

국방 사이버 무기체계와 기존 재래식 무기체계의 핵심기술 수준 및 특성 비교 연구

이 호 균,^{1†} 임 종 인,² 이 경 호^{2*}
¹국방기술품질원, ²고려대학교 정보보호대학원

Comparison Study between the Cyber Weapon System and the Conventional Weapons Systems on Their Core Technologies Levels and Features

Ho-gyun Lee,^{1†} Jong-in Lim,² Kyung-ho Lee^{2*}
¹Defense Agency for Technology and Quality,
²Graduate School of Information Security, Korea University

요 약

2006년 방위사업청 개청 이후 국방 핵심기술 연구개발 사업은 단순히 무기체계 자체개발뿐만 아니라 첨단기술 확보를 통한 과학기술력 향상, 방위산업 육성 그리고 민간기술과의 상호 발전을 기대하는 수준에 이르렀다. 2015년부터 새롭게 국방 무기체계로 추가된 사이버 무기체계는 이스라엘의 사례에서 보는 바와 같이 국방력 향상과 산업 발전 모두를 기대할 수 있는 유망 무기체계 분야이다. 본 논문은 사이버 무기체계의 기술기획 방향 수립을 위해 지금까지 발표된 국방 핵심기술 수준조사 결과를 활용하여 사이버 무기체계의 기술수준과 특성을 다른 무기체계와의 비교를 통해 다 각도로 분석하였다. 분석결과 사이버 무기체계는 민간 분야의 기술 축적을 통해 상대적으로 높은 기술수준을 보유하고 있으나 국방 분야에서 상대적으로 늦게 정식 무기체계로 편입되었고, 능동적 대응사례가 부족하기 때문에 국가 순위는 낮게 조사되었다. 그러나 선진국과의 기술격차는 가장 낮은 그룹으로 분석되어 무기체계 획득 및 핵심기술 연구개발 사업을 효율적으로 추진한다면 빠른 시일 내에 우수한 사이버 전력을 확보할 것으로 기대된다.

ABSTRACT

Since the inauguration of Defense Acquisition Program Administration(DAPA) in 2006, the national defense core technology research & development business has not only pertained to the weapons systems development but also to the improvement of the national science & technology capability via the acquisition of cutting-edge technologies. Furthermore, it has been closely related to the promotion of the defense industry and the mutual improvements of defense and civil technologies. The cyber warfare weapon system, a newly added national defense weapon system field since 2015, has become a promising weapon system branch for improving the national defense power as well as the national defense industry as shown in the case of Israel. By utilizing the existing result of the national defense core technology level, in order to establish the direction of technology planning of the cyber warfare weapon system, this paper analyzes the technology level and features of the cyber warfare weapon system in various aspects via comparisons with other weapons systems. The result of these analyses shows that the cyber warfare weapon system possesses a relatively high technology level due to the technology accumulation in the civilian sector while the relatively slow inclusion to the national weapons systems and the lack of the correspondence case regarding aggressive cyber responses in the defense sector yields a relatively low national rank. However, the technological gap between South Korea and

the most advanced country in the field of cyber warfare technology is analyzed to be among the lowest, which indicates that with efficient and effective pursuits in terms of the weapons systems acquisitions as well as the core technologies research & development business, an outstanding cyber warfare capacity can be obtained in a short time.

Keywords: Technological Planning, Cyberwarfare, Information Security, Technology Level Assessment

I. 서 론

국방부에서는 국방 분야가 직면한 다양한 도전을 극복하기 위해 창조국방 정책을 추진 중에 있다. 창조국방은 과학기술을 다양한 국방 업무와 융합하여 혁신적인 가치를 창출하는 패러다임으로 창의적 운용 개념 도출, 고효율 국방경영, 선도형 군사력 건설, 민군 상생의 융합 생태계 조성으로 구성된다[1].

사이버무기체계는 2015년 8월부터 전력발전훈련령 개정을 통해 정식 무기체계로 분류되었다[2]. 사이버무기체계는 창조국방을 실현할 수 있는 주요 분야로 많이 선정되곤 한다. 북한의 비대칭 전력에 대응하는 전력을 구축할 수 있다는 점에서 선도형 군사력 건설을 만족하면서 민간의 우수 정보보호 기술들을 접목할 수 있기 때문에 민군 상생의 융합 생태계 조성에도 다양한 기회를 찾을 수 있기 때문이다.

사이버무기체계가 각광받는 또 다른 이유는 기존 무기체계에 비해서 획득비용이 낮고 선진국과의 기술 격차가 작을 것이라는 믿음 때문에 북한과 같이 획득 비용이 높은 재래식 전력 확보가 어려운 국가가 취할 수 있는 매력적인 비대칭 전력으로 활용되기 때문이다. 또한 이스라엘의 사례에서 보듯이 강한 사이버 전력은 정보보호 산업 육성과 같은 경제적 파급효과도 높을 것이라는 기대도 한 몫을 하고 있다.

