情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

사이버전 중심의 미래전 고찰

강 태 원*, 황 정 섭**

요 약

선진/주변국에서는 C4ISR/PGM(Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance/ Precision Guided Missile)체계를 미래전의 핵심으로 인식하여 막대한 예산을 투입, 체계를 구축하고 체계의 극대화를 위해서 상호운영성, 표준화 등에 관심을 경주하고 있다. 그러나 이러한 모든 체계는 네트워크로 연결됨에 따라 미래전의 신종 위협으로 등장한 컴퓨터 바이러스, 웜(worm), 트로이 목마(Trojan Horse), 논리폭탄(Logic bombs), 트랩도어(Trap doors), 칩핑(chipping), 나노 머신으로 분류되는 초소형로봇, EMP/HPM(Electro Magnetic Pulse/High Powered Microwave)등에 대한 취약점을 지니게 되며 이에 대한 대비책도 강구하고 있다.

본 연구에서는 미래 디지털 전쟁의 핵심인 C4ISR/PGM복합체계를 소개하고, 미래전의 특성 및 C4ISR와 PGM체계의 역할에 대해 소개하며, 특히 비대칭 전력으로 선진/주변국에서 강력하게 추진하고 있는 사이버전 현황 및 발전 추세를 제시하고, 정보전의 한계와 문제점도 제시한다.

Ⅰ. 서 론

새로운 방식으로 새로운 행동을 취하는 길만이 생존의 유일한 방법인 시대에 우리는 살고 있다. 사람들은 흔히 변화가 낯설다는 이유로 변화 자체를 거부하곤 한다. 또 변화가 필요함에도 불구하고, 위험하다는 핑계를 대며 마지막 순간까지도 수용하려 들지 않는 경향이 있다. 그러나 예기치 않은 순간에 이미 예견된 결과는 나타나기 마련이다. 따라서 우리는 지금 즉시 적응해야 할 변화를 알아차리고 미래를 준비해야 한다. 왜냐하면, 과거에 집착하고 미련을 두는 것은 또 다른 변화를 알아차릴 수 없는 과오를 남기며 변화에 대한 감지 속도가 늦을수록 그 타격은 더욱 더 크기 때문이다.

우주항공, 정보통신, 생명공학, 초미세기술(nano/ MEMs) 등을 활용한 과학기술의 영역은 우주, 사이버 등 미지세계로 계속 확장되고 있고, 특히 정보기술(IT)의 폭발적 발전은 디지털혁명/인터넷혁명을 창출하였다. 아울러, 현재의 IT기술 성능은 지난 25년간 약 1만 배 증가하였으나 비용은 반비례하여 약 1만 배 감소하였고 향후 25년 후 컴퓨터 능력은 현재보다 1백만 배 증가될 것이나 비용은 반비례하여 오히려 감소될 것으로 예측된다. 정보화사회를 주도한 견인차는 첨단 정보통신기술, 그 중에서도 특히 컴퓨터 및 네트워크기술의 급속한 성장과 이 두 가지 기술의 융합이다. 또한 초고속·대용량의 정보를 실시간 전파할 수 있는 정보고속도로(Information Super High Way)는 처리된 정보의 유통속도를 혁신적으로 향상시키고 있다. 이러한 기술들을 근간으로 하는 고정밀 생산기술과 무인화·자동화기술의 발전은 사회생활의 혁신전인 변환을 예고하고 있다.

정보사회의 전쟁양상도 과거 농경사회, 산업사회의 전쟁양상과 큰 차이를 보이고 있다. 농경·산업사회에서의 전쟁이 대량살상전의 양상이었다면 정보사회의 전쟁은 인명살상을 최소화하면서 상대방의 심장부를 정밀타격·무력화하여 단기간에 전쟁의 목적을 달성하는 정밀파괴·마비전의 양상으로 변화하고 있다. 특히 정보통신기술의 발전은 인터넷 등 범세계적인 정보통신 네트워크의 등장으로 인해 빛의 속도로 정보를 전파할 수 있게 됨에 따라 지휘통제에서 가장 큰 제약요소였던 지역과 공간 그리고 거

* 국방부 군사혁신단(twkang1@hanmail.net)
** 국방과학연구소(hw2025@dreamwiz.com)

리개념을 사라지게 하였다. 또한 정보통신기술의 발전에 힘입어 타격체계는 정밀화·장사정화·경량화·고위력화되고, 센서체계는 정밀화·다양화됨에 따라 적보다 먼저 보고 먼저 결심하고 먼저 상대방 전력의 심장부를 정밀타격 해야만 전쟁에서 우위를 확보할 수 있는 시간전·속도전의 양상으로 발전되고 있다.

이러한 전쟁양상에 대비하기 위해서 미국 등 선진국들은 초고속·대용량의 정보고속도로를 이용하여 고정밀 센서체계와 타격체계를 결합한 C4ISR/PGM(Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance/Precision Guided Missile) 복합체계 개념을 정립하고 미래전의 핵심전력으로 집중 개발하고 있다. C4ISR의 비약적인 발전은 전장의 가시화 · 정보공유의 실시간화를 이루었고, 전장의 안개와 우연성을 현저히 감소/제거하게 되었으며 ISR의 경우, 걸프전시에는 고가치 표적의 15%를 탐지 할 수 있었으나 2005년경에는 90%까지 탐지 가능할 것이고 2010년경에는 완전한 전장가시화가 실현될 전망이다. 지휘통제를 위한 정보전달속도도 과거에는 수 시간이 소요되었으나 2005년에는 수분/수초만에 전달이 가능하고 2010년경에는 실시간으로 변할 것으로 전망된다. 이는 전장상황의 완전 인식을 통하여 계획 변경·자원낭비의 대폭적인 감소를 가져올 수 있고, 지휘관이 확신을 갖고 전투력을 할당하여 기동 및 타격, 전장지배 등이 가능하며, 빠른 템포의 작전 수행을 통해 적을 전투준비 이전에 타격 함으로서 시간적 기습이 가능하도록 한다.

이미 선진국에서는 C4ISR/PGM체계를 미래전의 핵심으로 인식하여 막대한 예산을 투입, 체계를 구축하고 체계의 극대화를 위해서 상호운영성, 표준화 등에 관심을 경주하고 있다. 그러나 이러한 모든 체계는 네트워크로 연결됨에 따라 미래전의 신종 위협으로 등장한 컴퓨터 바이러스, 웜(worm), 트로이 목마(Trojan Horse), 논리폭탄(Logic bombs), 트랩도어(Trap doors), 칩핑(chipping), 나노 머신으로 분류되는 초소형로봇, EMP/HPM등에 대한 취약점을 지니게 되므로 이에 대한 대비책도 강구하고 있다.

본 연구에서는 미래 디지털 전쟁의 핵심인 C4ISR/PGM복합체계를 소개하고, 특히 비대칭 전력으로 선진국에서 강력하게 추진하고 있는 사이버전 현황 및 발전 추세를 제시한다.

II. 미래전의 특성 및 C4ISR/PGM의 역할

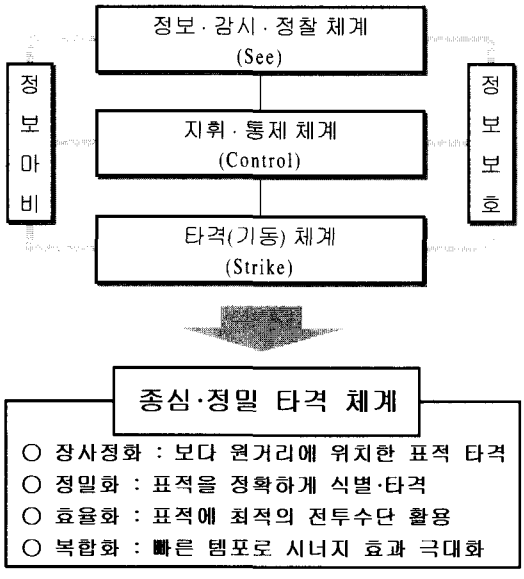
미래전의 성패는 "먼저 보고(先見)-먼저 결심하고(先決)-먼저 타격(先打)"하는 일련의 전투행위 주기를 얼마나 줄일 수 있는가에 달려있다고 해도 과언이 아니다. 이러한 주기에서 C4ISR체계는 먼저보고-먼저 결심하게 하는 핵심수단을 제공하고 이를 이용하여 PGM이 먼저 타격을 하게 되는 것이다.

