사이버전의 개념과 대응방안에 관한 연구

박찬수* · 박용석*

*정보보호대학원, 세종사이버대학교

A Study on the Concept of the Cyber Warfare and the Plan of Reaction

Chan-soo Park* · Yongsuk Park**

*The Gradate School of Information Security, Sejong Cyber University

E-mail : jeil0912@hanmail.net, yongspark@sjcu.ac.kr

요 약

컴퓨터와 네트워크 기술의 발전으로 인터넷 사용이 급증하고 있고, 현재는 스마트폰, Table PC와 같은 스마트 기기들의 출현으로 일상생활이 사이버공간으로 확대되는 획기적인 변화를 가져왔으며, 삶의 가치 또한 한층 높아졌다. 이러한 사이버 공간이 개개인의 일상생활만을 변화시켜온 것이 아니라 전 영역과 세계적으로 변화를 주고 있다.

현재의 글로벌 트렌드는 에너지 자원 확보 및 보호가 주요관심사로 부각되고 있으며, 정치 경제, 안보 등 국가내 정보체계 의존이 심화되고 있다. 주요기반시설이 전략적 공격 목표로 부상하여 효율적인 공격 수단으로 사이버전의 중요성이 부각되고 있다.

본 학술지는 사이버전의 개념과 국가별 사이버 역량을 살펴보고 향후 사이버전 발생시 최선의 방어로 피해를 최소화하기 위한 대응방안을 모색해 보고자 한다.

ABSTRACT

Because of the development of computers and networks, the use of the internet has been rapidly increased. The smart devices, such as smart phones and tablet PCs, have made an epoch-making changes, which have brought people's daily lives to the cyber world and life values have been improved. The cyber world not only just changed individual's lives, but also affected all areas and the world.

The recent global trends reside mainly in protection of energy sources, and nation's dependency of the information system such as politic, economic and national security. Since major national infrastructure becomes a stragic attack target, the importance of cyber warfare has rised as an effective way to attact enermy.

This article explores the concept of cyber warfare and national cyber capability, and then figure out the plan of reaction to minimize damages with best protection when cyber warfare occurs.

키워드

Cyber Warfare, 사이버 역량, 사이버 기반, 사이버 공격 및 방어

Ⅰ. 서 론

컴퓨터와 네트워크 기술의 발전으로 인터넷 사용이 급증하고 있고, 현재는 스마트폰, 테블릿 PC와 같은 스마트 기기들의 출현으로 일상생활이 사이버공간으로 확대되는 획기적인 변화를 가져왔으며, 삶의 가치 또한 한층 더 높아졌다. 이러한 사이버 공간이 개개인의 일상생활만을 변화시켜온 것이 아니라 전 영역과 세계적으로 변화를 주었으며, 전쟁양상 또한 변화되고 있다.

예전의 전쟁양상은 물리적 타격 수단으로 인명살상과 영토 확장을 목적으로 한 재래전이었다면 현재는 사이버 공간의 확대로 정보 우위를 기반으로 한 네트워크 중심전으로 이동한 전쟁환경

의 변화를 가져왔다. 물리적 파괴에서 전쟁수행체계를 마비시키는 공격대상도 변화하였으며, 전쟁영역은 물리적 영토에서 사이버 공간으로 변화하게 되었고 미래전은 사이버전과 재래전을 결합한 형태의 융복합전이 될 것이다.

본 학술지에서는 사이버전의 개념과 국가별 사이버 역량을 살펴보고 향후 사이버전 발생시 최선의 방어로 피해를 최소화하기 위한 대응방안을 모색해 보고자 한다.

II. 사이버전의 개념

2.1 사이버전의 정의

육군에서는 사이버전을 컴퓨터에 의해 조성되는 가상현실의 세계(Cyber Space)와 가상인간의 영역과 같이 인공지능 체계가 운용되는 공간에서의 전쟁으로서, 이는 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 강요할 수 있는 총체적인 가상공간에서의 정보마비전을 추구하는 전쟁수행 방식으로 정의하고 있다.[1]

2.2 사이버전의 형태와 위협

사이버전쟁의 위협을 형태별로 살펴볼 때 네가지로 구분된다.

첫째, 사이버 타격 / 방어전은 해커이용 조직적 공격으로 2009년 러시아 해커가 키르기스스탄 내 미 공군기지 주둔 등의 정치문제로 주요 인터넷서비스사업자 전산망을 대상으로 사이버 공격을 한 사례와 61개국 총 435대 서버 이용 DDoS 공격으로 국내 정부부처, 금융기관, 인터넷서비스 사업자 전산망 등 일시적인 서비스를 마비시킨 사례를 주요 예로 들 수 있다.