본 논문에서는 2013년부터 국방 분야에서 발표된 조사 자료들을 활용하여 사이버무기체계의 기술수준 및 각종 특성을 분석하고 있다. 이를 통해서 앞서 언급한 다양한 사이버 무기체계에 대한 기대들이 타당한지 확인한다. 논문의 구성은 다음과 같다. 2장에서는 기존 선행연구의 조사결과를 기술한다. 3장에서는 본 논문에서 적용한 연구방법론을 설명하고 4장은 연구방법론에 따른 조사분석 결과를 항목별로 제시한다. 마지막으로 5장에서는 결론을 기술한다.

II. 선행 연구

2.1 국방 분야 기술수준조사 사례 및 방법론

국방 분야에서는 2007년부터 국방기술품질원에서

무기체계 기술에 대한 국가별 수준조사 및 국내 기술별 수준조사를 수행하고 있다. 2013년 국방과학기술 조사서는 최초로 사이버무기체계가 추가되어 기술분류별 기술수준, 핵심기술군 선정, 핵심기술군 기술수준, 핵심기술 로드맵 등을 수록하고 있다[3]. 특히 핵심기술군에 대한 기술수준과 특성 조사에는 최고기술 보유국, 최고기술보유국 기술수준, 한국의 수준, 기술 난이도 등을 포함하고 있다.

2015년 국방 정보기술 조사서는 민군 협력 측면에서 유망 민간 정보기술을 선정하고 선정 기술의 국방 적용방안을 조사하였다[4]. 정보기술 5개 분야를 조사했으며 여기에는 사이버무기체계에 해당하는 정보보호기술도 포함된다. 선정된 유망기술들에 대해서 최고선진국 대비 기술수준, 기술격차, 국방분야 활용 가능성, 기술 중요성, 파급효과 등을 조사하였다.

2015년 국가별 국방과학기술 수준조사에서는 8대 무기체계 분야, 26개 대표무기체계를 대상으로 16개국의 기술수준을 조사하여 국가별 순위를 도출하였다[5]. 이 조사에서는 국가별 수준조사 최초로 사이버전 분야를 추가하여 선진국 대비 한국의 순위를 조사하였다.

2.2 사이버전 분야 기술수준조사 사례 및 방법론

사이버전 전문가의 단행본 또는 민간연구기관 등에서 수행한 기존 연구들은 당시의 주요 이슈와 그 이슈로 인한 연구자의 방법론 수립 방향, 조사결과 분석 등을 검토할 수 있는 연구 자료가 될 수 있다. Technolytics는 2009년 연구에서 160여개국 대상의 정량적인 군 사이버 역량 평가모델을 제시하였다[6]. 역량 평가모델은 역량목적, 공격역량, 정보수집 세 가지 요소로 구성되며, 공격역량과 정보수집에서 높은 평가를 받아 미국과 중국이 공동 1위, 한국이 9위로 선정되었다. 이때 공격 역량은 다시 세분화되어 공격 경험, 공격역량 등급, 정보수집 경험으로 구성되었고, 공격 역량에서는 중국이 단독 1위, 한국이 9위로 평가되었다. Richard는 2010년 그의 저서에서 주요 5개국에 대한 사이버 전투력 평가 순위를 제시하였다. 평가모델은 공격력, 의존도, 방어력 세

가지 평가요소로 구성되었으며, 의존도와 방어력 측면에서 인터넷에 거의 의존하지 않는 북한을 1위 국가로 선정하고 한국은 조사대상에 포함되지 않았다 [7]. Economist지는 2011년 Cyber Power Index와 그 방법론을 발표하였다[8]. 이는 법/규제, 경제/사회적 여건, 기술 인프라, 산업적용 4개 요소로 구성되며 4개 항목에 대한 가중치 합산 결과 영국이 종합 1위, 한국은 종합 7위로 선정되었다. McAfee사에서는 2012년 사이버 방어 보고서에서 23개국에 대한 순위를 발표하였다. 본 조사는 정보보안업체에서 실시한 조사로써 방어 분야에 한정지어 분석하였고, 스웨덴, 핀란드 등 유럽의 IT 강국이 높게 평가받은 특성이 있었다[9]. 같은 해에 발표된 국가보안연구소의 국가 사이버 역량 평가방법론은 Technolytics와 유사한 정량적 평가모델로서 한국의 주변 강대국 5개국으로 대상으로 조사하였다. 조사결과 미국이 종합 1위, 한국은 러시아, 일본을 제치고 전체 3위로 조사되어 전체 조사결과 중 한국이 가장 우수하게 조사되었다[10]. 2013년 KEIT에서 발표한 산업기술수준조사는 한국의 정보보안 산업기술 수준에 대한 평가로 KISTEP, 기품원 등 정부출연 조사·분석·평가 전문기관의 조사방법론과 맥을 같이 한다. 주요 선진 5개국에 대한 설문조사를 통해 조사했으며 조사결과 한국은 미국, EU, 일본 다음인 4위권으로 조사되었다[11]. 가장 최근의 조사 결과는 호주 전략연구소에서 발표한 한태평양 지역 사이버 성숙도 조사이다. 정량적 방법론을 사용했으며 평가요소는 정부, 국방, 디지털 경제, 사회 4가지 요소로 구성되었다. 조사 대상 16개국 중 미국이 1위, 한국은 미국, 영국, 호주 다음인 4위로 조사되었다[12].

