

국방과학기술과 무기체계



국방대학교
국가안전보장문제연구소

2020 안보연구시리즈 제6권 4호

국방과학기술과 무기체계

인 쇄 2020년 12월 31일

발 행 2020년 12월 31일

발행처 국가안전보장문제연구소

발행인 국가안전보장문제연구소장

주 소 33021 충청남도 논산시 양촌면 황산별로 1040

전 화 TEL : 041-831-6412 FAX : 02-748-7588

홈페이지 <http://www.kndu.ac.kr>

<http://www.kndu.ac.kr/rinsa>

디자인 및 인쇄 선우(주) TEL : 041-632-2363

© 국가안전보장문제연구소 2020

비매품

ISSN 2586-5323

1. 본 연구보고서 내용은 연구진의 개인적인 견해이며 소속 기관의 공식적인 견해가 아닙니다.
 2. 본 연구보고서는 정책입안시 참고자료로만 활용하고 타기관에 불필요한 자료유출을 삼가주시기 바랍니다.

올 한해는 코로나19 바이러스 발생 된 대규모 감염병으로 우리나라는 물론이고 지구촌 모두가 지금까지 경험하지 못했던 새로운 일상을 꾸려가고 있습니다. 미·중 간의 무역분쟁과 전략적 경쟁은 코로나 발생의 책임 공방까지 더해져 더욱 악화되었고, 이런 상황 속에서 대통령 선거에서 승리한 민주당 바이든 당선자는 기존 정책과는 확연하게 다른 변화를 추구할 것으로 보입니다. 아울러 북한 핵문제 해결을 위한 협상과 노력은 재개의 기미가 보이지 않고 한반도 평화 정착은 요원해 보이기까지 합니다. 이러한 예상치 못한 위협의 출현과 변화하는 안보 상황 등에 대해서는 많은 논평과 해설을 담은 글들은 많아지고 있습니다.

하지만, 시사적인 논평과 해설의 역할도 물론 중요하다는 사실에 공감하면서도 사안의 본질을 정확하게 파악하기 위해서는 보다 깊이 있고 체계적인 연구가 필요하지 않는가라는 생각을 하게 됩니다. 이러한 문제의식으로 국방대학교 안보문제연구소에서는 매년 국방부, 합참, 각 군 본부의 의견수렴을 바탕으로, 보다 근본적이고 거시적인 분석이 필요한 주제를 선정하여, 관련분야의 저명한 학자 및 전문가들에게 연구를 의뢰하고 있습니다. 관측된 현상의 원인을 심층적으로 연구하여 근원적인 대답을 제공해주는 이론적 탐구로부터 실제 활용할 수 있는 정책적 대안까지 망라한 연구가 진행되었으며 그 결과를 종합하여 안보 연구시리즈로 발간하게 되었습니다. 올해는 특히 외교·안보와 북한, 국방정책 및 군사전략, 국방경영 및 군수혁신, 국방과학기술과 무기체계, 예비전력 미래혁신, 2020-21 RINSA 세계 안보정세분석과 전망 등 6개 대주제를 중심으로 29개의 세부 연구과제에 집중하였습니다.

아무쪼록 이러한 연구결과가 안보 관련 정책담당자분들과 연구자분께 정책을 개발하고 집행하는 데 있어서 필요한 유용한 아이디어를 제공하고, 참고자료로 활용 될 수 있기를 바랍니다. 끝으로 제한된 연구기간에도 불구하고 좋은 연구를 해주신 참여 연구자 여러분께 깊은 감사의 말씀을 전합니다.

2020년 12월 30일

국방대학교 총장 겸 국가안전보장문제연구소장 육군소장 **김 중 철**

1. 빅데이터 기술의 사업관리 적용방안 : 경영, 제조 및 서비스 분야 중심 1

(우석대학교 황현호 / 우석대학교 이승현 / 우석대학교 이형우)

I. 연구개요	1
II. 빅데이터 분석도구를 활용한 사업관리 동향	8
III. 빅데이터 분석도구 분석	26
IV. 분야별 빅데이터 분석도구 적용 방안	32
V. 정책적 제언	39

2. 인공지능 기술의 국방분야 적용방안 연구 43

(건양대학교 최명진 / 호원대학교 심행근)

I. 서론	52
II. 문헌연구 / 시사점	55
III. 국내·외 인공지능 시스템을 활용한 모범사례 분석	68
IV. 인공지능 기술분야별 활용방안 식별 및 과제도출	102
V. 정책적 시사점 및 발전방향	133
VI. 결론	154

3. 현대전에서의 사이버전 워게임 연구 161

(국방대학교 강동수 / 아주대학교 이민우)

I. 연구 개요	162
II. 현대전에서의 사이버전과 워게임	164
III. 사이버 워게임 사례분석 및 시사점	176
IV. 한국군을 위한 사이버 워게임 활용 방안	187
V. 결론	201

4. 하드웨어 보안기술의 적용을 통한 국방사이버보안 연구 205

(국방대학교 이수진)

Ⅰ. 연구개요	207
Ⅱ. 하드웨어 기반 사이버보안 기술	209
Ⅲ. PUF 기술	221
Ⅳ. PUF 기반의 국방 사이버보안 강화 방안	232
Ⅴ. 결론	250

5. 최신 북한의 미사일 기술진전과 위협 257

(육군협회 김항록 / 육군협회 신동호)

Ⅰ. 서론	259
Ⅱ. 최신 북한의 미사일 고도화와 위협 분석	261
Ⅲ. 북한 미사일 위협 종합 및 전망	289
Ⅳ. 북한 미사일 대응전략	292
Ⅴ. 결론	311

빅데이터 기술의 사업관리 적용방안

: 경영, 제조 및 서비스 분야 중심

우석대학교 교수 **황 현 호**

우석대학교 교수 **이 승 현**

우석대학교 교수 **이 형 우**

- I. 연구개요
- II. 빅데이터 분석도구를 활용한 사업관리 동향
- III. 빅데이터 분석도구 분석
- IV. 분야별 빅데이터 분석도구 적용 방안
- V. 정책적 제언

I. 연구개요

1. 개요

1) 빅데이터¹⁾

‘빅데이터’의 순수 단어에서 오는 뜻은 큰 데이터로 보여질 수 있지만, 미국의 기업인 가트너(Gartner)는 2001년에 빅데이터의 특징을 데이터의 양(Data Volume), 데이터의 속도(Data Velocity), 데이터의 다양성(Data Variety)으로 정의했다. 데이터의 양은 일반적으로 쓰이던 데이터베이스 시스템의 관리·처리·수집의 한계를 넘는 방대한 크기의 데이터를 말한다. 데이터 속도는 데이터가 수집 되는 속도와 처리하는 속도를 말한다. 데이터 다양성이란 정형화된 데이터(Formal Data)와 소셜 미디어(Social Media) 등에서 만들어지는 비정형 데이터(Informal Data)까지에 이르는 다양한 데이터를 말한다.

1) 박영길, '국방분야 빅데이터 활용의 선결 과제와 유의점 검토', 국방연구원, 2018

3V(Variety, Volume, Velocity)는 가장 흔히 통용되는 빅데이터의 정의이며, 사용에 따라 가변성(Variability), 가치(Value), 정확성(Veracity)을 추가하여 정의하기도 한다. 이와 같이 빅데이터는 수 많은 데이터를 처리하는 과정이고, 기술 및 결과를 포함하는 말로 사용되고 있다.

2) 사업관리

사업관리는 사업과 관련된 이해 관계자의 요구 사항을 충족시키기 위해 사업과 모든 과정을 체계적으로 관리하여 사업 성공을 보장하는 활동이다. 사업 성공 및 완수를 위해서는 사업의 통합관리, 범위관리, 시간관리, 원가관리, 품질관리, 리스크관리, 인적자원관리, 의사소통 관리, 조달관리 등의 요소를 적절히 관리 할 필요가 있다. 이때 각 요소별로 하나 이상의 입력을 통해서 가치 있고 의미 있는 결과값을 얻어야 하며, 이러한 입력과 결과값을 얻는 과정은 참여인력들의 직무(task)로 나눌 수 있다. 결과적으로 직무는 기업의 서비스 또는 제품을 사용자에게 공급하여 가치 창출하는 사업관리의 전반적인 프로세스(통합, 최적화, 자동화 등)이다. 사업관리 프로세스의 요소로는 첫 번째, 활동이다. 활동은 정보와 자원을 또 다른 형태로 변환한다. 둘째는 의사결정이다. 의사결정은 사업관리에서 사업 성공을 이끌기 위한 선택 단계이다. 세 번째는 역할이다. 역할은 의사결정에 따른 직무를 구분하여 업무처리 하는 것을 뜻한다. 네 번째는 자원이다. 자원은 역할에 따른 이해관계자 또는 시설, 프로그램이다. 다섯 번째는 저장소가 있다. 저장소는 사업관리 프로세스를 기록한다.



〈그림 1〉 사업관리 프로세스

이와 같은 단계별 과정에서 사업관리 프로세스의 각 구성 요소를 관리하기 위해서는 비즈니스 프로세스 관리(BPM : Business Process Management)가 필요하다. 비즈니스 프로세스 관리는 기업의 프로세스를 통합하여 최적화하는 자동화 기술을 뜻한다. 비즈니스 프로세스 관리의 목표는 프로세스 활동 순서와 각 프로세스 활동 간의 정보 저장과 관리 하기 위함이다. 특히, 의사결정단계(탐색 ⇨ 설계 ⇨ 선택 ⇨ 수행)는 4단계로 구분되는데,

비즈니스 프로세스 관리는 최적의 의사결정의 대안과 평가에 도움을 준다. 의사결정의 설계단계에서 비즈니스 프로젝트 관리의 역할은 의사결정 유형에 따라 다르다. 즉, 재고 관리나 채용심사와 같이 구조화될 수 있는 경우는 컴퓨터로 프로그램화되어 자동화 처리될 수 있지만, 영업 효과 및 투자대비 효과 분석, 직원 교육효과 분석 등은 비정형화된 구조이다. 이런 경우 비즈니스 프로세스 관리로 분석하여 의사결정의 필요 요소를 추출하여 의사결정자에게 정보를 제공한다면 보다 효과적이며, 최적화된 선택을 이끌 수 있다. 이와 같은 정보를 제공하는 대상의 이해관계를 살펴보면, 최고경영층이 대상이 될 수 있다. 최고경영층은 사업 방향의 설정과 사업전략 및 제품 경쟁력 고도화 등의 장기적인 계획 수립을 통하여 전반적인 조직목표 등을 세우는 전략기획 업무수행을 실행한다. 두 번째 정보 제공대상자를 살펴보면 중간관리자층이 대상이 된다. 중간관리층은 경영자원의 조직화, 획득, 업무의 구조화, 직원교육, 직원채용 등 중기 계획을 수립하여 하위 부서에게 최고경영자의 목적을 구체화 및 전달 하는 업무를 실행한다. 마지막 대상으로는 하위관리층이 있다. 하위관리층은 정해진 목적, 절차, 정책에 따라 단기적인 계획을 수립 및 실행하여 경영자원을 직접 활용하며 운영을 담당한다.

3) 빅데이터를 통한 사업관리와 생태계²⁾

세계적으로 빅데이터 분석 시장은 연평균 25% 성장하고 있으며, 2023년에는 약 160억 달러에 이를 것으로 전망되고 있고, 국내 또한 빅데이터 분석 시장이 연평균 13% 성장한 것으로 나타났다. 폭발적으로 증가하는 정형 및 비정형화된 데이터의 양은 사업관리의 효율성을 향상시키기 위한 수요 또한 증가시키고 있다. 이러한 시장 환경을 바탕으로 빅데이터 분석 도구 솔루션은 매출 증대, 신시장 투자성, 사업의 투명성 증대, 소비자 니즈, 시장 트렌드 예측, 업무 성과향상, 고객 및 시장 세분화, 의사결정 지원, 제품 및 서비스의 혁신 등을 위하여 사용된다. 빅데이터 분석 도구를 활용한 사업관리 생태계를 살펴보면, 기존 데이터베이스 관리 도구로 데이터 저장, 관리, 수집, 분석의 범위를 넘어서는 대용량의 정형 또는 비정형 데이터에서 의미 있는 정보를 추출하고 의사결정 및 실행, 효과를 도출하기 위한 정보화 기술로 사용된다. 빅데이터 분석은 국방, 교통, 사회, 재난, 의료 등 다양한 분야에서 생성되는 데이터를 기반하여, 데이터의 규모, 생성 속도, 다양성 관점에서 과거의 데이터 분석에 비해 고도화 되었다. 또한 데이터 저장 관리 기술과 데이터 분석 기술로 구분되며, 다양한 기술들이 복합적으로 사용된다. 빅데이터 분석기술의 고도화로 비정형 데이터의 활용도가 증가하였으며, 비정형 데이터의 분석 능력은 기업의 경쟁력으로

2) 최지영, '빅데이터 분석 솔루션', 한국IR협의회, 2019.11.17. 참조

이어졌다. 빅데이터 분석 솔루션은 대량의 정형 또는 비정형 데이터로부터 숨어 있는 정보와 정보 간에 관계를 찾아낼 수 있었고, 사업관리에서 의사결정을 지원하게 되었다. 이를 위한 빅데이터 분석 도구는 소프트웨어 또는 하드웨어가 해당되며, 분석도구를 통해 소비자 니즈 발견과 트렌드 예측, 성과관리, 타겟 고객 세분화, 의사결정 지원, 비즈니스 모델 및 서비스의 혁신 등으로 사용하기에 이르렀다.

빅데이터 산업의 특징은 첫 번째로 규모의 경제다. 시중에 나와 있는 일반 상품의 경우, 매출 증가는 곧 생산량 증가에 따른 생산비용 증가로 이어질 수 있지만, 소프트웨어의 경우는 판매가 증가할수록 소프트웨어의 평균 개발비용이 감소함으로써 규모의 경제 특성을 갖게 되어 사용자의 수가 생산비용 측면에서 중요한 역할을 하게 된다. 두 번째는, 기술 및 지식 집약적 산업이다. 빅데이터는 소프트웨어, 하드웨어, 서비스 모두가 융합되어야만 성과를 낼 수 있을 정도로 고난도의 역량을 요구하는 기술과 지식이 집약적이다. 세 번째는 경기 동행 산업이다. 패키지 소프트웨어 산업은 경기에 후행하는 특성을 보여 왔지만, 최근에는 동행하는 추세를 보인다. 소프트웨어에 대한 투자가 비용이라는 인식에서 기업의 경쟁력 강화 방안으로 전환이 되는 추세다. 네 번째는 제품 라이프 사이클이 짧은 산업이다. 급속한 기술발전은 제품 라이프 사이클을 짧게 만들었으며, 신시장의 지속 창출 및 업그 레이드가 필요한 산업이다. 다섯 번째는 낮은 진입장벽 산업이다. 비교적 대규모의 초기 투자 비용이 발생되지 않고 소자본으로 시장 진입이 가능한 산업이며, 현재도 신규 진출 기업이 지속적으로 증가하여 같은 산업 내 경쟁이 치열해 지고 있다.

4) 빅데이터 솔루션 및 서비스 국내외 시장규모³⁾

국내는 과학기술정보통신부의 ‘데이터 산업 현황 조사’(2019.03)에 따르면, 빅데이터 분석 시장은 데이터솔루션 중분류별 시장에 속한다. 또한 데이터솔루션 전체 시장은 2014년 1조 3,619억 원, 2015년 1조 4,124억 원에서 2018년 1조 7,561억 원으로 연평균 7.5% 성장한 것으로 나타났다. 데이터솔루션 시장에서 높은 비중을 차지하는 시장은 데이터 베이스 관리 시스템 시장으로 2018년 기준 전체 데이터솔루션 시장에서 약 36%를 차지하고 있으며, 데이터 분석 시장은 약 10%의 비중을 보이고 있다.

3) 최지영, ‘빅데이터 분석 솔루션’, 한국IR협의회, 2019.11.17. 참조

〈표 1〉 데이터 솔루션 중분류별 시장규모

(단위 : 억원)

구분	2014년	2015년	2016년	2017년	2018년	증감률 (17~18)	CAGR (15~18)
데이터 관리	4,531	4,699	5,367	4,628	4,887	5.6%	9.5%
데이터 보안				1,213	1,279	5.5%	
데이터 플랫폼	1,389	1,426	1,611	1,766	1,907	7.4%	10.2%
데이터수집	1,076	1,115	1,345	1,393	1,499	7.6%	10.4%
DBMS	5,502	5,727	6,148	6,121	6,403	4.6%	3.8%
데이터분석	1,121	1,157	1,249	1,329	1,584	19.5%	11.0%
전체	13,619	14,124		16,457	17,561	6.7%	7.5%

* 출처 : 2018년 데이터산업 현황 조사, 과학기술정보통신부(2019.03)

국내 빅데이터 분석 시장은 2015년 1,157억 원에서 2018년 1,584억 원으로 연평균 11% 성장했으며, 2018년 빅데이터 분석 시장은 전년 대비 약 19.5% 성장한 약 1,584억 원의 시장을 차지하는 성장세를 보였다. 최근 빅데이터 분석도구 성능의 고도화로 필요 산업 군으로 부터 적극적으로 대응하는 양상을 보이고 있으며, 범용 솔루션에서 산업 및 업종별 특화 솔루션으로 변화하는 과정에서 괄목할 성장세를 보이고 있다고 평가받고 있다. 주요 수요로는 범정부 차원의 대민 서비스 고도화와 대량의 데이터 분석을 요구하는 금융 솔루션, 머신러닝, 자연어처리, 언어학적 규칙을 사용한 비정형 데이터 분석, 시각화 서비스 이용자가 대상이 되고 있다.

국외는 시장조사기업인 ‘마켓츠 앤 마켓츠’(2018.09)에 따르면, 전 세계 빅데이터 및 데이터 엔지니어링 서비스 시장은 2018년 약 344억 7,000만 달러에서 연평균 17.6% 성장했으며, 2023년 약 773억 7,000만 달러에 이를 것으로 전망되었다.

〈표 2〉 전 세계 빅데이터 및 데이터 엔지니어링 서비스 시장규모

(단위 : 억 달러)

구분	2016년	2017년	2018년	2023년	CAGR (15~18)
데이터 품질	55.3	64.3	76.2	180.1	18.8%
데이터 모델링	67.2	74.8	84.4	162.8	14.0%
데이터 통합	100.6	113.2	130.0	275.3	16.2%
분석	34.4	42.7	54.0	155.5	23.6%
계	257.4	295.0	344.7	773.7	17.6%

* 출처 : Big Data and Data Engineering Services Market - Global Forecast to 2023, 마켓츠 앤 마켓츠(2018.09)

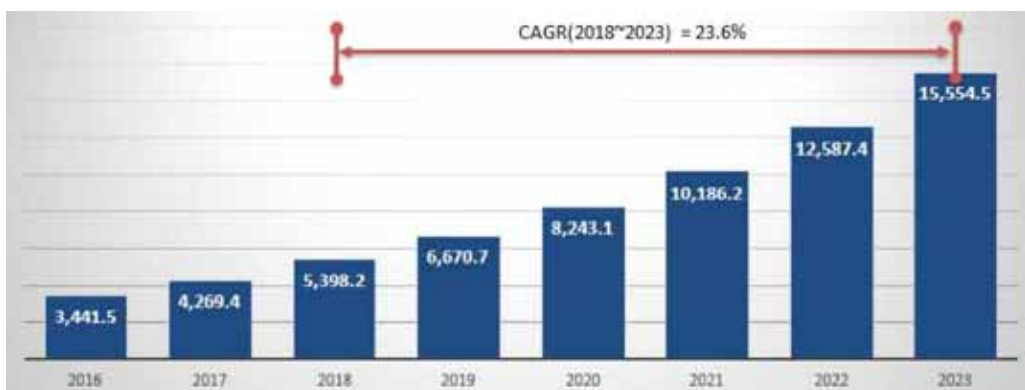
〈표 3〉 전 세계 빅데이터 분석 시장 규모(지역별)

(단위 : 백만달러)

구분	2016년	2017년	2018년	2023년	CAGR (15~18)
아시아 태평양	617.8	799.3	1,054.1	3,429.2	26.6%
북미	1,544.4	1,901.4	2,382.4	6,648.6	22.8%
유럽	836.6	1,018.0	1,262.9	3,437.8	22.2%
중동, 아프리카	216.2	262.7	325.3	881.1	22.1%
라틴아메리카	226.5	288.1	373.5	1,157.8	25.4%
계	3,441.5	4,269.4	5,395.2	15,554.5	23.6%

* 출처 : Big Data and Data Engineering Services Market - Global Forecast to 2023,마켓츠 앤마켓츠(2018.09)

빅데이터, 데이터 엔지니어링 서비스 시장은 데이터 통합, 데이터 모델링, 데이터 품질, 데이터 분석 등으로 구분되는데, 동 시장에서 높은 비중을 차지하는 시장은 데이터 통합 시장으로 전체 빅데이터, 데이터 엔지니어링 서비스 시장에서 37.7%를 차지하고 있다(분석 시장은 15.7%의 비중을 보임). 동 보고서에 따르면, 전 세계 빅데이터 분석 시장에서 2018년 약 53억 달러의 연평균 23.6% 성장했으며, 2023년에는 약 155억 달러에 이를 것으로 전망되었다. 지역별로 구분시 빅데이터 분석 시장에서 가장 높은 비중을 차지한 시장은 북미 시장이며, 2018년 기준 전체 빅데이터 분석 시장의 44.1%를 차지하고 있다(아시아 태평양 시장은 19.5%의 비중을 보임).



〈그림 2〉 빅데이터 분석 세계 시장 규모

* 출처 : Big Data and Data Engineering Services Market - Global Forecast to 2023,마켓츠 앤마켓츠(2018.09)

다양한 비즈니스를 통해 발생 되는 데이터, 비즈니스의 효율성 향상에 대한 필요성 증가, 데이터 통합 플랫폼 저장관리 요구 등이 빅데이터 분석 솔루션 시장 성장을 이끌고 있다.

2. 연구 필요성

1) 빅데이터 분석도구를 통한 사업관리의 한계점

빅데이터 분석도구를 통한 사업관리의 융합은 한계가 있다. 빅데이터는 데이터베이스에 대한 기술, 지식뿐 아니라 해당 산업군 및 업무 분야에 대한 지식을 필요로 하는 융합산업이라고 할 수 있다. 예를 들어, 보건 산업군에 빅데이터를 도입한다고 하면, 보건 산업에 대해서 필요 지식이 없이 빅데이터 지식만 갖고는 적절한 시스템을 디자인하기 어렵다. 또한, 기업이 채용 분야에 대하여 빅데이터 기술을 도입한다고 했을 때, 채용 분야에서 채용기준과 기업의 인재상, 경험 기반에 요구사항 등을 정확히 파악하지 못하고 기술적인 부분만으로 시스템을 구축시 개발이 어려울 것이며, 개발자는 기업 및 사용자의 요구를 충족시킬 수 없다.

이러한 부분에 한계를 극복하기 위해서는 융합 지식의 전제가 필요하다. 웨어러블 기기에 의료기기의 기능을 삽입한 제품을 통해 고객 니즈를 충족시키고 시장 성공하려면 기기 자체에 대한 지식과 데이터베이스에 대한 지식만으로는 부족하다. 반드시 의료지식이 필요로 한다.

2) 사업관리 분야의 빅데이터 활용 쟁점

대기업 위주의 빅데이터 활용 및 도입에 따라 중소기업과의 정보격차 확대가 문제점으로 발생 된다. 현재 우리나라에서 빅데이터를 도입하고 있는 대표 제조 기업 중에서도 삼성, 현대, 포스코 등 최정상 기업을 중심으로 빅데이터 활용과 수익성, 효율성을 높이고 있다. 특히, 해당 기업은 다년간 축적된 정보를 보유하고 있으며, 충분한 재화나 시설 및 빅데이터 활용 기술 능력을 보유하고 있다. 하지만 중소기업의 빅데이터 도입은 다음과 같은 이유로 쉽게 이루어지지 않고 있다. 대기업의 시장 전략 및 행보가 중소 기업에게 큰 영향을 미친다고 보았을 때, 중소기업은 규모의 경제에서 약자로서 자체적 빅데이터 사용 및 도입하기에는 투입 비용이 과다할 수 있다.

II. 빅데이터 분석도구를 활용한 사업관리 동향

1. 국내 활용 동향 분석

1) 경영 분야⁴⁾

유유제약의 빅데이터 분석도구를 활용한 사례는 영업, 마케팅 분야에서 사용되었다. 유유제약은 소비자의 인식조사를 위해 자사 데이터와 자사 외 외부 데이터를 활용했다. 유유제약은 다음소프트가 제공한 소셜 분석 기술인 소셜 매트릭스를 통해 소셜 데이터를 분석하여 유유제약의 마케팅 및 소셜 데이터를 적용한 응용 제품으로 확대했다. 유유제약의 ‘베노플러스’라는 제품은 증상 완화에 작용하는 기존 파스나 연고와 다르게 피부 속에 흡수되어 질환 원인을 제거하고 멍든 피부를 되돌리는 데 효과가 탁월하다. 또한 멍 외에 단순 타박상이나 벌레 물린 데에도 좋은 효과를 보인다. 생약 성분의 복합처방으로 무자극, 흡수력도 빠르며, 피부가 민감한 고객 이들을 위해 피부침윤, 발진, 피부건조 등의 부작용도 최소화했다. 이러한 제품을 유유제약 측에서 마케팅하기 위해 빅데이터 분석 도구를 활용하여 잠재적 고객 정보평가를 진행했다. 그 결과, 기존 마케팅 대상인 어린이에서 여성들로, 마케팅 시기인 여름에서 겨울로, 기존의 치료 용도에서 미용 용도로 사용한다면 매출 증대 효과를 이끌 수 있다는 빅데이터 분석 결과를 도출했다. 결과적으로 유유제약은 매출의 50% 이상 증가 하였으며, 성공적인 성과 거두었다.

두 번째 사례로는 대한생명의 빅데이터 분석 도구를 활용한 무결성 의사결정이다. 보험 계약은 온라인 자동화를 통해 효율성을 확대 시켰지만 반대로 부정행위 또한 증가한다는 관점에서 사업의 무결성이 필요했다. 따라서 부정 및 사기 방지를 위해 빅데이터 분석도구를 활용한 의심 거래 후보군을 이전보다 더 정밀하게 파악했다. 대한생명은 국내 벤처기업인 지식시스템(KSTEC)과 아이로그 제이룰즈(ILOG JRules)를 개발하였고, 대한생명의 보험사기 방지시스템을 만들었다. 예측분석을 통해, 사기 의심 거래 후보를 더 효과적이며 정밀하게 실시간으로 파악할 수 있게 되었다. 이 시스템은 보험금 청구 고객에 대하여 스코어링(Scoring) 수단을 통해 보험금 지급을 판단할 수 있도록 만들었다. 보험사기 청구에 대하여 데이터 분석 스코어링이 일백 여개 팩터(Factor)로 분류하여 사기 방지 프로세스가 구축되었고, 사기 징후에 대한 감지 기준을 표준화시켰다. 이를 통해 보험사기로 적발된 사례들을 수집하고 패턴화하여 보험사기 혐의자를 자동으로 추출하는 시스템이다. 사기유형,

4) 송민정, ‘빅데이터를 활용한 비즈니스모델 혁신’, KT경제경영연구소, 2013

계약, 개인, 보험 모집인, 병원, 정비업소별로 구분하여 다양한 지표들이 개발되었고, 혐의자 추출을 통해 피해자, 가해자, 동승자가 자동 도출되며, 사고 관련성과 공모 여부를 판단하는 분석시스템이기 때문에 체계적이면서도 실시간으로 분석이 가능하게 되었다. 보험사기 방지시스템을 가동한 결과, 보험사기 적발률을 향상 시켰으며 보험사기 예방효과가 나타났다. 결과적으로 선량한 보험 가입자들의 보험 혜택에 기여하게 되었다. 지식시스템(KSTEC)의 보험사기 방지시스템인 ‘스마트웍스 보험사기 감지 시스템’은 보험사고 허위 사실 또는 확대 청구 등 다양한 사기 행위를 객관적, 현실적으로 적발 할 수 있는 지능형의 예측모델 시스템이다. 이후, 대한생명은 자사의 데이터만 활용한다는 한계를 극복하기 위해 보험사기 방지시스템을 업그레이드 시켰다. 타 보험사와 차별점은 자사 데이터뿐만 아니라 보험협회, 보험개발원, 보험관련 공공데이터 등의 데이터를 함께 활용했다는 점이다. 이와 함께 손해보험, 생명보험의 전체 계약을 기축하여, 대한생명은 세부적인 계약 항목까지 진단 및 평가할 수 있게 되었다. 결과적으로 연간 약 50억 원의 사기방지 효과가 발생 시켰다.