둘째, 물리연계전은 국가기반 시설을 마비하는 공격으로 2008년 러시아와 그루지아 무력충돌 확산 중에 러시아 '러시아 비즈니스 네트워크' 사이버범죄 조직이 그루지아 대통령 홈페이지를 비롯한 의회/국방부/외교부 사이트에 대해 서비스 거부 공격한 사례를 예로 들 수 있다.

셋째, 사이버 첩보전은 국가 기밀 수집 및 절취하는 공격으로 2009년 사이버스파이들이 미 국방부 전산망에 침투해 차세대 전투기 F-35 설계 자료와 전자시스템 관련 정도 등을 유출한 사례를 예로 들 수 있다.

넷째, 사이버심리전은 국론분열 및 기만정보 전파의 공격으로 2010년 천안함 사태에 대한 기만정보를 전파한 사례를 예로 들 수 있다.[2]

2.3 사이버전의 특징

사이버전의 특징은 첫째, 저비용으로 사이버전을 수행할 수 있으며, 둘째, 사이버 공격 징후를 포착할 수 있는 조기경보 체계 구축이 어렵다. 셋째, 사이버 공격에 대한 공격대응 시간이 충분히 확보될 수 없고, 넷째로는 사이버 공격에 대한 피해가 사이버 공간 뿐만 아니라 물리적 공간에도 발생하고 전투피해평가가 곤란하다. 다섯째는 정보수집 양상이 진화되고 있다는 점이다.[3]

III. 각국의 사이버전 역량 비교의 한계점

손자병법에 보면 '知彼知己 百戰不殆'라는 말이 이쌀. 상대를 알고 나를 알면 백번 싸워도 위태롭지 않다는 듯이로 세계 강대국들이 육·해·공·우주에 이어 제 5의 전장으로 사이버 공간을 간주하고 사이버 전쟁준비에 박차를 가하고 있는 실정이지만, 각국의 사이버전 역량을 비교 분석 할 수 있는 명확한 기준이 없어 적을 알 수 있는 각국의 사이버전 역량을 알기에는 상당히 제한적이다.

세계 최초로 미국은 사이버 역량 평가 방법론을 개발하여 세계 국가들에 대한 평가를 수행함으로써 사이버 강대국 다운 면모를 보여주고 있으면서도 평가 방법론은 공개하지 않고 있다.[4]

미국의 사이버 역량 평가 방법과 국내 연구소의 사이버 역량 평가 방법의 특징을 분석해보고 객관적이고, 정량적인 표준안을 제시해보고자 한다.

3.1 Technolytics, 군 사이버전 역량평가(2009)

Technolytics는 2009년 사이버 무기 및 첩보 활동을 하는 160여개 국가의 사이버 역량을 아래 세가지 분야(사이버 역량 목적, 사이버 공격 역량, 사이버 정보수집 등급)로 평가하고 측정 점수 합의 평균으로 종합 역량 등급을 산정하였다[5]

Technolytics의 군 사이버 역량 평가에서는 주로 공격 역량에 대한 평가로 사이버 역량 목적은 목적 달성을 위한 목표와 상태, 사이버 공격역량은 전시 특수 목적을 달성하기 위한 능력, 사이버 정보 수집 등급은 새로운 사이버 영역에서의 정보 수집 능력으로 나누어서 사이버전 역량 평가가 되었다. 사이버전 역량은 사이버 공격 역량만 평가되어서는 안되고, 사이버 방어 역량까지 같이 평가가 되어야 한다.

국 가	역량목적	공격역량	정보수집	역량등급
중 국	4.2	3.8	4.0	4.0
미 국	4.2	3.8	4.0	4.0
러시아	4.3	3.5	3.5	3.7
인 도	4.0	3.5	3.5	3.7
이 란	4.1	3.4	3.4	3.6
북 한	4.2	3.4	3.3	3.6
일 본	3.9	3.3	3.5	3.6
이스라엘	4.0	3.8	3.0	3.6
한 국	3.5	3.0	3.2	3.2
파키스탄	3.9	2.7	2.6	3.1

표 1. Technolytics 사이버 역량 평가(5점만점)

3.2 Richard A. Clarke, 사이버 역량 평가(2010)

Richard A. Clarke는 공격(Offense : 타 국가를 공격할 수 있는 능력), 방어(Defense : 공격에 대한 저지 및 완화 능력), 의존(Dependence : 국가 기반시설이 네트워크에 연결된 정도로 전산화가 덜 될수록 높음) 세가지 범주에 대해 저자의 주관적인 판단에 의해 점수를 부여하고 각 분야의 점수를 총합하여 평가를 수행하였다.[6]

