情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

정보전 개념

권 태 환*, 황 호 상*

요 약

지금까지의 전쟁은 주로 국가 및 군사 분야에 한정하는 경향이 있어왔으나 정보전은 기업은 물론이고 일반 개인에게 까지 직접 관련이 되고 있다. 그러나 아직 까지 정보전에 대한 명확한 개념이 정립되지 않은 상태에서 정보전과 관련된 용어들이 난무하고 있어 일반인은 말할 것도 없고 정책 입안자나 군사 기획가마저도 많은 혼란을 겪고 있다. 따라서 본 고에서는 이러한 정보전에 대한 명확한 이해를 도모할 목적으로 정보전이 출현된 배경, 정보전의 정의 및 분류, 정보전의 특징 등을 살펴보고 몇 가지 쟁점들에 대해 논한다.

Ⅰ. 서 론

오늘날 정보전이란 주제는 군에서뿐만 아니라 일반사회에 까지 많은 관심의 대상이 되고 있다. 정보기술의 폭발적인 발전에 의해 정보사회로 급격히 진전되면서 전쟁의 성격과 수행방법이 크게 변화되고 미래의 국제 안보환경이 근본적으로 영향을 받게 될 것이다. 즉, 분쟁의 성격 및 군사작전의 수행과 관련하여 정보기술은 새로운 전략지정학적 환경에 지대한 영향을 미치고 있다. 과거의 전쟁은 지리적 우세를 확보하기 위해 수행되었으며 그 결과에 따라 국력이 좌우되었으나, 정보전에서는 정보 우위를 점령하고 적의 정보를 탈취하는 능력에 의해 승패가 좌우될 것이다. 지금까지의 전쟁은 주로 국가 및 군사 분야에 한정하는 경향이 있어왔으나 정보전은 기업은 물론이고 일반 개인에게까지 직접 관련이 되고 있다. 그러나 아직 까지 정보전에 대한 명확한 개념이 정립되지 않은 상태에서 정보전과 관련된 용어들이 난무하고 있어 일반인은 말할 것도 없고 정책 입안자나 군사 기획가마저도 많은 혼란을 겪고 있다. 따라서 본 고에서는 이러한 정보전에 대한 명확한 이해를 도모할 목적으로 정보전이 출현된 배경, 정보전의 정의 및 분류, 정보전의 특징 등을 살펴보고 몇 가지 쟁점들에 대해 논하고자 한다.

Ⅱ. 정보전의 출현 배경

지난 반세기 동안 통신 및 컴퓨터 기술의 급속한 발전에 힘입어 지금의 선진국은 후기산업시대, 미래학자 앨빈 토플러의 제3의 물결시대로 일컬어지는 고도의 정보사회이다. 정보사회의 개념은 주로 학자들간에 다양한 접근을 통하여 지속적으로 다루어지고 있지만 산업사회에서 자본주의 체제가 가장 적합한 체제임이 입증된 것은 산업사회가 저물어가는 80년대 말이었듯이 계속 진화 중인 정보사회의 참 모습은 그 변화의 속도가 더욱 빨라지고 있는 만큼 아직 단정할 수 없다.

한편, 인류사회의 발전과 더불어 전쟁의 양상도 변화되었다. 오늘날 정보기술의 혁명적 발전은 전쟁의 속성을 변화시키고 있다. 앨빈 토플러는 인류사회의 발전에 따른 전쟁양상의 변화를 제1물결전쟁, 제2물결전쟁, 제3물결전쟁으로 설명하였는데, 농업사회와 산업사회에서의 전쟁은 병력, 화력과 기동중심의 전쟁으로서 소모전, 대량살상 및 파괴의 성격을 가지고 있었다. 그러나 정보사회에서의 전쟁은 정보와 지식이 중심이 되고, 첨단과학기술이 바탕이 된 정밀무기와 정보자산으로써 파괴와 살상을 최소화하면서 승리를 추구하는 방향으로 전개된다.(〔표 1〕 참조)

* 국방대학교 ({thkwon, afhosang}@kndu.ac.kr)

〔표 1〕 시대별 전쟁양상 변화

구분	농업 시대	산업 시대	정보 시대
전쟁 수행 주체	무사계급, 용병 시민군	직업 군인, 시민	정보 전사
부의 원천	토지	물질	정보
전쟁의 특징	대리전	대규모 군대 다수의 사상자	정보 공격 소수의 사상자
전쟁 수단	칼, 창, 활 등	핵, 화학 대량파괴 무기 등 하드 킬	중요 정보 삭제 등 소프트 킬
지휘구조	계층 구조	계층 구조	수평 구조
정보 기반 전쟁	O	O	O
정보기술을 전쟁에 사용	X	O	O
정보에 대한 전쟁	X	X	O

현대전에 있어서 군사과학기술 및 무기체계의 발달로 속도, 사거리, 치명도의 증가와 전장의 광역화로 위협요소가 증가됨에 따라 상황의 판단과 지휘결심을 더욱 어렵게 하고 있으며 위기관리를 위한 정보의 요구를 증대시키고 있다. 미 합참의장 John Shalikashvili 대장이 말한 바와 같이 "정보 기반 기술의 폭발적인 진보는 모든 단계, 군사작전의 영역, 그리고 전쟁의 모든 수준을 통해 전투에 중요한 영향을 준다."[1)]

한편, 미 국방대학교의 퀄 교수는 정보전의 배경으로 (1)사이버 공간의 확장, (2)디지털 통합(convergence), (3)세계적인 디지털 전방위 연결, (4)컴퓨터에 의한 기반체계 통제를 들고 있다.[2)] 첫 번째 사이버공간의 확장은 사회가 점차 정보에 의존하게 됨에 따라 전자적 디지털 기술의 결합된 효과가 크게 증폭되기 때문에 정보가 작전환경을 형성하고 사이버 공간은 그 물리적 요소가 되었다. "사이버 공간이란 전자기적 스펙트럼을 통하여 효과를 미치는 컴퓨터네트워크, 원격통신시스템 및 기타 장치 등 전자시스템이 서로 연결되고 상호 작용하는 장소를 말한다." 사이버 환경은 19세기에 전신이 발명되면서 처음 출현되었는데 20세기에 들어와서 해저전신, 라디오, TV, 극초단파 중계, 통신위성을 활용할 수 있을 정도의 기술적인 진보를 이룩하였다. 우리는 정보를 저장, 처리, 전송할 수 있는 정보의 양을 과거에는 상상할 수 없을 수준으로까지 증가시키고, 군 및 사회가 이러한 기술의 이용법을 배우기 시작하여 사이버 공간이 전면적인 환경으로 등장하게 된 것은 20세기 후반의 25년 정도이다. 사이버 공간은 2가지 추가적인 발전사항으로 인해 새로운 전망을 만들어내고 있다.