세 번째 사례는 빅데이터 분석 도구를 기반으로 서비스능률을 향상시킨 아모레퍼시픽이다. 아모레퍼시픽은 고객을 만족시키기 위한 핵심 전략 및 목표로 보다 나은 제품, 지속적인 구매력, 합리적인 가격을 제시했다. 이를 완성시키기 위해서 빅데이터 분석도구를 활용한 고객 대응방안 메뉴얼을 도출했다. 기업의 고객 대응에 최전선에는 마케팅이 있으며, 마케팅은 웹사이트의 상품 추천을 광고하여 우연히 최종 소비자에게 명시적 판매 포인트로 활용되기도 한다. 다시 말하자면 마케팅 대상 선정의 정확성이 판매 포인트의 핵심으로 작용된다. 부수적으로 고객 만족을 일어나게 하여 시너지를 발생시킬 수 있다. 이와 마찬가지로 서비스 능률 향상, 품질관리 등 개선 효과도 소비자의 요구 수준을 충족시켜 고객 만족을 일으킬 수 있다. 즉, 이와 같은 판매 포인트를 빅데이터 분석도구를 통해 정확도를 향상시켰다. 또한, 기업이 성장하면 비즈니스 측면에서 새로운 규모의 경제가 발생시키게 되는데 기업의 효율 향상을 통해 가격 인하하는 것은 대표적 예일 것이다. 처음에는 생산 비용적 측면에서 절감을 목표로 시작하여 예측분석의 결과가 소비자에게 더욱 매력적인 가격으로 제안 및 작용하는 것이다. 그런데 처음부터 고객 경험이 시장 경쟁의 초점이 될 것으로 예측하여 고객 만족 전략에 중점으로 두었다. 아모레퍼시픽은 구매자의 최초 구매 이력 정보부터 콜센터의 불만 접수까지의 데이터 뿐만아니라 과거 약 10년 동안 수집해 왔는데, 여기에 SNS(Social Network Services/Sites) 데이터를 통합했고, 특히 최근 1년 내 거래 고객을 ‘활성고객’으로 정의하여 이들의 구매정보에 집중했다. 이렇게 쌓은 데이터는 B2C(business to consumer) 데이터 경우 15.2테라바이트, B2B(Business to Business) 데이터는 13.2테라바이트로 늘어났다. 여기에는 매장의 판매시점 정보관리

시스템(POS)의 환불 및 교환 내역, 판매 기록, 콜센터로 접수된 고객 불만 사항, 페이스북의 의견 및 ‘좋아요’ 클릭 횟수, 캠페인 결과, 트위터의 멘션 등과 아모레퍼시픽 ERP(Enterprise Resource Planning), 비즈니스 데이터웨어하우스, 협력사 관계관리 등의 데이터가 모두 포함된다. 아모레퍼시픽은 B2C 데이터로 고객의 관심을 분류하고 빅데이터 분석에 활용했다. 이를 통해 분석한 결과를 고객진화 단계 모델로 구체화 했으며, 각 단계에 맞는 마케팅을 실행으로 옮겼다. 아모레퍼시픽은 IBM 컨설팅을 통해 고객을 상세하게 분류하였고, 조합하여 고객 행동 패턴을 정의했으며, 컨설팅 산출물을 토대로 시스템을 설계 및 구축했다. 결과적으로 빅데이터 분석도구를 활용하여 상품 중심에서 고객 중심으로 전환했고, 고객이 어떤 생각을 하는지 대하여 구매 이전에 고려 단계와 관심 단계별로 구분하여 각각 생각과 행동이 다르다는 것을 파악했다. 또한 신규 고객으로 구매할 때부터 고객으로서 이탈할 때까지 신규, 유보, 시도, 정착, 휴면, 이탈의 과정을 구분하여 고객의 행동이 변화 및 예측할 수 있었다. 이 과정에서 단골로 유지되는 고객이 있는가 하면, 구매력이 감소하거나 증가하는 경우도 있다. 아모레퍼시픽은 정착 단계를 유지 ⇨ 증가 ⇨ 쇠퇴 3가지로 다시 재분류하여 전체 고객 진화단계를 8가지로 구분했다. 아모레퍼시픽은 고객이 구매 단계에서 어떤 행동 및 생각을 하는지 패턴화하여 분석한 결과 약 50개 행동 지표를 이끌어냈고, 1,500개의 변수로 만들어 분석했다. 그 결과, 몇 가지 의미 있는 패턴을 발견했다. 가령, 마일리지의 약 90%를 소진한 고객은 휴면 또는 이탈로 이어질 확률이 일반 고객 대비 3.5배 높아서 이들의 휴면 또는 이탈을 방지하기 위해 기업의 노력이 필요하다 분석하여 해당 고객층의 성향에 맞는 맞춤 서비스를 제안하게 되었다. 아모레퍼시픽의 고객은 십대부터 장년층까지 다양한데 같은 연령층의 사람이라 하더라도 기호 제품이 변화한다. 특히 여성의 경우 사춘기, 연애, 대학, 취직, 출산 등을 거치며 피부톤이 바뀌기 때문에 20대는 ‘라네즈’ 제품을, 30대에서는 ‘헤라’ 제품을, 40대에 들어서는 ‘설화수’ 제품으로 바뀌는 경우의 수를 확인했다. 한편, 고객 한 사람이라 할지라도 정보가 방대하여 아모레퍼시픽은 대용량의 데이터를 처리 가능한 시스템이 필요로 했다. 이 기업의 데이터 처리를 위해서 선택한 IBM의 네티자(Netezza)는 심층분석에 소요되는 시간을 과거 소요 시간 대비 획기적으로 줄 일 수 있게 만들어 주었다.

2) 제조 분야⁵⁾

포스코는 철광석 가격 예측과 생산 공정 개선을 위해 빅데이터 분석도구를 활용했다. 포스코는 런던금속거래소(LME; London Metal Exchange) 상황, 호주 광산 상황, 남미

5) 정해식, ‘빅데이터를 활용한 기업의 경쟁우위 확보 사례’, 정보통신산업진흥원, 2013.

상황을 수집하여 광물의 가격 데이터를 실시간으로 분석하여 철광석 가격 예측했으며, 가격 변동성이 큰 철광석 등 자원을 적시에 국내 조달하기 위해 전 세계 철광산과 현물 거래소의 가격 데이터를 조합 및 분석하여 최적의 구매시기와 가격대를 결정했다. 한편 철강 생산 공정별 과정에서 각종 데이터를 수집 분석하기 위해 0.001초 단위로 정보 수집, 분석해 불량률을 최소화하여 생산 과정에서 공정별로 온도, 습도, 압력에 대하여 어떤 성분을 넣었을 때 성공하고 실패했는지에 대한 데이터 분석을 통해 최상의 철을 생산했다.

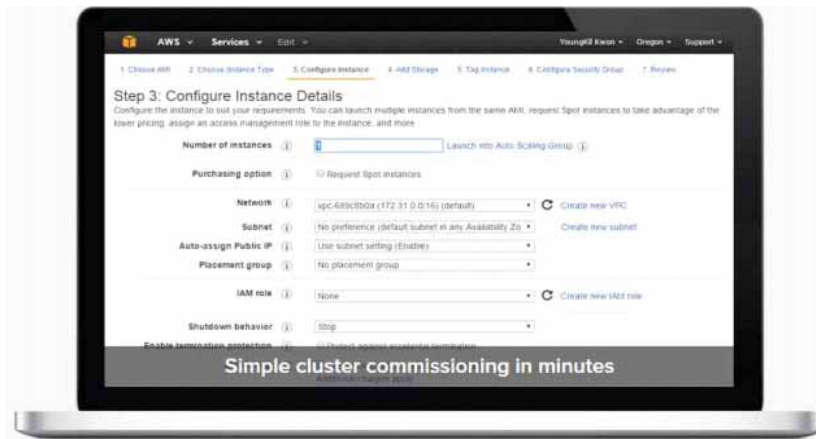
삼성전자는 전사 차원에서 빅데이터 분석 도구를 도입하여 프로젝트를 추진했다. 삼성전자는 SAP, 오라클, EMC, IBM 등 글로벌 기업을 대상으로 빅데이터 PoC(기술도입 타당성검토)를 진행했다. 이를 통해 삼성전자 정보전략실과 삼성SDS가 주축이 되어 빅데이터 사업을 주도하고 있으며, SDS 웹 보안 사용자 로그 분석, 생산설비 센싱 로그 분석, 소셜데이터 분석, 콜센터 데이터 분석, 전사적 자원관리 분석 등 다양한 분야에 빅데이터 분석 도구를 활용했다. 또한, 삼성전자의 빅데이터 분석도구 도입은 경영 혁신과 새로운 비즈니스를 발굴뿐만 아니라 규모 및 파급력 측면에서 빅데이터 생태계 구성에 긍정적 영향을 미치고 있다.

현대자동차의 품질 관리를 위해 빅데이터 분석도구를 도입했다. 현대자동차는 KT넥스알, IBM, EMC, 오라클, 테라데이터 등의 기업을 대상으로 빅데이터 도입 분야 및 PoC에 대하여 현대자동차는 정보전략팀을 중심으로 빅데이터 태스크포스팀을 가동 시켰다. 생산로그 분석, VCRM(자동차 관련 데이터) 등에 빅데이터 분석을 통해 품질관리 시스템 개선과 비용 절감 등 혁신성 및 신 비즈니스 발굴에 빅데이터를 활용했다.

3) 빅데이터 서비스 분야⁶⁾

그루터는 빅데이터 솔루션 및 플랫폼 전문업체로, 주요 제품으로 Qrytica, Tajo Enterprise Gear, TaaS (Tajo-as-a-Service), Cloumon 등이 있다. Qrytica는 표준 SQL로 빅데이터 분석 및 실행하는 빅데이터 분석 도구이고, TaaS는 하둡 에코 시스템 기반한 오픈소스 빅데이터 웨어하우스 솔루션이며, Tajo Enterprise Gear는 빅데이터 처리를 위해 설계된 엔드-투-엔드 빅데이터 웨어하우스 플랫폼이다. Cloumon은 Hadoop 통합 관리 도구이다.

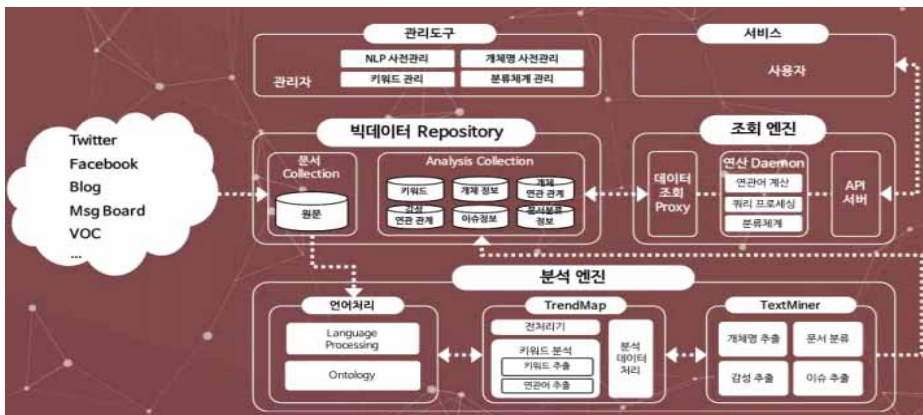
6) 최지영, '빅데이터 분석 솔루션', 한국IR협의회, 2019.11.17. 참조



〈그림 3〉 Gruter Enterprise Tajo on AWS

* 출처 : <http://gruter.com/products/taas/>

(주)다음소프트는 인공지능을 기반한 빅데이터 전문기업으로 인공지능 자연어 처리와 및 대화기술 처리를 보유하고 있다. 제품에는 소셜 빅데이터 분석 서비스 Social Big Data Mining, 빅데이터 마이닝 솔루션인 Contextual Finder™ 등이 있다. Social Big Data Mining는 소셜 미디어로부터 소비자들의 대화 데이터를 수집하고 분류하여 언어에 대한 이해를 텍스트로 분석하고 의미 있는 정보를 추출하는 분석 서비스이다. Contextual Finder™는 텍스트 마이닝기술과 자연어 처리기술을 이용하여 기업 내·외부에 존재하는 대량의 문서로부터 필요정보 추출하고 이슈를 모니터링하는 하둡 기반의 빅데이터 마이닝 솔루션이다.



〈그림 4〉 다음소프트의 Contextual Finder™ TECHNICAL ARCHITECTURE

* 출처 : <http://www.daumsoft.com/contextualFinder.html>

(주)레브웨어는 1999년에 한국후테로시스템으로 설립되어, 2017년 현 사명으로 변경했다. (주)레브웨어는 빅데이터 솔루션 전문기업으로 스마트 제조원가 구축서비스 및 솔루션 제공, 빅데이터 기반 실시간 예측분석 서비스 및 솔루션 제공 등을 주요 사업으로 하고 있다. 주요 제품인 LevSPA는 빅데이터 기반의 실시간 예측분석 OLAP 솔루션을 통해 과거 데이터로부터 머신러닝 모델을 개발하고, 개발된 모델을 PMML(Predictive Model Markup Language) 형태로 저장 및 활용 가능하여 실시간 스트리밍 데이터를 분석하고 예측 가능한 특징이 있다.



〈그림 5〉 레브웨어(Levware)의 LevSPA 프로세스

* 출처 : <http://www.levware.co.kr/toPageProducts?path=levSPA>

(주)비아이매트릭스는 2005년 설립되어, BI(Business Intelligence) 및 빅데이터 분석 솔루션 전문업체로 Big Data 핵심기술을 보유하고 있다. 주요 제품으로는 i-CANVAS로 우수한 분석 보고서 제작에 최적화된 BI 솔루션으로 웹에서 DB(Data Base)에 연결하여 보고서 생성, 편집, 수정, 공유, 배포 가능한 강력한 개발도구를 제공한다. 또 다른 주요 제품인 i-STREAM는 데이터를 추출하여 분석 및 결과를 시각화하는데 데이터 분석의 전 과정을 지원하는 통합데이터 분석 솔루션으로 분석을 위한 ETL(Extract, Transform, Load), 이기종 데이터 소스의 통합 분석, 통계, 예측분석, 데이터마이닝 등 다양한 기능을 수행하여 복잡한 데이터 처리 요구 사항에 신속히 대응하여 데이터 분석가가 쉽게 활용할 수 있도록 사용자 중심의 UI(User Interface)를 제공한다.



〈그림 6〉 비아이매트릭스의 통합 데이터 분석 솔루션 i-STREAM

* 출처 : <http://www.bimatrix.co.kr/products/i-stream/>

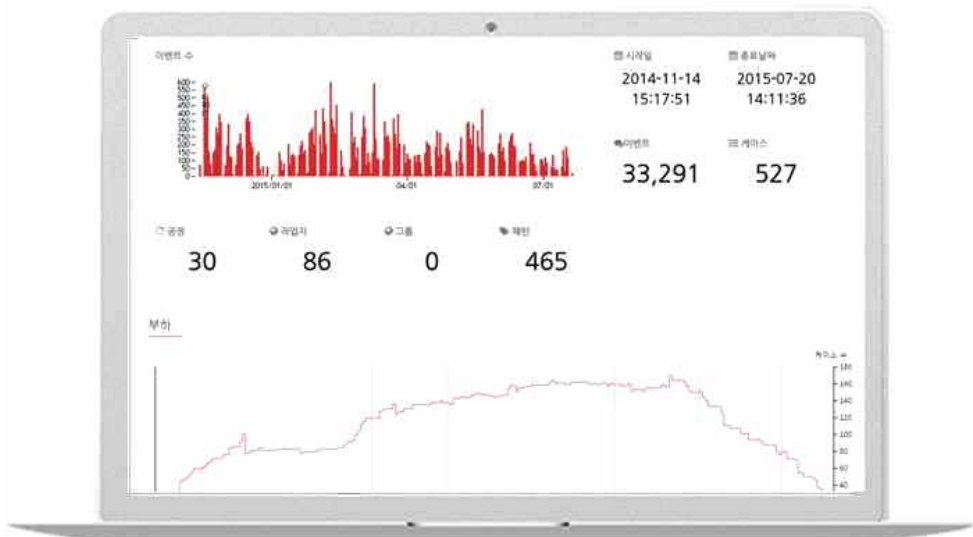
(주)사이람은 소셜 네트워크 분석에 특화된 기업으로, 2000년에 창립되었다. 2001년에 세계 최초의 상용 소셜 네트워크 분석(Social Network Analysis) 소프트웨어인 NetMiner를 출시했다. NetMiner는 GUI(Graphical User Interface) 기반의 편리한 사용법과 유연한 데이터 분석 환경을 제공하여 세계적인 명성을 보유하고 있다. 그 외 제품으로는 2003년에 출시된 NetExplorer가 있으며, 이것은 범죄 네트워크 분석과 사기범죄 적발 솔루션이다. 급증하고 있는 보험사기, 범죄 수사에서 혐의자들 간의 직·간접적 인과관계를 시각적으로 분석해 범죄 집단을 적발하는데 효과적으로 활용되고 있다.



〈그림 7〉 사이람의 소셜 네트워크 분석 소프트웨어 NetMiner

* 출처 : http://www.cyram.com/product/product_01.jsp

(주)사이버다임은 1998년 비정형 콘텐츠 관리 국산화를 위해 설립된 업체로 문서를 체계적 시스템화 하는데 주력하고 있다. 기업용 클라우드 솔루션, 문서관리 기술 등을 보유하고 있으며 (주)사이버다임의 Process Analyzer는 ERP, 제조정보시스템, 그룹웨어 등 기업의 업무처리 진행에서 기록되는 이벤트를 로그 분석하여 의미 있는 정보를 찾아내는 제품이다. Process Analyzer를 사용하면 Hadoop, 클라우드 서비스, 데이터베이스에 이르기까지 모든 데이터를 탐색할 수 있다. 기본적인 Data Dashboard부터 데이터 흐름을 표현하는 Animation, Process Map 등에서 다양한 시각화 도구를 제공하고 웹 기반 프로세스 마이닝을 어디에서나 서버에 접속하여 통계 정보, 분석 정보를 확인할 수 있다.



Data Dashboard

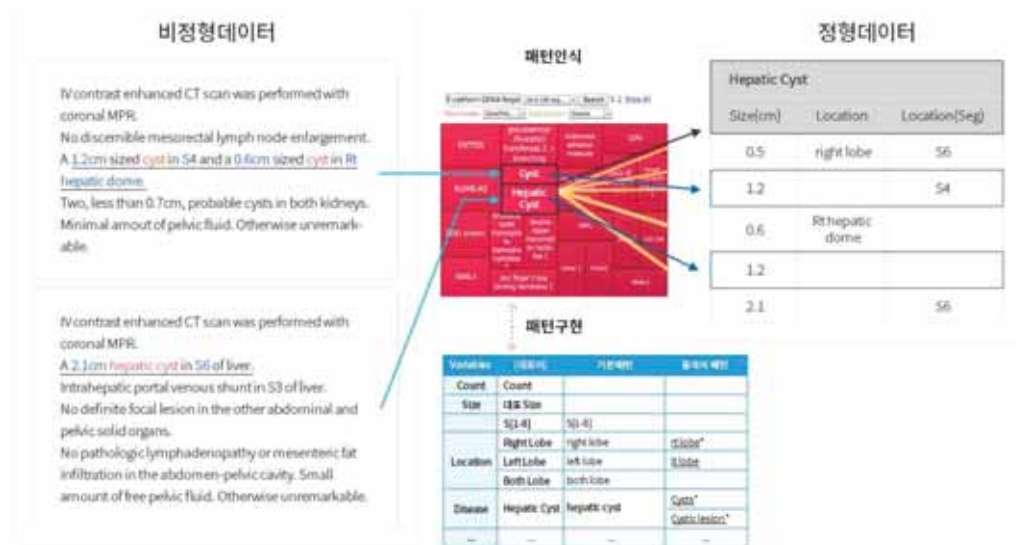
분석을 통해 얻어진 다양한 통계 값들에 대한 대쉬 보드 화면

〈그림 8〉 사이버다임의 Process Analyzer 시각화 기술

* 출처 : <https://www.cyberdigm.co.kr/products/process-analyzer/>

(주)소프트센은 1988년 (주)비티씨코리아로 설립되었으며, 2014년 현 상호로 변경한 업체다. (주)소프트센은 빅데이터 서비스, 빅데이터 솔루션, IT인프라, IT 솔루션 등의 사업을 하고 있다. 빅데이터 솔루션으로 주요 제품은 Big Cen TA, Research Assistant 등이다. Big CEN TA(Text Analysis)는 고객사의 기간계의 시스템에서 비정형 텍스트로부터 의미 있는 항목을 자동 추출하여 정형화한다. 또한, 정형과 비정형화된 데이터를 결합하여 하이브리드 검색기능 제공이 가능한 솔루션이다. Research Assistant는

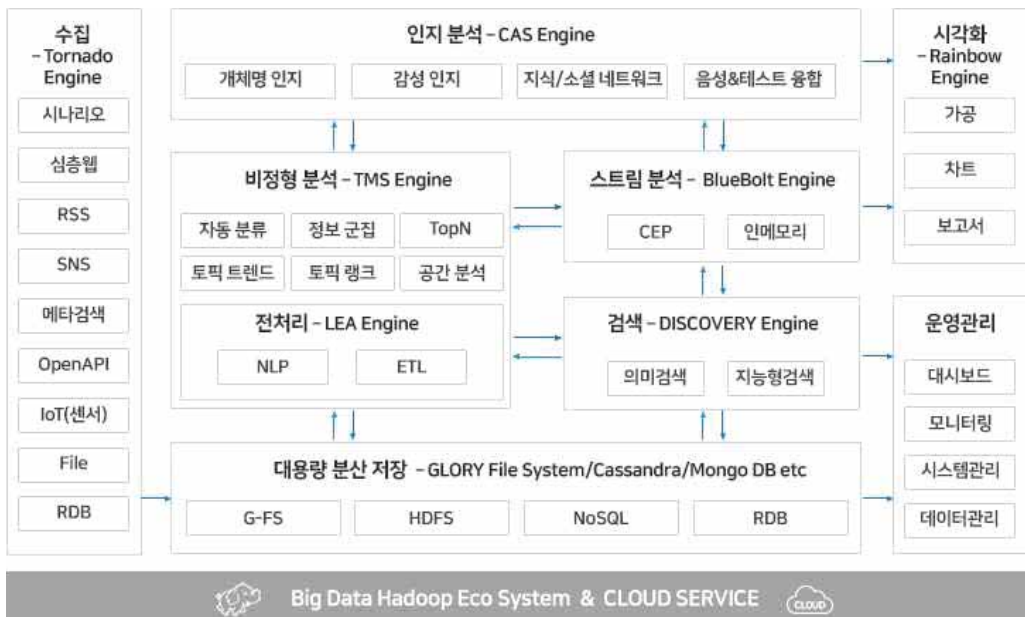
임상연구 방법 절차에 따라 사용자 중심의 화면 구성 및 복합 검색(키워드 검색 + 조건 검색)지원과 동의어와 유사어 사전 제공, 다차원 분석정보 제공하여 의료진 중심의 연구와 임상 정보 제공하는 솔루션이다.



〈그림 9〉 소프트센의 Big CEN TA 시스템 예시

* 출처 : <http://www.softcen.co.kr/app/view/business/department>

(주)솔트룩스는 2000년에 설립된 (주)시스메타로부터 시작했으며, 인공지능과 빅데이터 기술에 전념해 왔다. (주)솔트룩스의 Bigdata Suite는 End-to-End One stop 지능형 빅데이터 분석 통합 플랫폼으로, 시각분석 엔진(Rainbow), 수집 엔진(Tornado), 스트림 분석 엔진(BlueBolt), 저장 및 검색 엔진(DISCOVERY), 비정형 분석 엔진(TMS), 인지 분석 엔진(CAS) 등 6개의 엔진을 제공한다.



〈그림 10〉 솔트룩스의 Bigdata Suite 구성도

* 출처 : <http://www.saltlux.com/bigdata/summary.do?menuNumber=2>

(주)아이지에이웍스는 2006년 설립된 모바일 빅데이터 업체로 AI와 머신러닝 기반의 DMP(Data Management Platform), 모바일 데이터분석, 마켓 인텔리전스, 마케팅 자동화, 트레이드 데스크 등 모바일 데이터와 플랫폼을 제공하는 Data-Tech SaaS(서비스형 소프트웨어) 기업이다. (주)아이지에이웍스의 애드 브릭스(adbrix)는 앱 광고 성과 측정부터 타겟팅 광고, 사용자 분석, 운영을 동시에 해결하는 솔루션으로 고객사는 애드 브릭스를 통해 광고 성과를 측정하고 유입된 고객을 분석하여, 그 결과 데이터를 활용 및 광고와 운영을 고도화한다.

(주)와이즈넷은 1999년 미국 실리콘밸리에서 출발한 기업으로, 자체 인공지능을 기반 기술로 기업용 인공지능 소프트웨어(챗봇 및 빅데이터 수집, 분석, 검색) 제품을 제공한다. (주)와이즈넷의 주요 빅데이터 제품으로 텍스트마이닝 솔루션 WISE TEA V2, 빅데이터 정보수집 솔루션 WISE BICrawler, 빅데이터 의미분석솔루션 WISE BIC Analyzer, 빅데이터 검색솔루션 Search Formula-1 V5, 소셜분석 서비스 BuzzInsight 등이 있다.

(주)이씨마이너는 빅데이터 분석에 특화된 솔루션 개발 업체로, 2000년 창업 이래 데이터 마이닝 기술력을 기초로 데이터마이닝 소프트웨어 판매 및 응용 프로젝트 수행, 데이터 웨어하우스 및 데이터 마트 구축, 통합 분석 솔루션 공급과 시스템 구축 등으로 그 사업 영역을 넓히고 있다. (주)이씨마이너는의 제품으로는 자금세탁방지 솔루션 ECMinerAML™,

데이터마이닝 기반 지능형 모니터링시스템 ECMinerIMS™, 데이터마이닝 소프트웨어 ECMiner™ 등이 있다. ECMiner™는 통계 기반의 실시간 빅데이터 분석 솔루션으로 텍스트 및 이미지 마이닝, 연관분석, 지능형 모니터링 등이 가능하다.

