# 사이버 정보전 준비 해야

오 제 상*
* 국방대학교 정보화 소요공학실

## 요 약

오늘날의 정보기술 분야의 발전 추세로 판단하여 볼 때에 미래 전쟁은 사이버 전쟁 양상으로 나아갈 것이 필연적이라 판단된다. 사이버 전에서의 공격은 민.군 정보통신체계를 막론하고 가능하며, 특히 국방 C4ISR 체계에 해킹, 바이러스, 전자기파 폭탄 공격이 가해진다면 군사작전은 마비 및 대혼란이 야기될 것이다. 그리고 물리적인 거리, 시간, 날씨, 공간에 구애받지 않고 실시간으로 공격이 가능하기 때문에, 전쟁비용이 초저비용인 반면 공격효과는 인명 엄청난 파급효과인 정보마비, 국민혼란, 전시공포, 약탈, 범죄 등에 효과적인 공격무기로 높이 평가받고 있다. 본 논문에서는 "사이버 전의 공격무기"에 관하여 소개하고, "주변국들의 사이버 전 공격능력 및 현황"을 고찰하고, 사이버 기술/무기들 중에서 가장 핵심 전력이라 할 수 있는 미래 지식 전쟁에 대비한 최소한의 "사이버 전투 조직과 임무"에 대하여 언급한다.

# Future Cyber Information Warfare

Oh Che Sang*

## ABSTRACT

Currently if we are to make a thought to depend on our fast developing information technology, a future war is necessarily to be made a situation of a cyber information warfare. A attacker in the cyber information warfare is able to make attack a military or a civil information and communication system, especially if a attack of a hacker, a virus or a electromagnetic pulse bomb at a military C4ISR system is able to make a confusion or a interruption in military operations, they are available to attack as a real time with non restrictions of physical distance, time, weather and space. While a expenditure of carrying out the cyber information warfares is the lowest expenditure, a effect of carrying out the cyber information warfares is the greatest effect in side of a interruption of information, a confusion, a terror, a pillage and crime of the people. This paper is to introduce "weapons of cyber information warfares", "offence capability of cyber information warfares about several nations" and to propose "a cyber information warfare organization" for the future knowledge warfare.

# 1. 서 론

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 되도록 하는 치핑(chipping : 소프웨어적으로 위치 혹은 기타 정보자료를 이용하여 미리 설정되어 있는 주어진 조건이 충족되면 설치자의 의도대로 자동적으로 작동하는 장치) 장치를 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.

# 2. 사이버 정보전 무기들

## 2.1 사이버 전 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(그림2.1과 그림2.2 참고)인 해커, 바이러스, 전자기 파폭탄(electromagnetic pulse bomb : EMP), 기타 사이버 무기 등을 확보하여야 할 것이다.

그림2.1 사이버 전 SW공격무기

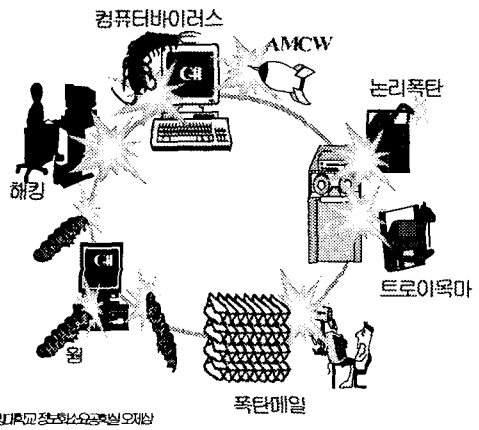
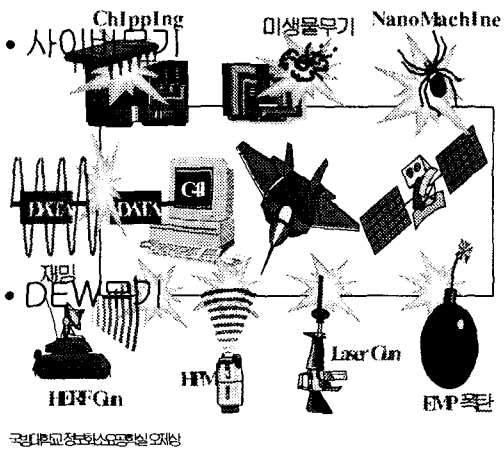



그림2.2 사이버전물리적공격무기



### 2.2 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 강구하여야 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 전자기 펄스(EMP) 폭탄에 대한 위력을 다음과 같이 소개한다.