하나는 거의 모든 종류의 정보를 2진법의 수치로 전환할 수 있는 능력이 점차 신장되어 이른바 디지털 통합을 달성하였으며, 다른 하나는 세계적인 전방위 연결이라고 부를 정도로 세계적인 원격통신 매체가 인터넷으로 점차 연결되고 있다는 점이다. 이러한 발전사항들은 명확하게 서로 구별됨과 동시에 상호의존적이다. 20세기 중반까지 통신기술의 진보는 선형적이었으나 마이크로 칩의 발명은 하나의 전환점이 되었다. 이후 정보를 저장, 처리, 전송하는 능력의 진보가 디지털 통합에 의하여 가속을 받아 기하급수적으로 이루어지고 있기 때문이다. 이러한 발전의 특징은 2가지인데 하나는 정보처리/전송의 속도이며, 하나는 정보의 양이다. 컴퓨터에 의하여 향상되고 통제되는 원격통신시스템의 이러한 특성들이 서로 결합되자 전자적 디지털 세계가 점차 인터넷화되고 전방위 연결이 이루어졌다(지구촌은 망으로 연결되었다). 오늘날 정치, 경제의 활력소인 디지털 정보를 매일 전달함에 따라 전 세계적인 연결은 확대되고 있으며 사회는 점차 이러한 환경에 대한 의존성이 증가하게 되었다. 마지막으로 영향을 미치는 사항은 선진사회가 핵심기반체계의 통제 및 운영을 위하여 컴퓨터화된 네트워크에 점점 더 의존

1) 합참, 정보인증부(J6K)와 정보전 특수기술작전부(J38) Pam, 정보전 - 평화를 위한 전략..... (Washington, DC: GPO, 1996)
2) Kuehl, Daniel"정보작전, 정보전 및 메타네트워크,"공군대학 국제심포지엄 프로시딩 2000, pp. 98-103.

하고 있다는 사실이다. 우리가 경제, 사회, 정치 및 심지어는 군사력이 의존하는 기반체계를 통제하는 이러한 시스템을 점점 더 신뢰할수록 이점과 함께 취약성도 증가한다. "사용은 의존을 야기하고 의존은 취약성을 만들어 낸다."[3] 에너지의 공급, 수송수단의 관리, 디지털 재화의 이전, 혹은 전체 사회구조를 지원하는 시스템의 운영 등 어떤 분야가 되었든 간에 현대사회에서 거의 모든 분야의 이면을 들여다보면 인터넷화되고 상호 연결된 컴퓨터 시스템을 발견하게 된다. 이러한 정보기술의 발달은 엄청난 기회를 제공하여 정보사회 발전의 원동력이 되고 있지만 또한 취약성을 증가시키고 있다. 지난날 동력기술이 산업사회를 탄생시키고 기동력 중심의 타격전을 잉태 시켰듯이 새로운 정보기술이 정보사회를 탄생시키고 정보전이라는 새로운 전쟁양상을 출현시키고 있는 것이다.

Ⅲ. 정보전이란 무엇인가?

미국은 1970년대부터 정보전의 개념과 기술에 대하여 연구하였으나, 1990년대 미국이 지휘통제전에 대한 개념을 발표할 때까지는 밖으로 잘 알려지지 않았다. 정보전이라는 용어는 1976년 당시 미 국방부 과제를 연구하던 토마스 로나(Thomas Rona) 박사가 '초토화전에서 정보전으로'[4]라는 글에서 최초로 사용한 것으로 인정되고 있다.

정보전을 한 마디로 표현하기는 지극히 어려운 일이다. 미 공군은 "정보 그자체가 무기요 표적인 전쟁"이라고 표현하고 있으며, 조지 스테인은 "정보전은 본질상 사고와 인식에 관한 것이며, 인간과 인간이 내리는 의사결정에 관한 것"이라고 주장하고 있다. 나아가 "넓은 의미에서 정보전이란 국가목표 달성을 위해 정보를 사용하는 것" 이라고 생각하였다. 정보전이란 용어를 최초로 만든 토마스 로나는 "정보전은 의사결정체계에서의 싸움"으로 묘사하였다. 이 경천동지할 개념은 본래는 기술적 접근이었다. 어떤 면에서 보면 전투란 항상 의사결정체계 간의 투쟁이었다. 앨빈 토플러는 넓은 의미에서 '새로운 형태의 전쟁'이라고 묘사하였다. 그들의 개념과 더 최근의 많은 논자들의 주장은 "정보전은 전쟁, 전투, 그리고 분쟁에 대하여 생각하는 방식이다." 그것은 군사력을 적용하는 다른 방식이다. 정보전의 비결 - 약속 또는 징후 - 의 일부는 정보전은 넓게는 전통적인 군사력을 사용할 필요성을 제거하기 위하여 고안된 국가정책의 한 부분으로 적용될 수 있다는 점이다. 무기는 보이지 않으나 그 결과는 확실히 보이는 외교의 경계를 넘어선 어떤 의미에서는 정치적 전쟁이다. 이것은 탄환의 연기를 남기지도, 어떤 흔적도 남기지 않는 새로운 종류의 무기이다. 그것은 국가의 총수가 군사력을 개입시키거나, 또는 시키지 않고도 수행할 수 있는 무기이고 전투이다.[5]

미 국방부가 1996년 정보작전과 정보전에 대한 공식적인 정의를 내렸음에도 불구하고 미군 내에서도 많은 사람들이 서로 다른 생각을 가지고 있는 것 같다. 정보전 스펙트럼은 적의 인지를 조작하여 싸우지 않고도 이길 수 있다는 전략적 정보전에서부터, 전장을 투명하게 파악하여 클라우제비치의 '전장의 안개'을 걷어낼 수 있다는 전술적 정보전에까지 다양하다.

또한 민간분야에서는 "사이버공간에서의 정보원의 가치에 대한 득실활동"으로 표현하고 있으며 그 호칭도 사이버전, 사이버테러, 해커전과 같이 다양하다. 이와 같이 정보가 곧 재산이요, 힘인 정보사회를 살아가는 많은 사회구성 집단들은 집단의 이해관계에 따라 자기 나름대로의 정보전을 정의하고 준비해 나가는 것은 지극히 당연하다고 할 수 있다. 사회집단 전체가 동의하는 공통의 정보전의 정의는 어쩌면 존재하지 않을 수도 있다.