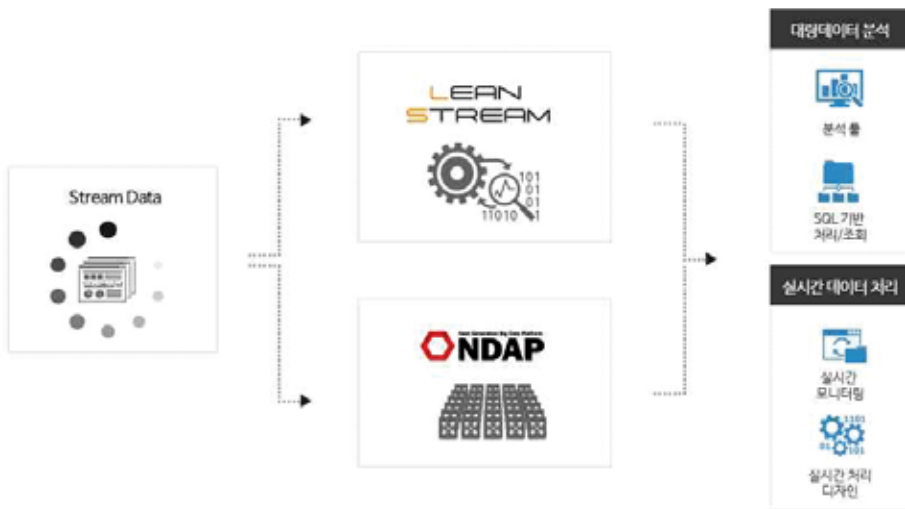


〈그림 11〉 이씨마이너의 데이터마이닝SW ECMiner™ 제품 개요

* 출처 : http://ecminer.com/?page_id=132

(주)케이티넥스알(kt NexR)은 빅데이터 End-to-End 서비스 및 제품을 제공하는 기업으로 빅데이터 글로벌 표준 기술인 하둡(Hadoop)과 견줄 수 있는 국내 최고 수준의 기술력 보유 기업이다. 제품으로는 실시간 빅데이터 처리와 분석을 위한 엔터프라이즈 솔루션 Lean Stream, 빅데이터 플랫폼 NDAP(kt NexR Data Analytics Platform)이 있다.

(주)코난테크놀로지는 인공지능을 기반하여 비정형 데이터 마이닝 전문기업이다. 주요 제품으로 시맨틱 검색 기술 기반의 텍스트 마이닝 분석 서비스인 pulse-K, 검색로그 분석 솔루션 Konan Log Analytics, 비정형 데이터 통합 분석 플랫폼인 Konan Analytics 4가 있다.



〈그림 12〉 kt NexR의 빅데이터 제품군

* 출처 : <https://www.ktnexr.com/product/product.html>

SK텔레콤(주)은 SK그룹 계열의 이동통신업체이며, 하드웨어와 소프트웨어를 결합한 실시간 빅데이터 분석 솔루션을 제공한다. SK텔레콤(주)에서 제공하는 Metatron은 실시간 빅데이터 분석 솔루션으로 대량의 로그 데이터를 수집하여 실시간 분석을 통한 시각화에 이르기까지 한 번에 제공한 End-to-End 분석 솔루션이다.

2. 국외 활용 동향 분석

첫 번째 사례로는 구글의 리더십 개발 솔루션으로 팀의 리더와 팀의 성과 간에 상관관계를 분석하는 데이터 기반 성과 측정 솔루션이다. 팀을 성공적으로 이끈 리더들의 특성을 데이터화 하고 빅데이터 분석도구를 통해 팀이 성공하는데 과정을 분석하여 리더십 개발 방안을 도출하는 것이다. 이를 통해 산출된 결과를 교육프로그램에 적용하여, 좋지 못한 성과를 낸 팀을 대상으로 교육한 결과 리더십 개발 효과에 성과를 이끌었다.

두 번째 사례는 제록스로 성과와 성격을 빅데이터 분석 도구를 통해 분석했다. 성과가 훌륭한 직원의 이직 및 퇴직의 원인을 빅데이터를 통해 분석하여 인사관리 방법론 개발, 근무 연수 및 성과 그리고 직원의 성격이 어떠한 상관관계가 있는지에 따라 '창의성'이 높은 직원의 성과가 높으며 근무 연수가 높다 라는 결론을 냈다. 이에 따라 창의력과 관련된 잠재력을 보유한 직원을 채용하기 위한 방안 모색하였고, 이직률을 20%까지 낮췄다.

세 번째는 다우 케미칼로 인력구조 개선 사례다. 7년 주기로 호황과 불황을 반복하는

업계의 특성 때문에 인사 조정 필요 및 발생시 4만 명의 인력을 빅데이터 분석도구를 활용하여 직원을 5개의 연령 그룹으로 나누고, 10개의 직급으로 나눠서 분석한 결과를 도출했다. 데이터 기반 인력구조를 예측한 시나리오를 개발하여 그에 맞는 대응 및 대책을 마련하고 사업관리에서 성공적으로 활용했다.

네 번째는 Bon Ton Company(백화점)의 직원 채용 및 관리 사례다. 빅데이터 분석 도구를 통해 백화점 영업직군에서 ‘인지 능력’이 중요함을 발견했다. 그 결과 백화점 1층 직원은 외모가 보다 ‘인지 능력’이 뛰어난 인력을 투입하여 매장당 평균 이직률 25% 감소와 매출을 1,400달러 증가시켰다.

1) 제조 분야

첫 번째는 인텔의 제조 공정 비용 절감 사례다. 2012년 제조 공정의 비용 낭비를 제거하기 위하여 빅데이터 분석 도구를 도입하여 3백만 달러의 낭비 요소를 제거했다. 또한 빅데이터 분석 시스템을 제조 공정의 전 분야로 확대시켜 총 3천만 달러의 비용을 절감시켰다.

두 번째는 지멘스의 공장 자동화 및 불량제거 사례다. 빅데이터 분석도구를 활용한 공장 자동화 시스템을 구축하기 위해서 약 2억 유로를 투자하여 불량률은 제품 100만개 중 11.5개 수준으로 줄였고, 생산성은 8배 증가시켰다. 매일 축적되는 5,000만 건의 데이터를 분석하여 기계의 가동 여부와 에너지 효율을 높이는 최적의 공정을 모색 및 진단했다. 오랜 시간 작동을 안 해도 된다고 판단된 기계의 전원은 자동으로 차단 시켰으며, 컴퓨터가 재가공한 정보를 제품 개발 부서에 통보하여 상품 개발 과정을 개선했다. 상품의 기획·설계 단계부터 판매 이후까지 모든 정보를 수집하여 제조생산 효율을 증대시키는데 활용했다.

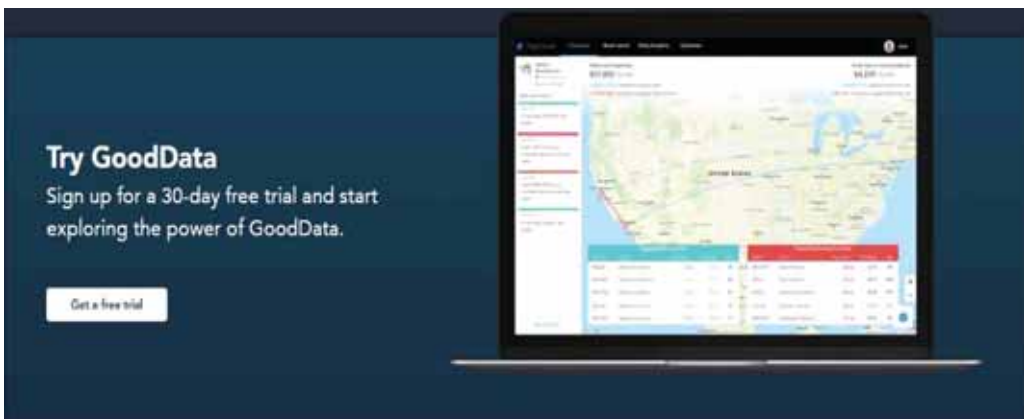
세 번째는 제너럴 일렉트릭의 항공 생산에서의 개선 사항 분석 사례다. 제너럴 일렉트릭 항공은 빅데이터 분석 도구를 활용하여 제품 생산 프로세스를 개선하여 약 25%의 생산성을 향상 시켰다. 또한, 분석 결과를 적용한 후에는 예상하지 않았던 생산 속도 분야에서 25%의 향상을 이끌었다.

네 번째는 IBM의 반도체 제조 분야에서 공정을 개선한 사례다. 반도체 공장에서 복잡한 제조과정 및 공정을 빅데이터 분석 도구를 통해 효율화하여 제조 라인에서 생산 시간을 약 15% 단축하는 효과 확보했다. 또한, 공급망 부문에서는 품질에 대한 조기 경보시스템을 도입하여 결함이 발생할 수 있다는 경보를 6주 이전에 제공 받아, 연간 약 1,000만 달러라는 비용을 절감했다.

2) 빅데이터 서비스 분야)

미국의 Teradata는 데이터 웨어하우스 및 빅데이터 관련 컨설팅 서비스와 분석 솔루션을 제공하는 글로벌 기업으로 미국 샌디에고에 본사를 두고 있다. 이 회사는 1979년 캘리포니아주 브렌트우드에서 칼텍의 연구원과 씨티은행의 첨단 기술 그룹 간의 협력으로 설립되었다. DW(Data Warehouse)/CRM(Customer Relationship Management) 관련 플랫폼과 기업 인텔리전스 및 데이터웨어하우징 분야, 산업별 특화된 솔루션 및 포괄적 전문 서비스의 역량을 보유하고 있다. 2011년 Hadapt(2014), Revelytix(2014), 애스터(Aster) 등의 인수합병을 진행하며 빅데이터 역량을 강화시켰으며, 최근에는 아키텍처 컨설팅, 기술 솔루션, 포트폴리오로 비즈니스 솔루션으로 구성된 새로운 전략을 제시하고 있다. 주요 솔루션으로는 Borderless Analytics, Aster Analytics, Teradata Everywhere, AoTAs(Analytics of Things Accelerators) 등을 공급하고 있다.

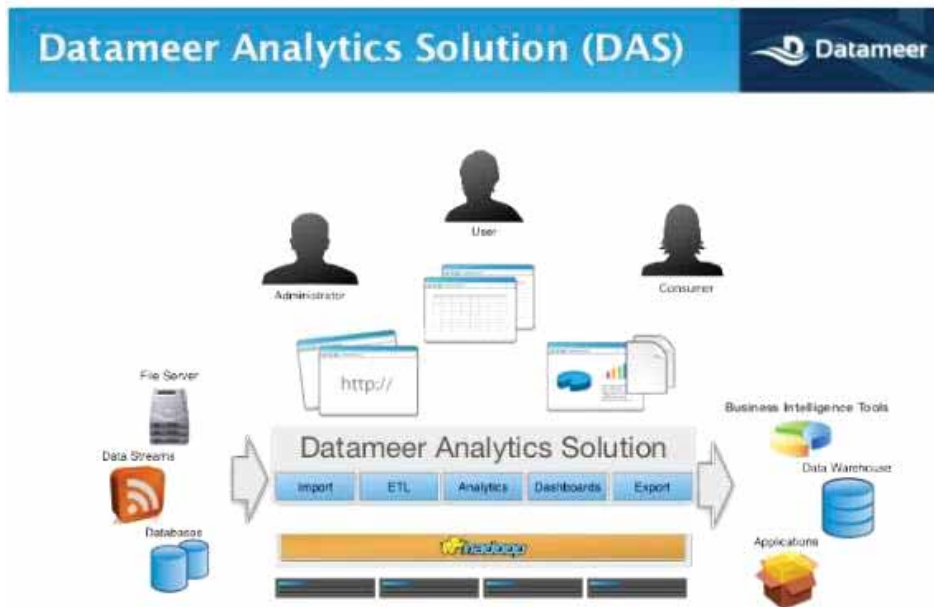
미국의 GoodData는 클라우드 컴퓨팅 기반 빅데이터 BI와 어널리틱스를 지향하는 플랫폼 개발 기업으로 2007년 설립되었으며, 샌프란시스코에 본사를 두고 있다. 자료의 저장, 수집, 분석, 연계, 시각화 등 BI의 모든 핵심 솔루션을 만들 수 있는 Tool, API(Application Programming Interface), 프레임워크 툴로 구성된다. GoodData의 모듈식 플랫폼은 높은 수준에서 데이터 준비, 수집, 분석, 변환, 쿼리, 시각화, 응용 프로그램 통합을 위한 도구, 스토리지 및 런타임을 제공한다. 이를 통해 기업은 기존 인프라와 원활하게 통합되고 고객, 직원, 비즈니스 파트너를 위해 분석 솔루션을 쉽게 구현할 수 있다.



〈그림 13〉 GoodData의 30-day free trial version

* 출처 : <https://www.gooddata.com/>

미국의 Datameer는 빅데이터 분석 시각화 회사로서 미국 샌프란시스코에 본사를 두고 빅데이터 어널리틱스 플랫폼을 제공한다. Datameer의 제품인 DAS(Datameer Analytics Solution)은 데이터 리소스 통합, 200개가 넘는 분석 기능을 보유한 스프레드시트 인터페이스가 제공되고 클라우데라, 아마존, 아파치, 맵알 등 주요 하둡 배포판에서 활용 가능하다.



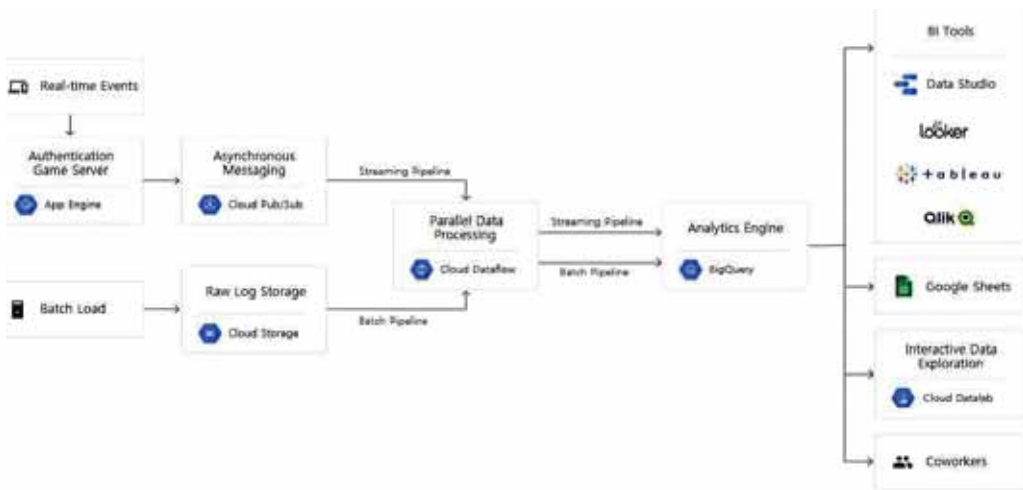
〈그림 14〉 Datameer의 Datameer Analytics Solution(DAS)

* 출처 : <https://www.datameer.com/>

미국의 1010data은 2000년 설립된 빅데이터 분석 기업으로 미국 뉴욕에 본사를 두고 정형 또는 비정형 데이터의 다양한 종류의 데이터를 분석하기 위해 툴 및 플랫폼으로 제공하고 있다. 1010data는 기본 비즈니스 쿼리에서 정교한 데이터 과학 모델까지 데이터에서 실행 가능한 전체 정보를 추출할 수 있는 도구를 제공하고 있다. 또한 통계 함수, 최적화, 시계열 분석, 기계 학습 등을 포함한 함수 라이브러리를 사용하여 진단, 예측, 설명 및 규정 분석을 수행한다.

미국의 Google은 1998년 세르게이 브린과 래리 페이지에 의해 설립된 업체로, 포털 사이트, 웹 검색, 관련 사이트를 운영하여 광고를 주 사업 영역으로 두고 있다. BigQuery는 높은 확장성으로 비용 효율성을 갖춘 서버리스 클라우드 데이터 웨어하우스로

메모리 내 머신러닝과 BI Engine을 갖고 있다. BigQuery의 특징은 기존 RDBMS에서 사용되는 SQL과 유사한 언어를 사용하며 클라우드 서비스(NoOps), 데이터 복제를 통한 안정성, 대용량 지원과 빠른 성능, 저렴한 가격, 배치와 스트리밍 모두를 지원한다. 3,600개의 디스크와 8,800개의 CPU를 사용하는 대규모 인프라로 약 1,000억 개의 레코드에 대하여 질의를 약 30초 수행한다. Hadoop, Spark 등은 SparkSQL 또는 Map&Reduce 로직으로 사용하기 위해선 일정 수준 이상 전문성이 필요하지만, 상대적으로 BigQuery는 실질적 사용과 유지보수 등 매우 간편하다는 장점을 갖고 있다 평가받고 있다.



〈그림 15〉 Google의 BigQuery 솔루션 아키텍처

* 출처 : <https://cloud.google.com/bigquery>

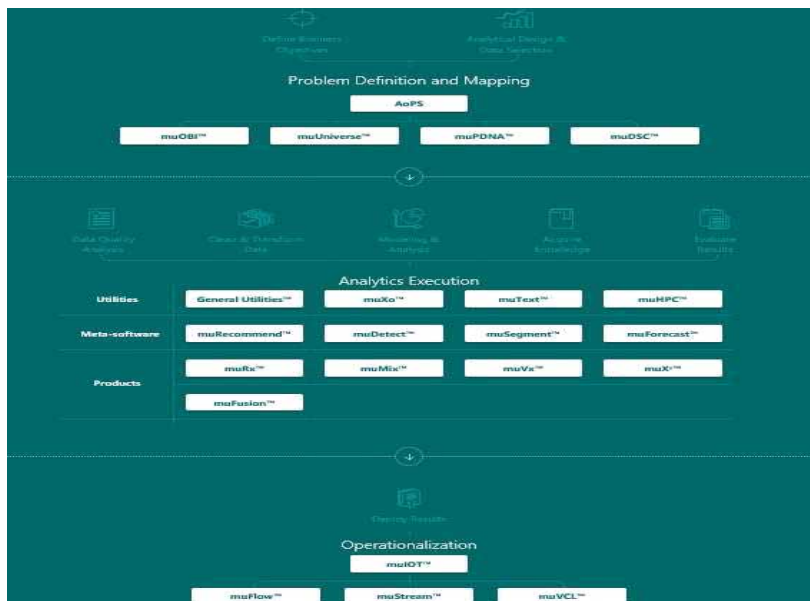
미국의 Splunk는 IT분야에서 발생하는 실시간 이벤트 데이터, 로그 데이터, 다양한 장비 데이터를 수집하고 모니터링하며 분류, 검색, 분석할 수 있는 엔진을 제공하는 미국의 기업으로 2004년 설립되어 미국 샌프란시스코에 본사를 두고 있다. 동사는 이벤트 데이터, 로그 데이터 등 기계가 생성한 빅데이터를 웹 기반 인터페이스를 통해 모니터링, 검색, 분석하는 소프트웨어를 개발 및 공급하고 있다. 대부분의 Fortune 100대 기업들과 마찬가지로 전세계 100개국의 약 9,000여 개의 기업과 서비스 공급자, 정부가 Splunk 소프트웨어를 사용하고 있다. 국내에서는 통신사, 금융, 인터넷 포털, 게임개발사, 제조사 등 300여 개사에서 도입하여 사용되는 솔루션이다.



〈그림 16〉 Splunk의 Splunk® Enterprise

* 출처 : https://www.splunk.com/en_us/software/splunk-enterprise.html

인도의 Mu Sigma는 데이터 분석 서비스를 제공하는 인도의 경영 컨설팅 회사로 2005년 설립되었으며, 인도 벵갈루루(Bengaluru)에 본사를 두고 있으며, 빅데이터 분석 소프트웨어, 통계 분석 소프트웨어, 빅데이터 시각화 및 리포팅 도구 등 많은 유틸리티를 개발하였다. 동사의 big data analytics software는 고객사가 문제 정의 및 매핑에서 분석 솔루션 검색 및 운영에 이르기까지 데이터 분석 솔루션을 확장할 수 있도록 도와준다.



〈그림 17〉 Mu Sigma의 analytics value chain

* 출처 : <https://www.mu-sigma.com/our-platform/big-data-analytics-software>

미국의 Syncsort는 1968년 설립된 글로벌 소프트웨어 회사로 미국 뉴욕주 펠리버에 본사를 두고 있으며, 빅데이터, 초고속 정렬 제품, 데이터 통합과 서비스를 제공하는 소프트웨어 회사로서 MS windows, UNIX, Linux, Hadoop를 지원하고 있다. 동사는 Splunk, Hadoop, cloud와 같은 차세대 분석 플랫폼을 지원하며, 각 플랫폼 특화된 솔루션을 제공한다.

미국의 Attivio는 최고의 인지 검색 및 인사이트 플랫폼 회사로 미국 매사추세츠주 보스턴에 본사를 두고 있으며, Attivio Cognitive Search and Insight Platform은 자연 언어 처리, 기계학습 및 지식 그래프와 같은 자체 학습 기술을 결합한 안전한 기업용 플랫폼으로 형식에 관계 없이 엔터프라이즈 데이터 및 콘텐츠를 색인화하고 분석하며 행동 데이터를 통합하여 사용자 경험을 개인화한다.

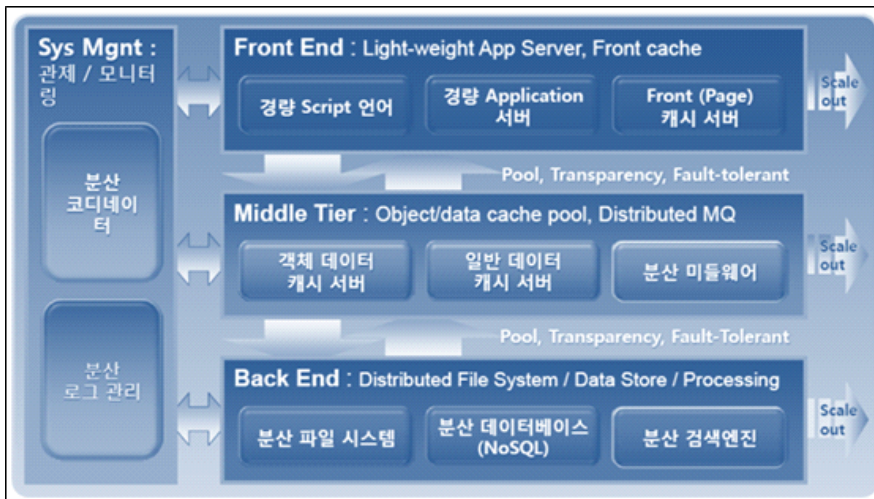
미국의 FICO는 선도적인 분석 소프트웨어 회사로 미국 캘리포니아주 산호세에 본사를 두고 있다. FICO Big Data Analyzer는 비즈니스 사용자, 분석가 및 데이터 과학자가 Hadoop에서 모든 유형 및 크기의 데이터를 탐색하고 분석하여 귀중한 인사이트를 얻을 수 있는 맞춤형 분석환경이다. 데이터 프로파일링을 활용하여 한번에 한 변수씩 데이터를 즉시 시각화한 다음 머신러닝을 적용하여 향후 결과에 대한 예측을 수행한다.

네덜란드의 Flytxt는 네덜란드 뉘베게인(Nieuwegein)에 본사가 있으며, 전 세계 CSP와 모바일 업체를 위한 빅데이터 분석 솔루션을 제공하는 업체로 2008년 설립되었다. 동사의 NEON-dX는 분석, 인공지능, 마케팅 자동화를 클라이언트의 CRM 환경과 원활하게 통합되고 즉시 사용 가능한 솔루션으로 패키지화한 것으로, 기업의 마케팅팀이 쉽고 빠르게 측정 가능한 수익증가를 창출할 수 있도록 실시간으로 학습, 예측, 권고 및 행동한다.

Ⅲ. 빅데이터 분석도구 분석

1. 빅데이터 아키텍처 분석

1) 빅데이터 아키텍처 구성도



〈그림 18〉 빅데이터 아키텍처 구성도

빅데이터 가용성 제고를 위하여 데이터 처리에 최적화된 기술 요소로 구성된다. 위 구성 요소를 구체적으로 보면 표 4와 같다.

