JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 5 : 1251~1258 May. 2015

사이버전의 역량평가 개선과 역량 강화 방안에 관한 연구

박찬수 · 박용석*

A Study on the Improvement of Capability Assessment and the Plan for Enhancing Cyber Warfare Capability of Korea

Chan-soo Park · Yongsuk Park*

Graduate School of Information Security, Sejong Cyber University, 121 Gunja-ro, Gwangjin-gu, Seoul 143-839, Korea

요 약

최근 사이버 무기의 발전으로 사이버전의 위협이 점점 더 증가되고 있다. 이미 사이버전을 경험한 국가들은 피해가 사이버상에서만 국한 되는 것이 아니라 물리적인 피해까지 영향을 받게 되어 피해가 상당하다. 이렇기 때문에 각국은 사이버전에 대비하기 위해 끊임없이 노력을 하고 있다. 먼저, 사이버전을 대비하기 위해서는 각국의 사이버전 역량이 파악되어야 하며, 비교 / 분석을 통해 사이버전 대응방안을 모색해야 한다. 본 논문에서는 기존 사이버전의 역량평가 방법에 대해서 비교 / 분석해보고, 향상점을 도출하여 사이버전 역량 평가 개선안을 연구하였다. 개선된 사이버전 역량 평가를 통해서 한국에 영향을 줄 수 있는 국가들을 대상으로 사이버전 역량 평가를 실시하였으며, 평가 결과를 비교 / 분석함으로 한국의 사이버전 역량의 보완점을 도출하여 사이버전 역량 강화 방안을 제시하였다.

ABSTRACT

Recently, as the development of cyber weapons, the threat of cyber warfare has been increasing. Nations, which experienced cyber warfare already, have been damaged not only in the cyber space as well as in real war field. Therefore, each nation is constantly making efforts to prepare for cyber warfare. First of all, to prepare for cyber warfare, each nation's capability of cyber warfare should be understood. A plan of reaction of cyber warfare should be searched by comparison and analysis of capability of cyber warfare. This paper compares and analyzes established methodology of capability assessment about cyber warfare, and this paper finds a better point to suggest the improvement of capability assessment about cyber warfare. This paper applies capability assessment of cyber warfare to nations, which can influence on Korea with improved capability assessment of cyber warfare. Comparing and analyzing the result of assessment, this paper deducts complementary point of Korean cyber warfare to suggest the plan to enhancing capability of cyber warfare.

키워드 : 사이버전, 역량 평가, 기반 역량, 공격 역량, 방어 역량

Key word : Cyber Warfare, Capability Assessment, Foundation Capability, Offence Capability, Defence Capability

Received 15 April 2015, **Revised** 30 April 2015, **Accepted** 08 May 2015

***Corresponding Author** Yongsuk Park(E-mail:yongspark@sjcu.ac.kr, Tel: +82-2-2204-3894)
Graduate School of Information Security, Sejong Cyber University, Seoul 143-839, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.5.1251 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

일상생활이 사이버 공간으로 확대됨에 따라 삶의 질이 더욱 향상되었고, 전 영역과 세계적으로 변화를 주었으며, 전쟁 양상까지도 변화되고 있다. 예전의 전쟁 양상은 물리적 타격 수단으로 인명살상과 영토 확장을 목적으로 한 재래전이었다면 현재는 사이버 공간의 확대로 사이버 공격을 감행하여 국가기반 시설과 전쟁수행체계를 마비시키거나 파괴하는 전쟁환경의 변화를 가져왔다. 미래전은 사이버전과 재래전을 결합한 형태의 융복합전이 될 것으로 판단된다.

미국은 세계 최초로 사이버전 역량 평가 방법론을 개발하여 세계 국가들에 대한 평가를 수행함으로써 사이버 강대국다운 면모를 보이고 있다[1]. 사이버전을 대비하기 위해서는 국가에 대한 사이버전 역량을 알아야한다. 한국은 아직 전쟁 중인 휴전 국가이며, 북한은 여전히 다양한 방법으로 도발을 해오고 있다.

