碩 士 學 位 論 文

戰鬪空間 擴大에 따른 軍事力 運用方案 硏究

-사이버戰 對應戰略을 中心으로-

2010年

漢城大學校 經營大學院

經 營 學 科

國 防 經 營 專 攻

李 漢 億

碩 士 學 位 論 文
指導敎授 金善浩

戰鬪空間 擴大에 따른 軍事力 運用方案 硏究

-사이버戰 對應戰略을 中心으로-

The study on military operation due to battle space expansion
-Focused on counter cyber warfare operation-

2009年 12月 日

漢城大學校 經營大學院
經 營 學 科
國 防 經 營 專 攻
李 漢 億

碩 士 學 位 論 文
指導敎授 金善浩

戰鬪空間 擴大에 따른 軍事力 運用方案 硏究

-사이버戰 對應戰略을 中心으로-

The study on military operation due to battle space expansion

-Focused on counter cyber warfare operation-

위 論文을 經營學 碩士學位 論文으로 제출함

2009年 12月 日

漢城大學校 經營大學院

經 營 學 科

國 防 經 營 專 攻

李 漢 億

李漢億의 經營學 碩士學位論文을 認准함

2009年 12月 日

審査委員長 _____ 印

審 査 委 員 _____印

審 査 委 員 _____印

목 차

【 표 목 차 】

제 1 장 서 론

제 1 절 연구의 목적

20세기에 들어서면서 과학기술에 의한 무기체계의 발달과 미래전 수행 개념은 상호 보완적으로 변화되었다. 이에따라 선진국을 비롯한 세계의 군대들은 현대의 과학기술 발전을 최대한 활용할 수 있도록 군사혁신을 추진해 왔고, 최근의 전쟁사례를 통하여 새로운 전쟁수행방식이 현실화됨으로써 그 성능 및 운용개념이 더욱 구체화 되고, “미래전이 어떻게 수행될 것인가”에 대한 개략적인 모습이 점차 드러나고 있다.

미래 전장에서는 무엇보다도 인간 중심의 전투가 중시되면서 인명손실의 최소화를 추구하고, 전투원을 대체하거나 보호하기 위한 다양한 무인전투 방식과 무기체계가 사용될 것이다.

또한 전장에서는 정보의 신속하고 정확한 수집과 공유에 대한 요구가 증대되고, 그 질이 전쟁의 승패에 결정적인 영향을 미치게 되므로 정보우위 달성을 위하여 다양한 수단이 집중적으로 운용되게 될 것이다. 따라서 우리의 정보 및 정보체계는 보호하고, 적의 정보 및 정보체계는 파괴 또는 마비시키기 위한 ‘정보작전’의 중요성과 비중이 증대될 것이다.

전쟁은 과학기술의 발전과 작전환경의 변화에 따라 첨단화된 무기체계들이 사용되는 가운데 더욱 정교화 될 것이며, 이러한 과학기술은 국가경쟁력의 우위를 결정하는데 중요한 요소로서, 국가 안보와 군사혁신을 위한 주요수단으로 작용할 것이다. 또한 과학기술의 발전은 과학과 기술의 융합화, 시스템화, 지능화현상이 가속화되고 과학적 발명으로부터 실용화까지의 순환주기가 크게 단축되며, 극한 기술의 추구와 응용을 통해 인간의 활동 능력과 이용 공간을 확장해 나아가는 방향으로 발전할 것이다. 특히 정보기술(Information Technology)이 급속히 발전하고 있고, 이것은 앞으로 군대의 전투효율성을 급증시킬 것으로 판단된다. 정보기술을 효과적으로 활용하면 시간과 공간이 주는 제약을 상당부분 극복할 수 있고, 또한 상대

방보다 효과적으로 활용한다면 전투력의 우열을 근본적으로 변화시킬 수 있기 때문이다. 정보기술은 적에 대한 파악, 그 결과에 대한 종합, 분석, 평가의 정확성을 향상시킴으로써 '전쟁의 불확실성(Fog of War)'을 상당 부분 제거하거나 감소시켜, 결심의 신속성과 정확성, 대응의 효과를 증대시킬 수 있다. 또한 과학기술의 발전은 공중에 대한 활용도를 증대시키고 있다. 공중은 지상과 해상의 어느 공간에도 신속하게 도달할 수 있는 편의성과 융통성이 있기 때문에 공중을 효과적으로 이용할 경우 전쟁수행에 있어서 상당히 유리해질 수 있다. 따라서 현대의 과학기술은 이러한 공중뿐만 아니라 우주공간의 군사적 활용 범위도 확대하고 있고, 이는 공군을 비롯하여 모든 군종(Services)들에게 골고루 적용되고 있는 추세이며, 앞으로의 전쟁에서는 공중과 우주를 활용하는 능력의 정도가 승패에 결정적인 요소로 작용하게 될 것이다.

현대의 과학기술은 원거리 정밀타격, 무인전투, 비살상전투를 가능하게 함으로써 새로운 개념 및 양상으로 미래전이 수행될 가능성을 예고하고 있다. 정밀타격(또는 유도)무기와 탐지회피 기술의 발전에 힘입은 '효과기반작전'[1]을 통하여 꼭 필요한 결정적인 목표 위주로 가장 효과적인 방법과 수단을 사용하여 공격함으로써 전체 전투력의 운용 효율성을 증대시키고 있고, 다양한 무인무기·장비 및 비살상 무기체계의 개발을 통하여 인명손실에 대한 부담을 극소화하고 있다. 따라서 이러한 새로운 무기체계를 이용한 공격과 방어가 미래전에서 핵심적인 비중을 차지하게 될 것이다. 전쟁에서의 인명중시의 경향은 적 무기체계의 핵심적 기능(센서 및 전자회로, 사격통제 시스템 등)을 마비시키는 초고주파 음향무기와 초저주파 음향무기 등 비살상무기의 개발을 가속화시킬 것이다. 정밀제어 위성 및 장시간 체공 UAV(Unm- anned Aerial Vehicle : 무인항공기)에 탑재된 고감도 영상센서와 영상처리, 고속통신기술은 정보, 감시, 정찰체계를 비약적으로 발전시키고, EO(Electro-Optical : 전자광학), SAR(Synthetic

---

1) 효과기반작전(Effect Based Operations : EBO) : 전·평시 아군이 가용한 모든 군사 및 비군사적 능력을 상승적으로 적용하여 아군이 원하는 전략적 결과나 효과를 달성하기 위한 작전으로, 신속결정적작전의 핵심개념이다.
* 주간국방논단 제1062호(2005. 8. 29), 효과기반작전(EBO)에 대한 종합적 이해 참조

Aperture Radar : 종합영상정보레이더), 레이저, 항법위성 등 첨단 기술을 활용한 항법 및 탐색장비의 능력 발전으로 점표적에 대한 초정밀 유도가 가능하게 될 것이다.

또한 고에너지 추진제 및 추진력 제어를 통한 장거리 비행이 가능해지고 스텔스 성능 등을 보유한 초정밀 장거리 유도무기가 실용화될 것이다. 무기체계는 초소형 고속연산 컴퓨터, 인공지능, 극소정밀센서, 소형 고출력 전기모터의 발전 등으로 더욱 지능화, 자율화될 것이며, UAV나 군사용 로봇중 견마로봇 등과 같은 무인화 무기가 광범위하게 사용될 것이다.

앞서 설명한 것처럼 과학기술의 혁신적인 변화가 현실공간(지상, 해상, 공중, 우수)속 전투수행에서 그야말로 충격적인 변화를 가져왔으나 이번 연구를 통해 밝히고자 하는 것은 다른세상을 만들어낸 20세기의 최고의 발명 '컴퓨터'와 이를 이용한 '인터넷'을 통한 사이버공간이란 또 다른 삶(전투)의 영역이다.

많은 개인 혹은 기업, 정부는 사이버 공간을 통해 다양한 형태의 수많은 미확인 정보를 분석하고 검증하여 양질의 정보를 만들어 내고 그것을 통해 앞으로의 변화를 많은 부분 예측해 내고 있다. 그러나 사이버 공간이란 것은 단순히 정보를 분석하고 수집하는 1차원적인 공간이 아니다.

손자[2]는 말했다.

"전쟁은 국가의 중대사 이며, 국민의 생사가 달려있고 국가의 존망이 달려 있으니, 가히 신중하게 살펴보지 않을 수 없다."

"대저 아직 싸우지 아니하고서 작전회의에서 이기는 사람의 승산을 얻음이 많고, 아직 싸우지 아니하고서 작전회의에서 이기지 못하는 사람은 승산을 얻음이 적다."

전쟁이란 개인으로서는 자신의 목숨을 걸고 싸워야 하는 것이며, 국가 또한 국가의 존망을 걸어야 하는 중차대한 것이다. 이러한 전쟁을 함에 있어 사이버전은 한명의 희생자도 없이 적을 무력화 할 수 있는 단 하나의 공간이라 하겠다.

우리나라의 경우 정보통신기술의 발전 속도를 감당하지 못할 정도의 급

2) 손자 : 이름은 무(武)이며, 제나라 사람. 인간사의 원리도 이해한 병법가. (BC 514~496)

격한 인프라 구축으로 인해 정보화 역기능현상이 두드러진다. 사이버 공간상의 허위정보 유포, 스팸메일, 해킹 등의 현상이 만연하고 있고, 08년 수차례에 걸친 군 해킹 피해, 09년 1월 해외 전문해커 조직의 군 관련 정보 무차별 수집, 09. 7. 7 국가기관 및 중요포털 싸이트를 대상으로 한 DDos(Distributed Denial of Service attack : 분산 서비스 거부 공격)[3] 등으로 우리사회의 개인과 군(軍)·관(官)의 사이버 대응태세가 얼마나 허술한지 확인할 수 있었다. 특히 사이버전 대응 체계구축이나 사이버전에 관한 주변국의 대비현황, 사이버전의 특성등에 대한 분석과 국가 차원에서의 사이버전 전략 수립이나 인력관리 등에 관한 연구는 부족한 실정이다. 물론 2010. 1. 1 기무사 예하조직으로 창설을 앞두고 있는 사이버방호사령부가 있으나 이는 사안의 시급성 때문에 우선적으로 창설되지만 관련부지와 청사, 첨단장비 구축등은 정확히 알려진바 없다.

따라서 본 연구의 목적은 미래전의 양상과 지금까지 발생한 사이버전 유형을 살펴보고, 주변국의 대응태세 분석 및 현재 우리나라 사이버전 대응현황을 살펴봄으로써 향후 사이버전 대응방안을 정립하는데 있다.

3) DDos(Distributed Denial of Service attack) : 분산 서비스 거부 공격으로 여러 대의 좀비 PC를 분산적으로 배치해 특정 시스템을 악의적으로 집중 공격하여 해당 시스템의 용량 및 자원을 부족하게 함으로써 정상적인 서비스를 중지하는 등의 영향 초래

제 2 절 연구의 범위와 방법

본 연구는 미래 사이버전의 위협에 대비한 군 사이버 대응방안 정립에 중점을 두어 분석하였다.

이와 같은 연구목적을 달성하기 위하여 사이버전의 특징과 사이버전을 수행하는 전사(Combatant)의 구비조건, 사이버전의 유형과 주요사례, 주변국의 사이버전 대응태세를 분석하여 군사적 사이버전 대응방안을 제시하였다.

연구방법은 사이버전의 이론적 배경, 선진국의 사이버전 대비현황 및 인력운영 사례를 고찰하기 위해 국·내외 문헌 및 석·박사학위논문, 인터넷 사이트를 통해 자료를 수집·분석하였고, 논리의 전개는 이론적 고찰, 우리나라 사이버전 대응 현황, 향후 사이버전 대응태세 강화방안을 도출하는 순으로 진행하였다.

본 연구문은 모두 6개의 장으로 구성하였으며, 2장에서는 사이버전의 이론적 배경에 대해 알아보고 3장에서는 사이버전 유형과 사례를 분석하고, 4장에서는 주변국 사이버전 대응태세와 우리나라 사이버전 대응현황을 비교하였으며, 5장에서는 우리군의 사이버전 대응태세 강화방안과 이를통한 군내 보안의식 고취 및 전산보안 교육강화, 감시체계 강화방안과 더불어 사이버전 전문인력 양성방안을 도출하는 순으로 정리하였다.

제 2 장 사이버전의 이론적 배경

제 1 절 정보사회와 가상공간

1. 정보사회의 정의

토플러가 예언한 것처럼 우리는 지금 농업 사회와 산업사회를 지나 정보 사회로 들어섰다. 정보사회는 information society 라는 영어를 우리말로 옮긴 것으로, 여러 가지 뜻으로 정의 된다. 다니엘 벨(Daniel Bell)은 정보사회를 “정보와 지식이 사회적, 경제적 교환수단으로 중요한 기능을 하는 사회”로 정의했고, 오브라이언(Rica Cruise O′Brien)은 “경제활동이 상품 생산의 제조에서 정보와 지식을 만드는 영역으로 변모하고 정보와 새로운 지식이 결합된 새로운 기술의 효율적 이용이 각광을 받는 사회”로, 그리고 이토 유이치는 “풍부한 정보를 저장 유통시킬 수 있으며 정보의 분배와 변형이 신속하고, 효율적이며 사회의 모든 구성원이 값싸게 정보에 접근할 수 있는 사회”로 정의한다. 그런가 하면 마크 포랏(Marc U. Porat)은 정보 사회를 “1차, 2차, 3차 산업에 추가하여 정보 산업을 고려할 경우, 노동력의 절반 이상이 정보 산업에 종사하는 사회”로 정의하며, 일본의 전기통신총합연구소(Research Institute of Telecommunication & Economics, RITE) 는 좀 더 자세하게 “노동 인구의 50% 이상이 정보부분에 종사하고 적령 인구의 50% 이상이 대학생이고 개인소득이 4,000달러 이상이며 총 지출 중 정보비가 35% 이상인 사회”라고 정의한다. [4]

이처럼 정보사회는 여러 가지로 정의되나 가장 단순한 정의는 “정보가 사회의 모든 부문을 지배하는 사회”라고 할 수 있다. [5] 이것은 정보사회가 물질이나 에너지를 대신하여 상징, 메시지, 데이터, 지식 따위로 대표되

4) 신윤식 외, 「정보사회론」, 서울 : 데이콤출판부, 1992, 안문석, 「정보체계론」, p. 561~562에서 재인용

5) ‘정보가 사회의 모든 부문을 지배하는 사회”라고 할 때 ‘지배한다’는 의미는 정보가 사회를 유지, 발전시키는데 다른 어떤 요소보다도 중요하다는 말이 된다. 또 ‘중요하다’는 말은 다른 어떤 요소보다도 사회에서 큰 가치를 갖는다는 말과 이 요소 없이는 사회가 유지, 발전되지 않는 다는 의미를 함축한다.

는 정보의 가치가 상대적으로 높아지는 사회라는 것이다. 마치 농업 사회에서는 농사에 필요한 노동(labour) 과 가축(domestic animals) 이 중요한 자원이 되고, 산업사회에서는 자본(capital)과 노동(labour)이 중요한 자원이 되듯이, 정보사회에서는 정보와 지식이 정치·경제·문화·사회구조 전반에 걸쳐 사회를 변혁시키는 전략 자원이 된다는 것이다. 6) 물론 정보사회라고 해서 모든 사회가 온통 지식과 정보만으로 지배된다는 것은 아니다. 아무리 정보사회라 해도 농업 사회와 정보사회가 동시에 존재하기 때문이다. 다만 농업 부문이나 제조업 부문보다는 정보를 처리하는 부문에 종사하는 사람이 높은 비율을 차지한다는 것, 그리고 농업부문과 제조업 부문에서도 점점 많은 사람들이 정보와 관련된 일에 종사하게 된다는 것이다.

이런 맥락에서 볼 때, 정보사회의 참된 의미는 정보주의 사회가 된다. 정보주의 사회는 자본주의 사회에 대응하는 말로, 자본주의 생산요소 가운데 자본이 가장 가치를 갖는 사회라는 의미이다. 따라서 자본주의 사회에서는 자본을 소유한 사람이 다른 부문에 대한 통제권까지도 갖는 것으로 이해된다. 정보주의 사회는 자본보다 정보의 가치가 보다 중요한 생산요소가 되는 사회이다. 자본주의 사회의 논리를 그대로 정보주의 사회에 적용하면, 정보주의 사회에서는 정보를 보유하는 사람이 사회에서 가장 지배적인 지위를 갖는다는 의미로 해석할 수도 있다. (안문석, 「정보체계론」, 서울 학연사, 1999, p.559~561)

2. 정보사회의 특징

정보사회는 인간의 주요 활동이 정보통신기술이 제공하는 서비스의 지원을 받아 이루어지는 사회를 뜻한다. 좀 더 구체적으로 말해서, 정보사회는 대부분의 고용이 지식과 정보의 생산·처리·유통과 관련된 정보 산업에 집중될 뿐만 아니라 인간의 일상생활과 주관적인 감정이나 희망 같은 추상적인 부분까지도 정보통신기술의 영향을 받는 사회를 말한다. 따라서 정보사회의 특징도 외형상의 특징과 사람의 가치관이나 마음상태와 관련된 내적인 특징으로 나누어 볼 수 있다.

---

6) 존 네이스 비트, 「메가 트렌스」, 서울 : 고려원, 1982, p. 29~31; 피터 드러커, 「자본주의 이후의 사회」, 서울: 한국경제신문사, 1997, p. 19~30

먼저 외형상의 특징은 다음과 같은 것들을 들 수 있다.

첫째, 정보사회는 정보산업이 1차·2차·3차 산업을 제치고 선도 산업으로 등장한다. 이것은 종사자 수 뿐 만 아니라 국민 총 생산에서 차지하는 비중도 월등해진다는 것이다. 정보산업이 선도 산업으로 등장하는 정보사회는 정보의 중요성이 큰 사회이기 때문에 정보를 수집하고 정리하는 기계, 즉 컴퓨터와 원격통신(telecommu- nication) 기술이 정보사회의 핵심 기능을 수행한다. 특히, 컴퓨터의 역할이 중요해서 정보사회는 컴퓨터 사회라고 부를 정도로 컴퓨터가 광범위하게 보급된다. 정보사회는 컴퓨터와 인터넷 같은 정보통신기술이 사회를 이끌어 가는 견인차 역할을 하는 사회로 컴퓨터와 인터넷 사용에 관한 지식이 상식이 된 사회이다. 컴퓨터와 인터넷 사용이 상식화 된 사회이기 때문에 사용법을 알지 못하면 세상을 제대로 살아가기가 어려운 세상이다.