1. 정보(Information)

정보전을 정의하기 전에 정보전의 근본이 되는 정보에 대한 명확한 인식이 필요하다. 전통적인 군사작전에서 정보는 군사정보(intelligence)[6]로서 적에 관한 사항, 지형에 관한 사항, 작전지역 기상을 대상으로 하였다. 그러나 정보혁명의 영향으로 작전의 템포는 엄청나게 빨라졌으며 신속한 의사결정을 위하여 적에 관한 사항 못지않게 아군에 관한 사항 역시 중요한 요소가 되었다. 따라서 정보전에서 사용하는 정보(information)라는 개념은 과거와 달

3) 미 합참, CJCSI 6510.1"방어적 정보전 적용", 1996. 5
4) 황호상 역, "정보전, 사이버전, 네트전", 2001, 합참대학, pp.5-8
5) Dearth, Douglas H. and Goodden, R. Thomas "사이버전 후기", 「사이버전」, AFCEA, 1996
6) 이 글에서는 information과 구별을 위하여 intelligence를 군사정보라고 표기한다.

리 적군에 대한 군사정보(intelligence)와 아군에 관한 사항, 작전환경에 관한 모든 자료를 아우르는 확장된 개념으로 보아야 한다.

군사정보의 관점에서 보면 분석되지 않은 원시자료는 첩보(information)이며, 정리되고 분석된 자료는 정보(intelligence)라고 호칭하고 있다. 미 국방용어사전[7]에 따르면 "정보(intelligence)는 (1) 외국과 외국지역에 관한 가용한 정보(information)를 수집, 처리, 융합, 분석, 평가, 해석한 결과로 만들어진 산출물, (2) 관측, 조사, 분석, 이해를 통하여 산출된 적(adversary)에 관한 정보(information)와 지식(knowledge)"이라고 정의하고 있다. 군사정보분야에서는 여전히 첩보(information)와 정보(intelligence)라는 용어를 사용하고 있다.

이와 달리 정보전에서는 정보(information)는 군사정보(intelligence)보다 확장된 개념으로 사용되고 있다. 미 국방군사용어집은 정보를 (1) 어떤 매체 또는 형태이든 표현된 사실(facts), 데이터, 지시(instructions), (2) 표현에서 사용되는 알려진 관례에 따라 인간이 데이터에 부여한 의미[8]의 두 가지로 정의하고 있다. 미 공군은 정보는 첫째 '모든 종류의 처리되지 않은 데이터'로 설명하고 있다. 처리되지 않은 데이터의 사례로는 정보체계 내에서 움직이는 전자 비트/바이트(bits/bytes)에서부터 우리를 둘러싸고 있는 세계로부터 수집한 환경을 그래픽, 음성 또는 문자로 표현하는 것에 이르기까지 다양하다. 두 번째 정의는 정보를 '우리가 인식하여 데이터에 부여한 의미'로 설명하고 있다. 의미는 데이터를 해석하는 행위로부터 도출되며 최종적으로 의미는 지식(knowledge)과 지혜(wisdom)에 이르게 된다. 다른 방식으로 설명하면, 분석과 해석에 의하여 도출된 이면에 숨어있는 의미 없이는 데이터는 제한된 가치만을 가질 뿐이다.[9]

정보는 또한 이용 가능성과 그 비용에 따라 세 가지로 나눌 수가 있다. ① 아무런 비용을 지불하지 않고 누구나 이용할 수 있는 정보와 ② 판매를 목적으로 취급되는 정보 그리고 ③ 가능한 정보 접근을 차단하여 보호하려는 정보가 그것이다.

정보가 군사작전을 수행하는 인간의 능력에 어떻게 영향을 미치는가를 이해하기 위해서 세 개의 영역 - 물리적 영역, 정보 영역, 인지 영역에 대한 설명이 필요하다.[10]

- 물리적 영역 : 물리적 영역은 군이 영향을 미치고자 하는 상황이 존재하는 장소로 지·해·공 우주를 가로질러 타격, 방호, 기동이 일어나는 영역이다. 여기에는 물리적 플랫폼과 그들을 연결하는 통신망이 상주한다. 비교적 이 영역의 요소들은 측정이 가장 용이해서 결과적으로 전투력은 주로 이 영역에서 측정된다. 이 영역에서의 전투력을 측정하는 주요 척도는 살상력과 생존성이다. 물리적 항목은 정보에 영향을 주기 위한 수단으로서 공격을 받을 수 있다. 컴퓨터의 파괴 또는 절취; 설비, 통신 노드나 선로, 데이터베이스 파괴 등 이들은 종종 "하드 공격"으로 불려진다.
- 정보 영역 : 정보 영역은 정보가 상주하는 곳으로 정보가 생성되고, 조작되고, 공유되는 영역이다. 정보 내용과 공정은 표적에 대한 물리적인 영향이 정보 공정이나 내용에 직접적으로 영향을 주기 위해 전자적으로 (정보 보안 방호를 깨뜨림으로써 전자기적 변환을 통하여 또는 접근 가능한 네트워크에 대해)공격을 받을 수 있다. 이러한 접근을 간접 또는 "소프트 공격"이라 한다.
- 인지 영역 : 인지 영역은 참가자의 마음이며 인지, 인식, 이해, 신념, 가치와 결심이 이루어지는 곳이다. 여기서의 공격은 전기적, 인쇄물, 또는 구두의 전송 경로를 통해 인간의 마음을 직접적인 표적으로 한다. 선전활동, 세뇌, 잘못된 오정보 기법은 이 영역 내에서의 공격들의 예이다.

2. 정보전의 정의

미 합참은 1996년 발간한 '합동비전2010'에서 작전영역을 지상/해상/공중/우주/정보(land/sea/air/space/information)의 5가지 영역(domain)으로 구분하고 '전 영역에서의 우세확보(full spectrum

7) 미 합참, JP 1-02, 2000. 1.
8) 전게서
9) 미 공군, AFDD 2-5 "정보작전", 2002. 1. p.2
10) Waltz, Edward "Information Warfare Principles and Operations," Boston/London: Artech House, 1998. p.27.

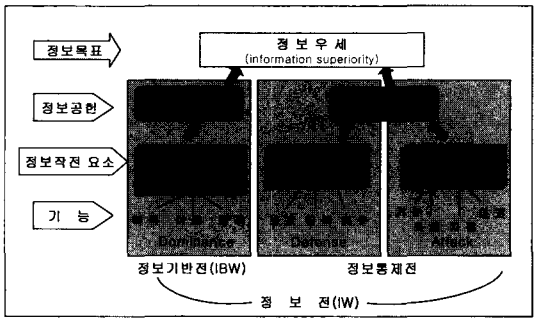
dominance)'를 위한 전제조건으로 정보우세의 중요성을 강조하였다. 이 정보영역(information domain)에서의 우세확보를 위한 전투를 정보전이라고 볼 수 있다. 그 후 1998년 발간된 합동교범 3-13 '합동정보작전'에서 "정보작전은 적의 정보 및 정보체계를 공격하는 한편 아군의 정보 및 정보체계를 방어하기 위하여 취하는 활동이며, 정보전은 위기나 분쟁 시에 특정 적을 상대로 하는 정보작전" 이라는 정의를 채택하였다. '합동비전2020'에서 언급하였듯이 정보기술의 진보와 함께 정보작전의 교리도 진화 중에 있으므로 정보작전/정보전의 정의도 지속적으로 변화하고 있는 실정이다. '최초의 정보전(the first information war)'의 저자 A. Campen은 "정보전 용어로의 접근[11]"에서 정보전은 전장정보(information-in-warfare)에서 지휘통제전(C2 warfare)으로, 다시 지휘통제전에서 정보전(information warfare)으로 진화하고 있다고 설명하고 있다.

