국방사이버전 연습체계 개선 방안 연구*

권 문 택**

요 약

본 연구는 현재의 국방사이버전 대응 연습체계의 문제점을 도출하고 이에 대한 개선방안을 제시하기 위해 수행하였다. 군은 현재 사이버전 대응을 위해 각급 제대별로 CERT팀 편성 운영하고, 국정원 주관으로 실시하는 국가사이버위기 대응훈련에 참가하거나 합동참모본부 주관의 인포콘(INFOCON) 연습을 실시하고 있으나 체계적인 기획 및 연습체계에 의해 실시되지를 않아 소기의 목적 달성에는 미흡하다고 평가되고 있다. 본 논문은 이러한 문제점을 해소하기 위해 연습형태와 연습기획 절차를 체계화함으로서 국방사이버안전을 위한 연습관리에 지침으로 활용할 수 있을 것이다.

A Study on the Defense Cyber Warfare Exercise

Moon Taek Kwon**

ABSTRACT

In the information society, information security is a critical issue for defense cyber network system. This paper provides a result of a study on the defense cyber exercise system for cyber warfare. So far, defense cyber exercise system has been uneffective and is not systematic even if several exercises has been implemented. In order to overcome these problems, a systematic and integrated cyber exercise process is suggested. Under the suggested system, we expect that cyber exercise for cyber warfare will be implemented with more effective manner.

Key words : Cyber Warfare, Cyber Exercise

접수일 : 2009년 11월 20일; 채택일 : 2009년 12월 20일

* 본 논문은 2009년 국방부 연구과제로 수행한 연구결과물의 일부임.

** 경희대학교 테크노경영대학원

1. 서 론

군사적인 의미에서 조명해 보면 사이버전은 선전포고, 총성, 그리고 전선이 없는 전쟁이다. 개인화기, 미사일, 탱크 등의 물리적 수단을 이용하여 수행하는 재래전과는 달리 사이버전은 키보드 및 마우스와 소프트웨어 등을 이용하여 국방망을 통해 거미줄처럼 연결되어 있는 국방 자원의 운용을 마비시키고 무력화 시킨다. 또한 군 항공기와 함정의 운항을 통제 불능상태로 만들기도 하며, 국방정보통신망을 마비시켜 지휘통제를 불가능하게 하기도 한다. 따라서 사이버전에 대한 방호 대책으로 평소 부단한 연습이 필요함은 아무리 강조해도 부족함이 없을 것이다.

사이버상에서 예상할 수 있는 공격의 주체는 적의 군부대에서 양성한 정보전 전사 및 적대적인 해커 등이 될 것이며 심지어는 개인적인 적대감을 품고 있는 해커가 될 수 있을 것이다. 이들 공격자의 공통적인 공격 목적은 국방기능을 마비시켜 혼란을 야기 시키고 궁극적으로는 방위능력을 훼손시키는 목적을 가지고 있을 것이다. 공격방법은 다양하게 전개 될 것이 예상 되는데 주요 예를 든다면 해킹, 바이러스, 웜, 스파이웨어, 스팸메일, 논리폭탄을 비롯하여 초미세형 로봇, 전자적 미생물 등이 될 것이다. 따라서 미래의 전쟁 양상인 네트워크 중심전(NCW : Network Centric Warfare) 환경하에서 적으로부터 사이버 공격을 당했을 때를 대비한 평시의 연습을 통해 준비하여야 할 것이다.

본 논문에서 연구자는 이러한 인식을 바탕으로 현행 군 사이버전 대비 연습실태를 분석하고 문제점을 도출하여 이에 대한 개선 방안으로서 통합된 사이버전 연습관리 방안을 제안하고자 한다.

2. 현 연습체계 및 문제점 분석

2.1 현 국방사이버전 연습체계

군은 NCW 상황하에서 사이버 방호를 위하여 국방 산하 각 급 부대에 사이버 보호 인력 확보, 조직 정비 등을 추진하고 있다.

국방부 본부를 비롯하여 육, 해, 공군 본부급에는 CERT팀을 편성하여 운영하고 있고, 국군기무사령부에는 2003년 11월 '국방정보전대응센터'를 설립하여 군 인터넷 홈페이지 관제체계, 국방 통합 바이러스 방역체계 구축 등을 마치고, 국군기무학교에 국방정보보호교육센터를 개소하여 전군 정보보호 실무자 및 CERT 요원들을 대상으로 정보보호 전문화 교육을 실시하고 있다.

또한 정보보호 업무를 원활하게 수행하기 위해 합동참모본부 주관으로 매년 인포콘(INFOCON : Information Operation Condition)연습을 실시하고 있으며, 이 연습을 통해 바이러스 공격, 해킹, 네트워크 무력화에 대한 대비를 하고 있다. 여기에 추가하여 국정원 주관으로 매년 실시하는 사이버안전 위기대응통합연습에 기무사령부 산하 '국방정보전대응센터'가 참여하고 있다.

2.2. 현 연습체계의 문제점

현행 국방 사이버전 대응 연습체계를 분석하여 보면 다음과 같은 문제점을 발견하게 된다.