둘째, 정보사회는 먼 거리에 있는 사람들에게 정보를 값싸게 전달할 수 있는 수단이 발달한다. 통신이라는 면에서 보면 정보는 음성정보, 문자정보, 그림정보로 나누어지는 데, 정보화가 진행되면서 이들 정보가 하나로 통합되어 전달되는 기술이 보급된다. 이미 인터넷이 전 세계로 보급되어 정보 유통에서 국경선이 의미를 상실했다. www(World Wide Web) 등을 이용한 홈페이지(homepage)가 일상화 되고, 홈페이지를 활용한 EG(Electronic Goverment : 전자상거래)를 구현한다.

셋째, 정보의 유통 면에서 국경선이 실제로 사라졌다는 것은 경쟁의 공간적 범위가 전 지구로 확대된 무한경쟁의 사회가 되었음을 뜻한다. 따라서 정보사회는 1등만 살아남고 나머지는 모두 패자(敗子)가 되는 사회이다. 정보사회는 '실험실과 공장의 구분'이 사라진다. 실험실에서 성공한 시제품을 즉시 대량 생산으로 들어갈 수 있고, 생산 능력은 전 세계의 수요를 충족시킬 수 있게 된다. 정보사회를 다품종 소량 생산의 사회라고 부르는 것은 수정할 필요가 있다. 곧 정보사회는 다품종 대량생산 사회가 될 수도 있기 때문이다. '1등만 살아남고 모두 패자가 되는' 정보사회는 '소수

의 승자와 다수의 패자'가 존재하는 사회로, 이런 현상은 정보격차(information divide)에서 더욱 두드러지게 나타난다.

넷째, 정보사회는 지식과 정보의 수준이 현저히 단축된 사회이다. 산업사회에서 지식과 정보의 평균 수명은 10년 정도였으나 지식사회에서는 2년 정도로 단축되었다. 또한 지식과 정보를 전달하는 매체가 종래의 종이에서 전자매체로 서서히 변한다. 즉 종래에는 거의 대부분의 최종정보가 종이를 매체로 하여 인쇄되는 형태를 취했으나 보관용 정보는 디스크나 테이프 형태로 전환되고 비보관용 정보는 화면을 통해서 전달되는 형태를 갖게 된다. (안문석, 정보체계론 , p.566~567)

다음으로 정보사회가 가져다 줄 내적 특성은 외형상의 특징에 견주어 뚜렷하지 못하고 점진적으로 나타나지만 그 영향은 장기적이고 심대하다는 속성을 갖는다.

첫째, 공간이 심리적으로 축소된다. 이 말은 공간이 교통수단을 통하여 점으로 연결되기 때문에 물리적으로 떨어져 있다는 것이 심리적으로는 아무런 부담을 주지 않게 되는 현상을 갖는다. 정보사회는 열린사회이다. 정보사회의 근간이 되는 정보 고속도로는 세계와 지역과 개인을 하나로 엮어 이들 간의 자유로운 의사소통을 빛의 속도로 가능하게 한다. 전시대적인 비밀과 폐쇄, 그리고 권위주의적 닫힌 사회를 유지하기가 그만큼 어려울 것이다. [7] 유행가 가사에서 볼 수 있는 '고향을 그리는' 마음가짐은 사라지고, 출퇴근이 가능한 지역은 모두 하나의 공간으로 인식된다.

둘째, 정보사회는 문화의 통일성(conformity)과 다양성(variety)이 공존하는 사회가 된다. 통일성이란 교통통신의 발달로 지역이 의미를 갖지 못하기 때문에 경쟁에서 살아남은 생활양식이나 물건, 사고방식이 광범한 지역에서 통용되기 시작한 현상이다. 이것은 우리나라에서 어느 곳을 가나

7) 서삼영, 고도 정보사회 구축을 위한 정보통신정책의 방향 모색, '정보화와 정부·언론의 역할', 한국언론학회·한국 행정학회 공동 심포지엄(1996), p 25~26

음식이 비슷해지고 건물의 모양이 비슷해지며 옷차림이 동일해지는 모습에서 증거를 찾아볼 수 있다. 한편 다양성이란 정보화 사회는 다양한 정보가 원활하게 유통되고, 공작기계 등 소위 만능기계가 등장하기 때문에 각자의 취미와 취향에 맞는 제품이 다양하게 등장 할 수 있게 된다는 것을 말한다. 이 두 가지 현상을 종합하면 큰 흐름면에서는 사람들의 마음속에 통일성이 존재하나 자세한 부분에서는 변혁이 의미를 갖게 된다는 것을 말한다.

셋째, 정보사회에서는 개인이 당면하는 문제를 해결하는 데 가장 중요한 자원으로 정보, 이 가운데에서도 지식이 등장한다. 이것은 상당히 중요한 의미를 갖는 것으로, 리즈만(D. Riesman)이 말한 외부 지향적 인간(out-directed person) 이후에 지식 지향적 인간(knowledge-directed person) 이 등장하게 된다는 것을 뜻한다. 따라서 정보사회에서는 전문가의 지식이 일반화 되는 현상을 갖는데 이것은 일반인이 컴퓨터를 통해 전문가의 지식을 싼값으로 손쉽게 이용할 수 있게 된다는 것을 전제로 한다. 정보사회에서는 종래 사무실에서 전문가에게 비싼 돈을 주면서 하던 일을 개인용 컴퓨터를 이용해 집에서 자신이 하게 되는 것을 흔히 볼 수 있게 된다.

넷째, 정보사회는 컴퓨터와 정보통신의 세계가 만들어내는 가상공간(Cyber Space)이 사람의 머릿속에 실존하는 것으로 인식된다. 가상공간에서 구성된 현실을 가상현실(Virtual Reality)이라고 부르는데, 이러한 현실에서 맺어지는 인간관계는 수평적이고, 직접적이며, 현장 중심적이고 다양성이 존중된다는 특징을 갖는다. 그러나 인간관계의 기본문제인 빈부격차, 가치관의 차이가 주는 문제, 공익과 사적인 이익 사이의 갈등 등이 새로운 형태로 등장한다. (안문석, 「정보체계론」, p.568~569)

그에 따라 정보사회는 윤리 문제가 더욱 심각하게 제기되며 윤리적 파장은 많은 점에서 산업사회와 질적으로 다른 형태를 띠게 된다. 특히 불건전한 정보의 홍수 속에서 자아와 인성의 실체, 익명성과 인간 신뢰성의 문

제, 인간의 컴퓨터化 같은 문제들이 개인의 정체성을 위협하는 동시에 인간의 생명과 인생의 의미와 관련된 윤리 문제를 심각하게 제기하고 있다.

3. 정보통신기술의 발달에 따른 사이버전의 도래

정보기술(IT)의 발달은 국가안보에도 매우 중요한 영향을 미치고 있다. 국가안보는 국내외로부터 발생되는 모든 종류와 형태의 위협으로부터 국가의 기본이익과 국가목표, 그리고 제 가치를 보전하고 향상시키기 위하여 군사를 비롯하여 정치, 외교, 경제, 사회, 문화, 과학기술, 환경 등의 제반 관련 정책들을 통합, 조정, 체계화하여 운용함으로써 기존의 위협을 배제하거나 효과적으로 대처하고, 새로운 위협을 사전에 억제 및 대처하는 것이다. 이러한 관점에서 볼 때, 정보기술(IT)은 안보 요소인 정치, 외교, 경제, 사회, 문화, 과학기술, 환경 등의 성장과 발전을 촉진시켜 국가의 안보역량을 우회적으로 강화시키기도 하지만, '사이버전'이라고 하는 새로운 전쟁 패러다임(paradigm)을 탄생시켜 국가안보에 보다 직접적이고도 결정적으로 영향을 미치고 있다. 정보기술(IT)의 발전은 물리적 공간에 있던 정보들이 센서 등을 통해 컴퓨터 및 네트워크 환경인 가상공간(Cyber Space)으로 대량 이동하여 용기(container)와 기록기(recorder)에 저장하고 전송할 수 있게 되었다. 즉, 정보가 가상공간으로 점점 밀집되고 있는 것이다.

인류가 사회를 구성한 이래로 전쟁이 시작되어 농업사회, 산업사회, 정보사회를 거치는 동안 그 양상이 끊임없이 변화되어 왔다. 앨빈 토플러가 그의 저서 War and Anti-war(1993)에서 농업사회의 백병전과 산업사회의 대량파괴 살육전에 이어 제3의 물결시대의 전쟁은 하이테크 전쟁, 사이버 전쟁이 될 것으로 전망한 바와 같이 전쟁의 양상은 점차 사이버공간을 전장으로 삼게 될 것이다(Alvin Tofler, 1993 : 89).

사이버전에서는 아군이나 적군 모두 인명피해가 발생하기 전에 적을 굴복시키는 '무혈전쟁', '싸우지 않고도 승리하는 전쟁'을 가능하게 함으로써 세계 각 국은 사이버 전쟁 승리를 위해 투자를 하고 있는 실정이다(제임스 아담스, 2000(하) : p.26~27).

이처럼 정보화가 진전됨에 따라 전통적인 의미의 전쟁은 무의미해지고 정보·지식 전, 사이버전의 형태로 전쟁의 양상이 변화되고 있다.

<표2-1> 전쟁양상의 변화

사회변화	농업사회	산업사회	정보사회
전쟁양상	육체·백병전	기계·화학전	정보·지식·사이버전
전장공간	1차전(지상)	3차원(지·해·공)	5차원 (우주·사이버 추가)
전력구조	병력집약형	자본집약형	정보집약형
지휘구조	장수 중심구조	수직적 계층구조	수평적 네트워크 구조
전투형태	선형	선형, 비선형 (대부대, 집중)	비선형(소부대 분산)
파괴·피해	노획·포로	대량파괴·대량살상	정밀파괴·소량피해

자료 : 장명순, 1996, p. 19

이와 같은 전쟁양상변화로 인한 미래전은 정보통신기술의 발달에 따라 전장통제능력이 증대되고 무기체계의 성능, 운용개념, 효과가 향상되어 기존의 지리적 공간에 국한되었던 전장공간이 우주 및 무한대로 확장되고 나아가 사이버공간을 포함한 넓은 영역에서 전쟁이 수행될 것이다. 정밀타격, 비 살상 무기체계를 운용하여 적의 두뇌, 중추신경계만을 무력화시켜 인명살상을 최소화하는 인명 중시의 전쟁(soft kill)이 될 것이며, 모든 전장에서 상황별 제대별 동시 전투를 수행하는 비선형 및 분산 상태에서의 작전 수행이 이루어질 것이다. 네트워크와 C4I(command, control, communication, computer and Intelligence)체계를 통해 아군의 제반 전력을 연계 통합하여 시공간적으로 통합된 작전을 수행하여 전력발휘의 극대화를 추구할 것이다. (황철준, 2003 : p.68~69).

이상에서 언급한 미래의 전장에서는 적의 정보체계, 네트워크 그리고 지식능력은 파괴 또는 마비시키는 반면 아군의 능력을 최대한 발휘하도록 보장하는 정보우위(information superiority)의 확보가 필요하게 될 것이다.

미래전의 양상은 학자에 따라 다양하게 제시하고 있지만 정보전 이론에서 빼놓을 수 없는 인물은 미 국방대학의 리비키(Martin C. Libiki) 교수

이다. 그는 정보전을 군과 민간을 모두 포함하는 관점에서 분류하고 있다. 그는 정보와 정보 기술을 적용할 수 있는 모든 종류의 방법을 식별하고 각각의 특성에 따라 군과 민간 관련부문으로 분류한다. 걸프전에서 이미 적용한 심리전, 전자전, 지휘통제전 등은 물론이고 아직은 적용하기가 어려운 분야까지 포함하고 있어 현재 상상 할 수 있는 거의 모든 분야를 포함한다.

우선 지휘통제전(Command and Control Warfare, C2W)은 지휘부와 통신망을 대상으로 한다. 군사정보전(Intelligence Based Warfare, IBW)은 군사정보를 수집·처리·전파하는데 사용하는 군사정보체계를 대상으로 하는 것으로 적이 전장의 아군 정보를 탐지하지 못하게 하거나 사실과 다르게 보이게 하는 것이 목적인 수세적 군사정보 작전과 적의 전장 정보를 최대한 수집하는 공세적 군사정보전으로 나뉜다. 전자전(Electric Warfare, EW)은 지휘통제전과 군사정보전에서 전자기술과 암호기술을 군사통신에 적용하는 것으로서 전자전의 많은 부분은 레이더와 재밍(Jamming), 반(反)재밍 등과 관련된 반(反)레이더에 대한 것이다. 이에 비해 심리전(psychological)은 정보를 이용하여 사람의 의지와 행동을 심리전을 수행하는 쪽에 유리하도록 변화시키는 것으로서 적 국민에 대한 대(對)군(counterforce), 적 지휘관에 대한 대(對)지휘관 그리고 문화충돌에 대한 거부감을 희석시키는 문화전쟁(kulturkampf)등으로 분류 할 수 있다. 해커전(hacker Warfare)은 컴퓨터 네트워크에 대한 공격이다. 이때 바이럿, 논리폭탄, 트로이목마, 스니퍼(sniffer)등의 도구를 사용한다. 경제정보전(Economic Information Warfare, EIW)은 정보전과 경제전이 결합한 것으로서 특정 국가에 대하여 외국과의 정보교류를 방해하는 정보봉쇄, 특정 국가가 모든 정보를 독점하는 정보제국주의(Information imperialism)등의 형태로 나타난다. 마지막으로 사이버전(cyber warfare)은 정보전 형태 중에서 가장 이해하기 힘든 것으로 사이버공간을 대상으로 한 정보 테러리즘, 시맨틱 공격(semantic attack), 시뮬러전(simular warfare), 기브슨전(gibson warfare)등의 형태가 있다. 정보테러리즘은 컴퓨터 해킹의 하부부류로 정보시스템을 물리적으로 파괴하지 않고 개인정보를 무단으로 공개

하거나 조작하여 개인을 공격하는 것을 말하고, 시맨틱 공격은 공격당하는 쪽에서 보았을 때 시스템이 정상적으로 동작하는 것 같이 보이지만 시스템의 수행 결과가 실제 세계와 다르게 나타나도록 만드는 것이다. 시뮬러전은 시뮬레이션 된 전쟁결과를 실제전쟁의 결과로 받아들이는 것이며 기브슨전은 기브슨(william Gibson)의 뉴로맨서(neuromancer)같은 소설에서처럼 사람이 가상인물(virtual character)로 바뀌어 여러 시스템의 내부를 돌아다니며 살면서 다른 가상의 인물들과 분쟁을 일으키는 것을 말한다.

정보화 시대의 대표적인 특징 중의 하나는 정보통신, 인공위성, 온라인 금융결제, 국제무역, 인터넷 통신판매, 최첨단 무기체계 등 거의 모든 분야가 디지털 네트워크로 연결되어 있다는 것이다. 따라서 정보전이 지닌 두드러진 특징 중의 하나는 국가의 성역을 전반적으로 위협할 수 있는 새로운 형태의 위협의 대두다. 그런데 전통적으로 간주되어온 경계선이나 관할권 개념이 사이버 시대에는 적용되지 않음에 따라 비 국가적 또는 비 정부적 행위가 확산될 것으로 보인다.

미래전 에서는 또한 네트워크의 중요성이 크게 증가할 것으로 전망된다. 네트워크는 감시체계, 타격체계, 컴퓨터 등 단말기를 하나의 체계로 결합한다는 관점에서 시멘트와 같다고 할 수 있다. 그러나 지역 공간적으로 멀리 떨어진 체계를 하나로 묶는 네트워크는 무한한 양의 정보를 실시간에 제공을 하면서도 물리적 소프트웨어적인 공격에서 생존성을 보장할 수 있어야 한다. 그러나 군사과학 기술의 발전은 무기체계를 지능화, 자동화, 정밀화, 장사정화, 광역화, 소형화 시키고 있다. 이는 또한 전장 감시체계를 광역감시 체계로, 타격체계를 장거리 정밀타격 체계로, 기동탑재 체계를 고속, 스텔스 기동탑재 체계로 군수지원 체계를 적시, 적소, 적량의 군수지원 체계로 발전시키고 있다. 즉 센서체계, 컴퓨터, 통신기술의 발전은 전장의 넓은 영역에 대해 표적을 정밀탐지하고 식별추적 할 수 있는 능력을 갖추도록 하고 있다. 예를 들어 정보전의 막을 연 걸프전에서 미군의 정찰감시체계는 표적의 15%를 탐지했으나 2005년에는 90%이상을 탐지할 수 있었다고 한다.

또한 고속이동 수단, 스텔스 기술, 무인화 기술의 발전은 기동탑재 체계

의 혁명적 발전을 가져왔다. 정보전에는 기존의 살상무기체계(hard kill)를 사용할 수도 있고 비 살상 무기체계(soft kill)를 사용할 수도 있다. 특히 미국 러시아 등 선진 각국은 나노(nano)제어 기술을 이용한 나노머신(nano machine), 핵폭탄이 터질 때 강한 전자기 충격파를 발생하는 것과 비슷한 원리를 이용한 전자기탄, 고출력 전자파를 발생시켜 전자 장비를 마비, 파괴시키는 전자총 등의 개발에 주력하고 있다.

나노머신들은 컴퓨터를 찾아 사무실을 돌아다니다가 슬롯 등의 틈을 이용해 컴퓨터에 잠입한 뒤 기판이나 회로 등을 파괴한다. 전자기탄의 경우 목표물에 접근해 발사하면 네트워크, 전투기, 미사일, 레이더, 전산센터, 은행, 발전소 등 어떤 목표물이라도 내장된 지능화, 자동화를 위한 컴퓨터칩, 마이크로웨이브 집적 회로 등을 순식간에 파괴할 수 있다. 현재 미국은 로스앨러모스의 한 연구소에서 이미 가방크기의 전자기 포탄을 개발 완료한 것으로 전해진다. 미국 ABC 방송은 지난 1999년 2월 사이버관련 프로그램에서 사제 전자총 실험을 한 바 있다. 또 당시 한 전직 KGB 요원은 ABC 방송에 출현해 러시아정보당국이 전자총으로 모스코바주재 미 대사관에 화재를 일으켜 소방수로 변장한 정보요원들이 대사관에 진입해 기밀을 탐지한바있다고 증언했다. 러시아가 이미 갖고 있는 이런 무기를 미국이 안 갖고 있을 리는 없다.