3. 정보전의 분류

정보전을 보는 관점에 따라서 정보전에 대해서 다양한 정의가 존재하는 것과 마찬가지로 정보전을 보는 관점에 따라 정보전을 다양하게 분류 할 수 있다. 따라서 어느 한 가지 측면만을 강조한 정보전의 의미는 특정한 유형만을 나타냄을 알아야 하겠다. 그래서 리비키는 '정보전을 이해하려는 것은 마치 장님 코끼리 만지기와 비슷한 면이 있다'[12]고 했다.

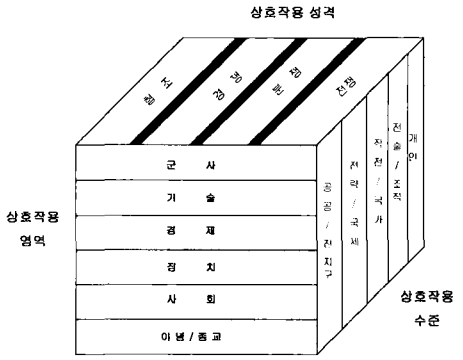
정보전에 대한 최초의 교과서라 할 수 있는 "정보전 원리와 작전"을 쓴 에드워드 월츠(Edward Waltz)는 국가적 관점에서 정보전을 크게 2가지로 분류할 수 있다고 기술하였다. "첫 번째는 정보기반전(IBW: information-based warfare)으로 우세한 전장인식(dominant awareness of the battle space)을 달성하기 위하여 정보를 획득하고 처리하고 전파하는데(혹은 이용하는) 초점을 맞추고 있다. 전형적인 활동에는 정보·감시·정찰(ISR)이 있다. 이 요소는 지식을 획득하여 정보이점 달성에 기여한다. 두 번째 요소는 정보이점의 차별화를 달성하기 위하여 상대의 지식을 공격하고 자신의 지식은 방어한다.

이 요소는 정보전-공격(IW-A)과 정보전-방어(IW-D)로 구성된다. 이 두 가지 요소는 서로 다른 수단에 의하여 정보우세(information superiority) 달성에 기여한다."[13] 이러한 구성요소들 간의 상호관계가 [그림 1]에 표현되어 있다.



[그림 1] 정보전 요소와 목표

또한, 정보전의 범위는 [그림 2]에서와 같이 행위자와 세 개의 영역 - 상호작용의 성격, 상호작용의 수준, 상호작용 영역에 의해 구분될 수 있다.[14]



[그림 2] 정보전의 범위

슈아르토는 정보공격의 대상에 따라 세 가지로 구분하였다.[15] 즉 정보전의 대상이 개인일 경우에 개인 정보전(Personal Information Warfare), 기업들의 기밀을 훔치거나 정보를 확산 시키는 기업정

11) Campen, Alan D. 등 공저, "Coming to terms with IW", 「사이버전 1」, AFCEA국제부, 1996, p. 289.
12) Libicki, M., "What Is Information Warfare?," Strategic Forum, No. 28, May 1995. p.4.
13) Waltz, Edward "Information Warfare Principles and Operations," Boston/London: Artech House, 1998, pp.20-21.
14) Alberts, David "Defensive Information Warfare," INSS, 1996, pp. 2-3.
15) Win Schwartau, "Information warfare: Chaos on the Electronic Superhighway, Tunder's Mouth Press, 1994.

보전(Corporate Information Warfare), 그리고 전 세계적인 경제주체, 국가 혹은 여러 국가들을 겨냥한 범 세계 정보전(Global Information Warfare) 등 세 가지로 분류하고 있다.

정보전 관련 폭넓은 연구를 해 온 미 국방대학의 리비키는 정보전이 전쟁을 수행하는 별개의 기술이 아니라 좀더 광의적인 개념에 포함될 수밖에 없는 일곱 가지의 정보전 유형 - 지휘통제전, 정보기반전, 전자전, 심리전, 해커전, 경제정보전, 사이버전(cyber warfare)을 제시하였다.[16] 이러한 정보전 유형의 분류는 정보의 보호, 조작, 파괴, 그리고 거부에 따라 구분된 것이다.

4. 정보전 특징

정보전을 구체적으로 충분히 이해하기 위해서는 정보전의 특징을 통해서 기존의 전쟁과 어떻게 다른지 알아볼 필요가 있다. 정보전 특징에 대해서는 미 국방과학위원회의 보고서에도 나타나 있지만 박상서의 논문[17]에서 가장 잘 설명하고 있어서 여기에 인용하였다.

'첫째, 정보전을 준비하고 수행하는데 드는 비용이 저렴하다. 핵무기나 화학 무기의 경우 연구 개발에 막대한 비용이 소요되지만 정보전을 수행하는데 필요한 정보전 기술과 정보전 무기는 많은 비용이나 국가 차원에서의 지원을 필요로 하지 않는다. 정보체계에 대한 전문지식만으로 정보전 기술과 무기를 연구 개발할 수 있고, 공격 대상이 되는 정보체계와 연결된 네트워크에 접근할 수만 있으면 개발된 정보전 무기를 사용하여 공격할 수 있다. 현재 정보체계에 대한 기술은 누구나 쉽게 입수할 수 있고 전세계의 거의 모든 정보체계들은 인터넷을 통하여 상호 연결되어 있어 적은 비용으로 전세계의 거의 모든 정보체계에 접속할 수 있다. 따라서 적국이나 반정부 단체 심지어 사회에 적의를 품는 개인도 네트워크를 통해서 정보체계를 공격할 수 있고 네트워크를 마비시킬 수 있다. 즉 정보전에서 정보체계를 공격하는 적은 국가뿐만 아니고 국가에 불만을 품은 개인도 될 수도 있다.

