J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

사이버공간에서의 효과중심작전 적용방안 연구☆

A study on the Application of Effects-based Operation in Cyberspace

장 원 구[1] 이 경 호[1*]
Won-gu Jang Kyun-ho Lee

요 약

전쟁 수행간 유발되는 불필요한 노력과 무의미한 희생을 줄이는 동시에 전략적인 공격으로 적 지도부의 의지에 닿을 수 있는 효과중심작전은 항공력이외의 군사력에 적용이 어려운 이유로 폐기되었다. 하지만 철저히 논리적이고 계산될 수 있는 사이버공간은 효과중심작전 수행에 적합하다고 할 수 있다. 본 논문에서는 이러한 사이버 공간에서 효과중심작전을 수행할 수 있는 방안을 연구하였다. 과거의 전쟁사례에서 드러난 효과중심작전의 한계를 극복하고 물리공간과 사이버공간의 경계가 점차 없어지는 사이버전장공간에서 효과중심작전 수행을 위한 토대를 마련하였으며 과거 사이버공격사례를 분석하여 효과중심작전을 수행할 수 있는 군사전략을 수립함으로써 사이버공간에서 효과중심작전이 수행 가능함을 증명하였다.

☞ 주제어 : 효과중심작전, 사이버 공간, 사이버 공격, 5 전략동심원 모델, 병렬전쟁

ABSTRACT

The effects-based operation, which would reduce unnecessary efforts and meaningless sacrifices incurred during a war and simultaneously reach the will of the enemy leadership by strategic attacks, was discarded for the reason that it was difficult to apply it to military power except for airpower. However, cyberspace, which can be thoroughly logical and calculated, can be suitable for conducting effects-based operations. This study examined a way to carry out effects-based operations in such cyberspaces. It laid the foundation for overcoming the limitations of effects-based operations revealed in previous battle cases and executing the operations in cyber battlespace where the boundary between physical and cyberspaces gradually disappeared. Futhermore, it demonstrated that effects-based operations could be carried out in cyberspace by establishing a military strategy, which could conduct the operations through an analysis of previous cyber-attack cases.

☞ keyword : Effects-based Operation, Cyberspace, Cyber attack, Five Strategic Rings Model, Parallel Warfare

1. 서 론

전쟁은 동서고금의 역사 속에서 종족의 생존을 보장하고 사회집단의 정치적 목적을 달성하기 위하여 수행되어 왔는데 주로 물리적인 폭력을 이용하여 인명과 장비에 대한 손상, 살상을 유도함으로써 적의 핵심전력을 무너뜨리고 최고 권력자의 의지를 상대방에게 강요하기 위한 도구로 사용되어서 전쟁 수행간의 폐해는 상상을 불허할 정도였다. 전쟁을 수행하기 위해서는 전략과 전술을 바탕으로 군사력을 효과적으로 사용하여 원하는 군사적 목표를 달성하고자 하는데 과거에는 전투원과 비전투원을 구분하지 못하는 대량의 피해를 유발하는 것이 일반적이었다. 하지만 현대전에서는 정밀유도무기, 스텔스 기술과 같은 첨단 기술을 동원하여 불필요한 인명과 장비의 손실을 줄이고 신속히 원하는 군사적 목표를 달성함으로써 전쟁을 조기에 종결하고자 하는 움직임이 일었다. 이것은 1991년 걸프전에서 미국이 항공력을 이용하여 이라크에 대한 전략표적들만을 빠른 시간 안에 공격하는 방식으로 수행되었는데 바로 항공력을 중심으로 하는 효과중심작전(EBO : Effects-based Operation)에 의한 것이었다. 하지만 당시 육·해·공군력의 입체전 환경 하에서 이 작전개념은 철저히 계산되어지고 계획되어질 수 있는 항공력에서는 효과적이었으나 지상군에서는 모호하고 적용이 어려웠으며 특히 정규전과 비정규전이 혼합되는 아프카니스탄 전과 같은 4세대 전쟁에서는 적합하지 않은 것으로 드러남에 따라 2008년 공식적으로 폐기되고 효과중심작전 관련 군사이론들을 부분적으로만 활용하는 방식으로 기존의 합동작전계획 수립절차를 보완하였다. 본 논문에서

1 Graduate School of Information Security, Korea University, Seoul, 02841, Korea
* Corresponding author (kevinlee@korea.ac.kr)
[Received 18 November 2019, Reviewed 21 November 2019(R2 10 December 2019), Accepted 23 December 2019]
☆ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다.(UD190016ED)

는 이러한 효과중심작전을 사이버공간에서 적용하고자 한다. 사이버 공간은 수많은 노드들로 이루어진 가상의 공간으로서 인간에 의해 창조된 공간이다. 또한 컴퓨터와 네트워크를 이용한 사용자들 간의 소통과 참여의 공간이며 사회활동이 가능한 공간이자 사이버전이 발발하는 전장의 공간이다. 따라서 이러한 사이버공간에서 전쟁수행간 효과중심작전을 수행할 수 있는지에 대한 분석을 통해 불필요한 노력과 피해를 최소화하면서 적의 의지에 영향을 줄 수 있는 방안을 모색하고자 한다.

본 논문에서는 제 2장에서 효과중심작전과 관련된 선행연구와 관련 이론들, 그리고 연구방법을 알아본다. 제 3장에서는 사이버공간에서 효과중심작전을 적용하기 위한 전제요건들과 과거 사이버공격사례를 선정, 분석하여 효과중심작전을 수행할 수 있는 군사전략을 수립한다. 제 4장에서는 연구결과를 요약하고 향후 연구 과제를 도출한다.