1. 미래전의 특성

미래전, 특히 21세기 지식·정보사회의 전쟁양상과 핵심 전력체계는 어떻게 발전될 것인가? 엘빈 토플러(Alvin Toffler)는 인류가 전쟁을 수행하는 방식은 인류가 '일'을 하고, 부(富)를 창출하는 방식을 그대로 반영해 왔다고 주장했다.[1] 이러한 논리에 의하면 오늘날 사회에서 일어나고 있는 여러 가지 혁신적인 변화는 미래 군대와 전쟁의 변화를 예고해 주는 것이라고 해도 과언이 아닐 것이다. 우선, 미래 전쟁에서는 지식·정보가 군사력의 가장 핵심적인 요소가 될 것이다. 지식·정보가 경제적 富를 창출하는데 있어서 가장 큰 역할 및 기능을 수행하는 것처럼 전쟁에서도 지식·정보가 승패를 좌우하는 핵심 요소가 될 것이다. 둘째, 지식·정보사회의 전쟁에서는 파괴의 탈 대량화(demassification)가 이루어질 것이다. 21세기 정보사회에서는 전장을 투명하게 보고(ISR), 전장의 정보를 공유할 수 있을 뿐만 아니라(C4I), 정밀 유도무기(PGM)의 성능도 대폭적으로 향상될 것이므로 대량파괴, 대량살상을 하지 않고서도 승리할 수 있게 된다. 셋째, 지식·정보사회에서는 전장공간을 우주와 사이버 공간까지 확대시킬 것이다. 미래에는 항공·우주를 통제할 수 없으면 작전지역에 대한 지식·정보를 실시간으로 제공할 수 없고, 우주를 이용한 상업적 용도의 정보통신 시스템이 적에게 파괴당하면 정보사회 전체가 일시에 마비될 수 있다. 넷째, 지식·정보사회의 전쟁은 로봇(robot)에 의한 무인화 전쟁이 될 것이다. 로봇은 전투기·정찰기의 조종사와 전차 운전병을 대신하고 정보수집 및 표적발견, 불발탄 및 지뢰 제거, 유독 환경에서의 작전활동 등과 더불어 적의 표

1) Alvin & Heide Toffler, War and Anti-War (Boston : Little, Brown & Company, 1993), p. 3.

적을 직접 공격·파괴하는 데에도 이용될 것으로 보인다. 다섯째, 미래의 군사조직은 네트워크형의 소규모·비 계층적·유연 조직이 될 것이다. 여섯째, 지식·정보사회에서의 전투원(warrior)은 고도의 지식 및 정보로 무장하게 될 것이다. 하이테크 무기체계들은 고지식·고기능·고기술의 전투원을 요구하게 된다. 일곱째, 정보사회의 전쟁수행 방식은 최소의 희생으로 최단 기간 내에 승리하는 방법이 요구될 것이다. 이와 같은 21세기 지식·정보사회의 전쟁에서 주도적 역할을 담당하게 될 핵심 전력체계는 어떤 것일까? 그것은 바로 전 미합참차장 오웬스 제독이 주장한 「신 시스템 복합체계」라고 판단된다. 이는 감시체계(see : ISR)와 통제체계 (control : Advanced C4I), 그리고 정밀 타격체계 (strike : PGMs / platforms)를 상호 유기적으로 연결, 복합하여 하나의 거대한 「광역·원거리·정밀 감시(see)-통제(control)-타격(strike) 복합체계」를 형성하는 것으로서[2], 〔그림 1〕과 같이 표현 할 수 있다.



〔그림 1〕 미래 핵심전력체계 구성 및 특성

더불어 이러한 핵심전력을 효과적으로 순식간에 무력화시킬 수 있는 고출력 마이크로웨이브(HPM: High Powered Microwave)나 전자기파탄(EMP: Electro Magnetic Pulse), 빛의 속도로 공격할 수 있는 능력을 가진 레이저 및 플라즈마 무기, 바이러스를 이용한 사이버무기 등이 집중 개발될 것이다.

과거에도 그러했지만 미래에도 정보우세는 전쟁승패의 핵심이 될 것이다. 특히 미래전에서는 C4ISR체계가 정밀타격체계(PGM)와 결합시 핵무기에 버금가는 수준의 효과를 발휘할 것으로 예측되고, 아군의 이러한 체계는 보호하면서 적의 체계는 마비시키는 일, 즉 사이버전이 미래전에서 아주 중요한 전쟁의 양상으로 대두되었다

2. C4ISR체계의 역할

C4ISR체계는 표적정보 등 전술 및 전략정보를 정확하게 획득하고 인지된 정보를 빛의 속도(300,000km/sec)로 원하는 제대에 적시에 전파할 수 있는 능력을 가진다. 또한 다양하고 방대한 데이터를 실시간 분석할 수 있는 정보처리능력과 인간이 쉽게 이해할 수 있는 형태로 정보를 표현하는 능력을 가지고 있다. 이러한 능력들을 토대로 C4ISR체계가 전쟁양상을 변화시키는데 기여할 수 있는 역할을 분석하면 다음과 같다.

첫째, 실시간 상황인식 및 정보공유능력을 크게 향상시킬 것이다. C4ISR체계가 구축되면 실시간 전투상황을 인식할 수 있는 환경도 지금보다 훨씬 더 좋아질 것이다. 전장에서 전투원이 사용하는 단말기는 현재 사회에서 통용되고 있는 핸드폰보다 더 작으면서 3차원 칼라지도를 지원하고 야간작전에 필수적인 적아 및 위치식별 정보까지 심벌로 칼라지도상에 실시간 나타낼 수 있고, 지휘관에게는 전투원의 행동상황 등을 포함한 전장의 모든 정보를 전투원이 보고하지 않더라도 자동적으로 적시에 확인할 수 있는 기능을 제공한다. 필요에 따라 전장에서 발생하는 모든 정보를 수직적·수평적으로 실시간 공유할 수도 있다. 단지 실시간 정보공유 및 상황인식의 지리적 범위는 센서를 탑재한 플랫폼의 능력과 네트워크의 확장성에 좌우될 것이다. 둘째, 전장공간의 확대 및 동시성을 크게 증대시킬 것이다. 우주센서를 이용한 정찰·감시능력, 원거리 정밀타격능력, 네트워크 체계 등의 발전은 우주공간과 사이버 공간으로 전장영역을 확장하였을 뿐만 아니라 기존의

2) Admiral Owens, "The Emerging System of Systems", *U.S. Naval Institute Proceeding*, vol. 121, No. 5, (May 1995), pp. 36~39.

지·해·공 전장영역을 지리적으로 크게 확대하였다. 우주공간은 각종 정찰·감시체계뿐만 아니라 통신체계 등이 위치하는 공간으로 이들 자산의 마비는 첨단 무기체계를 중심으로 하는 전쟁수행을 불가능하게 한다.

지·해·공 전장공간의 지리적 확장과 컴퓨터 병렬처리 능력 향상은 전후방 구분이 없는 동시전투수행을 가능하도록 할 것이다. 미 공군에서 발전시키고 있는 동시병렬전(Parallel War), 해군의 협동적 교전능력(Cooperative Engagement Capability)[3], 육군의 차세대 전쟁개념(Army After Next)은 이러한 개념을 반영한 것이다.