III. 연구 방법

3.1 기술수준 조사 방법론

3.1.1 가 설

본 연구에서는 사이버무기체계에 대한 일반적인 기대와 관련된 세 가지 가설을 검토하고자 한다. 첫째, 국방분야의 핵심기술군에 대한 기술수준조사 데이터를 활용하여 사이버무기체계 소요기술은 선진국과의 기술격차가 낮을 것이라는 기존의 가정을 분석 및 확인하고자 한다. 분석을 위한 가설은 다음과 같다.

가설 1. 사이버무기체계 소요기술들은 기존 재래식 무기체계 소요기술에 비해서 선진국과의 기술격차가 작은 그룹에 속할 것이다.

둘째, 정보보호 분야 유망기술은 민군기술 협력 가능성이 높을 것이라는 기존의 가정을 검토하기 위해서 다음과 같은 가설을 설정한다.

가설 2. 사이버전(정보보호) 분야 민간 유망기술들은 기존 재래식 무기체계 관련 유망기술에 비해서 국방분야 활용 가능성이 더 높을 것이다.

셋째, 2015년 기품원에서 발표한 사이버전 분야에 대한 국가별 국방과학기술 수준조사 데이터를 활용하여 사이버무기체계의 발전은 실제 작전 사례의 경험과 비례할 것이라는 기존의 가정을 검토한다. 검토를 위한 가설은 다음과 같다.

가설 3. 사이버무기체계 기술수준은 실제 작전 사례와 양의 관계를 가질 것이다.

3.1.2 조사대상

본 논문에서는 앞서 제기한 세 가지 가설을 검증하기 위해 2013년부터 발표된 세 가지 국방과학기술 조사 자료의 데이터를 분석하고 있다. 2013년 국방과학기술조사서에서는 미래 무기체계 확보를 위해 필요한 소요 핵심기술을 선정하고 핵심기술에 대한 수준 및 특성을 조사하였다. 27대 대표무기체계, 215개 미래무기체계에 대해서 314개 핵심기술군, 1,163개 핵심기술을 조사하였다. 핵심기술군이란 미래소요 핵심기술 중 선택과 집중에 의해 자원투자가 필요한 분야로 하나 이상의 핵심기술로 구성되어, 기술개발시 획득 목표가 되는 단위 또는 기능/목표가 유사한 기술의 조합을 말한다. 26개 대표 무기체계의 핵심기술군의 기술수준과 특성 데이터를 가설 1의 검증을 위한 분석대상으로 선정하였다. 이때 2013년 국조서에서 국방SW 분야는 핵심기술군별 기술수준조사가 시행되지 않아 제외하였다.

2015년 국방 정보기술조사에서는 국방 적용가능 IT 기술 255개와 순수민간 IT 기술 245개를 검토하여 총 500개의 정보기술로 구성되는 민군통합 정보기술 목록을 수립하고, 5개 분야, 43개의 유망기술을 선정하였다. 각 유망기술에 대해서 국방분야 활

Table 1. Survey Participants Statistics for Defense Core Technology Assessment for 3 years

	Total	Industry	ADD	DTaQ	Military	Academia	Research Institute
2013 Defense Science and Technology Survey	552	225	170	45	40	38	34
2013 Defense Science and Technology Survey (Cyberwarfare)	12	0	5	0	0	2	5
2015 Defense Information Technology Survey	71	25	13	0	2	8	23
2015 Defense Information Technology Survey (Information Security)	12	1	2	0	1	2	6
2015 Defense Science and Technology Level Assessment by Country	254	112	46	39	9	18	30
2015 Defense Science and Technology Level Assessment by Country (Cyberwarfare)	9	2	2	0	0	2	3

용 가능성, 전략적 중요성, 파급효과, 기술수준 및 기술격차, 파급효과, 투자주체, 개발주체, 군 적용방안 등을 조사하였으며, 5개 분야 중 3개 분야(지휘통제, 사이버전, 전술통신) 27개 유망기술의 조사결과를 가설 2의 검증을 위한 분석대상으로 선정한다.

