미 래 사 이 버 전 쟁 능 력 필 요

오 제 상*

순 서

*국방대학교

1. 사이버 전 능력 및 무기들

○ 오늘날의 정보기술 분야의 발전 추세로 판단하여 볼 때에 미래 전쟁은 사이버 전쟁 양상으로 나아갈 것이 필연적이라 판단된다. 본 논문에서는 "사이버 전의 능력 확보 및 기술/무기 예측"에 관하여 소개하고, "주변국 및 선진국들의 사이버 전 기술능력 및 현황"을 고찰하고, 사이버 기술/무기들 중에서 가장 핵심 전력이라 할 수 있는 미래 지식 전쟁에 대비한 최소한의 "사이버 전투 부대구조와 임무"에 대하여 언급한다.

○ 정부의 사이버 전 관련 의지

현재 정부에서 추진하고 있거나 추진할 예정인 개혁 과제들 중에서 미래 사이버 군의 필요성과 관련된 과제들을 살펴보면 다음과 같이 4가지 과제들로 구분할 수 있다. 첫째는 장차 육.해.공군의 무기체계가 모두 탐지로부터 타격까지 실시간으로 연동되는 국방통합정보체계(합동전장정보화체계)를 건설한다(국방부장관 국방정보화 전략회의 훈시문중에서, 2001.1.30)는 것이고, 둘째는 국가적인 정보화 추진차원에서 계속적으로 추진하고있는 장병 정보화 교육의 일환이며, 셋째는 현대전은 정보통신전으로 발전되고 있는 만큼 장병들의 정보통신 교육 강화 및 해킹 문제에 대한 주의 및 지시와 군의 컴퓨터 해킹을 통한 정보 교란 등 "사이버 테러"에 대비한 방안을 마련하라는 지시가 있었다 (대통령 지시사항, 2000. 2. 18, 국방부 업무보고 시). 넷째는 유사시에 활용 가능한 "사이버 방위군" 10만 명의 해커를 양성할 필요성이 있음을 정부부처에서 보고한 바가 있다(정통부장관 연두 업무보고 중에서, 2000. 3. 27).

그리고 주변국 및 선진국들은 해커 부대창설, 해킹 능력 보유자를 국가적으로 포용하고, 법령을 수정하여 해커들을 양성하는 방향으로 법제화하며, 사이버 윤리교육을 초등학교 교육과정에 반영하는 등의 시대적인 변화에 적응을 적극적으로 순응하고 있는 반면에, 국내에서는 실효성이 미약한 일부 학계에서 10만 해커 양병설을 주장하지만 정부에서는 해커 포용, 법제화, 양성화 등의 특별한 정책이 미진한 실정이라고 해커협회에서는 지적하고 있다.

미래 사이버 군이 적의 정보통신체계를 마비 및 무력화시킬 수 있는 인력 및 무기로써는 전문 해킹 인력 양성, 바이러스 및 사이버 무기, 비살상 무기 등을 경제적으로 연구개발 및 획득할 수 있어야 할 것이다.

○ 미래 학자 엘빈토플러의 주장

엘빈토플러의 제3의 물결 전쟁에서 주장은 21세기에는 무기체계를 판매하는 판매국이 향후 국제정세 변화 및 판매하는 무기의 수명을 고려하여 외국에 판매할 경우에 무기체계에 대하여 판매하기 전에 미리 소프트웨어적으로 정해진 특정조건이 충족되면 그 무기체계의 소프트웨어 체계가 자동으로 작동되어 그 무기체계가 스스로 자폭하거나 혹은 그 체계의 조종이 불가능한 상태 등이 되되록 하는 치핑(chipping : 소프웨어적으로 위치 혹은 기타 정보자료를 이용하여 미리 설정되어 있는 주어진 조건이 충족되면