〈표 4〉 빅데이터 아키텍처 구성 요소

구성요소		설명	사례
Front End	경량script언어	스크립트언어로 Front End 구성, GC (graphics context) 성능 및 UI 구현 이용	python, Ruby on Rails, Scala, JavaScript, PHP
	경량App Server	다수의 경량 Application Server를 이용하여 사용자 응답성의 극대화	Jetty, Apache Thrift, Apache Avro, Tomcat, NginX
	Front Cache	정적 리소스, 동적데이터에 대한 캐시 서비스로 App/DB 서버부하 절감 및 응답성 향상	squid cache, Apache traffic server, Varnish cache

구성요소		설명	사례
Middle Tier	캐시Pool	DBMS를 통해 빈번하게 조회된 데이터를 메모리에 캐시하여 DB 부하 절감 및 응답속도 향상	Coherence, Oracle, Memcached, Membase(CouchBase), Ehcache
	분산Middleware	분산Application 서버와 Data- base 간의 투명성과 Fault- tolerant를 제공하는 분산 메시지기반 미들웨어	ZeroMQ, Kestrel, Apache ActiveMQ,
Back End	분산파일시스템	분산Application 서버와 분산Database 를 수평적으로 확장 가능한 네트워크 기반 분산파일	Apache, HDFS, GFS
	연산처리/ 분산데이터 스토리지	기본적으로 데이터의 분산관리를 지원하며 인덱스의 최적화에 집중화된 DB로 데이터 쓰기가 많은 업무의 실시간 데이터 처리에 최적화된 DB	MongoDB, Hadoop, Cassandra, Map/Reduce, HBase
	DW/검색엔진	확장 가능하고 성능정보 검색 서비스용 라이브러리엔진과 DW 엔진	-
System Mgmt	모니터링/ 시스템관리/ 분석도구	성능, 시스템로그, 응답성 등을 분석하고 표현하여 신속한 문제 파악과 주요 지표 관리를 통해 운영조직의 대응 여부와 시점에 대한 의사결정 지원	Scribe, Apache Zookeeper, Jconsole, Java Melody, Apache Chukwa
	최적화 도구	CPU 및 메모리 사용량에 대한 Profiling 과 분석을 지원하는 SW 도구를 사용	yourkit

2. 빅데이터 분석도구

1) 빅데이터 분석기법

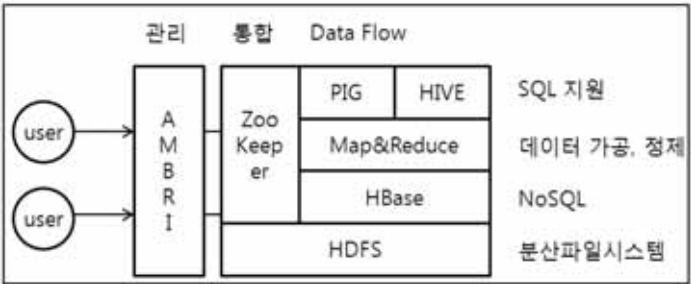
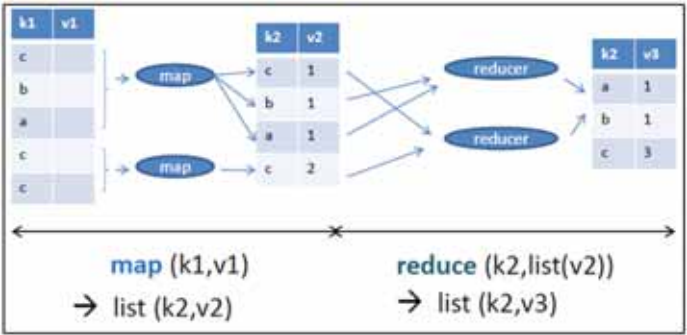
〈표 5〉 빅데이터 분석기법

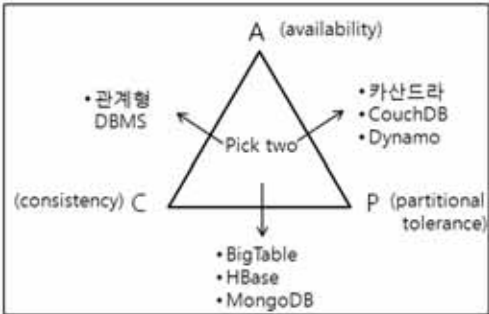
분석 기법	설 명
Text Mining	- 문서 요약, 추출, 문서, 문서 군집, 정보 분류, - 텍스트가 가진 카테고리 분류 - 자연어 처리기술 기반 정보 추출, 가공 - 텍스트 데이터에서 의미 있는 정보 추출 - 다른 정보와의 연계성 파악
Opinion Mining	- 입소문 분석 등에 활용, 특정 서비스 및 상품에 대한 시장규모 예측, 소비자 반응 - 정확성을 위해서는 전문가에 의한 선호도 표현 및 단어 자원의 축적이 필요함 - 소셜미디어 등의 긍정, 부정, 중립 선호도 판별 기술 - 평판분석 기법

분석 기법	설 명
Social N/W Analytics	• Social N/W 연결구조, 연결 강도를 바탕으로 사용자의 명성 및 영향력 측정 • Social N/W 상에서 입소문의 중심이나 허브 역할을 하는 사용자를 찾는 데 주로 활용
Cluster Analysis	• 비슷한 특성을 가진 개체를 합쳐가면서 최종적으로 유사 특성의 그룹 발굴

2) 빅데이터 분석도구

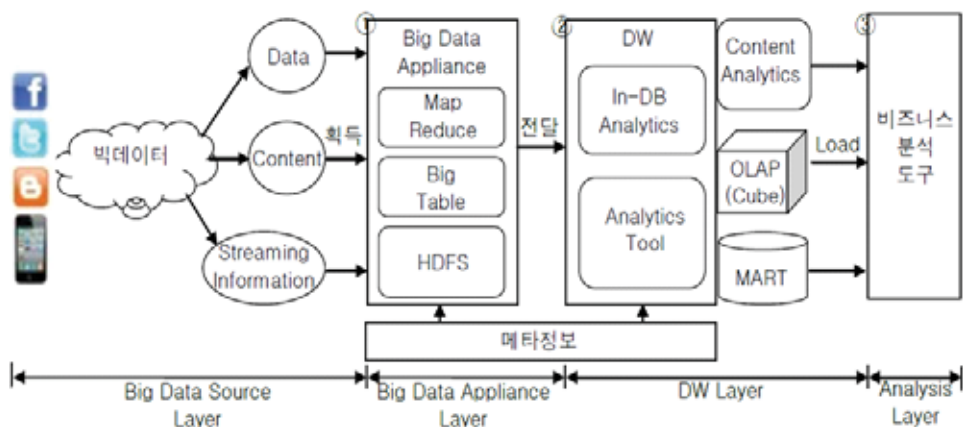
〈표 6〉 빅데이터 분석도구

기술 요소	설 명
Hadoop	• 현재 정형 및 비정형 빅데이터 분석에 가장 선호되는 솔루션 • 오픈소스 분산처리 기술 프로젝트 • Yahoo, Facebook 등  The diagram illustrates the Hadoop architecture. On the left, two 'user' circles point to an 'AMBI' (Application Master) box. The 'AMBI' box is connected to a 'ZooKeeper' box. To the right of 'ZooKeeper' is a 'Data Flow' section containing 'PIG', 'HIVE', 'Map&Reduce', 'HBase', and 'HDFS'. To the right of the 'Data Flow' section are labels: 'SQL 지원' (SQL support) for PIG and HIVE, '데이터 가공, 정제' (Data processing, refinement) for Map&Reduce, 'NoSQL' for HBase, and '분산파일시스템' (Distributed file system) for HDFS.
Map & Reduce	• Map: 흩어져 있는 데이터를 key 및 value구조로 묶는 연산 • Reduce: Map작업 후 중복데이터를 제거 및 데이터 추출  The diagram shows the Map & Reduce process. It starts with a table of (k1, v1) pairs: (c,), (b,), (a,), (c,), (c,). These are processed by 'map' operations to create (k2, v2) pairs: (c, 1), (b, 1), (a, 1), (c, 2). These are then processed by 'reduce' operations to create (k2, v3) pairs: (a, 1), (b, 1), (c, 3). Below the diagram, the process is summarized as: $\text{map}(k1, v1) \rightarrow \text{list}(k2, v2)$ and $\text{reduce}(k2, \text{list}(v2)) \rightarrow \text{list}(k2, v3)$.
R	• 통계 계산, 시각화를 위한 언어, 개발 환경 제공 : 최신 데이터마이닝 기법 구현, 기본적 통계기법부터 모델링 • 구현 결과를 그래프 등으로 시각화 가능 • C, Python, Java 등 다른 프로그래밍 언어와 연결 용이

기술 요소	설 명
	• 리눅스/유닉스, 윈도우, Mac OS 등 대부분의 컴퓨팅 환경 지원 • Hadoop 환경상 분산처리를 지원하는 라이브러리 제공 • Amazon, Google, Facebook 등
NoSQL	• No SQL, Not only SQL • 관계형 DB와 다르게 설계된 비관계형 DB • Table Schema 고정되지 않고 Join 연산 지원 안 함 • 수평적 확장 용이 • CAP Theorem 

빅데이터의 적극적 활용을 통한 서비스, 상품 혁신을 위해서는 내외부 데이터 통합, 수집 및 분석역량, 인프라, 조직 분야에서 체계적인 준비가 필요하다.

3) 빅데이터 관리 기법



〈그림 19〉 빅데이터 관리 기법 절차

〈표 7〉 빅데이터 관리 기법 구성요소

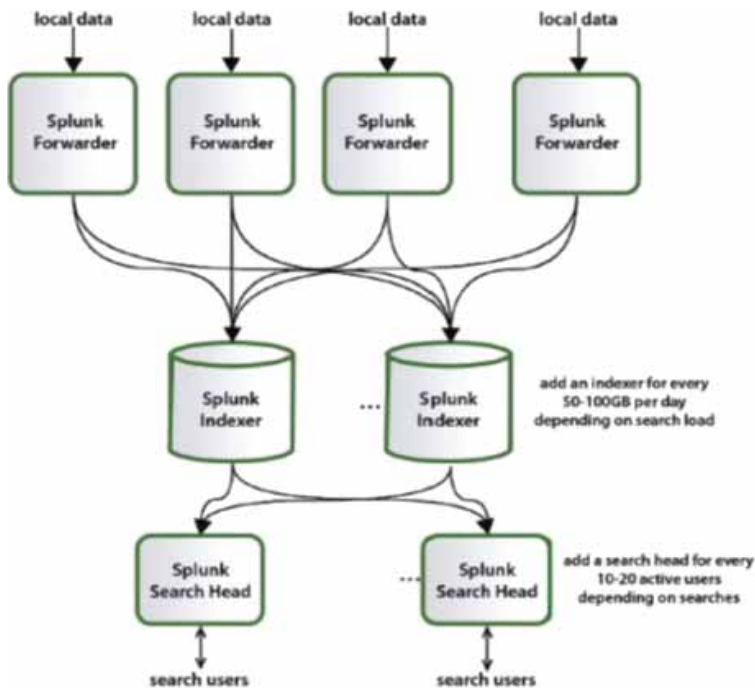
구분	주요 관리방안	적용기술
Big Data Appliance	- 외부로부터 유입된 빅데이터를 전문 Appliance에서 처리 - 빅데이터를 분산처리 방식에 의해 (Key-value) 형태로 처리 - 처리된 데이터는 Big Table에 저장 후 관리됨	Map-Reduce Big Table
Data Warehouse	- Big Table에 저장된 데이터 중 정형데이터를 추출하여 DW 적재 - 빠른 데이터 처리 및 데이터 컬럼 단위 압축 - 다차원 모델링에 의한 데이터 처리 수행	ROLAP, HOLAP Data Mining, Snowflake스키마, ETL Star스키마
비즈니스 분석 도구	- 고급 분석기술 및 데이터 사이언티스트를 통한 분석 실시 - 데이터의 가치에 따라 ILM과 연계하여 데이터 보관 및 관리	Content Analysis 예측분석 Real time Analysis

내용분석 기법 및 OLAP, MART 등 비즈니스 분석 도구로 의사결정을 위한 정보 분석 및 가치기반 저장 관리한다.

4) 빅데이터 수집기술의 개념과 도구 / 자동수집

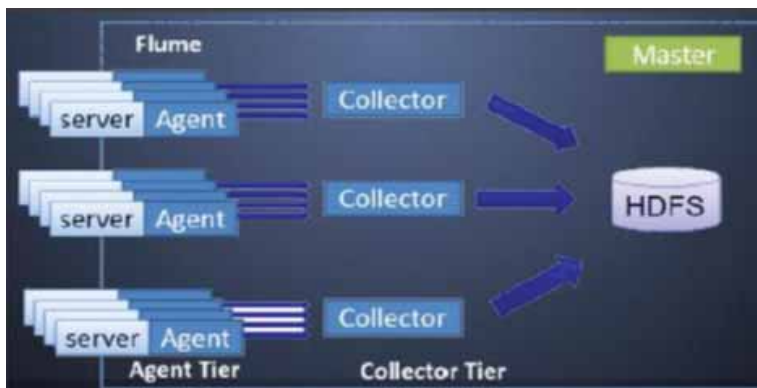
빅데이터 수집기술 개념은 조직 내부와 외부의 분산되어있는 여러 데이터 소스로부터 필요한 데이터를 검색하고 수동, 자동 수집하는 과정과 관련된 기술이다. 일반적으로 조직 내부에서 보유하고 있는 정형 데이터는 로그 수집기를 통해 수집되고, 조직 외부에 있는 비정형 데이터는 소셜 네트워크 서비스, RSS Reader, 크롤링에서 제공하는 오픈 API를 통해 프로그래밍하여 수집한다.

빅데이터 수집 도구로 첫 번째 Splunk(스플링크)이 있다. 프리버전과 엔터프라이즈 버전을 제공한다. 그리고 엔터프라이즈 버전에서의 하둡과 통합하여 HDFS에 데이터를 저장하고 하둡을 통해 분석 프로세싱을 할 수 있도록 업그레이드된다. 웹 기반의 GUI를 제공하여 그 사용성이나 관리자 적인 측면에서는 큰 강점이 있다.



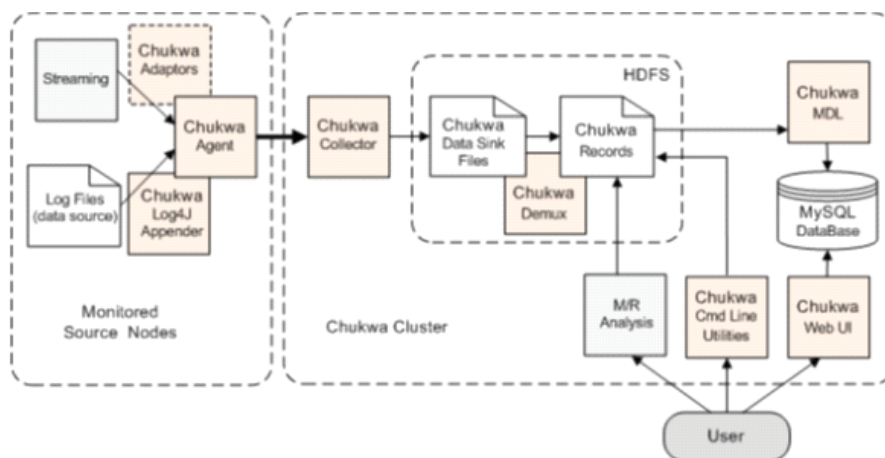
〈그림 20〉 스플UNK를 통한 빅데이터 수집

빅데이터 수집 도구로 두 번째 Flume(플럼)이 있다. 에이전트, 컬렉터, 스토리지티어로 구분된다. 데이터수집을 위하여 데이터 플로우 토폴로지를 구성할 수 있고 마스터 노드에서 통합하여 관리할 수 있는 웹페이지를 제공과 이를 쉽게 설정 및 변경하기 위하여 모니터링 가능하다. 또한, 마스터 노드를 이중화하여 가용성이 높고, Java로 구현되어 있어서 다양한 OS 플랫폼에 포팅 가능하다.



〈그림 21〉 플럼을 통한 빅데이터 수집

빅데이터 수집 도구로 세 번째 Chukwa(척와)가 있다. HICC(Hadoop Infrastructure Care Center), 컬렉터(Collector), 에이전트(Agent), MapReduce 처리로 구성된다. 척와는 확장성이 뛰어나고 대용량의 처리가 가능 분산시스템이며 모니터링과 분석 기능 클러스터 환경 로그 분석에 탁월하다. 그리고 오픈소스 기술이다.



〈그림 22〉 척와를 통한 빅데이터 수집

빅데이터 수집 도구로 네 번째 Scribe (스크라이브)가 있다. Facebook이 개발하여 2008년에 공개한 로그수집 기술이다. 대량의 서버로부터 실시간으로 수집되는 로그 데이터를 집약하기 위하여 개발되었다.

IV. 분야별 빅데이터 분석도구 적용 방안

1. 적용 선제 조건

1) 데이터 자원의 체계적 관리

데이터 자원의 체계적 관리를 위해 데이터 수집, 데이터 처리, 데이터 저장, 데이터 활용, 데이터 분석으로 구분하여 설명할 수 있다.

첫째, 데이터수집은 기술, 기법으로 자율형 사물인터넷(IoT)을 통한 데이터 센싱이고 크롤링, 오픈API(Application ProgrammingInterface) 등 데이터수집 기술 활용 및

데이터 수집·연계·통합을 통한 Customer360°확보다. 이때 비즈니스 고려사항으로 데이터로 해결할 비즈니스 이슈를 우선 정의, 비용과 효용을 고려해 데이터 수집 대상과 주기, 활용 기술을 선정, 데이터의 양적·질적 측면을 고려해 데이터 품질관리 강화가 있다.

둘째, 데이터 처리로 기술·기법은 실시간 데이터 처리를 위한 엣지 컴퓨팅과 오토 레이블링으로 데이터 처리 간소화, 암호기반 프라이버시 보호 기술로 데이터 비식별화이다. 이때 비즈니스 고려사항으로는 데이터의 상태를 확인하고 설계한 분석 요건에 맞도록 데이터 정제, IT 부서의 개입 없이도 현업담당자가 직접 데이터 처리를 할 수 있도록 데이터 전처리 간소화 도구 활용이 있다.

셋째, 데이터 저장의 기술, 기법은 클라우드 플랫폼을 통한 혁신 환경 구축과 데이터 웨어하우스에서 데이터 레이크(Data Lake) 그리고 RDB(Relational Database)에서 그래프 DB까지, 데이터베이스의 진화를 이끌었다. 이때 비즈니스 고려사항으로는 총 소유비용(TCO)을 고려한 클라우드 마이그레이션 여정 설계, 데이터 계층화를 통한 데이터 생명 주기 관리, 기업의 성격에 맞는 저장플랫폼 선정이 있다.

넷째, 데이터 활용의 기술, 기법은 자체적인 데이터 플랫폼 구축, 서드파티(Third-Party) 데이터 플랫폼 도입, 생태계 기반의 디지털 트윈 아키텍처 구축이 있다. 이때 비즈니스 고려사항으로는 조직의 비즈니스 목표에 대한 명확한 이해 필요, 고객의 니즈를 적극적으로 고려, 소규모 팀과 업무 단위로 데이터 활용 추진이 있다.

다섯째, 데이터 분석의 기술, 기법은 의사결정의 근간이 되는 기술 분석 및 진단 분석, 경영 활동의 불확실성을 낮추는 예측분석, 경험과 학습을 통해 진화하는 분석이 있다. 이때 비즈니스 고려사항으로는 사후적 분석에서 사전적 분석으로 진화하는 이행 로드맵 설계, 사업 목표와 일원화된 분석 프로세스 정립이 있다.

2) 데이터 기반 의사결정 프로세스 정립

데이터 기반의 의사결정 프로세스는 일반적으로 데이터 과학, 데이터 정책, 비즈니스 프레임워크, 비전의 네 가지 단계로 구성된다. 1단계(데이터 과학) 단계에서 수집된 데이터와 분석된 결과는 기업의 데이터 정책하에서 관리·운영되며, 비즈니스 프레임워크 단계에서는 기획자, 마케터 등 여러 이해관계자들과 커뮤니케이션 과정을 거치게 된다. 이 단계에서 의사결정자는 전략적 우선순위와 기술적 우선순위를 고려하여 비전에 부합하는 의사결정을 내린다. 데이터 기반의 의사결정 프로세스에서 고려할 사항은 크게 세 가지로 정리할 수 있다. 첫째, 기업의 비즈니스 목표에 대하여 명확히 이해해야 한다(그림 23의 'A'부분). 기업에서 데이터 자원을 활용하는 이유는 궁극적으로 조직의 목표를 달성

하기 위해서이다. 일부 기업의 경우 충분한 검토 없이 사내 데이터 사이언스 도입을 추진하여 미미한 성과를 거두는 데 그치기도 했다. 둘째, 고객의 입장에서 생각해야 한다(그림 23의 'B' 부분). 수익 창출의 원천인 고객에 대한 깊은 고민을 바탕으로 데이터 사이언스 전략을 추진해 나가야 한다. 단순히 업무에 데이터 사이언스를 도입하는 것만으로는 큰 의미가 없기 때문이다. 셋째, 처음에는 소규모 팀과 업무 단위로 데이터 활용을 추진해야 한다(그림 23의 'C' 부분). 기업이 처음 데이터 사이언스를 도입하고자 할 때 가장 어려운 점은 어디서부터 시작해야 할지 모른다는 점이다. 이런 경우, 가장 작은 업무로부터 적용 범위를 점차 넓혀 나가는 것이 중요하다.



〈그림 23〉 데이터 기반 의사결정 프로세스

2. 경영 분야

1) 재무관리

재무관리는 기업 활동과 관련하여 자금을 운영 및 관리하는 것이다. 즉, 자금의 조달과 운용에 관한 전반적인 활동에 관한 것으로 재무관리의 범위는 재무계획과 재무통제이다. 재무관리 빅데이터 사업관리 전략으로 재무 빅데이터 절차는 회계데이터 발생 ⇨ 회계 보고서 작성 ⇨ 재무정보 발생 ⇨ 재무계획 및 통제로 구분할 수 있다. 재무정보를 토대로 이루어지는 재무 빅데이터는 기업의 기업 여신 분석, 경영분석과 현금흐름 분석 등을 통한 의사결정을 위하여 실시된다. 의사결정 목적에 따라 의사결정자는 재무 정보를 근거하여 이익계획, 유형별 비용 투자를 분석한 재무정보가 의사결정자에게 제공하고, 수익계획

등의 재무계획 및 예산편성 등 재무통제 활동을 추진한다. 재무정보 유형으로는 첫째, 성장성이다. 기업의 미래가치를 측정하기 위하여 매출액 증가율, 총자산 증가율 등을 측정하며, 수익계획 수립을 위해 활용이다. 둘째, 활동성이다. 총자산의 회전을, 자기자본의 회전을, 재고자산의 회전을, 매출채권의 회전을 등은 기업자산이 얼마나 효과적으로 사용되고 있는가를 측정한다. 셋째, 수익성이다. 기업의 이익 여부를 판단하기 위하여 총 자본의 이익률, 자본의 이익률, 총 매출액에서 총 이익률 등을 측정하는 것이다. 넷째, 안정성이다. 기업의 재무상태가 건전한지 측정하기 위한 당좌비율, 유동비율, 이자보상비율, 고정비율, 차입금의존도 등을 측정하여 기업 자금계획을 수립하고 금융기관 여신계획 반영에 대한 의사결정을 한다. 재무부서는 차이 분석, 이윤, 시나리오의 모델링, What-if 분석과 같은 작업을 통한 매출원, 현금 유동성 및 재무성과에 영향을 미치는 변수를 분석하여 의사결정자의 통찰력을 획득 및 지원한다.

2) 인적자원

인적정보는 인적자원에 대하여 계획을 수립하고 인력의 수급을 활용·조정하며, 조직원의 능력을 개발하는데 필요한 정보다. 인사 분야와 관련된 정보 대부분이 여기에 해당 되고 외부에서 생성된 정보보다 내부에서 생성된 내부정보가 많고 보안이 요구되는 개인신상 정보가 많은 것이 특징이다. 인적자원관리는 인적자원을 효과적, 능률적으로 관리하는데 필요한 각종 정보다. 즉, 인적정보를 체계적으로 입수, 가공, 활용하는 과정과 함께 이를 활용하여 인적자원계획을 수립하는 일련의 활동이다. 인적자원 빅데이터 사업관리 전략으로는 분석·처리된 인적자원 정보는 기업전략에 따라 인적자원계획 수립하기 위한 빅데이터 활동으로 이어진다. 이를 통한 효과를 보면 비용 절감 전략에 따라 인적자원계획은 임금삭감, 연봉 재협상, 해고가 있으며 성장전략에 따른 인적자원계획은 채용 확대, 임금 인상, 합병전략, 교육 강화가 있다.

빅데이터 분석도구를 활용을 위한 기업 내부 데이터로 인사업무에서 인사관리, 조직관리, 복리후생 관리, 급여관리, 교육훈련관리, 노사관리, 채용관리 등으로 구성된다. 조직의 구성원 관리는 경영목표에 적합한 조직의 형태를 결정하고 관리하는 것으로 분업화 및 부문화 권한위양 등을 통해 의사결정을 하게 되며 부문별 이력 데이터로는 직급, 호봉 테이블 등이 있다. 인사관리는 근무 관리, 조직원에 대한 신상 등으로 하는 승급관리, 상벌 관리, 경력관리, 이직 관리 등이 있다. 데이터로는 조직원 정보, 조직원 이력, 인사 기록 카드, 인사발령 이력 등이 있다. 급여관리 조직원에 대한 보상을 관리하는 것으로 임금 결정, 보험관리, 기본급 및 성과급 관리 등이 있고, 데이터로는 연장근무, 4대 보험,

급여, 상여금 데이터 등이 있다. 채용관리는 소요 인원을 효율적으로 모집하고 선발하여 해당 부서에 배치하는 일련의 과정으로 선발관리, 배치관리, 직무관리, 모집관리로 나누어 축적되고 활용된다. 데이터로는 조직원 정보, 이력서, 연봉 및 직급 테이블 등이 있다. 노사관리는 영자와 종업원 사이의 문제, 노동조합의 법적 지위 문제, 경상사와 부하관계, 노동자와 사용자의 법률적 문제 등을 조율하고 관리하는 것으로 그 구체적인 활동으로는 협약, 교섭, 양자간 협의 등이 있다. 데이터로는 탄원서, 노동조합정보, 법률문서, 계약서, 파업 이력, 교섭 이력 등이 있다. 또한 교육훈련 관리는 신규 구성원 및 기존 구성원들의 교육과 훈련에 관한 각종 프로그램을 개발하고 실행하는 활동을 말하는 것으로 교육 훈련의 내용, 방법, 대상, 장소 등에 따라 데이터가 축적되고 활용되는데, 시험 결과, 승진 이력, 성과평가, 교육 참가 이력 등이 있다.

3) 마케팅 분야

마케팅 빅데이터 사업관리 전략은 비즈니스의 당면 이슈를 기업 내·외부데이터의 수학적·통계적인 분석에 이용하여 분석하는 의사결정 분석틀이다. 전술적, 전략적, 운영적 비즈니스 의사결정 문제를 데이터 분석 역량인 수학적·통계적, 전문적 지식, 데이터 프로그래밍을 통해 해결하려는 분석틀이자 강력한 해결책이다. 빅데이터와 결합하여 마케팅 실적을 적절히 평가함으로써 고객들의 니즈, 시장 트렌드, 구매습관에 대한 통찰을 얻고, 증거 기반의 마케팅에 대해 결정하는데 도움을 받기 위함이다. 차별화된 경쟁력을 확보하여 성장을 위한 기반이 된다. 마케팅 빅데이터를 활용하여 고객에 대한 정보를 관리함으로써 장기 충성 고객을 확보하는 방안 모색 등 맞춤형 서비스를 제공할 수 있다. 또한, 쿠폰을 발행하는 등 타겟 마케팅을 통한 수익창출과 빅데이터 활용을 기반하여 가격할인 및 프로모션의 의사결정을 하며, 콘텐츠 개발분야에서도 활용 가능하다. 빅데이터 분석도구를 통해 개인의 취향과 성향에 맞는 맞춤형 콘텐츠 제공 또는 사용자에게 호감을 얻을 수 있는 콘텐츠 노출 기회 제공 및 개발에 활용된다. 물류기업들도 빅데이터를 도입하여 실시간 지리적 환경적 요소, 수신자의 상황, 교통상황을 고려해 최적화된 배송경로를 실시간으로 제공하여 배송 지연 및 실패율을 낮추고, 불필요한 비용을 줄일 수 있다.

고객 정보 획득을 구분하면 업무상 데이터로 서비스를 제공하는 동안 필요한 제공된 기초 데이터(생일, 주소정보, 이메일, 성별)가 있다. 그리고 신체 데이터 정보를 직접적으로 획득이 어려우나 제품을 구매한 이력을 통해 예측할 수 있다(몸무게, 신장, 신체 사이즈 등). 또한, 보안데이터로 업무처리 과정에서 자연스럽게 획득되지만 외부 노출은 사고 발생 염려가 있어서 철저히 관리해야 할 데이터(핸드폰 번호, 신용카드번호, 예측한

소득 수준)가 있다. 마지막으로 개인 상세 데이터는 개인의 동의를 통해 획득 가능하지만, 국내에서는 잘 다루어지지 않는다.

