 기술을 시현하는 훈련을 실시한 이래 매년 봄마다 개최되고 있다.

국가 IT 시스템 보안 전문가 및 NATO 회원국과 파트너국의 법적 자문단 등 총 30여개국에서 천여명의 전문가들이 참여하고 있다. 에스토니아 방위군, 핀란드 방위군, 스웨덴 국방대학, 영국군, 미국 유럽 사령부, 항공작전사령부, 탈린 공대가 주 참여 기관이며, Simens AG, Threod Systems, Cyber Test Systems, Clarified Security, Iptron, Bytelife, BHC Laboratory, openvpn.net, GuardTime 등의 기업들이 함께 참여하여 IT 환경에 맞게 현실적 및 최첨단 기술, 네트워크와 최신 사이버 공격 유형을 적용해 진행하고 있다.

이 훈련에서는 체코 공화국 팀은 시나리오 투입 부문에서, NCIRC 팀은 법률 관련 부문에서, 독일 팀은 포렌식 부문에서, 영국 팀은 전략적 대처 부문에서 각각 최고점을 기록하고 있으며, 사이버안보 연례 컨퍼런스인 사이콘(Cycon)을 동시에 개최하고 있다.

2.3. Cyber Czech[5]

체코공화국은 2013년 체코 사이버보안센터(NCSC; National Cyber Security Centre)의 주관으로 DDoS 및 피싱을 캠페인으로 하는 최초의 도상훈련을 실시하였고, 2014년 사이버 보안법(Act on Cyber Security)의 제정하였다. 2015년 10월, 공식 사이버 훈련인 Cyber Czech 2015가 NCSC와 마사리크 대학(Masaryk University)의 주관으로 개최되었으며, 레드팀이 특정 취약점을 공격하고 블루팀이 방어하는 시나리오로 진행되었다.

2018년 11월에 개최된 Cyber Czech 2018에서는 한국, 크로아티아, 에스토니아, 이스라엘의 보안팀이 참여하였고, 네덜란드, 폴란드, 영국, 미국이 옵저버로 참가하였다. 4개팀으로 나뉘어 통합구조 ICT 시스템에 대한 공방으로 진행되었다.

미디어 대응 훈련은 GovCERT.CZ를 중심으로 사고 발생시와 사전 예방으로 구분하고, 협력기관들과의 즉각적인 위기 커뮤니케이션을 통한 기술지원을 목적으로 하고 있다.

2.4. Cyber Europe[6]

Cyber Europe은 2010년부터 2년 주기로 시행되고 있으며, ENISA(European Network and Information Security Agency)가 EU 집행위원회로부터 권한을 위임받아 훈련(Cyber Crisis Cooperation Exercise)에 관한 계획, 실시 및 평가를 맡고 있다. Cyber Europe 추진 현황은 [표 2]와 같다.

Table. 2 Cyber Europe Progress

Date	Training Themes
Cyber Europe 2010 (Nov. 2010)	Protection of corporate and personal information
Cyber Europe 2012 (Oct. 2012)	Protection of important information and communication facilities
Cyber Europe 2014 (Apr. 2014)	16 challenges selected
Cyber Europe 2016 (Apr. 2016)	Forensic and malware analysis
Cyber Europe 2018 (Apr. 2018)	Virtual attack on airlines
Cyber Europe 2020 (2020)	a scenario revolving around healthcare

2.5. APCERT 사이버방어 훈련[7]

아태지역침해사고대응팀협의회(APCERT: Asia Pacific Computer Emergency Response Team)는 2003년 2월 아·태지역내 국제 공동 침해사고 대응 및 정보공유 등 사이버 보안협력을 목적으로 출범하였다. 2011년부터

매년 1회씩 사이버 대응훈련을 실시하고 있으며, 2019년 6월 현재 한국(KISA), 일본, 호주 등 21개 국가, 30개의 사이버보안 기관으로 구성되어 있다. 주요 훈련내용은 [표 3]과 같다.