2. 선행연구, 관련이론과 연구방법

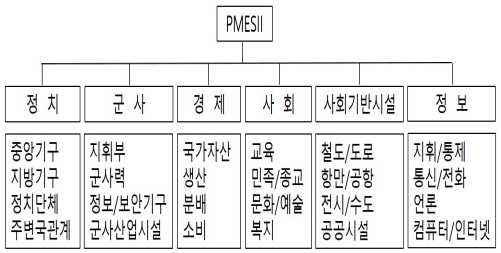
2.1 선행연구

효과중심작전은 적 군사력에 대한 파괴보다는 전략적·작전적 효과달성에 중점을 두고 적의 의지와 응집력에 대한 공격을 우선시하는 작전방식으로서 군사·비군사적 조치로 인해 발생하는 결과나 사건 또는 산물을 포함한다. 효과중심작전 관련 연구로서 Millan N. Vego[1]은 효과중심작전을 본질, 목표에 대한 접근방법, 계획 수립 및 실행, 효과평가 등 다양한 측면에서 비판적 견해를 제시하였고, 전덕종[2]은 전쟁의 본질에 대한 분석을 바탕으로 효과중심작전을 이론적으로 분석, 비판하고 그 한계점을 명시하였다. 전광호[3]는 제2차 레바논 전쟁에 대한 분석을 바탕으로 효과기반작전이 단독으로 승리나 실패를 가져오지 못한다고 주장하면서 지상군 역할의 재인식을 주장하였다. 백두현[4]은 효과중심작전에 대한 이해를 통하여 한국군 합동작전 수행개념의 발전방안을 모색하였다. 이처럼 효과중심작전은 전쟁에서 완벽한 작전수행개념은 아니지만 그 나름의 효용성을 가지고 있음을 시사하고 있다. 따라서 본 논문에서는 현재 그리고 앞으로의 사이버 공간에서 효과중심작전이 어떻게 적용될 수 있는가에 대한 연구를 시행함으로써 그 실용성과 한계점을 파악하고자 한다.

2.2 관련이론

2.2.1 복합체계 분석

효과중심작전을 수행하기 위해서는 적에 대한 복합체계분석(SoSA : System of Systems Analysis)이 선행되어야 한다. 복합체계분석은 그림 1과 같이 적을 정치, 군사, 경제, 사회, 정보, 기반시설의 6가지 체계(PMESII: Political, Military, Economical, Social, Information, Infrastructure) 속에서 분석하여 각 체계의 특성과 강·약점, 체계를 구성하는 노드와 노드간의 상호작용을 분석하여 지식기반을 구축하는 작업을 말한다. 이러한 심층적이고 종합적인 분석을 통하여 적을 이해한 상태에서 언제, 어디에, 어떤 조치를 취할 것인지를 결정하는 것이다.



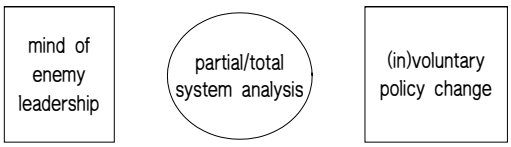
(그림 1) 효과중심작전을 위한 복합체계 분석[5]
(Figure 1) System of Systems Analysis for EBO[5]

2.2.2 5 전략동심원 이론[6]

미국 예비역 공군 대령 John A. Warden이 걸프전에서의 경험을 바탕으로 제시한 5 전략동심원 모델(Five Strategic Rings Model)은 전쟁을 물리적 요소와 심리적 요소의 결합체로 인식하고 적을 유기체적인 관점에서 전략적으로 분석하여 5개의 동심원 형태로 구성되어 있다고 생각하였는데 가장 바깥에서부터 군대, 시민, 하부구조, 핵심체계, 지휘부로 이루어져서 최외곽에 있는 군대가 시민부터 가장 핵심요소인 지휘부까지를 보호하는 형태로 생각하였다. 이러한 관점은 적의 중심(COG: Center of Gravity)을 신속정확하게 파악할 수 있게 해주고 각 체계간의 중요도를 파악하는데 유용하였다. 또한 이러한 시각은 접적지역에서부터 차례로 영토를 점령해서 지휘부로 진격해 나가는 과거의 군사전략, 전술과 달리 항공력과 원거리 정밀무기를 이용해서 적 지휘부를 포함한 모든 전략적 표적들을 동시에 공격함으로써 전략적 마비를 추구할 수 있는 병렬전쟁을 수행할 수 있게 하였다.

2.2.3 병렬전쟁[6]

병렬전쟁은 다양한 범주의 표적을 동시에 일제히 공격하여 적이 재정비, 재배치할 시간을 주지 않고 마비효과를 창출하여 단기간 내 전쟁을 종료하는 새로운 작전방식으로 적 시스템의 유기적 능력을 손상·와해·마비시킴으로써 적의 전쟁수행의지를 파괴하는 데 있다. 즉, 그림 2와 같이 적 지휘부의 심리적 변화를 목표로 5 동심원 체계의 모든 중심을 정확히 식별하여 공격함으로써 국가전체를 순식간에 마비, 무력화하여 자발적, 비자발적 변화를 유도하는 개념이다. 병렬전쟁은 정보·감시·정찰 능력의 비약적 발전과 이로 인한 지휘통제능력의 향상, 스텔스 기술과 우수한 전자전 능력, 그리고 정밀타격수단의 발달에 기인한 것으로서 그 잠재능력은 미래로 갈수록 더욱 증대할 것이다.