첫째, 사이버전 대응 연습이 단편적으로 1년에 한번 실시된다는 것이다. 일반적으로 군의 전술훈련은 제대별로 실시하되 그 종류는 개인훈련, 집체훈련으로 나누어 볼 수 있으며, 개인훈련은 다시 특기훈련과 간부 훈련으로 분류하여 실시하고 있다. 집체 훈련은 소부대 대대, 연대 및 사단급 이상 대부대 훈련으로 확대하면서 체계적으로 하고 있다. 또한 훈련의 성격에 따라 모의훈련, 모의 및 기동훈련, 야외기동훈련 등으로 다양화 하여 반복 실시함으로서 평시에 여러 가지 상황에 따른 대응조치 능력을 향상시키고 있다. 이런 점에 비추어 볼 때 현재의 군 사이버전 연습은 합동참모본부 주관하에 1년에 한번 전군이 통합하여 실시하기 때문에 훈련의 기본 목표인 '숙달'에 크게 미흡하다는 것이다.

둘째, 합동참모본부 주관하의 인포콘(INFOCON) 연습이든 국정원 주관하의 정부 통합훈련이든 다양한 상황하에서의 연습이 진행되지 않고 전군적 규모 또는 범 정부적으로 실시하기 때문에 실무자 입장에서는 평시에 탁상연습, 시뮬레이션에 의한 모의 연습 등 다양한 환경과 수준에 따라 체계적으로 연습을 하여 연습 및 훈련의 기본 목표인 '숙달'에 이르는 실질적인 성과를 달성하지 못한다는 것이다. 군사 연습 또는 훈련은 도상훈련, 모의훈련, 실기동 모의 훈련, 모의 장비훈련, 사단급 기동훈련 등을 반복적으로 실시함으로서 다양한 작전상황에 대처하는 능력을 '숙달'하도록 실시하고 있다.

이러한 문제점을 고려해 볼 때 현재의 사이버전 연습체계는 체계적인 연구방법론을 통해 개선하여 국방사이버위기 상황에 대비를 할 필요가 있다.

3. 개선방안 연구방법

3.1 연습체계 개선방안 연구방법

사이버전 대응 연습체계 개선 방안을 연구하기 위해 채택한 연구 방법은 그룹의사결정기법(Group Decision Making Technique)으로서 군 업무에 능통한 예비역 장교들로 구성된 전문가를 활용하였다. 일반적으로 객관적인 데이터에 의해 계량화 될 수 없고 참여자의 의견이 다양하게 표출될 수 있는 어떤 문제에 대한 합리적인 의사결정은 그 분야에 정통한 전문가 워킹그룹을 편성하여 의견을 취합하는 방식이 적합하다[7, 8]. 본 연구에서는 이와 같은 관점 하에 전문가 워킹그룹을 활용하여 네트워크 국방사이버전 대응 연습체계를 개발하였다.

본 연구에서 수행한 전문가 워킹그룹을 통한 그룹의사결정기법은 참가자들끼리 서로 자유로이 의견을 제시할 수 있는 브레인스토밍기법과 함께 참가자들이 자기의 생각을 조용히 기술하는 브레인라이팅기법을 사용하였으며, 최종적인 검증을 위해 워킹그룹에 포함되지 않은 타 전문가에게 의뢰한 설문을 통해 실시하였다.

본 연구를 위한 전문가 집단은 사이버전 대응 연습체계에 관환 내용이기 때문에 문제 영역에 부합되는 전문가로서 군 경력이 10년 이상 된 예비역 장교중에서 군사훈련 연습 경험자와 군의 정보통신병과 장교들로 구성하였다. 워킹그룹에 참여한 전문가들은 10년 이상 군 장교 생활을 하면서 각종 군사훈련 계획 수립과 연습에 참여 한 경험 있어 이 분야에 충분한 전문지식을 가진 우수 요원들이다. 따라서 본 연구에 참여한 워킹그룹의 그룹의사결정 참여자들은 경력 및 경험면에서 본 연구의 취지에 적합한 인력으로 판단되며, 연구에 적극적으로 협조를 하였기 때문에 네트워크 국방사이버전 연습체계 개선 방안을 도출하는데 큰 무리는 없다고 판단되었다.

3.2 연습체계 개선방안 도출방법

연구자는 연구에 참가하기로 동의한 참가자들에게 연구에 대한 공감대를 형성하기 위하여 본 연구 결과가 장차 국방 국방정보체계를 보호할 연습체계를 구축하는데 기초 지침이 될 수 있다는 점을 설명하고 공감대를 형성하였다.

공감대 형성 후 연구가가 사전에 수집한 군 교육훈련관리 교범(야전교범 7-10)과 관련 자료를 나누어 준 후 그들이 그동안 생각하고 경험했던 내용을 바탕으로 사이버전 연습체계에 대한 내용을 구상하도록 2주일간의 연구 기간을 부여하였다.

2주일간의 연구 기간이 부여된 이후에는 참가자 전원이 한 장소에 모여 전문가 워킹그룹을 통한 그룹의사결정기법에 대하여 설명을 듣고, 다른 구성원과 토론 없이 핵심내용을 일정 양식에 자유로이 기술하도록 하였다. 이렇게 기술한 내용을 가지고 각 팀별로 별도로 소회의실에 모여 항목별로 정리한 후 1차 정리된 결과를 보면서 참가자 전원이 토론을 통해 의견을 나누고 새로운 아이디어가

나오면 타당성을 검토 후 첨가하면서 아이디어를 교환하고 공감대를 형성하여 나가면서 주요 내용들을 식별하여 정리하였다.

2단계 최종 종합 단계에서는 효과적인 결과를 도출하기 위해 하나하나의 결과를 전동화면에 전시하면서 수정 기록하였으며 도출된 내용들은 그 타당성에 대하여 재 토론을 하면서 확정해 나갔다. 이와 같은 과정을 거쳐 도출된 국방사이버전 연습체계 개선(안)은 전문가 그룹에 포함되지 않은 5명의 타 전문가에게 설문조사 및 면담을 통해 최종 점검하고 다음과 같이 개선방안을 정리하였다.