2015년 국가별 국방과학기술조사에서는 8대 분야 26개 대표무기체계를 대상으로, 선진 국방기술 보유 16개국에 대한 국가별 기술수준을 조사하였다. 27대 대표무기체계 중 특수무기체계는 개발 실적이 있는 국가가 많지 않아 제외되었다. 조사대상 국가는 국방비 지출 규모, 국가별 국방R&D 투자규모 및 무기수출 등을 고려하여 16개국을 선정하고, 이중 한국의 사이버전 순위를 가설 3의 데이터로 활용한다.

3.1.3 전문가 구성

Table 1은 분석대상으로 활용한 세 가지 조사에 참여한 전문가들의 분야별 통계를 보이고 있다 [3][4][5]. 기술수준 설문조사를 위한 전문가 구성은 군·산·학·연 등의 국방기술전문가들로 분야별 대상그룹을 선정하였고, 3년 동안 3가지 조사에 대해서 877명의 전문가가 참여하였다. 전문가들은 방위사업관리규정에 의거하여 각 무기체계별/기술별 업무경력이 10년 이상인 연구원, 교수, 군인 등이 참여하였으며, 국과연의 경우 각 개발본부별로 공문을 통해 추천과정을 거쳤다. 13년 국조서에 552명, 15년 정보기술조사에 71명, 15년 국가별 수준조사에 254명이 각각 참여하였다. 전체 877명 중 사이버무기체계는 33명의 전문가가 참여하였다.

3.1.4 조사방법

2013년 국방과학기술조사에서는 핵심기술군에 대한 수준 및 특성을 조사하기 위해 2차에 걸친 설문조사와 전문가토론회 방식을 적용하고, 수준 분석에는 동태적 수준조사 방법을 사용하였다. 314개 핵심기술군에 대해서 최고기술보유국, 국내외 기술수준, 기술격차, 난이도, 파급효과 등을 조사했으며 기술성장모형(Gompertz 모형)을 활용하여 기술발전속도를 예측하였다. 본 논문에서는 조사항목 중 국내외기술수준과 난이도를 이용하여 가설 1을 검증한다 [3].

2015년 국방 정보기술조사에서는 KISTEP의 국가과학기술표준분류체계, KIAT의 2012 산업 기술로드맵, TTA의 2013 ICT 표준화전략맵, 기품원의 국방과학기술분류체계를 활용하여 민군통합 IT 기술분류를 수립하고 이를 기반으로 다원속성효용이론을 적용하여 유망기술 43개를 도출하였다. 이때 다원속성효용이론 공식의 요소로 국방분야 활용 가능성, 전략적 중요성, 파급효과를 적용하였으며, 이중 가설 2의 검증을 위해 국방분야 활용 가능성을 검토하였다 [4]. 식 (1)은 유망기술 선정에 적용한 다원속성효용이론 공식이다.

$$\text{총점}(P) = \sqrt{m^2 + t^2 + e^2} \quad (1)$$

m : 국방분야 활용 가능성 (5점 척도)

t : 전략적 중요성 (5점 척도)

e : 기술적/경제적/사회적 파급효과 (5점 척도)

2015년 국가별 국방과학기술조사에서는 국가별 기

Table 2. Core Tech. Group Average per 26 Weapon System in 2013 Defense Science and Technology Survey

No	Weapon Systems	Number of Core Tech. Group	Core Tech. Group Average per Weapon System			
			Tech. Level of Developed Contry	Tech. Level of Korea	Relative Tech. Level compared with Developed Contry	Difficulty
1	Command Control	9	79.2	58.9	74.7	3.9
2	Cyber Warfare	5	82.6	67.4	81.8	4.2
3	Tactical Communication	10	85.6	64.2	77.6	2.9
4	Radar	17	85.0	55.5	65.2	3.9
5	SAR	15	86.6	53.1	65.7	4.5
6	EO/IR	13	91.0	62.5	68.6	3.2
7	Underwater Surveillance	12	84.1	55.8	66.2	4.2
8	Electronic Warfare	11	88.7	67.1	75.8	3.5
9	Maneuver Combat	7	85.1	61.3	73.2	3.4
10	Ground Unmanned	10	76.3	62.6	82.5	3.1
11	Individual Combat	15	69.9	51.9	77.9	3.0
12	Surface Ship	5	89.2	62.2	69.4	2.8
13	Submarine	5	87.4	63.2	72.0	3.4
14	Maritime Unmanned	5	82.0	61.8	76.4	2.6
15	The Fixed Wing Aircraft	10	93.3	63.6	68.2	3.1
16	Rotary Wing Aircraft	10	90.2	54.7	60.7	3.3
17	Unmanned Aerial Vehicle	7	85.0	62.0	73.1	4.3
18	Space Weapons	9	94.0	48.6	51.8	3.1
19	Artillery Gun	11	84.1	62.3	72.0	2.9
20	Ammunition	7	91.6	57.2	63.4	1.9
21	Guided Weapons	36	91.2	62.4	67.8	2.9
22	Underwater Guided Weapons	19	88.4	65.5	74.6	3.3
23	Special Weapon	22	80.9	55.8	65.6	3.6
24	Air Defense Weapon	11	83.0	64.7	78.7	4.0
25	CBR Weapon	11	85.7	64.5	75.3	3.1
26	Defense M&S	6	88.9	69.9	78.7	4.4
	Average		85.7	60.7	71.4	3.4