(그림 2) Warden의 전략적 공격이론[7]
(Figure 2) Warden's Theory of Strategic Attack[7]

2.2.4 신속결정작전[6]

신속결정작전(RDO: Rapid Decisive Operations)은 걸프전 이후 미국 합참에서 발전시킨 합동작전 개념으로 적이 예상치 못한 시간과 장소에 비대칭 전력을 포함한 합동 전력을 동시적·병렬적·비선형적·비대칭적으로 운용하여 적을 신속하고 결정적으로 격멸하는 작전이다. 기존 작전이 시간·공간·제대별로 축차적, 점진적, 선형적, 대칭적으로 수행되는 반면 신속결정작전은 동시적, 병행적, 비선형적, 비대칭적으로 수행된다. 또한 이전의 작전이 소모전 중심, 부대 중심으로 수행되는 반면 신속결정작전은 효과중심, 응집력 공격 중심으로 수행된다.

2.3 연구방법

사이버공간에서 효과중심작전을 적용하기 위해 먼저 사이버공간의 생성과 근본적인 속성을 이해하고 국가를 대상으로 한 사이버공격의 특성을 이해한다. 다음으로 과거 사례에서 드러난 효과중심작전의 한계가 사이버공간에서 어떻게 극복될 수 있는지 그리고 이에 관련된 기술들은 무엇이 있는지 알아보고 사이버공간에서 효과중심작전을 수행하기 위해 필요한 전제들을 마련한다. 다음으로 그 전제들에 적합한 과거의 사이버 공격사례를 선정하여 분석한 후 실질적으로 효과중심작전이 수행 가능한 가상의 군사전략을 수립한다. 마지막으로 사이버공간에서의 효과중심작전이 가지는 한계점을 파악한다.

3. 사이버공간에서의 효과중심작전 수행

3.1 사이버전장과 사이버 공격작전

3.1.1 사이버전장

사이버 공간은 미 고등연구계획국(DARPA)에서 시작한 것으로 전장상황 하에서 물리적으로 이격된 공간에 정보를 실시간으로 공유하기 위해 컴퓨터들을 네트워크로 연결하는 방안을 모색하기 위한 연구에서 비롯되었다. 여기서 컴퓨터는 계산기에서 출발한 것으로 1936년 앨런 튜링이 인간의 사고방식을 본 뜬 최초의 개념적 컴퓨터 'Turing Machine'을 바탕으로 완성한 것이다. 이후 오늘날의 노트북, 스마트 폰까지 많은 변화를 거쳤지만 아직까지 대부분의 컴퓨터는 0, 1을 바탕으로 하는 논리적인 처리방식을 유지하고 있다. 이후 이러한 컴퓨터들을 연결하기 위한 유무선 네트워크 장치들이 개발되고 프로토콜이 적용됨으로써 사이버공간은 만들어지기 시작하였다. 따라서 사이버공간은 본질적으로 논리적이고 계산적인 공간이며 무수히 많은 노드가 생성, 소멸되는 변화와 확장을 무한 공간이다. 사이버공간을 공중공간과 비교해보면 표 1과 같다. 공중공간에서는 조종사가 탑승한 항공기가 모기지에서 군수지원을 받아 공중공간으로 이동하여 정밀무장을 발사하지만 사이버공간에서는 공격자가 네트워크상의 한 지점에 접속하여 알고리즘을 근간으로 하는 사이버무기를 명령어를 통하여 실행하면 통신라인 상의 패킷이나 전자기파 형태로 전달되어 적의 네트워크나 시스템 등에 손상을 주거나 데이터를 탈취하는 것이다. 이때 항공기가 지형지물, 스텔스 기술을 이용하여 적 레이더에 잡히지 않는 것처럼 사이버 공격무기도 공격자의 IP 주소를 위장하거나 적의 탐지 알고리즘에 잡히지 않는 알고리즘으로 운용되는 것이다. 공중공간에서 전투 간 유발될 수 있는 효과는 Destroy, Degrade, Deny, Disrupt 4가지이나 사이버공간에서는 여기에 Deceive가 추가된다.

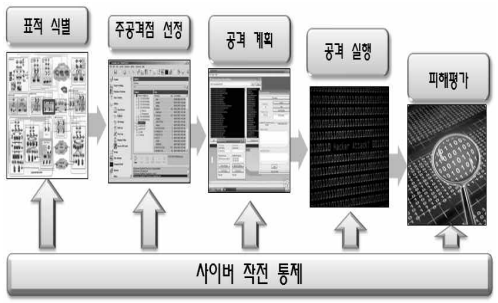
(표 1) 공중부문과 사이버 부문에서의 전투 비교[8]
(Table 1) Battles in air domain versus battles in cyber domain[8]

Character-istic	Air domain	Cyber domain
Vehicles	Unmanned aerial vehicles(UAVs)	Network protocols
Flight medium	Air	Physical wires, electromagnetic waves(ground, air, space)
Weapons	Missiles, bombs	Algorithms
Desired effect	Destroy, degrade, deny, disrupt(D4)	Destroy, degrade, deceive, deny, disrupt(D5)
Control	Pilot (on-board or remote)	Network links that support enemy air, space, ground movements as well as vehicles on-board algorithm
Low probability intercept	Stealth (physical)	Stealth (software)
Low probability detection	Terrain Masking	Network masking
Home base	Predetermined airfield	Any cyberspace portal
Logistics	Heavy, continual	Ranges from heavy/continual to light/infrequent