이와 같이 정보통신기술의 발전과 더불어 전장이 점차 사이버공간으로 이동하게 되고 현재의 전쟁과는 판이하게 다른 양상을 보이는 미래의 사이버전이 어느새 우리 앞에 다가와 있다.

4. 무기체계의 발달과 전투 수단의 변화

전쟁을 시대적으로 구분할 때, 전쟁사적 관점에서 고대전쟁, 중세전쟁, 근대전쟁, 현대전쟁 등 4단계로 분류하는 것이 일반적이나 학자마다 다소 차이가 있을 수 있다. 즉 어떤 학자는 중세전쟁에서 나폴레옹 전쟁만을 떼어내어 심도 있게 다루든가, 현대전쟁에서 걸프전을 별도의 장으로 구분하여 다루든가 하는 등 시대사에 얽매이거나 고정 틀에 집착하지 않고 그 당시 전쟁의 역사적 가치에 중점을 두어 다루고 있다.

마찬가지로 본인도 내용을 기술함에 있어 고정관념에 구속받지 않고 논리적으로 일관성 있게 전쟁의 역사를 살펴보면서 무기의 발달과 병사의 성격을 규명하고자 한다.

무기 발달사를 단계적으로 구분할 때, 일반적으로 4단계로 나누고 있다.

무기 제1단계는 병사 개인의 완력에 의해 조작되는 무기 즉, 칼, 창, 궁, 투석기 등과 같이 근력에 의한 에너지를 축적하여 일격에 이것을 방출하는 무기로부터 시작된다. 제2단계는 화약의 힘으로 탄환을 날리는 화포의 출현 이후이며, 완력 대신 화학적 에너지를 사용하는 무기의 출현으로서 이는 전쟁을 크게 변화시키는 단서가 되었다. 14~18세기에 걸친 제2단계 시대에 있어서 무기의 진보는 완만했지만 그 때문에 오히려 사회의 변혁이나 군대의 변화와의 상관관계가 명백해진 계기가 있었다. 18세기 말부터 19세기 초에 걸친 이른바 산업혁명으로 인한 개화 이후 화기의 비약적인 진보가 이루어져 무기 발달사도 제3단계에 접어들게 되었다. 과학의 발달에 따라 병기 기술의 이론적 연구가 촉진되고, 또 병기의 개발 및 생산의 파급효과에 의하여 민수산업이 발전한 것이다. 이시기에는 무연화약이 등장하고, 자동화기와 화학무기가 출현하였으며, 특히 내연기관의 발명은 무기에 획기적인 기동성을 부여하게 되었다. 또한 빛이나 음향, 전자파, 전기, 전자, 적외선, 초음파, 사진 등을 이용하는 신기술에 의하여 즉 무기의 효율을 향상시키기 위한 여러 가지 문제의 해결이 시도되고, 거기에 따라 무기는 점차 복잡화되어 갔다. 투척무기는 조준, 사격통제, 목표탐지 및 표적, 통신 및 무선명령 등의 부대 장치와 불가분의 관계로, 무기 그 자체가 아닌 시스템으로 발전되어 갔다. 무기 제2단계와 비교할 때 제3단계의 두드러진 특징은 무기의 구식화가 매우 빨라진 것이다. 무기의 발달 속도가 매우 급속하기 때문에 어떤 신무기가 사용된지 얼마 안 되어 그 존재 의미를 잃게 되는 일이 흔히 있었다. 이 같은 무기 발달의 가속화는 보다 나은 무기를 탄생케 하는 촉진제가 되면서 기술의 발달은 급속도로 확산되어 갔다. 무기발달사의 제4단계는 최초의 원자폭탄이 일본의 히로시마에 투하된 1945년 8월 6일 이후를 말한다. 핵탄두는 기존의 포탄이나 폭탄보

다 발생 온도가 훨씬 높고, 폭풍속도가 크며 또 무서운 방사선을 내기 때문에 이것에 의한 피해는 화약과 비교가 되지 않고, 효력 반경만 큰 것이 아니었다. 핵무기 효력의 향상과 수량의 증가, 그 운반 수단인 미사일의 진보에 의하여 세계 모든 사람의 전쟁관이 바뀌었다. 핵전쟁은 지구의 파멸을 가져오기 때문에 제4단계의 40여 년간은 전쟁 억제의 수단이 되어 왔으나 국지적 무력분쟁은 제3단계에 비해 오히려 증가되었다. 무기역사에 있어서 제4단계의 특징으로는 미국과 소련은 물론 영국, 프랑스 등 핵보유국가들이 거대과학(big science)의 조직적 대결에 익숙해 졌다는 것이다. 제3단계의 시대감각으로는 상상조차 할 수 없었던 고도의 무기가 예상을 뛰어넘어 단기간에 완성되어도 조금도 이상하게 생각하지 않게 된 것이다. 기술의 발달은 여기에서 머무르지 않고 또 다른 새로운 신무기를 개발하고, 새로운 전쟁을 유발케 하였는데, 이른바 하이테크 전쟁인 걸프전이 그것이다. 걸프전은 핵무기의 사용은 없었으나 첨단무기의 개발과 고도 정보수집수단의 등장으로 인마의 살상 전장이 아닌 원거리에서 요구하는 지점에 정확히 타격할 수 있는 무기가 사용되었다. 종래의 지상·해상·공중 합동작전으로부터 이제는 인공위성의 등장으로 우주까지도 전장화가 되어 가고 있는 고도 입체전의 양상을 보여주고 있다(김철환 외, 1997 : p.7~10).

따라서 향후 미래 전에서는 무인항공기, network cyber 무기화, 정보전자무기 등이 사용됨으로써 병사의 성격이 첨단화되고, 사이버 전사, 로봇 전사 등이 필요하게 될 것이며, 뛰어난 정보기술 능력을 갖춘 사이버 전사로 전력을 구축하여야 한다.

제 2 절 사이버전의 정의와 특징

1. 사이버전의 의의

1) 사이버 공간의 정의

컴퓨터와 통신 기술이 결합한 컴퓨터케이션 또는 컴퓨터 매개 통신을 통해 정보의 축적·처리·분석과 전달 능력이 획기적으로 증대되는 정보사회에서는 인터넷과 종합정보통신망(Integrated Services Digital Network, ISDN) 같은 다양한 멀티미디어의 정보통신망이 가정, 직장, 경제, 문화, 교육 등 사회의 각 분야에 걸쳐 사이버 공간(Cyber space)이 형성된다.

'사이버 공간' 이라는 말은 1984년 깁슨(W.Gibson) 이라는 미국의 과학소설 작가가 「뉴로맨서(Newromancer)」라는 작품에서 처음 사용한 이래 1980년대 중반부터 사이버 공간이란 "서로 연결된 컴퓨터들로 이루어진 네트워크를 통해 확보된 의사소통의 공간(communication space)"라는 뜻으로 본격 사용되었다. [8] 야후(yahoo)의 설립자 제리 양(Jerry Yang)은 '당신의 모니터와 내 모니터 사이'가 사이버 공간이라고 설명할 정보로 사이버 공간에 대한 정의는 다소 추상적이지만, 일반적으로는 컴퓨터 네트워크로 연결된 공간으로 인터넷과 PC 통신 등의 통신망을 통해 정보의 교환이 이루어지는 장(場)을 사이버 공간이라 일컫는다.

우리말로는 '가상세계' 또는 '가상공간'으로 번역되는 사이버 공간, 즉 가상공간은 실제로 존재하는 공간이 아니라 컴퓨터 네트워크 상에 존재하는 장(場) 다시 말해, 전 세계 거의 모든 통신망들을 접속하고 있는 인터넷 같은 컴퓨터 네트워크 상에서 존재하는 전자공동체(On-Line Community)를 말한다. 따라서 가상공간은 기계라기보다는 하나의 에코시스템, 곧 전화선·동축케이블·광섬유나 전자기파가 있는 곳이면 어디에나 존재할 수 있

---

8) 곽동수·정윤희, "정보통신·벤처기업 대 특집(권말부록)", 신동아 제 43권 2호(통권 485호), 동아일보사, 2000년 1월, p. 68 정진명·성위식은 사이버 공간을 구체적으로 전자 게시판 시스템(BBS), 상업자료 서비스, 연구자료 네트워크, 전자출판, 네트워크 노드(Network Nod), 전자우편 시스템(E-mail), 전자문서교환시스템(EFT)을 포함하는 모든 전자신호와 정보체계의 총체를 가리킨다고 하면서 이들 가운데 가장 중요한 요소로 상업적 온라인 서비스 전자게시판 시스템, 근거리 통신망(LAN), 그리고 컴퓨터 네트워크를 지적한다. (정진명·성위식, 사이버공간의 법 일반론적 과제-사이버 공간의 법 형성상의 문제, 류시조외, 「사이버 공간의 법률문제」, 부산: 부산외국어대학교 출판부, 1999, p. 15

는 생체 전자 환경(Bioelectronic Environment) [9]을 뜻한다.

사이버 공간은 다양한 형태로 나타난다. 예를 들어 상거래가 이루어지는 시장도 있고, 감동을 전해주는 영화관도 있다. 동영상을 갖춘 신문도 있고, 동호인들이 만드는 가상 마을도 있다. 이렇게 다양한 형태의 전자식 정보나 지식으로 채워져 있는 사이버 공간을 통해 사람들은 현실 공간과 가상 공간을 넘나드는 이중생활을 하게 된다. 사이버 공간은 물리적인 실제 세계와는 구분되며, 단지 컴퓨터에 접속된 참여자의 관념에서만 존재하는 새로운 차원의 추상적 공간을 의미한다. 여기서 공간은 어떤 물체가 차지하는 현실의 공간을 의미하는 게 아니다. 실제의 하드웨어 공간과는 다르지만 무엇인가가 존재하고 작동해서 마치 실제 공간처럼 여겨지는 가상현실을 의미한다. 따라서 사이버 공간은 그 안에 가상현실이 서로 연결되어 있는 광범위한 컴퓨터 네트워크이고, 가상현실이란 그러한 전자 공간속에서 일어나는 현상의 한 종류이다. 그러나 사이버 공간도 다른 매체와 마찬가지로 사람이 관여해야 하기 때문에 사이버 공간은 참여가자 일상세계의 틀과 수많은 정보 속에서 자신의 길을 발견할 수 있는 방향을 제시해 주는 공간으로써 의미가 부여된다. [10]

2) 사이버 공간의 특성

사이버 공간을 구성하는 컴퓨터 네트워크는 시간과 거리의 의미를 변화시키면서 사람과 정보 사이의 새로운 관계를 조성하면서 과거와 아주 다른 형태의 생활을 초래할 것으로 예측되는데, 이러한 변화는 사이버공간이 갖는 다음과 같은 특성에서 유래된다고 할 수 있다.

첫째, 사이버 공간의 가장 큰 특징은 비대면성, 곧 사람들이 사회생활이나 경제생활을 영위하면서 일일이 서로 만나지 않아도 된다는 것이다. 예컨대 판매자와 소비자간 물건을 사고팔면서, 국제간의 무역거래를 하면서, 은행 업무를 하면서, 사람들 간에 서로 대화를 하면서 굳이 만날 필요가 없다는 것이다. 이러한 비대면성 때문에 사이버 공간의 언어는 현실 사회

9) 류시조, 사이버공간의 헌법상의 과제, 류시조 외, 「사이버공간의 법률문제」, 부산, 부산외국어 대학교 출판부, 1999, p. 53~54

10) 노용덕, 「사이버현실과 사이버스페이스」, 서울: 세종대학교 출판부, 1994, p. 62

의 그것과 사뭇 다르다. 대체적으로 네티즌들은 너무나 솔직하게 자신의 생각을 표현하며 때로는 지나칠 정도로 직선적이다. 나아가 사이버 공간에서는 확인되지 않은 사실을 받아들이며 전파하고 동조하는 속도가 굉장히 빠르기 때문에 억울하게 명예가 훼손되어 피해자에게 심각한 피해를 입힐 수 도 있다.

둘째, 사이버 공간에서는 출입하는 주체들의 익명성이 보장된다. 컴퓨터 환경에서는 오로지 사전에 약속된 ID와 패스워드만 필요할 뿐, 이용자의 얼굴모습, 목소리, 신체구조, 성명 등을 밝힐 필요가 없기 때문이다. 이러한 특성은 네티즌으로 하여금 감정의 조절이나 표현에 대한 억제력을 약화(disinhibition) 시키는 요인이 된다. 사용자는 자신의 신분을 노출시키지 않고도 얼마든지 인터넷을 항해할 수 있다. 인터넷이라는 공간은 소위 “ID 주소”라는 것만 가지고 항해하는 곳으로 여러 군데의 홈페이지 게시판에 글을 게시하는 경우나 원격서비스를 이용할 경우에도 비록 일부에서 인증절차를 통해 검증하는 경우가 있기는 하지만 정확한 인적사항을 기재할 것을 요구하지 않는 경우가 대부분이다.

셋째, 시간과 공간의 개념이 무의미하다. 상대의 위치에 상관없이 이용이 가능하며, 전자우편과 같은 통신 수단은 24시간 실시간 의사소통을 가능하게 해주고, 산맥이나 바다 혹은 국경까지도 장애가 되지 않는다. 이는 사이버 공간이 열린사회의 특징을 갖는다는 것을 시사한다. 예를 들어, 사이버 공간에서 범죄를 하는 사람들의 경우를 보면, 하루 24시간 전체가 범행을 할 수 있는 시간이며, 남몰래 신분을 위장하고 외국에 갈 필요도 없고, 다른 회사에 위장 취업할 필요도 없다. 멀리 지구촌 반대편에서 네트워크를 이용해 얼마든지 가능한 일이기 때문이다.

넷째, 컴퓨터와 통신이 발달 하면서 각종 정보는 집중관리 되며 신속히 전달된다. 주요 언론사에서 운용하고 있는 홈페이지의 인물 정보란을 보면, 적어도 사회를 이끌어 가는 거의 모든 사람들의 프로필이 입력되어 제공되고 있다. 지난 신문기사를 찾기 위해 신문사 및 도서관을 뒤지며 돌아다닐 필요도 없다. 인터넷이 연결된 곳이면 어느 곳에서라도 신문 기사를 쉽게 찾아 볼 수 있다. 또한 네티즌이라면 누구라도 사이버 언론 기관을

통해서 기자들이 쓴 기사를 즉각 받아 볼 수 도 있고, 그 전파력 또한 굉장히 크다. 최근 어떤 학자들은 이런 사이버 공간의 특성 때문에 사이버 공간을 '제3의 여론 형성기관'이라고 부르기도 한다. 실제로 정부의 각 부처에서 사이버 여론을 정책 결정 과정에서 깊이 고려하는 경향이 늘고 있다. 과거 일부 소수 계층의 전유물이었던 인터넷이 이제는 국내에서 10명 중 6~7명 꼴로 사용하는 온 국민이 함께 공유하는 공간이 되었기 때문이다.

끝으로 사이버 공간은 동시에 다수의 이용자와 접속이 가능하며 이용장소의 제한을 받지 않는다. 컴퓨터 통신망의 '전자게시판'에 메시지를 올리는 방법으로 동시에 수많은 상대에게 의사를 전달 할 수도 있고, 특정인의 ID를 등록해 놓고 관심 있는 전자우편을 연속적으로 받아 볼 수 도 있으며, 개인용 PC와 모뎀만 있으면 어느 곳에서나 전화선을 이용한 접속과 통신이 가능하다. 더욱 중요한 점은 사이버 공간을 출입한 흔적이 남지 않는다는 것이다. 네트워크상에서 교류되는 정보들은 모두가 디지털자료(digital data)들이라서 동시에 대량 삭제가 가능한 반면에 삭제한 흔적이 전혀 남지 않는다. [11]

3) 사이버전의 개념

전장이 물리적 공간에서 사이버 공간으로 변화함에 따라 미래전이 정보통신기술을 활용한 사이버상의 전쟁으로 변화될 것은 자명한 사실이다. '사이버전'이란 용어의 정의는 명확하게 통일되지 않고, 관점에 따라 다양하게 정의되고 있다. 이러한 이유는 사이버전에 대한 정의 및 자료 자체가 불충분하고, 제시하고 있는 내용 또한 매우 상이하며, 군 및 학계에서도 그 정의를 공식적으로 내린 바가 없기 때문이다. 이러한 이유로 '사이버전'이라고 하는 용어는 정부조직, 군의 조직, 학문영역 그리고 개인마다 매우 다른 의미로 쓰고 있는 것이 사실이다.

또한 '사이버 테러'라는 용어가 '사이버전'과 혼용 되고 있는데, 사이버 테러는 컴퓨터 통신망상에 구축되는 가상공간인 사이버 공간을 이용한 폭

11) 정진섭, 인터넷과 컴퓨터 범죄 동향 변화, 「정보사회와 법칙」, 한국 형사 정책 연구원 제 18회 형사 정책 세미나 자료집, 1996년 5월, p. 59~67

력 행위를 가리키는 용어로, 컴퓨터 통신망을 이용하여 정부 기관이나 민간 기관의 정보 시스템에 침입, 중대한 장애를 발생시키거나 파괴하는 등의 범죄 행위를 뜻한다. 그러므로 본 연구에서는 '사이버 테러'가 아닌 사이버전에 국한하여 연구를 진행 하고자 한다. 따라서 사이버전에 대한 정의를 비롯하여 그 개념을 보다 명확히 할 필요가 있다.