이런 잠재적 적들은 다양한 범위의 능력을 가질 수 있으므로 정보전에서 국가 이익에 대한 위협은 점점 증가되고 있으며 점점 더 복잡한 정보체계가 개발되고 정보전 무기를 연구 개발하는데 필요한 전문지식을 사이버 공간을 통하여 누구나 손쉽게 습득할 수 있으므로 국가 이익에 대한 위협은 계속적으로 변화하고 있다.

둘째, 사이버 공간에서는 전통적인 경계가 불분명해진다. 사이버 공간에서 상호 작용이 증가함에 따라 과거에는 명확하였던 공공과 개인의 이익, 전쟁과 범죄 행위 등을 구분하기가 어려워지고 국가 사이의 지역적, 정치적 경계가 모호해지고 있다. 따라서 국가의 이익에 반하는 잠재적인 적이나 정보전 무기들이 사이버 공간에 배치되어 있을 경우 정보전 위협과 공격 행위가 국내에서 시작된 것인지 외국에서 시작된 것인지 구별하기가 점점 어려워진다. 또한 누가 공격하고 있는지 누가 공격당하고 있는지 누가 공격을 준비하고 있는지를 구별할 수 없게 된다. 따라서 전통적인 경계에 따라서 역할이 정해져 있는 국내의 법 집행기관과 국가 안보기관 및 첩보기관 사이의 역할 구분이 모호해지며 정보체계가 공격당하고 있을 때 그것이 범죄 행위에 의한 것인지 전쟁행위에 의한 것인지 구분할 수 없게 된다. 이처럼 전통적인 경계가 모호해짐에 따라 적대국은 국제적으로 문제점을 일으킬 수 있는 전통적인 군사행위나 테러를 하는 대신 개인이나 다국적 범죄 조직을 이용하여 공격할 수 있다.

셋째, 사이버 공간에서는 사실을 인지하는 지각 능력을 쉽게 조작할 수 있다. 새로운 정보기술을 이용하면 잠재적인 적의 기만과 영상조작 능력이 크게 증가될 수 있으므로 정부는 국가안보와 관련된 국민의 정치적인 지지를 상실 할 가능성이 많아진다. 예를 들면 정치활동 단체나 기타 반정부 기구는 인터넷과 정보기술을 이용하여 심리전을 수행함으로써 정치적인 지지를 손쉽게 획득할 수 있고, 정보전 스파이 역시 대중의 지각 능력에 중요한 영향을 미치는 거짓 정보를 생성하거나 특정 정보만 공개하여 여론을 조작할 수 있다. 이렇게 조작된 정보는 인터넷이나 TV등을 통하여 폭넓게 유포될 수 있으므로 국가는 국가 안보에 중요한 사안에 대해서 국민의 지지를 얻고 유지하기가 어려워진다.

넷째, 정보전을 위해서는 새로운 전략 첩보의 수집 및 분석 방법이 요구된다. 아직까지 정보전에 대해서

16) M., Libicki, "What Is Information Warfare?," Strategic Forum, No. 28, May 1995.
17) 박상서, "정보전: 새로운 전쟁 패러다임," 공군 창군 50주년 기념 국제 학술 세미나 논문집, 교리 발전 분야, pp. 25-86. 1999.

는 공격 대상과 취약성이 명확히 파악되어 있지 않기 때문에 기존 전쟁의 공격 대상과 위협을 기반으로 운영되는 전통적인 첩보 수집 및 분석 방법은 사이버 공간에서는 효과가 없다. 정보전은 앞에서 살펴본 것처럼 전통적인 경계가 모호하기 때문에 첩보 수집 대상을 식별하기 어렵고 위협이 계속하여 빠르게 변화하기 때문에 이들에 대한 첩보를 수집자원을 할당하기 어렵고 정보전 취약성과 공격 대상에 대해서 아직까지 명확하게 이해하지 못하고 있어 전통적인 첩보 수집 및 분석 방법은 정보전과 관련된 첩보에서는 사용이 불가능하다. 따라서 정보전에 초점을 맞춘 새로운 첩보 수집 및 분석 방법이 개발되어야 한다.

다섯째, 사이버 공간에서는 스파이 활동이나 사고 등을 정보전 공격과 구분할 수 있는 적절한 전술 경고 시스템 및 공격 평가 방법이 없다. 정보전에서는 정보전 공격을 하고, 시스템고장, 해킹 등 다른 사건과 구별하는 것이 거의 불가능하기 때문에 전술적 경고와 공격 평가가 기존 전쟁과는 완전히 다른 새로운 문제를 발생시킨다. 따라서 현재 정보전 공격이 잘 진행되고 있는지 누가 공격을 하고 있는지 공격이 어떻게 수행되고 있는지를 알기는 거의 불가능하다.

여섯째, 정보전에는 전선이 따로 없다. 앞에서 살펴 본 것처럼 정보기술은 시간적 공간적 차이를 무의미하게 하므로 기존 전쟁과 달리 후방도 전방과 동일하게 공격 대상이 된다. 정보화 사회에서는 통신, 전력, 유류, 저장과 전송 ,금융, 운송, 급수, 응급 서비스 등 국가의 모든 기반구조가 상호 연결된 정보기반구조에 의존하고 있고 정보전 공격은 이들이 연결 되어 있는 사이버 공간에서 수행되므로 공격하기 쉽고 공격의 효과가 높은 공격 대상들이 정보전 무기로 무장한 적에게 쉽게 노출된다. 따라서 정보전에서는 전방과 후방의 구분이 무의미해지고 네트워크를 통해 접근할 수 있는 곳은 어디든지 잠재적인 전방이 될 수 있다.

이들 특징에서 보듯이 정보전은 전방과 후방의 구분이 없으며 민간 분야가 먼저 공격의 대상이 될 수도 있다. 따라서 정보전에 대해서 논의할 때에는 대상에 군과 일반 모두를 포함하여야 한다. 그래서 미 합동정보작전은 이 점을 강조하고 있다. "정보작전은 국가 군사전략을 지원하지만 민간산업은 물론 정부의 다른 부서, 기관과의 지원, 협조, 참여를 필요로 한다. 많은 국방부 정보의 흐름은 민간기반체계에 의존하지만, 많은 경우에 이러한 기반체계의 보호는 국방부의 권한과 책임 밖의 일이다."[18]

Ⅳ. 정보전과 유사개념

1. 사이버 전(cyber-war)

정보전과 유사한 개념으로 사이버전이라는 용어를 흔히 사용한다. 사이버전이란 일반적으로 사이버공간(cyber_space)에서의 전투이기 때문에 우선 사이버 공간에 대한 정확한 이해가 필요하다.

조지타운 대학의 도로시 데닝교수는 "사이버공간은 모든 컴퓨터 네트워크의 총합으로 구성된 네트워크의 총합이다."[19]라고 표현하였는데 이것은 대표적인 민간분야의 정의로 보인다.