Richard A. Clarke의 사이버 역량 평가에서는 10점만점으로 공격과 방어는 역량이 높을 수록 높은 점수를, 정보시스템 의존도는 의존도가 높을 수록 낮은 점수를 부과하였고, 이에 대한 총합으로 사이버전 역량을 제시하였다.[7]

사이버전 역량이 미국이 낮은 이유는 미국의 사이버전 역량 강화의 필요성을 강조하기 위한 의도적인 결과로 Richard A. Clarke의 주관적인 견해로 인해 각 국가별 사이버전 역량을 정확하게 판단하기는 제한된다.

국 가	공 격	방 어	고 립	총 점
미 국	8	1	2	11
중 국	5	6	4	15
러시아	7	4	5	16
북 한	9	9	9	18

표 2. Richard A. Clarke 사이버전 역량 평가

3.3 국가 사이버 역량 평가 방법론 연구(2012)

ETRI 부설연구소에서 연구한 국가 사이버 역량 평가 방법론 연구에서는 사이버 역량 평가 분야를 기반(영토, 자원, 인구, 기타), 공격(정보수집, 침투, 파괴 / 무력화), 방어(예방, 대응, 탐지) 역량을 세가지 평가 그룹으로 점수를 부여하고 각 분야의 평균치로 평가를 수행하였다.

평가 항목을 세분화하여 평가를 진행하였지만, 평가 결과를 분석하여 보면 미국의 결과와 다소 차이를 보이고 있다. 한가지 예를 들어 러시아는 사이버전 수행 능력만큼은 세계 최고 수준으로 평가받고 있지만, 분석 결과를 보면 한국의 사이버전 역량에도 미치지 못하는 결과를 나타내고 있다.

국 가	기 반	공 격	방 어	총 합
미 국	8.6	8.9	9.5	9.0
중 국	6.9	8.9	5.3	7.0
일 본	4.2	5.5	6.0	5.2
러시아	3.3	8.4	5.6	5.8
한 국	5.5	6.0	8.0	6.5

표 3. ETRI 부설연구소 국가 사이버 역량 평가

3.4 국가 사이버 역량 평가 방법론 보완 방향

사이버전 역량은 사이버전을 수행할 수 있는 능력을 말하며 여기에 구성되는 요소는 크게 세 가지로 기반, 공격, 방어로 구성할 수 있다. 그런 의미에서 본다면 ETRI 부설연구소에서 연구한 국가 사이버 역량 평가 방법이 가장 근접하다고 할 수 있다.

대분류	중분류	평가항목
기 반	인프라	네트워크 수준
		시스템 수준
	예 산	IT 예산 규모
		정보보호 예산 규모
	병 력	사이버전사 규모
		보충역 규모
		컨트롤타워 유무
	기타	외교적 노력
		훈련 체계 구축
		교육 체계 구축
공 격	무기 체계	소프트 웨어 무기체계
		하드웨어 무기체계
	정보 수집	디지털 스누핑 수준
		사회공학기법(ATP)
	침투	트로이 목마 수준
		취약점 이용 수준
		웜바이러스 수준
		보안 시스템 우회수준
	파괴 / 무력화	DDoS 수준
		시스템 파괴수준
		EMP 수준
		GPS 교란 수준
방 어	예방	소프트웨어 보안 인증 수준
		보안서버 보급률
		패치 보급률(MS 패치)
	탐지	침입탐지 시스템 수준
		보안관제 수준
		백신수준
	대응	CERT 활동
		포렌식 전문가
		포렌식 준비도
		악성코드 분석 수준

표 4. 국가 사이버 역량 평가 항목 보완 요소

기반 역량 평가를 보완하자면 교육 체계 구축 항목을 추가하였으며, 교육훈련 체계를 구축하는 것은 사이버전사를 질적과 양적으로 육성할 수 있는 기반을 만드는 것이다. 이는 사이버전 역량의 기반을 다지는데 중요한 요소라 할 수 있다.

공격역량 평가를 보완하자면 정보 수집, 침투, 파괴 / 무력화로 항목이 나뉘는데 바꿔 말하면 사이버 무기체계의 일종이라고 표현할 수 있다. 사이버 무기체계는 소프트웨어 무기체계와 하드웨어 무기체계로 나누어진다. 소프트웨어 무기체계는 해킹, 인터넷 웜, 논리폭탄, 바이러스, 스팸메일, AMCW로 나뉘며, 하드웨어 무기체계는 EMP 폭탄, 칩핑(Chipping), HERF GUN, 나노머신(Nano Machine)이 있다.[3] 공격 역량을 평가하려면 사이버 무기체계의 보유여부와 기술능력(첩보수집, 침투, 파괴 / 무력화)으로 평가하는 것

이 적합하다고 볼 수 있다.