이미 언급한 사이버란 개념을 기반으로 '사이버전'용어를 최초로 사용한 바 있는 미국의 J. Arquilla & Ronfeldt(1993)등은 사이버전을 "정보전과 네트워크 전쟁을 작전적인 측면에서 확장시킨 것으로써 적 의사결정 과정에 대한 전술적인 측면에서의 와해, 지배, 재구성까지 포함하는 개념"으로 정의하면서 사이버전의 주요관심사를 지휘통제와 의사결정에 두고 있다고 말하고 있다. 한국군에서 사이버전이란 말이 실제 사용되고 있는 사례를 살펴보면, "사이버 공간에서 일어나는 새로운 형태의 전쟁으로써 컴퓨터시스템 및 네트워크, 통신망 등을 교란 및 마비, 무력화시킴으로써 적의 사이버체계를 파괴하고, 아군의 사이버체계는 방호하는 것" 또는 "컴퓨터가 합성한 가상현실세계(cyber space)와 가상인간의 영역과 같이 인공지능 체계가 운용되는 공간에서의 전쟁으로서, 정보화 사회의 과학기술을 이용하여 취약점을 공격함으로써 물리적인 파괴보다 훨씬 결정적인 손실을 강요할 수 있는 총체적인 가상공간에서의 정보 마비 전을 추구하는 전쟁수행 방식"이라고 정의되고 있다.

미 국방대학원에서는 사이버전을 "적을 교란·마비·파괴시키는 행위 및 군사력을 운용하는데 있어서 정보우위를 달성하려는 절차"라고 잠정적으로 정의하고 있다.(송기섭 "사이버 전쟁에 대한 대응", 「합참」 제21호, 서울: 국방부 2003 : p.291～292), 즉 "적의 컴퓨터 시스템 및 네트워크 통신망 등을 교란 또는 파괴하여 이에 의존하는 적의 모든 물리적 체계까지 치명적 영향을 주고, 동시에 우리 신경체계를 방호함으로써 궁극적으로는 아군 측에 유리한 결과를 가져오기 위한 전쟁수행 방식"이라고 정의할 수 있다.

사이버전과 정보전의 관계를 살펴보면, 사이버전은 컴퓨터와 네트워크 시스템에서 이루어지는 전쟁으로서 정보전의 한 유형으로 분류된다. 정보

전과 사이버전과의 관계는 과학기술 발전에 따른 군사 패러다임의 변화 측면에서 이해할 수 있다. 즉, 과학기술의 혁신적인 발전이 무기체계의 변화를 가져옴으로써 싸우는 방법이 필연적으로 달라지고, 궁극적으로는 전쟁을 바라보는 시각과 인식의 틀, 즉 군사 패러다임마저 변화를 초래하게 되었다.

본 논문에서는 앞서 언급한 개념을 종합하고, 본 논문의 목적에 맞게 사이버전을 “사이버 공간을 전장(戰場)으로 삼아 사이버체계의 탐색, 공격 및 방어를 수행하는 새로운 형태의 전쟁”이라고 정의하고, 사이버전과 해커전이 이원화되어 사용되고 있는 개념을 통합하여 컴퓨터 시스템을 이용한 인터넷 등 가상공간에서 일어나는 전쟁을 연구대상으로 한다.

2. 사이버전의 특징

사이버전의 특징은 사이버 공간의 특수성과 군 및 사회기반구조의 정보통신체계에 대한 의존성에서 도출될 수 있으며 미국의 국방과학 위원회 특별 팀의 보고 내용을 인용한다면 다음과 같다(US AF, Information Operations, 1998).

첫째, ‘전방이 없다’는 것이다. 이는 상호 복잡하게 연결된 사이버 공간에서 일정한 전선이 형성될 수 없음을 나타내며, 둘째, ‘흐려진 전통적 경계’로서 정보화 특히 인터넷의 세계화로 정보영역에서 국가 간의 경계가 별 의미가 없다는 것이다. 셋째, ‘저렴한 전쟁 비용’으로 전쟁 또는 테러행위의 수행이 가능하다는 것이다. 즉 인터넷에 접속할 수 있는 장비와 컴퓨터 그리고 공격 프로그램만 있으면 공격이 가능하며 공격자의 능력에 따라 치명적인 결과를 만들어 낼 수도 있다. 넷째, ‘인식 조작의 역할 확대’로서 이것은 사이버전 수행의 궁극적인 목적이 상대의 인식통제에 있음을 강조하는 것이며, 다섯째, ‘전략적 정보의 부족’으로서 이는 방어적 측면에서 초기에 사이버 공격을 탐지하더라도 이것이 단순 해커의 행위인지 또는 잠재적국의 공격 준비 단계인지를 판단할 수 있는 전략적 정보가 부족하다는 것이다. 여섯째, ‘전술적 경고와 평가의 어려움’으로 이는 앞의 항과 연관되는 사항으로서 우리가 사이버 공간상에서 특정한 위협을 감지하였을 때 수준에 따른 위협과 그 대응의 정의에 따른 경보의 발령 및 필요

한 사항을 조치 할 수 있어야 하지만 침투행위에 대한 평가가 어렵고 이에 따라 적절한 경보발령도 제한받게 된다. 일곱째, '동맹관계의 형성 및 유지의 어려움'으로 이는 인접 동맹국가와의 협조관계유지가 쉽지 않다는 것이다. 즉 사이버 방어체계가 잘 구축된 국가가 그렇지 못한 동맹 국가와의 상호체계 연동 하에서 훈련 또는 작전을 수행한다면 취약한 동맹국을 통한 우회공격을 허용할 수 있듯이 동맹국가의 취약점이 그대로 영향을 받게 된다. 이러한 이유에서 사이버공간상의 동맹관계유지는 상당한 비용이 요구되며 우리와 미국의 군사동맹관계에서도 시사 하는 바가 크다고 볼 수 있다(장재규, 2002 : p.16~17).

이외에도 사이버전은 '엄청난 파급효과'를 가지고 있다. 물론 정보시스템의 특정 일부 기능에 대한 손상이나 중요자료 탈취로 작전이 종결된다면 간단한 문제일 수 있으나 만일 잠재적국이 아국의 국가기반체계 마비를 공격목표로 하여 조직적으로 공격을 감행한다면 그 파급효과는 일부지역에만 한정되는 물리적 파괴무기가 갖는 효과를 능가하여 국가 전체를 마비시킬 수도 있다. 또한 사이버전은 핵무기처럼 "비대칭적 또는 억제 군사력으로 운용"이 가능하다. 따라서 현실적인 국제관계나 안보환경을 고려한다면 적의 비대칭적인 사이버 공격을 방어하는 방어체계는 기본적으로 구축해야 하고 나아가 응징보복의 능력을 구축해야만 보다 강력한 억지력을 보유할 수 있게 된다. 마지막으로 '사이버전은 정보기술 전문가에 의해 수행'된다는 점이다. 보병의 전투에서 소총수는 특별한 전문적인 능력이 요구되지 않았으나 정보전사라 불리는 미래의 사이버전 수행 인력은 정보기술 분야의 전문적인 능력 없이는 업무수행이 불가능하게 될 것이다. 이러한 사이버전의 중요성에 대해 혹자는 미래 전장에서 군사전략 구성요소에 사이버전 개념이 포함되어야 한다고 주장하였다.

제 3 절 사이버 전사의 정의 및 특징

1. 사이버 전사의 정의

일반적인 개념에서 '사이버 전사'란 사이버전을 수행할 수 있는 역량을 가진 전투원을 의미한다. 가상적국이나 여타 군사강대국이 우리를 향해 군사력을 사용할 징후가 보일 경우, 상대국의 모든 기반체계를 일거에 파괴 및 마비시킬 수 있는 능력을 보여 줌으로써, 상대국이 쉽게 군사력을 사용하고 싶은 생각이 나지 않도록 하여야 한다. 전쟁이 발발하더라도 상대국의 첨단무기 및 정보체계를 효과적으로 사용할 수 없도록 만드는 수단임과 동시에 우리가 상대방으로부터 사이버공격을 받았을 때 국가 및 군사정보체계를 보호할 수 있도록 강력한 사이버 방어역량을 갖추어야만 한다(장유진, "장차전 대비 사이버 전사 양성방안에 대한 제언" 「군사평론」 제351호, 대전: 육군대학 2001 : p.26).

2. 사이버 전사와 해커와의 관계

사이버 전사와 해커의 정의를 비교해 보면, 해커(hacker)는 원래 어려운 과제를 해결하기 위해 학교당국의 통제를 피해 밤마다 학교 컴퓨터시스템에 잠입하여 결국 문제를 해결해 낸 1950년대 MIT학생들과 그들의 '집념'을 의미하였다(http://www. ffstek.com). 처음에는 단순히 '컴퓨터 마니아'를 가리키는 가치중립적인 말로써 컴퓨터시스템을 위해 일하거나 시스템에 대항해서 일을 하는 두 부류를 모두 지칭하는 포괄적인 개념으로 쓰였으나, 1983년 미국에서 상영된 영화 '워 게임'에서 부정적인 이미지로 변화되었다. 이 영화에서 컴퓨터 기술을 사용하여 미국을 핵전쟁 일보 직전까지 몰고 간 한 소년을 언론들이 '해커'라고 명명하면서 해커는 사회에서 해악을 끼치는 사이버 범죄자의 대명사처럼 여겨지게 되었다.

오늘날 사전적 의미의 해커는 "타인의 컴퓨터에 불법으로 접근하여 컴퓨터에 고장을 일으키게 하거나 컴퓨터에 수록된 정보를 탐지하거나 자료를 변조 또는 파괴하는 사람"(http://kr.encycl.yahoo.com)으로 정의되고 있으나, 정보화 시대에 보편화된 해커(hacker)라는 용어는 원래 '컴퓨터에 정

열을 가지고 몰두하는 사람'이라는 뜻으로 시스템이 침투하여 파괴하고 정보를 훔치는 범죄자들은 해커라기보다는 크래커(Cracker)라고 보는 것이 합당하다.

최근 들어 해커는 특정 범죄조직이나 정보기관 또는 각국 정부의 대리인으로서 정보전이나 사이버전을 수행하는 정보전사(infowarriors) 또는 네트워크 스파이(network espionage)라는 용어로 불리고 있다. 이들은 해킹, 암호해독, 바이러스 생산 등의 기술로 무장하고 컴퓨터 가상공간에서 특정국가나 단체의 정치·군사·경제적 이익을 위해 치열한 투쟁을 하고 있다. 여기에서 '정보전사'란 국가에서 정치·경제적 목표를 달성하기 위해 조직적으로 양성하여 이러한 능력을 전문적으로 갖춘 사람들을 의미하며, '사이버 전사'와 동일한 의미로 사용되고 있다.

정보전사와 더불어 추가적으로 문제가 되는 집단이 기술적인 측면에서 해커와 비슷한 사이버 용병이다. 사이버 용병은 돈만 주면 컴퓨터에 대한 전문지식을 제공하는 직업적 해커이다. 주로 동유럽이나 제3세계 출신의 컴퓨터 전문가들이 경제적인 곤궁을 벗어나기 위해 사이버 용병의 길을 선택하는 것으로 알려지고 있으나, 서방의 전문가들도 불황기에 일자리를 찾지 못하면 사이버 용병이 되는 것은 마찬가지다. 경제적인 이유가 아니더라도 돈에 대한 탐욕 때문에 사이버 용병이 되는 경우도 있다.

3. 사이버 전사 양성의 필요성

1) 안보환경의 변화

21세기 정보화 시대에는 제3세계의 약소국가라 할지라도 일류 프로그래머 한둘만 있으면 효율적인 사이버 공격을 감행할 수 있으며, 미국과 같은 강대국을 한번 공격하려면 최소 수십억 달러 이상의 전쟁 자금이 드는 것은 이제 옛날이야기가 된 것이다. 이처럼 정보 전쟁은 적은 비용으로 적국에 치명상을 입힐 수 있다는 매력 때문에 특히 제3세계 국가들이 지대한 관심을 보이고 있는 것으로 알려졌다.

군대 조직과 운영에 컴퓨터가 도입되고, 디지털 기기가 부착된 첨단무기가 실전에 배치되고, 사회・경제 분야에서 컴퓨터 의존도가 높아지는 것은

이제 다른 나라만의 이야기가 아니다. 이러한 측면에서 한국의 미래 안보 환경을 분석해 보면 다음과 같다.

첫째, 정보화 사회로 진행되면서 사회전반에 걸쳐 정보공개요구가 팽배해짐에 따라 국방운영에 대한 국민의 투명화 및 개방화 압력이 더욱 거세질 것이다. 따라서 절대다수의 국민이 공감할 수 있는 더욱 과학적이고 효율적인 국방운영이 절실해지고 있다.

둘째, 그 동안 안정적으로 확보되어 온 국방예산의 긴축과 효율성 제고 압력 등에 의해 감소추세를 피할 수 없게 만들고 있다. 또한 고가화(高價化)된 무기체계는 국방 운영유지비의 절감압력을 피할 수 없게 만들고 있다.

셋째, 전장의 광역화, 동시전장화를 강요하고 첨단무기체계 및 체계간 연동을 통한 전장관리의 효율성 제고 등을 요구하여 근본적으로 국방환경에 영향을 미친다(조관식, 1998 : p.384~394).

넷째, 과학기술의 혁신적인 발전은 군으로 하여금 과거 산업 시대적인 군 구조와 관행으로부터 정보지식 중심의 정예 국방구조로 과감히 전환할 것을 요구하고 있다. 미군의 21세기 디지털화된 군의 모습 속에서 미래에는 총보다는 컴퓨터를 지니고 다니는 군인들이 더 많아질 수 있다는 것을 짐작케 한다. 실제 “미국은 걸프전에 80여만 명을 투입하였으나, 전쟁에 이긴 것은 불과 2,000명의 스마트한 군인들에 의해서였다”는 당시 걸프전에 참전했던 한 장군의 주장처럼 앞으로는 정보기술을 능숙하게 사용할 수 있는 기술적으로 전문적인 군대가 필요하게 될 것이라는 주장에 반론이 있을 수 없다.

2) 주변국 위협에 대응 수단

한국은 미국, 중국, 러시아, 일본 등 주변의 강대국들에 둘러싸여 있다. 오늘날 세계 최첨단 과학기술 보유국이면서 세계 2위의 경제대국인 일본과 현재도 우주기술 및 레이저기술 분야에서 매우 우수한 평가를 받고 있는 러시아와 21세기 동북아지역에서 최대의 군사대국이 될 가능성이 있는 중국 등을 고려해 볼 때, 본 지면에 구체적으로 주변국의 군사력 현황을

제시하지 않더라도, 한반도 주변국은 이미 우리 군사력 수준을 훨씬 넘어서고 있다는 것을 인정할 수밖에 없다. 현실적으로 향후 5~10년 후가 되면 미국의 뒤를 이어 일본과 러시아·중국은 상당한 수준의 정보전 수행능력을 구비할 것으로 예측된다. 따라서 각 국가가 어떤 군사력을 얼마만큼 갖고 있다는 단순히 수직적인 비교는 우리에겐 더 이상 큰 의미를 주지 못한다고 생각된다. 즉, 우리나라는 군비경쟁에서 도저히 살아남을 수 없는 환경에 처해 있다고 볼 수 있다. 이와 같은 이유에서 미래 전장 환경에서 사이버전은 결정적인 전역(戰役)을 담당할 것이며, 적은 비용으로 효과를 극대화시킬 수 있는 사이버전 능력 보유에 우선적인 노력을 기울여야 생존할 수 있다는 데 목소리가 모아지고 있다.

3) 사이버군의 경제적 효과

앞에서 언급한 바와 같이 안보여건 변화에 대한 능동적인 대응과 관련하여 오늘날 우리가 당면하고 있는 최대 현안은 현재의 북한위협은 물론 미래의 불확실한 위협에도 동시에 대비해야 하는 즉, 대북 억제전략과 미래전력 건설이라는 이중적 과제라 할 것이다. 우리의 가장 효율적인 대응방안은 첨단 과학기술의 혁신적인 발전과 한반도 주변국의 군사력 건설동향을 감안하여, 적은 비용으로 미래 안보환경에 효과적으로 대응하기 위한 국가의 인적 자원을 총동원하여 사이버전사를 양성, 운영하는 것이 매우 중요하다. 먼저, 사이버 전사는 비교적 경제적으로 양성할 수 있는 장점이 있다. 세계적으로 정보화가 진행될수록 앞으로의 전쟁에서 사이버전은 필연적으로 일어날 수밖에 없다. 따라서 컴퓨터 시스템을 매우 효율적으로 운용할 수 있는 전문 인력을 잘 양성한다면 막대한 군비를 들이지 않고도 강력한 국가방위력을 유지할 수 있다. 환언하면, 약소국가라 할지라도 일류 프로그래머 한두 명만으로도 강대국에 대해 치명적인 사이버공격을 할 수 있다는 것이다. 이처럼 사이버전은 적은 비용으로 상대국에 치명타를 입힐 수 있다는 장점 때문에 특히 약소국가 및 국제적인 테러리스트들에게는 매력적일 수밖에 없는 것도 사실이다. 실제로 9. 11테러를 감행한 알

카에다 연계조직이 12월 한 달 동안 미국 내 주식 시장과 은행 등에 대해 사이버 테러를 가하겠다는 협박을 해왔다고 미국정부가 밝힌 바가 있다고 한다. (2006. 12. 1. 쿠키뉴스).

물론, 아무리 강력한 사이버전사를 많이 양성했다 하더라도 효과적인 물리적 타격수단을 구비하지 못한다면 진정한 군사력을 갖추었다고 말할 수 없을 것이다(장유진, 2001 : 30). 정보전쟁은 전쟁의 상대적 비용을 절감시키고 전형적, 전통적인 전쟁과 달리 인명, 재산피해가 적다. 또한 정보운용의 역할이 확대되면서 고부가 가치 산업의 발전을 가져올 수 있다. 하지만 아직 전략적인 지식·정보 인력이 부족하고 전술적인 공격으로부터 방어가 어렵다. 따라서 정부에 정보전쟁에 대비할 부서를 운용하고, 범국가적으로 정보전에 대한 중요성을 부각시켜야 하고 현재의 힘 위주의 전략에서 보다 효율적인 차원의 전략수립이 필요할 것이다(Peter A. Wilson, 1996).

1997년도에 미 육군성에서 제작 배포한 'Army Experiment 3' 내용을 보면 미군이 건설하고자 하는 디지털화 된 군의 모습을 일부 엿볼 수 있는데 이는 장차전의 전투양상을 단적으로 예측케 한다.