미 국방대학교 '정보전과 정보기술'과정의 주임교수인 대니얼 퀄 박사는 "사이버 공간이란 전자기적 스펙트럼을 통하여 효과를 미치는 컴퓨터 네트워크와 원격통신 시스템 및 기타 장치 등 전자시스템이 서로 연결되고 상호 작용하는 장소"라고 정의하고 있다.[20]

사이버전을 정보전과 혼동하게 만든 데는 미국의 군사이론가 아킬라&론펠트, 리비키의 공헌이 크다. 아퀼라&론펠트는 그의 유명한 글 "사이버전이 오고 있다!"(1993)에서 미래전의 유형으로 네트전(netwar)과 사이버전(cyberwar)을 제시하였으며 리비키는 "정보전이란 무엇인가?"(1995)에서 정보전의 유형을 지휘통제전, 정보기반전, 전자전, 심리전, 해커전, 경제정보전, 사이버전(cyber warfare)의 7가지 유형으로 분류하였다. 우리는 여기에서 사이버전을 전자는 전쟁(war)의 한 유형으로 후자는 전투(warfare)의 한 유형으로 다루고 있음에 유의할 필요가 있다.

아퀼라&론펠트는 "사이버전이 오고 있다!"에서 "사이버전은 C3I를 강조하는 정보전의 기존 견해들과 유사하다. 20세기가 전격전의 시대였다면 21세기는 사이버전이 될 것이다. 사이버전은 정보관련 원칙에 따라 군사작전을 준비하는 것과 수행하는 것을 의미한다. 그것은 적이 상대방 - 그것이 누구인

18) 미합참, JP 3-13, pp. I-11-13

19) Denning, Dorothy"information warfare and security," 안보문제연구소(역), 안보총서 87(상권), 2000, p.52.

20) Kuehl, Daniel "정보작전, 정보전 및 메타네트워크," 「공군대학 국제심포지엄」,2000, p. 98.

지, 어디에 있는지, 언제, 무엇을 할 수 있는지, 왜 싸우려고 하는지, 어느 위치에서 싸워야 할 것인지, 어느 위협과 먼저 싸워야 할 것인지? 등 - 을 알기 위하여 의존하는, 넓은 의미에서는 군사문화까지도 포함하는, 정보와 통신체계를 와해시키는 것을 의미한다. 그것은 적은 우리자신에 대해서 많은 것을 알지 못하도록 억제하는 동시에 적에 대해서는 모든 것을 알려고 노력하는 것을 의미한다. 그것은 특히 군사력의 균형이 이루어지지 않은 상태에서 '정보와 지식에 대한 균형'을 우리에게 유리하게 전환시키는 것을 의미한다. 그것은 비용과 노력의 낭비를 줄이기 위하여 지식을 활용하는 것을 의미한다."[21] 라고 주장하고 있다. 월츠는 "이들의 사이버전은 바로 지휘통제전을 의미한다."라고 단언하고 있다. 그러나 일부 학자들은 아퀼라&론펠트의 사이버전은 지휘통제전의 수준에 머물지 않고 유혈에 의하지 않고 전쟁에서 승리하는 미래전을 표현하고 있다고 말한다.

리비키는 "정보전이란 무엇인가?"에서 "사이버전을 정보테러 행위, 의미론적 공격, 모의 전쟁, 깁슨(Gibson)전쟁을 포함하는 유형으로 현 시점에서는 실현 불가능하지만 미래에서는 있음직한 전투의 유형"이라고 주장하였다. 여기에서 "정보 테러행위는 정보체계를 파괴하는 것이 목적이 아니고 체계를 이용하여 다른 개인을 공격하기 위하여 체계를 부당하게 이용하려는 것이 목적인 컴퓨터 해킹의 한 형태이다. 의미론적 공격과 해커전의 차이는 후자는 무 작위적으로 혹은 계획적으로 시스템을 고장 나게 만들어 작동을 멈추게 하는 것이지만, 의미론적 공격을 받은 시스템은 정상적으로 작동되는 것처럼 인식되지만 실제는 모순된 결과를 만들어 낸다는 것이다. 모의 전쟁이란 실제전쟁을 하지 않고 모의전쟁(simulation)을 함으로써 승리와 패배를 결정하는 것이며, 깁슨전쟁은 인터넷상에서 대리인(agents)에 의한 전쟁을 의미한다."[22] 리비키의 개념은 미래에 사이버공간인 인터넷에서 일어날 수 있는 전투의 유형을 사이버전으로 보았다.

여기에서 아퀼라&론펠트와 리비키를 비교한다면 전자는 사이버전(war)을 더 큰 차원에서 전쟁양상으로 보고 있는데 반하여 후자는 전투의 한 형태로 보는 차이가 있다. 이와 같이 아퀼라&론펠트의 사이버전과 리비키의 사이버전은 전혀 그 내용을 달리하고 있음에도 불구하고 사이버 공간에 대한 개념부족과 민간부분에서 주장하는 사이버전과 혼동하여 개념상의 혼란을 일으키는 원인이 되고 있다.

2. 네트전(netwar)

세계는 컴퓨터, 광통신, 위성통신, 유/무선 통신기술을 융합한 범세계적 정보기반체계(global information infrastructure)를 구축하여 전 세계를 하나의 정보권으로 묶어가고 있다. 우리는 지금 인터넷으로 대변되는 범세계적 컴퓨터 네트워크 없이는 정보의 전파도, 기업 활동도, 행정도 불가능한 정보시대에 살고 있다. 컴퓨터와 통신망으로 구성된 네트워크야말로 현대사회의 가장 기본적인 기반체계(인프라)이며 이 정보기반체계를 대상으로 하는 전투를 네트전이라고 말한다. 이 컴퓨터 네트워크는 크게 범세계적 정보기반체계(GII: global information infrastructure), 국가정보기반체계(NII), 국방정보기반체계(DII)로 구분하며 대부분의 정보전 활동은 이 기반체계를 중심으로 이루어지기 때문에 정보전을 종종 네트워크전(network warfare)이라고 부르기도 한다.