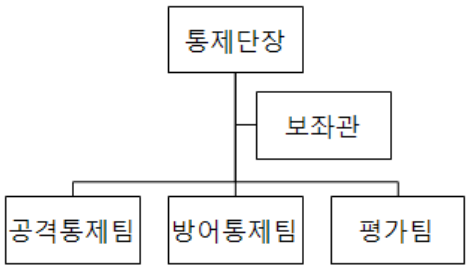
4. 사이버전 연습체계 개선 방안

4.1 연습기획 및 통제단 구성

사이버전연습을 효과적으로 수행하기 위해서는 무엇보다 계획 수립이 잘 되어야 하고, 다음으로는 연습 통제가 원활하게 이루어져야 한다. 이러한 관점에서 연습을 구상하는 부대나 조직은 먼저 연습계획 수립을 위한 조직과 실제 연습시에 통제와 평가를 담당할 조직을 구성하여야 한다.

연습계획수립은 평상시에 사이버전 담당자가 지휘관이나 부서 책임자의 지시에 의해 꾸준히 준비하는 과정이기 때문에 반드시 별도의 조직이 필요한 것은 아니나 연습통제단은 단기간에 실시하는 연습을 성과 있게 수행하기 위해 반드시 (그림 1)과 같이 구성한다. 연습통제단은 공격을 담당하는 공격통제팀, 방어를 담당하는 방어통제팀, 평가를 담당하는 평가팀으로 구성하는 것이 바람직하다.

(그림 1)에서 공격통제팀은 공격 시나리오에 따라 공격을 주도하게 되며, 방어통제팀은 사이버전 방어부대나 조직의 방어 행태를 통제하고 지원해 주는 역할을 한다. 평가팀은 연습 전체과정에서 연습참가 부대나 조직이 제대로 원칙에 입각하여 조치를 하고 있는가를 관찰하고 평가하며, 사후 보고서를 작성한다.



(그림 1) 통제단 편성 "예"

4.2 연습계획 수립

사이버전 대비 연습을 하기 위한 계획수립과정은 연습 시나리오와 실제 연습시 수행할 여러 가지 조치들에 대한 내용을 사전에 계획하는 행위이다. 연습계획수립을 위해서는 연습을 주관하는 부대 또는 조직에서 우선 연습기획팀을 편성해야 한다. 연습계획팀은 계획수립을 하기 전에 지휘관 의도를 지침으로 하여 우선 연습의 목적을 확실히 할 필요가 있다.

연습 목적이 단순히 도상 연습을 통해 참모들이나 지휘관 및 대응요원들의 경각심을 높이고 준비태세 인식을 강화하는 것인지, 또는 전군적으로 실제 상황에 부합하는 사이버 침해 사고를 유발하여 정보체계를 마비시킴으로서 기존의 대 사이버전 대비책의 견고함과 유용성을 테스트 하는 것인지 등 연습 목적에 따라 연습의 수준, 참가 규모 및 시나리오가 달라져야 한다. 따라서 연습 목적에 따라 시나리오의 복잡성이 달라지고, 이에 따라 연습상황 부여와 기대되는 참가자들의 대응 태세도 달라질 것이다.

연습계획을 준비함에 있어서 당연히 관계부대 또는 조직과는 사전 협조가 이루어져야 한다. 이를 위해서는 실제 연습 실시 수개월 전부터 관계 부대 및 조직 간에 계획수립을 위한 협조회의가 이루어져야 하며, 특히 대규모 실제상황에 대한 연습을

계획하고 있다면 더 더욱 이른 시기부터 이러한 협조 행위가 이루어져야 한다.

만약 연습계획 수립시에 참여하지 않은 부대나 조직이 있다면 실제 연습 상황에서는 이 부대나 조직의 참여를 배제하거나 또는 중간 단계라도 참여시켜서 실제 상황에서 연습 참가 각 부대나 조직들이 그들의 역할, 조치해야 할 사항 등 자세한 내용에 대해 공동의 인식을 가지고 참여함으로서 불협화음을 방지 하도록 하여야 한다.

연습계획 수립 단계에서 가장 중요한 요소 중의 하나는 그 연습 참가 부대나 조직 중에서 가장 상위 부대의 지휘관의 역할이다. 연습 참가 조직의 최상위 지휘관의 리더쉽과 관심이 따르지 않으면 자연히 그 연습은 맥이 빠지고, 예하 조직의 지휘관도 관심을 기울이지 않게 되어 실무자들만의 연습으로 마무리 되고, 의미 있는 성과는 얻지 못할 것이다. 따라서 연습계획 수립단계에서 실무 책임을 맡은 사이버전 기획관은 반드시 최고 지휘관을 설득하여 연습의 중요성, 기대효과, 향후 계획된 연습 확장 계획 등에 대한 확고한 승인을 획득하고 참가 규모 결정, 연습 시나리오 작성 등 다음 과정을 진행 하여야 한다.

연습계획수립은 몇 단계를 거쳐 이루어지는데 그 순서는 1) 1단계-개념수립 회의, 2) 2단계-최초 계획수립 회의, 3) 3단계-중간 점검회의, 4) 4단계-최종 계획수립회의로 나누어 단계별로 연습 계획을 다듬고 세분화해서 완성해 나간다. 다음은 단계별 주요 활동이다.