설치자의 의도대로 자동적으로 작동하는 장치) 창치를 구매국이 알지 못하도록 설치하여 둠으로써, 향후 국제정세의 변화로 인하여 자국이 판매한 무기체계에 의하여 자국이 공격을 받지 않도록 하는 스마트(치핑) 장치를 설치하기 때문에, 타국으로부터 믿고 구매할 할만한 무기체계가 없을 것이라고 주장한다[1]. 이러한 주장이 대단히 설득력이 있는 주장이라는 것은 오늘날 무기체계가 컴퓨터 소프트웨어에 의하여 대부분이 자동화 제어체계로 구축되어있기 때문이다. 그래서 국방 무기체계는 타국에 의존할 수 없는 체계라고 미래 학자 엘빈토플러의 주장하고 있다.

○ 사이버 전 공격 무기들

미래 전쟁에서 정보작전의 전 범위에 걸쳐 정보우세를 성취하기 위하여, 실시간 가시화 전장, 실시간 지휘관 결심, 실시간 전투원의 공격 혹은 방어적인 조치를 가능하게 하기 위하여 실시간 탐지/타격 체계(sensor to shooter systems)의 기반구조가 국방정보통신체계로 구성되어야 하고, 이러한 아군의 국방정보통신체계를 적의 공격으로부터 보호할 수 있는 능력을 구비하여야 하며, 반면에 유사시에 적의 국방정보통신체계를 마비시킬 수 있는 정보공격 무기(그림 1.1 참고)인 해커, 바이러스, 전자기 파 폭탄(electromagnetic pulse bomb : EMP), 기타 사이버 무기 등을 확보하여야 할 것이다.

그림 1.1 사이버 전 공격 무기(예)

○ 사이버 능력 구비 방안 강구해야

미래 사이버 전쟁에서는 적의 정보자원을 효과적으로 공격할 수 있는 능력을 확보하여야 하며, 그러한 능력을 확보할 수 있는 방안은 다음과 같은 3가지 방안을 강구하여

야 할 것으로 판단한다. 첫째는 전문 해킹 요원을 양성하는 방안을 강구하여야 할 것이고, 둘째는 신종 바이러스, 논리폭탄, 등 신종 사이버 무기를 효과적으로 연구 개발하는 방안을 강구하여야 할 것이고, 셋째는 정보통신체계를 마비시키는 비살상 무기(전자기 펄스 탄, 고출력 마이크로웨이브 총, 고출력 섬광 탄, 흑연 섬유 탄, 등)를 효과적으로 연구 개발하는 방안을 강구하여야 할 것이다. 그리고 사이버 전 무기들 중에서 비살상 무기인 물리적인 EMP 폭탄에 대한 위력을 다음과 같이 소개한다.

○ **전자기파(EMP) 무기의 위력**

* 직접 에너지(DEW) 무기

직접 에너지 무기는 전자 광학적인 정보통신 망 체계의 물리적 구성품에 대하여 치명적인 손상 및 마비를 유발 가능한 잠재 능력을 제공한다. DEW(directed energy weapon) 무기는 레디오 주파수(RF), 레이저, 입자 에너지 무기로 사용되며, DEW를 응용하여 공격거리 및 용도에 따라서 무기운용에 대한 주요 작전 개념은 단거리의 법집행용 HERF(high energy radio frequency) 총, 중거리의 전자기적 공격용 EMP 탄, 장거리의 레이저나 EMP 빔을 조사하는 무기를 운용할 수 있으며 직접 에너지 범주가 다음 <표1.1>과 같이 구분된다.

특히 RF 에너지 무기(EMP)의 폭발은 자연의 번개처럼 짧은 시간에 강렬한 효과를 제공하며, 지구표면상에 전자기 파동을 유발시키는 원거리선(line)으로 연결되어진다. 만약에 고공 300 마일에서 10KT(백만Kg) 무게의 EMP 탄 한발을 투하하면, 미국 대륙크기의 지역에 영향을 줄 수 있다.