동시병렬전은 일정한 짧은 시간이내에 적의 전략적, 작전적, 전술적 중심을 거의 동시에 압도적인 능력으로 공격하여 파괴, 마비시키는 전쟁형태이다. 특히 이는 전략적 중심을 신속하게 마비시켜 적의 전쟁의지를 조기에 굴복시키는데 주안점을 두고 있다. 동시병렬전의 목표는 적이 반응하고 복구할 수 있는 시간보다 더 신속하게 적의 중심을 공격, 마비시킴으로써 적이 공격의 충격으로부터 회복이 불가능하여 더 이상 전쟁을 수행할 수 없는 상황을 조성, 전쟁을 종결시키는 것이다.[4]

육군의 차세대 전쟁개념은 소규모 전투부대들을 전장 중심에 신속히 분산 배치(split-based operations)하여 후방에 위치하고 있는 화력수단들에게 정보를 제공, 가용한 모든 화력을 동원하여 적의 중심을 타격, 마비시키는 개념이다. 차세대 작전개념은 전장의 정보·지식에 기반을 둔 기동과 공격의 속도를 중시하고 있다. 이러한 작전은 지·해·공·우주 전력을 모두 결합하여 거의 동시에 전장에 적용함으로서 가능하다. 워게임 결과에 의하면 이러한 전쟁의 승리는 적을 물리적인 공격으로 파괴하는 것이 아니라 심리적으로 마비시킴으로서 얻어진다. 그러나 이와 같은 마비의 효과는 적이 화력의 충격으로부터 점차 벗어나고 기만, 분산 등의 전쟁방법을 체득함에 따라 급격히 약화될 것이다. 따라서 저비용으로 신속하게 승리를 거두기 위해서는 마비의 효과가 가장 큰 순간에 전쟁을 종결할 수 있어야 한다.[5]

셋째, 저비용으로 장거리 정밀타격능력을 크게 향상시킬 것이다. 시공간에 무관하게 대용량 정보를 실시간 전파할 수 있는 네트워크가 구축될 경우는 미사일의 시커(seeker)기능을 정밀감시체계가 대신할 수가 있다. 물리적으로 떨어져 있지만 전자파의 속도가 빛의 속도 ($C=3\times10^8$미터/초)와 동일하기 때문에 정밀 감시체계가 미사일에 장착된 것과 다를 바가 없다. 그러므로 미사일에 설치된 시커의 가격이 평균적으로 미사일 도입 가격의 30퍼센트 정도라고 가정한다면, 미사일 3기를 구입할 비용으로 4기를 구입할 수 있다. 또한 감시체계의 틈새 음영구역은 정밀감시체계가 탑재된 비행선이나 무인항공기 등을 네트워크에 연결하여 효과적으로 해소할 수도 있다. 미 해군의 협동적 교전능력(CEC)은 정찰·감시 장비들을 네트워크로 결합시키므로 상호 취약성을 보완할 뿐만 아니라 보다 정밀하고 신속한 정보를 획득하도록 하는 개념이다.

넷째, 효과의 집중 및 전쟁의 속도를 크게 증대시킬 것이다. 네트워크 중심의 정보전은 집중의 개념을 근본적으로 변혁시키고 있다. 산업화 시대의 전쟁은 병력과 장비의 집중을 통해서 전투효과를 최대화시키는 개념으로 수행되었다. 산업화 시대의 무기체계는 표적 탐지 및 식별수단, 화포의 사정거리 등의 제한 때문에 군사작전이 무기체계의 능력 범위에서 한정될 수밖에 없었다. 따라서 적 부대를 무력화시키고 화력을 효과적으로 운용하기 위해서는 병력

3) 협동적 교전능력은 전장의 모든 전투요소가 적아의 전장상황에 대한 정보를 공유할 뿐만 아니라 각 전투요소의 무장체계를 네트워크로 결합시켜 최적의 무장체계를 자동으로 선정, 표적을 공격할 수 있는 능력을 갖추는 것이다. 이는 표적을 탐지하여 공격할 수 있는 속도를 획기적으로 증대시키므로 먼저 보고 먼저 공격하여 전장의 주도권을 장악할 수 있도록 한다. 협동적 교전능력은 해양의 작전적, 전술적 수준의 전장환경에서 다양한 적 표적에 대하여 최단시간 내에 최적의 무장을 선정하여 가용한 전 세력이 동시에 교전을 할 수 있는 능력을 갖도록 요구한다.

4) 이론적인 측면에서 보면 동시병렬전은 다음과 같은 네가지 능력을 확보할 경우에 가능할 수 있다. 첫째, 적의 전략적, 작전적, 전술적 중심에 대한 모든 정보를 획득 가능하여야 한다. 둘째, 지휘관들은 정보화시대의 지휘통제 수단을 활용하여 신속, 정확하고 조화롭게 공격과 방어를 수행할 수 있어야 한다. 셋째, 무기체계는 적의 방어체계를 돌파하여 공격을 감행할 수 있어야 한다. 넷째, 적의 방어체계를 돌파하여 공격을 실시하는 플랫폼들은 표적을 정밀하게 타격할 수 있어야 한다. Barnett, Jeffery R., *Future War*(Maxwell Air Force Base, Alabama: Air University Press, 1996), pp. 8-12.

5) Scales, Jr., Robert H., *Future Warfare Anthology* (Carlisle, Barracks, Pennsylvania: U.S. Army War College, 1999), pp. 129-135, 145-154.

과 장비의 집중이 필연적으로 요구되었다. 그러나 미래에는 광역전장감시체계, 원거리 정밀타격체계, 네트워크 체계 등의 발전에 의하여 시간과 거리에 관계없이 전 전장의 표적을 원거리에서 정밀타격 할 수 있을 것으로 전망된다. 이는 병력과 장비의 집중이 오히려 적에게 손쉽게 탐지되어 공격받을 수 있는 기회를 부여하는 취약점만 증가시키는 결과를 초래할 수 있음을 의미한다. 따라서 네트워크 중심의 정보전하에서는 분산되어 있는 각 전투요소를 네트워크 체계로 결합시켜 화력을 집중시키고 전투효과를 최대화하는 것이 중요하다. 미군이 발전시키고 있는 동시전의 개념들은 이를 잘 반영하고 있다.

전쟁수행의 속도는 미래전의 결과를 결정짓는 중요한 요소이다. 네트워크 중심의 정보전하에서는 거리나 위치에 관계없이 거의 어떠한 표적도 정밀 타격 할 수 있는 능력을 확보할 수 있기 때문에 먼저 적의 핵심 정보자산을 마비시키는 측이 결정적으로 전장의 우위를 점할 수 있을 것으로 전망된다. 이미 설명하였던 동시전의 개념은 이를 잘 설명하고 있다.

다섯째, 전략적/작전적 정보전의 역할을 크게 증대시킬 것이다. 산업화사회에서 가장 빠른 정보전달 매체는 비행기이나 정보사회에서 보편화된 정보전달 매체는 네트워크를 통해서 빛의 속도로 전파되는 전기적인 신호이다. 미래에는 국내·외간의 무역이나 유통을 위한 행정절차는 네트워크를 통해서 전달되는 전기적인 신호에 의해서 이루어질 것이다. 이와 더불어 미래에는 가스관리체계, 송전체계 등 국가기반체계들이 네트워크에 연결된 컴퓨터에 의해서 자동적으로 통제될 수 있게 될 것이다. 그러나 여기서 간과할 수 없는 것은 편리한 만큼 위험요소도 그만큼 더 크다는 것이다. 이러한 위험요소를 유사시 활용한다면 매우 효과적일 수 있다.[6] 특히 군사적 후진국이 선진국을 공격하고자 할 때 가장 적합한 비대칭적 무기가 바로 소프트웨어 무기이다. 이것은 소수 전문가를 이용하여 개발이 가능하고 세계 어디에서나 공격이 가능한 반면에, 네트워크의 특성상 취약점이 매우 많아 침투만 한다면 사용된 기술이나 표준은 대부분 세계표준을 사용하기 때문에 쉽게 공격이 가능할 것이다. 또한 전략 정보전의 범주에 포함되는 심리전이 전쟁의 중요한 변수로 등장할 것으로 예상된다.

3. PGM의 역할

21세기에 전개될 미래 전쟁은 「미사일 전쟁」, 「우주 전쟁」, 「무인 로봇 전쟁」, 「스마트 전쟁」 등으로 불려지고 있다. 이러한 용어들은 종심·정밀 타격체계 즉, 장거리 미사일과 첨단정밀 미사일에 의한 전쟁 수행방식을 나타낸 함축어 들이다. 미사일은 2차 대전 말 독일이 영국을 공격하기 위해 개발한 V-1과 V-2에서 출발하여 눈부신 발전을 거듭하였다. 지중해의 한 가운데서 이라크 정보본부의 자료실을 정확히 공격한 토마호크나 핵탄두를 장착하고 지구 반대편으로 날아가는 대륙간 탄도탄도 모두 그 후예들이다.