본 논문에서는 사이버전의 개념 연구와 국가별 사이버 역량 평가 방법을 비교 분석하고 보완점을 도출하여 국가 사이버전 역량 평가 방법을 향상 했다. 한국에 영향을 줄 수 있는 국가들로, 먼저 한국과 군사력으로 대치하고 있는 국가인 북한, 북한과 밀접한 관계를 맺고 있는 중국과 러시아, 한국과 동맹국인 미국을 주요 5개국으로 선정하여 사이버전 역량 평가를 실시하였으며, 이를 기반으로 한국의 사이버전 대응 방안에 대해서 제시했다.

Ⅱ. 사이버전 역량평가 방법 관련 연구

세계 강대국들이 육·해·공·우주에 이어 제 5의 전장으로 사이버 공간을 간주하고[3] 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.

미국의 사이버 역량 평가 방법과 국내 연구소의 사이버 역량 평가 방법의 장·단점을 분석해보고 사이버전 역량 평가 방법에 대한 객관적이고, 정량적인 표준안을 제시해보고자 한다.

2.1. Technolytics 군 사이버전 역량평가

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 산정하였으며, 표 1과 같이 정리된다[4].

표 1. 국가 사이버 역량 평가[4]
Table. 1 Country Cyber Capabilities Ratings[4]

Cyber Military Capablities	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
China	4.2	3.8	4.0	4.0
United States	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.5	3.7
India	4.0	3.5	3.5	3.7
Iran	4.1	3.4	3.4	3.6
Korea, North	4.2	3.4	3.3	3.6
Japan	3.9	3.3	3.5	3.6
Israel	4.0	3.8	3.0	3.6
Korea, South	3.5	3.0	3.2	3.2
Pakistan	3.9	2.7	2.6	3.1

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 안 되며, 사이버 방어 역량까지 같이 평가가 되어야 한다.

2.2. Richard A. Clarke 사이버 역량 평가

Richard A. Clarke는 공격(Offense : 타 국가를 공격할 수 있는 능력), 방어(Defense : 공격에 대한 저지 및 완화 능력), 의존(Dependence : 국가기반시설이 네트워크에 연결된 정도로 전산화가 덜 될수록 높음) 세가지 범주에 대해 저자의 주관적인 판단에 의해 점수를 부여하고 각 분야의 점수를 총합하여 평가를 수행하였으며, 표 2와 같이 정리된다[5].

표 2. Richard A. Clarke 사이버전 역량 평가[5]
Table. 2 Richard A. Clarke, Competency evaluation of the cyber warfare[5]

Nation	Offense	Defence	Dependence	Total
United States	8	1	2	11
China	5	6	4	15
Russia	7	4	5	16
Korea, North	9	9	9	18

Richard A. Clarke의 사이버 역량 평가에서는 10점 만점으로 공격과 방어는 역량이 높을수록 높은 점수를, 정보시스템 의존도는 의존도가 높을수록 낮은 점수를 부과하였고, 이에 대한 총합으로 사이버전 역량을 제시하였다[9].

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.

2.3. 사이버戰 抑止力 평가모델에 관한 연구

참고문헌 [8]의 내용 중에서는 사이버 역량 평가 분야를 제도, 방어(국가통합관제, 관문관제, 전역・광역 관제, 지역관제, 경량관제, 정보공유, 복구), 공격(공격 전 단계 : 정찰・준비, 침투 및 생존 단계 : 침투・은닉・회피, 목표달성 단계 : 정보획득・파괴・선전, 공격 후 단계 : 평가・종료) 역량을 세가지 평가 그룹으로 점수를 부여하고 각 분야에 가중치를 도출하고 평가항목별 수준값을 산출함으로써 평가를 수행하였으며, 표 3과 같이 정리된다[8].