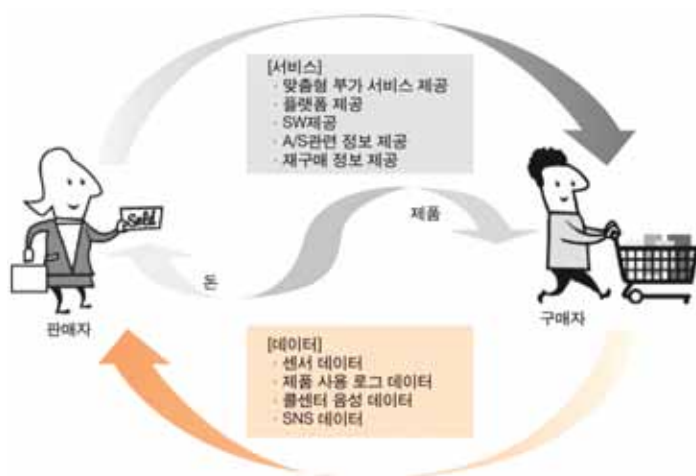
빅데이터를 통한 마케팅 효과 측정에서는 마케팅 성과증대 및 다양한 원천으로부터 나온 데이터를 결합하여 관계를 도출, 예측, 개별 고객 수준의 데이터연결, 채널간의 속성과 상호작용의 측정, 데이터 정확도와 품질개선이 있다.

3. 제조 및 서비스 분야

1) 제조 및 서비스 분야

시장 경쟁 격화에 따라 수익성 악화 및 고객 니즈의 다양성 증가로 인한 제조업에서의 빅데이터 분석도구 활용은 필수적이다. 제조업의 서비스화란 제조업에서 서비스의 역할이 증대되면서 점차 제조업과 서비스업의 구분이 모호해 지고 있다. 제조업의 서비스화 추세에 따라 고객은 순수 제품 자체보다도 제품이 갖고 있는 ‘기능’에서 만족을 느낀다. 이에 따라 제조업에서도 서비스가 중시되던 고객 관계 관리와 고객 맞춤화와 같은 개념들이 중요해지고 있다. 고가의 전자기기, 자동차 등의 제품의 경우 그동안 긴 구매주기로 인해서 고객이 관리 대상이 아닌 것으로 생각되어 왔지만, 점차 부가서비스를 판매할 수 있고 A/S를 제공해야 하는 관리 고객으로 변화했다. 즉, 공급자 중심에서 수요자 중심으로 시장의 판도가 변화하면서 제품의 생산 및 판매에 있어 고객 개인의 취향을 반영한 디자인과 설계 등이 시도 되고 있다. 빅데이터 분석도구를 통해 고객 정보 수집, 분석, 활용은 고객 관계 관리와 고객 맞춤화 서비스를 가능케 하는 제조업의 서비스화를 실현함에 있어서 큰 촉진 및 기여를 할 수 있다.

빅데이터 분석도구를 활용한 맞춤형 서비스 제공 전략과 유형은 그림 24와 같이 정리할 수 있다. 제품을 일회로만 판매하는 데에 그치지 않고 제품에 장착된 센싱과 임베디드 소프트웨어 등을 통해 지속 수집되는 데이터를 분석하여 고객이 필요한 맞는 맞춤 제품 및 서비스 제공이다. 첫 번째는 빅데이터를 활용한 연구개발 및 맞춤형 신제품을 개발하는 것이다. 제품에 부착된 센서와 임베디드 소프트웨어 등을 통해 수집된 데이터를 통해 고객의 습관 및 행동을 면밀하게 조사하여 기존 제품의 단점을 보완하여 신제품을 개인 맞춤형으로 설계에 이용하는 것은 물론, 개인으로부터 수집된 데이터의 분석을 통해 개인에 최적의 맞춤형 제품 설계까지 가능하다. 이 경우 제공되는 것은 서비스가 아닌 제품 자체이지만 고객의 행동을 면밀히 분석한 맞춤형 제품 제공이라는 측면에서 고객에게 전달되는 것은 단순한 하드웨어 이상의 가치라는 점에서 제조업의 서비스화가 이에 해당 된다.



〈그림 24〉 제조 / 생산분야 빅데이터 활용

두 번째는 빅데이터를 활용한 콘텐츠 개발 분야이다. 제품과 관련된 콘텐츠 플랫폼을 제공하여 생태계를 구성하는 것이 중요하다는 것은 이미 iTunes의 성공을 통해 널리 알려진 사실이다. 제조업은 플랫폼 제공에서 더 나아가 소비자의 제품 로그 분석 및 SNS 분석 등을 통해 플랫폼에서 유통되는 콘텐츠를 분석하여 콘텐츠 개발에 필요한 정보를 수집해야 한다. 삼성전자는 플랫폼에서 콘텐츠 거래의 활성화를 위하여 사용자 로그 분석을 통한 콘텐츠 이용 위치정보, 패턴과 선호도 등 파악하여 개발자들의 신규 콘텐츠 유통 모델 개발을 돕고자 다양한 사용자 정보를 오픈 API로 구성하여 외부 개발자들에게 공개하고 있다.

세 번째는 빅데이터 소프트웨어를 통한 부가서비스 제공이다. 제품과 함께 제공된 소프트웨어는 하드웨어의 작동에서 나오는 데이터를 분석하여 하드웨어의 기능을 개선하기도 하고 하드웨어를 사용하는 사람의 습관과 동작을 분석하여 피드백을 제공함으로써 하드웨어를 효율적으로 활용할 수 있는 방법을 제시했다. 제너럴 일렉트릭은 기 판매한 제트 엔진의 연료 효율성을 높게 하기위해 소프트웨어를 소비자인 항공사 측에 제공이 소프트웨어는 센서에서 수집되는 엔진의 작동 데이터에 패턴을 분석 및 적용하여 항공기 엔진을 지속적으로 관리하는데 도와줌으로써 연료의 효율성을 향상시켰으며 항공사가 매년 2천억 달러를 연료 구매에 지출한다는 사실을 감안하면 1%만 절약해도 약 20억 달러 절약이 가능하게 만들었다.

네 번째는 빅데이터를 통한 고도의 A/S 제공이다. 예를 들어 자동차에 부착된 센서 및 각종 기기들로부터 수집된 정보가 차 수리가 필요한 시점과 가까운 수리점의 위치

및 수리 점에 비치된 부품 사용 가능성 여부를 알려준다면 이를 통하여 사전 수리를 해 준다는 시점에서의 고장을 방지한다. 제너럴일렉트릭은 비행기가 착륙을 하는 시점에 제트 엔진이 SNS를 통해서 지상의 엔지니어들에게 알람을 울려 줄 뿐 아니라, 사람과 마찬가지로 상태를 지속적으로 업데이트 해 줌으로써 어떤 문제를 겪고 있는지 확인 및 바로 수리를 진행할 수 있도록 돕고 있다. 닛산 자동차는 전기자동차 ‘리프’로부터 주행 데이터 또는 충전지의 정보를 수집, 분석하여 자동차의 불편을 조기에 감지할 수 있는 서비스를 제공한다. 이를 통한 신속 대응으로 제품과 관련한 소셜 네트워크 분석과 콜센터 데이터 분석 등을 통하여 제품을 구입한 고객들이 어떤 문제들을 겪고 있는지 사전에 포착한 후 신속한 후속 조치를 이끌었다. 제너럴일렉트릭은 빅데이터 분석 도구를 활용하여 차량의 이상 유무를 원격 모니터링하고, 이상 발생 시 신속하게 리콜에 대응한다. 또한 수집된 누적 데이터를 활용하여 소비자에게 판매된 제품의 고장으로 수리를 받게 되다면 A/S센터에서는 고장의 원인이 무엇인지 확인하고 본사에서는 전 세계 A/S센터에서 수집된 고장 원인에 대한 보고서를 통하여 가장 자주 일어나는 고장의 원인을 확인하고 필요 부품에 주문량을 조절할 수 있게 되었다.

다섯 번째는 재구매 정보 제공이다. 소비자가 구매한 제품 수명이 다해 갈 때 제품 수명주기와 제품 고장 로그 등을 통하여 빅데이터 분석도구로 미리 예측 및 제품 교체 시점을 고려 미리 마케팅하고 고객 선점을 도모할 수 있다.

V. 정책적 제언

1. 실행과 적용

기업은 아직 빅데이터와 기업의 사업관리 영역을 별개로 여기고 있어서 빅데이터 분석 도구를 대다수 기업이 활용하지 못하고 있다. 물론, 본 보고서의 사례를 통해 과거 대비 특정 기업에서는 빅데이터 분석도구를 활용하고 있다. 이유는 빅데이터 분석 도구를 기술 집약적으로만 보고 있기 때문이다. 오히려 변화하는 기업 환경에서의 생존 전략으로 해석하는 것이 타당하다고 본다. 기업이 수집된 데이터를 통해 경쟁력을 확보하여 사업관리의 정확성을 증대시키기 위한 필수 요소이기 때문이다. 일반적으로 기업은 신기술의 도입에만 집중한다면 데이터에 숨겨진 가치를 찾지 못하고 있다. 아직 빅데이터를 전사적으로 도입하지 못한 기업은 단순 데이터 활용 작업부터 실행해보는 편이 바람직하다 보여진다. 기초적인 기술의 적용부터 시작해서 사업관리에 적용하여 성공적인 활용 사례를 만들고,

점차 이를 시스템화해 나가는 편이 효과적이다. 이러한 방법은 기업이 데이터 활용 사례를 학습하면서 목적에 부합한 데이터 활용 체계를 갖추기 용이하기 때문이다.

2. 데이터의 언어로 소통하는 조직 문화

변화하는 시장의 형세와 빠른 기술발전은 기업이 빅데이터 기반 사고방식을 활용하도록 요구하고 있다. 과거에는 경영자에 의한 통찰과 감각이 기업 의사결정의 가장 중요한 요소였지만, 현재는 객관적인 사실과 현상으로부터 도출되는 패턴에 대한 신속한 대응이 중요해지고 있다. 이는 기업의 특정 계층에 국한되는 이야기가 아니다. 재무팀의 매니저, 고객과 대면하는 영업팀 사원, R&D 부서의 연구원에 이르기까지 전사적으로 데이터 언어에 익숙해질 필요가 있다. 즉, 모든 직원이 업무를 수행하면서 축적되는 데이터를 처리, 분석하여 새로운 통찰력을 창출할 수 있는 기초 체력을 갖추어야 한다. 이러한 기초 체력으로 데이터 분석 역량이 필수적이며, 데이터 분석 툴에 대한 교육과 전파하는 커뮤니티가 필요하다. 더 나아가, 기업 내에서 데이터 언어로 소통하고 온톨로지 적으로 쌓은 데이터를 갖고 작은 실험을 반복하며 빠르게 혁신하는 데브옵스(DevOps) 문화 또한 마련 되어야 한다. 조직이나 개인의 주관적인 의견이 아니라, 객관적인 사실과 해석을 기반으로 소통하는 기업만이 새로운 데이터의 시대에서 생존할 수 있을 것이다.

3. 데이터 사이언스 솔루션 도입

최근 클라우드 환경의 보편화로 SaaS, PaaS 환경에서 도입할 수 있는 데이터 사이언스 솔루션이 증가하고 있다. 마이크로소프트, 아마존 등의 클라우드 사업자는 대규모의 스토리지를 제공하는 동시에, 각사의 마켓플레이스(Marketplace)에서 다양한 기법으로 빅데이터를 분석할 수 있는 서드파티 애플리케이션을 제공하고 있다. 이러한 애플리케이션의 활용은 데이터 사이언스 시스템을 구축하는 시간과 비용을 줄여주고, 점차 증가하는 데이터량에 대응할 수 있는 확장성을 제공한다. 클라우드 환경으로 이행하지 않은 기업의 경우에도, 다수의 서드파티 데이터 사이언스 솔루션을 활용할 수 있다. 시장에서 각종 데이터베이스 소프트웨어, 애널리틱스 도구가 출시되고 있는 상황이다. 목적과 예산에 맞게 적절한 데이터 사이언스 솔루션을 구입하여 사용하는 것도 기업이 취할 수 있는 전략의 하나로 볼 수 있다. 외부 솔루션 도입 과정에서 기업은 데이터 분석을 위해 투자한 비용 대비 산출한 성과를 측정할 수 있는 지표를 함께 검토해야 한다. ROI(Return on Investment)에 대한 심사숙고 없이는 효과적인 데이터 전략이 지속적으로 추진되기 어렵기

때문이다.

4. 데이터의 가치를 극대화 하기 위한 데이터 연결성

기업은 고객 데이터를 효과적으로 센싱하고 이를 기업 내부 데이터와 연결 할 경우 데이터의 가치를 증폭시킬 수 있다. 기업은 데이터 자원을 수집하고 처리, 저장, 분석하는 목적은 고객 중심으로 디지털 혁신하기 위함이다. 조직을 고객 데이터 중심으로 연결 되도록 재설계하고 기업의 각기 다른 기능과 프로세스 통합관리한다면 밸류체인 전반의 가시성이나 투명성을 제고할 수 있다. 더 나아가 제품과 서비스 혁신, 그리고 새로운 비즈니스 기회를 발굴할 수 있다.

5. 중소기업 빅데이터 활용 지원⁸⁾

중소기업의 빅데이터 활용 지원을 위하여 정부 또는 민간 차원의 노력이 지속 필요하다. 아마존은 시장에서 판매되고 있는 자체 구축 서비스에서 빅데이터 웨어하우스와 BI 솔루션을 중소기업이 구입하기에는 고가이다. 전통적으로 데이터 웨어하우스의 약 10% 정도의 비용으로 페타바이트급 데이터를 쉽고 빠르게 분석할 수 있게 하는 레드시프트(Redshift)가 있다. 물론, 국내에서 이를 지원하기 위해 SK텔레콤의 빅데이터 분석엔진인 T-MapReduce를 중소 IT기업인 T클라우드 비즈니스 사용자들에게 시범 서비스 형태로 무료 제공했다. 또한 한국생산기술연구원은 중소기업과 중견기업 제조업에 적용할 수 있는 빅데이터 솔루션인 '아이오피스(i-OPIS)'를 개발해 선보였다. 중소기업청 역시, 소상공인과 전통시장 지원을 위하여 2014년부터 신용카드 정보 및 상가 인허가 정보 등 약 7억 건의 빅데이터를 분석하여 업종별 매출 전망 및 추이, 임대시세 등의 정보를 제공하는 서비스를 강화하기로 했다. 그럼에도 불구하고 국내 중소기업에서 빅데이터의 활용 건은 미미한 것이 사실이다. 국내 중소기업을 대상으로 진행한 빅데이터 지원 수요조사에서 벤처기업 10곳 중 7곳이 요청했다. 이유는 고가의 분석 인프라, 데이터 셋(SET) 확보가 어렵기 때문이었다. 중소기업은 규모 및 유연성을 고려하여 대기업과는 다른 분야에서의 빅데이터 자료에 대한 니즈를 가지고 있었으며, 이를 충족시켜 줄 수 있는 솔루션을 개발하는 기업에게 인센티브를 주고 확보한다면 중소기업에게 배포 할 수 있을 것이다. 중소기업의 경우 축적된 데이터가 대기업에 턱없이 부족할 수 있으며 이는 공공데이터 개방 사업과 연계하여 일정 수준까지 보완해 줄 필요가 있다.

8) 이훈해, '제조업 경쟁력 강화를 위한 빅데이터 활용 방안' 산업연구원, 2013.

〈참고 문헌〉

- <https://www.samsungsds.com/kr> 202010.01 검색 및 참조
- 과학기술정보통신부, '2018년 데이터 산업 현황조사', 2018.
- 과학기술정보통신부, '2019년 데이터 산업 현황조사', 2019.
- 김기범 외 2명, '기업 운영 혁신을 위한 데이터 과학: 기업의 활용 방안', 삼성, 2020.03.
- 마켓츠 앤 마켓츠, '세계의 빅데이터 시장', Globalinforesarch, 2018.09
- 박영길, '국방분야 빅데이터 활용의 선결 과제와 유의점 검토', 국방연구원, 2018.
- 송민정, '빅데이터를 활용한 비즈니스모델 혁신', KT경제경영연구소, 2013
- 유한석, '빅데이터 비즈니스의 이슈와 전망', DIGIECO, 2012.06.
- 이상현, '빅데이터 기반 자동차 부품산업 스마트팩토리 구축 사례', 유라, 2019.10.
- 이훈혜, '제조업 경쟁력 강화를 위한 빅데이터 활용 방안' 산업연구원, 2013.
- 정해식, '빅데이터를 활용한 기업의 경쟁우위 확보 사례', 정보통신산업진흥원, 2013.
- 최종명 외 2명, '빅데이터 기술 및 응용 특집', 한국스마트미디어학회지, 2013.09.
- 최윤정 외 3명, '빅데이터를 활용한 벤처 중소기업 글로벌 기술사업화 지원모델 개발', 한국과학기술정보연구원, 2014.
- 최지영, '빅데이터 분석 솔루션', 한국IR협의회, 2019.11.17. 참조

인공지능 기술의 국방분야 적용방안 연구

건양대학교 교수 **최 명 진**
호원대학교 겸임교수 **심 행 근**

- I. 서론
- II. 문헌연구 / 시사점
- III. 국내·외 인공지능 시스템을 활용한 모범사례 분석
- IV. 인공지능 기술분야별 활용방안 식별 및 과제도출
- V. 정책적 시사점 및 발전방향
- VI. 결론

요 약

1. 인공지능(AI) 관련 문헌연구 / 시사점

- 미래의 국방 분야에서 무인 무기체계는 무인 항공기(드론 등), 자율주행 자동차, 로봇 등은 더욱 많이 활용될 것이며, 이 무기체계를 총괄 제어하기 위해서는 사람과 같이 인식하고 판단할 수 있는 인공지능(AI)이라는 핵심기술이 필요함
- 모든 사물이 연결되는 사물인터넷(IoT) 환경은 다양한 분야에서 활용될 수 있으나, 보안의 취약점이나 외부의 공격에 노출됨
- 국방 분야의 특성상 보안 취약점으로 인한 정보유출은 막대한 피해와 인명손실을 야기할 수 있기 때문에 국방 분야의 사물인터넷(IoT) 기술 도입은 더욱 신중하게 접근해야 하며, 이를 위한 보안체계가 새롭게 구축되어야 함
- 국방 분야에서 사물인터넷(IoT) 기술을 도입하기 위해서는 『저사양의 사물인터넷

(IoT) 기기에서 활용하기 위한 경량·고속 암호 모듈 기술, 사물인터넷(IoT) 기기의 유출, 불법 포획으로 인한 내부 해킹을 방지하는 암호키 은닉 및 원격 데이터 삭제 기술, 식별되지 않은 디바이스의 접근이나 비인가 사용자의 접근 차단 기술 등 디바이스 측면의 보안뿐만 아니라 비인가 무선랜 장비에 의한 위협을 방지하기 위한 무선랜 보안기술, 기존의 업무망과 사물인터넷(IoT)망의 분리 운영을 위한 연계구간 설정 및 보호기술, 사물인터넷(IoT) 기기로부터 전송된 정보를 안전하게 보호할 수 있는 암호화 및 메시지 무결성 검증 기술, 사물인터넷(IoT) 기기나 네트워크의 트래픽 모니터링 및 분석을 통해 악성코드나 해킹 등의 이상 징후를 탐지하고, 실시간으로 대응할 수 있는 침입탐지 대응기술 등 다양한 측면의 보안기술들도 연구개발을 통해 보안성을 필수적으로 확보해야 함

- 4차 산업혁명 시대 핵심 기술인 AICBM(IoT, Cloud, Big Data, Mobile) 기반의 스마트 부대 구축을 통해 첨단과학기술 군으로 탈바꿈하여 한계를 넘어서는 초일류 육군 건설, 표준화된 시스템 기반으로 체계적인 대응과 신속하고 신뢰성 있는 서비스 제공 가능, 효율적 부대 운영을 통한 장병 삶의 가치 향상, ICT/IoT 및 빅데이터 분석의 신기술을 부대 운영 전반에 적용함으로써 사람 중심의 부대 운영과 각종 문제(안전사고 예방, 화재예방 등) 해결로 쾌적한 병영문화 조성이 가능할 것으로 판단됨
- 사물인터넷(IoT) 기반의 스마트 부대관리는 먼 시점의 이야기가 아니며 현재 연구 추진 예정인 사항에 대해서 지속적으로 추진한다면 조기에 구현이 될 것으로 확신 하며, 부대관리 측면에서 사물인터넷(IoT)을 적용한다면 예상되는 기대효과 다음과 같음
 - 첫째, 국방 자원관리에 창조적, 혁신적 사물인터넷(IoT) 서비스 적용시 부대관리에 획기적 변화가 예상되며, 병력, 총기관리 실시간대 파악으로 사고예방에 크게 기여할 것으로 판단됨
 - 둘째, 인명사고 및 차량사고 감소로 지휘부담 경감과 차량, 장비 정비수요 예측 및 적기 예방정비 가능으로 유지보수비용 절감으로 국방개혁 2.0과 연계된 부대관리 개선으로 대군 신뢰 증진에 기여할 것으로 기대됨
 - 셋째, 직접적인 자료수집 방식인 사물인터넷(IoT)와 빅데이터 분석으로부터 스마트 부대관리 구축을 통해 스마트 육군 건설과 국방개혁 2.0의 성공적인 추진 여건을 보장하여 육군의 체질 개선 및 정예화가 가능할 것으로 판단됨
- 안정적인 서비스와 다양한 사용자 맞춤형 서비스 제공 등으로 장병 만족도·신뢰도 향상될 것으로 기대됨

2. 국내·외 인공지능 시스템을 활용한 모범사례 분석

- 민간에서의 활용 중인 인공지능(AI)에 대한 기술은 웨어러블(Wearable) 로봇, 왓슨(Watson) 등 의료, 무인 주행차량 등에서 빠르게 성장하고 있는 추세이며, 인공지능(AI)은 미래 산업의 총아(寵兒)로 4차 산업혁명을 주도 할 것으로 예상됨
- 파괴적 상용기술(AI+ICBM)을 국방에 적용하기 위한 연구개발 및 발전은 우리나라에만 국한된 것이 아니라 미국을 비롯한 일본, 중국 및 세계 각국에서도 관심과 노력을 기울이고 있으며, 우리와 대립 관계에 있는 국가에서도 인공지능(AI)을 활용할 가능성이 매우 높다고 할 수 있음
- 우리나라의 경우 국방 분야에서 인공지능(AI) 활용을 위한 체계적인 연구개발은 아직 미흡한 실정이며, 현재 각 군에서는 미래혁신센터를 창설하고 지능정보사회 추진단과 연계된 사업을 통해 국방 분야 인공지능(AI)에 대한 사업계획을 수립하고 예산화하여 실증을 위해 추진하는 초기 단계에 있음
- 또한, 현재 법규와 제도 및 환경은 인공지능(AI)에 적용된 융합(복합)체계를 획득하는 절차를 지원하지 못할 뿐만 아니라 오히려 규제를 받는 상황이 발생하고 있어, 이에 대한 지속적인 관심과 개혁에 대한 노력이 필요함
- 인공지능(AI)의 기반이 되는 빅데이터 체계 축적 등에 대한 준비가 부족하며, 국방 인공지능(AI)을 활용하기 위한 산·학·연·군이 연계된 전문가 및 소요군 내 인재 양성이 미흡한 실정임
- 특히, 군 체계의 특성상 창조적 개념과 설계 역량이 뒤쳐질 수 있기 때문에 인재와 기술력에 대해 외부 위탁 등 보완 제도 도입이 요구됨
- 빅데이터를 활용한 혁신적인 사례들은 향후에도 지속적으로 많이 나올 것으로 예상되며, 미래에는 새로운 정보기술력인 빅데이터 속에서 발굴한 가치 있는 데이터들을 어떠한 방식으로 정리하고 활용하느냐에 따라 경쟁력이 결정지어질 것임
- 공공 및 민간분야 활용사례와 군에 적용할 수 있는 방안에 대해서 도출하면 다음과 같음
 - 빅데이터를 활용한 국방정보 분야의 각국 동향 예측 적용방안
 - 부대관리 측면에서 SNS 분석을 통한 CRM(Customer Relationship Management) 및 군 홍보분야 활용방안
 - 군 보급품 재고관리에서의 빅데이터 활용방안
- 빅데이터의 활용으로 우리의 국방 정보력은 더욱 강화될 것이고, 그동안 직관과

통찰력에 의존하여 부대를 관리해왔던 군 지휘관의 과학적인 부대 관리가 가능해질 것임

- 하지만 군의 특성상 빅데이터의 긍정적인 활용성과에도 불구하고 빅데이터 기술에 대한 활용만을 주장할 수는 없기 때문에 빅데이터 기술을 활용함에 앞서 군 조직의 특수성으로 인해 가볍게 여겨질 수 있는 개인정보 관리에 대한 확실한 지침을 마련하고, 빅데이터 수집 및 활용범위의 확대로 발생할 수 있는 정보제공 권한, 소유권 및 군사보안 문제에 대한 대비책이 철저히 마련되어야함
- 우리 군에서 활용 중인 빅데이터 기술 내용과 다양한 국가들의 빅데이터를 활용사례를 구체적으로 포함시키지 못했기 때문에 향후 주변국들의 다양한 빅데이터 기술 활용 사례들을 분석하여 빅데이터 기술에 대한 긍정적인 활용성과를 극대화하고 제도적 장치 및 보안 문제에 대한 해결방법 등의 지속적인 논의가 필요함
- 선진 과학화를 추구하는 우리 군이 빅데이터의 긍정적인 활용을 통해 발전 가능성을 더욱 증대시켜 가치 있는 미래 국가 수호의 초석으로 자리매김 할 수 있기를 기대함

3. 인공지능(AI) 기술분야별 활용방안 식별 및 과제 도출

- 국방부는 인공지능(AI) 중점 추진과제별 활용 가능한 분야 식별 및 과제를 도출하여, 인공지능(AI) 시스템을 적용하고자 하는 요구과제별 사업계획의 구체화 가능 분석하고 있음
- 현재 ‘인공지능(AI) 교관 개발’, ‘지능형 네트워크 트래픽 분석 및 조치 도구 개발’, ‘전투 조종사용 인공지능(AI) 시뮬레이터 개발’등 3개 과제에 대한 운용 개념과 이에 따른 적용 대상 인공지능(AI) 기술 등에 대한 구체화 및 연구개발을 진행 중에 있음
- 4차 산업혁명을 각 산업별 터줏대감들이 주도할 것으로 믿는 이유는 혁신의 원천이 ‘Data’와 ‘Operation 경험’이기 때문에 기존 군이 보유한 운용데이터 활용과 운용데이터의 접목과 활용이 필요하므로, 빠른 기술 변화로 Big-Bang식 추진보다는 Test & Learn을 통해 Use case를 점진적으로 혁신해 나가는 방법론을 채택해야 함
- 인공지능(AI)를 기술을 적용한 국방 분야 활용 방안은 다음과 같음
 - 챗봇의 활용사례로 인공지능(AI) 기술교범 체계를 개발하는 방안으로 실제 야전에서 발생된 정비/점검 데이터와 실제 야전 운용데이터를 빅데이터로 축적하고 운용한 데이터로 가공하여 정비서비스 챗봇에서 제공하여 지속적으로 현실적인 정비 가이드 서비스가 가능하도록 인공지능(AI) 기술교범체계를 개발하고 여기에 가상(증강)

현실 데이터를 합성하여 챗봇과 증강현실로 정비를 경험하도록 하는 서비스를 제공하는 방안

- C4I : 인공지능(AI) 기반의 실시간 M&S 및 위계임 체계, 지능형 지휘결심지원체계, 지능정보센터, 초연결·초지능 네트워크 등
 - 정보 : 지능형 사이버·전자전 공격/방호시스템, 지능형 군사정보관리체계(Smart MIMS) 등
 - 화력 : 인공지능(AI) 기술을 적용한 지능탄, 지능형 표적탐지 레이더, 지능형 사격 지휘통제체계 등
 - 기동 : 지능형 워리어 플랫폼, 인텔리전트 전투복, 인공지능(AI) 기반 자율 및 군집형 기동체계 등
 - 방호 : 지능형 사이버전 수행 기술개발, 지능형 과학화 경계시스템, 지능형 사이버 방호 시스템, 지휘시설 및 무기체계의 지능형 방호체계 등
 - 작전지속지원 : 인공지능(AI) 교관, 지능형 합성전장훈련체계(LVCG), KCTC와 연계한 AI기반의 지휘결심지원체계, 인공지능(AI)기반의 훈련 시뮬레이터/전장훈련 체계, 정비수요예측시스템/탄약 저장관리체계, 지능형 안전관리 정보체계/원격치료 시스템, 지능형 물자보충/재고 관리체계, 인공지능(AI) 기반의 인력획득 및 인사 관리체계 등
- 인공지능(AI)을 적용하여, 현시점 기준으로 사업화 및 구체화 가능성은 다음과 같음
 - 의료 흉부진단 : 대학병원과의 연구 경험을 노하우로 군에 최적화된 시스템을 위한 진단 프로세스를 개발하기 위해 ‘국방의료정보 빅데이터 분석체계 구축사업 연구용역’을 통해 흉부 엑스레이 영상 판독 지원시스템 부분의 연구용역을 진행함
 - 지능진화형 엑소브레인 : 자연어를 이해하여 지식을 자가 학습하며, 인간과 기계의 지식소통이 가능하도록 지식과 지능이 진화하는 것으로, 언어를 처리하며 판단 및 예측을 통해 문제해결방안에 대한 참모 판단을 대체하고, 의사결정을 지원하는 시스템 개발
 - 인공지능(AI) 아담 : 인간의 두뇌 분석을 통한 인공지능(AI)의 원천 기술로 인공지능(AI) 기술과 가상현실(VR), 증강현실(AR) 기술의 결합으로 발전된 사례이며, 유·무인 체계의 최적 이동경로 수립 및 원격지원, 임무수행 경로의 사전 검증에 활용이 가능함(유·무인 무기체계 편대들의 시각화된 원격 지휘 통제, 전장에서 전투 원격 지휘 통제, 최적 전략 및 작전 수립 지원, 가상전장 환경에서의 전투체험 및 전투지휘 연습 등)
 - 인공지능(AI) 비서 : 다국적군과의 작전 수행 시 실시간 언어통역 역할을 수행하고

무선 웨어러블 디바이스를 통해 원격지에 있는 병사들에게 작전임무 수행을 위한 정보지원 가능

- 소부대 몰입형 훈련시스템 : 훈련자가 모의이동시뮬레이터에서 충분한 체감 안정도를 유지할 수 있도록 실시간 정밀 제어 및 훈련자의 위치와 자세 인식, 분대급 전술 시뮬레이터 또는 상용 게임과의 연동을 통한 3D 가상현실 속의 객체들과 탐지, 교전 등의 상호작용 모의 가능

• 무기체계별 인공지능(AI)을 적용 가능한 분야는 다음과 같다.