다음으로 사이버공간은 심리적, 인식적 공간이다. 물리공간에서 사람은 객관화되고 대상화된 자신을 이용하여 다른 수많은 사람들과 소통하고 교류하며 사회활동을 지속해 나간다. 하지만 사이버 공간에서는 사람들이 특정한 시간과 장소에 모여 얼굴을 맞대고 대화하는 것이 아니며 컴퓨터 모니터 위에 투영된 모습을 통해 사이버공간에 있는 존재들을 인식한다. 이때 이러한 것들을 가능하게 해주는 것은 키보드를 통해 전달된 자신의 정보가 컴퓨터와 네트워크를 통해 사이버공간 저 너머에 있는 상대방에게 전달되고 그 대상이 정보에 대한 반응을 보냄으로써 서로 소통하고 있다고 인식하게 되는 것이다. 이러한 행위의 확장은 소셜네트워크 서비스의 발달로 이어져 사이버공간에서 다양한 주제에 대한 논의와 교류가 활발히 이루어 질 수 있는 장을 마련하였고 이러한 관심과 교류의 정도를 확인하는 방법으로는 실시간 검색어 순위나 빅데이터 분석을 통하여 가능하다.

3.1.2 사이버공격

해킹은 최초에는 호기심과 재미로 시작되었지만 비대면성, 익명성, 시간과 공간상의 장애 제거 등 사이버공간의 특성과 결합된 파급력과 효과를 알게 됨으로써 점차 범죄의 성격을 띠게 되었고 이제는 사회 기반시설을 마비시키거나 국가를 뒤흔들 정도의 공격도 발생하고 있어 사회적인 혼란을 유발하거나 공포심을 자극하기에 충분한 힘을 가지고 있다. 그 근본적인 원인은 사이버 공간이 처음부터 공간자체를 지키고 방어하는 기능을 포함해서 설계된 것이 아니기 때문이며 이에 따라 사이버범죄, 사이버테러와 같은 다양한 위협에 대응하는 보안대책이 마련되고 있는 실정이다. 따라서 고도로 숙련된 해커일수록 기존에 알려지지 않은 취약점을 이용하여 공격할 가능성이 높으며 사이버 공격에 드는 시간과 비용은 일반적인 물리공격에 비해 저렴한 반면 효과는 매우 좋은 편이다. 해킹절차는 보통 공격대상에 대한 정보 수집을 통해 취약점을 공격하고 그 흔적을 지우는 형태이지만 국가에 대한 사이버 공격은 일반적인 해킹과 달리 좀 더 군사전략, 전술적인 측면이 강조된다.



(그림 3) 사이버 작전계획[9]
(Figure 3) Cyber realtime sensor to shooter[9]

3.2 효과중심작전의 한계 극복

3.2.1 과거 사례에서 드러난 한계 극복

효과중심작전을 수행하기 위해서는 먼저 적에 대한 복합체계 분석으로 많은 정보를 수집해서 완벽히 분석해야 하는데 이는 현실적으로 매우 힘든 일이다. 둘째, 효과중심작전은 물질적 요소와 심리적 요소를 동시에 고려해야

하는데 걸프전과 같은 과거 사례에서는 전략표적과 같은 물질적인 요소에만 치중하고 심리적인 요소를 등한시 하였다. 셋째, 효과중심작전을 실행하기 위한 효과설정, 실행계획 수립, 시행 및 효과평가의 과정은 매우 복잡하고 작전환경 변화에 대한 계산이나 측정이 어려웠다.[1][2] 이에 대해 사이버 공간은 근본적으로 열린 공간으로서 간단한 검색만으로도 상대에 대한 많은 정보를 알 수 있다. 또한 앞서 언급한 바와 같이 사이버공간에 대한 알려지지 않은 수많은 취약점들이 존재할 수 있으며 보안의 가장 취약한 요소인 사람에 대한 공격으로도 많은 정보를 얻어낼 수 있다. 두 번째로 사이버 공간에서 활동하는 이들의 심리나 관심사항 등은 간접적으로 측정할 수 있는 다양한 방법이 있다. 예를 들어 트위터와 같은 SNS 서비스에서는 공개된 자료를 이용하여 사회적 현상에 대한 관심도를 빅데이터를 이용하여 측정할 수 있고 대형포탈 사이트에서 제공하는 실시간 검색순위 기능은 접속자들의 관심사를 연령별, 주제별로 다양하게 알아볼 수 있다. 그 외에도 인터넷 뉴스에 대한 기사분석을 통해 사회적인 영향력을 알 수 있다. 셋째, 이러한 것들을 포함하여 상이버공간 상의 모든 것들은 모두 수치화될 수 있어서 원하는 효과가 나타났는지 또는 다른 사건과 연계적인 효과가 있는지는 지속적으로 발전하는 컴퓨팅 능력과 기술들을 이용하여 알 수 있으므로 사이버 공간상에서의 효과중심작전은 가능한 것으로 판단할 수 있다.