표 3. 한·미 사이버戰 抑止力 지수 종합 비교[8]
Table. 3 Index integrated comparison cyber warfare deterrent force, Korea & America[8]

Nation		System	Defence	Offense	Total
Weight		0.20	0.45	0.35	1
United States		4.69	4.74	4.71	4.72
Korea, South		1.91	2.10	1.89	1.99
Deterrent Force	Index	2.78	2.64	2.82	2.73
	Percentage(%)	40.72	44.30	40.13	42.16

평가 항목을 세분화하여 델파이(Delphi) 기법을 이용하고 AHP(Analytic Hierarchy Process) 기법을 적용한 체계적인 평가를 진행하였지만, 한국과 미국만의 사이버전 억지력 지수를 비교하여 실질적으로 북한과 대립하고 있는 실정에서 북한의 사이버戰 抑止力 지수를 산출한지 못한 한계점을 나타내고 있다.

2.4. 국가 사이버 역량 평가 방법론 연구

참고문헌 [1]의 내용 중에서는 사이버 역량 평가 분야를 기반(영토, 자원, 인구, 기타), 공격(정보수집, 침투, 파괴 / 무력화), 방어(예방, 대응, 탐지) 역량을 세 가지 평가 그룹으로 점수를 부여하고 각 분야의 평균치로 평가를 수행하였으며, 표 4와 같이 정리된다[1].

표 4. ETRI, 국가 사이버 역량 평가[1]
Table. 4 ETRI, Competency evaluation of the national cyber warfare[1]

Nation	Foundation	Offense	Defence	Total
United States	8.6	8.9	9.5	9.0
China	6.9	8.9	5.3	7.0
Japan	4.2	5.5	6.0	5.2
Russia	3.3	8.4	5.6	5.8
Korea, South	5.5	6.0	8.0	6.5

참고문헌 [2]의 내용 중에서는 북한의 사이버전력에 대해서 체계적으로 분석을 진행하였는데, 이러한 부분 중 기반역량 세부평가 항목으로 교육 체계 구축, 연구개발, 전략과 전술, 사이버 독트린 / 정책을 적용하는 것에 대해 한계점과 현재의 사이버 공격 무기체계들을 최신화하여 적용하는 것에 대한 한계점을 보였다.

Ⅲ. 사이버전 역량평가 방법 보완 방향

사이버전 역량은 사이버전을 수행할 수 있는 능력을 말하며 군사력의 일부분으로 포함된다. 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.

3.1. 사이버전 기반 역량 평가 방법 보완

사이버전 기반 역량은 ETRI 부설 연구소에서 개발한 '국가 사이버 역량 평가 방법론 연구' 중 기반 역량을 기초로 작성하였다[1]. 추가적인 보완은 '북한의 사이버 전력 현황과 한국의 국가적 대응전략'에서 북한의 사이버 전력을 10가지(사이버 인프라, 사이버전력에 관한 관심 및 투자, 사이버무기 체계와 기술적 능력, 사이버전사, 교육훈련체계, 수행조직체계, 사이버전 관련 연구개발, 사이버 독트린 : 정책 및 제도, 사이버 전략과 전술, 사이버 국제협력)로 나누어 분석을 하였는데 이러한 10가지 중 사이버 무기 체계와 기술적 능력을 제외한 9가지를 기반 역량에 추가 보완하였으며, 표 5와 같다[2].

표 5. 사이버전 기반 역량 평가 방법 보완
Table. 5 Complementary methods of foundation capability of the cyber warfare

Division	Detailed Capability Item
Territory (Infrastructure)	Network Level, System Level
Resources	IT Budget, Information Protection Budget
Troops	Cyber Warrior, Training System, Education System, Research & Development, Control Tower
Ect	International Cooperation , Strategy & Tactics, Cyber Doctrine / Policy

3.2. 사이버전 공격 역량 평가 방법 보완

사이버 공격 역량은 '사이버전 개론' 중 사이버전 공격 무기 체계에 관한 내용[6]을 토대로 사이버전 공격 역량 평가 방법을 보완하였다.