첨단무기들이 고도화되면 될수록 컴퓨터와 네트워크에 더욱 의존하게 될 것이다. 또한, 조그마한 목표를 하나 타격 하더라도 모든 체계들이 이와 같이 통합되어야만 전쟁수행이 가능할 것이다. 따라서 사이버공격수단으로 상대국의 컴퓨터시스템과 네트워크에 침입하여 이러한 시스템 연결고리만 파괴한다면 아무리 첨단무기라 해도 제 기능을 발휘할 수 없다. 따라서 사이버전 능력은 약소국이 함부로 물리적인 타격수단을 통해 자국의 의지를 관철시키려 할 때에도 강력하게 대응할 수 있는 힘을 줄 수 있다. 더구나, 디지털 및 인터넷 혁명으로 인해 전 세계가 시·공간 구분 없이 하나의 생활권으로 변화하고 있고, 사이버공격 수단도 시간이 흘러갈수록 더욱 고도화 및 지능화되어 가고 있다. 이러한 체계들은 근본적으로 개방된 상태에서 운용될 수밖에 없기 때문에 사이버전에 매우 취약하다. 결과적으로 사이버 전사는 향후 군사 강대국에 대해 매우 효과적이고도 강력한 대응수단이 될 수 있다.

제 3 장 사이버전 유형과 사례

제 1 절 사이버전의 유형

사이버전은 파괴의 방법과 목적에 따라 운용 및 응용소프트 웨어전, 컨텐츠전으로 구분할 수 있다.

1. 운용 및 응용 소프트웨어전

네트워크의 운용이나 네트워크를 기반으로 특정용도를 달성하기 위해서 제작된 운용 및 응용 소프트웨어를 왜곡·파괴하여 네트워크에 연결된 광역전장감시체계, 정밀타격체계, 컴퓨터 등의 단말기로부터 생성된 정보의 흐름을 마비·지연시키는 것이 주목적이다. 물리적으로 네트워크를 파괴할 경우는 교체하기까지 장기간이 소요될 수도 있지만 파괴구간이나 장비를 교체하거나 우회 네트워크를 구축할 수 있을 것이다. 그러나 해킹을 통해서 바이러스를 침투시켜 운용소프트웨어를 왜곡시킬 경우에는 더 큰 피해를 입을 수 있다.

2. 컨텐츠전

네트워크를 통해서 흘러 다니거나 네트워크의 단말기체계에 저장된 정보를 왜곡·파괴시키는 것이 목적이다. 적용되는 소프트웨어무기는 운용 및 응용소프트웨어전에 사용되는 것과 유사하지만 용도가 다르다. 그러나 군에서 운용하는 네트워크 및 단말기 체계는 생존성·신뢰성을 보장하기 위해서 체계를 물리적으로 분리하거나 다중화 체계로 대부분 구축하기 때문에 접근이 어렵다. 그러나 내부 동조자 등을 이용하여 정보에 접근하여 정보를 파괴하거나 왜곡하는 등의 활동은 손쉽게 할 수도 있을 것이다. 따라서 이를 방지하기 위한 인증관리제도, 보안통제 및 안전운영방안 등의 대책이 마련되어야 할 것이다.

제 2 절 사이버전 주요 사례

1. 소말리아 분쟁

1993년 8월에 시작된 소말리아에서 미군은 전술적 승리에도 불구하고, 전략적으로는 패배한 것으로 평가되고 있다. CNN 방송은 소위 CNN효과(CNN Effect)를 통해 결코 전쟁이라는 전통적 국가적 행위가 이제는 일반 대중의 여론에 의해 좌우될 수 있음을 증명하였는데, CNN 화면을 통해 방영된 한 미국 병사의 시체는 미국 내 엄청난 반향을 불러 일으켰다. 전쟁의 잔혹함에 대해 피상적으로만 알고 있던 미국 국민들은 CNN 덕분에, 시간과 공간적 한계를 초월해 한 병사의 비참한 시신을 통해 전쟁에 대한 반감을 갖게 되었다. 이러한 현상은 정책적 측면에서 전쟁 여부를 결정하는 정치적 지도자에게 많은 영향을 미쳤을 뿐만 아니라, 전장의 지휘관 입장에서도 전술적 변화를 강요하게 되었다. 미군 지휘관들은 특정 전술이나 작전 구사시, 어찌 보면 군사작전상 불가피한 미군의 인명피해를 최소화하는 것이 가장 중요한 전술적 목표가 되었다. 그리고 이와 같은 시대상황의 변화에 따라, 두 번 다시 전장에서 병력과 병력이 서로 충돌하는 전쟁을 하지 않는다는 개념으로서 '무병력 전장(empty battle field)'을 제창하는 "사이버전"이라는 새로운 형태의 전쟁 방식이 크게 부각되었던 것이다.

2. 보스니아 분쟁

미군을 포함한 NATO(North Atlantic Treaty Organization : 북대서양조약기구)군이 개입한 보스니아 분쟁은 미군이 최첨단 정보능력을 통해 NATO군이 피해를 최소화 하고 공격력을 극대화하는 「정보우산」개념을 성공적으로 수행한 대표적 사례이다. 실시간 영상과 화상 데이터를 통해 분쟁 당사자가 이미 합의된 내용을 준수하고 있는지 여부를 감시할 수 있도록 공중에서 열원(熱援)을 탐지함으로써, 차량조차 임의로 이동하는 것이 불가능하게 되었다. '정보우산'은 상대방에게 사실 그대로를 입증해 보임으로써 납득시키고 합의로 이끌 수 있는 새로운 분쟁해결 형태의 단초를 제공하는 한편, 지금까지 의혹과 반발이 일어나기 쉬웠던 국가 간, 기관과 기관간의 상호 협력 체제를 가능하도록 하였다. 결국 소말리아와 보

스니아전을 통해 분쟁을 해결하되 아군의 희생을 최소화 할 수 있는 효과적 대안으로 사이버전 능력이 더욱 부각되는 계기가 되었다.

3. 코소보 분쟁 : 제 1차 사이버전

일반적으로 걸프전이 사상 최초의 사이버 전쟁으로 평가받고 있으나, 사실 코소보 전쟁의 경우 아래에 제시하는 모든 형태의 사이버전이 전개되었다는 점에서 본격적인 제1차 사이버전이라 할 수 있다.

1) 심리전 : 선전전

1999년 3월 24일에 NATO의 공죽폭격 개시후 불과 4시간 만에 베오그라드의 반체제파 독립계 라디오 'B 92'의 방송이 중지되었다. 그러나 TV, 신문과 같은 대중매체에 대한 정보통제는 용이하지만, 경계와 국경이 없는 인터넷에 대해서 규제가 어렵다는 사실을 알고 있는 시민들은 그 후에도 인터넷을 통해 정보를 입수하였다. 인터넷은 시민뿐만 아니라 유고 정부에 있어서도 강력한 무기로써 세르비아 정부의 정보부 홈페이지에는 "NATO의 오발 사건에 관한 조사를 요구", "공중폭격의 희생자 더욱 늘어나다", "NATO의 공격과 나치와의 유사점", "NATO의 범죄" 등의 기사가 게재되어 전 세계를 향해 선전심리전을 펼쳤다.

한편 알바니아계 주민의 홈페이지들은 엄격한 규제 속에서도 국경 없는 네트워크를 통해 "유고군의 학살행위 계속되다", "NATO 공격강화"와 같은 내용을 지속적으로 게재하였으며, 공중폭격을 거듭하던 NATO의 홈페이지는 전 세계를 향해 공중폭격의 정당성을 계속 주장하였다.

당시 신문을 살펴보면, "유고 심리전에서 '맹반격', NATO의 비인도주의적 행위를 강조(1999. 5. 24.자 요미우리 신문)" 등과 같은 기사들이 주목되는데, 코소보 분쟁이래 인터넷을 중심으로 국경을 초월한 격렬한 공방을 펼치게 되어 전형적이 사이버전이 전개되었던 것이다.

2) 해커전 : 정보 시스템의 기능 교란

1999년 3월 31일, NATO의 대변인은 기자회견을 통해 “여러분들 중 대다수는 우리의 홈페이지 내용을 토대로 기사를 쓰고 계실 것으로 생각되는데, 그 홈페이지가 3월 28일 이후 매우 불안정해진 사실을 이미 알고 계신 분도 있을 것입니다. 사실 NATO군사령부의 홈페이지를 구동하는 컴퓨터 서버가 누군가에 의해 해킹 당했으며, 우리도 그 사실을 확인하였습니다. 현재 주의 깊게 조사하고 있는 상황으로, 우리는 베오그라드의 해커 소행일 것으로 추정합니다. 웹사이트의 과부하(overflow)를 노린 공격, 개인이 하루당 2,000통 이상의 전자 메일(e-mail)을 계속해서 보내는 행위로 인한 전자 메일 시스템다운, 그리고 유고슬라비아에서 보내오는 ‘매크로 바이러스’로 인해 우리는 매우 고심하고 있습니다.”라고 밝힌바 있다.

美 국방부 조사에 따르면 미 국방부 및 NATO 군사령부에서는 ‘메릿사’와 ‘파파’라 불리는 컴퓨터 바이러스를 전송시켜 서비스 기능을 중지시키려는 공격을 확인하고 서버의 보안을 강화시켰다. 또한 1997년부터 NATO 지역 내 은행을 포함한 각종 온라인 상거래를 위한 ‘e-commerce-mi2g′라 불리는 소프트웨어가 가동되기 시작하였는데, 이에 대한 공격이 우려되었다.

3) 사이버전 : 홈페이지 내용 변경

1999년 5월 9일, 해킹을 통해 유고 주재 중국 대사관에 대한 오폭(誤爆)을 비난하는 사이버전이 치열하게 전개되었다. 미국의 에너지부, 내무부, 백악관의 홈페이지가 연이어 해킹을 당해, 홈페이지 내용이 오폭으로 희생된 사망자들의 사진과 항의 메시지로 변경되는 사건이 발생하였다. FBI(Federal Bureau of Investigation : 미 연방수사국)는 해커수색을 개시하여 해커 집단인 ‘Global Hell(GH)′의 가택을 수사하였는데, 이에 대한 보복으로 5월 26일에 FBI 자신의 홈페이지도 공격을 받아 수일간 폐쇄될 수밖에 없는 지경에 놓이기도 하였다.

4) 사이버전 : 정보 데이터의 조작

뉴스위크지는 1999년 5월 23일에 “클린턴 美 대통령이 유고 국내의 정보 네트워크를 교란할 목적으로 사이버전을 치를 것을 CIA(Central Intelligence Agency : 미 중앙정보국)에 명령했다”고 보도하였다. 명령 내용은 컴퓨터 해커를 동원하여 밀로세비치 대통령의 해외예금 구좌를 자유롭게 사용할 수 없도록 조작하였고, 또한 석유 비축금을 사용할 수 없도록 국가 주요 기반구조에 대한 정보시스템을 조작함으로써 유고 국내를 마비 및 교란시킨다는 내용이었다. 그러나 법률적 윤리적 측면의 문제점이 대두되어 결국 본격적 실행은 이루어지지 않은 것으로 알려져 있다.

그러나 뉴욕 타임즈지는 199년 11월 9일 “美 합동참모본부 의장이 코소보 분쟁에서 일종의 컴퓨터 무기를 사용한 점을 인정하였는데, ‘시스템의 일부를 사용하였다’고 언급하였으나 상세한 내용은 밝히지 않았다”고 보도하였다.

5) 경제 사이버전 : 비살상 무기에 의한 공격

NATO군은 유고의 전기 공급원 파괴를 위해 베오그라드 근교의 발전소 등을 탄소섬유 폭탄 등으로 공격하였다. 이 공격으로 유고전역에 원활한 전력공급이 불가능하게 됨으로써 정보 시스템과 민간시설의 가동이 중지되었다. 탄소섬유 폭탄은 발전시설의 파괴 전용무기가 아니라 송전선 상공에서 망 형태의 탄소섬유를 살포하여 송전선을 절단시킴으로써 일시적으로 기능을 중지시키도록 하는 ‘비살상 무기’이다. 비살상 무기라 함은 대량 파괴와 인명 피해 없이 적국에 피해를 가할 수 있는 무기체계 전반을 총칭한다. 물론 이러한 공격은 사이버전과 직접적 연관은 없는 듯 보이나 정보시스템 공격과 같이 특별한 인명살상 없이 전력설비 등 국가 경제기반에 대한 공격을 수행한다는 점에서 ‘경제 사이버전’이라고 할 수 있다.

6) 정보기반전 : 정밀 유도무기(Precision Guided Munitions/Missile, PGM)에 의한 공격

경제 기반시설에 대한 NATO의 정밀 유도무기 공격은, 유고에게 엄청난 경제적 손실을 야기함으로써, 결국 유고 정부가 NATO의 제안을 받아들이게 된 주요 이유라고 평가받고 있다. 정밀 유도무기에 의한 공격은 유고 석유 정제설비 전체를 폐쇄하게 만드는 한편 발전소 14개, 교량 63개, 민·군 각각의 석유저장 시설의 절반가량을 파괴하였다. 이러한 공격은 미국의 GPS(Global Positioning System : 위성항법체계), 관성유도 시스템(Inertial Navigation System, INS), 무인 정찰기 등에 탑재된 센서들과 정밀 유도무기와의 데이터링크에 의해 수행되었으며 그 공격의 정확도는 상상을 초월하여 목표물 명중도는 9.6m나 된다고 한다. 바로 이것이 사이버전 중에서도 정보기반전이라고 할 수 있다.

이상과 같이 코소보 분쟁은 사이버전의 중심이 되는 사이버전 이외에도 정보 기반전이 철저하게 실시되었다는 점에서 전쟁 역사상 커다란 전화점이 되는 한편 미래전 양상을 예측할 수 있는 단초를 제공하였다. 즉 지상전을 전개하지 않은 채 압도적인 공군력만으로도 상대방을 항복시킨 것은 처음 있는 일이다. 위에서 언급되지 않은 지휘 통제전과 전자전은 이제까지 어떠한 전쟁에서도 필수적으로 실행되었으며, 따라서 Libick이 분류한 사이버전 유형이 모두 드러난 코소보 분쟁은 가히 세계 최초의 '제1차 사이버전' 이라 할 수 있으며 21세기의 새로운 형태의 전쟁이 가시화되고 있음을 증명하였다.

제 4 장 주변국 및 우리나라 사이버전 대응 태세

제 1 절 주변국 사이버전 대응 태세

미국을 비롯한 선진국들은 사이버전 기술을 바탕으로 고도의 첩보전과 사이버전을 전개함으로써 사이버전에서 우위를 차지하려고 치열한 경쟁을 벌이고 있다. 세계 각국은 사이버전을 수행한 해커부대를 공식화하기에 이르렀고, 유력한 사이버무기들도 속속 개발되고 있다. 미국을 비롯한 영국, 중국, 프랑스, 러시아, 이스라엘, 북한, 일본 등에서는 이미 90년대 중반부터 사이버전을 본격 준비해 오고 있다.

1. 미국

1) 사이버전 부대 현황 및 결성 계획

1996년 7월 미 국방부 국가안보국(National Security Agency, NSA)과 FBI(Federal Bureau of Investigation : 미 연방수사국)를 중심으로 정예 해커를 뽑아 사이버전부대를 구성했다. 이 부대는 미 국방부에서 사이버전쟁 시나리오를 작성하고 이에 대한 공격 및 방어 훈련을 지속해 오고 있다. 사이버전 전문인력 양성을 위해 사이버전부대 프로그램에 의해 선정된 대학의 정보보안 전공학생에게 2년간 장학금을 주고 졸업 후 등록금 수혜 기간만큼 관련 기간에서 근무토록 하고 있다.

2) 기본개념과 전략

일반적으로 미국의 사이버전 전략은 「전략 사이버전(strategic information warfare)」과 「종심방어(defense in depth) 전략」의 두가지 형태가 근간을 이루고 있다. 우선 사이버테러나 침해에 대한 방어전략으로 「종심방어전략」은 정보기술의 발전에 따라 고도화·지능화·전문화 되어가고 있는 정보 위협에 대해 자국의 정보 및 정보시스템을 보호가기 위한

전략이다. 종심방어는 다양한 형태의 공격에 대해 하나의 방어시스템으로 모두 대응할 수 없다는 인식하에 다양한 공격에 다양한 보안수단을 강구하여 하나의 보안수단의 약점을 다른 보안수단의 강점으로 상호 보완한다는 전략이며 이러한 정보 보증의 달성을 위해 인력, 운영, 기술 등 3대 요소의 균형적인 집중을 중요한 원칙으로 강조하고 있다. 구체적인 내용은 아래의 표와 같다.

<표4-1> 미국의 종심방어전략 운영

구 분	업 무
인 력	전문인력 양성, 교육, 훈련, 현장경험 프로그램 수립
운 영	보안정책의 집행, 신속대응, 중요서비스의 복구
기 술	복수장소에서의 보호메카니즘 및 계층적 보호메카니즘 구현, 채택된 보호 메카니즘의 강점 및 취약점의 식별, 강력한 키관리, 공개키 기반구조의 채택, 침임탐지를 위한 하부구조 구축 등 기술획득과 관련된 정책 및 절차

자료 : 공성진, “21세기 신 10만 양병”, 「2006 국정감사 정책자료집 시리즈 4」, p. 19

이러한 종심방어는 국가안보국이 국방부를 포함한 각 부처 및 기관의 효과적 사이버대응을 위한 전략으로 개발하였는데, 다중계층, 다층차원의 방어를 위해 대상 계층을 지역 컴퓨팅 환경, 네트워크 경계, 네트워크 및 기반구조, 지원기반구조의 4가지 영역으로 구분하고 각 계층적 영역에서의 목적에 따른 정보보호기술 및 시스템 구축에 대한 지침을 제공하고 있다.

이러한 종심방어전략이 대테러 예방 및 대응 차원에서 이루어진 수동적 방어 전략이라면, ‘전략적 사이버전 전략’은 탈냉전이후의 국제안보환경의 변화와 정보혁명에 의한 기술적 변화에 대응하기 위한 능동적이며 보다 적극적 공세적 전략이라고 할 수 있다. 랜드연구소에 의해 처음 개발되어 점차 미 국방부의 핵심전략으로 발전된 전략적 사이버전(strategic information warafare)은 전쟁의 저비용, 공격자의 전통적 경계선의 부재, 인식조절, 전략적 정보활동, 전술경보와 공격평가, 동맹구성과 유지, 미국 본토의 취약성 등에 기초하여 마련되었다.