### 2.3 전자기파(EMP: ElectroMagnetic Pulse Bomb) 무기의 위력

직접 에너지 무기(DEW : directed energy weapon)는 정보통신 체계의 물리적 구성품에 대하여 치명적인 손상 및 마비를 유발 가능한 잠재 능력을 제공한다. DEW 무기는 레디오 주파수(RF), 레이저, 입자 에너지 무기로 사용되며, DEW를 응용하여 공격거리 및 용도에 따라서 무기운용에 대한 주요 작전 개념은 단거리의 범 집행용 HERF(high energy radio frequency) 총으로 헌병이 도주하는 차량을 쏘면 도주차량이 엔진이 꺼지고 정지하며, 중거리의 전자기적 공격용 EMP 탄은 전투기, 포 등으로 공격이 가능하며, 장거리의 EMP 탄, 레이저 빔을 조사하는 무기는 우주선 대 우주선, 우주로 올라오는 탄도탄 공격에 운용할 수 있다. 특히 전자기파 무기의 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 대륙 크기의 지역 내에 존재하는 정보통신체계에 나노초~1분내에 마비/무력화에 영향을 줄 수 있다

## 3. 주변국 사이버 전 공격능력

주변국들의 사이버 전 공격 능력 및 현황을 다음과 같이 알아본다. 아군의 통합된 국방정보통신체계(C4ISR)로써 실시간 지휘통제는 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 전자기 파 폭탄 등의 전자기 무기를 사용하여 적의 국방정보통신체계들을 마비시키기 위하여 공격할 것이다.

<표 1> 주변국 사이버 전 공격 능력 현황

| 구 분 | | 현 황 |
|---|---|---|
| 중국 | 사이버 전 공격 | · 사이버군 창설 : 해킹/바이러스부대 창설 (1000여명 규모)<br>· 사이버 무기개발 : 해킹 기법, 바이러스, 트로이목마, 논리폭탄, 치핑, AMCW, 저주파음파, 전자기파폭탄, 레이저 등 |
| 러시아 | 사이버 전 공격 | · 비살상 공격 무기 연구 : 바이러스, 전자기파폭탄, 전자기 총, 레이저 등의 무기<br>· 사이버 무기개발 : 치핑, AMCW, 음파무기,심령술 등 |
| 대만 | 사이버 전 공격 | · 대만 국방부 사이버 전 수행 부대 창설 결정(2000.11)<br>· 해커로부터 군용 정보통신체계 보호용 관제체계 구축 등[7] |

<표 1> 주변국 사이버 전 공격 능력 현황(계속)

| 구 분 | | 현 황 |
|---|---|---|
| 미국 | 사이버 전 공격 | · 미공군 사이버 전쟁 총책임부대 : 미공군 우주사령부(콜로라도 위치)<br>· 사이버 무기개발 : 해킹 기법, 바이러스, 트로이목마, 논리폭탄, 치핑, 자동이동 사이버 무기(AMCW) 등<br>· 전세계 전자우편, 팩스 및 유무선 통신 감청기관(Echelon) 운영<br>· 비살상 공격무기인 전자기파폭탄(EMP), 전자기 총, 레이저, 입자무기 등<br>· 육해공군에 사이버 전 전담부대 있음[5]<br>· 사이버 전시 해킹을 공격수단으로 전술개발 중 |
| 일본 | 사이버 전 공격 | · 일본 정부 해킹, 바이러스, 전자기파폭탄 등에 대처할 국가기관 필요(2000.1)<br>· 일본 방위청 2000년 백서에 사이버 전 부대 창설[7] |
| 싱가포르 | 사이버 전 공격 | · 공세적 사이버 전 작전요구 충족위한 국방부 내에 사이버 전 전담부대 창설[7]<br>· 군용정보통신체계 보호 위한 연구조직 창설 |
| 북한 | 사이버 전 공격 | · 북한은 평양자동화대학(옛미림대학)해커 100여명 양성중이며, 해커 능력은미국 CIA나 국가 보안국(NSA) 수준으로 판단함[6,7]<br>· 사이버 무기개발 : 해킹 기법, 바이러스 등 |