아퀼라&론펠트는 '사이버전이 오고있다!'에서 "인터넷이라는 통신수단을 통한 사회적 수준의 심리전을 네트전"[23]으로 정의하였다. "네트전은 통신의 인터넷 형태를 통하여 수행하는 사회적 수준의 관념적 분쟁이다. 네트전은 보다 높은 수준에서 국가간 혹은 사회간 정보관련 분쟁을 지칭한다. 그것은 목표 집단이 자신과 주변세계에 대하여 알고 있는 것이나 생각하고 있는 것을 방해하거나 손상시키거나 변경시키려는 시도를 의미한다. 네트전은 대중이나 엘리트 혹은 양자 모두의 여론에 초점을 맞출 수도 있다. 그것은 공개적인 외교수단, 선전과 심리적 캠페인, 정치 문화적 전복, 지역매체에 간섭하거나 기만, 컴퓨터 네트워크와 데이터 베이스침입, 컴퓨터 네트워크를 통해 반체제 인사나 저항운동을 고무시키는 노력들을 포함할 수도 있다." 다시 말하자면 네트전은 인터넷을 통하여 적의 인지를 조작하고 적의 가치와 신념체계를 바꾸고 그들의 행동을 변화시켜 목표를 달성하는 인지와 관념의 분쟁으로 고차원의 전쟁을 의미한다. 상기 네트전은 독특한 이론으로 우리가 일반적으로 생각하는 네트워크전 - 적의 국가기반체계와 국방기반체계를 공격하는 - 과는 구별되어야 한다.

21) 황호상, 김재연 역, "정보전, 사이버전, 네트전", 2001, 합참대학, pp. 18-19.
22) 전게서, pp. 98-103.
23) 전게서, p.15.

3. 해 커 전

'해커'란 원래 컴퓨터 시스템의 내부구조와 작동원리 등에 심취하여 이를 알고자 노력하는 사람으로 컴퓨터와 통신에 뛰어난 실력을 가진 사람들을 지칭하였으나, 90년대 초에는 다른 컴퓨터에 불법으로 침입하여 자료를 무단으로 열람, 변조, 파괴하는 등의 행위를 하는 침입자, 파괴자를 함께 해커로 부르고 있다. 그리고 최근에는 인터넷을 주무대로 하는 가상공간에서 사이버 범죄를 일으킬 가능성이 있는 사람들을 통칭하여 부르고 있다.

리비키는 '정보전이란 무엇인가?'에서 "물리적 전투에서와 달리 이러한 컴퓨터와 네트워크 시스템을 향한 공격들은 시스템의 보안구조에서 발견할 수 있는 허점을 이용하기 때문에 시스템의 특성에 따라 독자성을 갖는다. 해커전의 특성은 매우 다양하다. 공격자는 일반적인 상상력으로 어디에든지 있을 수 있기 때문에 대부분 은밀한 곳에 숨어 있을 것으로 생각하지만 평소에 잘 보이는 곳에 숨어 있을 수 있다. 공격의 목적은 간헐적인 시스템 기능정지, 무작위 자료변조, 대량의 자료손실, 서비스의 무단중단, 불법적인 시스템 감시와 정보수집, 거짓 메시지 유입에 의한 전산마비, 공갈의 목적을 띤 자료입수까지 다양하다. 자주 쓰이는 도구들에는 바이러스, 웜, 트로이 목마, 논리폭탄 그리고 트랩도어가 있다."

해커전이 정보전에 유용한 도구인가? 대부분의 군 지휘통제시스템(C4I)이나 중요한 시스템들은 물리적으로 인터넷과 분리되어 있다. 그렇다고 해커전은 군 정보체계와 전혀 관계가 없는가? 현재 대부분 국가의 국방정보기반체계들과 국가정보기반체계들은 긴밀하게 연계되어 있다. 우리나라의 경우, 논리적으로 국방망은 인터넷과 연결이 차단되어 있지만 민간 광케이블이나 위성통신을 임차하여 쓰고 있으므로 물리적으로는 같은 인프라를 쓰고 있는 상태이다. 따라서 국가정보기반체계가 와해된다면 국방정보기반체계도 동시에 와해되는 것이 현실이다. 또한 국가운영에 핵심이 되는 정보통신기반체계 예를 들어 정보통신망, 에너지 관리, 수송관리, 물류관리, 행정망들은 인터넷으로 연결되어 있다. 이러한 국가중요기반체계들이 해커의 공격으로 기능이 마비될 경우 국가기능이 제대로 수행될 수 없다.

해커전에 대한 미 국방부의 공식적인 용어는 컴퓨터 네트워크작전(CNO: Computer Network Operation)이다. 미 국방부는 컴퓨터네트워크작전의 책임을 미 우주사령부에 부여하였고, 우주사령부는 1999년에 컴퓨터네트워크방어(CND) 임무를, 2000년에는 컴퓨터네트워크공격(CNA) 임무를 인수하였다고 발표하였다. 즉, 미국은 CNO를 공식적인 군사작전으로 채택하였음을 공개적으로 선포한 것이다.

기타 독일, 중국, 북한 등 많은 국가들에서 정보전사로서 해커를 양성하고 있다는 것은 잘 알려진 사실이다. 해커전은 정보전의 중요한 수단이며 미래에는 그 역할이 더욱 증가될 것이다.

4. 사이버 테러

미 연방 수사국 전문요원인 '마크 폴리트'는 실용적인 정의를 내어놓았다. "사이버 테러리즘은 미리 고려되고, 정치적 동기를 받아 국가예하 단체나 비밀기관에 의해 비 전투 표적들에게 폭력을 야기 시킬 정보, 컴퓨터 시스템, 컴퓨터 프로그램, 그리고 데이터에 대한 공격이다."

우리나라 대통령 훈령 '국가 대테러 활동지침'에는 "컴퓨터 통신망을 이용한 정보조작 및 전산망 파괴"를 테러 유형의 하나로 규정하고 있다. 국정원 발표자료에 의하면 "사이버 테러는 사이버 공간에서 일정한 목적을 가지고 계획적으로 정보시스템을 공격하는 행위"라고 정의하고 있다. 이는 단순한 해킹이나 바이러스 유포행위와는 구별되게 사용되어야 함을 의미한다. 또한 사이버 테러의 수단은 해킹뿐만 아니라 최근에 등장하고 있는 치핑, 나노 머신, HERP총, EMP폭탄 등을 거론하고 있어 물리적 공격에 대해서도 관심을 갖고 있는 것을 알 수 있다.

그러나 최근 입법된 '정보통신 기반보호법'[24]에서는 사이버 테러라는 용어대신에 '전자적 침해행위'라는 용어를 사용하고 있으며 그 정의는 "정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위."라고 표현하고 있다.[25] 즉, 정부의 정보통신망 운영부서에서는 전자적 침해행위, 법집행기관인 국정원, 검찰, 경찰에서는 사이버테러라는 용어가 쓰이고 있다.

종합적으로 사이버 테러는'정치적, 이념적 목적을 가진 사이버공간에서의 테러행위'를 의미한다고 볼 수

24) 정통부, '정보통신기반 보호법' 시행령 제정 공포, 2001. 7.
25) 정통부, '정보통신기반 보호법' 제정 공포, 2001. 1.