표 6. 사이버전 공격 역량 평가 방법 보완
Table. 6 Complementary methods of offence capability of the cyber warfare

Division	Detailed Capability Item
Information Collection	Foot-Printing(Insider Threat, Scavenging), Scan, Digital Snooping
Attack techniques of System	Buffer OverFlow, Backdoor, DDoS, Tunneling Malicious code(Computer Virus, Internet Worm, Trojan Horse Logic Bomb)
Attack techniques of Network	DoS, Spoofing
Hardware Weapon Systems	Chipping, TEMPEST, Nano Machine, EMP, HERF GUN

사이버전의 목표는 개인이 아닌 국가를 대상으로 하기 때문에 현존하는 사이버 공격 기술들을 토대로 국가에 위협하는 공격 항목을 선정하여 보완하였으며, 표 6과 같다.

3.3. 사이버전 방어 역량 평가 방법 보완

참고문헌 [1]의 내용 중 방어 역량과 참고문헌 [6]의 내용 중 사이버전 방어 체계를 토대로 사이버전 방어 역량을 보완하였다. 사이버전 방어 역량은 현존하는 사이버 무기를 방어할 수 있는 시스템을 체계적으로 물리적, 시스템, 네트워크 보안기술, 기타 활동(사이버 포렌식 기술과 CERT 활동, 통합보안관리 시스템)으로 나누어 보완하였으며, 표 7과 같다.

표 7. 사이버전 방어 역량 평가 방법 보완
Table. 7 Complementary methods of defence capability of the cyber warfare

Division	Detailed Capability Item
Physical Security Technology	Facility Security, Access Control
System Security Technology	User Authentication, System Security Settings, Access Control, Antivirus Programs, Malware Analysis
Netwark Security Technology	An Early Warning System, Intrusion Detection System, FireWall, Intrusion Prevention System, Virtual Private Network, Honey System(Honey Pot)
Ect	Cyber ForensicReadiness, Forensic Experts, CERT Activities, Enterprise Security Management

Ⅳ. 사이버전 역량 평가 비교 / 분석

4.1. 주요 5개국의 사이버전 역량 평가 결과

주요 5개국에 대한 사이버전의 역량 평가를 연구하기 위해 델파이(Delphi) 기법을 활용하여 정보보호 전문가 및 군사 전문가 20명을 대상으로 설문조사를 실시하였으며, 세부 역량 평가 결과는 표 8, 표 9, 표 10과 같다. 사이버전 종합 역량은 표 11과 같으며, 각국에 대한 비교 그래프는 그림 1과 같다.

표 8. 주요 5개국에 대한 사이버전 기반 역량 평가
Table. 8 Foundation capability assessment of the cyber warfare about five major countries

Detailed Capability Item	United States	China	Russia	Korea, North	Korea, South
Network Level	0.68	0.47	0.35	0.19	0.37
System Level	0.35	0.22	0.15	0.12	0.21
Territory Total	1.03	0.69	0.50	0.31	0.58
IT Budget	0.1	0.06	0.05	0.04	0.05
Information Protection Budget	0.3	0.22	0.18	0.09	0.11
Resources Total	0.4	0.28	0.23	0.13	0.16
Cyber Warrior	0.7	0.51	0.35	0.30	0.23
Training System	0.53	0.4	0.24	0.31	0.17
Education System	0.5	0.35	0.28	0.23	0.2
Research & Development	0.45	0.35	0.26	0.14	0.17
Control Tower	0.8	0.56	0.43	0.32	0.29
Troops Total	2.98	2.17	1.56	1.3	1.06
International Cooperation	0.25	0.17	0.14	0.08	0.11
Strategy & Tactics	0.25	0.18	0.13	0.12	0.08
Cyber Doctrine / Policy	0.05	0.04	0.03	0.02	0.02
Ect Total	0.55	0.39	0.3	0.22	0.21
Overall Foundation Rating	4.96	3.53	2.58	1.95	2.01