21세기의 핵심 전력은 종심·정밀 타격체계 즉, 장거리 첨단정밀 미사일이다. 장사정 정밀 타격체계를 정보·감시·정찰체계(ISR)와 지휘통제체계(C4I)와 상호 연계·결합시킴으로서, 우월한 전장인식을 통하여 표적을 발견·식별하고, 임무를 할당하여 타격한 다음, 그 결과를 평가하는 일련의 전투행위 사이클(OODA loop)을 매우 신속하게 회전시킬 수 있다. 전투행위 사이클을 신속하게 회전시켜 작전템포가 빨라지면 상대가 전투 준비 태세를 갖추기 이전에 적을 기습, 공격할 수 있고 전쟁을 수행간에는 속도에 의한 시간의 지배로 주도권을 장악할 수 있다. 미래의 종심·정밀 타격체계는 장사정화가 가속화되는 추세이다. 미국 중앙정보국(CIA)의 평가보고에 따르면 세계 30개국 이상이 탄도미사일을 보유하고 있으며 북한과 이란은 5년 이내, 이라크는 10년 이내, 그리고 대부분의 국가들은 2015년이 되면 대륙간 탄도 유도탄(ICBM)을 개발 배치할 수 있을 것이라고 한다.[7] 미 국방기술목표기획서에 의하면 전술 유도탄 사거리가 2015년까지 현재의 2배로 증가될 것으로 전망되고 있다. 이러한 추세는 타격체계가 갖는 다양한 특징, 즉 탄두위력의 증대, 정밀도 향상, 스텔스화 및 요격의 곤란성 등 성능을 획기적으로 향상시켜 미래전의 양상을 근원적으로 변화시킬 것으로 판단된다.

군사혁신의 차원에서 타격체계의 사거리 증가는

6) 네트워크를 활용한 정보전은 항만을 봉쇄하기 위해 사용하는 기뢰가 적과 아군을 구분 하지 못하는 것과 같이 아측도 피해를 입을 수 있다. 그 이유는 바이러스 등 소프트웨어 무기는 특성상 네트워크만 연결되어 있으면 어디든지 동시다발적으로 매우 빠른 속도로 은 밀하게 공격할 수 있기 때문이다.

7) 권용수, "유도무기체계와 군사전략 발전방향"(국방대학원, 1999), pp. 6~8.

전장 공간을 확대시켜 적의 작전 활동을 제한할 뿐만 아니라 분산 배치된 적의 주요 작전적 내지 전략적 표적을 타격 할 수 있게 될 것이다. 장거리 타격체계는 원거리에 위치한 표적을 정확하게 타격 할 수 있기 때문에 미래의 전장은 전·후방 구분이 없어지고, 기존의 접적·선형전투는 비접적·비선형 전투로, 기존의 순차적 전투는 동시·병렬적 전투로 변화될 것이다. 이러한 작전수행 방식의 변화를 보여준 것이 코소보(Cosovo) 전쟁이다. 코소보전에서 미국의 해·공군은 유고의 방공망 밖에서 합동직접공격탄(JDAM : Joint Direct Attack Munitions)과 순항미사일 등을 사용하여 정치·군사적 목적을 달성하였다. 그 당시 미국은 무인 정찰기도 방공망 밖에서 운영하였다. 무인 정찰기(Predator) 50기를 600회 출격시켜 전천후로 정보를 획득하였고, 항공기를 1만여 회 출격시켰으나 미국의 손실은 무인기 4대와 항공기 2대에 불과했다.[8]

미래의 미사일 타격체계는 정밀도가 더욱 획기적으로 향상되어 표적을 보다 정확하게 식별 타격할 수 있을 것이다. 탄두의 위력을 2배 증가시킬 경우 표적에 대한 파괴효과는 40% 증가되지만, 정밀도를 2배 증가시키면 그 효과는 400%나 증가된다.[9] 북한을 포함한 대부분의 제 3세계 국가들의 미사일 개발 기술은 비슷한 수준이다. 사거리 1,000km일 때 정확도(CEP)는 1,000m 정도로 추정된다. 그러나 기술 선진국인 미국, 러시아, 영국 등은 탄도탄이라 하더라도 사거리에 관계없이 정확도(CEP)는 100m 미만이다. 순항유도탄의 경우 현재에도 기술 선진국들은 사거리에 관계없이 10m 정도의 정확도(CEP)를 보이고 있으나 미래에는 수 m로 줄일 수 있을 것이다. 유도탄의 정확도(CEP)가 향상되면, 표적 공격에 필요한 유도무기 수를 감소시킬 수 있다. 미국은 2015년까지 현재의 1/3로 숫자를 축소할 수 있을 것으로 예상하고 있다.[10]

미래의 미사일 타격체계는 파괴력의 효과가 더욱 증대되어 평시에는 전쟁을 사전에 예방·억제하고 전시에는 전략적 마비를 달성할 수 있을 것이다. 제프리 바넷(J. Barnett) 박사는 스텔스 크루즈 미사일 1발당 가격을 10만불 미만으로 확보할 수 있다고 하였다. 그러므로 만약 한 국가의 전략적 표적이 1,000개라고 할 경우, 1개 전략적 표적에 10발의 유도탄을 사격한다면 필요한 유도탄 수는 10,000발이 되어 미사일을 획득하는 비용은 약 10억불이 소요되므로 F-16 전투기 50대의 획득비용(약 11억불), Leopard-II 전차 300대의 획득비용(약 10.5억불), 그리고 Patriot 미사일 1개 대대 구축비용(약 12억불)보다 훨씬 저렴하고, 핵무기 개발비용(2~20억불로 추정)보다도 더 적은 액수이다.[11] 스텔스 크루즈 미사일의 위력과 전투효과를 상상해 보자. 10억불의 적은 금액으로 10,000발의 스텔스 크루즈 미사일을 적의 전략적 중심에 우박처럼 솟아부어, 동시병렬적으로 공격한다면, 이는 핵무기의 위력보다 큰 엄청난 효과를 가질 것이다. 따라서 이 경우 전쟁 억제력은 물론, 전시에는 적의 전략적 마비도 가능할 것이다.

미래의 미사일 타격체계는 각각의 핵심체계가 상호 연계·결합하여 전투의사결정 사이클을 반복, 빠른 템포로 전투력의 시너지 효과를 극대화할 수 있을 것이다. 인공 위성이나 UAV 등을 통한 광정면을 원거리까지 감시 및 정찰하여 필요한 정보를 획득하고, 지휘통제체계를 통하여 분석·판단한 다음, 그 결과를 타격체계 임무로 할당하는 일련의 사이클을 미래에는 현재보다 10배 이상 빠른 템포로 진행시켜 전투효과를 극적으로 증가시킬 수 있다는 것이다. 그러므로 이러한 종심 정밀 미사일 타격체계야말로 진정한 의미의 군사혁신 전력이라 아니할 수 없다.

III. 정보전(사이버전) 발전 추세

전통적인 정보보호는 국방, 외교 등 특수분야의 보안에 중점을 두었다. 그러나 정보통신 기반구조가 사회 전 분야에 걸쳐 확대된 지금은 새로운 형태의 위협과 파괴에 대한 폭 넓은 정보보호가 고려되어야 할 것이다.

사이버전이란 크래커, 범죄, 테러조직 또는 적국의 물리적·논리적 공격으로부터 국내 통신망을 보호하고 필요시 적대세력의 정보통신망을 공격하여

8) IISS, *The Military Balance 1999~2000*, (London : Oxford University Press, 1999), pp.288~290.
9) 육군본부, "육군 장기기획서"(육군본부: 2001), p.Ⅳ-157-97.
10) 국과연, "미래전에 적합한 유도무기 개발전략"(국과연 2000년 연구과제), pp. 288~290.
11) 권태영, 「국방정책연구」 "21세기 전력체계 발전추세와 우리의 대응방향"(KIDA, 권51, 2000 겨울)

적의 정보/시스템에 피해를 줌으로써 국가의 군사 전략을 지원하기 위한 새로운 개념의 전쟁으로 정보 우위(information Superiority) 선점 활동을 말하며 사이버 테러란 일정한 정치, 경제적 목적에 따라 행정, 금융, 항공관제, 전력 등 공공 컴퓨터 시스템에 불법 침입하여 시스템 자체의 오조작, 정지, 파괴 및 중요 정보의 불법 취득, 변경, 바이러스 투여 등을 야기하는 행위를 말한다.

사이버전을 말할 때 정보작전과 정보전과의 관계를 언급하게 되는데 미 합참에서는 정보작전(Information Operation)을 아군의 정보 및 정보체계를 방어하고, 상대방의 정보 및 정보체계에 영향력을 행사하기 위해 전·평시 취하는 행동으로 정의하고 있다. 역시 미 합참에서는 정보전(Information Warfare)을 특정한 적에 대하여 특정목표를 달성하거나 이를 진척시키기 위하여 위기시나 분쟁시에 수행하는 정보작전으로 정의하고 있다.

학자들에 따라 차이점은 있지만 미 국방대 Martin Libicki 교수의 분류에 따르면 사이버전의 위치를 정보전의 많은 유형 중 하나로 보고 있다. 즉 정보전을 〔표 1〕과 같이 구분하여 설명하고 있다.