전략적 사이버전의 특징은 첫째 누구라도 약간의 비용으로 국가적 위해를 가할 수 있으며, 둘째 누가 공격하였는지 밝혀내기가 매우 어렵다는 익명성, 셋째 무엇이 사실이며 무엇이 거짓인지 식별하기 어려울 수준의 인식 조절 가능성, 넷째 전략 정보활동이 쉽게 가능하지 않기 때문에 누가 적이며 누가 아군인지 판단하기 곤란하고, 다섯째 전술경보의 한계로 인해 언제 공격을 받을 것인지, 누구로부터 받을 것이지 사전에 알아내는 것이 불가능 하며, 여섯째 적대적 사이버전의 환경에 노출되기 쉬운 상황에서 새로운 동맹관계가 구축될 경우, 동맹 당사자들 역시 위험에 빠질 수 있기 때문에, 동맹의 구성과 유지가 어려울 수 있는 측면, 마지막으로 미국이 군사적 초강대국이라는 우월적 지위에도 불구하고, 국제 경제의 효율적 관리를 위한 정보시스템과 인프라의 보호에 주력해야 한다는 점 등을 고려한 것이다.

3) 국가 사이버안보 대응체계

- 국토안보부

2002년 6월 6일 대통령령에 따라 테러대응 종합대책부서로 창설된 기관으로, 16,900여명 달하는 인원과 연간 예산 374억불이 소요되는 방대한 기관이다. 연방재난관리국, 해안경비대, 교통안전국, 세관국, 이민국, 연방보호국 등 여러 부처들이 통합된 최고 기관으로, 주요 임무는 미국 내 테러 공격방지, 미국 내의 취약성 경감, 테러 공격 시 피해 최소화 등이다.

- 사이버안보담당 대통령 특별보좌관

사이버전에 대비, 민간부분과의 협력강화를 위해 대통령 직속 사이버안보 담당 보좌관으로서 정보시스템 보안을 위한 각 부처 및 연방정부, 지방청의 활동에 대한 총괄조정, 침해사고 발생시 복구 작업의 총괄, 정보통신시설을 운용하는 민간분야와의 업무조정 및 협의역할 등을 수행한다. 국토안보부장과 대통령에게 상시 보고하면서 대통령 주

요기반 보호위원회의 참여위원으로 활동한다.

- 국토안보회의

2001년 10월 29일 국토안보에 대한 대통령령 제1호에 의거, 테러범의 위협과 공격으로부터의 미국본토의 수호, 잠재적인 테러위협의 감소, 공격발생시에 피해를 최소화하기 위한 연방정부와 주정부와의 총괄적 조정의 필요성에 의해 설립된 조직으로 미국본토 안보에 대한 모든 정책의 효율적 개발과 실행, 유관부서들의 업무에 대한 조정기능의 강화 역할을 담당한다. 이러한 목적을 수행하기 위해 고위급위원회와 부장관급위원회 정책조정위원회가 있다.

- 대통령 주요기반보호위원회

2001년 10월 16일 대통령행정명령 13231 「정보시대의 주요기반보호」라는 정책목표 아래 비상대비 통신망을 포함한 주요 기반 정보시스템을 지원하는 물리적 자산의 안전을 확보하여 미국 국민, 경제, 정부서비스 및 국가안보 보호를 목적으로 구성되었다. 효율적 목적달성을 위해 대통령직속 주요기반보호위원회(President's Critical Infrastructure Protection Board, PCIPB)를 설립하여 주요기반보호정책을 강화하고 효과적으로 집행할 수 있는 조직체계를 마련한 것으로 국토안보부와 긴밀한 협력체계를 구축하여 주요 정보통신기반보호를 강화하고 국가적 차원에서 정보안보를 확보할 수 있는 선도적 장치의 마련에 주안점을 두고있다.

4) 미국의 사이버공격 및 전담대응기구

- JTF-CNO(Joint Task Force - Computer Network Operation)

미국의 사이버전 대응체계의 핵심은 미국 전략사령부(US Strategic Command) 산하의 JTF-CNO와 미공군사이버전 센터로서, JTF-CNO는 미군 전략사령부의 컴퓨터 네트워크 작전 수행을 위한 작전부서로

서 미군의 군사력 가동시 컴퓨터 네트워크에 대한 공격과 방어에 있어 전략사령관의 보좌역할을 담당한다. JTF-CNO는 현재 47명의 인원과 연간 3백만 달러의 예산으로 운영되는데 주요 임무는 각 통합사령부, 부서 및 국방부 컴퓨터 시스템과 네트워크의 방어 조정·감독과 사령관 명령 발효시 국가목표달성을 위해 컴퓨터 네트워크에 대한 공격 조정 등이다. J산하 주요 조직으로는 육군 제1정보작전 사령부, 해병대 컴퓨터 네트워크 통합 방어팀, 해군 컴퓨터 방어 T/F(Task Force : 대책본부)팀, 공군 컴퓨터네트워크 작전팀, 국방정보체계국의 비상대응팀 등이 있다.

- 미공군사이버전센터(공군정보전본부)

1993년 걸프전에서의 혁혁한 전과에 고무된 미국은 공군전자센터와 공군암호지원 센터의 보안부서들을 통합하여 사이버전 전담부서로서 미공군의 사이버전 개념과 전략 개발을 담당하는 공군사이버전센터를 창설 하였다. 주요 임무는 우주항공 및 합동군의 사이버전 요구에 필요한 작전수행, 목표식별 및 포착을 위한 사이버전 분석 및 자료생산 등이며, 공세적 측면에서 사이버전 능력을 극대화시키기 위한 전략전술 개발도 담당하고 있다. 정보지휘국(IO Directorate), 사이버전 전장실험실(IW Battle-Lab), 분석실(Analysis Division), 대방어 정보실(Defensive Counter Information Division), 대공격 정보실(Offensive Counter Information Divison) 및 기타 다수의 사이버전 부대 등으로 구성되어 실질적인 사이버전 대응능력을 갖추고 있는 것으로 알려져 있다.

2. 중국

1) 사이버전 부대 현황 및 결성 계획

중국은 1991년 1차 걸프전 직후 사이버전의 중요성을 절감하며 1997년 4월, 중앙군사위원회 직속의 인민해방군 소속 사이버 해커 부대를 창설했다. 우수 요원 확보를 위해 해방군 산하 사관학교, 미국에 유학생 출신, 중

국내 대학의 컴퓨터 관련 학과 우수 졸업생을 선발하고 있다. 해커부대는 1998년, 베이징, 선양, 난정에서 논리 폭탄(메일 폭탄)을 사용한 사이버 전쟁 훈련을 거쳐 1999년 미국과 전 세계에 있는 파룬궁 사이트를 초토화하여 중국의 사이버전 능력을 대내외에 과시하였다. 2001년 4월, 미군 정찰기와 해방군 공군 전투기의 하이난다오 부근 공해상에서 충돌 사건으로 빚어진 중-미 사이버 전쟁으로 중국 해커들이 백악관과 FBI, NASA(National Aeronautics and Space Administration : 미 항공우주국) 등 미국의 대표적인 정부기관 전산망을 집중 공격했다. 이에 미 국방부는 컴퓨터 시스템 비상 경계령인 '인포콘 알파'를 발령하기도 했다. 현재 중국은 사이버전 특수 인력 양성 및 각종 사이버전 무기와 전술을 개발해 미국에 못지않은 최강의 사이버전 능력을 보유하고 있다.

2) 중국 인민해방군 대응 태세

중국은 해커부대 넷포스와 사이버전시험센터, 국방과학기술정보센터 등의 해커양성기관을 운영하고 있으며, 이들을 활용하여 정례적인 사이버전 모의 훈련을 실시하고 있다. 비록 이들의 활동은 기밀사항으로 중국정부 역시 이들의 활동에 대해 대부분 부정을 하고 있지만, 중국 인민해방군의 사이버공간을 공격적으로 활용하기 위한 군사 전략적 목표와 방향은 비교적 분명한 것으로 알려져 있다. 중국은 대만의 분리 독립 움직임을 차단하기 위한 무력충돌 상황에서 외부의 군사지원을 저지하기 위해 기술적으로 우위에 있는 적대 국가의 군사 작전을 사전에 봉쇄할 수 있는 선제공격 수단으로 사이버전을 수행하려는 것이다. 이에 따라 중국군은 사이버 안보를 위한 군사훈련의 빈도수를 높이는 가운데, 다양한 분쟁상황을 상정한 사이버전 훈련을 실시하고 있다. 실례로 중국군은 2000년 6월, 100여 개 이상의 컴퓨터 터미널들을 연결하여, 인터넷상 사이버전 수행 훈련을 통해 군사훈련을 조직하고 기획하는 측면, 방송과 정보를 통제하는 훈련, 사이버 공간의 침투와 방어 훈련 등을 실시한 바 있다. 이 훈련과 관련, 주목할 만한 사실은, 2000년에 개최된 중국공산당 중앙위원회는 통합적 사이버

전 수행을 위한 포병사단 창설과 인민군 감축 등을 포함한 軍 현대화를 결정했다는 점이다.

반면에, 중국은 비대칭적인 군사력 열세를 만회할 수 있는 전략으로써의 사이버전뿐만 아니라 외부의 정보공격에 대응하기 위한 방어전략, 즉 사이버 안보 역시 중시하고 있다. 1997년 10월 선양지역방위군은 육군, 전술부대, 의료부대, 공군부대 합동으로 참여한 가운데 사이버 공격으로 군의 통신 시스템이 마비된 상황을 상정하고, 이를 격퇴하기 위한 바이러스 퇴치 소프트웨어를 동원하였으며 1998년에는 훨씬 광범위한 지역에서 지역방위군간 합동 대응훈련이 실시되기도 하였다. 1999년 베이징 방위군들은 첩보, 사이버 공격에 의한 침투, 사이버 봉쇄, 공습을 저지하기 위한 훈련을 중점적으로 실시한 바도 있다.

특이한 점은 중국 인민군이 사이버전에 대비하여 세 가지 유형의 집단을 설정하고 집단별 특성에 맞는 대비 훈련을 하고 있다는 사실이다. 중국 당국은 사이버전이란 지식중심의 전쟁(knowledge-style)으로 규정하고, 특별한 재능을 지닌 행위자들 간의 힘의 대결로 인식하고 있다. 또한 중국의 정보통신기술에서 선진국에 비해 열세임을 인정하고, 유능하고 잠재력 있는 집단을 크게 세 가지로 구분하여 효율적인 대응책을 마련하고 있다.

첫 번째 유형은 지원 그룹으로, 40대 이상의 정책결정을 담당하는 그룹이며, 훈련 목표는 사이버전의 영향과 중요성을 일깨워주는 한편, 훈련을 통해 사이버전의 의미에 대한 명확한 이해를 유도하는 것이다. 이 집단에게 요구되는 훈련의 기본적 내용은 기초적인 정보기술, 사이버전의 이론, 정보공격 무기에 대한 일반적 지식들이다.

두 번째 집단은 전환기 그룹이다. 30~40대의 미래 지도자로 성장 가능성이 있는 그룹으로 훈련 목표는 사이버전 환경에서의 지휘 통솔력 향상이다.

세 번째 집단은 역량강화가 필요한 그룹이다. 30대로 이미 정보사회에 대한 상당한 이해가 있고, 현대 정보통신기술에 대한 전반적인 기초지식을 갖추고 있는 집단으로 훈련 목표는 사이버전 상황에서 통솔력 숙달 및 첨단기술에 대한 지식 배양이다.

중국 인민군은 사이버 공격이나 지휘통제의 교란을 장악하기 위한 다양한 유형의 시나리오를 준비하고 전술적인 훈련을 지속적으로 하고 있다. 사이버전의 다른 대비 방향은 군 구조를 현대화 하여 사이버전에 효율적으로 적응할 수 있도록 적극 추진하고 있다. 그리고 지휘부를 형성하는 장교들을 위상과 역할에 따라 미래전에 대처할 수 있도록 교육하고 훈련하고 있다.

중국은 다른 대상 국가들의 경제와 병참, C4I(command, control, communication, computer and Intelligence) 등에 대한 공세적 사이버전 프로그램을 구상하고 있는 것으로 알려지고 있다. 구체적으로, 외국의 군사·민간 컴퓨터망에 바이러스를 침투시켜 무능력하게 만드는 방안을 구상하면서 한편으로는 자신들의 전자전 능력을 개선시키기 위한 다양한 방법(인터셉션, 재밍, 전자정보수집)을 시도하고 있다. 특히, 중국인민군은 새로운 IT기술을 실제 전장에서 사용하기 위한 다양한 방안을 구상하면서 1997년 이래로 적의 군사통신시스템을 교란시키고 파괴시키기 위한 많은 군사작전을 수행해 오고 있으며 최근에는 통합전자전능력으로 무장된 첨단 포병사단까지 창설한 것으로 알려지고 있다. 물론, 해외 첨단 기술에 계속 의존해야만 하는 중국으로서는 향후 계속해서 자신의 정보망에 대한 외부 공격의 위험성(공격취약성)을 잘 인지하고 있으며 실제로 2006년 6월 중국인민군의 군사작전 연습에 사이버전 관련 시나리오를 포함시키고 있어 특히, 전자·통신 분야에 있어 고급암호기술력을 배양하고 광섬유 통신망을 확대하는 등 정보안보강화를 위한 대책마련에 부심하고 있다.

3. 북한

북한의 사이버전 능력의 확대에 가장 큰 영향을 미치고 있는 것은 북한의 지도자인 김정일과 그 일가이며, 향후 유관분야의 지속적이 발전도 이들 지도층의 의지에 달렸다고 보여진다. 실제 평양의 고위 지도층은 IT 분야를 주목하고 있으며 이 분야의 지속적인 발전을 위한 비용을 지불하고 있다. 특히 “미디어광”으로 소문난 김정일은 인터넷에 매우 심취하고 있는 것으로 알려져 있다. 특히 김정일의 지휘로 북한의 컴퓨터 소프트웨

어 및 통신 기술에 대한 투자를 강화하였으며, 군, 당, 그리고 학술 분야 리더들 간의 국내 인트라넷(intranet)의 설치를 직접 지원하였다. 또한 최근 10년 간, 북한은 외부 침입으로부터 중요한 국내 통신과 데이터베이스를 보호하기 위해 인터넷 방화벽 응용을 연구했다고 보고되었다. 그리고 김정일의 아들인 김정남은 김책공과대학과 김일성대학, 약촌 연구소, 평양 정보센터 및 북한과학아카데미의 각종 컴퓨터 관련 작업 및 프로그래밍 활동을 직접 감독 및 주도하고 있는 것으로 알려져 있다. 특히 1984년 인민무력부 총참모부 산하에 5년제 지휘자동화대학(金日군사대학)을 설립하여 전문인력의 양성을 시작하였다. [12]

1) 북한의 대남 사이버전 수행 거점 및 특성

이미 언급한 알려진 북한의 사이버전 동향 실태보다 더욱 주의를 기울여야 하는 부분은 북한이 실제 어떠한 사이버전 및 정보네트워크를 통한 첩보·정보 수집활동을 전개하고 있으며 그 실태와 위협의 정도가 어는 수준인지를 파악하는 것이라 판단된다. 다양한 비공개 소스로부터 수집된 첩보 수준의 정보에 기초하면 우선 북한은 중국의 흑룡강성, 산동성 및 복건성과 북경 인접지역에 대남사이버전수행 거점을 확보하고 있는 것으로 파악되고 있다. 그러나 이들 지역 보다 더욱 왕성한 대남 사이버전수행 및 정보네트워크를 통한 첩보·정보 수집활동 거점으로는 중국 요녕성 단동시를 지목할 수 있다. 특히 북한 신의주를 압록강 건너 마주보고 있는 단동시는 북한의 대중 무역의 중심지며 한국과의 교류의 주요 창구로서의 역할을 담당하는 중국의 주요 국경 도시이다. 무엇보다도 지리적인 인접성, 직통철도 및 도로 등의 교통 편의성으로 인해 단동지역의 북한인들의 활동은 매우 왕성한 것으로 판단된다. 실제 2004년 북한 용천역 열차 폭발사건 발생시 한국 및 기타 여러 국가로부터 구호품이 단동을 중심으로 북한에 철도와 도로를 통해 배급되었으며, 당시 단동이 한국 언론의 주목을 받기도 한 북한에게 있어서는 매우 중요한 주요 전략 거점이다. 동 지역에

12) 金日군사대학 : 기술정찰과, 프로그램과, 전자계산기과 등 6개과 총 500명으로 구성되어 매년 10~20여명의 사이버전 관련 전문인력 양성(김선호, "북한의 사이버전 능력과 대비책", 『自由』 통권 397호, 성우안보연구소, 2006)

는 이미 십 수개 소의 북한인 직영·합영 한국식당, 수 곳의 합영 호텔, 또한 다수의 직영·합영 상점들이 산재하고 있어 북한인들이 다양한 경제, 정치 및 첩보 활동을 전개하기에 매우 유리한 조건을 제공하고 있다. 특히 최근 들어 동 지역의 북한인들의 진출 및 활동이 급격히 활발해지고 있으며, 이전과 같은 한국인 경계태도와 같은 신중한 접근은 더 이상 목격되지 않고 있으며 오히려 식당 등에서의 합석행위도 자연스럽게 이루어지는 상황이다. 또한 북한 사업가들의 진출이 매우 활발하며, 외환벌이와 함께 식량 수입을 포함한 다양한 소비재 무역에 종사하고 있고, 이들 북한 사업가들은 현지 조선족, 또는 중국인들과 결탁하여 다양한 이권사업을 전개하는 것으로 판단된다. 실제로 단동과 신의주를 연결하는 압록강 철도·도로를 통해 이들 북한 사업가, 정부 관련 인사들이 조달한 막대한 양의 물자가 매일 북한으로 수송되고 있으며, 최근에는 TV, 컴퓨터 등 전자제품과 식량과 같은 소비재의 북한 반입이 급증하고 있는 것으로 목격되었다.