3.2.2 효과중심작전 수행을 위한 관련 기술들

효과중심작전을 수행하는 사이버 공간은 앞서 언급한 바와 같이 기존의 물리공간과는 매우 다르다. 사이버 공간은 시간과 물리적인 공간의 개념이 없으며 가상의 공간으로서 네트워크화 된 컴퓨터들 사이를 데이터가 이동하면서 사용자들에게 노출되어 그들의 인식에 영향을 미칠 뿐이다. 뿐만 아니라 네트워크를 오가는 데이터 외에도 각 종 기기들의 접속기록, 사람들의 생활기록 등이 실시간으로 기록되고 사물인터넷과 4차 산업혁명이 현실화됨으로써 이들의 기록 등 무한한 빅데이터들이 만들어지고 있다. 따라서 이러한 빅데이터들을 처리할 수 있는 기술도 같이 발전하여 기존의 인력이나 제한된 컴퓨터 자원에서 하던 일들을 계속 발전되는 컴퓨팅 능력과 인공지능 기술을 이용하여 처리할 수 있게 된 것이다. 따라서 기존의 물리전장에서의 효과중심작전의 한계 중 하나였던 복잡하고 많은 시간이 소요되는 효과기획, 분석, 평가 작업 또한 보다 수월하게 된 것이다.

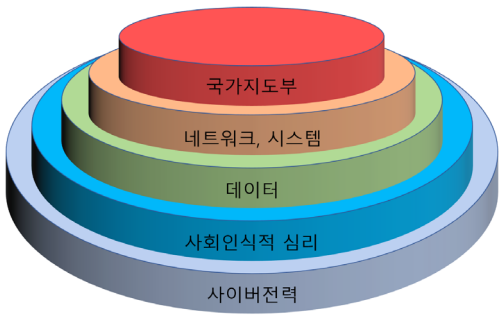
3.2.3 사이버공간 변화

사이버공간은 컴퓨터의 탄생과 이들의 네트워크화에서 비롯되었으며 무선통신기술과 휴대용 장비의 발달로 급격히 팽창하기 시작했다. 현재 사물인터넷과 4차 산업혁명 시대를 맞아 다시 한 번 폭발적인 성장을 예고하고 있다. 이에 따라 사이버공간은 향후 세상의 모든 사물을 연결하여 보다 지능화하는 초연결, 초영역, 초지능의 공간이 될 것으로 예상된다. 네트워크로 연결되는 순간 모든 것들이 사이버공간으로 합쳐질 것이며 이러한 것들이 급격히 확대됨으로써 송수신되는 정보 또한 확장될 것이며 양 끝단까지 동시성을 강화할 것이다. 이러한 변화는 사이버공간과 물리공간의 경계를 더욱 허물어뜨려서 마치 동일한 공간에서 작동하는 것처럼 상호연동될 것이며 또한 이렇게 팽창하는 가운데 공간관리 뿐만 아니라 넘쳐나는 데이터들을 실시간으로 종합, 분석, 관리하고 그 안의 숨겨진 패턴과 지식을 활용하는 스마트형 공간이 될 것이다.[10]

3.3 효과중심작전 수행을 위한 전제들

3.3.1 사이버 공간에 대한 5 전략동심원 모델

사이버공간에서 효과중심작전을 수행하기 위해서는 Warden이 제시한 5 전략동심원 이론에 따라 사이버공간을 재구성하여야 한다. 사이버공간 구조는 장원구[11]가 제시한 물리, 논리, 데이터, 인식영역 4개 Layer, 물리네트워크와 지리적 요소, 논리네트워크와 소프트웨어 논리, 일반 데이터와 중요/비밀 데이터, 인물정보과 사회활동 8 Component를 이용하여 아래와 같이 구성한다.



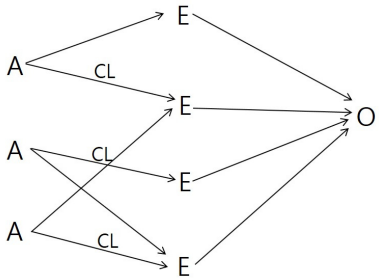
(그림 4) 사이버공간 5 전략동심원 모델
(Figure 4) 5 Strategic Rings Model for cyberspace

5동심원은 가운데 원부터 적의 리더십, 핵심시스템, 하부구조, 시민, 군대로 구성되는 데 이것은 적을 5가지 전략적 목표물로 구분하고 이들의 중심을 파악하기 위한 것이다. 따라서 사이버 공간에서 전략적 목적의 5동심원 요소는 각각 사이버 공간을 이끄는 국가 지도부, 사이버 공간을 이루는 핵심요소인 네트워크와 시스템, 하부구조로서 네트워크와 시스템을 기반으로 저장되거나 사이버 공간을 오가는 데이터, 사이버 공간에서 활동하는 사람들을 통해 나타나는 사회인식적 심리, 그리고 사이버공간을 방어하는 사이버전력이 된다. 여기서 사회인식적 심리는 Warden의 모델에서는 시민에 해당하는데 이는 사이버 공간에서는 ID, 아바타와 같은 가상 개체와 이를 활용하는 사람들의 의식만이 있으며 가상 개체는 공격을 받아 삭제되어도 언제든지 복구될 수 있으므로 심리적 요소로서 공격에 의해 전략적 영향을 받을 수 있는 사회인식적 심리로 선정한다.

이상과 같이 사이버 공간에 대한 5 전략동심원 모델은 사이버 공간의 군사전략적 요소로서 적 공격에 의해 타격을 받을 시 국가적 위기로 이어질 수 있으므로 PMESII 체계와 연계하여 사전에 중요 자산을 선정하고 강력한 방어대책을 수립하여야 한다.