술수준 조사를 위해 인텔리전트 델파이 조사방법을 활용하였다. 기존 델파이 설문은 합의가 이뤄지지 않을 경우, 설문 반복으로 시간과 비용이 과다 증가하는 단점이 있고, 국방 분야 수준조사는 정보공개가 제한되어 참여 전문가마다 보유하고 있는 기반 정보가 다르다는 문제점이 있었다. 이를 개선하기 위해 기초자료를 사전에 제공하고, 웹 방식으로 2차에 걸쳐 설문조사를 진행하였다. 전문가 간 합의도 목표는 80%를 설정하였으며, 합의가 되지 않을 경우, 전문가토론회를 통해 전문가 간 합의를 유도하였다. 식

(2)는 전문가 간 합의도를 계산하는 공식이다.

$$TheAgreementLevel = 1 - \frac{(3rdQuartile - 1stQuartile)}{Median} \quad (2)$$

1차 설문에는 각 국가의 사이버전 관련 연구개발 및 운용현황, 조직 및 연구개발사업의 주요 특징 등이 포함된 기초자료를 제공하여, 제공한 기초자료와 전문가의 의견을 기반으로 한 최고선진국 대비 기술수준을 평가하고 평가근거를 작성하도록 하였다. 이때

점수대간의 명확한 의미를 사전에 정의하여 제공함으로써 전문가의 기술수준 판단에 기준을 제공하였다 [5].

IV. 분석 결과

4.1 사이버무기체계 소요기술의 기술수준

Table 2는 26개 대표무기체계별로 도출된 핵심

기술군의 최고선진국 절대기술수준, 국내 절대기술수준, 국내 상대기술수준과 난이도의 평균을 보이고 있다[3]. 상대기술수준이란 국내 절대기술수준을 최고선진국 절대기술수준으로 나눈 값을 말한다. 사이버 무기체계의 경우 최고선진국 절대기술수준은 26개 무기체계 중 21위, 국내 절대기술수준은 2위, 상대적 기술수준 2위, 난이도는 4위였다. 지상무인체계와 사이버무기체계 모두 기존 재래식 무기체계에 비해서 신설된 무기체계 분야로 최고선진국도 우리와

Table 3. 2015 IT Promising Technologies Assessment for Defense Sector

분야	Promising Technologies	Tech. Level compared with Developed Contry	Technology Gap/year	Defense Application Possibility	Strategic Importance	Sillover Effect Average
Cyber Warfare (Information Security)	Intrusion Detection	82	2	5.0	5.0	5.0
	VPN	80	1.5	5.0	4.9	4.8
	IoT/M2M Security	70	6	4.1	4.5	5.0
	Video Security	80	2	4.8	4.7	4.8
	Security Vulnerability Anlysis	70	6	3.7	4.6	4.9
	SW Security Evaluation	70	6	4.2	4.7	4.7
	Smartphone Security	80	5	4.7	4.8	5.0
	Secure OS	85	3	4.3	4.9	4.9
	Biometrics	85	2	3.9	4.6	4.5
	Security Platform	70	3	4.7	4.8	4.5
	Confidential Leakage Prevention	85	5	4.7	4.7	4.2
	Average	77.9	3.8	4.5	4.7	4.8
Tactical Communication (Information Communication Network)	Maneuver/Anti Electronic Warfare Battle Mobile Comm	85	7	4.6	4.3	4.5
	Large Capacity/Maneuver Multi-Link Wireless Transmission	85	5	4.5	4.4	4.3
	Anti Jamming/Large Capacity Satellite Comm. Payload	50	15	4.6	4.3	3.6
	Anti Jamming/Multi Band/OTM Satellite Terminal	70	6	4.6	4.1	3.8
	Air Relay Wireless Node	70	10	4.5	3.9	3.6
	Tactical Datalink Communication	80	6	4.4	3.8	3.4
	Advanced Multiple Antenna for Mobile Comm.	95	0.5	4.0	3.4	3.9
	Human Communication	90	2	3.8	3.8	3.7
Average	78.1	6.4	4.4	4.0	3.9	
Command Control (Battlefield/Resource Management)	Big Data	50	6	4.8	5.0	5.0
	Battlefield Information Fusion	66	6	5.0	5.0	4.3
	Intelligent Situational Awareness	50	10	4.9	5.0	4.4
	IoT	80	3	4.2	4.7	4.9
	Situational Awareness SW Framework	77	5	4.6	4.0	4.3
	Voice Processing SW	90	1	3.7	3.9	5.0
	Semantic Space Information	70	4	4.0	4.0	4.3
	3D Printing	66	6	3.2	4.0	5.0
Average	68.6	5.1	4.3	4.5	4.7	

마찬가지로 시작한 역사가 길지 않기 때문에 최고선진국의 기술수준이 상대적으로 낮고 국내 수준은 상대적으로 높은 수준으로 평가되었다. 또한 신설된 분야인 만큼 난이도도 상대적으로 높게 평가되었다.