Table. 3 APCERT Main Training Contents

Date	Training Themes
Feb. 2011	Critical infrastructure protection
Feb. 2012	APT attacks and international cooperation
Feb. 2013	DoS attack response
Feb. 2014	Response to cyber activities through regional coordination
Mar. 2015	Cyber attacks that transcend traditional methods
Mar. 2016	The evolution of cyber threats and financial fraud
Mar. 2017	Responding to new types of DDoS attacks
Mar. 2018	Stealing IoT information through malware infection
Mar. 2020	The drill of “Banker doubles down on Miner”

Ⅲ. 국내 사이버 훈련 동향

국내에서는 2006년 을지연습시부터 사이버 훈련이 병행되었으며, 공공분야와 민간분야로 구분되어 훈련이 실시되어 왔다. 공공분야에서는 2019년부터 안보 환경의 변화를 고려하여 국가위기상황에 대응하고 전시에 대비하는 민·관·군 합동의 을지태극연습으로 변경되었다. 민간분야는 KISA가 주관하고 있으며, 통신사업자, 백신사, 가상통화 취급업소 등 60개 민간 기업, 26,000여명이 참가하고 있다.

또한 2017년부터 국가정보원과 국가보안기술연구소가 미션풀이(Jeopardy) 방식으로 진행하는 사이버 공격방어대회를 개최하고 있으며, KISA가 주관하는 HDCON (Hacking Defense Contest), 코드게이트보안포럼이 주관하는 국제해킹 방어대회 CODEGATE(코드게이트)가 일반, 대학생, 주니어를 중심으로 매년 개최되고 있다.

2013년부터는 국방 사이버 보안강화를 위해 일반인과 청소년들이 각각 팀을 이뤄 해킹방어 능력을 겨루는 화이트햇 콘테스트(WITHCON)가 국방부와 국군사이버사령부에 의해 매년 개최되고 있다.

Ⅳ. 결 론

사이버 공격은 시스템 권한획득을 위한 침투, 정보 훼손, 기밀정보 유출, 정상적인 서비스 방해, 정보 임의수정 등을 목적으로 진행되며, 공격 성공에 따른 피해는 상상을 초월하며 가늠하기 힘들다.

따라서, 세계 각국은 사이버 공격에 대응하는 방어능력을 고도화하기 위해 매년 꾸준히 사이버 훈련을 실시하고 있다. 국내에서도 2년전부터 Locked Shield 훈련에 참가하는 등 사이버 훈련 프로그램 개발에 박차를 가하고 있다. 사이버 능력 수준이 국가의 안보능력과 직결되는 만큼, 향후 지속적인 관심을 갖고 자체 실정에 맞는 사이버 훈련 프로그램 개발과 평가 기준이 정립되어야 한다.

본 연구를 통해 세계 주요국의 사이버 훈련 동향과 국내 훈련동향을 살펴보았다. CPS(Cyber Physical System)가 전 세계적으로 진행됨에 따라, 4차 산업사회에서의 사이버 폐해가 급증하고 있는 만큼 세계 각국은 실전을 방불케 하는 사이버 훈련을 실시하기 위해 많은 노력과 개선을 아끼지 않고 있다. 따라서 우리도 세계 각국과 견줄 수 있는 사이버 훈련 개선을 위한 노력이 지속적으로 진행되어야 한다. 또한, 만일에 발생할 수 있는 사이버 침해 시에도 운영상에 문제가 없도록 사이버 회복력이 가동되어야 하며, 이를 위한 제반 여건을 개선해야 한다[8].

ACKNOWLEDGEMENT

This paper was supported by RESEARCH FUND offered from Catholic University of Pusan(2019)

REFERENCES

[1] E. Kim and H. Ahn, “Study on effective cooperation of disaster safety management for central and local governments,” Seoul, Korea: KIPA Research Report, 2009.

[2] Homeland Security [Internet]. Available: https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

[3] Cybersecurity and Infrastructure Security Agency CISA [Internet]. Available: https://www.cisa.gov/cyber-storm-2020.
[4] NATO Cooperative Cyber Defense Center [Internet]. Available: https://ccdcoe.org.
[5] Cyber Czech [Internet]. Available: https://crp.kypo.muni.cz/en.
[6] European Network and Information Security Agency [Internet]. Available: https://www.enisa.europa.eu/.
[7] Asia Pacific Computer Emergency Response Team [Internet]. Available: https://www.apcert.org/.
[8] Office of National Security, *National Cybersecurity Strategy*, Blue House, 12-1025000-000003-01, 2019.