그리고 핵탄이 폭발하면 폭풍(55%), 열(30%), 초기방사선(15%), 잔류방사선에 의한 방사능 오염과 전자기 파동(EMP)이 발생한다. 이 전자기파는 핵 폭발시 방출되는 초기 감마 방사선 전체 방출 에너지의 0.003%가 주위 공기중의 원자들과 상호작용을 일으켜 1MHz에서 수백 MHz에 이르는 강력한 전자기를 발생시키며, 이전자기 파는 상당히 광범위한 지역에 반도체와 각종 전자장비인 첨단 군사장비, 미사일, 항공기, 전산망, 등에 치명적인 손상을 시켜서 무용지물의 고철로 만들어 버릴 수 있다. 실험에 의하면 병사들이 소지하고있는 시계, 전화기, 레디오, 군용차량, 전자수첩, 계산기 등에 이르기까지 기능이 파괴되어 버린다고한다.

그리고 다음의 <표 1.2>에서는 각종전자소자들이 전자기 파(EMP)로부터 공격을 받았을 때에 전자장비가 정상작동으로부터 EMP 방해 에너지와 파괴 에너지 량에 따른 영향을 나타낸 것이고, 또한 <그림 1.2>은 재래식 폭탄인 MK84의 외형을 이용여 개발한 EMP 폭탄의 구조와 폭발시에 방사하는 전자기 방사 패턴을 그림으로 표현한 것이다.

<표 1.2>에서 EMP탄의 각종 전자소자에 대한 영향을 볼때에 컴퓨터 및 정보통신망에 핵심부품인 RAM/ROM 칩 등이 가장 미소한 에너지에도 치명적인 영향을 받아 마비될 수 있다.

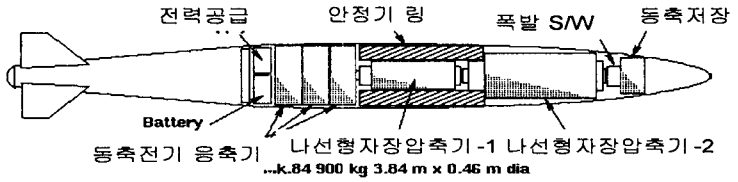
<표 1.1> 직접 에너지 무기(DEW)[2]

DEW 범주	특 성 / 내 용	비 고
RF 에너지 무기	- RF 전자기 에너지에 민감한 적의 전자장치에 RF 전자기 에너지를 조사하면 반도체와 결합하여 전기적인 과부하를 유발하며, 저항성분이 없는 축전기, 유도회로, 전산 레지스터 등은 과부하에 민감하게 파괴 - HPM(high power microwave): 고전력 고주파 무기로서 좁은 밴드폭, 좁은 빔 폭, 고주파 에너지, 고전력 레이더와 같이 방출됨 · 전력: 메가와트에서 수십 기가와트 까지, · 주파수: 10MHz에서 100GHz 까지 - EMP: 전자기 전파는 3가지 수단에 의해서 생성가능하며, 자연의 번개발생과 유사함 · SG(system generated)EMP : 전리선과 전자생성 장비와 결합으로 EMP 발생 · Switching EMP : 일시적 반복적 과도전류 발생으로 파괴 · G(generated)EMP : 압축된 펄스의 저장과 방출로 파괴	· RF에너지 무기 2가지종류
고 에너지 레이저 (HEL) 무기	- 평균 수배KW의 전력을 생성 가능한 화학적인 구동 레이저는 장거리에 있는 전자광학 센서(추적기, 거리측정기, 감시기, 전자광학 센서 등)의 고강도 광량장치를 표적으로 삼는 레이저 무기로서 잠재력을 제공 -미공군 공중 고출력 레이저 무기로 표적 미사일에 조사하여 가열/파괴 - HEL 무기는 대기전달(흡수, 산란, 교란), 빔 조사 지점 안정성, 표적의 표면 특성에 대단히 민감함.	· 미공군 화학적 산소 옥도 레이저 보유