설문조사데이터 분석결과 가설1에서 제시한 바와 같이 사이버무기체계는 선진국과 기술격차가 가장 낮은 그룹인 것으로 확인되었다. 설문에서 보듯이 사이버무기체계는 새롭게 운영개념이 수립되고 있는 분야인 만큼 기술기획을 잘 해서 국내 무기체계개념 수립 및 무기체계 개발을 잘 추진한다면 경쟁력 있는 무기체계 분야로 육성할 수 있을 것으로 판단된다.

4.2 정보보호 기술의 국방분야 활용 가능성

Table 3은 국방정보기술 관련 3개 대표무기체계별(지휘통제, 전술통신, 사이버전)로 도출된 민간 유망기술들의 최고선진국 대비 기술수준, 기술격차, 국방분야 활용 가능성, 전략 중요성, 파급효과의 대표 무기체계별 평균을 보이고 있다(4). 정보보호 기술의 경우 기존 무기체계에 비해서 기술격차가 가장 작고, 국방분야 활용 가능성, 전략 중요성, 파급효과가 가장 높은 것으로 조사되었다.

다른 정보기술의 경우 국방분야 활용을 위해서 별

Table 4. The score and rank of Korean Cyber warfare in 2015 Defense Science and Technology Level Assessment by Country

Weapon Systems	Sorted by Korean Rank		Weapon Systems	Sorted by Korean Score				
	2015			2015		2012		2010
	Score	Rank		Score	Rank	Score	Rank	Score
Artillery Gun	88	5	Maneuver Combat	89	7	88	7	83
Maneuver Combat	89	7	Artillery Gun	88	5	90	4	90
Unmanned Aerial Vehicle	85	7	Unmanned Aerial Vehicle	85	7	84	7	76
Ground Unmanned	81	7	Surface Ship	84	8	86	9	85
Surface Ship	84	8	Submarine	83	9	79	9	76
Command Control	81	8	Underwater Guided Weapons	83	10	82	10	82
Submarine	83	9	Tactical Communication	82	9	82	9	79
Tactical Communication	82	9	Guided Weapons	82	9	81	9	80
Guided Weapons	82	9	Air Defense Weapon	82	10	82	10	83
Defense M&S	79	9	Cyber Warfare	82	11	-	-	-
Individual Combat	77	9	Ground Unmanned	81	7	81	7	80
Underwater Guided Weapons	83	10	Command Control	81	8	81	8	76
Air Defense Weapon	82	10	Ammunition	81	10	77	11	77
Ammunition	81	10	Defense M&S	79	9	78	9	79
Rotary Wing Aircraft	79	10	Rotary Wing Aircraft	79	10	77	11	74
Electronic Warfare	76	10	EO/IR	79	11	80	11	77
Space Weapons	72	10	Maritime Unmanned	79	12	81	10	72
Cyber Warfare	82	11	Radar	78	12	79	12	75
EO/IR	79	11	Individual Combat	77	9	78	8	78
CBR Weapon	77	11	CBR Weapon	77	11	78	11	79
The Fixed Wing Aircraft	75	11	Underwater Surveillance	77	13	77	13	76
Maritime Unmanned	79	12	Electronic Warfare	76	10	77	10	79
Radar	78	12	SAR	76	12	75	12	73
SAR	76	12	The Fixed Wing Aircraft	75	11	73	13	72
Defense SW	75	12	Defense SW	75	12	76		
Underwater Surveillance	77	13	Space Weapons	72	10	71	11	74

도의 핵심기술연구와 체계개발이 필요하지만 사이버 무기체계의 경우 기존 정보보호기술의 많은 부분이 사이버무기체계로 적용될 수 있기 때문에 국방분야 활용 가능성에서 높게 평가되었다. 국방 분야에서는 아직 사이버 무기체계를 위한 핵심기술개발 실적이 많지 않음에도 최조선진국 대비 기술수준과 기술격차에서 높은 평가를 받은 것은 국가보안기술연구소, 한국전자통신연구원 한국인터넷진흥원 등 민간 분야의 유관 연구기관에서 1990년대부터 많은 기반기술을 축적해 왔기 때문인 것으로 보인다.