4.2.1 1단계-연습개념 수립 회의

어떤 군사연습이든지 연습을 시행하려면 우선 그 연습을 통해 무엇을 얻고자 하는지에 대한 전체적인 연습 구상, 즉 연습개념을 수립하는 것이 첫 번째 하는 일이다. 마찬가지로 사이버전 대비 연습을 실시하고자 할 때 우선적으로 착수 할 일은 전체 연습개념을 수립하는 것이다.

연습에 대한 개념수립은 최초 개최되는 1단계-개념수립회의에서 진행된다. 개념수립회의는 국방사이버전 담당 조직이 주관하여 정보보호 내부 전문 인력에 의해 수행된다. 여기에 참여하는 인원은 국방 사이버전을 담당하는 실무자와 그 조직의 최고 책임자가 포함되어야 한다. 예를 들어 국방부 주관 전군적 차원의 사이버전 연습을 실시한다면 최소한 국방부 정보화 기획실장, 정보보호담당 과장 및 실무자, 각군 정보보호 담당 과장 정도는 참여하여 전체적인 연습 개념을 수립하여야 한다. 이러한 개념 수립회의는 전군적 차원의 연습을 목표로 할 때는 최소한 연습 개시 6~12개월 이전에 착수해야만 정상적인 절차에 의해 최종 계획 완성이 이루어지고 관계 부대 및 부처의 협조를 얻어 원활한 연습이 진행 될 것이다.

개념수립 회의에서는 주로 연습의 목표, 연습 기간 및 실시일정, 연습 참가범위 등 큰 그림에 대한 것을 결정하게 되는데 개념수립회의에서 결정되는 결과물은 다음과 같다.

- 개념수립 회의에서 결정하여야 할 사항
  - 연습 목표
  - 연습 수준 결정
  - 연습 일정 결정
  - 참가 범위(부대/부서 결정)
  - 추가적인 민, 관, 군 합동 연습 여부 결정
  - 부대 및 부서별 준비사항 결정
  - 위 사항을 포함한 개념계획서 작성

4.2.2 2단계-기본계획 수립 회의

2단계 기본계획 수립 회의는 1단계 개념계획 수립 회의 후 통상 1~2개월 후에 개최하는 것이 바람직하다. 이 회의에는 최초 개념계획 수립시 참여했던 인원을 포함하여 연습에 참가하게 되는 모든 조직의 사이버전 관계자 대표가 참여 하여야 한다. 그 이유는 추후 원활한 연습 진행을 위해서는 연습 참가 부대나 조직이 연습 취지와 계획에 대해 초기 단계부터 계획 수립에 참여하여 이해도

를 높이고 협조할 사항, 수행해야 할 임무 등을 명확히 정립해야 하기 때문이다.

2단계 기본계획 수립 단계에 참가하는 부대나 조직은 1단계에서 수립한 개념 계획을 열람하여 의문나는 사항이나 예상되는 문제점 등에 대한 사항을 회의 주관자에게 질문을 통해 확실히 이해하고 수정이나 보완 할 사항은 건의를 통해 반영하여야 한다. 이 단계에서서는 연습 실시간 각 참가자들이 수행하여야 할 조치사항(action items)들이 세부적으로 정의되어야 하며, 이 조치사항들은 참가부대나 조직들이 열람을 통해 확정되어야 한다. 또한 2단계 기본계획 수립 회의에는 공격팀도 참여하여 전반적인 연습 협조체계를 조율해야한다.

일단 기본계획 수립회의에서 확정된 연습 목표, 연습 수준, 연습 일정 및 참가범위는 원칙적으로 이후 계획수립 과정에서 변경하지 않는 것이 좋다. 그 이유는 이러한 기본 사항을 변경하게 되면 세부적으로 진행 할 시나리오와 수행할 조치사항들이 다수 변경되어야 하기 때문에 가능하면 원안대로 진행하도록 노력해야 한다.

- 기본계획수립 회의에서 결정하여야 할 사항
  - 연습 목표, 수준, 일정 및 참가범위 최종 확정
  - 공격팀에 의해 유발되는 상황에 대한 대응조치방식 결정
  - 연습간 참가자 연락 및 접촉 포인트 작성(전화, 이-메일, 사무실 등)
  - 추가적인 민, 관, 군 합동 연습 여부 결정
  - 기획팀에서 사전 작성한 연습 시나리오 리뷰 및 잠정 확정
  - 상황에 따른 조치사항 배분
  - 위 사항을 포함한 연습 기본계획서 잠정 작성

4.2.3 3단계-중간 점검 회의

3단계 중간 점검회의는 2단계 기본계획 수립 회의 후 통상 1~2개월 후에 개최한다. 이 회의에는 2단계 기본계획 수립 회의시 참여했던 인원들이 다시 모여 추가적인 보완 사항이 있는가를 점검하고, 다시 한 번 연습 참가 부대나 조직이 연습 취지와 계획에 대해 확인 해 주고 이해도를 높이고, 협조할 사항, 수행해야 할 임무 등을 명확히 한 후 최종적으로 연습계획을 확정한다.

- 3단계-중간 점검 회의에서 결정하여야 할 사항
  - 추가적인 상황 조치사항 배분
  - 최종적인 보완사항 반영 후 연습계획 확정

4.2.4 4단계-최종계획수립 회의

4단계 최종 계획수립 회의는 연습실시 1개월 전에 개최한다. 이 회의에서도 3단계 중간점검회의와 같이 2단계부터 계획 수립 회의에 참여했던 인원들이 모두 모여 추가적인 보완 사항이 있는가를 최종 점검한다. 이 회의에서는 새로운 상황 시나리오를 추가하거나 연습 계획과 목표 등 기본 사항을 변경하지 않는다.