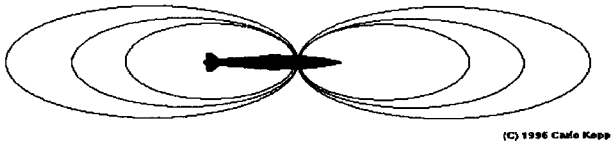
<표 1.2> 각종 전자소자에 대한 EMP 영향[3]

전 자 소 자	작동방해 에너지(J)	소자파괴 에너지(J)
RAM/ROM 칩	$10^{(-7)}$	$10^{(-6)}$
HF 트렌지스터(TR)	$10^{(-6)}$	$10^{(-5)}$
S/W 다이오드 TR	$10^{(-5)}$	$10^{(-4)}$
신호 다이오드 정류기	$10^{(-4)}$	$10^{(-3)}$
릴레이(접점용해)	1	10
파워 다이오드	10	100

EMP 폭탄의 구조 및 방사 페턴



저 주파수 EMP 폭탄 구조



자장 압축 변환기로부터 방사페턴

그림 1.2 EMP 폭탄의 구조/방사 페턴

2. 주변국 사이버 전 기술 능력 현황(4)

주변국들의 사이버 전에 관한 능력 및 현황을 사이버 기술 및 무기들을 중심으로 다음과 같이 알아본다. 그리고 그림 2.1에서는 미래 사이버 전의 수행도를 표현한 것으로써, 아군의 통합된 국방정보통신체계로써 실시간 작전운용은 물론이고 해커들은 적의 정보통신체계를 공격하기 위하여 적의 정보 해킹, 바이러스 유포, 각종 에이전트 설치 등으로 적의 정보를 마비, 절취 등을 수행할 것이고, 또한 항공기 등을 이용하여 물리적인 비살상 무기인 EMP 폭탄 등의 DEW 무기를 사용하여 적의 국방정보통신체계들을 마비시키기 위하여 공격할 것이다.

2.1 미국의 사이버 전 현황

2.1.1 사이버 전 방어

○ 미국방성은 1998년 9월에 미국군이 운영하고 있는 인터넷 관련 사이트에 게시하여 둔 다음과 같은 미군의 주요정보들을 삭제할 것을 지시하였다.

(가) 미국에 대한 잠재적 적들을 이롭게 하는 정보

(나) 미국 군인들을 위험에 처하게 할 수 있는 정보

○ 1998년 여름, 미국 중앙정보국 국장 의회 및 증언에서 다음과 같은 내용들을 발표하였다.

(가) 10여 개국 이상이 해킹 전문 프로그램을 개발하고있으며,

(나) 미국에 적대적인 국가들도 포함되었음을 발표

그림2.1 공격적 사이버 전 수행도

○ 국방성 예하 연구소인 DARPA의 연구개발 전략 및 내용은 다음의 그림 2.2와 같으며, 그것들에 대한 내용을 간략히 설명한 것이 다음과 같다.

(가) 전략적 침입평가(Strategic Intrusion Assessment) 기술개발
- 현재 이용 가능한 침입 탐지 센서와 탐지기 분배 구조의 개선
- 지역탐지기의 정보공유 및 잘못된 탐지에 대한 알람 제거
- 공격자 추적 및 다음 행동 예측 알고리즘
- 피해평가 기능개발 및 피해수집 방법론 개발

(나) 침입 감내 시스템(Intrusion Tolerant Systems) 기술개발
- 침입과 결함이 발생한 상황에서도 데이터와 프로그램의 일관성을 유지하기 위한 기술
- 서비스 거부 공격에 대응하는 기술과 높은 시스템 가용성을 유지하는 기술

(다) 고장 감내 네트워크(Fault Tolerant Network) 기술개발
- 고장 감내 생존성
- 서비스 거부 장치
- 액티브 네트워크 대응