〔표 1〕 정보전의 분류

구분	유 형	개 념
군사부문	지휘통제전	적 지휘부의 지휘의사결정 및 지휘수단 무력화 예) 걸프전시 이라크 지휘통제체계 파괴
	전자전	적의 전자통신 성능을 저하시키거나 감청 예) 재머, 채프 등
	군사정보전	전장감시체계에 대한 공격과 방어 예) 이라크군 위성을 이용한 전장감시 불능
민군중첩부문	심리전	적의 민간인, 병사, 지휘관에 대한 심리조작 예) 방송을 통한 전투참가 반대 여론 형성
	해커전	컴퓨터의 보안취약점을 이용하여 컴퓨터, 네트워크, 데이터 등을 공격 예) 유고의 미국/나토에 대한 조직적 해킹시도
	사이버전	사이버 공간에서 가상인간 사이의 분쟁 예) 컴퓨터 바이러스, 웜 등의 공격
민간부문	경제정보전	정보전과 경제전의 결합 예) 미 NSA에 의한 유럽/일본기업의 이메일 도청

1. 정보전 연구의 필요성

전통적인 정보보호와 함께 새로운 유형의 위협요인은 정보전에 관한 연구의 필요성을 대변하고 있다. 더 이상 단순히 보호를 위한 보호가 아닌 적극적인 보호로서, 자구적 적극대응의 논리인 공격력의 확보가 요구되고 있다. 또한 급속한 네트워크 대역폭의 증가와 함께 새로운 유형의 공격에 대한 침입방지시스템인 능동형시스템의 필요성을 요구하고 있다. 정보전은 적들로부터 자신의 중요 정보자원 및 정보시스템에 대해 보호하려는 측면이 강하다. 또, 적의 중요 정보자원 및 시스템에서 우위를 차지하려는 행동으로 정보 파괴, 정보흐름 변경, 정보에 대한 신뢰성 감소, 서비스 부인 공격 등이 포함된다. 정보전은 상대방의 위협에 대응하여 자신의 정보자산을 보호하기 위한 기술이며 자신의 정보통신기반구조에 대한 비밀을 보장함과 동시에 상대방의 비밀을 절취하는 기술이다. 정보전은 정보를 소유하고 있는 자로부터 정보를 얻어내는 기술이며 상대방이 자신의 기술과 정보를 사용하지 못하도록 하는 것이다. 정보전은 국가 안보 및 국가 경제 보호차원에서 전력시스템, 금융시스템, 전화망, 영공관리시스템 같은 민감하지만 비밀로 분류되지 않은 데이터에 대한 공격이 초래할 대혼란을 대비하는 영역까지 확장되고 있다. 새로운 공격에 대한 결과는 아직 알려지지 않았지만 종래의 전쟁과 비교하여 볼 때 저렴한 개발비용, 실행의 용이성, 감시/ 감지/ 추적의 어려움, 익명성 보장, 실행시 미치는 거대한 파급효과 등 그 영향력은 핵전쟁의 파괴력에 버금갈 것으로 예상된다.

2001년 2월에 발간된 미 국방부 산하의 국방위원회(Defense Science Board)의 최근 보고서의 제목은 'Protecting the Homeland'이며, 주요 내용 중 미국은 향후 핵 공격이나 생화학전보다는 현실적으로 사이버테러로 야기되는 전력·항공·가스·정보통신 등 주요 기반구조를 위협하는 테러리스트의 위협에 지대한 관심과 투자가 필요함을 밝히고 있다. 이미 전세계 20여개국은 이러한 대재앙을 몰고 올 능력이 있고, 전 세계 120여 개 나라에서 이러한 사이버 테러 준비를 하고 있다고 미CIA국장이 의회에서 증언한 바 있어서 현재의 국방정보체계(컴퓨터 시스템 및 네트워크) 및 중요 정보통신 기반(전력, 항공 시스템 등)에 대한 해킹·바이러스 공격 위협 증가에 대한 대책이 시급한 실정이다.

미국의 DISA(Defense Information Systems

Agency)가 실시한 컴퓨터 보안 시험결과, 할당된 미 국방부 컴퓨터 9,000대 중 대체로 90%는 인터넷을 통해 광범위하게 이용되는 툴을 사용하여 쉽게 피해를 입을 수 있음이 드러났다. 미 국방부 네트워크는 계속해서 거의 매일 보안 위반 사건이 생기는데, 이와 같은 사건의 95%는 네트워크 관리자의 눈에 띄지 않는 것으로 추정된다. 현 보안 전략은 공통으로 사용되는 Unix와 같은 운용 체제와 TCP/IP와 같은 네트워크 소프트웨어의 많은 고유 결함에 초점을 맞추고 있다. 이와 같은 취약점으로 말미암아 해커들이 국방부의 네트워크에 침투가 가능하게 된다. 해커들은 군용 시스템의 보호를 위한 보안 조치를 교묘하게 회피하면서 점차 새롭고 정교한 방법을 동원하고 있다. 정보전은 산업사회를 거쳐 고도 정보화 사회로 진입하면서 나타나는 새로운 형태의 위협이며 그 피해는 개인 프라이버시 침해, 국가경제위기, 사회혼란, 국가안보 침해까지 다양한 형태로 나타나기 때문에, 21세기 정보통신 고도화사회에서 정보전의 위협을 극복하고 국가적 보안체계 확립을 구축하는 일은 시급하다.

현재까지의 연구는 단순히 침입 유형에 대한 대응에 머물러 있다. 비근한 예로 현 제품으로는 미리 나올 바이러스나, 백도어의 실행을 인지하지 못하는 것이다. 또한, 침입 차단 시스템이나 침입 탐지 시스템 또한 알려진 공격에 대응하도록 구성되어 있고 하나의 도메인에 국한되어 있어서 능동적으로 대처하지 못한다. 따라서 침입이나 바이러스 등의 악의적인 공격에 대응 할 수 있는 유기적이고 조직적이며 종합적인 연구가 필요하다.

2. 주변국 정보전(사이버전) 동향

먼저 선진 주변국의 사이버전 준비 동향을 살펴보면 미국은 정보전 개념을 정보우위(Information Superiority)의 차원을 넘어서 결심우세(Decision Dominance)로 발전시키고 있고, 9.11테러 이후 사이버전/사이버테러 대응 조직을 신설하고 사이버 공간을 보호하기 위한 사이버전 전담 대통령 특별 보좌관직을 신설하였으며, 국가안보회의(National Security Council)를 분리하여 국가 사이버 보안을 논의할 본토안보회의(Homeland Security Council)를 별도로 신설하였다. 본토안보회의는 본토안보국(The House Office of Homeland Security)을 신설하여 국방부, 합참, 육·해·공군뿐만 아니라 정보체계국, DARPA 등도 상호 긴밀한 협조하에 사이버전을 대비하도록 조직체계를 구성하였다. 또한 미래 사이버전에 대비하여 체계/조직 및 전문인력을 집중 양성하고 있는데, 미 국방부는 『향후 모든 전쟁에서 사이버전 개념이 포함된 작전을 수행하기로 했다』고 발표('00. 1. 5)하고, 전담 특수요원을 양성 중에 있으며 우주전사령부에 전문가들로 구성된 사이버전 담당부서를 신설('00. 10월)하고, 『OPLAN 3600』으로 명명된 사이버 공격작전을 수립하여 체계를 개발 중에 있다. 더불어 국가안보보장협의회(NSC) 산하에 사이버안보국('01.10월) 신설하였고, 합참 산하에는 정보전 대응을 위한 부서인 JTF-CND (Joint Task Force-Computer Network Defense)를 이미 설치하여 운영 중에 있다. 또한 사이버전에 대비, 전략적 방책을 개발하기 위해 DARPA 주관으로 연간 5~10억불을 투자하여 전략적 침입평가(Strategic Intrusion Assessment), 침입 감내 시스템(Intrusion Tolerant System), 고장 감내 네트워크(Fault Tolerant Network), 자율적 정보보증(Autonomic Information Assurance), 사이버 지휘통제(Cyber Command & Control), 정보보증 과학 및 공학(Information Assurance Science & Engineering) 등을 연구 개발 중에 있으며, 컴퓨터 바이러스, EMP(Electro Magnetic Pulse), HPM(High Powered Microwave)등 신종 무기도 집중 개발하고 있다.