이 단계에서 보완 할 사항은 사소한 조치사항 변경이나 참가자 연락사항 변경, 일정 내 세부 시간계획 변경 및 연습 참관을 위한 VIP 방문자 추가 등 비교적 사소한 사항에 그쳐야 한다.

- 4단계-최종계획수립 회의에서 결정하여야 할 사항
  - 연습계획 최종 리뷰
  - 연습 참가 부대 및 기관들이 수행해야 할 사항 조치사항 확인
  - 연습기획팀과 공격팀 간 업무 협조
  - 시나리오 및 목표 최종 확인
  - 전반적인 연습계획 최종 확인

4.3 사이버전 연습유형

사이버전 연습체계와 이를 위한 계획수립 절차는 통상의 다른 군사연습체계와 큰 틀에서는 대동소이하다. 그러나 세부적인 실행계획과 시나리오는

연습의 목적에 따라 매우 다른 면이 있다. 즉 여러 가지 다른 목적으로 사이버전 연습을 실시하게 되는데 그 연습의 목적에 따라 묘사하는 시나리오 및 절차, 그리고 평가 사항이 다를 수 있다는 것이다.

사이버전 연습은 몇 개의 유형으로 분류 할 수 있다. 본 논문에서 제시되는 4개의 연습 유형은 군 교육훈련 체계를 바탕으로 전문가 그룹에서 사이버전의 특성에 부합되도록 창의적으로 구상하고 도출한 방안이다. 따라서 각 연습 유형별로 그 목적, 참가자 등을 이해하고 상황에 따라 적절한 유형의 연습을 실시한다면 그 효과는 크게 증진 될 것이다. 다음은 연습체계의 유형별 설명이다.

4.3.1 탁상 연습 : 실제 침해상황 부여 없이 페이퍼 워크(paper work)만 실시

탁상 연습은 사이버전 연습체계의 유형중에서 가장 낮은 수준의 연습체계이다. 이 연습은 연습에 참가하는 부대나 참가자들간에 의사소통과 협력능력을 배양하는데 주로 사용되는 연습 형태로서 통상 본격적인 연습 이전에 예행연습으로 실시하거나 단위 부대별로 수시 연습에 사용할 수 있는 연습유형이다.

탁상 연습은 연습기획팀에서 작성한 가상의 시나리오를 전파하고 관계 기관이나 개인이 어떻게 상황을 전파하고 조치를 하기 위한 협조를 하는가에 초점을 맞추고 평가한다. 이 연습은 연습통제단 요원과 참가자들이 같은 장소에 모여 테이블을 사이에 두고 마주하여 통제단에서 시나리오에 따라 상황을 부여하고, 이에 대해 참가자들이 조치하는 행동을 관찰하고 평가하여 문제점을 도출하고 개선책을 강구한다.

탁상연습은 크게 연습기획팀, 연습통제단, 연습 참가기관 또는 개인과 소규모의 관찰자가 배석하며, 실제 상황이 아닌 페이퍼 상황으로 설계된 시나리오에 따라 연습을 실시한다. 연습 효과를 증진하기 위해 연습기획팀, 연습통제단, 참가자들 모두가 모여 사전에 작성된 각본에 따라 실시한다.

다음은 간략히 요약한 탁상 연습 개요이다.

- 목적 : 향후 실제 연습에 대비한 예행 연습 또는 수시 실시 연습
- 목표 : 기존 사이버전 대응 계획 및 절차 검증, 반복적인 연습으로 상황 이해
- 교훈 : 잘된점, 문제점 등을 도출하여 문제점이 있을 경우 개선책 마련
- 기대효과 : 사이버전 준비태세 강화에 기여
- 개선 사항 : 차후 강화된 연습에서는 실제상황 부여

탁상 연습은 제대별 단위부대에서 수시로 실시하여 인접부대간 및 기관간 정보를 공유하고, 기존의 사이버전 대응 계획의 유효성과 준비태세 수준을 검증하는데 활용하면 유용하다.

4.3.2 탁상/실제상황 혼합연습(페이퍼 워크/각본에 의한 가상상황 부여 병행)

본 연습은 탁상연습을 보완한 연습형태다. 이 연습형태는 탁상연습에서 실현하지 못했던 실제 상황을 일부 부여하여 도상 연습 개념의 탁상연습을 보완한 것이 특징이다. 이 연습에서는 공격통제팀에 의해 가상 상황이 부여되며, 참가자들에게 실제와 유사한 경험을 하게 하는 것이 목적이다. 따라서 이 연습에서는 탁상연습을 통해 습득한 교훈을 보강하고 여기에 좀 더 복잡한 실제 상황을 부여하여 다양한 사이버전 보호체계를 검증하는 역할을 수행한다. 따라서 이 연습을 통해 가상적인 사건 이벤트와 실제 이벤트 시나리오를 혼합하여 부여함으로서 연습의 효과를 증진하게 될 것이다.

탁상/실제 혼합 연습 기획자는 연습계획 수립단계에서 가상상황이 부여될 목표를 선정한다. 공격의 대상이 되는 목표는 단일 부대일 경우도 있고, 경우에 따라서는 여러 부대 및 유관기관 전부를 대상으로 할 수 도 있다. 따라서 복수의 연습참가 부대들과 사전 정밀한 협조를 위해서 대략 3~6개월간의 계획수립 기간이 필요하다. 이 계획 기간내

에 연습기획팀은 연습 대상 기관과 충분한 시나리오를 협의하여 설정하고, 경우에 따라서는 실제 상황이 부여되기 전에 탁상 연습을 먼저 실시하여 연습의 적합성을 검증 해 볼 수도 있다.