4.3 사이버무기체계 기술수준과 실제 작전 사례와의 관계

Table 4는 26개 대표무기체계별로 국방과학기술 선진국 16개국 간의 순위조사 결과를 보이고 있다 [5]. 사이버무기체계는 15년 8월 무기체계로 편입되었기 때문에 15년부터 순위조사에 포함되었다. 각 무기체계별 국가순위조사결과 사이버무기체계는 16개국 중 11위로, 26개 무기체계 중 18번째로 조사되었고 화포가 5위로 가장 높게 조사되었다. 각 무기체계별 점수조사결과 사이버무기체계는 82점으로 26개 무기체계 중 10번째로 조사되었고 기동전투체계가 89점으로 가장 높게 조사되었다.

기동전투나 화포체계는 흑표전차나 K-9 자주포와 같이 국외에서도 높은 평가를 받는 무기체계 개발 사례가 있기 때문에 전체 무기체계 중에서 높은 평가를 받았다. 특히 K-9는 연평도 포격사건 등에서 우수한 실전 평가를 받았기 때문에 더욱 높은 평가를 받고 있다. 그러나 사이버전의 경우 앞의 두 조사결과에서 확인한 바와 같이 높은 수준의 기반기술 수준을 확보하고 있음에도 낮은 평가를 받고 있다. 설문에 참여한 전문가들의 의견은 15년 처음 무기체계로 편입됐기 때문에 아직 사이버 무기체계에 대한 운영개념이 확립되지 못했고, 이스라엘이나 이란 등과 같이 사이버전 관련 실전 사례가 많은 타 국가에 비해서 공격을 받은 사례는 많아도 공격 받은 이후 구체적으로 능동적 대응을 하거나 사이버 무기체계 관련 포렌식 기술을 활용하여 공격자를 구체적으로 식별하고 국제법적으로 제소한 실적이 없기 때문에 상대적으로 낮게 평가한다고 하였다. 사이버전은 상대적으로 진입장벽이 낮기 때문에 선진권, 중진권에 국가들이 많이 포진하고 있어 기술수준이 높아도 순위가 낮은 반면, 난이도가 높거나 개발국가가 적은 분야의 경우 선진권, 중진권에 국가들이 적게 포진하고 있어 낮은

점수로도 높은 순위를 받은 경우가 있었다.

가설 3에서 사이버무기체계 기술수준은 실전경험에 비례할 것이라고 가정한 바와 같이 한국의 사이버전 전문가들은 사이버무기체계의 운용 수준과 국가의 기술수준을 양의 상관관계로 판단하고 있음을 알 수 있었다.

V. 향후 연구과제

본 논문에서 분석한 2013년 국조서에서는 사이버 무기체계를 위한 미래 소요기술을 민관군의 협의를 통해서 도출하긴 하였으나, 아직 사이버무기체계가 정식으로 규정에 편입되지 않고, 한국의 사이버전 교리가 확립되지 않은 상태에서 미래의 기술들을 가정하여 도출한 기술들이었다. 그 이후 사이버무기체계가 전력발전훈령에 정식으로 편입되고 합동사이버작전교육회장이 발표됨에 따라 한국의 사이버전 운영개념에 부합하는 새로운 소요기술들을 도출해야 할 필요가 있다. 다음 논문에서는 새롭게 정의된 무기체계 정의와 교리에 부합하는 소요기술 도출 및 기술수준 분석을 다룰 수 있을 것이다.

또한 본 논문에서는 기술들의 모임인 핵심기술군에 대해서 거시 분석하였으나, 사이버 운영개념에 부합하는 소요기술들이 도출된 이후에는 소요기술들별로 미세 분석도 가능할 것이고, 이를 기반으로 핵심기술 추진 방안에 대한 구체적인 제안도 가능할 것이다.

2015년 국가별 국방과학기술수준 조사에서는 한국의 사이버전 전문가들을 대상으로 한국의 전문가들이 인식하는 국가별 수준을 조사하였으나, 국가별 수준조사가 되기 위해서는 수준조사 대상국에 속하는 다른 국가의 전문가들도 참여하는 수준조사가 되어야 할 것이다. 다음 논문에서는 다른 국가의 전문가들도 참여하는 국가별 수준조사결과에 대한 분석도 제시할 수 있을 것이다.

VI. 결 론

본고에서는 사이버무기체계에 대한 세 가지 가설을 수립하고 한국의 군·산·학·연 무기체계(사이버전) 전문가들을 대상으로 3년에 걸친 설문조사를 수행하여 가설의 대한 분석결과를 제시하였다.

분석결과, 수립한 가설처럼 사이버무기체계 소요기술들은 기존 재래식 무기체계 소요기술에 비해서

선진국과의 기술격차가 작았으며, 기존 재래식 무기 체계 관련 민간 유망기술에 비해서 국방분야 활용 가능성이 더 높았고, 사이버무기체계 기술수준은 실제 작전 사례와 양의 관계를 가지고 있음을 확인할 수 있었다.