방어역량 평가를 보완하자면 포렌식 준비도(Forensic Readiness)를 추가하였다. 사이버전은 공격에 대한 피해 대응 효율을 높이기 위한 기준으로 사이버전 공격시 대응에 대한 역량 평가의 중요한 요소라고 할 수 있다.

Ⅳ. 한국 사이버전의 역량 강화 방안

한국군의 사이버전 향상방안을 위해 다음과 같이 세가지 방법을 제시하고자 한다.

첫째로는 전문인력 확충이 필요하다. 고급 전문인력 확보를 위해 2012년에 사이버 국방학과를 설립하여 2016년 이후 장교 30명씩 임관할 예정이고, 지식 경제부 SW Maesrto 과정 연수생을 전문병으로 활용할 계획[8]이지만, 장교와 병사를 연결해주는 중추적인 역할인 부사관의 양성 계획은 없다. 현재 항공과학고등학교나 영북고등학교와 같은 부사관 고등학교와 전문대학의 부사관 학과가 있듯이 이러한 부사관 고등학교 또는 대학의 부사관 학과에서 전문적으로 사이버국방과를 설립하여 부사관의 확충도 시급하다.

두 번째로 국가간 사이버 역량 평가 방법론을 개발하여 사이버 역량 비교·분석이 필요하다. 손자병법에 보면 '知彼知己 百戰不殆'라는 말이 있듯이 상대를 알고 나를 알면 백번 싸워도 위태롭지 않다는 뜻으로 사이버전도 적을 알아야 대비할 수 있는 것이다. 그렇기 때문에 국가간 사이버 역량을 비교 분석 할 수 있는 명확한 기준이 제시 되어야 한다.

세 번째로 사이버전에 대비한 훈련이 필요하다. 우리 군이 연례적으로 훈련을 하는 KR/FE, UFG, 호국훈련 등이 있는데 이러한 훈련들은 한반도의 전시상황을 가정하여 훈련을 하는 것이다. 위에서도 언급했다시피 미국이 연례적으로 훈련을 하고 있으며 한국군은 기존에 DDoS 공격사례를 분석하여 똑같이 공격을 하고 방어를 하는 훈련을 해보면 실전적인 경험을 쌓을 수 있으므로 훨씬 사이버전 역량이 크게 향상 될 것으로 판단된다.

Ⅴ. 결 론

사이버전에 대한 관심사가 더욱 높아지고 있는 지금 주변국들의 사이버 역량 강화를 위해 여러가지 방안을 강구하고 있는 실정이며, 북한 또한 언제든지 대한민국의 적화통일하기 위해서 비대칭 전력을 대폭 강화하고 있다. 비대칭 전력 중 하나로 사이버전 역량을 중요시 여기고 있으며, 지도층부터 관심을 갖고 사이버 무기를 개발하고 사이버 전사를 양성하는 등 지속적으로 사이버전 역량을 강화하려고 노력하고 있다.

우리나라도 마찬가지로 북한의 사이버전 역량에 대해서 정확하게 비교 분석 할 수 있어야 하며, 사이버전사의 양성과 사이버 무기 개발 등 대응방안을 마련해야 한다. 군의 역할은 평시에 전쟁억제 역할을 수행하지만 전시에는 적과 싸워 이길 수 있어야 한다. 전·평시가 따로 구분되지 않는 사이버 공간에서의 사이버전에서 승리하려면 사이버전의 역량 강화가 하루 빨리 이루어져야 한다.

참고문헌

[1] 참고교범-1-21, 군사용어사전, 2012년
[2] 국가기술보안연구소, "거대한 위협 사이버 전쟁" 2012년
[3] 엄정호, 최성수, 정태명. "사이버전 개론", 2012년
[4] 강정민, 황현욱, 이종문, 윤영태, 배병철, 정순영, "국가 사이버 역량 평가 방법론 연구", 2012년
[5] Technolytics, "Cyber Commander's eHand -book version 2.0", 2012년
[6] Richard A. Clarke, "Vyber War : the Next Threat to National Security and Waht to Do About It", copyrighted Material, 2010년
[7] 손영동. "사이버전 억지력 평가모델에 관한 연구", 2011년
[8] 김재윤, "국정감사 보도자료" 2012년 10월 8일