그림 2.2 국방성(DARPA) IT 연구개발 전략

(라) 동적 협력(Dynamic Coalitions) 프로그램 개발 체계
- 다차원 보안정책 관리
- 안전한 정보보호 관련기관/업체 관리
- 인증관리 기반구조간의 상호인증, 도메인 보안정책

(마) 정보보증(Information Assurance) 기술개발
- 기존의 다양한 보안관리를 통합환경에서 관리
- 운영체제는 내장 프로세서 개념을 도입하여 신뢰할 수 없는 프로그램은 보안 매니저가 프로세스 실행
- 침입탐지 및 격리 프로토콜을 공통 침입탐지 프레임워크로 개발

(바) 정보보증 과학 및 공학(Information Assurance Science & Engineering) 개발
- 설계와 평가를 위한 통합된 환경과 도구개발
- 논리, 추론 및 의사결정 등에 사용되는 수학 및 모델개발

(사) 자율적 정보 보증(Autonomic Information Assurance) 기술
- 자동화된 공격에 대응하기 위한 자동화된 방법 개발
- 방어통제 시스템의 프로토타입 개발
- 운영체제, 방화벽, 응용, 데이터베이스 별로 대응할 수 있는 방법과 기능 정립

(아) 사이버 지휘통제(Cyber Command & Control) 기술개발
- 자동으로 상황인식 및 전파
- 대응방책 개발 및 수행
- 의사소통 및 피해평가

2.1.2 사이버 전 공격

○ 미국 국방성과 중앙정보국은 1998년 7월에 사이버 전쟁에 관한 다음과 같은 조치를 취하였다.

(가) 사이버 전쟁에 대처하기 위한 본격적인 공격 및 방어 정책을 검토

(나) 적의 군사, 정보 전산망과 컴퓨터를 해킹으로 공격하는 컴퓨터 해킹 부대를 창설하고 국비훈련에 들어 갔음

○ 영국 가디안지 보도내용(1998. 7)

(가) 미국은 해킹을 전시에 공격수단으로 적극적으로 활용하는 방안 추진

(나) 미국 국방성은 사이버 공격작전에 중점을 두고 내부개편 실시

(다) 군 지휘관들에게 사이버 공격수단을 염두에 둔 작전계획 수립 지시

○ 컴퓨터 해커를 이용한 전술들을 연구개발 중

(가) 적 방공망 무력화

(나) 주요 도시 전화망 마비

(다) 허위정보 입력

○ 사이버 무기 연구개발

(가) 컴퓨터 바이러스, 트로이목마, 논리폭탄 등

(나) EMP, HPM, HERF Gun 등

○ 미국 국방성은 조직개편을 1999년 하반기에 다음과 같이 수행하였다.

(가) 미국 공군 우주사령부(콜로라도)가 사이버 전쟁의 총책임을 맡음

(나) 대서양사령부(버지니아) : 사이버전쟁 통합사령부(1999. 10)로 지정

○ 사이버 전쟁 개념변화

(가) 수비위주에서 ⇒ 공격 · 수비위주(셜던 합참의장)

(나) 사이버 전 개념정립 특별팀 운영 : 36명

(다) 정보전 프로그램 강화예정(2000. 10)

○ 민간 해커 사이버 전쟁

(가) 1999. 4. 7. 미군 전투기가 유고 베오그라드 주재 중국 대사관을 폭파한 사건으로 중국과 미국간에 민간 해커들이 자국을 위한 사건/ 피해/ 대응 등을 홍보 및 상대국 국가기관 정보통신망을 공격한바 있다.

(나) 2001. 4.1 중국남단의 해남도 부근 상공에서 발생한 중국 전투기와 미국 EP-3 정찰기의 충돌 사고로 해남도에 미국 EP-3 기가 비상착륙한 사건으로 양국간에 민간 해킹 사이버 전쟁으로 발전되어 갔다. 해커 조직인 "중국 프로젝트(Project of China)" 그룹(7-8 개의 민간 해커 그룹 연합)이 등장하여 더욱더 공격이 치열하였으며, 중국의 수백여개의 민간기관 및 공공기관의 사이트를 공격하였다. 친미국의 해커들은 사우디아라비아, 인도, 브라질, 아르헨티나, 파키스탄이고, 친중국 해커들은 일본, 인도네시아 등이라고 한다.