있으며, 향후 정부 쪽에서는 사이버테러와 전자적 침해행위라는 두 가지 용어가 혼용될 것으로 보인다.

V. 정보전과 관련된 이슈

1. 정보우세는 정보작전의 최종목표인가?

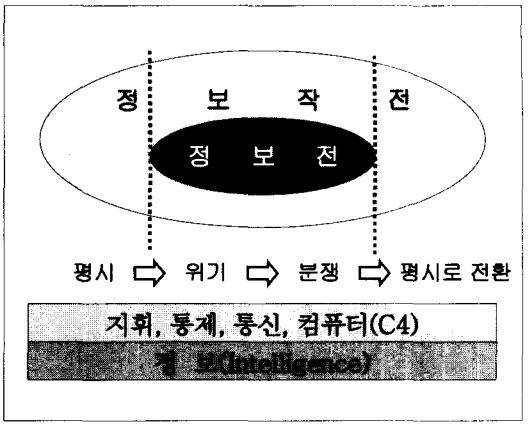
항공전에서 공중우세 달성은 지상군 및 해상군의 자유로운 활동을 보장하고, 공세적 항공작전을 수행할 자유를 획득하기 위하여 우선적으로 성취해야하는 목표인 것은 사실이나 항공전의 최종목표가 아니듯이 정보작전에서 정보우세는 우선적으로 달성해야 하는 목표이나 그 자체가 최종목표는 아니다. 공중우세와 마찬가지로 정보우세는 국지적/일시적으로 유지될 수 있지만 전 지역에서 지속적으로 유지한다는 것은 사실상 어렵거나 어렵지 않더라도 비용 대 효과 측면에서 바람직하지 않다. 미 합동비전 2020은 "정보우세의 확보는 그 자체로 최종목적은 아니다.(The creation of information superiority is not an end in itself.). 합동군은 우세한 정보를 결심우세(decision superiority)를 달성하기 위하여 우세한 지식으로 전환할 수 있어야 한다."[26] 고 기술하고 있다.

2. 정보전과 정보작전의 관계는?

〔그림 3〕[27]에 보는바와 같이 정보전은 '위기 및 분쟁 시에 특정한 적을 상대로 특정한 목표를 달성하거나 증진시키기 위해 행해지는 정보작전'으로 정의된다. 즉, 정보전은 주로 위기 시 및 전시의 군사분야를 대상으로 하는 반면, 정보작전은 평시까지를 포함하는 전 시간영역을 대상으로 비 군사분야까지 포함하는 보다 포괄적인 개념이다.

미국의 경우 종래의 정보전이라는 용어는 1996. 12. DODD S3600.1 '정보전'에 와서야 정보작전과 정보전으로 분리되었다. 여기에 보면 지휘통제전(C2W)에 컴퓨터와 네트워크 공격을 포함하여 정보전이라 하고 정보전에 비 국방 정보활동을 포함 하였을 때를 정보작전이라 일컫고 있다. 따라서 정보작전이 정보전 보다 포괄적임을 알 수가 있다. 다만 국방 측면에서만 보면 정보전과 정보작전은 동일시 될 수 있다.

26) 미합참, JV2020, p.8
27) 미 합동교범 3-13, "합동 정보작전", 1998, p.17.



〔그림 3〕 미 합참 정보전과 정보작전의 관계

3. 정보작전이 전반적인 작전을 수행하는데 있어 단순히 '전력을 보강' 하는 차원에서 일조를 할 것인지, 아니면 완전히 새로운 작전 수행방식으로서 지금까지 존재하지 않았던 새로운 전투수행능력을 제공할 것인지?

이 문제는 군의 임무와 조직, 역할과 관련된 매우 중요한 사항으로 지금까지는 주로 전자에 비중을 많이 두고 있다고 볼 수 있지만 앞으로 정보사회가 성숙되어 가면서 정보기술의 고도화와 함께 후자 쪽의 가능성이 높아 질 것으로 보인다. 그렇게 되면 현재의 군 구조를 새롭게 편성해야 함은 물론이고 국가안보의 틀이 근본적으로 변화하게 될 것이다.

VI. 맺음말

본 논문에서는 정보전이 출현된 배경, 정보전의 정의, 분류, 특성을 통해 그리고 정보전의 유사 개념을 통해 정보전의 개념을 명확히 정립 하고자 하였다. 또한, 정보전과 관련된 이슈들을 살펴봄으로서 정보전에 대한 올바른 이해를 얻고자 하였다. 하지만 필자들의 경험과 환경의 영향으로 대부분 군사정보전에 치우쳐 있음을 부언해 둔다.

참 고 문 헌

〔1〕 Alberts, David "Defensive Information Warfare", INSS, 1996.

[2] Arquilla, John and Ronfeldt, David "Cyberwar Is Coming!," Comparative Strategy, Vol.12, No.2, 1993.
[3] Dearth, Douglas H. and Goodden, R. Thomas "사이버전 후기", 「사이버전」, AFCEA, 1996.
[4] Dorothy Denning, "information warfare and security", 안보문제연구소(역), 안보총서 87(상권), 2000.
[5] Libicki, M. "What Is Information Warfare?," Strategic Forum, No. 28, May 1995.
[6] Stein, George J. "Information Warfare," Airpower Journal, Spring 1995.
[7] Waltz, Edward "Information Warfare Principles and Operations," Boston/ London: Artech House, 1998.
[8] 미 합참의장지시 6510.1, "방어적 정보전", 1996.5.
[9] 미 합동교범 3-13, "합동 정보작전", 1998.
[10] 박상서, "정보전: 새로운 전쟁 패러다임," 공군창군 50주년 기념 국제 학술 세미나 논문집, 교리 발전 분야, 1999, pp. 25-86.
[11] 황호상 역, "정보전, 사이버전, 네트전", 합참대학, 2001.

〈著者紹介〉

권 태 환 (Taehwan Kwon)

1976년 3월: 공군사관학교 졸업
1979년 2월: 서울대학교 전자공학과 졸업
1982년 2월: 서울대학교 대학원 전자공학과 석사
1990년 8월: 미 오리건 주립대학교 전기 및 컴퓨터 공학과 박사
1982년~1997년: 공군사관학교 전자공학과 교수
1997년~현재 : 국방대학교 무기체계학과 교수
관심분야 : 정보전, C4ISR, 군사통신체계

황 호 상(Hosang Hwang)

1973년 3월 : 공군사관학교 졸업
1984년 12월 : 미 해군대학원 전기공학과 석사
1999년 8월 : 서울대학교 행정대학원 정보통신방송정책과정 수료
1998년~1999년 : 국방부 정보화기획관실 정보화정책과장
2000년~현재 : 합참대 작전학과 교수
관심분야 : 정보전, C4ISR