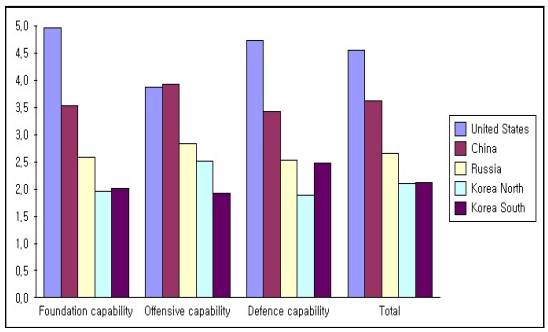

그림 1. 주요 5개국에 대한 사이버전 역량 평가 비교
Fig. 1 Comparing capability assessment of the cyber warfare about five major countries

표 9. 주요 5개국에 대한 사이버전 공격 역량 평가
Table. 9 Offence capability assessment of the cyber warfare about five major countries

Detailed Capability Item	United States	China	Russia	Korea, North	Korea, South
Insider Threat	0.44	0.46	0.26	0.26	0.28
Scavenging	0.09	0.09	0.05	0.05	0.04
Scan	0.08	0.08	0.05	0.04	0.06
Digital Snooping	0.14	0.17	0.13	0.09	0.07
Information Collection Total	0.75	0.80	0.49	0.44	0.45
Buffer OverFlow	0.25	0.23	0.2	0.14	0.12
Computer Virus	0.35	0.32	0.23	0.23	0.18
Internet Worm	0.26	0.27	0.22	0.21	0.09
Trojan Horse	0.35	0.32	0.24	0.13	0.16
Logic Bomb	0.2	0.19	0.16	0.12	0.08
Backdoor	0.35	0.36	0.24	0.23	0.18
DDoS	0.23	0.29	0.16	0.22	0.13
Tunneling	0.28	0.26	0.23	0.21	0.13
Attack techniques of System Total	2.27	2.24	1.68	1.49	1.07
DoS	0.28	0.32	0.27	0.23	0.13
Spoofing	0.17	0.18	0.12	0.15	0.1
Attack techniques of Network Total	0.45	0.50	0.39	0.38	0.23
Chipping	0.16	0.17	0.11	0.1	0.06
TEMPEST	0.11	0.12	0.1	0.06	0.05
Nano Machine	0.05	0.04	0.03	0.02	0.02
EMP	0.05	0.04	0.03	0.02	0.02
HERF GUN	0.05	0.04	0.03	0.02	0.02
Hardware Weapon Systems	0.42	0.41	0.3	0.22	0.17
Overall Offense Rating	3.87	3.93	2.84	2.52	1.92

표 10. 주요 5개국에 대한 사이버전 방어 역량 평가
Table. 10 Defence capability assessment of the cyber warfare about five major countries

Detailed Capability Item	United States	China	Russia	Korea, North	Korea, South
Facility Security	0.34	0.25	0.21	0.12	0.18
Access Control	0.48	0.35	0.28	0.28	0.26
Physical Security Technology Total	0.82	0.6	0.49	0.4	0.44
User Authentication	0.39	0.33	0.23	0.20	0.21
System Security Settings	0.30	0.23	0.20	0.15	0.16
Access Control	0.36	0.25	0.17	0.16	0.19
Antivirus Programs	0.2	0.13	0.1	0.07	0.11
Malware Analysis	0.05	0.04	0.02	0.02	0.03
System Security Technology Total	1.3	0.98	0.72	0.6	0.7
An Early Warning System	0.45	0.33	0.21	0.20	0.17
Intrusion Detection System	0.25	0.18	0.11	0.09	0.12
FireWall	0.4	0.29	0.19	0.15	0.2
Intrusion Prevention System	0.29	0.21	0.17	0.08	0.15
Virtual Private Network	0.13	0.1	0.07	0.06	0.11
Honey System (Honey Pot)	0.2	0.15	0.11	0.06	0.09
Netwark Security Technology Total	1.72	1.26	0.86	0.64	0.84
Cyber Forensic Readiness	0.05	0.04	0.03	0.02	0.03
Forensic Experts	0.1	0.07	0.06	0.03	0.05
CERT Activities	0.15	0.1	0.07	0.05	0.09
Enterprise Security Management	0.6	0.38	0.34	0.18	0.36
Ect Total	0.9	0.59	0.5	0.28	0.8
Overall Defense Rating	4.73	3.42	2.54	1.88	2.48