- 기동분야(전차 / 장갑차 / 전투차량)
 - 화력 증대를 위해 인공지능(AI) 표적 추적 자동화, 유도화 지능탄 개발
 - 사격통제장치 분야의 인공지능(AI) 표적 자동 추적장치(포탑 구동장치와 연계)
 - 대전차 유도탄 방어를 위한 인공지능(AI) 방어체계(대전차 로켓 및 유도탄의 탐지, 추적, 요격)
 - 전차 탑재형 인공지능(AI) 무인조종 자동화기(열 감지 및 자동 추적 사격)
 - 기동성 향상을 위해 지형 조건에 따른 인공지능(AI)형 안정화 주행장치
 - 생존성 향상을 위해 자동으로 오염도 측정 및 전차 내부 밀폐, 공기 정화 기능 개발
- 개인전투체계
 - 자율표적획득장치 연구 : 음원 탐지 기반 적의 방향, 위치, 탐지정보 제공, 사격 원점 등 표적/인원 등의 자율탐지, 인식, 위치등록, 추적 및 공유
 - 자율상황인식, 의사결정 장치 연구 : 원시정보와 정보, 영상 기반의 자율인식정보 및 피아 작전 정보를 통합한 자율상황인식을 기반으로 인공지능(AI) 의사결정, 자율적, 반자율적 자산의 하무 임무에 할당
 - 계층별 자율상태인식 및 의사결정 : 인공지능(AI) 기반의 각 계대별 상태 인식과 임무분할, 할당, 수행의 계획과 실행 상태를 전시
 - Wearable 별 원시, 인식 정보 구분 및 활용
 - 다양한 전시 기능 지원 MMI
 - 지휘통제 체계화 : 전장정보 공유, 초소형 피아식별, 음성/데이터 통신
 - 화력 자동화: 사거리 증대, 이동표적 정밀타격, 초소형 미사일 장착 운용
- 화력분야(포병 / 대화력 / 탄약 / 화생방)
 - 사표 자동 산출을 위해 공기 밀도 측정 및 고도, 온도, 풍속 등에 따른 변화 자동 계산, 사표 산출 프로그램 및 장치
 - 화력 및 사거리 증대를 위해 인공지능(AI) 표적 추적 자동화, 유도화 지능탄 개발

- 기동성 향상을 위해 지형 조건에 따른 인공지능(AI) 안정화 주행장치
- 생존성 향상을 위해 자동으로 오염도 측정 및 전차 내부 밀폐, 공기 정화 기능 개발 여부
- 병커에서 원격조종 사격이 가능한 표적탐지, 추적, 자동 사격장치
- 병사의 안전을 위해 화기 자세에 따라 사격 가능 여부를 자동으로 제어하는 사격 안전장치
- 인공지능(AI) 교전 시스템 : 대테러전과 같은 근접전투에서 교전이 가능한 살상용 인공지능(AI) 교전체계
- 지능탄약 개발 활성화로 사거리 연장, 정밀 표적 타격
- 지휘통제·통신 분야
 - 인공지능(AI) 구현을 위한 빅데이터 분석 정보체계 구축 : 전투지휘훈련 빅데이터, 인공지능(AI) 기반 스마트 인재관리 시스템, 지능형 해안감시체계 구축을 위한 인공지능(AI) 학습모델 등
 - 인공지능(AI) 플랫폼 : 인공지능(AI) 및 인지 컴퓨팅 플랫폼 기반 의사 보조 시스템, 중요회의 의사결정 지원시스템, 자연어 이해 및 딥러닝(Deep Learning) 학습기능 등 다양한 인공지능(AI) 솔루션 개발 도구, 인공지능(AI) 전술계획 수립체계, 교리 연구 시스템 등
- 무인화
 - 전투원과의 협업 및 자율적인 임무수행으로 전투 효과를 극대화하기 위해 '전투 행위 분석 ⇒ 전장환경 Big Data 구축(야외훈련) ⇒ 알고리즘 학습(딥러닝, Deep Learning) ⇒ 인공지능(AI) 성능향상 ⇒ 추가 Big Data 소요도출(야외훈련 필요성 도출)'의 순환구조 분석시스템 개발
 - 인공지능(AI) 교전 전투 시뮬레이터, 하이브리드 형태의 자율순항체계, 무인 합동 훈련체계, 인공지능(AI) 전투기 조종사 등

4. 정책적 시사점 및 발전방향

- 인공지능(AI)을 적용한 무기체계 획득을 위한 제도개선
 - 현재 4차 산업혁명의 기술력을 보유한 업체들의 대부분이 중소기업체임을 고려할 때, 현재 시행되고 있는 방산물자지정제도는 민간업체에게 높은 진입장벽으로 작용할 가능성이 크기 때문에 무기체계 완제품 외에 세부 부품단위까지 방산물자로 지정하여 독과점적 지위를 보장하는 제도에 대해 완화할 필요가 있음

- 정부가 필요로 하는 4차 산업혁명 기술을 보유한 민간업체가 무기체계개발 또는 성능개량에 참여할 경우 자금지원 및 가점 인정 등이 고려되어야 함
 - 무기체계의 정비와 운영유지간 필요한 시스템 구축에 빅데이터 구축 등의 추진이 요구되며, 필요시 네이버, 다음 등 국내 관련 대형 업체와의 협력을 통해 시범사업 등을 추진하고 이를 통해, 군사보안에 관련된 현안 문제들을 해소하고 군 사이버 보안역량을 강화하는 중장기적인 대안 마련이 필요함
 - 4차 산업혁명 위원회 내 방위산업분과 신설을 위한 정부 차원의 거버넌스(Governance)가 필요함
 - 쌍방향 무기 소요제기 시스템을 구축하고 국내 방산업체와 4차 산업혁명 기술력을 보유한 민간업체를 조사하고 분석하여, 정부 주도 또는 정부와 기업간 매칭된 형태로 관련 사업들을 추진하는 것이 필요함
- 중장기적인 인력양성
 - 세계적으로 인공지능(AI) 인재확보를 위한 경쟁이 더욱 치열해질 것으로 예상되며, 인공지능(AI) 인재에 대한 수요에 비해 공급이 절대적으로 부족하여 수급 불균형에 따른 산업 생태계 혼란이 야기될 수 있기 때문에 우리나라에서도 국가 차원의 중장기적인 인력양성 방안 및 전략적 대응이 매우 필요한 시점임
 - 현재 소수 국가에만 인공지능(AI) 핵심인재(h-index 상위 10.0%)가 집중되어 있기 때문에 인공지능(AI) 격차 해소를 위해서는 석·박사급 고급 인력양성 체계 구축 및 질적인 고도화가 필요함. 향후 핵심인재가 많은 국가일수록 인공지능(AI) 전문가 양성 및 고용, 기술혁신의 주도권을 가질 것으로 예상되며, 그렇지 못한 국가와의 격차가 점차 심화될 것으로 전망됨
 - 과학기술정보통신부 주관 ‘인공지능(AI) 대학원’사업은 인공지능(AI) 시장을 선도할 세계적 수준의 인공지능(AI) 석·박사급 고급 인재를 양성할 것으로 예상되지만, 인공지능(AI) 대학원의 질적 고도화 및 성과 확산을 위해 체계적인 커리큘럼을 개발하고 HW·SW 인프라 확충, 실증적 교육 연구를 위한 협업 환경 구축, 전문 교원 확보, 글로벌 네트워크 활성화 등 추가적인 프로그램 추진이 반드시 필요함
 - 세계를 선도할 최고의 인공지능(AI) 인재로 성장할 수 있는 토양을 마련하기 위해 인공지능(AI)에 대한 사회적 수용성(Public Acceptance) 향상을 위한 교육을 확대하고 인공지능(AI) 지식을 습득하기 위한 STEM 교육 강화, 인공지능(AI) 비학위 프로그램 개설 및 기존 인공지능(AI) 인재의 재교육 등 사회 전반에서의 인공지능(AI) 활용 능력 제고를 위한 교육 프로그램 확충이 필요함

- 인공지능(AI) R&D 정책과 연계한 협의체 구성
 - ‘인공지능(AI) 전략 협의체’구성 및 운영을 통해 추진체계를 마련하여 인공지능(AI) R&D 전략 실행력 확보가 필요함
 - 협의체는 정부부처 공무원(실국장급)과 민간위원(산·학·연 전문가)으로 구성하며, 위원장은 과학기술정보통신부 2차관으로 하여 분야별 전략이 서로 연계 및 통합적으로 관리될 수 있도록 인공지능(AI) 전략 협의체의 하위 분과로는 기술·인재·기반 분과 운영이 필요함
 - 협의체는 중점 과제의 추진상황과 기술·정책 환경 변화에 따른 R&D 전략 및 목표를 재검점하고 기술·인재·기반 분야의 핵심과제에 대한 세부 추진전략을 마련하며 분기별로 1회 운영을 원칙으로 하되, 기술·인재·기반 분과별로 안전에 대한 수시 논의가 필요함
- 인공지능(AI) 플랫폼 구축
 - 물리적인 관점 : 인공지능(AI) 서비스 구축을 위해 해당 서비스에 대한 개발 자원 및 배포 자원(서버)의 통합적인 관리(버전 및 형상 관리), 딥러닝(Deep Learning) 등 개발 환경, 자원 모니터링 등의 기능을 제공
 - 활용 프로세스 관점 : 인공지능(AI) 서비스 구축에 필수적인 기계학습 과정은 일반적으로 ‘데이터 준비 → 교육(훈련) 데이터 생성 → 기계학습 모델 생성 및 훈련 → 검증’과 같은 단계를 거치므로 각 프로세스를 효과적으로 실행할 수 있는 인터페이스를 제공
 - 논리적 관점 : 기계학습에서 사용되는 다양한 알고리즘들을 내장하고 있는 기계학습 프레임 워크의 준비
 - 인공지능(AI) 플랫폼 도입 전략 수립을 위해 인공지능(AI) 플랫폼 도입의 필요성에 대해 데이터 부문, 서비스 부문, 엔지니어 부문, 조직 부문에 대해 체계적인 점검이 필요함

5. 결론

- 본 『인공지능(AI) 국방 분야 활용방안 연구』를 통해 제시된 방안들을 기반으로 과제화하여 창의적이고 도전적인 국방 R&D 연구를 추진할 수 있는 기회가 마련됨. 즉, 인공지능(AI) 관련 신개념, 신기술 아이디어를 국방에 적용하도록 관련 우수 인력을 영입하여 수행하는 개방형 연구로의 발전 가능성이 있음

- 또한, 미래 운용개념 개발과 신무기·신기술 융합을 위한 원천핵심기술 연구 가능성 (예산 확대 필요)을 보여 주었으며, 고난이도 연구개발에 대하여 창의적이고 도전적인 연구개발을 유도하는 기회를 제공함
- 기존의 무기체계에 인공지능(AI) 기술을 접목하는 방법으로의 발전을 통해 세부 분야별 지속적 발전이 가능한 국방 R&D 개발 근간 마련 기회를 제공함. 즉, 인공지능(AI) 관련 과제 연구 및 방안 제시를 통해 기존의 무기체계 성능개량을 유도하고 지속 발전 가능한 연구개발 선진화를 통해 최소 예산 투입만으로 국방력 향상에 기여에 기대되며, 인공지능(AI) 과제 발굴을 통하여 분야별 기술 진부화를 방지하는 최소 예산의 성능개량 연구 활성화가 기대됨
- 더불어, 개념연구 등 운용의 혁신과 빅데이터, 인공지능(AI), 만물인터넷(IOE) 등 기술 혁신을 동시에 지속적으로 추구할 수 있는 기회가 될 것으로 판단됨

I. 서론

1. 연구 배경 및 목표

가. 연구배경

인공지능(AI)이라는 용어는 4차 산업혁명의 핵심기술로서 1965년에 처음 등장하였으며, 최근 데이터의 양적 증가, 첨단 알고리즘, 컴퓨팅 파워와 스토리지의 개선으로 매우 활발히 연구되고 있는 분야이다. 이에 본 연구에서는 인공지능(AI) 기술의 중요성과 산업의 적용 사례 등 활용실태 분석, 인공지능(AI) 작동 방식 및 인공지능(AI) 시스템 분석을 통해 국방 분야에서의 적용방안을 제시하고자 한다.

또한, 막대한 예산을 사용하는 국방 분야에서 인공지능(AI) 기술을 활용한 시도가 많이 이루어지고 있지 않고 있어 이를 활용할 수 있는 방안을 제시하며, 더불어, 인공지능(AI) 기술 분야별 국방 분야의 활용방안 식별 및 과제 도출 등을 통해 기대효과를 분석하고, 국방 분야 인공지능(AI) 활성화를 위한 제도 및 정책개선 사항을 제시하고자 한다.

나. 연구목표

1) 인공지능(AI)의 개념 및 이론, 기술의 분류

- 가) 인공지능(AI)의 역사와 중요한 이유
- 나) 인공지능(AI)의 작동 방식
- 다) 인공지능(AI)의 활용 및 구현방안과 인공지능(AI) 기술분류

2) 국내·외 인공지능(AI) 시스템을 활용한 모범 사례 분석

- 가) 국내 주요 민간, 정부, 국방 분야 사례 분석
- 나) 인공지능(AI) 시스템의 국방 분야의 역할 및 실현 가능성 분석

3) 인공지능(AI) 기술분야별 활용방안 식별 및 과제 도출

- 가) 국방부 인공지능(AI) 중점 추진과제별 활용 가능한 분야 식별 및 과제 도출
- 나) 소요 군의 인공지능(AI) 시스템을 적용하고자 하는 요구과제별 사업계획의 구체화 가능 분석
- 다) 국방 무기체계별 인공지능(AI) 적용 가능한 분야 식별 및 과제 도출

4) 국방 분야 인공지능(AI) 적용 활성화를 위한 제도 및 정책적 제언

- 가) 국방 인공지능(AI) 활성화를 위한 사전 필요한 제도 및 정책 개선사항 분석 및 도출

2. 연구범위 및 방법

가. 문헌연구 / 현 실태 분석

- 1) 문헌 및 선행 연구자료 등 자료수집 및 분석
- 2) 인공지능(AI) 기술의 국방 분야 적용 필요성 분석

→ 검토자료 : 국내·외 기관 및 관련 업체로부터 획득한 자료, 기고문, 논문 등

나. 국방분야의 역할 및 실현 가능성 분석

- 1) 인공지능(AI) 개념 및 이론, 인공지능(AI) 기술의 분류
- 2) 인공지능(AI)의 역사와 중요한 이유

- 3) 인공지능(AI)과의 공존 및 구현(작동) 방안(기술 분류)
 - 4) 국내 주요 민간, 정부, 국방 분야 사례 분석
 - 5) 인공지능(AI) 시스템의 국방 분야의 역할 및 실현 가능성 분석
- 검토자료 : 국방백서, 관련 논문, AI 관련 기술자료

다. 인공지능 기술분야별 활용방안 도출

- 1) 인공지능(AI) 중점 추진과제별 활용 가능한 분야 식별 및 과제 도출
 - 2) 인공지능(AI) 시스템을 적용하고자 하는 요구과제별 사업계획의 구체화 가능 분석
 - 3) 국방 무기체계별 인공지능(AI) 적용 가능한 분야 식별 및 과제 도출
- 검토자료 : 국방부/합참 관련 훈령, 무기체계 획득 및 개발 관련 기술분석 자료

라. 정책적 시사점 및 발전방향 제시

- 1) 우리 군의 인공지능(AI)를 적용한 무기체계의 신속한 획득을 위한 제도 개선사항 발굴
- 2) 중장기적인 인력 성 및 기술 개발(R&D)
- 3) 국가 인공지능(AI) R&D 정책과 연계한 전문가 협의체 구성 방안 제시
- 4) 국방 인공지능(AI) 플랫폼 구축방안 제시
- 5) 검토자료 : 국방정책 및 군사전략 보고서 등

II. 문헌연구 / 시사점

1. 인공지능의 역사와 중요성

가. 인공지능(AI)의 역사

1965년에 처음 등장한 인공지능(Artificial Intelligence, 이하 AI)이라는 용어는 최근 데이터의 양적 증가, 첨단 알고리즘, 컴퓨팅 파워, 스토리지가 개선되어 더욱 활발히 연구되고 있는 분야이다.

1950년대에 시작된 초기 인공지능(AI)에 대한 연구 주제는 문제 해결과 기호법 등이었으며, 1960년대로 접어들면서 미 국방부는 컴퓨터가 인간의 기본적인 추론 방식을 흉내낼 수 있도록 훈련하기 시작하였다. 미국 국방고등연구기획국(DARPA)이 1970년에 수행한 도로지도화 프로젝트가 대표적인 사례라고 할 수 있다. 미국 국방고등연구기획국(DARPA)은 Siri나 Alexa, Cortana 등과 같은 인공지능(AI)이 개발되기 전인 2003년에 지능형 개인 비서를 개발하기도 하였다.

이와 같은 노력들은 오늘날 일상에서 우리가 접하고 있는 자동화와 형식 추론 기술에 대한 기틀을 다지는 역할을 하였다고 볼 수 있다. 이러한 기술에는 사람의 능력을 보완하고 확장할 수 있는 의사 결정 지원 시스템과 스마트 검색 시스템이 포함된다.

인공지능(AI)은 할리우드 영화나 공상 과학 소설에서 세상을 위협하는 인간형 로봇으로 묘사되고 있지만, 현재 인공지능(AI) 기술은 그 정도로 발전되거나 위협적이지는 않으며, 모든 산업 분야에서는 인공지능(AI)의 장점을 활용하고 있다.

나. 인공지능(AI)이 중요한 이유

인공지능(AI)은 반복적 학습과 데이터 인사이트를 통한 발견을 자동화하는 것으로 하드웨어에 기반을 둔 로봇 자동화와는 다른 개념으로 수작업을 자동화하는 차원을 넘어 반복적인 대량 전산 작업을 간단하게 수행하고 있다. 이러한 유형의 자동화를 위해서는 지속적으로 시스템 설정하고 정확한 질문을 전달할 수 있는 사람의 노력이 필요하다.

인공지능(AI)은 기존 제품에 지능을 더하는 개념으로 인공지능(AI)이 개별 애플리케이션으로 판매되는 경우는 거의 없다. 대신 Apple의 신제품에 Siri가 새로운 기능으로 추가된 것처럼 이미 사용 중인 제품에 인공지능(AI) 기능을 탑재하여 제품을 개선하는 방식이 이루어지고 있다.

※ 스마트 머신과 자동화, 대화 플랫폼, 챗봇 등이 대량의 데이터와 결합되면서 보안 인텔리전스, 투자 분석 등과 같이 직장가 가정에서 이용하는 많은 기술을 개선할 수 있다.

인공지능(AI)은 점진적인 학습 알고리즘을 통해 스스로를 개선하여 데이터가 최적의 프로그래밍을 수행하도록 지원한다. 인공지능(AI)이 데이터의 구조와 규칙성을 찾아내면, 알고리즘이 이를 학습하도록 지원하고, 알고리즘 분류 도구는 조건자로 만들게 된다. 이러한 알고리즘은 온라인 구매시 사용자에게 최적화 제품에 대한 추천을 찾아서 제시할 수 있으며, 새로운 데이터가 입력되면 스스로 학습하고 성능이 개선된다.

인공지능(AI)은 빅데이터를 심도 있게 분석하기 위해서 숨겨진 다양한 레이어를 가진 신경망을 활용한다. 즉, 컴퓨팅 파워와 빅데이터 분석 덕분에 신경망 구성이 가능해졌으며, 딥러닝(Deep Learning) 모델은 빅데이터를 이용해 직접 학습하는 모델로 입력하는 데이터가 많을수록 정확도가 더욱 높아지게 된다.

인공지능(AI)은 이전에는 불가능했던 딥 신경망 분석을 통해 놀랍도록 향상된 정확도를 제공하고 있다. 예를 들어 사용자와 Alexa, Google Search, Google Photos의 인터랙션은 모두 딥러닝(Deep Learning) 기술을 활용하고 있으며, 많은 사용자가 서비스를 이용할수록 더 높은 정확도로 원하는 결과를 획득할 수 있게 된다. 의료 분야에서는 딥러닝(Deep Learning)과 이미지 분류, 개체 인식 등과 같은 인공지능(AI) 기술을 MRI 이미지 분석에 활용해 정확한 결과를 얻어내고 있다.

이처럼 인공지능(AI)은 데이터의 활용을 극대화한다. 즉, 데이터는 알고리즘이 스스로 학습을 수행할 때 그 자체가 지적 재산이 될 수 있는 것이다. 모든 문제에 대한 해답은 데이터에 있기 때문에 인공지능(AI)에 데이터를 적용한다면 해답을 찾을 수 있다. 따라서 경쟁이 치열한 산업이라면 데이터로 경쟁 우위를 차지할 수 있으며, 유사한 기술을 보유하고 있다고 하더라도 최상의 데이터를 보유한 기업이 더욱 성장하게 되는 것이다.

인공지능(AI) 주요 활용 분야는 새로운 가치와 인사이트를 발견하고 의사결정을 지원하며, 자연어 이해를 통한 상호작용을 통하여 다양한 산업 분야에 적용하여 다각도로 활용이 가능하다. <그림 II-1>은 산업분야에서 인공지능(AI)의 주요 활용 분야를 크게 3가지로 분류하여 제시하였다.



〈그림 II-1〉인공지능(AI) 주요 활용 분야

2. 인공지능의 활용 및 구현방안과 인공지능 기술 분류

가. 인공지능(AI)과의 공존 및 구현(작동) 방안(기술분류)

인공지능(AI)은 인간의 역할을 대신하는 것이 아니다. 인공지능(AI) 알고리즘은 인간과는 다른 방식으로 학습하기 때문에 대상을 보는 시각도 다르다고 볼 수 있다. 인공지능(AI) 알고리즘은 인간이 놓치고 있는 데이터와 데이터 간의 관계와 패턴을 도출할 수 있으며, 이를 통해 인간과 인공지능(AI)이 상호 보완관계 형성하고 더 많은 활용의 기회를 제공할 수 있다. 그 예는 다음과 같다.

- 현 분석기술에 대해 제대로 이용하지 못하고 있는 산업과 분야에 도입
- 컴퓨터 비전과 시계열 분석과 같은 기존의 분석기술 성능을 더욱 높임
- 인간이 가진 기존의 능력을 확장하여 과제 수행 능력을 개선
- 비전, 이해력, 기억력 등 인간이 가진 다양한 능력을 개선

인공지능(AI)의 역할은 대량의 데이터 처리와 반복적인 작업을 빠르게 처리할 수 있는 알고리즘을 결합한 소프트웨어로 데이터에 존재하는 패턴이나 특징을 분석하고 스스로 자동 학습하도록 지원하는 다양한 이론 및 방법론, 기술 등을 포함한 종합적인 영역이라고 할 수 있다. 인공지능(AI)의 주요 세부 분야는 다음과 같다.

- 분석 모델구축을 자동화하는 머신러닝 (Machine Learning)은 신경망이나 통계분석, 운영분석, 물리학 등에서 활용되는 기법들을 활용하여 프로그래밍 없이 특정 위치를 찾거나 결론을 내리는 것과 같이 데이터에 숨어있는 인사이트를 찾아낸다.
- 신경망 (Neural Network)은 뉴런과 같이 외부 입력에 반응하며, 각 단위 사이의 정보를 연계하고 처리하는 일종의 머신러닝 (Machine Learning)이다. 서로의 연계성을 찾아내어 정의되지 않은 데이터로부터 의미를 추론하기 위해서는 처리과정에서부터 다중 데이터 패스가 필요하다.
- 딥러닝 (Deep Learning)은 컴퓨팅 파워의 발전과 학습 기법의 개선을 바탕으로 여러 레이어를 포함한 대규모의 신경망을 활용한다. 이를 통해 대량의 데이터로부터 복잡한 패턴을 학습할 수 있다.
- 인지 컴퓨팅 (Cognitive Computing)은 기계에서 인간과 가장 유사한 인터랙션을 이끌어내는 인공지능(AI)의 한 분야이다. 인지 컴퓨팅이 추구하는 궁극적인 목표는 기계에 이미지와 음성을 이해하는 능력을 부여하여 사람과 같은 방식으로 행동하고 반응하도록 만들어 내는 것이다.
- 컴퓨터 비전 (Computer Vision)은 패턴 인식과 딥러닝(Deep Learning) 기술을 바탕으로 이미지 또는 비디오의 내용을 인식하는 것을 말한다. 기계가 이미지나 비디오를 실시간으로 포착하여 분석하고 이해할 수 있다면 그 주변 상황을 해석할 수 있다.
- 자연어 처리(NLP; Natural Language Process)는 컴퓨터가 사람의 언어(음성 포함)를 분석하고 이해 및 생성할 수 있는 기술이다. NLP의 다음 단계는 사람이 평상시와 동일한 언어적 표현을 사용하여 컴퓨터와 소통하고 작업을 지시할 수 있는 자연어 인터랙션이다.