이미 언급한 바와 같이 북한인들의 동 지역 요식, 호텔업 진출이 두드러진바, 독자 진출의 형태보다는 합작형태를 선호하고 있고 그중 중국인 소유의 3성 호텔인 000호텔에서는 요식업소 운영은 물론 1~2개 층을 전세내어 북한인 전용 숙소로 활용하고 있으며, 여타 호텔에서도 유사한 형태의 합영이 진행 중인 것으로 파악된다. 특히 이들 호텔에는 비즈니스센터 내 다양한 전산시설이 운영되며 일부 목격자들을 통해 호텔 객실 내에서도 여러 전산장비가 운영되고 있는 사실이 확인 되었다.

결론적으로 단동지역은 북한이 지리적 이점으로 자국의 첩보활동을 통제하기 용이할 뿐만 아니라 북한의 열악한 통신 인프라를 우회하여 중국으로부터 조달 가능한 상대적으로 우수한 정보통신 장비의 획득 및 운용이 용이하고, 무엇보다 통상적인 경제활동으로 위장이 가능하기 때문에 논리적으로 북한의 대남 사이버전 수행 및 정보네트워크를 통한 첩보·정보수집활동 중요 거점으로서의 매력이 충분한 장소라 사료된다.

2) 북한의 대남 사이버전 수행 현황(실제 사례)

단동 지역을 중심으로한 북한의 대남 사이버전은 북한이 동 지역에 확보한 수 곳의 안전가옥을 중심으로 수행되고 있는 것으로 알려져 있다. 우선 대표적인 장소로서는 중국 조선족 교포가 운영하는 000호텔로서, 얼마전 까지 북한은 동 호텔에 식당·카페 등을 합작형태로 운영 하면서 4층에 별도의 안전가옥을 운영하여 사이버전 수행능력 및 정보네트워크를 통한 첩보·점보 수집활동을 확보·강화하고 있는 것으로 파악된다.

동 거점은 000호텔이 2002년 초기에 개관하면서부터 운영되기 시작했으며, 전산관련 장비는 2003년 말부터 구성되기 시작하여 2004년 중반부터 본격적으로 운용된 것으로 알려져 있다. 실제 거점은 동 호텔 4층에 위치한 출입이 통제된 약 35평 정도 크기의 사무실로 10여 명의 인력이 상주하며 약 10여대의 컴퓨터 세트를 광케이블 네트워크로 연결하여 운영하고 있다. 특히 동 호텔이 ADSL망으로 사용하는 것과는 별개로 별도의 광케이블망을 이용하고 있다는 사실을 주목할만 하며, 북한과의 직접통신채널도 역시 가동되고 있다고 파악되어진다.

동 거점 개설 초기에는 동 호텔에 투숙한 한국인을 포함한 여러 방문객에 대한 통상적인 감시 활동을 전개하였으나, 이후 전산 장비 확충과 함께 다수의 숙련된 전산장비 인력이 투입됨으로서 보다 본격적인 사이버상의 정보수집 및 첩보, 정보활동 전개, 그리고 심리전 활동을 확대해 나가고 있는 것으로 판단된다.

2004년 말 당시 운영되었던 장비로는 10여대의 삼성 데스크탑, 역시 동수의 삼성 CRT(Cathode Ray Tube : 브라운관) 및 LCD(Liquid Crystal Display : 액정표시기) 모니터, 대형 네트워크 프린터 등이며 여타 다수의 네트워크 장비를 보유하고 있는 것으로 파악되어진다. 특히 동 거점의 장비 및 인력은 24시간 운영·유지되어지고 있으며 대형 네트워크 프린터를 통해 지속적으로 출력물을 확보하는 것으로 알려져 있다.

이와는 별도로 2004년 말, 단동지역 개발구에 위치한 4성호텔이 000호텔 건너편에 신축한 오피스텔에 약 80여 평의 대규모 신규 거점을 확보하고 있는 중이며, 동 거점에는 기존의 000호텔 거점과는 비교할 수 없는 수준

의 전산장비와 네트워크가 구축되고 있다는 사실도 확인되고 있다.

3) 북한의 사이버전 수행 능력 평가

1990년대부터 발간된 다수의 보고서에 의하면 북한 지도자의 대망이 “디지털 경제”의 달성임을 지적하고 있다. 그러나 오늘날에 공개된 증거로는 이 목표는 한낱 꿈에 불과한 것으로 볼 수밖에는 없는 게 현실이다. 개발되지 않은 전자 및 컴퓨터 산업 기반구조, 낙후되고 부실한 북한내 통신 기반구조, 지속되는 국가 거시경제 위기, 그리고 전국적 전력난, 폐쇄적이고 경직된 사회, 그리고 내부 국가기관들의 부실화는 북한이 IT 기반의 C4ISR(command, control, communication, computer and Intelligence, Surveillance and Reconnaissance : C4, 정보, 감시 및 정찰)과 사이버전 능력을 지속 개발할 수 있는지에 대한 의문을 제기시키기 충분하다. 그러나 북한 정권의 과대 망상적 구조, 전체주의는 역설적으로 사이버 분야의 집중 및 필요자원·인력 배치를 용이케 하는 구조를 가지게 한다. 특히 최근의 제한적이나마 북한의 개방은 북한이 다수의 외국의 소스로부터 정보 인프라 극대화 및 이에 필연적인 결과물인 북한의 사이버전 능력 강화를 지원해주는 주요 수단으로 부상하고 있다. 무엇보다 불법으로 획득하는 외국기술, 군사중심주의에 의한 인력과 자원의 집중배분으로 북한은 필요시 해킹 및 네트워크 침투를 통해 한국 및 여타 국가들의 IT 네트워크 및 데이터베이스에 위협을 가하는 것이 가능하다. 실제 북한은 관련 기술과 자원이 부족함에도 불구하고 현재 장거리 미사일 및 핵무기 개발 선도국으로 부상한 것과 같은 원리를 북한의 사이버전 수행 능력을 평가하는데 적용해도 무리가 없을 것으로 판단된다.

북한은 산업화에는 뒤졌지만 정보화에는 앞서겠다는 각오로 일찍부터 군사 사이버전 능력의 강화에 큰 관심을 기울여 왔다. 광케이블을 구축해 통신망을 업그레이드하고 각 부처와 기관들의 컴퓨터망 연결 작업을 확대하는 등 북한은 나름대로 정보화 노력에 주력해 왔는데, 이러한 노력으로 북한은 상당한 해킹능력을 갖추게 된 것으로 파악된다. [13)]

제 2 절 우리나라 사이버전 대응 태세

현재 국방부는 전자정부망과는 별도로 국방부, 육·해·공군, 기무사 등이 공동으로 사용하는 국방전용망을 운영하고 있다. 국방망은 현재 다양한 규칙과 지침을 기반으로 운영되고 있으나 아직 안정화 단계를 극복하지 못하고 있는 상황으로 많은 보완이 요구되는 실정이다.

우선 「국방정보통신기반보호지침」은 정보통신기반보호법('01. 1. 26, 법률6383호) 및 동법 시행령에 따라 국방정보체계의 안전한 운용을 목적으로 관련 업무 절차와 기준을 정의하는 것을 목적으로 제정되었다. 국방정보통신기반보호지침의 기본 목표는 국방정보체계의 훼손, 파괴, 마비, 변조, 절취 등의 불법 사용자로부터 보호하며, 국방정보체계에 대한 침입 예방, 탐지, 대응 및 침해사고에 대한 복구와 정당한 사용자의 가용성을 보장하고 편의성 극대화 추구를 목적으로 하고 있으며, 국방정보통신망의 생존성 및 운영의 연속성 극대화와 정보체계 기술의 발전추세에 따른 보호체계의 적시성 확보를 목표로 삼고 있다. 이 지침은 국방정보통신기반보호위원회의 심의를 거쳐 국방 차원의 보호가 필요하다고 인정되는 주요 국방정보체계를 지정, 관리하도록 하고 있으며, 각 군 및 기관의 장에게 소관 분야 주요정보체계에 대한 취약점 분석, 평가수행 및 이를 기반으로 한 보호대책의 수립을 요구하고 있다. 또한 이 지침은 기존 국방 컴퓨터침해사고 긴급대응반 운영지침의 내용을 포함하여 침해 사고 예방 및 대응과 관련된 업무절차 및 활동들을 포함하고 있다. 그러나 이 지침은 국방 정보보호 추진 조직의 변경에 따라 현실성 있는 정보보호담당관 역할 및 기능 등의 개정 소요가 있으며, 각 군 및 국방부의 실태를 고려하여 효율적인 활동을 보장할 수 있는 내용으로서의 조정이 필요하다.

---

13) 국정원은 09. 7. 7 DDos 공격에 따른 공격 배후를 추정하면서 북한의 소행일 수 도 있다는 부분을 조심스럽게 내비쳤다. 만약 북한의 소행이 맞는다면 이는 남한의 사이버안전체계를 시험해 보려는 의도에 따른 것이라는게 전문가들의 분석이다. 이번 공격이 군사정보 또는 국가문서를 빼내가기 위한 것이 아니라 주요 기관의 인터넷 홈페이지를 무력화하는데 중점을 둔 것으로 드러나고 있다는 점이 그런 분석에 무게를 싣는다. 또한 북한은 중국을 경유해 우리군의 전산망 해킹을 시도하고 있다는게 정보당국의 판단이다. 현재 북한은 인민군 총참모부 정찰국 소속의 '기술정찰조'를 통해 대남, 대비 첩보를 수집하고 전산망을 교란하고 있다. 기술정찰조는 군 컴퓨터 전문요원을 양성하는 평양의 지휘자동화대학 졸업생을 위주로하여 100여명으로 구성·활동하고 있다.

그러나 실질적인 사이버보안과 관련된 조치는 이전 2000년 12월 발표된 「컴퓨터침해사고 긴급대응반(Computer Emergency Response Team, CERT) 운영지침」을 통해 그 기반이 마련되어져 있다고 봐야할 것이다. 동 지침은 국방부 합참 및 각 군 본부 등의 긴급대응반 설치 운영 및 긴급대응반의 임무·기능, 침해사고 예방·조치·보고·복구 등과 관련된 운영을 정의하였다. 이 지침은 현재 관련 내용이 국방정보통신기반보호지침에 포함되어 적용되고 있다. 그러나 동 조직과 여타 국방부 내 사이버 안전 및 정보보호 조직과의 연계, 그리고 실전상황에서의 대비 태세 마련에는 크게 부족한 실정이라고 하겠다.

이와 함께 「육군규정 200 : 군사보안규정」(구 : 군사보안업무시행규칙)에는 군사보안업무와 관련한 물리적·관리적 보안, 정보통신보안, 암호자재 운용관리 등의 내용을 포함하고 있으며, 이는 2008년 7월 1일과 2009년 3월 1일 전면개정을 통해 보안업무시행규칙 사용체계변경, 사용자별 비밀문서 관리, 효율적인 보안업무 수행여건 보장, 비현실적 조항 개선, 정보통신 보안대책 강화 등의 내용을 보완하였으나 최신 정보보호 기술 및 해킹, 바이러스 등 사이버전 위협에 대응하기 위한 실무적인 내용은 극히 미흡한 실정이다.

정보보호에 대한 필요성 및 관심이 커지는 상황에서 국방 정보보호 추진을 위한 각 군내 업무 소요가 증가하고 있으며, 이에 따라 현재 각 군 본부에는 중앙전산소에 침해사고긴급대응반(CERT)을 편성, 운영하고 있으나 기술적·전문적 대응을 위한 예산 및 인력자원이 부족한 실정이다.

1. 육군본부

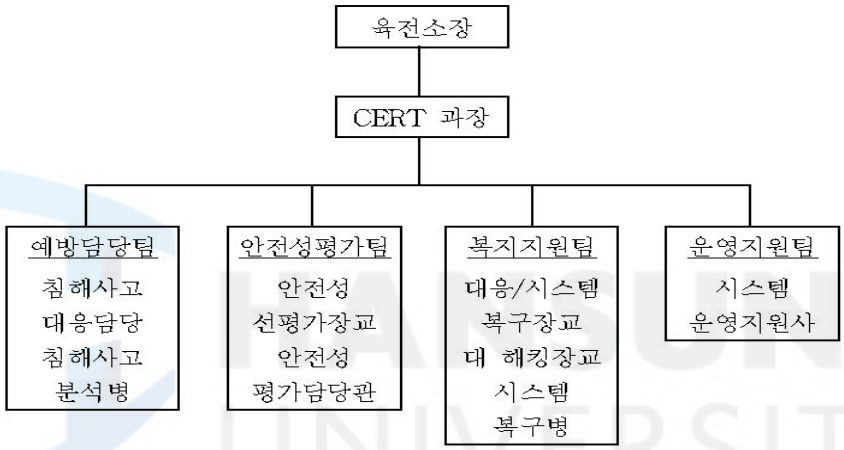
1) 컴퓨터 안정성 평가 및 긴급복구체계 구축 : 네트워크 취약점진단 시스템 운영, 분기별 주장비 취약점 진단/보완지원, 침해사고 긴급복구체계 구축 및 시험, 육군 CERT 컴퓨터 침해사고 관리도구 관리운영
2) 침해사고 탐지 및 분석 : 국방망감시분석시스템 운영, 각종 탐지 및

해킹 로그 분석 지원, 사이버 해킹 체계 연구 및 소요제기

3) 침해사고 긴급대응 : 통합보안관제시스템 운영, 침입차단시스템 운영, 24시간 상담 / 지원체계 유지

5) 침해사고 예방 및 교육 : 군별 CERT 홈페이지 운영, PC용 바이러스 백신 자동갱신 체계 구축 / 운영, 전자우편 바이러스 차단시스템(VirusWall)운영

<표4-2> 육군 CERT팀 조직



자료 : 공성진, "21세기 신 10만 양병", 「2006 국정감사 정책자료집 시리즈 4」, p. 37

2. 국통사

지휘소자동화체계 및 국방 정보통신기반시설에 대한 보호대책을 수립 중에 있으며, 국방 침해사고긴급대응반 및 국방 통합보안관제체계 운영 중

3. 기무사

취약성 분석 및 평가 기술지원 조직 및 인력의 확보를 추진 중에 있으며, 국방 침해사고 긴급대응반의 침해 사고처리 및 사이버 수사업무 수행

4. 국방정보본부

전산보안업무 수행, 전산보안 제도·절차 수립 및 적용업무 수행, 암호장비 소요판단, 제작승인, 시험평가 및 운용에 대한 통제기능 수행

제 5 장 사이버전 대응태세 강화 및 대응체계 구축방안

제 1 절 사이버전 대응태세 강화방안

군사차원의 사이버전은 HARDKILL 및 SOFTKILL 요소를 모두 포함한 전군차원의 통합 사이버전·사이버전 교리의 신속한 정립이 필요하다. 또한 독자적인 사이버전·사이버전 부대의 창립, 공격·방어전략의 수립 및 유기적인 통합방어체계 확보가 절실하며, 특히 사이버 범죄로 위장한 사이버 테러는 사이버전으로 파급될 수 있는 가능성이 농후하기에 평시 대테러 대책 강구가 필요할 것으로 판단된다. 그러나 무엇보다 가장 중요한 것은 사이버전이라 함은 특정한 공간과 시간, 대상을 선정하여 이루어지는 것이 아니라 불특정 다수와 불특정 시간, 공간을 통해 이루어지기 때문에 군내 모든 인원들의 보안의식 강화 및 확대가 절대적으로 필요하다.

현대 그리고 미래전은 정보·사이버전이며 더 이상 전쟁과 사이버전을 분리해서 생각할 수 없고, 정보우세(Information Dominance)는 향후 국가안보 및 국력을 보장해 주는 핵심수단으로 정보보호의 중요성을 인식하고 보다 많은 시간과 자원을 투입하여 해당분야 세계 최고 수준의 기술력과 역량의 확보를 지향해야 할 것이다.

이와 함께 포괄적인 국가 정보통신 사이버네트워크를 종합적으로 관리할 수 있는 체계를 구축·운영하고, 국가 사이버 위협 조기예·경보체계의 개발 및 정보우세(Info- rmation Dominance)를 위한 다양한 공세적, 수세적 정보·사이버전 인력과 조직을 정책적으로 양성하는 것은 매우 시급한 과제이다.

또한 앞서 강조한 것처럼 군내에서 진행되고 있는 다양한 방법의 보안의식 고취교육이 현실적으로 실시되어야 한다. 많은 수의 컴퓨터가 보급되고 다양한 저장매체[14]가 사용되면서 과거와 달리 군 관련 정보와 비밀의

외부유출 및 노출이 더욱더 용이해졌기 때문이다. 이를 예방하기 위해서는 현재 실시되는 각종 보안강화 노력이 강력해지고 치밀해 져야한다.

이로서 사이버전·사이버전 대응 다양한 고유장비 및 기법, 인력의 확보와 사이버테러 및 사이버범죄 대응 첨단수사대처 능력의 강화를 통한 유관분야 세계 선도국 위치 및 미래정보사회 국제적 지배력을 확보하고, 군사정보·사이버전 및 민간 사이버테러·범죄에 포괄 대응할 수 있는 국가사이버안전체계 구축 및 관련장비, 인력, 조직, 기술을 선도해야 한다.

그리고 무엇보다 군과 정부기관의 조직문화 및 사고체계의 변화를 통해 광속의 정보·사이버전 환경에서 적극적, 공세적, 선제적 선택을 가능케 유도해야 미래의 정보 주도권과 정보 지배력을 확보하여 국가와 국민의 안위를 보장할 수 있을 것이다. [15]

14) 현재 군에서는 '간부 1인당 1대의 컴퓨터'라는 기준에 따라 보급이 가속화 되고 있으며, 90% 이상의 부대가 만족스런 사양의 컴퓨터를 사용하고 있다. 또한 04년도 이후 USB를 활용한 각종 문서의 저장이 활성화 되면서 보안을 위한 노력이 급격히 증대되고 있다.

15) 2004년 2월 20일에 국가사이버안전센터가 개소했으며, 2005년 1월 31일에 대통령 훈령 제141호에 의해 국가 사이버 안전관리 규정이 제정, 시행되었다.