# 4. 미래 지식 전쟁 대비한 사이버 전 조직

미국군의 미래 정보전에 대한 조직을 고찰해 보면, 미군의 정보보호를 위한 사이버 테러 대응 조직이 각 군의 CERTs가 별도로 있고 정보전 수행을 위해서는 각군에 정보전 본부(예; air force information warfare center)가 별도로 존재함을 알 수 있다[5]. 그리고 미국 공군의 정보전 본부(air force information warfare center)의 임무는 정보 전투공간을 통제하기 위하여 정보 검색, 개발, 응용과 대응 정보 기술, 전략, 전술과 자료를 통하여 유리한 정보전을 수행할 수 있도록 하는 것이 정보전 본부의 임무이라고 한다.

## 4.1 미래 사이버 전 공방 능력 구비

다음 <표4.1>은 미래의 사이버 전쟁을 수행할 사이버 전 센타 조직을 예상하여 본 것이다. 경제적인 군의 인력 및 자원 운용을 하기 위하여, <표 4.1>의 군의 사이버 전투 조직에서 방어적인 임무를 수행하는 정보보호 실 및 정보감시/복구 실은 기존의 정보통신체계의 운영 부서의 운영 요원들과 CERT팀 요원들을 활용하여 조직화할 수 있을 것이라 판단한다. 그리고 조직 표 <표 4.1>에서 보는바와 같이 각 군의 공격임무(Red Team 역할 : 가상 해커 팀)를 수행하는 정보마비 실 및 정보평가/모의 실은 미래 사이버 전투에 대비하고 아군의 정보통신체계의 위협과 취약성 등을 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 전 조직 창설이 이루어져야 할 것으로 판단한다.

| <표4.1> 사이버 전 조직(예상) | | | |
|---|---|---|---|
| 방어임무 | | 공격임무 | |
| 정보보호 부 | 정보감시/ 복구 부 | 정보마비 부 | 정보평가/ 모의 부 |
| .체계보호 실 | .감시/관제 실 | .암호해독 실 | .정보 평가 분석 실 |
| . 네트웍 보호 실 | .침해추적 실 | .해킹 기법 개발 실 | .정보 표준화 실 |
| .암호설계 실 | .피해복구 실 | . 바이러스 개발 실 | .정보 모델/모의화 실 |
| .체계운영 유지 실 | .네트웍/장비 실 | .사이버 무기개발 실 | .정보교육/ 훈련 실 |

## 5. 결 론

선진국들처럼 군이 민간 정보통신, 금융, 수도, 에너지, 교통 등의 국가 정보망 전체를 보호하듯이 우리군도 사이버 전에 대비한 방어와 공격 분야의 능력을 구비하여야 할 것이다. 결론적으로 미래 사이버 전쟁에서 가장 핵심 방어와 공격 기술 및 무기인 해커의 조기양성 및 획득은 필수적인 사이버 전 능력의 확보 방안이므로 사이버 전을 수행할 수 있는 전투부대의 지식무기를 제공할 수 있는 사이버 전쟁 연구소와 전투부대를 창설하는 것은 피할 수 없는 시대적인 요청인 것으로 판단한다.

## 참고문헌


[1] 엘빈 토플러, "전쟁과 반전쟁", 한국경제신문사 번역, 1996. 3.

[2] Edward Walts, "Information Warfare Principles and Operations", ArtecHouse, 1998.

[3] 권태영외 다수인,"21세기 군사혁신과 한국의 국방 비젼", 한국국방연구원, 1998. 8.

[4] 박재근, 오제상, 윤현철,"정보전 체계 설계 및 구축 방안", 국방과학연구소, 2000.11.

[5] Timothy L. Thomas Retired U.S. Army Lieutenant Colonel, "The Future of War", InfowarCon 2000, 2000. 7.

[6] 인터넷 한겨레, "미국방부 북한 해킹 능력 CIA 수준", 2000. 10.

[7] "Jane's Intelligence Review", 2000. 12. pp.32~36



### 오 제 상

1973년 공군사관학교 항공공학과(학사)

1882년 고려대학교 산업공학과(석사)

1888년 고려대학교 산업공학과(공학박사)

1988년 ~ 2000년 국방과학연구소 책임연구원

2001년 ~ 현재 국방대학교 정보화소요공학실 연구관/교수