3.3.2 효과기반 방법론

효과는 공격으로부터 즉시 직접적으로 초래되는 직접적인 효과와 연차적인 결과에 의한 것이거나 최종적인 결과인 간접적인 효과로 구분할 수 있으며 각각 전략적, 작전적, 전술적 수준에서 그 효과를 평가할 수 있다. 세부적으로 직접적인 효과는 Physical, Functional, Collateral, Psychological effects로 나뉠 수 있으며 간접효과는 Functional, Cascading, Cumulative, Collateral, Systemic, Psychological effects로 나누어진다. 효과중심작전은 MOE(Measure of Effectiveness), MOP(Measure of Performance)를 이용한 효과평가와 E(효과)-N(노드)-A(조치)-R(전투력할당)를 이용한 적 복합체계에 대한 작전체계 평가(ONA: Operational Net Assessment)를 통하여 작전절차에 따라 지속적으로 수행해 나간다. 사이버공간에서의 효과는 앞서 언급한 바와 같이 Destroy, Deny, Degrade, Deceive, Disrupt이며, 심리적인 효과는 사이버공간 피해에 따라 관련된 사람들의 심리적인 영향여부를 간접적으로 측정하는 것이다. 사이버공격을 이용하여 적의 의지에 변화를 주기 위해서는 그림 5와 같이 다양한 조치들을 통하여 나타난 효과들이 중첩되어야 한다.



(그림 5) 효과기반 방법론[12]
(Figure 5) The Effect-based Methodology[12]

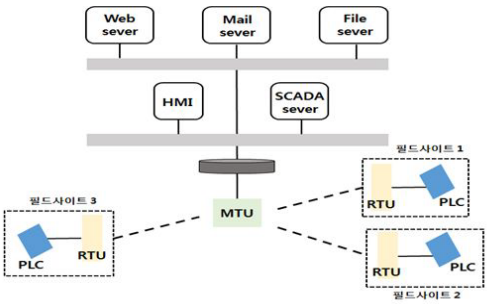
3.3.3 적 체계분석

적에 대한 효과중심작전을 적용하기 위해 우선 적을 복합체계로 보고 PMESII 틀 속에서 분석한다. 예를 들어 적의 정치구조는 다음과 같다.

(표 2) 정치구조 분석 예시
(Table 2) Examples of political structure analysis

구 분	대통령	비서실	경호처	교육부	...
인 원	○○○	○○○ ○○○	○○○ ○○○ ○○○	장관 ○○○ 차관 ○○○ 3급 ○○○ 4급 ○○○	...
이메일	..@...com	..@...net	..@google.com	..@google.com	...
홈페이지	..go.kr	..go.kr	..go.kr	..go.kr	...
SNS	..facebook.com	Twitter	카카오톡	..facebook.com	...
스마트폰	010...	010...	010...	010...	...
...	...	...	...	...	...

다른 예로 전력, 석유, 확학, 교통시스템 등 SCADA로 대표되는 제어시스템은 그림 6과 같다. 제어시스템은 하드웨어와 소프트웨어로 구성되는 데 하드웨어는 제어센터에 위치한 제어용 중앙통제시스템(MTU: Master Terminal Unit)과 무선, 유선, 위성 등의 통신장비, 그리고 작동을 제어하고 센서를 모니터링하는 원격단말장치(RTU: Remote Terminal Unit), 프로그램 가능 로직 제어기(PLC: Programmable Logic Controller)로 구성된다. 또한 집중화된 모니터링과 제어 시스템을 제공하기 위해 데이터 수집 시스템을 데이터 송신 시스템과 기계를 동작시키기



(그림 6) 제어시스템[13]
(Figure 6) Control System[13]

위한 입출력장치(HMI: Human Machine Interface) 소프트웨어와 융합한다. [13]

이러한 것들은 모두 사이버공간에서 네트워크와 노드로 표현되며 사이버공격의 표적이 된다. 사이버표적은 그 중요성, 체계간 상호의존도와 공격 취약점 등을 파악하고 군사적 목적을 고려하여 선정한 후 공격을 시행한다. 따라서 방어자는 중요한 사이버 자산에 대하여 취약점을 사전에 식별하고 이를 해소하는 노력을 지속적으로 기울여야 한다.

3.4 효과중심작전 적용을 위한 군사전략 수립

3.4.1 과거 사이버공격 사례

효과중심작전을 위한 공격사례는 아직까지 존재하지 않으므로 과거의 사례를 살펴본 후 이를 이용하여 군사전략을 수립하는 방법을 이용한다. 먼저 사이버공격사례로서 표 3과 같이 6.25 사이버테러[14], 국방망 해킹사건[15], 웹호스팅 업체 '인터넷나야나' 랜섬웨어 공격사건[16], 한수원 해킹사건[17]의 4가지 사례를 선정하였으며 선정사유는 6.25 사이버테러는 금융, 방송, 정부망에 대한