제 2 절 사이버전 대응체계 구축방안

1. 보안의식 고취 및 전산보안교육 강화, 감시체계 강화

2006년 실시한 현역간부들의 사이버전 인식 조사분석에 따르면 장차 사이버전을 수행하고 지휘 감독해야할 군내 현역 장교들의 상당수가 사이버전 수행을 위한 우리군의 인프라 구축이 미흡하다고 인식하고 있었으며, 군에서 실시하는 정보화 교육 등의 교육제도 또한 많은 부분 개선이 필요한 것으로 인식하고 있었다.[16)]

앞서 언급한 것처럼 급속한 컴퓨터의 보급 및 다양한 저장매체의 개발 및 군내 반입 등에 비해 개인의 보안의식은 오히려 축소되어 각종 보안위규·반 사례가 빈번히 발생하고 있다. 특히 인터넷과 국방망의 혼용사용, 대용량 USB를 활용한 음성비문 보관, 노트북 보급 확대에 따른 노트북내 군사자료 음성보관, PDA기능 핸드폰내 각종 군사자료 보관, 비인가 CD를 통한 군내 바이러스 유포, 국방망내 불법 게시판 개설 등 위반사례의 형태와 방법이 다양해지고 있다.

더욱이 향후에는 해킹기술 발달로 전산보안의 중요성이 더욱 증가하는 반면 이에 대한 대책과 중장기 계획에 따른 첨단 보안대책의 조기 마련은 더욱더 제한될 것으로 보인다. 결국 현 상황에서 단시간에 최상의 효과를 얻기 위해서는 개인의 의식개혁과 이에 따른 감시체계 강화가 절실하다 하겠다.

1) 보안의식 고취 및 전산보안 교육강화

주기적인 정보통신 및 전산분야 보안의식 고취교육을 통한 개인별 위기의식 확대 및 제대별 평가를 통한 차후 개선소요 도출이 필요하다. 이를위해 우선 제대별 보안교육 및 정보화 교육에 대한 심도있는 교육내용 마련

16) 최해필, “사이버 시대 군 사이버 전력의 강화방안 연구”, 건양대학교, 2006, p93~109

과 체계적인 교육이 필요하다.

<표5-1> 제대별 보안 및 정보화교육 방안

구 분	대 상 / 내 용	
	병	간 부
중·소대	월 1회 정보통신윤리 / 사고사례교육(1H)	월 1회 정보통신윤리 / 전산보안 교육(1H), 평가
대 대	분기 1회 정보통신윤리 / 사고사례교육(2H), 평가	분기 1회 정보통신윤리 / 전산보안 교육(2H), 평가
사단이상	반기 1회 정보통신윤리 / 사고사례교육(2H), 보안평가 경연대회	반기 1회 정보통신윤리 / 전산보안 교육(2H), 평가

※ 평가주관 : 차상급부대 보안담당부서 및 담당관

2) 감시체계 강화

중장기적 계획에 따라 다양한 첨단 보안대책 마련이 시급하다. 현재 1일 기준 약 100건에 이르는 바이러스가 국방망을 통해 유포되고 있을 정도로 군내 비인가 매체의 유입이 증가했으며, 이러한 바이러스는 출타복귀 장병에 의해 CD, 대용량 USB 및 하드디스크, PDA, MP3 플레이어 등의 형태로 반입된 각종 자료에 의해 유포되고 있다. 그러나 저장매체 반입근절을 위해 모든 복귀 장병이나 군내 출입자를 확인하기에는 현실적인 제약이 많다. 더욱이 최근의 저장 매체들이 소형화 또는 형태 변형화[17]되고 있는 현실을 볼 때 단순 육안식별로는 한계에 도달한 것이 사실이다. 매년 군에서 유출되는 다양한 형태의 군사자료와 정보의 누출에 따른 금전적, 전략적인 손실을 고려한다면, 첨단 보안대책(출입자 감시 시스템) 마련이 시기상조는 아닐 것으로 판단된다.

2. 사이버전 전문인력 양성방안

미래 사이버전 대비를 위해서는 실제 적국의 사이버공격에 방어와 역공격을 수행할 수 있는 전문 부대의 창설이 시급하다. 미국과 중국 등 강대국들은 이미 1990년대 중반부터 사이버전 수행부대를 창설하여 운용해 오

17) 저장매체의 소형화 및 형태의 변형 : micro SD 카드, 펜슬형·시계형 USB 등으로 소형 및 변형화 되고 있으며, 저장매체의 급격한 가격하락과 용량의 증가로 인해 문제점은 더욱더 심각해 지고 있다.

고 있으며, 2000년대 중반 북한과 일본도 사이버전 부대를 창설하였다. 우리군은 사이버공격에 방어 기능을 가진 정보보호팀들이 각 군 전산소에 배치되어 있으나 실제 사이버전을 수행하기에는 역부족이다.

<표5-2> 사이버공격에 대비한 조직 및 전문인력 확보현황

구 분	인 원	편 성
계	210명	
정책 / 연구요원	34명	국방부 정보보호담당, 합참 / 각 군 정보보호과, 연구원(KIDA, ADD)
컴퓨터침해사고 대응팀 (CERT)	152명	국방부, 각 군 본부 및 군단급이상 설치
국방정보전 대응 센터	24명	국가사이버테러대응체계 구축의 일환으로 국방분야 사이버 침해사고 대응

자료 : 공성진, "21세기 신 10만 양병", 「2006 국정감사 정책자료집 시리즈 4」, p. 42

현재 우리나라의 사이버전 부대 창설의 장애요인은 기본적으로 아래와 같다.

- 군내 사이버전 전문인력 부재
- 군내 교육기관 및 교육인력 부재
- 정부기관, 군 등의 고위정책결정권자들의 인식 부족
  (사이버방호사령부[18] 예산삭감 검토 : 국회예산정책처, 09년 11월 4일)
- 잦은 보직 이동으로 인한 전문 지휘관급 요원 양성 불가능

사이버전을 대비하기 위해서는 군 자체는 물론 국가주요 정보통신 기반시설이 1차적인 보호대상이 된다. 따라서, 위와 같은 장애 요인을 해결하고 사이버전을 수행할 수 있는 전문인력을 양성하기 위해서는 기존의 병역특례 제도와 공익근무요원제도 등을 활용할 수 있다고 판단된다.

18) 사이버방호사령부 : 국방개혁 기본개혁에 따라 2012년 추진예정이었으나 09년 7월 발생한 DDos 공격후 사이버전 위협 조기대비를 명분으로 창설계획을 2년 앞당겼다(09. 8). 편성은 기무사 정보전대응센터 80여 명, 사이버 보안인력 100여 명, 육·해·공군 보안인력 240여 명 등 총 420명 규모.

1) 사이버전 부대요원 양성을 위한 공익근무요원제도 도입

입영대상자들을 대상으로 사이버전요원 시험을 통하여 우수자들에게 사이버전 훈련기간(2~3개월) 수료 후 정부주요정보통신기반시설을 보유한 기관에 대체 복무(의무복무 22개월)시킴으로서 각 주요기관의 정보보호담당관 역할을 담당케 할 수 있다(국가 주요기관에 정보보호담당관제도가 도입되어 있으나 예산 및 인력부족으로 인해 훈련이 안된 전산요원이 정보보호담당관을 겸임하고 있어 제 역할을 담당하지 못하고 있음).

2) 병역특례제도를 활용한 사이버전 전문인력 양성

사이버전 고급 전문인력양성에는 상당한 기간이 필요하다. 일반적으로 컴퓨터공학이나 정보통신을 전공한 자는 단기간 교육 후, 사이버전에 투입할 수 있다고 생각하기 쉬우나 사이버전 수행을 위한 공격 및 방어 기술 습득을 위해서는 상당기간이 소요된다. 또한 이를 담당할 수 있는 인력은 사이버상에서 공격과 방어 업무를 수행해야 하기 때문에 상당히 고도로 훈련된 특수집단을 양성해야 한다. 우수한 인재를 양성하기 위해 수도권 대학에 사이버전 학과를 설치하고 이들 중 3, 4학년을 대상으로 우수인력을 선발하여 군복무를 면제해 주는 조건으로 재학기간 중 군 관련기관에 대한 보안관제요원, 사이버전 무기개발 연구 등과 같은 업무를 수행하게 하는 방안도 고려할 만하다. 또한 경력에 대한 인정을 통해 2010년 창설되는 '사이버방호사령부' 요원지원 자격부여등도 가능할 것으로 생각된다.

3) 사이버전 지휘관급 인력 양성

수도권 대학에 사이버전학과 졸업자 혹은 육군사관학교·3사관학교내 관련학과 졸업자 중 엄격한 선발기준과 시험을 통해 우수자를 선발하고 이들을 장교로 임관시켜 요원으로 활용하여야 한다. 물론 임관이후 짧게는 5~6개월, 길게는 1년 이상의 기간을 통해 사이버전 수행능력을 훈련받도록 해야 한다.

사이버전을 담당할 전문인력은 컴퓨터공학이나 유사 관련학을 전공한다고 해서 할 수 있는 분야는 아니다. 따라서 이를 담당할 수 있는 고급인력 양성을 위해 국가적 차원에서 수도권대학과 사관학교에서 관련 전문학과를 설치 운영해야 한다. 향후 이를 전국적으로 확대하여 대대적인 사이버전전문인력을 양성해야 함은 물론이다. 그동안 전문가들 사이에서 주장된

10만 사이버전사 양병설을 현실적인 차원에서 준비해야할 시기가 다가왔고, 이제는 더 이상 늦출 수 없는 시기이다. 가까운 중국의 경우, 사이버전 지원그룹, 역량그룹 등 이미 10만을 넘어서는 사이버전사를 보유하고 있다. 따라서, 주변국들과의 사이버전 우위를 점하기 위해서는 전문인력 양성은 필수적인 사항이라 하겠다.

4) 군차원에서의 사이버전사 양성을 위한 전문교육기관 설립

우리나라는 현재도 수만 명의 정보기술 인력이 부족하고, 앞으로도 이러한 현상은 군이 필요로 하는 전문인력을 사회에서 쉽게 획득하기 어렵게 만든다. 앞서 언급한바 있는 수도권 대학 내 전문학과 설치 운영시 군복무기간내 인력획득은 가능하나 군에서 필요로 하는 종류의 인력획득과 인력부족현상은 지속되리라 판단된다. 그러므로 사이버전사 양성을 위한 일부 핵심 전문요원을 제외하고는 대부분의 소요 인력확보를 위해서는 종합행정학교나 또는 정보학교 등에 이스라엘의 '탈피오트'[19]와 같은 사이버 전사 전문양성과정을 설치 운용해야 할 것으로 생각된다. 이렇게 함으로써 산업시대적인 군 구조에서 탈피, 점진적으로 미래지향적인 기술군 구조로 자연스럽게 변모시켜 나갈 수 있는 효과도 동시에 얻을 수 있을 것이다.

19) 탈피오트 : 이스라엘에서는 매년 전국 각지에서 컴퓨터, 과학 등에 재능이 뛰어난 고교 졸업생 중 약 30명을 선발하여 '탈피오트'라는 특별훈련과정에 투입 및 우수한 정보기술 인력을 배출중.

제 6 장 결 론

사이버분야 선진국이자 동시에 사이버 안전 취약국이기도 한 한국으로서는 향후 중장기 국가사이버안전 및 외부로 부터의 사이버전 도발 대응태세 확보, 사이버테러 및 범죄로부터의 국익과 국민을 보호해야하는 중요한 과제를 안고 있다. 특히 지정학적인 문제와 함께 현실적인 경쟁관계를 두고 볼 때 향후 한국과 갈등관계에 놓일 수 있는 러시아, 중국, 그리고 북한으로부터의 잠재적인 사이버 위협은 매우 심각한 사안이라 아니할 수 없다.

따라서 주변 강대국들의 사이버전 전략과 정보안보 강화전략, 그리고 그들의 사이버 테러 및 범죄에 대한 대응 및 지원활동에 대해 정확한 인식을 가지고 향후 한국의 대응방안을 고찰할 필요가 있다. 무엇보다 우리도 이제 나름대로 우리의 여건과 상황에 걸맞은 독자적인 사이버전 전략과 사이버 안보 강화전략을 마련할 필요성이 있다는 것이다. 이를 위해 무엇보다 우선적으로 독자적인 전략의 수립과 군 장병들의 확고한 정보보호의식 확산 및 이를위한 교육방안이 필요하다.

현재 각 군의 기초보수 과정에서 극히 작은시간동안 진행되는 정보보호의식화 교육이 강화되어야 하며, 제대별 정기적인 보안교육이 진행되어야 한다. 이와함께 함께 2010년 1월 1일 창설하겠다고 계획되어 있는 '사이버방호사령부'의 정상적인 가동이 시급하다고 판단된다. 물론 '사이버방호사령부'의 창설 및 운용을 위한 전문인력 양성이 우선되어야 하는 것은 당연하다. 고급전문인력 양성을 위한 노력과 전문인력에 대한 병역특례제도 및 공익요원제도 도입, 전문교육기관의 설립등도 시급하다. 아울러 기존의 사이버테러 대응체계, 사이버범죄 방지대책과 조직의 확대 개편 및 인력 충원을 통해 현재의 수동적이며 방어적인 정보안보전략의 한계를 극복하고, 향후 범세계적인 정보주도권을 확보하는 노력에 집중해야 할 것이다.

본 연구가 최근 발생되고 있는 정보시스템 침해사고를 비롯한 다양한 정보화 역기능 현상들 및 사이버전을 대비하는 인접국가들의 대응책을 분석하여 우리군의 대응전략을 초보적인 단계로 제시하였기에 만족할 만한 연구결과를 도출하는데 부족한 점이 많이 있다는 것을 자인하면서 향후 지속적인 연구를 통해 사이버전에 대한 전반적인 연구와 그 대책이 마련되는 초석이 되었으면 하는 바람이다.

【참고문헌】

1. 국내문헌

1) 단행본

국가정보원, 「국가정보보호백서」, 국가정보원, 2003

국방대학원, 「미국의 안보정책결정과정」, 안보총서39, 국방대학원, 1984

국방부, 「사이버전」, 교육회장 00-3-3, 국방부, 2000

권영근, 「미래전과 군사혁신」, 연경문화사, 1999

김선호, “북한의 사이버전 능력과 대비책”, 『自由』통권 397호, 성우안보연구소, 2006

김철환 외, 「전쟁 그리고 무기의 발달」, 양서각, 1997

노병천, 「도해손자병법」, 가나문화사, 1991

던닝(James F. Dunning), 「미래의 전장과 디지털 전사」, 국방대학교, 2000

앨빈 토플러, 「전쟁과 반전쟁」, 이규행 역, 한국경제신문사, 1994

이필중, 「한국의 군사전력과 군사력 건설방향」, 국방대학원, 1998

2) 논문 및 기타간행물

강진국, “신 정보전이 국가안보와 전쟁수행에 미치는 영향 연구 : 미·중의 정보전 수행능력 비교/분석을 중심으로”, 국방대학교, 2001

권문택, “국방정보화 전문인력 양성 및 확보방안 연구”, 한국경영정보학회, 2001

권창률, “전쟁사례분석을 통한 미래 정보전 대비 방향”, 국방대학교, 2001

김행복, “소련-아프가니스탄전쟁의 역사와 교훈”, 군사 제44호, 군사편찬연구소, 2001

김현철, “미래의 전쟁양상에 관한 연구”, 한남대학교, 2006

남길현, “군 정보보호의식 확산을 위한 장병 교육방안 연구”, 교수논총

박권식, “정보보호체계 구현 방안”, 육군교육사령부, 2004

박진영, “군 정보통신망 통합방안”, 성균관대학교, 2007
백용기, “사이버 전쟁 대비 정보화 군 건설”, 『국방저널』, 국방부, 2000
송기섭, “사이버 전쟁에 대한 대응”, 『합참』, 국방부, 2003
안서기 외, “군 사이버 공보 운용”, 육군교육사령부
장재규, “사이버전의 개념과 체제구축에 관한 연구”, 국방대학교, 2002
조영갑, “이라크전쟁이한반도에미치는영향”,군사제50호,국방대학교,2003
한국사이버테러정보전학회, “사이버전 전문인력 양성체계”, 『제4회 사이버테러 정보전 컨퍼런스 2003』, 한국사이버 테러정보전학회, 2003
합동참모대학, “사이버전에 관한 연구”, 국방대학교, 2000
허평환, “한국군 억제전략과 군사력 건설방향”, 동국대학교, 2006

3) 인터넷

http://kr.encycl.yahoo.com
http://www.ffstek.com
http://news.kbs.co.kr
http://www.sejong.org/
http://eyenews.hankooki.com
기사, “軍 인터넷망이 국가기밀 유출창구라니”,매일경제[사설], 2009. 10. 18
기사 “軍 사이버사령부 ‘기무사 직할’논란”, 문화일보, 2009. 10. 05
기사, “국회예산정책처, ‘사이버방호사령부’예산 전액삭감 주문”,오마이뉴스, 2009. 11. 04

ABSTRACT

The study on military operation due to battle space expansion

-Focused on counter cyber warfare operation-

Lee, Han Eok
Major in Division of National Defence Management
Dept. of Business Administration
Graduate School of Business Administration
Hansung University

In the 20th century, the development of high-technology has been pronouncing. The developed nations have achieved military renovation and development of weapon systems through state-of-the-art technology. Among these, advancement of information and communication technology has changed the concept of future warfare. The wars in the past used guns and swords in a tangible space like the ground, see and sky. But a space where warfare occurs now is expanded not only a material space but also into a Cyber space. The definition of cyber space is virtual world where computer and internet creates. Cyber space is intangible but it is rapidly expanding. and it has great influence on individuals and society.

But cyber space also have brought malfunction of information. There are some examples like spreading of false information in the Internet, junk mails, several trials to hook military secrets by North Korea in 2008, collecting military-related datum indiscriminately by foreign expert hacker organization in January 2009, DDos - Distributed Denial of Service attack - targeting at national agency and major portal sites in Korea like Naver and Daum in July 2009 etc. These fact show the carelessness of cyber countermeasures in our society. Particularly, the types of cyber warfare are not well known, the analysis of other nation's reaction status is not sufficient. There is no specified cyber warfare strategies on national level. Finally, management of human resources are insufficient now.

Of course there is Headquater of Cyber Warfare Defense : a tentative name that will be founded as a subordinate of DSC - Defense Security Command - It is just organized because of urgency of the case. There is no specification ever known.

The warfare in cyber space can make enemy disarmed without any victims. So importance of cyber space is increasing.

Thus, the purpose of this study is to establish Korea's preparation plan of cyber warfare in the future on the basis of the types of cyber warfare which has occurred so far and the analysis of other nation's preparation-readiness.