중국은 '컴퓨터 바이러스 침투가 원자탄 사용보다 효율적 전략'이라는 판단 하에 군사혁신 차원에서 점혈무기(點穴武器)로 집중개발하고 있으며, '97. 6월에 100명 규모의 컴퓨터 바이러스 부대를 창설하였고, '00년 하반기부터 사이버공격 및 정보교란 모의훈련을 하는 『Net Force』 부대를 운영 중에 있다. 더불어 '99년 해커부대를 창설하고, 정보전 부대를 전국에 배치('00년)하였으며, 유고전시에는 미국에 해킹을 감행하였고, 대만과도 사이버전을 수행하였다. 대만에는 72,000건의 사이버공격('00. 8)을 감행하였고, 공개되지 않은 바이러스 약1000여 개를 보유하고 있는 것으로 추정되며 논리폭탄, EMP 등도 개발하였다. 미 공군기가 자국 전투기와 충돌했던 사고('01. 5)시에도 미국과의 사이버전을 수행한 적이 있다.

러시아는 KGB 후신인 FSB내에 사이버전 전담부서를 설치, 컴퓨터 바이러스 등 사이버 무기 및 물리적 마비 무기를 개발하여 실전 배치하였으며,

FSB에서는 정보전 무기중 하나인 고출력전자파무기(HPM)를 이용하여 미대사관에 화재를 발생시킨 사례가 있다.

일본은 사이버전 대비, 바이러스와 해킹기술을 독자적으로 개발하기 위한 「사이버 부대('00년말)」를 창설하였고, 방위예산('01년)에 사이버테러 공격을 방어하기 위한 첨단 전자장비 및 관련기술 개발비용으로 1,398억 엔을 책정하는 등 정보전/사이버전 대비 노력을 강화하고 있다.

북한의 사이버전 능력을 미 국방부에서 모의 실험한 결과, 태평양사령부 지휘통제소 마비 및 미 본토 전력망에 피해를 줄 수 있는 정도로 상당 수준인 것으로 추측되고 있다. 미국은 사이버전을 수행할 수 있는 북한과 중국의 해킹능력을 미 CIA 수준으로 평가하고 있다.

선진/주변국 사이버전 동향에서 보았듯이 특히 미래전의 신종위협으로 등장하고 있는 웜 바이러스, 트로이 목마(Trojan Horse), 논리 폭탄(logic Bombs), 트랩도어(Trap doors), 칩핑(chipping), 나노 머신(Nano Machine), HPM(High Powered Microwave), EMP(Electro Magnetic Pulse) 등에 대한 대비책을 강구할 필요가 있다. 이와 더불어 상용기술과 장비들을 활용하여 체계를 구축할 경우는 표준이나 적용된 기술의 대부분이 외부에 공개되어 있기 때문에 해킹과 생존성 보장대책을 별도로 강구해야 할 것이다.

이에 대한 대비책으로 우리나라는 2001년 7월에 법률 제6383호 "정보통신기반보호법"을 제정하여 사이버테러 등 주요 정보통신 기반시설의 침해사고에 대한 예방 및 복구대책을 강구하고 있다. 정부는 정보보안 산업을 핵심 전략사업으로 육성하기 위해 정보보호기술개발 5개년 계획을 수립하고, 이를 추진하기 위해 2,777억원[12]의 예산을 투자하고 있다. 또한 사이버 대응체계를 마련하기 위해 국가정보원에 "보안 119", 검찰청에 중앙수사부, 경찰청에 사이버테러 대응센터를 설치 운영하고 있다.

사이버전에 활용되는 신종무기나 기술 대부분은 민간에 의해서 만들어지고 민간 해커들의 공격에 의해서 피해를 입고 있기 때문에 사이버무기 개발기술은 민수용을 효과적으로 활용하면 경제적으로 개발이 가능할 것으로 생각된다.

3. 정보전(사이버전) 발전추세

1991년 1월 걸프전과 '99년 4월 발칸반도의 코소보 전쟁에서 볼 수 있듯이 사이버 공간이 점차 새로운 전쟁 무대로 등장하고 있다. 프랑스 르몽드지('99. 4. 13.)는 '코소보 사태를 계기로 인터넷이 사상 처음 전쟁 무기화 되고 있다'고 보도했고 중국 인민해방군 기관지 해방군보(解放軍報)는 '99. 11. 18.자 기사에서 사이버 전쟁 특집을 게재하고 '인터넷 전쟁은 육.해.공군의 실전 작전과 똑같이 간주돼야 한다' 고 역설했다.

사이버전쟁은 전·평시를 막론하고 우방국간에도 수행된다는 것이 상식이다. 더구나 남·북으로 분단된 우리 현실에 비추어 볼 때 현존위협세력인 북한을 비롯하여 가상적국 또는 경쟁국에서 국가 기밀 및 산업 정보 수집을 위해 사이버 테러분자를 비롯한 정보전사(Info Warrior)나 네트워크 정찰자(Net Espionage)를 침투시킬 수 있다. 사이버 테러분자나 스파이는 상대국 정보통신망에 침투하여 기밀자료를 복사하거나 전산망 혼란을 야기하는 등 지상전 못지 않은 성과를 거둘 수 있다. 잘 키운 해커 1명은 10만 대군의 역할을 사이버 전선에서는 충분히 수행할 수 도 있다.

걸프전시 다국적군은 정찰위성과 공중조기경보통제기(AWACS), 표적탐지 레이다 시스템인 JSTARS 등을 이용해 1000㎞ 밖에서 바그다드 시내 30㎝ 정도의 표적까지 정확하게 보고 지휘부, 비행장, R/S 등 군사적 요충지만을 골라 정밀사격을 가했다. 이렇게 39일간 다국적군은 전혀 이라크 땅을 밟지 않고 항공작전을 펼쳐 이라크 군의 지휘·방공체계를 파괴하고 지상군을 무력화시킨 다음 100 시간의 지상작전을 수행하여 43일 만에 이 전쟁을 종결지었다. 즉 3차원의 전쟁을 펼치는 다국적군에 대항하여 1차원의 이라크 군은 전차, 항공기, 야포 등 산업시대 전쟁무기로 맞섰던 것이다. 다국적군이 정보화 지식전쟁을 했다면 이라크는 산업시대 전쟁을 했던 것이다. 걸프전은 전쟁의 패러다임이 산업사회의 기계·화학전에서 정보사회의 정보·지식전으로 바뀌고 있음을 예고한 것이었다. 이후 8년 뒤 99년 3월24일 발발한 코소보전은 이와 같은 현상을 더욱 극명하게 드러내 보였다.

12) ADD, "정보마비·보호체계 설계 및 구축방안"(2000년 연구보고서)

미군은 적의 도달거리 밖에서 지상군 투입 없이 센서체계와 지휘통제 네트워크를 기반으로 한 토마호크 미사일 등으로 유고의 군사목표를 정확하게 타격 하였으며 레이저 유도폭탄은 지하 수 십 미터 깊이에 위치한 유고의 지휘소 벙커까지 파괴했다. 이 때부터는 실제 전장과 별개로 사이버공간까지 전쟁터로 활용됐다. 세르비아가 전쟁에 대한 미국 내 여론을 악화시키기 위해 인터넷을 통해 전자우편물을 대량 보내는 정보테러를 시도했는가 하면 미군은 유고연방대통령의 외국은행 개인구좌 비밀번호를 해독해 자금줄 차단을 시도했다.

걸프전과 코소보전 뿐만 아니라 아프카니스탄 전쟁은 미래전이 정보전·사이버전쟁이 될 것임을 극명하게 보여준 사례이다. 미래의 사람들은 이들 전쟁으로부터 지식전쟁의 시대가 열렸다고 이야기 할 것이다. 정보우위를 점하기 위한 정보전을 한마디로 말하면 지식전쟁인 것이다. 최근 언론보도에 의하면 미국의 주요 도메인 루트서버에 대한 DOS공격은 지금까지 없었던 가장 강력한(최악의) 공격이라는 등 소란을 떠는 모습이 보인다. 정보전의 본질을 이해한다면 이는 지극히 상식적이고도 예상되어 왔던 일로 기술적 관점에서 보면 그렇게 소란을 떨 만큼 어마어마하거나 위협적인 일이 아니다.