표 11. 주요 5개국에 대한 사이버전 역량 평가
Table. 11 Capability assessment of the cyber warfare about the five major national

Division	United States	China	Russia	Korea, North	Korea, South
Foundation capability	4.96	3.53	2.58	1.95	2.01
Offensive capability	3.87	3.93	2.84	2.52	1.92
Defence capability	4.73	3.42	2.54	1.88	2.48
Total	4.56	3.62	2.65	2.1	2.12
Ranking	1	2	3	5	4

4.2. 한국의 사이버전 역량 강화 방안

주요 5개국과 한국의 사이버전 역량을 비교한 결과 기반역량의 5가지(컨트롤 타워 개선, 사이버 전사 규모 확장, 훈련 체계 보완, 교육 체계 보완, 연구개발 활성화), 공격역량의 전반적인 역량 강화, 방어역량에서 통합방위체계의 강화가 필요하다.

첫번째로 기반역량의 컨트롤 타워 개선이 필요하다. 2010년 1월 사이버 사령부를 창설하였으나, 준비단계에 머물러 아직은 적극적인 활동이 없는 것으로 판단되며, 그 실효성에 대한 개선을 촉구하는 의견도 나오고 있다[10]. 사이버사령부를 개편하여 육・해・공군 예하에 사이버 작전 부대를 창설하고 국방부 직속 사이버사령부가 총괄하도록 지휘체계를 구축하여 사이버전에 대비하여야 한다.

두번째로 사이버 전사 규모 확장을 위한 전문 인력 양성과 교육체계 보완을 위해서는 정보보호와 관련된 학과 개설로 전문 인력을 양성하고 중학교 때부터 전산 과목의 교육을 추가하는 등의 노력이 필요하다.

세번째로 사이버전에 대비한 훈련은 미국의 '사이버 스톰(2006년 국토안보부 주도로 격년으로 시행)'[7]처럼 국가 차원의 사이버전 대응훈련이 필요하며, 훈련의 취지도 국가 기반 시설을 보호 할 수 있는 능력을 갖추기 위해 실시를 해야 한다. 연구개발을 위해서 국방고등기술원 등에서 창의, 도전적 연구개발을 목표로 꾸준한 연구를 진행해야 한다.

네번째로 공격역량 강화는 전반적으로 이루어져야 하며, 사이버 공격 발생시 지체없이 원점까지 식별하여 역으로 타격을 하는 대응능력을 갖추어야 한다. 2010년

1월 윌리엄 린(William Lynn) 국방부 부장관은 “국방부에만 하루 수천 건의 해킹시도가 이뤄진다. 마지노선 뒤에 숨는 진지 방어로는 이런 공격을 막을 수 없다. 해커를 찾아내 반격을 가하는 방식의 ’능동적 방어‘가 이뤄져야 한다.”고 하였다[11].

사이버사령부 키스 알렉산더(Keith Alexander) 사령관은 미국이 북한이나 이란과 같은 적성국가로부터 사이버 공격을 받게 되면 지체 없이 대응해야 한다고 언급하였다[12].

다섯번째는 방어역량 강화로 사이버 공격에 대비하기 위해 이스라엘의 ‘디지털 아이언 돔(Ditital Iron Dome)’처럼 한국형 사이버 아이언 돔 체계를 구축하여야 하며, 미국 존스홉킨스대학 국제대학원의 Alexandre Mansourov 객원 연구원의 조언[13]처럼 'Kill-Chain'까지 확보해야 한다.

위에서 제시한 5가지의 세부 역량에 대해서 강화한다면 한국의 사이버전 역량은 북한의 사이버전 역량을 뛰어넘어 중국과 비슷한 역량을 갖게 될 것이다. 그렇게 된다면 세계 어느 국가도 쉽게 공격하지 못할 것이다.