다음은 간략히 요약한 탁상/실제상황 혼합 연습 개요이다.

- ◦ 목적 : 사이버전 대비 탁상/실제 통합 연습
- ◦ 목표 : 사이버전 담당요원 교육, 기존 사이버전 대응 계획 및 절차 검증, 침해 탐지, 대응 및 복구 능력 검증
- ◦ 연습수준 : 실제 침투상황 부여하여 참가자 액션 유발
- ◦ 기대효과 :
  - 연습을 통해 잘 된점, 문제점 도출후 추후 대비계획에 반영
  - 부대내 사이버전 대비태세 인식 제고
  - 상위 단계인 실제 상황 연습에 기초자료 제공

4.3.3 전군적 실제상황 연습 -사전 협조된 가상 상황을 실제 적용하여 실시

전군적 실제상황 연습은 사이버전 연습중에서 두번째로 높은 난이도와 실제 상황에 부합되는 연습이다. 이 연습은 사전 협조된 가상 상황을 실제 시스템에 적용하여 실시하는 것으로서 제2단계 수준의 연습에서의 미비점을 보완하고 최상위 레벨-사전 협조 없는 실제상황 부여 연습-을 대비한 연습이다. 이 연습에서는 공격통제팀에서 가상 상황을 부여하여 참가자들에게 실제와 유사한 경험을 하게 하는 면에서는 탁상/실제상황 혼합연습과 유사하나 연습 참여 부대의 범위가 전군적으로 광범위하게 실시된다는 점과 페이퍼 워크에 의한 도상연습이 생략 된다는 점에서 다르다.

따라서 이 연습에서는 탁상/실제상황 혼합연습을 통해 습득한 교훈을 보강하고 여기에 좀 더 복잡한 상황을 전군적으로 부여하여 다양한 사이버전 대응체계를 검증하는 역할을 수행한다. 따라서 이 연습을 통해 가상적이고 사전 협조된 것이기는 하지만 실제상황과 유사한 이벤트 시나리오를 부여함으로서 연습의 효과를 극대화 하게 될 것이다.

이 연습에서 연습 기획팀은 연습 계획 수립단계에서 실제상황과 유사한 시나리오를 작성하고 이 상황이 부여될 부대와 사전에 협조를 하여야 한다. 따라서 전군적 수준의 연습 시나리오, 필요한 인력 및 정보보호 자원을 동원하기 위한 협조와 연습 일정 협의를 준비하는데 통상 6~12개월의 계획수립 기간이 필요하다. 이 계획 기간내에 연습 기획팀은 연습 대상 부대 및 기관과 충분한 시나리오를 협의하여 설정하고, 경우에 따라서는 실제 상황을 부여하기 전에 소규모 수준의 탁상/실제상황 혼합연습을 먼저 실시하여 연습의 적합성을 검증 해 볼 수도 있다. 이때 소규모 탁상/실제상황 혼합연습에서 발견된 사이버전 취약점에 대해서는 공격팀이 추가로 기획팀에 연락하여 시나리오를 보완하여 수정 할 수 있다.

다음은 간략히 요약한 전군적 실제상황을 부여한 연습 개요이다.

- ◦ 목적 : 사이버전 대비 전군적 통합 연습-사전 협조된 각본에 의한 실제 상황
- ◦ 목표 : 사이버전 담당 전문요원 교육, 기존 사이버전 대응 계획 및 절차 검증, 침해 탐지, 대응 및 복구 능력 검증
- ◦ 연습수준 : 실제 침투상황 부여하여 참가자 액션 유발
- ◦ 기대효과 :
  - 전군적 규모의 실제 상황 연습을 통해 잘된 점, 문제점 도출 후 추후 대비계획에 반영
  - 조직내 사이버전 대비태세 인식 제고
  - 상위 단계인 실제 상황 연습에 기초자료 제공 및 대비태세 보완
  - 추가적인 문제점 보완하여 사이버전 대비 계획 완성

4.3.4 전군 실제상황 연습-사전협조 없이 실제 긴급상황부여

본 연습은 사이버전 연습중에서 가장 높은 수준의 연습형태다. 연습체계 상 전 단계 연습들은 사전 협조된 각본에 의한 시나리오를 가지고 실시하는 것이기 때문에 참가 부대나 기관들은 언제, 어디서, 어떻게 상황이 벌어질지를 알고 있다. 그러나 전군 실제 상황 연습은 비록 연습이기는 하지만 전혀 사전 통보 없이 불시에 실시하는 전군 규모의 연습이다. 따라서 가장 실제 상황과 유사하다는 것이 특징이며, 이 연습을 통해 국방 사이버전 대비태세의 실제적 대응 능력이 판명 될 것이다.

이 단계의 연습은 연습기획팀이 인위적으로 상황을 조작하거나 유도해서는 안 된다. 왜냐하면 이 단계의 연습을 통해서 국방 사이버전 대응 능력을 적나라하게 파악하여야 문제점을 보완 할 수 있기 때문이다. 이 단계에서의 주도자는 사이버전 공격통제팀이다. 공격통제팀은 참가 부대와 사전 협조 없이 다양한 유형의 사이버전 공격 기술을 구사하여 불특정 부대나 기관에 공격을 감행할 수 있다.