(표 3) 사이버공격 사례 분석
(Table 3) Analysis of cyber attack cases

구분	내 용	5동심원	의도한 효과
6.25 사이버 테러	2013.6.25.~7.1까지 방송, 신문사 서버 파괴, 청와대, 국무조정실 등 홈페이지 변조, 정부통합 센터 DDOS발생	적 지도부 네트워크/ 시스템, 데이터, 사회인식적 심리	·언론,정부기능 마비(Disrupt) ·컴퓨터 파괴 (Destroy) ·사회적 혼란
국방망 해킹	2016.9.23.일 북한추정 해킹세력이 백신중계 서버에 침투하여 서버와 PC에 악성코드를 유포하고 다수의 비밀을 유출한 사실이 식별됨.	네트워크/ 시스템, 데이터, 사회인식적 심리, 사이버 전력	·군동향 파악 (Deceive) ·군기밀 획득 ·사회적 공포감 조성
웹호스팅 업체 랜섬웨어 공격	2017.6월 국내 웹호스팅 업체 '인터넷나야나'가 랜섬웨어 공격을 당해 3,400여 업체 운영마비	네트워크/ 시스템, 데이터, 사회인식적 심리	·기업활동 마비(Disrupt) ·금전적 이득 ·사회혼란 유도
한수원 해킹 사건	2014.12.15. 북한 추정 해킹 세력이 한수원 관련 자료를 6차례에 걸쳐 공개하고 한수원 직원에게 악성코드 메일을 발송하여 하드디스크 파괴시도	네트워크/ 시스템, 데이터, 사회인식적 심리	·컴퓨터 파괴 (Destroy) ·내부자료 획득 ·사회혼란 유도 ·공포감 조성

공격이며 국방망 해킹사건은 군사시설에 대한 공격, 웹호스팅 업체 사건은 민간부문에 대한 공격, 그리고 한수원 해킹사건은 국가기반시설에 대한 공격으로 자행된 사례이어서 선정하였다. 선정된 사이버 공격들은 사이버 5동심원 모델의 각 요소를 대상으로 전략적 중심(COG)을 선정하여 공격을 시행한 것으로 판단할 수 있으며 각각의 효과 측정은 언론/정부의 기능 가동율, 파괴된 컴퓨터 수, 국방망 침투 기간, 침투 범위, 유출된 기밀 종류 및 수량, 렌섬웨어에 감영된 기업체 수, 피해 금액, 공개된 자료 종류 및 수량, 파괴된 컴퓨터 수 등에 대한 MOE, MOP를 이용하여 평가할 수 있다. 동일한 방법으로 심리적 효과 또한 소셜네트워크 서비스나 인터넷 뉴스에 대한 빅데이터 분석, 포탈사이트의 검색어 순위 서비스에서 확인할 수 있다. 효과 평가가 이루어진 후에는 작전체계평가(ONA)을 통해 요망되는 최종효과를 달성하기 위한 지식체계를 구축하여 차후 조치방안을 지휘관에게 건의한다.

3.4.2 효과중심작전 수행을 위한 군사전략 수립

앞서 선정한 4건의 사례를 바탕으로 전략적인 수준에서 직접적인 효과를 이용하여 효과중심작전을 수행하기 위한 군사전략을 수립한다. 군사전략은 군사적 목표와 목표를 달성하기 위한 수단, 그리고 이를 실행하는 방법으로 구성[18]되어 있으며 세부내용은 표 4와 같다. 즉, 국가 기능 마비를 통한 적 지도부의 행동 변화를 목표로 사

이버 공격무기를 이용하여 해킹, DDOS 공격, 랜섬웨어를 이용한 데이터 암호화 등 사이버 공격을 감행하되 이때 전략적 마비를 유도하기 위해 선정된 표적들에 대한 병렬공격과 신속결정작전을 수행하는 것이다. 공격에 대한 예상효과는 Destroy, Deceive, Disrupt의 물리적, 기능적, 시스템 효과와 소셜네트워크에 대한 빅데이터 분석, 실시간 검색어 순위 등을 통해 드러난 혼란, 공포 등 심리적 효과이다.

(표 4) 효과중심작전을 위한 군사전략 수립
(Table 4) Establishing military strategy for EBO

구 분	내 용
목 표	국가기능 마비, 적 지도부 행동변화
수 단	사이버 공격무기
방 법	·해킹, DDOS, 랜섬웨어를 이용한 사이버 공격 시행 ·전략적 마비를 위한 병렬공격, 신속결정작전 수행
공격대상	·신문사, 방송사, 중앙정부 ·국방망, 백신 공급업체 ·웹호스팅 업체 및 관련 기업 ·한국수력원자력
효 과	·직접효과 - 물리적 효과: Dsetroy - 기능적 효과: Deceive, Disrupt - 시스템 효과: Disrupt - 심리적 효과: 사회혼란 3회 공포심 유발 2회 · 기타 : 군사기밀 등 데이터 탈취 및 변조 금전적 이득 획득

3.4.3 효과중심작전의 한계점

이상과 같이 군사전략 수립을 통하여 사이버공간에서의 효과중심작전 수행 및 이에 따른 효과를 확인하였으며 이에 대한 실질적인 검증은 사이버전 사례분석이나 실제 작전 수행을 통해서도 가능하다. 하지만 사이버공간에서의 효과중심작전은 다음과 같은 한계점을 가지고 있다. 첫째, 사이버전에서도 인간의 의지와 같은 불확실 영역이 존재하므로 사이버공격을 이용한 효과중심작전이 항상 원하는 군사목표 달성을 보장하지는 않는다. 둘째, 적이 국가와 같은 복합체계가 아닌 비정규군이나 소규모 조직, 단체에 대한 적용은 용이하지 않다. 셋째, 개발도상국이나 낙후된 국가처럼 사이버공간이 충분히 발달하지 않은 적에게는 효과중심작전 적용이 불가하다. 넷째, 본 논문에서는 효과중심작전을 위해 사이버공격만을 이용하였는데 효과중심작전은 이외에도 DIME(Diplomatic, Informational, Military, Economy)요소를 이용한 공격도 병행해야 한다.