Ⅴ. 결 론

이 연구를 통해 사이버전 역량 평가 방법론을 재정립하고 한국에 영향을 줄 수 있는 주요 국가들과 비교 / 분석하여 한국의 사이버전 역량을 강화할 수 있는 방향을 제시하였다.

날로 높아지는 사이버전의 위협 속에서 한국이 사이버전을 수행할 수 있는 기반을 굳건하게 다지는 계기가 되고, 사이버전 무기 체계를 계발하여 사이버전 공격 능력을 향상시킴과 동시에 사이버전 방어 능력까지도 갖춤으로 사이버 전쟁의 억제와 유사시에는 사이버전에서 승리함으로 사이버상에서의 평화는 물론 물리적인 국방력의 시너지 효과에도 기여하고자 한다.

REFERENCES

[1] J. M. Kang, H. U. Hwang, J. M. Lee, Y. T. Yun, B. C. Bae, and S. Y. Jung, "A Study on National Cyber Capability Assessment Methodology," *Korea Institute of Information and Cryptology*, Vol. 22, No. 5, pp 1039-1055, 2012.

[2] J. I. Im, Y. J. Kwon, G. H. Jang, and S. J. Baek, "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *The Quarterly Journal of Defense Policy Studies*, Vol. 29, No. 4, pp 9-45, 2013.

[3] U.S. Department Of Defense, “QUADRENNIAL DEFENSE REVIEW REPORT," February 2010. Available : http://www.defense.gov/qdr/QDR%20as%20of%2026JAN10%200700.pdf

[4] Kevin Coleman, “*Cyber Commander’s eHand-book version 2.0*,” Techolytics, 2012.

[5] Richard A. Clarke, “*Cyber War : the Next Threat to National Security and What to Do About It*,” copyrighted Material, 2010.

[6] J. H. Eom, S.S. Choi, and T. M. Jung, "*An Intoroduction of Cyber Warfare*," Hongrung Publiching Company, 2012.

[7] Y. D. Son, "*I WAR : How to Survive Cyber Cold War Countries*," Golden Owl, 2010.

[8] Y. D. Son, "An Evaluation Model for the Cyber War Deterrence," Department of IT Policy Management Graduate School Soongsil University, 2010.

[9] Charles Billo et al, “Cyber Warfare:An Analysis of The Means and Motivations of Selected Nation States," Institute for Security Technology Studies, 2004, Available : http://www.ists.dartmouth.edu/projects/archives/cyber-warfare.html

[10] H. J. Kim, "Paper Cyber Command," Chosun Ilbo, 2010. 5. 30, Available : http://premium.chosun.com/site/data/html_dir/2010/05/30/2010053067001.html

[11] Y. I. Muk, "US 'Hacking Yen Retaliation' Cyber Evolution Declared," Chosun Ilbo, 2010. 1. 28, Available : http://www.chosun.com/site/data/html_dir/2010/01/28/2010012800095.html

[12] G. Y. Lee, "The US, Should Respond without Delay to the North Cyber Attacks," YTN, 2010. 4. 15, Available : http://www.ytn.co.kr/_ln/0104_201004150213183052

[13] K. D. Ryu, "If North Korea of Cyber Attacks, ROK-US Defense Treaty Should Be Applied," ETNEWS, 2014. 12. 3, Available : http://www.etnews.com/20141203000241

박찬수(Chan-soo Park)

계명대학교 수학과 (학사)
세종사이버대 정보보호 대학원 (석사)
현재 육군 간부
※관심분야 : 산업/국방 보안

박용석(Yongsuk Park)

서강대학교 컴퓨터공학 (학사)
뉴욕(POLY)대 (석사, 박사)
AT&T Bell Labs
삼성전자
현재 세종사이버대학교 정보보호 대학원 주임교수
현재 정보보호컴퓨터정보통신 학부 교수
※관심분야 : IT 서비스 및 보안, 산업보안, 클라우드, 웨어러블 컴퓨팅 등