군사 작전 우위 확보의 필수요건인 정보 우위는 '정확한 정보를 필요한 인원에게, 적시에, 적절한 양식으로 제공하면서도 적에게는 이와 같은 정보를 차단하는 능력'으로 정의되어 있으며 그 본질은 상호운용성과 보안성의 확보이다. 특히 최근의 정보전에 대한 대처는 이제까지와는 전혀 다른 전쟁의 양상, 즉 인적자원에 기반한 보이지 않는 전쟁, 지식전쟁, 정보우위전쟁으로서 혁명적인 군사혁신(RMA : Revolution in Military Affairs)을 요청하고 있다. 더구나 고도의 정보전을 수행하는 개인이 조직 또는 국가를 상대로 전쟁을 일으킬 수 있는 상황이 조성되었다. 정보통신 기반구조가 사회 전 분야에 걸쳐 확대된 지금은 새로운 형태의 위협과 파괴에 대한 전방위적이며 체계적인 정보보호가 고려되어야 한다. 지금까지의 침입방지와 대응체계로는 방어가 불가능하고, 상상을 초월하는 새로운 형태의 지능적인 위협들이 나타나고 있기 때문이다. 따라서 현실에 적용 가능한 정보우위 확보를 위한 구체적인 정보전의 대안은 국익과 함께 생존성의 보장이라는 측면에서 추진되어야 한다.

정보전의 본질을 두 가지로 크게 분류하여 살펴보면 다음과 같다.

첫 번째는 주로 ① 지휘통제전 ② 정보기반전 ③ 전자전과의 조합에 의한, 「신속하게 결정적으로 그리고 현저히 적은 희생자를 내도록」 실행되는 정보전이다. 이것은 지휘통제 기능 및 적외선 센서, GPS, 위성 등의 각종 센서와 정밀 유도무기 및 전자전 기능을 네트워크로 연결하여 적의 중심을 발견, 확실하게 파괴하는 것으로서 지금까지의 물량동원에 의한 무차별적인 대량 파괴와는 전혀 다른 방식의 전술적 운용 변화를 요구하고 있다. 코소보 분쟁은 모든 재래식 병력의 전력 배가 요소로 작용하는 IT에 의해 새로운 형태의 전쟁 혁명을 이룩하는 첫걸음을 내딛었다고 해도 과언이 아니다. 「신속하게, 결정적으로 그리고 현저히 적은 희생자를 내도록」하는 전쟁 개념이 미래 전쟁에서는 전적으로 구현되어야 할 뿐 만 아니라 필연적으로 요구되는 전쟁수행의 방향일 것으로 판단된다.

두 번째 정보전의 본질은 '정보 시스템'과 '정보 그 자체'를 전력으로 하여 사이버 공간에서 쌍방이 공방전을 펴는 전쟁이다. 전술한 유고 대통령 밀로세비치의 예금구좌 조작 계획과 경제정보 기반구조에 대한 마비와 교란이 여기에 해당한다. 군사적인 측면에서는 목표 데이터와 보급 데이터를 변경시켜 전술적 승리를 거두는 것과 목표 데이터를 변경시켜 오폭하도록 하여 국제 여론을 불러일으킴으로서 전략적인 승리를 거두는 것이 있다. 따라서 단 한 발의 포탄을 사용하지 않고도 목적을 달성할 수 있다는 것이다. '블랙호크 다운(Blackhawk Down)' 영화에서 보여주었듯이 미래의 전쟁은 전력의 우위가 아닌 여론에 의하여 중단되는 복잡한 상황도 고려되기 때문이다. 이 두 번째의 본질에 해당되는 것이 홈페이지의 내용변경이나 서비스 거부공격 등으로 나타나고 있으나 정확하게 모든 것을 설명하는 사례는 아직 없으며, Libicki교수 역시 앞으로 무엇이 등장할 것인지 알 수 없는 미지의 분야를 'grab bag' 이라는 용어로 표현하고 있다. 이것이 정보전에 관해 향후 우리가 가장 주목해야 할 분야이다. 지식기반의 정보전은 과거의 전쟁과 다르다. 직접적인 인명 피해가 없는 보이지 않는 정보우위에 의한 정보전은, 재래무기에 투입될 막대한 비용을 치루지 않는 인간의 지식에 기반한 전쟁이기 때문인 것이다.

4. 정보전의 한계와 문제점

정보전에는 많은 한계와 문제점들이 존재한다. 그 중 첫째는 정보 인프라에 의존하지 않는 구태의연한 사회 구조를 가진 국가에 대해 괄목할 만한 효과를 얻을 수 있을지가 의문이다. 전술한 '블랙호크 다운'이라는 영화를 통해 실상이 알려진 1993년의 소말리아 작전에서, 미군은 소말리아 반군의 지도자인 아이디드 장군의 소재를 파악하기 위해 최첨단의 무기에 의존한 것에 반하여 아이디드 장군 휘하의 부대는 연락 수단으로서 기술수준이 매우 낮은 워키토키와 '토킹드럼'이라 불리는 북을 사용하고 있어 최첨단의 무기를 갖추었다 하더라도 소재 파악엔 전혀 쓸모가 없었을 뿐만 아니라 기술력의 차이가 역설적으로 미군에게 불리하게 작용한 결과를 초래하였다. 수준의 차이로 인해 상호운용성을 기대할 수 없거나, 다른 운영체제를 사용하는 적군에 대해 가질 수 있는 정보 우위는 상대적 입장에 의해 효과성에 의문을 가지게 만들기 때문이다. 이는 정보전이 극복해야할 하나의 과제이자 도전사항이다.

두 번째는 국제법, 윤리 도덕적인 문제이다. 국경을 초월하여 민간인에게 크게 관련되어 있는 사회기반과 경제기반에 대한 공격이 허용되는가 하는 것이다. 정보전은 어떤 형태로든 민간과 연결되어 있다. 미군의 일상생활중에 통신의 90% 이상이 민간통신망을 이용하고 있다고 한다. 정보화 시대의 교육에 윤리교육이 필요하다고 제언하고 세계경찰임을 자임하고 나서는 미국 스스로가 밀로세비치의 은행구좌 예금을 조작하는 등의 계획을 실행에 옮기기 위해 국제법과 윤리적인 문제를 검토한 결과, 그 실행을 단념하지 않을 수 없었다고 전해지고 있다.

세 번째는 전쟁행위인지 범죄행위인지의 경계가 모호하다는 점이다. 국가에 의한 전쟁행위인가, 단순한 개인에 의한 범죄행위인가를 구별하는 일이 어렵고 지리적인 것도 포함하여 경계가 모호하다. 1994년 3월 23일 미국 롬 연구소에 대한 공격으로 시작된 그 유명한 '데이터스트림·카우보이' 사건은 결국 16세의 소년에 의한 장난으로 밝혀졌으나, 전쟁행위가 아닌가 하고 한동안 미 공군을 떨게 만들었다. 이 사건은 한 소년이 한국의 모 연구소에 침입하여 데이터를 롬 연구소에 다운로드한 것이었는데, 미군 관계자는 이 연구소가 북한에 있다고 착각하고 이것이 '북한에 의한 전쟁행위라 판단할 수 있는 소지가 있다'고 여기고 극도의 긴장 상태가 펼쳐진 사건이었다.

마지막으로는 군사력 강행이 용이해진 점이다. 아프카니스탄 전쟁의 사례(센서와 정밀 유도무기에 의한 고도의 정밀 공격)와 같이 IT 등의 기술혁신이 전쟁이라는 상황에서 지도자로 하여금 군사력 행사를 쉽게 결행하도록 하는 요인이 아닌가 하는 점이다. 생존과 인류의 미래에 대한 더 많은 고민없이 바로 군사력을 동원할 수 있다는 자만감으로 해석될 수도 있는 정보우위는 궁극적으로 지탄의 대상이 될 수 있다는 것이다.

정보전은 과거의 교훈을 삼을 만큼의 충분한 역사를 가지고 있지 않기 때문에 한계와 문제점이 점차 많은 영역에서 나타날 것이다. 그러나 이는 오늘의 전쟁이자 미래의 전쟁이기 때문에 궁극적으로 극복되어갈 것이다.

IV. 결 론

강대국의 틈바구니 속에서 어떻게 우리의 미래를 대비할 것인가? 미래를 준비하는 방안으로 본고에서는 미래 디지털 전쟁의 핵심인 C4ISR/PGM복합체계 구축의 필요성과 비대칭 전력으로 선진국에서 강력하게 추진하고 있는 정보전(사이버전)에 대한 고찰을 통해 우리의 미래 대비방안을 제시하였다.