그 밖에 인공지능(AI) 구현과 지원을 위한 몇 가지 추가적인 기술을 제시하자면 다음과 같다.

- 그래픽 처리 장치는 반복적인 작업에 필요한 컴퓨팅 파워를 제공하는 인공지능(AI)의 핵심 요소이다. 신경망 학습을 위해서는 엄청난 양의 데이터뿐만 아니라 컴퓨팅 파워가 요구된다.
- 사물 인터넷(IoT)은 연결된 장치로부터 많은 양의 데이터를 생성하는 것을 말한다. 인공지능(AI)을 통해 모델을 자동화하게 되면 데이터를 실시간으로 분석하는 등 매우 유용하게 활용할 수 있다. 첨단 알고리즘은 많은 데이터를 다양한 수준에서 빠르게 분석하기 위해 새로운 방향으로 개발 및 결합되고 있으며, 이를 통해 매우 드물게

발생할 수 있는 것을 예측할 수 있다. 따라서 복잡한 시스템을 이해하며 고유한 시나리오를 최적화 하는데 필수적인 요소이다.

- 애플리케이션 처리 인터페이스(API)는 기존 제품과 솔루션 패키지에 인공지능(AI) 기능을 부가할 때 필요한 코드 패키지를 말한다. API를 이용하여 각종 보안 시스템에 이미지 인식 기능을 추가할 수 있으며, 데이터의 설명, 캡션 및 헤드라인의 생성 등 데이터의 흥미로운 패턴과 인사이트를 알려주는 Q&A 기능도 추가할 수 있다.

위와 같이 입력 데이터를 바탕으로 추론하여 결과물을 설명할 수 있는 솔루션을 제공하는 것이 인공지능(AI)의 목표로 인공지능(AI)은 사람과 같은 방식으로 소프트웨어와 인터랙션을 하고 특정한 과제에서 사람의 의사결정을 지원하는 역할을 담당하므로 이를 활용할 수 있는 국방 분야를 도출할 수 있다.

나. Big Data

맥킨지에 의하면 의료, 공공행정, 소매, 제조, 개인 정보 부문에 빅데이터를 적용할 경우 1%의 추가 생산성이 향상될 것으로 예측⁹⁾하였다. 특히 미국 의료부문에서는 연간 3,300달러의 직·간접적 비용 감소 효과가 있을 것으로 예상되며, 이는 미국 의료비용의 8%에 달하는 값이다. 유럽 공공부문의 경우에는 2,500억 유로의 가치가 있을 것으로 판단되고 있다. 영국의 Policy exchange 연구기관에서는 공공부문에 빅데이터 도입시 연간 160억~300억 파운드를 절감할 수 있으며, 이는 정부 총 예산 2.5 ~ 4.5%에 해당된다고 보고¹⁰⁾하였다. 우리나라는 공공분야에 빅데이터의 활용시 10.7조 원 이상의 경제적 가치를 창출할 것이라고 제시¹¹⁾하고 있다. EU는 단일 온라인 창구를 통해 모든 정보를 누구에게나 무료로 제공하기 위해, ‘an-European’이라는 데이터 포털을 구축¹²⁾하고 있는데, 우리 정부도 최근 빅데이터에 관심을 쏟으며 대통령 산하 국가 정보화 전략 위원회에서 “빅데이터 국가전략 포럼”을 실시한 바 있다.

빅데이터를 활용한 국내 사례로 서울시의 심야버스 노선 최적화를 위한 빅데이터 활용을 들 수 있다. 서울시는 2010년도부터 열린 데이터 광장을 통해 공공 데이터를 오픈 API 형태로 시민들에게 개방하여 서울시가 가진 문제를 빅데이터로 해결하려는 노력을 지속

9) McKinsey Global Institute(2011), Big data: The next frontier for innovation, competition, and productivity.

10) Yiu, C.(2012), The big data opportunity: making government faster, smarter and more personal.

11) 국가정보화전략위원회(2013), “빅데이터를 활용한 스마트 정부 구현”.

12) 고숙자, 정영호(2012), “국민건강 미래예측 시스템 구축 방안,” 한국보건사회연구원, 『보건복지포럼』, 통권 193호, p. 46.

적으로 해왔다. 그 중에서 가장 눈부신 성과를 낸 것이 바로 심야버스 노선 활용이라고 할 수 있다. 서울시는 심야에 택시를 사용할 수 밖에 없는 시민들을 위해 심야버스를 도입하고자 하였다. 하지만 심야버스를 아무 노선에나 투입시킬 수는 없었다. 이는 예산상의 문제 뿐만 아니라, 도입 후 시민들의 활용도가 낮다면 세금을 낭비하는 것이기 때문이다. 이러한 문제를 해결하기 위해 서울시에서는 빅데이터를 활용하여 노선을 결정하기로 하였다. 이를 위해 심야시간대의 휴대전화 통화량과 택시의 스마트카드 이용량에 대한 빅데이터를 확보하였고, 이 자료에 노선 부근의 유동 인구 가중치를 더하여 노선을 정하고 운영하였다. 그 결과 하루 평균 2,000여 명 정도의 시민들이 심야버스를 이용하였으며, 버스 만족도 조사에서도 시민들이 심야버스에 80점 이상의 점수를 주며 긍정적인 반응을 보였다.

다. 사물인터넷(IoT)

사물인터넷(Internet of Things, 이하 IoT)은 세상에 존재하는 모든 객체가 인터넷으로 연결되어 정보를 지능적으로 처리할 수 있는 환경으로 4차 산업혁명을 주도할 핵심기술이다. 4차 산업혁명 등 인공지능(AI) 기반의 급격한 첨단 과학기술의 변화와 맞물려 혁신의 물결을 맞이한 미래전장에 대비하기 위해 IoT 기술을 병력, 물자, 시설, 수송, 교육과 관련된 국방자원관리체계, 무기체계 및 지휘통제통신(C4I) 체계와 연계한 활용방안을 추진하고 있다.

1) IoT 개념과 표준화 동향

사물인터넷(IoT)란 세상에 존재하는 모든 객체(사람, 사물, 공간, 데이터 등)를 인터넷으로 연결해 정보가 생성·수집·공유·활용될 수 있는 환경을 말한다. 기존의 블루투스나 지그비(Zig-Bee)와 같은 M2M(Machine-to-Machine) 통신은 디바이스 사이의 근거리 통신을 중심으로 단순한 정보를 수집하는 역할에 사용되지만, 사물인터넷(IoT)은 인터넷망을 중심으로 각종 디바이스에서 수집된 정보를 활용해 다양하고 지능화된 서비스를 제공한다. 사물인터넷(IoT)이 4차 산업혁명의 핵심기술로 발돋움할 수 있었던 배경에는 아두이노, 라즈베리파이, 비글본 등과 같은 소형 임베디드 장치의 저가격화와 함께, BLE (Bluetooth Low Energy)와 같이 저전력 통신 기술이 활성화되면서 누구나 손쉽게 사물인터넷(IoT) 환경을 구축하고 서비스를 창출할 수 있게 되었기 때문이다.

특히, 사물인터넷 환경에서는 수백억 이상의 사물들간 상호운용성을 확보하기 위해 TTA(한국), ETSI(유럽), ATIS·TIA(북미), CCSA(중국), ARIB·TTC(일본) 등 7개의 SDO (Standard Development Organization)가 공동으로 oneM2M이라는 표준화 기구를

설립하여 사물인터넷 국제표준을 정의하고 있다. 또한 OCF(Open Connectivity Foundation)는 삼성, 인텔 등을 중심으로 운영되고 있는 기업 표준화 단체로 RESTful (Representational State Transfer) 구조 기반의 CoAP(Constrained Application Protocol) 프로토콜을 활용해 사물인터넷(IoT) 장치들을 플랫폼에 연결하는 표준을 정의하고 있다.

사물인터넷(IoT) 기반의 통신기술로는 IETF(Internet Engineering Task Force)에서 표준화가 진행 중인 CoAP, OASIS (Organization for the Advancement of Structured Information Standards)에서 국제표준으로 정의한 MQTT 가 대표적이다.

〈표 II-1〉 M2M 통신기술과 IoT 비교

구분	M2M	IoT
통신·네트워크	근거리망, 이동망 중심	인터넷 중심
디바이스 형태	센서 중심	센서, 액추에이터, 데이터, 프로세스 등
디바이스 서비스 구동수준	단순 정보 수집·수동적	자율 판단하는 지능보유·자율적
서비스 플랫폼	모니터링 정보처리	의미 기반 모니터링 및 자율제어
서비스 관리 규모	수천만 개의 사물	수백억 이상의 사물
서비스 적용성	통시적 서비스 제공	즉각적 스마트 서비스 제공
통신기술	블루투스, 지그비 등	CoAP, MQTT, MQTT-SN 등

〈표 II-2〉 CoAP와 MQTT 비교

구분	CoAP	MQTT
통신모델	클라이언트·서버 Publish-Subscribe(Optional)	Publish-Subscribe
프로토콜 구성	두 개의 sub-layer로 구성 (Message layer and request-response layer)	한 개의 계층으로 구성
네트워크 계층	UDP	TCP
전력 소모량	상대적으로 낮음	상대적으로 높음
Quality of Service(QoS)	CON 메시지를 이용한 데이터 전송	세 개의 QoS 레벨자원(0, 1, 2)
Security	Datagram Transport Layer Security(DTLS)	Secure Sockets Layer(SSL)

2) 생활 속의 사물인터넷(IoT) 활용사례

현재 민간분야에서는 스마트 홈, 스마트 시티, 스마트 팩토리, 자율주행 자동차, 헬스케어 등 다양한 분야에서 사물인터넷(IoT) 기술이 사용되고 있다. 대표적인 사례로, 아마존에서는 물류 창고 로봇 ‘키바(Kiva)’를 사용해 직원이 근무하기 힘든 물류창고에서의 근무환경을 개선하고 20% 정도의 물류비용을 절감하고 있다.

구글 네스트 플랫폼에서는 사용자의 온도조절 패턴을 학습하고 기상정보 등을 활용해 자동으로 온도를 조절하는 등 다양한 스마트 홈 관련 서비스를 제공하고 있다. 구글의 모기업 알파벳의 산하기업 웨이모(Waymo)는 V2X(Vehicle-to-X) 기술을 활용하여 미국 애리조나주 피닉스 일부지역에서 무인자동차 서비스를 수행할 예정이며, SK텔레콤에서는 자율주행 자동차로 고속도로 운행을 성공적으로 수행했다. 미국 미모(Mimo)사의 스마트 베이비 모니터는 아기의 옷에 센서를 부착해 아기의 호흡과 피부 온도, 잠자는 자세, 활동량 수준 등의 정보를 부모의 스마트 폰으로 실시간 전송하는 헬스케어 서비스를 제공하고 있다.



아마존 물류 창고 로봇



구글 네스트 플랫폼



웨이모 자율주행 자동차



미모 스마트 베이비 모니터

〈그림 II-2〉 사물인터넷(IoT) 활용사례

라. Big Data + IoT

1) Big Data 분석기술의 군 적용 및 활용실태

빅데이터는 단순히 큰 데이터를 의미하는 것이 아니라 부피(Volume)가 크고, 변화의 속도가 빠르며(Velocity), 데이터의 속성이 매우 다양한(Variety) 데이터를 의미한다. 빅데이터는 최근 10여 년 사이 인터넷이 일상화되면서 데이터가 폭증하는 데이터 홍수현상과 함께 등장하게 되었다.

빅데이터의 군 활용사례로 미군은 자살을 예방하는데 활용하였다. 미군은 현재 전 세계 각지에서 작전을 수행 중이며, 직접 전투를 하고 있는 곳도 있다. 특히 이라크와 아프가니스탄의 경우 자살 폭탄 테러 등과 같이 미군에 대한 공격이 끊이지 않고 지속되고 있으며, 이 곳에서 작전을 수행하고 돌아온 군인들의 자살이 늘어나고 있는 추세이다. 이라크와 아프가니스탄 재향 미군회(IAVA, Iraq and Afghanistan Veterans of America)가 4,104명의 재향 군인들을 대상으로 진행한 설문에 따르면 자살로 생을 마감한 현역 군인 수가 전투 중 사망한 군인 수보다 많았다고 한다. IAVA의 보고서에 의하면 전체 응답자의 30%는 자살을 생각해 보거나 고민해 보았고, 45%는 자신의 동료 중 자살을 시도한 이를 알고 있으며, 37%는 실제 동료의 자살을 접한 경험이 있는 것으로 조사되었다. 또 설문에 참여한 퇴역 군인 가운데 50%가 '자신의 가까운 지인이 정신 질환 치료의 필요성을 암시했다'라고 응답하기도 했다. 따라서 국방성과 재향군인회에서는 소셜미디어와 빅데이터를 통해 자살위험이 있는 퇴역 군인들을 확인하고, 그들에게 적절한 치료를 지원하여 해결하고자 하는 프로젝트를 계획하였다. 왜냐하면 정신적 문제를 겪고 있는 퇴역 군인이 자신의 고민을 말로 직접 표현하는 경우는 드물지만 페이스북이나 트위터 등의 소셜미디어에서는 충분히 자신의 문제를 드러낼 가능성이 있기 때문에 페이스북과 트위터 활동을 분석하여 자살을 예측하고 예방하고자 한 것이다. 문맥에서 자살을 암시하는 단어들을 찾아내고 이를 소셜미디어에서 실시간으로 분석함으로써 정신적인 문제를 겪는 개인을 찾아내어 자살을 시도하기 전에 도움을 줄 수 있다는 것이 이 프로젝트의 기본적인 아이디어였다. 이 프로젝트를 1897년 자살이라는 논문을 통해 자살 위험에 대한 분석 연구의 기틀을 마련하고, 자살을 사회적 단절의 개념과 연관 짓는 이론적 해석의 틀을 제공한 에밀 뒤르켐(Emile Durkheim)의 이름을 가져와 '뒤르켐 프로젝트'라 명명하였다. 페이스북, 트위터, 링크드인 등 소셜미디어에서의 거대 기업들과 파트너십을 구축하였으며, 모바일 SNS 애플리케이션들을 이용하여 사용자들의 자발적 참여를 통해 구성되는 소셜미디어 및 모바일 폰 데이터베이스를 구축함으로써 임상가가 자살 등 위험 행동을 야기할 가능성이 있는 심리적 위험 지표를 실시간으로 평가할 수 있게 하였다. 애플리케이션은 연구를 위해 참여에

동의를 한 퇴역 군인들의 온라인 활동 기록은 자동으로 의료 데이터베이스에 통합하게 되며 텍스트 저장소는 지속적으로 자료가 업데이트가 되고 분석이 이루어진다. 이를 기반으로 통계학적으로 자살과 연관성을 지니는 텍스트 콘텐츠 및 행동 패턴을 실시간으로 모니터링 하고 퇴역 군인들의 자살 징후를 도출하여 미연에 사고를 방지하였다.

2) 국방 IoT 인프라 구축현황

군에서 사물인터넷(IoT) 기술을 적용한 사례는 시범사업으로만 추진 중에 있으며, 현 추진계획 중인 시범사업은 육군훈련소 사물인터넷(IoT) 기반 스마트 훈련병 관리체계, 공군 전투기 조종사 u-Health 환경구축, 대대급 병영생활 사물인터넷(IoT) 환경구축, GOP 과학화 경계시스템 구축 운영에 활용 중에 있다.

『병력관리』측면에서의 사물인터넷(IoT) 기술의 적용은 분대 또는 소대 단위 생활관에서 공동생활에 따른 행동패턴 분석 등을 위한 데이터 수집 대상에 적용하고 있으며, 교육 훈련, 작전 활동 등 일과시간 이외는 일과표에 의한 생활관 단위 활동(자기개발 및 자율 활동시간, 점호 등) 간 데이터수집 대상에 적용하고 있다. 또한, 경계작전 및 주둔지 근무 투입·복귀 후 지휘관 또는 당직 근무자에게 신고 절차간 수집대상 데이터를 측정하기 위해 적용하고 있다. 이는 실시간대 병력위치 파악을 할 수 있는 시스템이 없는 실정으로 경계근무자 이동간이나 위치 이탈시 즉시 위치파악이 제한과 부대이탈(탈영)시 주변 수색 정찰 및 군견에 의한 추적, 연고지 탐문 수사 등으로 위치파악에 장시간 소요 발생에 따른 보완사항으로 적용한 사례이다. 또한, 병사 개인 건강상태는 본인이 보고하기 전에는 파악이 어려운 상태로 긴급 구호조치가 제한되거나 시간 과다 소요(골든타임 상실 우려)와 병력의 위치 및 개인건강상태를 실시간대 파악할 수 있는 센서 디바이스 필요성 검토 결과에 따라 적용하고 있다. 다음은 현재 연구개발 추진 예정사항으로 부대관리 차원에서 사물인터넷(IoT) 적용할 경우 필요한 센서 디바이스 등에 대한 검토 및 분석한 내용이다.

가) 『총기·탄약관리』측면에서의 IoT 소요파악을 위한 분석내용 예)

- 개인화기(소총, 기관총)는 생활관 단위 총기함에 2중 잠금장치를 통하여 보관, 관리 중이며, 교육훈련, 작전활동시, 경계 근무 투입 등 총기함을 개방하여 개인에게 지급(휴가자 총기 및 잔여총기, 박격포는 무기고에 보관) → 총기 수불에 따른 절차상 근거자료 유지 등 데이터 수집대상 도출
- 총기휴대 탈영 또는 총기 은닉시 총기소재 파악에 장시간 소요 및 실시간대 개인화기 위치 파악은 시스템이 없어 파악이 어려운 실정으로 이를 극복하기 위해 적용방안 연구
- 탄약은 대대 탄약고에 통합 보관, 관리 중에 있으며, 수불행위가 이루어지면 탄약수불카드, 탄약고내

비치한 현황판 및 탄약정보시스템에 의해 탄약에 대한 재고관리를 하고 있음 → 탄약 수불에 따른 데이터 수집대상 도출

- 즉, 사격훈련 및 작전활동 후 탄약, 탄피반납을 통해 탄약 소모량과 재고를 파악하고 탄약 재물조사시 납봉인된 탄박스와 개봉된 박스의 낱발을 육안으로 실شم하여 탄약 재고량 파악
- 육안 실شم 및 수기에 의한 재고 관리로 오류 발생우려, 관리자 측면에서 필요하지만 현 탄약정보 시스템으로 구현할 수 없는 사항에 대해서 도출

즉, 총기 수불일지 및 위치와 총기보관함 등 시설 내부의 보유수량 등을 실시간대 파악할 수 있는 센서 디바이스 적용이 필요하며, 탄약의 위치와 재고량 등을 실시간대 파악할 수 있는 센서 디바이스 및 현 탄약정보시스템(AIS 등) 연동이 필요하다. 2011년 RFID를 활용한 탄약관리를 추진하였으나 중단된 사례가 있다.

나) 『시설·장비(정바)·물자관리』측면에서의 IoT 소요파악을 위한 분석내용 예)

- 화생방장비, 통신장비 등 주요 장비는 창고에 보관, 관리 중(장비·물자 관리대장과 창고내 현황판에 의해 출납 및 재고관리)으로 주기적인 재물조사를 실시하나 육안에 의한 실شم으로 재고량 파악 간 오류 발생 우려
- 편성부대에서의 장비정비는 예방정비 등을 실시하고 있으며, 정비실적을 국방장비정비정보체계(Delis)를 통해 관리하고 있음
- 유류는 유류고내에 드럼상태로 관리하며, 유류 주입시 정확한 주입량 계측이 제한(주유기 보급제대는 정량 주입가능) 되고 있는 실정으로 → 유류 수불에 따른 데이터 수집대상 도출
- 편성부대 시설은 무기고, 탄약고, 유류고 등을 운영하고 있으며, 무기고 및 탄약고에는 경계초소(1개소)와 사각지역에 CC-TV를 설치하여 출입통제 및 출입일지를 유지를 하고 있는 등 관련 데이터 수집대상 도출
- 무기고, 탄약고 출입문(철문) 개방시 경고벨이 지휘통제실에 작동하도록 운영(출입문 장시간 개방시 경고벨 소음으로 지휘통제실에서 확인 후 벨소리를 Off 하는 경우 발생)

즉, 주요장비·물자(화생방장비, 통신장비, 유류 등)의 위치와 재고량을 실시간대 파악할 수 있는 센서 디바이스 필요성 검토와 장비정비 실적에 대한 데이터 구축을 위해 현 Delis와 연동이 필요하며 시설관리(무기고, 탄약고, 유류고, 격오지, 경계초소 등)의 개폐관리를 실시간대 파악할 수 있는 센서 디바이스가 필요하다.

다) 『차량관리』측면에서의 IoT 소요파악을 위한 분석내용 예)

- 편성부대(대대급)의 모든 차량은 수송부 차고지에 보관, 관리하고, 일일배차계획서에 의해 승인된 차량 운행, 운행일지 기록 유지 중에 있으며 이와 관련 데이터 수집대상 도출
- 일일 차량점호를 실시하여 차량 상태확인, 예방정비계획에 의거 예방정비를 실시하고 Delis 등에 기록 유지 중으로 이를 사물인터넷(IoT) 적용 방안 검토
- 차량이 주둔지를 벗어나 이동중에는 차량의 위치를 실시간대 파악할 수 있는 시스템 없어 파악이 어려운 실정(선담간부의 유선보고에 의존)

즉, 차량(지휘관, 수송, 화포 차량 등)의 실시간 위치와 장비의 상태정보(상태진단, 운용도 진단 등)를 실시간대 파악할 수 있는 센서 디바이스가 필요하다.

라) 『스마트 부대관리시스템』에 적용할 부대관리분야 선정 : 5개 분야로 구분

부대관리분야	세부 대상
① 병력관리	병사, 간부
② 총기·탄약관리	총기: 개인화기(소총, 권총), 기관총, 박격포, 야포 등 탄약: 소총탄, 권총탄, 기관총탄, 박격포탄, 포병탄 등
③ 차량관리	지휘관차량, 수송차량, 화포차량, 화생방차량 등
④ 주요장비·물자관리	화생방장비, 통신장비, 보안장비, 유류 등
⑤ 시설관리	무기고, 탄약고, 유류고, 격오지, 경계초소 등

마) 부대관리분야별 센서디바이스

부대관리분야	센서디바이스	
	고정시설 센서	이동체 센서
① 병력관리	-	병사용, 간부용
② 총기·탄약관리	-	개인화기용, 공용화기용, 야포용
		소총탄, 권총탄, 기관총탄, 박격포탄, 포병탄
③ 차량관리	-	지휘관 차량, 수송 차량, 화포 차량, 화생방차량
④ 주요장비·물자관리	-	화생방장비, 통신장비, 유류
⑤ 시설관리	탄약고, 무기고, 유류고, 경계초소 등	-

바) 부대관리 센서별 수집/분석해야할 데이터

부대관리 센서	수집/분석 데이터
① 병력관리 센서	병사 개인건강상태, 병력 위치정보
② 총기·탄약관리 센서	총기(화포) 위치정보, 탄약 위치정보, 탄약 재고정보관리 등
③ 차량관리 센서	차량운행정보관리, 위치정보, 차량 정비상태정보 등
④ 주요장비·물자관리 센서	화생방·통신장비 위치정보, 장비 정비상태정보, 유류재고 정보관리 등
⑤ 시설관리 센서	무기고/탄약고/유류고 개폐관리, 무기고/탄약고 내부상태관리, 경계초소관리, 격오지 개폐관리 등

3) 시사점

- 무인장비는 무인 항공기, 로봇, 자율주행 자동차 등 미래의 군사 분야에서 더 많이 활용될 예정이며, 이 장비를 총괄 제어하기 위해서는 ‘조종기’나 ‘리모컨’이 아닌, 사람과 같이 인식하고 판단할 수 있는 기술이 필요하며, 이것이 인공지능(AI)의 핵심기술에 필요함
- 모든 사물이 연결되는 사물인터넷(IoT) 환경은 다양한 분야에서 활용될 수 있으나, 보안의 취약점이나 외부의 공격에 노출됨.
- 국방 분야의 특성상 보안 취약점으로 인한 정보유출은 막대한 피해와 인명손실을 야기할 수 있기 때문에 국방 분야의 사물인터넷(IoT) 기술 도입은 더욱 신중하게 접근해야 하며, 이를 위한 보안체계가 새롭게 구축되어야 함.
- 국방 분야에서 사물인터넷(IoT) 기술을 도입하기 위해서는 『저사양의 사물인터넷(IoT) 기기에서 활용하기 위한 경량·고속 암호 모듈 기술, 사물인터넷(IoT) 기기의 유출, 불법 포획으로 인한 내부 해킹을 방지하는 암호키 은닉 및 원격 데이터 삭제 기술, 식별되지 않은 디바이스의 접근이나 비인가 사용자의 접근 차단 기술 등 디바이스 측면의 보안뿐만 아니라 비인가 무선랜 장비에 의한 위협을 방지하기 위한 무선랜 보안기술, 기존의 업무망과 사물인터넷(IoT) 망의 분리 운영을 위한 연계구간 설정 및 보호기술, 사물인터넷(IoT) 기기로부터 전송된 정보를 안전하게 보호할 수 있는 암호화 및 메시지 무결성 검증 기술, 사물인터넷(IoT) 기기나 네트워크의 트래픽 모니터링 및 분석을 통해 악성코드나 해킹』등의 이상징후를 탐지하고, 실시간으로 대응할 수 있는 침입탐지 대응기술 등 다양한 측면의 보안기술들도 연구개발을 통해 보안성을 필수적으로 확보해야 함.
- 4차 산업혁명 시대 핵심 기술인 AICBM(IoT, Cloud, Big Data, Mobile) 기반의 스마트 부대 구축을 통해 첨단과학기술 군으로 탈바꿈하여 한계를 넘어서는 초일류 육군 건설, 표준화된 시스템 기반으로 체계적인 대응과 신속하고 신뢰성 있는 서비스 제공 가능, 효율적 부대 운영을 통한 장병 삶의 가치 향상, ICT/IoT 및 빅데이터 분석의 신기술을 부대운영 전반에 적용함으로써 사람 중심의 부대 운영과 각종 문제(안전사고 예방, 화재예방 등) 해결로 쾌적한 병영문화 조성이 가능할 것으로 판단됨
- 사물인터넷(IoT) 기반의 스마트 부대관리는 먼 시점의 이야기가 아니며 현재 연구추진 예정인 사항에 대해서 지속적으로 추진한다면 조기에 구현이 될 것으로 확신하며, 부대관리 측면에서 사물인터넷(IoT)를 적용한다면 예상되는 기대효과 다음과 같다.