2.2 중국의 사이버 전 현황

2.2.1 사이버 전 방어

○ 정보망의 생존성 보장에 초점

○ 군 정보망 특성 제시

(가) 다중설비, 다중 라벨, 다중 밴드, 다중 전원 등

(나) 각 노드들이 정찰, 버그등에 대한 대비책 보유

(다) 생존능력과 융통성 보유

(라) 은익이 잘되고 다양한 조건에서도 동작 가능

2.2.1 사이버 전 공격

○ 미하원 제출 보고서(1997. 6)

(가) 바이러스부대 창설(1000여명 규모)

(나) 컴퓨터 바이러스를 침투시키는 전략이 원자탄을 사용하는 것보다 더 효율적임(중국중앙군사위원회)

○ 인민해방군 도상전쟁 및 훈련 시나리오(미의회 제출보고서, 1998)

(가) 오판 유도 정보입력

(나) 데이터 변경

(다) 컴퓨터 작동 중지

(라) 해커 활용

○ 최근의 공격사례 및 준비

(가) 미국, 나토, 일본, 대만 등에 공격(1998년 이후)

(나) 중국과 대만의 양안 전쟁주에 대만에 72,000건 공격(2000. 8)

(다) 사이버전쟁 담당기구 창설 검토중

(라) 중국은 대만의 사이버 전쟁 능력을 추월한 것으로 예상

○ 민간 해커 사이버 전쟁

(가) 1999. 4. 7. 미군 전투기가 유고 베오그라드 주재 중국 대사관을 폭파한 사건과 2001. 4.1 중국남단의 해남도 부근 상공에서 발생한 중국 전투기와 미국 EP-3 정찰기의 충돌 사건으로 미국의 민간 및 공공기관 사이트를 공격하는 중국의 대표적인 해커 그룹은 "중국 홍객 연맹(中國紅客聯盟 Honkers Union of China)"이 주도적인 민간 해커 그룹이다.

2.3 러시아의 사이버 전 현황

2.3.1 사이버 전 방어

○ 통신 시스템 분야

(가) 통신 시스템 수입 최소화

(나) 외국업체와의 합작 강조

○ 논리폭탄, 바이러스 등의 위협대비책 강구

(가) 바이러스 탐지 및 파기를 위한 파라메터 설정

(나) 방어 프로그램 개발

2.3.2 사이버 전 공격

○ 공격능력 확보

(가) 바이러스, EMP탄, HERF Gun, 레이저 등

○ 공격사례

(가) 미 우주해양 시스템 센터의 네트워크의 정보를 가로채어 전송(1999. 6)

(나) 체첸 반군이 RF 무기사용

○ 무기연구

(가) HERF GUN, 음파무기

(나) 심령술 등

2.4 주변국 사이버 전 공격 능력 요약

구 분		내 용
미 국	사이버전 공 격	· 미공군 사이버 전쟁 총책임부대 : 미공군 우주사령부(콜로라도 위치) · 사이버 무기개발 : 해킹 기법, 바이러스, 트로이목마, 논리폭탄, Chipping, AMCW 등 . 전세계 전자우편, 팩스 및 유무선통신 감청기관(Echelon) 운영 . 비살상 공격무기인 EMP, HERF-GUN, 레이저 등의 전자기파 무기 . 육해공군에 사이버 전 전담부대 있음[8] * 사이버 전시 해킹을 공격수단으로 전술개발 중
중 국	사이버전 공 격	· 사이버군 창설 : 해킹/바이러스부대 창설(1000여명 규모) · 사이버 전쟁 담당기구 창설 검토중 · 사이버 무기개발 : 해킹 기법, 바이러스, 트로이목마, 논리폭탄, Chipping, AMCW 등
러시아	사이버전 공 격	· 비살상 공격 무기 연구 : 바이러스, EMP, HERF-GUN, 레이저 등의 무기 · 사이버 무기개발 : Chipping, AMCW 등