이 단계 연습에서는 실제 상황이 예고 없이 부여되는 만큼 부대나 조직의 기본 임무에 지장을 줄 것이 우려된다. 특히 고급 지휘관들은 예고 없는 실제 상황 부여로 자기 부대의 기본 임무 수행에 큰 지장이 올 것을 우려하여 연습을 방해하거나 비 협조적일 수도 있다. 따라서 이 연습은 자주 할 수는 없고, 12~18개월의 긴 기간 동안 치밀한 준비를 한 후에 전군적 규모 또는 필요시 선정된 일부 부대에 국한 하여 실시한다. 이 계획 기간 내에 연습 기획팀은 공격통제팀과 협조하여 충분한 시나리오를 설정하고, 경우에 따라서는 실제 상황이 부여되기 전에 탁상 연습을 먼저 실시하여 연습의 적합성을 검증 해 볼 수도 있다.

다음은 간략히 요약한 사전협조 없는 실제 긴급 상황부여 연습이다.

- 목적 : 사이버전 대비 사전협조 없는 실제 긴급 상황부여 연습
- 목표 : 사이버전 요원 교육, 기존 사이버전 대응 계획 및 절차 검증, 침해 탐지, 대응 및 복구 능력 검증
- 연습수준 : 사전협조 및 각본 없이 실제 침투 상황 부여하여 참가자 액션 유발
- 기대효과 :
  - 사전 협조 없이 불시로 실제 상황을 부여한 연습을 통해 잘된 점, 문제점 도출 후 추후 대비계획에 반영
  - 부대내 사이버전 대비태세 인식 제고
  - 추가적인 문제점 보완하여 사이버전 대비계획 완성에 기여

상기 연습형태 및 내용은 <표 1>에 정리하였다.

4.4 연습 실시

사이버전 연습 실시는 연습통제단에 의해 주관되고 통제 된다. 일단 연습 기획을 담당하는 부서에서 연습 계획이 작성되어 확정 된 이후의 모든 연습 진행은 철저히 연습 계획에 나와 있는 시나리오대로 통제단에서 주관하여 진행한다. 연습 참가 부대나 조직은 공격통제팀에 의해 시나리오에 따라 수행하는 공격에 대응하는 적절한 조치를 수행하면 된다. 공격에 대해 적절한 조치를 하는 가 못 하는가가 연습 성공의 열쇠이다. 평가관은 참가부대가 사이버 공격에 어떻게 대응하는가 하는 상태를 관찰하여 평가하고, 이 평가서를 바탕으로 연습 종료 후 사후보고서를 작성한다.

4.4.1 연습 관찰

평가팀의 평가관은 연습 전 과정을 관찰하면서 사건 하나 하나에 대한 대응 조치들의 적합성 여부를 판정하여 일정 양식에 기록하여 매 상황 종료 후 즉시 통제단장에게 보고한다. 이 관찰 기록은 연습 부대 및 조직 책임자에게도 제공하여 지

〈표 1〉 사이버전 연습형태 및 주요 내용

연습 유형	연습 내용	특징	필요 자원	연습 대상 조직
탁상 연습 (1단계)	◦ 주관 : 연습통제단 ◦ 핵심내용 : 사전 협조된 시나리오에 의한 페이퍼 연습	◦ 신속한 계획수립 가능 ◦ 소규모 조직도 연습가능 ◦ 기획기간 : 1~2개월 ◦ 연습기간 : 1~3일간	◦ 인력, 장비 등 큰 자원 없이 실행 가능	◦ 필요시 소규모 단위부대, 참모조직 별 단독 수행
탁상/실제 상황 혼합 연습 (2단계)	◦ 주관 : 연습통제단 ◦ 핵심내용 : 공격통제팀에 의해 기 작성된 페이퍼 시나리오 및 실제상황 시나리오에 의한 혼합 연습	◦ 탁상연습 보다는 긴 계획수립 기간 필요 ◦ 소규모 참가 조직도 연습가능 ◦ 기획기간 : 3~6개월 ◦ 연습기간 : 5~7일간	◦ 인력, 장비 등 비교적 큰 자원 필요 ◦ 참가 대상 조직과 사전 협조 필수	◦ 다수의 참가 부대 및 조직이 관련됨으로 사전 긴밀한 협조 전제됨
전면적 실제상황 연습-사전 각본 의존 (3단계)	◦ 주관 : 연습통제단 ◦ 핵심내용 : 공격통제팀에 의해 기 계획된 실제 상황 시나리오에 의한 연습 ◦ 필요시 페이퍼 시나리오 활용/탁상 연습 병행	◦ 탁상/실제상황 혼합연습 보다는 긴 계획수립 기간과 참가 조직간 긴밀한 협조 필요 ◦ 비교적 다수의 대규모 조직 참가 전제 실시 ◦ 기획기간 : 6~12개월 (필요시 2~3개월 보완기간 추가 필요) ◦ 연습기간 : 7~14일간	◦ 다수의 참가 조직으로 큰 규모의 IT인력, 장비, 예산 등이 자원 필요 ◦ 참가 대상 조직과 사전 협조 필수	◦ 다수의 참가 부대 및 조직이 관련됨으로 사전 긴밀한 협조 전제됨 ◦ 참가 조직은 사전에 1, 2단계 연습을 통해 연습 목적, 상황 등에 대한 이해도가 높아야 함
전면적 실제상황 연습-사전 각본 없음 (4단계)	◦ 주관 : 공격팀 주도/연습기획팀 협조 ◦ 핵심내용 : 공격통제팀에 의해 불시에 사전 예고없이 공격 감행하는 연습 ◦ 실제 상황과 가장 유사한 연습	◦ 제 3단계보다는 긴 계획수립 기간 및 세밀한 연습 상황 조율 필요 ◦ 기획기간 : 12~18개월 ◦ 연습기간 : 약 3개월 이상의 장기간내의 불특정 시간에 공격 실시	◦ 인력, 장비 등 비교적 큰 자원 필요 ◦ 참가 대상 조직의 최고 지휘관의 사전 동의 및 개략적인 연습 개요 합의 필수 (부대 일상 업무에 지장이 없도록 조율)	◦ 다수의 참가 부대 및 조직이 관련되고 불시에 실제 사이버 침투 행위가 발생하기 때문에 대비태세 수준을 실제 상황에서 평가해야 할 조직으로 국한하여 실시(예 : 통신망 운영부대, 데이터베이스 관리조직 등)