본 논문은 그 동안 사이버전 분야에 대해서 당연한 사실처럼 언급되던 몇 가지 명제에 대해서 국내의 전문가들을 대상으로 다 각도의 설문조사를 수행함으로써 해당 명제들을 설문 데이터에 기반해서 분석/확인했다는데 의의가 있다.

가설의 검증에서 확인한 것처럼 사이버 무기체계는 신생 분야로써 선진국과의 기술격차가 비교적 적기 때문에 정책적인 집중 육성을 통해서 기존 기동/화력 분야의 K-2나 K-9과 같이 방산시장을 대표하고 국가 경쟁력을 가질 수 있는 무기체계를 개발할 수 있을 것으로 예상된다. 또한 민·군간 협력 가능성 또한 높기 때문에 이스라엘의 사례에서 보는 바와 같이 민간 정보보안업체와의 동반 발전 또한 가능할 것이다. 그러나 사이버전 분야의 발전은 기술적인 투자뿐만 아니라 군 주도의 운용개념 발전과 북한의 사이버 공격에 대응하는 실전 실적이 있어야 종합적인 발전을 이룩할 수 있을 것이다.

추후 본 논문을 더욱 발전시켜 사이버전 분야의 특성에 기반해서 미래 소요기술을 발굴하고, 핵심기술 기획방향을 정립하며, 미래 사이버 무기체계 개념을 정립하는 등의 후속 연구가 가능할 것이다.

References

- [1] Creative Defense Concept, <https://creative.mnd.go.kr/concept>.
- [2] The Directive for National Defense Enforcement, <http://www.law.go.kr/admRulAstSc.do?schType=0&menuId=7&dataCls=lsAstSc&query=국방전력발전업무훈령&cptOfiCd=&tabNo=3#cptOfiAll>.
- [3] Hogyun Lee, vol 2. C4I - Defense Science and Technology Survey 2013, DTaQ research report, pp. 246-262, 2013.
- [4] Hogyun Lee, vol 3. Information Security - Defense IT Technology Survey 2015, DTaQ research report, pp. 13-14, 2015.
- [5] Hogyun Lee, Cyberwarfare part - Defense Science and Technology Level Assessment by Country 2015, DTaQ research report, pp. 108-131, 2015.
- [6] Technolytics, "Cyber Commander's eHandbook version 2.0," Technolytics, 2011.
- [7] Richard A. Clarke, "Cyber War: The Next Threat to National Security and What to Do About It," Ecco, 2010.
- [8] Unit, E. I. "Cyber power index: findings and methodology." Booz Allen Hamilton, 2011
- [9] The Security & Defence Agenda (SDA), "The Cyber Defense Report," McAfee, 2012.
- [10] JungMin Kang, "A Study on National Cyber Capability Assessment Methodology," Journal of the Korea Institute of Information Security & Cryptology, 22(5), pp.1039-1055, Oct. 2012.
- [11] Korea Evaluation Institute of Industrial Technology, "2013 Industrial technology level evaluation report", 2013.
- [12] Tobias Feakin, "Cyber maturity in the Asia-Pacific Region 2014," The Australian Strategic Policy Institute, 2014.

..... <저자 소개>



이 호 균 (Ho-Gyun Lee) 정회원
 1998년 2월: 경북대학교 컴퓨터공학과 학사
 2000년 2월: 경북대학교 컴퓨터공학과 석사
 2011년 3월~현재: 고려대학교 정보보호대학원 박사과정
 2000년 2월~2002년 11월: LG정보통신 생산기술연구소
 2002년 12월~2007년 6월: 한국전자통신연구원 정보보호연구단
 2007년 7월~현재: 국방기술품질원 기술기획부 기술조사팀 선임연구원
 <관심분야> 사이버전, 정보보호, 국방과학기술기획, 기술수준조사



이 경 호 (Kyung-Ho Lee) 중신회원
 1989년 8월: 서강대학교 수학과 학사
 1997년 8월: 서강대학교 정보통신대학원 석사
 2009년 8월: 고려대학교 정보경영대학원 박사
 1994년 2월~현재: 삼성그룹, nhn, 시큐베이스 등 근무
 2011년 9월~현재: 고려대학교 정보보호대학원 부교수
 <관심분야> 위협관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책



임 종 인 (Jong In Lim) 중신회원
 1980년 2월: 고려대학교 수학과 졸업
 1982년 2월: 고려대학교 수학과 석사
 1986년 2월: 고려대학교 수학과 박사
 현재: 고려대학교 정보보호대학원 교수, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원장, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원, 국방기술품질원 임명직 이사
 <관심분야> 사이버 국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안