2.5 기타 국가 해커 국방분야 활용 사례

○ 아랍 해커들, 유대인 웹사이트 집중 공격

2001년 초에 5주간 계속되고 있는 이스라엘과 팔레스타인간의 유혈 충돌이 최근 사이버 세계로 까지 확산되고 있다. 아랍 해커들이 이스라엘과 미국의 유대인 웹사이트들을 집중 공격하였다.

2001. 2 2일 친 아랍 계의 파키스탄 인으로 추정되는 해커들이 미국에서 활동 중인 친 이스라엘 성향의 유대교 랍비의 웹사이트를 해킹, 사이트 회원들의 개인정보를 빼내 이스라엘 계의 미국인 공공위원회(AIPAC)의 웹사이트에도 누군가가 침입해 기부자들의 신용카드 번호를 훔쳐내 인터넷상에 공개했다. 2001.2.3일에는 아랍 회교도라고 밝힌 해커들이 유대교 성경협회(JBA)와 이스라엘 방문학생 협회(VISA), 이스라엘 민간회사

의 웹사이트에 침입해 팔레스타인 희생자들의 사진과 함께 이스라엘을 비방하는 문구를 남겼다.

○ 영국 사이버 경찰대 창설

영국은 2000만 파운드(400억원)의 예산을 투입하여 인터넷 사기, 아동 성범죄자, 해커 등과 싸울 사이버 경찰대를 창설할 계획이라고 선데이 타임지가 보도(2001년 2월12일)했다. 영국 내무성은 "사이버 범죄가 가장 중요하고 어려운 도전이며 이는 최고 수준의 기술로만 대응할 수 있다"고 한다.

○ 독일 해커의 미국 ICANN 발상은 불법 주장

미국정부가 미국의 ICANN(Internet Corporation for Assigned Name and Number) 위원회를 통해서 미국이 세계 인터넷의 중심이고 계층적인 네임 시스템에 영향력을 발휘하고 있으므로, 유럽의 인터넷 사용자에 의해 선출된 5명의 지부장 가운데한 사람인 독일 해커 엔디 뮤러마군은 미국의 ICANN의 발상은 미국의 기술적인 제국주의의 도구이고 또한 ICANN은 전혀 합법적인 위원회가 아니라고 비난하며, 세계 해커들이 자신들이 어떻게 생각하고 있는지 이야기 해야하고, 해커는 해킹을 배우고자하는 동기에 의하여 유발되는 중대하고 창조적인 기술을 취급하는 것으로 생각해야 한다고 주장하였다. 해킹은 새로운 기술에 대한 탐험이며 정보의 자유를 돕는 것이며, 1980년대 초기와 오늘날을 비교하면 그 당시 NASA 해킹 사건은 지금 보면 아무런 문제가 되지 않으며 그 정도는 지금은 인터넷 서핑이라고 한다.

3. 미래 지식 전쟁 대비한 사이버 전투 부대 구조

○ 미국군의 미래 정보전에 대한 조직을 고찰해 보면, "The Future of War"라는 제목 하에 Timothy L. Thomas retired U.S. Army Lieutenant Colonel라는 사람이 InfowarCon 2000, 2000년 7월에 발표한 자료에 의하면, 미군의 정보보호를 위한 사이버 테러 대응 조직이 각 군의 CERTs가 별도로 있고 정보전쟁을 위해서는 각군에 정보전 본부(에; air force information warfare center)가 별도로 존재함을 알 수 있다[8].

예를 들어 미국 공군의 정보전 본부(air force information warfare center)의 임무는 정보전투공간을 통제하기 위하여 정보 검색, 개발, 응용과 대응 정보 기술, 전략, 전술과 자료를 통하여 유리한 정보전을 수행할 수 있도록 하는 것이 정보전 본부의 탁월한 임무이라고 한다.