미래전은 네트워크기술의 발전으로 센서체계와 타격체계가 C4I체계를 이용하여 상호 결합, 적보다 우세한 정보력과 공격능력을 활용하여 전쟁에서 승리를 쟁취하는 방향으로 전쟁양상이 바뀌고 있다. C4ISR/PGM체계 등 정보전력체계는 미래전의 핵심전력으로 이러한 체계를 보유하지 않고는 전쟁수행 자체가 곤란할 수도 있다. 따라서 열악한 우리나라의 여건에도 불구하고 지혜를 모아 단기간에 경제적으로 원하는 수준의 정보전력체계를 확보할 수 있도록 방책을 개발하여 적극 추진해야 할 것이다.

C4ISR/PGM체계 구축과 더불어 사이버 디지털 전쟁으로 총칭되는 미래전에 대비하기 위해서는 정보전(사이버전)에 적극 대비를 하여야 하겠다. 컴퓨터 바이러스, 웜(Worms), 트로이 목마(Trojan Horses), 논리폭탄(Logic Bombs), 트랩도어(Trap Doors), 하드웨어 칩에 이상기능(Malfunction)을 첨가하는 행위, 컴퓨터 하드웨어의 고장을 야기 시키는 소위 나노머신(Nano Machine)으로 분류되는 초소형 로봇, 전파방해 및 전자 목표물의 기능을 마비시키는 고출력 무선주파수 총(High Energy

Radio Frequency Gun), 강력한 자장으로 전자 목표물을 마비시키는 EMP(Electro Magnetic Pulse) 등 새로운 정보전을 위한 각종 정보전자전 체계에 능동적이고 효과적으로 대응할 수 있는 체계를 개발, 발전시켜야 하겠다.

미래전의 핵심인 C4ISR/PGM체계 구축과 사이버전에 대비하기 위해서는 군은 국가차원의 중장기 플랫폼 개발계획에 적극 참여하여 군의 요구시기와 성능을 만족하는 체계가 개발되도록 해야할 것이다. 즉 제한된 예산속에서 효과적으로 핵심체계를 구축하기 위해서는 국가차원에서 구축중인 플랫폼을 사전 협조속에 적극 활용하고, 군은 핵심기술/부품 개발에 주력하여야 할 것이다. 특히 성층권비행선, 무궁화위성, 다목적위성, 우리별위성 등 군용으로 활용 가능한 상용체계들은 군의 소요시기와 연계하여 개발될 수 있도록 국가차원에서 조정통제하거나 필요시 민·군 겸용예산 등을 지원하여 개발을 독려할 필요가 있을 것이다. 이러한 플랫폼에 우리군이 개발한 EO/IR/SAR등 센서체계와 정보고속도로를 구축하기 위한 통신중계기를 생존성이나 보안성의 문제를 고려하여 탑재한다면 별도의 국방예산을 들이지 않고, 적은 비용으로 경제적인 C4ISR 체계를 구축할 수 있을 것이다.

더불어 향후의 무기체계 도입은 가능한 국외 직도입을 피하고, 우리의 국내기술을 이용하여 체계를 구축해야할 것이다. 향후 Sensors to Shooters를 실현할 수 있는 전술데이타링크 체계의 경우, 복잡한 기존 무기체계에 통합의 어려움이 있지만 국내기술을 이용하면 개발시 낮은 가격으로 안정적인 조달이 가능하고, 정보통신기술을 이용하는 무기체계는 발전속도가 빨라 빈번한 업그레이드가 요구되는데 이로 인한 추가비용을 줄일 수 있고, 선진 무기체계의 종속을 피하며 독자적인 체계를 구비할 수 있는 장점이 있을 것으로 생각된다. 상용 및 군용 플랫폼을 이용한 지상 및 공중의 정보고속도로 구축도 재밍 및 보안성을 고려한 통신중계기를 개발/탑재한다면 군은 경제적으로 구축이 가능하고, 민간부문에는 기술축적 및 타분야 파급효과가 지대할 것이다. 또한 군 차원에서는 상용체계와 기술의 표준을 고려하여 국방 표준을 지정토록 하여 추가 개선 보완없이 상용장비 및 기술들을 도입과 동시에 활용할 수 있도록 해야할 것이다. 체계표준을 통한 상호운용성 확보는 가장 저렴한 가격으로 체계를 통합할 수 있는 최적의 방법이다. 또한 민군위성 사업처럼 체계개발 초기부터 공동 참여하여 군의 요구가 반영되도록 체계를 개발할 필요도 있을 것이다. 특히 생존성 및 신뢰성을 보장하기 위한 분야는 적극 참여해야 한다. 왜냐하면 개발이 완료된 후 군의 요구에 적합한 체계로 개선 보완하는 것은 체계를 개발하는 것 수준으로 예산이 투자될 수도 있기 때문이다.

변화는 예나 지금이나 있어왔지만 지금의 우리는 변혁의 소용돌이 속에 살고 있다. 급변하는 시대의 소용돌이 속에서 새로운 방식으로 새로운 행동을 취하는 길만이 생존의 유일한 방법인 시대에 지금 우리는 살고 있는 것이다.

참 고 문 헌

[1] 국방과학연구소, "광역전장감시체계 설계 및 구축방안", 2000.

[2] 국방과학연구소, "상용 이동통신기술을 이용한 군 초고속 대용량 종합정보통신체계 개략설계", 2000.

[3] 권태영, 정춘일, "미국의 군사혁신(RMA/MTR) 발전추세", KIDA, 1996.

[4] 권태영, 정춘일, "선진국방의 지평", 을지서적, 1998.

[5] 권태영, "한국의 군사혁신 개념과 접근전략," "국방연구", 제42권 제1호, 1999.

[6] 육군교육사령부, "NATO의 유고공습 분석", 1999.

[7] 이병기 외 다수, "광대역정보통신", 교학사, 1994.

[8] 전자통신연구소, "상용 이동통신기술을 이용한 군 초고속 대용량 종합정보통신체계 개략설계", 2000.

[9] 전자통신연구소, "상용차세대 이동통신기술을 이용한 한국형 JTIDS연구", 2000.

[10] 전자통신연구소, "정보전에 대비한 정보·마비 보호체계구상에 관한 연구", 2000.

[11] 주성환, "우리개발사업과 미래세계", 진한도서, 1999.

[12] 한국국방연구원, "신세기 정보사회의 새로운 군사 패러다임", "국방정책연구", 제47호, 1999.

[13] 황정섭, "네트워크 중심전 양상 분석", 전략문제연구소, 2000.

[14] Albert, David S. and Others. *Network Centric Warfare: Developing and Leveraging*

Information Superiority. Washington DC : DoD C4ISR Cooperative Research Program. August 1999.
[15] Braken Paul. *The Military After Next. The Washington Quarterly*. Autumn 1993.
[16] G. Maral, M. Bousquet. *Satellite Communication Systems*. John Wiley & Sons INC. 1994.
[17] Jeffery R. Barnett. *Furture War An Assessment of Aerospace Campaigns in 2020*. Air University Press. 1996.
[18] Mark A. Stokes. *China's Strategic Moderenization; Implications for The United States*. U.S Airforce. 1999.
[19] Michael Pillsbury. *Chinese Views Of Furture Warefare*. National Defense University Press. 1996.
[20] Richard O. Hundley. *Past Revolution Future Transformations*. RAND.

〈著 者 紹 介〉

강 태 원(Taewon Kang)
1984년 : 공군사관학교 졸업(공학사)
1994년 : 연세대학교 전자공학과 졸업(공학석사)
1998년 : 연세대학교 전자공학과 졸업(공학박사)
1984년~1986년 : 공군 31전대 전시반장, 주장비반장, 통제반장
1987년~1988년 : 공군 31전대 통신중대장, 정비중대장
1989년~1991년 : 공군 작전사령부 통신담당
1998년~2000년 : 국방부 정보화기획관실 정보화정책담당, 정보기술담당
2000년~현재 : 국방부 개혁위원회 군사혁신단 전력체계담당

황 정 섭(Jeongseop Hwang)
1980년 : 해군사관학교
1987년 : 한양대학교(공학사)
1990년 : Naval Postgraduate School(공학석사)
1995년 : 한양대학교 대학원(공학박사)
1991년~1992년 : 1함대사령부
1995년~1995년 : 해작사 정보통신단
1995년~1999년 : 국방부 정보체계국
1999년~1999년 : 해군전투발전단
1999년~2002년 : 국방개혁위 RMA단
2002년~현재 : 국방과학연구소