휘관 상황 판단에 도움을 주도록 한다.

연습관찰 기록은 연습이 진행중일 때도 후속 조치에 참고할 중요 정보로서 가치가 있지마는 연습 종료 후 사후 보고서에 반영되어 보다 발전된 사이버전 대응 계획 수립 및 시스템 개선에 큰 도움을 줄 것이다.

4.4.2 연습을 통해 획득한 교훈

연습 실시를 통해 얻어지는 교훈은 1) 적절한 조치로서 장려할 사항, 2) 부적절하거나 미흡한 조치로서 개선할 사항으로 나누어진다. 이와 같은 장려사항과 개선할 사항은 사이버전 연습의 목적에 비추어 제대로 임무 수행이 달성되었는가를 판정하는데 매우 유용한 정보로서 일반적인 개선사항은 다음과 같이 정리 할 수 있다.

- 추후 연습 개선을 위한 개선사항
  - ◦ 업무 절차가 정보보호에 방해가 되는 경우
  - ◦ 침해사고 보고 체계 및 절차의 부적절성
  - ◦ 적절한 시기에 침해사고 보고 지연
  - ◦ 상위 직급의 참모 또는 지휘관의 무관심
  - ◦ 외부 참가 기관의 비협조 또는 적시 참여 지연
  - ◦ 상황대처 및 보고문서의 부적절성
  - ◦ 침해사고 대응 소프트웨어의 부 적절성

◦ 각종 행정 지원 조치 지연 또는 미흡
◦ 침해 사고 일지의 미기록 또는 불가용
◦ CERT 팀 전문인력 또는 전문성 부족
◦ 참모들의 지식 부족
◦ 상황별 시나리오의 부적합성
◦ 공격에 대한 대응규칙의 불명확성
◦ 연습 참가자들간의 불협화음

5. 결론 및 기대효과

미래의 전쟁 양상은 네트워크 중심전(MCW)이 될 것이다. 네트워크 중심전(MCW)은 전투공간내의 모든 상황이 공유되고 이에 따라 동시적인 의사결정과 정보우위를 달성하고 전투력의 상승효과가 달성되는 전쟁개념이다. 이러한 개념의 새로운 전쟁 패러다임을 원활하게 구현하기 위해서는 무엇보다 정보보호체계 구축이 시급이 요구되고 있다.

이러한 상황 인식하에 최근 국방 정보화 분야에서는 네트워크 중심전(NCW)에서의 우위를 달성하기 위해 필수적인 사이버안전을 위한 연습을 강화하고 있다. 그러나 국방정보체계를 보호하기 위한 사이버전 대응 연습을 위한 체계와 절차가 아직은 미흡하다는 문제점이 대두되었다.

본 연구는 이러한 문제점을 인식하고 국방 정보체계 분야에 다년간 근무했던 경험과 학문적인 연구방법론을 바탕으로 국방사이버전 연습체계 개선방안을 수립하여 가이드라인으로 제시하였다. 본 연구에서 제시된 연습체계 개선방안은 국방 실무자들에게 추가적인 계획을 수립하는데 도움이 될 것으로 기대된다.

참 고 문 헌

[1] Australian Goverment, *Cyber Storm II-National Cyber Security Exercise Final Report,* 2008.
[2] P. H. J. Davies, “Intelligence, Information Technology, and Information Warfare”, Annual review of information science and technology, Vol. 36, 2002.
[3] FEMA, A Nation Prepared Federal Emergency Management Agency Strategic Plan, 2001.
[4] Jason Kick, “Cyber Warfare Exercise Overview”, MITRE, 2005.
[5] U. S Department of Homeland Security, Homeland Security Exercise and Evaluation Program, Vol. 4, 2006.
[6] 김종훈 외, “국가 주요기반 구조 보호를 위한 정보전 대응체계 연구”, WISE 99호, 1999.
[7] 박홍국, 전기정, *의사결정지원시스템*, 경문사, 1999.
[8] 신유근, *경영학원론,* 다산출판사, 2006.
[9] 육군본부, 야전교범 5-14 : 사이버전, 육군본부, 2002.
[10] 육군본부, 야전교범 7-10 : 교육훈련관리, 육군본부, 2004.
[11] 육군본부, 야전교범 101-1 : 지휘관 및 참모업무, 육군본부, 2003.
[12] 육군본부, 야전교범 5-14 : 사이버전, 육군본부, 2002.

권 문 택
1970년 육군사관학교(이학사)
1981년 미국 University of Iowa(공학석사)
1987년 University of Wisconsin (경영정보학 박사)
경희대학교 테크노경영대학원 정교수
경희대학교 정보지원처장
경희사이버대학교 초대 학장