○ 다음 <표 3.1>은 미래의 정보전에 대비한 조직을 예상하여 본 것이다.

<표3.1> 사이버 전투 부대 구조(예상)

정보보호 실	정보감시/복구 실	정보마비 실	정보평가/모의 실
. 체계보호 팀	. 감시/관제 팀	. 암호해독 팀	. 정보 평가분석 팀
. 네트웍 보호 팀	. 침해추적 팀	. 해킹 기법개발 팀	. 정보 표준화 팀
. 암호설계 팀	. 피해복구 팀	. 바이러스 개발 팀	. 정보 모델/모의화 팀
. 체계운영유지 팀	. 네트웍/장비 팀	. 사이버 무기 팀	. 정보 교육/훈련 팀

○ **미래 사이버 전 공방 능력 구비**

* 경제적인 군의 인력 및 자원 운용을 위하여, <표 3.1>의 군의 사이버 전투 부대 구조에서 방어적인 임무를 수행하는 정보보호 실 및 정보감시/복구 실은 기존의 정보통신체계의 운영 부서의 운영 요원들과 CERT팀 요원들을 활용하여 조직화할 수 있을 것이라 판단한다.

* 위 조직 표 <표 3.1>에서 보는바와 같이 각 군의 공격임무(Red Team 역할 : 가상 해커팀)를 수행하는 정보마비 실 및 정보평가/모의 실은 미래 사이버 전투에 대비하고 아군의 정보통신체계의 위협과 취약점을 평가 및 분석하여 정보통신체계의 보호방안을 강구해야할 것이며, 적의 정보통신체계의 위협과 취약점을 탐색하여 마비시킬 수 있는 해킹, 바이러스, 사이버 무기기술, 암호해독, 등을 연구개발 및 교육훈련을 수행할 수 있는 신규 사이버 전투 조직창설이 이루어져야 할 것으로 판단한다.

4. 맺는 말

○ 사이버 전 공격 기술 및 무기는 재래식 물리적 공격 기술 및 무기와 미래 사이버 전쟁의 소프트웨어적 공격기술/무기로 구성되어 있으며, 미래 사이버 전에서는 물리적 공격 기술 및 무기보다 소프트웨어적 공격기술이 수십 배로 경제적이고 효과적인 공격 기술 및 무기인 것으로 부각되고 있다.

○ 결론적으로 미래 사이버 전쟁에서 가장 핵심 공격 기술 및 무기는 해커이고 해커의 조기 양성 및 획득은 필수적인 사이버 전력 확보 방안이므로 사이버 전을 수행할 수 있는 전투부대의 지식을 제공하는 사이버 전쟁 연구소와 전투부대를 창설하는 것은 피할 수 없는 시대적인 요청에 의하여 절대적으로 필요한 조직일 것으로 판단한다.

참 고 문 헌

[1] "전쟁과 반전쟁", 엘빈 토플러, 한국경제신문사 번역, 1996. 3.
[2] "Information Warfare Principles and Operations", Edward Walts, Artec House, 1998.
[3] "21세기 군사혁신과 한국의 국방 비젼", 권태영외 다수인, 한국국방연구원, 1998. 8.
[4] "정보전 체계 설계 및 구축 방안", 박재근, 오제상, 윤현철, 국방과학연구소, 2000.11.
[5] "월간 마이크로 소프트웨어, 2001.2월호", 마이크로 소프트 사, 2001. 2. pp186-211].
[6] "월간 인터넷, 2001. 02월호", 2001. 2. pp120-123].
[7] "2000 정보 시스템 해킹.바이러스 현황 및 대책", 한국정보보호센터, 2000. 12.
[8] "The Future of War", Timothy L. Thomas Retired U.S. Army Lieutenant Colonel, InfowarCon 2000, 2000. 7.