4. 결 론

전쟁수행에 있어 항공력이 전쟁 승리의 핵심적인 역할을 할 수 있음을 증명하였던 효과중심작전은 비록 공식적으로는 사라졌지만 실질적으로는 과거에도 있어왔고 앞으로도 계속 그 역할을 할 것이다. 사이버공간은 이러한 효과중심작전을 구현하기에 적합한 공간으로서 적의 심리와 행동에 영향을 미칠 수 있는 공간이다. 또한 사이버 무기는 본질적으로 비살상 무기이므로 기존의 전쟁에서는 피할 수 없었던 무의미한 희생과 노력을 다소나마 줄일 수 있을 것이다. 앞으로 사이버공간은 4차 산업혁명과 관련 기술들의 발달에 따라 더욱 확대되고 고도화 될 것이다. 따라서 사이버공간상에서의 효과중심작전의 중요성은 더욱 커질 것이므로 향후 연구과제로서 효과중심작전 수행에 따른 사이버공간상의 피해평가 측정방안에 대한 연구가 이루어져야 할 것이다.

참고문헌(Reference)

[1] Millan N. Vego, “Effect-Based Operations: A Critique”, Institute for National Strategic Studies, pp. 52-54, 2006
https://apps.dtic.mil/docs/citations/ADA521851

[2] Dukjong Jeon, “Study on the Theoretical Limitation of Effect Based Operation: Critical Analysis Based on the Nature of War”, A thesis on master’s degree on Chungnam National University, pp. 46-47, 2010.
http://www.riss.kr/link?id=T11936779

[3] Kwangho Chun, “Effect-based Operations in US Doctrine”, The Journal of Humanities and Social science, Vol. 10, No. 1, 2019, pp. 673-688, 2019.
http://dx.doi.org/10.22143/HSS21.10.1.47

[4] Doohyun Baek, “A Study on the impact about EBO

gets to the development of Joint Force Achievement Concept for ROK Military", A thesis on master's degree on Chungnam National University, pp. 1-69, 2010. http://www.riss.kr/link?id=T11936780

[5] Jinhang Kim, "A war of fire and paralysis", sisun, pp. 112, 2004

[6] Military research council, "On War", Planet media, pp. 246-248, 2015.

[7] The school of advanced Airpower Studies, "The Paths of Heaven: The evolution of Airpower Theory", Air University Press, pp. 376, 1995. https://books.google.co.kr/books?hl=ko&lr=&id=pb5KxjjN64gC&oi=fnd&pg=PR2&dq=The+Paths+of+Heaven:+The+evolution+of+Airpower+Theory&ots=VWAg3LlYWv&sig=fm8BxjMYIGV-NicNXBeRKG7jLaU#v=onepage&q=The%20Paths%20of%20Heaven%3A%20The%20evolution%20of%20Airpower%20Theory&f=false

[8] Paul W. Phister Jr, "Cyberspace: The Ultimate Complex Adaptive System", The International C2 Journal, vol. 4, no. 2, pp. 11, 2011. https://apps.dtic.mil/dtic/tr/fulltext/u2/a541010.pdf

[9] Hyongu Shin, "Establishment of Cyber Security Strategy according to the change of cyberspace environment", Journal of Security Engineering, vol 14, no. 4, pp. 251-262, 2017 http://dx.doi.org/10.14257/jse.2017.08.04

[10] Jungho Eom, "Cyber Defense Strategy for Information Superiority in Cyberspace", Journal of Security Engineering, vol. 9, no. 5, pp. 384, 2012 https://www.earticle.net/Article/A202374

[11] Wongu Jang, "Bigdata Governance Model for Effective Operation in Cyberspace", The Journal of Bigdata, vol 4, no. 1, pp. 45, 2019 http://doi.org/10.36498/kbigdt.2019.4.1.39

[12] Col Edward C. Mann, et al, "Thinkg Effect: Effects-Based Methodology for Joint Operations", CADRE Paper No.15, pp. 40, pp. 49, 2002

[13] Hyunju Lee, "The Study on Security Enhancement of National Control System for Critical Infrastructure: Focusing on Comparision About Policy of Major Countries and Domestic", A thesis on master's degree on Sangmyung University, pp. 4, 2016 http://dlps.nanet.go.kr/SearchDetailView.do?cn=KDMT1201661919&sysid=nhn

[14] Red Alert, "6.25 Cyber terror analysis report", pp. 4-6, NSHC, 2013 https://izigom.tistory.com/entry/625-%EC%82%AC%EC%9D%B4%EB%B2%84%ED%85%8C%EB%9F%AC-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C?category=431843

[15] http://www.itworld.co.kr/news/102451

[16] http://www.sisain.co.kr/news/articleView.html?idxno=29610

[17] https://science.ytn.co.kr/program/program_view.php?s_mcd=0082&s_hcd=&key=201507141550438658&page=2213

[18] Changhee Park, "On Military Strategy", planet media, pp. 101, 2013

◐ 저 자 소 개 ◑

장 원 구(Won-gu Jang)
1996년 공군사관학교 전산학과(공학사)
2011년 아주대학교 정보통신대학원(공학석사)
2014년 9월~현재 고려대학교 정보보호대학원 박사과정
관심분야 : 사이버정보, 사이버안보, 빅데이터, 위험관리.
E-mail : jwg1019@naver.com, goo1019@korea.ac.kr

이 경 호(Kyung-ho Lee)
1989년 서강대학교 수학과(이학사)
1997년 서강대학교 정보통신대학원(공학석사)
2009년 고려대학교 정보경영대학원(공학박사)
2011년 9월~현재 고려대 정보보호대학원 교수
관심분야 : 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호 정책
E-mail : kevinlee@korea.ac.kr