- 첫째, 국방 자원관리에 창조적, 혁신적 사물인터넷(IoT) 서비스 적용시 부대관리에 획기적 변화가 예상되며, 병력, 총기관리 실시간대 파악으로 사고예방에 크게 기여할 것으로 판단됨.
- 둘째, 인명사고 및 차량사고 감소로 지휘부담 경감과 차량, 장비 정비수요 예측 및 적기 예방정비 가능으로 유지보수비용 절감으로 국방개혁 2.0과 연계된 부대관리 개선으로 대군 신뢰 증진에 기여할 것으로 기대됨.
- 셋째, 직접적인 자료수집 방식인 사물인터넷(IoT)와 빅데이터 분석으로부터 스마트 부대관리 구축을 통해 스마트 육군 건설과 국방개혁 2.0의 성공적인 추진 여건을 보장하여 육군의 체질 개선 및 정예화가 가능할 것으로 판단됨
- 안정적인 서비스와 다양한 사용자 맞춤형 서비스 제공 등으로 장비 만족도·신뢰도 향상될 것으로 기대됨

Ⅲ. 국내·외 인공지능 시스템을 활용한 모범사례 분석

1. 주요 민간, 정부, 국방 분야 사례분석

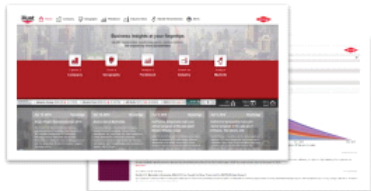
가. 민간 및 정부 적용사례 분석

모든 업계에서 인공지능(AI)의 적용과 활용을 요구하고 있으며, 다양한 산업에서 효율적으로 인공지능(AI)을 활용하고 있다. 먼저, 헬스케어에서는 인공지능(AI) 어플리케이션이 맞춤 의료와 X-ray 판독에 활용하고 있다. 그 예로 개인 건강 관리 어플리케이션은 약 먹을 시간을 알려주고 운동이나 건강한 식습관 유지를 지원하는 생활 지도사로서의 역할을 수행한다. 소매업에서는 인공지능(AI)이 상품을 추천하고 소비자의 구매 결정을 도와주는 가상 쇼핑 기능을 제공하며, 재고관리 시스템과 사이트 레이아웃에서도 인공지능(AI) 기술을 적용하고 개선할 수 있도록 구축되어 있다. 제조업에서는 인공지능(AI)이 연결된 장비들이 주고받는 공장 사물인터넷(IoT) 데이터를 분석하고, 딥러닝(Deep Learning) 네트워크의 일종인 반복 네트워크를 활용하여 작업량과 수요를 예측하여 최적의 생산을 할 수 있도록 구축되어 있다. 스포츠에서는 인공지능(AI)이 경기의 이미지를 캡처하고 필드 위치와 전략을 최적화하여 경기를 보다 효과적으로 계획하는 방법을 알려주는 보고서를 제공할 수 있도록 구현되어 있다.

〈표 III-1〉 인공지능(AI) 기술을 적용한 사례

구분	내용
알리바바 (Alibaba)	• 세계 최대의 전자 상거래 플랫폼으로 아마존과 이베이를 합친 것보다 더 많은 상품을 판매 • 알리바바를 이용하는 고객들이 어떤 상품을 사고 싶어하는지를 예측하는 데 사용 • 시티 브레인(City Brain)이 인공지능(AI)을 사용해 도시의 모든 교차로 동영상과 자동차 위치 GPD 데이터 등 도시 전역의 정보를 수집하고 교통을 제어 • 농업용 '사물인터넷(IoT)' 기술을 통해 농작물의 생장 상황을 검측하여 정확한 위치에 필요한 양을 관개 용수로 공급하여 농업 용수 비용 절감에 적용
알파벳 (Google)	• 구글(Google)의 모회사로 자율 주행 기술 관련 사업인 '웨이모(Waymo)' 프로젝트를 시작 • 웨이모(Waymo)의 자율 주행 차는 캘리포니아에서 '자율주행차 시범 승객 서비스'의 참여 승인을 받아 탑승자를 태울 수 있도록 허가
애플 (Apple)	• 아이폰에 인공지능(AI)과 기계학습을 사용하여 페이스 아이디(Face ID) 기능을 사용 • 에어팟, 애플워치 또는 스마트 스피커 홈팟과 같은 제품에 스마트 보조 Siri를 지원 • 인공지능(AI)을 이용하여 애플 뮤직에서 노래를 추천하거나, 아이클라우드에서 사진을 찾거나, 지도를 사용하여 다음 목적지로 이동할 수 있도록 도와주는 등 다양한 서비스 제공

Dow Chemical은 머신러닝(Machine Learning) 기반의 기업고객 통합분석 플랫폼을 도입, 기업고객 정보를 통합 분석함으로써 영업 Cycle을 단축 및 매출의 향상을 달성하였다.

Key Challenges	주요 변화	Key Benefit
다양한 데이터를 실시간으로 분석하여 기업고객 및 시장에 대한 통찰력을 얻기를 희망 • B2B Sales의 효과와 기업고객, 경쟁사에 대한 통찰력이 비즈니스 성공에 매우 중요 • 전사적으로 통합된 Customer Dashboard의 부재	통합 Customer Dashboard (iHunt) 구축 • 내외부 데이터의 통합적 활용 • 기업고객 Profile, 최근 계약현황, 마케팅 효과, 영업기회, 인터넷에서 취합된 기업고객 관련 정보 등을 통합 및 시각화 (고객 360° View) • 인지 능력을 바탕으로 기업고객 관련 뉴스를 유의미한 방식으로 그룹화하여 제시 	1 제안부터 계약까지의 영업 Cycle 단축 2 신속한 영업기회 인지 3 Cross-sell을 통해 영업실적과 전체 매출 향상

또한, 비정형 데이터 분석 기반 Analytics Dashboard를 도입함으로써, 고객에게 발생 하는 이슈의 종류 및 발생 원인을 빠르게 파악하고 대응할 수 있도록 하였다.

Key Challenges	주요 변화	Key Benefit
고객 데이터 분석을 통해 빠르고 정확한 품질 이슈 대응을 희망 - 자동차에 사용되는 고무 Seal 원료의 80~90% 공급  - 제품의 생산 및 사용 과정에서 발생하는 주요 이슈의 원인 파악 및 해결이 중요	Analytics Dashboard 구축 - 내/외부 비정형 데이터의 통합적 활용 - 증상별/차종별/부품별 이슈 발생 빈도 제시 - 이슈 발생 부품 별, 채널 별 Social 언급 빈도 및 언급 맥락 상의 긍/부정 현황 및 추이 제시 - 자동차 브랜드 별 이슈 현황 비교 제시 	1 시간대별 Tracking을 통한 신속한 제품 이슈 발견 2 정확한 이슈 원인 파악 및 대응 3 새로운 니즈 발견 및 제품 개발 반영

국내 선진 금융사는 인공지능(AI) 기반 데이터 분석을 통해 효율적으로 시장 전망을 예측하고, 우수한 상품을 적시에 발굴하기 위한 프로젝트 추진하고 있다.

Key Challenges	주요 변화	Key Benefit
 - 시장의 전망을 빠르고 정확하게 예측 필요 - 우수한 금융 상품 적시 발굴 필요	다양한 데이터의 활용 - 정형 데이터 (금융 시장 관련 이벤트, 시장 지표 등) - 비정형 데이터 (뉴스, 레포트, 웹사이트 등) 효율적이고 정확한 데이터 분석 - 시장의 전망 및 금융 상품 비교 프로세스의 자동화 - Deep Learning을 활용하여 시장과 금융 상품의 전망에 대한 정교한 예측 모델 개발	1 시장 전망 예측 소요 시간 단축 (2주 단위 → 日 단위) 2 인공지능을 활용하여 시장 전망 예측, 시장변화에 선제적 대응

혼다(Honda)는 인공지능(AI) 기반 상담원 서비스 ‘Ask Dave’를 통해 제품 관련 고객 문의의 대응 및 코칭을 통해 고객 경험 혁신을 이룩하였다.

Key Challenges & 주요 변화	Key Benefit
- 운전자 코칭 시스템 (Driver Coaching System) 프로토타입을 구축해 초보 및 베테랑 운전자들이 주행 시 위험할 수 있는 상황을 감지 - AI를 활용하여 비정상 주행 움직임이나 운전자의 주의집중도, 피로도를 탐지해 운전자 상태에 맞는 코칭을 실시간 제공 - AI 기반 가상 온라인 상담원 서비스(Ask Dave)를 통해 24시간 언제든지 고객 문의에 응대	1 운전자 상태에 맞는 코칭을 통해 운전자 및 보행자 위험 감소 2 24시간 AI기반 챗봇 서비스를 통해 2,500여건의 리콜 접수 및 답변 제공



인공지능(AI)에 관해 활발히 연구하고 있는 기업은 IBM과 구글이 대표적이다. IBM은 사사의 인지 컴퓨팅 기술인 왓슨을 기업용 솔루션으로 제공하며, 구글은 자율주행 자동차나 딥러닝(Deep Learning) 구글 나우 등의 음성인식 서비스를 내놓았다.

IBM의 왓슨은 인간의 언어를 인지하고 생각하는 기술로 2001년 미국의 유명 퀴즈쇼에 출연하여 무려 74연승을 거두면서 주목받기 시작했다. 수많은 데이터가 담긴 컴퓨터가 정해진 답을 맞히는 퀴즈쇼에서 우승한 것에 대해 대단하게 여기지 않을 수도 있지만, 여기에서 주목해야 할 점은 왓슨이 문제 제출자가 하는 말을 실시간으로 이해하고 분석하여 질문 내용을 파악한 뒤 정답을 저장장치에서 찾는 다는 점이다. 만약 왓슨이 인터넷에 연결돼 저장된 데이터 이외의 것까지 얻을 수 있다면 지식이 무한대로 확장되는 것도 가능할 것이다.

왓슨의 실제 적용사례는 미국의 요리 전문 잡지 본아페띠(Bon Apéti)와 IBM이 지난 2015년 협력해 만든 ‘쉐프 왓슨’이다(그림 III-1). ‘쉐프 왓슨’은 사전에 학습한 1만여 가지의 레시피를 바탕으로 사용자에게 다양한 재료와 조리 방법을 추천해 준다. 예를 들어 돼지고기, 당근, 양파 등의 재료를 선택하면 ‘쉐프 왓슨’은 이와 함께 사용할 수 있는 다양한 재료를 선별해 보여준다. 단순히 데이터베이스에 있는 재료만을 보여주는 것이 아니라 각 재료의 향이나 맛이 얼마나 조화로운 것인지에 대한 예상 결과도 보여주었다. 이 결과를 바탕으로 사용자는 왓슨이 제안한 재료와 레시피를 선택하거나 다른 몇 가지 재료나 조리법을 추가해 새로운 요리를 만들 수 있다. 즉 지식의 영역은 왓슨이 담당하고 최종 선택에 해당하는 지혜의 영역은 인간이 담당하는 셈인 것이다. IBM 관계자는 ‘쉐프 왓슨’에 대해 ‘인간의 창의성을 높여 줄 수 있다’고 설명한다. 또한, 특정 재료에 알레르기가 있다면 ‘쉐프 왓슨’에서 해당 재료를 배제하는 것만으로 새로운 재료나 조리법을 발견할 수 있을 것이다.



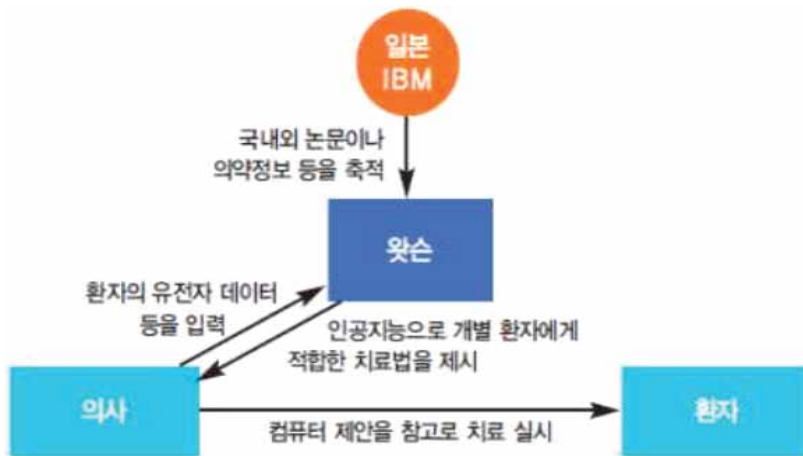
〈그림 III-1〉 IBM 셰프 왓슨

또한, IBM 왓슨은 특정 전문직의 교육을 받는다면 그 사람의 직책을 대체하는 것도 가능하다고 설명하고 있다. 예를 들어 애널리스트가 장기간에 걸쳐 왓슨을 학습시키면 관련지식을 그대로 학습하여 결과를 ‘정답’이 아닌 ‘신뢰도’를 바탕으로 보여주고 인간은 가능성 있는 여러 가지 결과를 토대로 정확한 판단을 할 수 있게 된다.

현재 기술 수준에서 인공지능(AI)에 관해 상용화 시도가 가장 활발하게 일어나고 있는 분야는 바로 의료 분야이다. 2000년대 중반부터 세계 여러 연구자와 발명가는 의료용을 주 타깃으로 하여 다양한 벤처기업을 설립하고 이 분야에 뛰어들기 시작하였다. 일본 쓰쿠바 대학의 산카이 요시유키 교수가 2004년 설립한 ‘사이버다인’, 미국 실리콘밸리를 기반으로 2005년에 세운 ‘엑소 바이오닉스’, 2001년 처음으로 미국 식품의약국(FDA) 승인을 얻은 이스라엘 기업 ‘리워크’ 등이 여기에 속하는 대표적인 기업들이다. 국내에서 2008년 처음으로 장애인을 위한 웨어러블 로봇 ‘헥사’를 공개한 바 있는 한양대 한창수 교수(로봇공학과)의 한겨레 인터뷰에서 “인공지능(AI)은 의료용이 가능성이 가장 높은 분야”라고 말하였다. 의료분야에서 주요 제품군은 하반신 마비 환자가 다시 걷도록 돕는 현대의 ‘에이치-맥스(H-MAX)’가 있다. 구체적인 기술 사양과 성능 등 세부적인 면에서는 차이는 있지만, 주요 회사의 제품은 모두 에이치-맥스(H-MAX)와 비슷한 방식으로 작동하는 구조이다. 미국의 ‘메모리얼 슬론 케터링 암 센터’는 전문의와 함께 암 치료를 돕는 ‘왓슨 헬스’를 도입하여 〈그림 III-2〉와 같이 방대한 데이터베이스를 기반으로 전문의에게 객관적인 의료

정보를 제공한다. 전문의는 이러한 정보를 바탕으로 환자의 증상에 대한 정확한 치료법을 쉽고 빠르게 찾을 수 있으며, 이를 통해 개인 맞춤형 진료도 가능하게 하고 있다.

산업용으로는 SK텔레콤이 2001년 자연어 처리, 즉, 음성인식 기술에 대한 연구를 시작하면서 국내 최초로 음성인식 기반 인공지능(AI) 서비스 ‘누구(NUGU)’를 개발하였으며, 이 외에도 산업용 보조로봇 에이치-웍스(H-WEX), 보행 보조로봇 에이치-렉스(H-LEX), 헥사(한양대 로봇공학과) 등이 있다.



〈그림 III-2〉 IBM 왓슨 의료

나. 국방 분야 적용사례 분석

1) 객체 인식(이미지, 영상, 음성) 플랫폼

국방부는 먼저 보고, 먼저 결심하고, 먼저 타격함으로써 전투 승수 효과 극대화를 위해 인공지능(AI)을 활용하여 적 기동장비, 이동형 발사차량, 함정, 항공기 등 표적을 식별하고 객체를 인식하는 방안을 구축하였다.

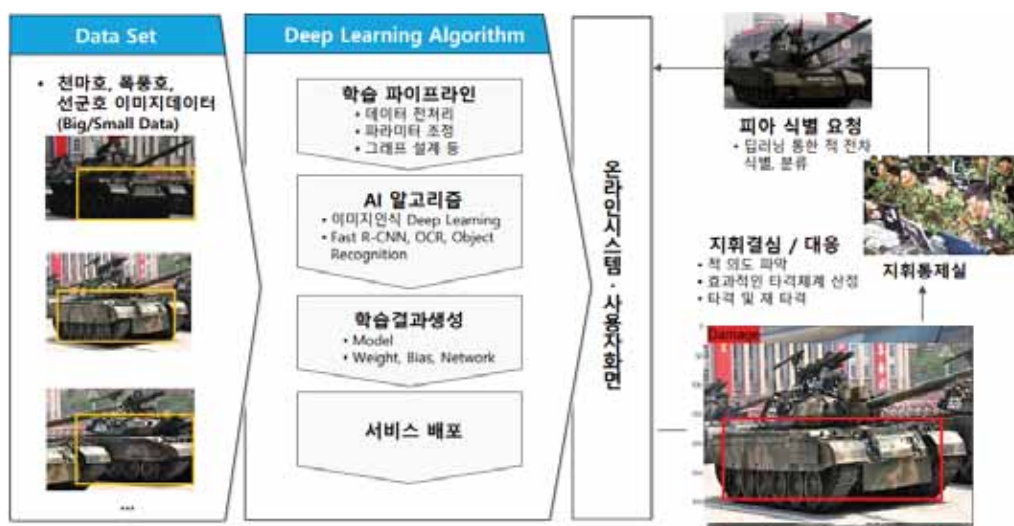
천마호, 폭풍호, 선군호의 이미지를 데이터화하여 수집하고, 이를 토대로 표적 및 객체 인식에 활용하는 데이터를 수집하였다. 이후, 딥러닝 알고리즘(Deep Learning Algorithm) 단계를 통해 학습 파이프라인, 인공지능(AI) 알고리즘, 학습결과 생성, 서비스 배포의 단계를 거친다.

먼저, 학습 파이프라인에서는 데이터 전처리, 파라미터 조정, 그래프 설계 등의 작업이 진행된다. 데이터 전처리는 수집된 데이터를 분석하기 좋게 변형하는 작업으로, 각 전차, 무기, 함정, 항공기 등의 데이터를 정규화 하여 정확하고 적시성 높은 데이터로 변형한다.

파라미터 조정 작업은 데이터의 전체적인 추이, 경향을 추출하는 것으로, 각 무기 및 공격력에 대한 데이터 분석을 진행한다. 두 번째로 인공지능(AI) 알고리즘에서는 이미지를 인식하여, 이를 딥러닝(Deep Learning)을 진행하고, Fast R-CNN, OCR, Object Recognition을 진행한다. 마지막으로 학습결과생성은 전차, 무기, 함정, 항공기 등의 데이터를 토대로 학습 파이프라인과 인공지능(AI) 알고리즘 단계를 거쳐 Model을 만들고 Weight, Bias, Network를 진행한다. 위 세 단계를 거쳐 수집되고 정제된 데이터를 서비스 배포한다.

데이터 세트(Data Set)와 딥러닝 알고리즘(Deep Learning Algorithm) 단계를 거치면 온라인 시스템 및 사용자 화면을 통해 지휘, 피아식별 요청, 대응을 진행한다. 지휘결심 / 대응 단계에서 적 의도를 파악하고, 효과적인 타격체계를 산정하고, 타격 및 재 타격을 결정한다. 결정한 의견을 지휘통제실을 통해 전달하고, 피아 식별을 요청하면 딥러닝(Deep Learning)을 통하여 적 전차를 식별하고 어떤 무기체계를 가지고 있는지 분류한다.

객체인식 플랫폼은 적보다 먼저 보고, 먼저 대응을 결정하고, 먼저 타격함으로써 전투 승수 효과를 극대화하고, 적의 기동장비, 이동형 발사차량, 함정, 항공기 등의 표적 식별 객체 인식 체계를 구축한다.



〈그림 III-3〉 객체 인식(이미지, 영상, 음성 식별) 플랫폼

2) 사이버전 대비(해킹 침해사고 분석) 플랫폼

국방부는 인공지능(AI)기반 보안관제 및 침해사고 예방을 위한 종합분석 플랫폼 개발을 통해서 네트워크 보호대책, 사이버침해 조사, 분석, 사이버 위협 수집체계를 구축하였다.

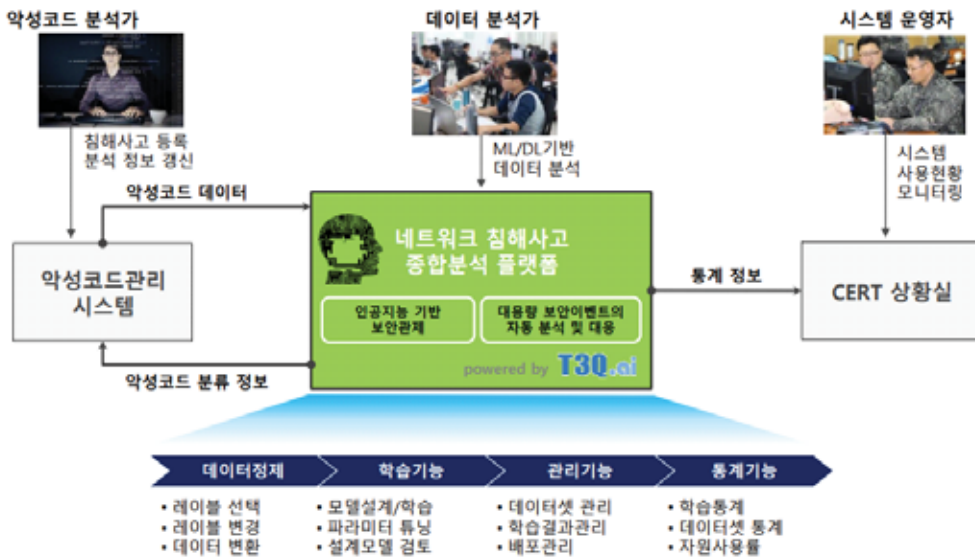
악성코드 분석가, 데이터 분석가, 시스템 운영자를 활용하여 각각의 업무를 분담하였다.

악성코드 분석가는 침해사고 등록, 침해사고에 대한 분석 정보를 갱신하며, 데이터 분석가는 ML/DL기반 데이터를 분석한다.

시스템 운영자는 시스템 사용현황을 모니터링하여 CERT 상황실에 보고하는 체계를 구축하였다. 악성코드 관리시스템을 통하여 악성코드 데이터를 네트워크 침해사고 종합 분석 플랫폼에 보내고, 네트워크 침해사고 종합분석 플랫폼에서는 악성코드 분류 정보를 악성코드 관리 시스템에 보내어 악성코드 분석가가 분석을 진행한다.

데이터 분석가는 네트워크 침해사고 종합분석 플랫폼에 ML/DL기반 데이터 분석을 전송하며, 네트워크 침해사고 종합분석 플랫폼은 모든 정보를 취합하고 통계를 내어 통계 정보를 CERT 상황실로 보내며, 시스템 운영자는 시스템 사용현황을 모니터링 한다.

사이버전 대비 플랫폼은 데이터 정제, 학습기능, 관리기능, 통계기능의 네 단계를 거친다. 데이터 정제 단계에서는 레이블을 선택하고, 레이블은 변경하고, 데이터로 변환한다. 학습 기능 단계에서는 모델 설계/학습, 파라미터 튜닝, 설계모델을 검토하며, 관리기능에서는 데이터셋 관리, 학습결과 관리, 배포관리를 진행한다. 마지막으로 통계기능에서는 학습 통계, 데이터셋 통계, 자원 사용률을 분석한다. 또한, 인공지능(AI) 기반을 통해 보안관계 및 침해사고를 예방하기 위한 종합분석 플랫폼으로, 네트워크 보호 대책, 사이버 침해 조사/분석, 사이버 위협 수집체계를 구축한다.



〈그림 III-4〉 사이버전 대비(해킹 침해 사고분석) 플랫폼

3) 시스템 관제(E2E, End-to-End) 플랫폼

국방부는 'T3Q.ai 플랫폼'의 빅데이터 부분을 적용하여 국방 시스템 인프라 관제체계 구축이 가능하도록 하였다. 즉, 주요 및 핵심 서버 장비 장애 예측, 사이버 침해시도 분석 등을 한눈에 알아볼 수 있는 시스템 관제 플랫폼을 구축하였다.

시스템 관제 / E2E(End-to-End) 플랫폼에서는 서비스 트랜잭션, 종합 상황 표시, 주요 비즈니스 트랜잭션, 도메인 처리 건수 & 평균 응답시간, 시스템 처리 건수 & 평균 응답시간, 채널별 유입 건수 트랜잭션, 통계 및 오류 모니터링 영역을 한눈에 파악할 수 있다.

서비스 트랜잭션에서는 각 시간별 서버 이용 현황을, 주요 비즈니스 트랜잭션에서는 고객 조회, 가입, 운영자 고객관리, 조회 및 처리 건수를, 도메인 처리 건수 & 평균 응답 시간에서는 각 요청 건에 대한 평균 응답시간, 시스템 처리 건수 및 평균 응답시간에서는 각 처리 건에 대한 평균 응답시간, 통계 및 오류 모니터링 영역에서는 최근 오류 및 최초 오류 발생 시스템을 한눈에 파악할 수 있게 지원해 준다.



〈그림 III-5〉 시스템 관제 / E2E(End-to-End) 플랫폼

4) 실시간 지능화 지휘통신망 통합 플랫폼

빅데이터(Big Data) 및 딥러닝(Deep Learning) 통합처리 국방망, 전장관리망, 통합 관리시스템에 적용가능 하도록 하였다. 즉, 국방망 및 전장관리체계망, 네트워크 장애

예측을 위하여 실시간 지능화 지휘통신망 통합 플랫폼을 구축하였다.

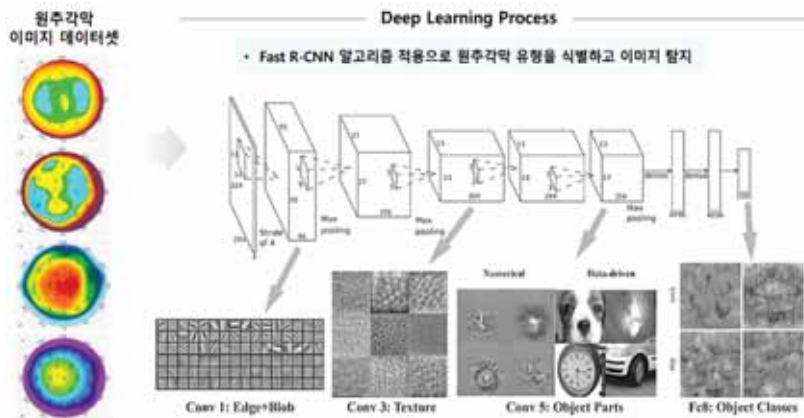
실시간 지능화 지휘통신망 통합 플랫폼은 국방망 관리시스템으로부터 수집되는 빅데이터 수집 / 분석, 반복적 딥러닝(Deep Learning)을 통한 망 운용 의사결정 지원 플랫폼을 구축하였으며, 실시간 지능화 지휘통신망 통합 플랫폼은 빅데이터를 기반으로 데이터수집 현황, 데이터 처리현황을 그래프화 하여 보여주며, 딥러닝(Deep Learning)을 기반으로 인공지능(AI) 학습 및 운용 데이터를 보여주며, 응용서비스를 통해 고장판단, 트래픽 예측, 고장원인을 분류한다. 각 서버에서 분석, 수집 / 저장단계를 거치며 데이터를 정제, 정밀화 하여 저장한다.



〈그림 III -6〉 실시간 지능화 지휘통신망 통합 플랫폼

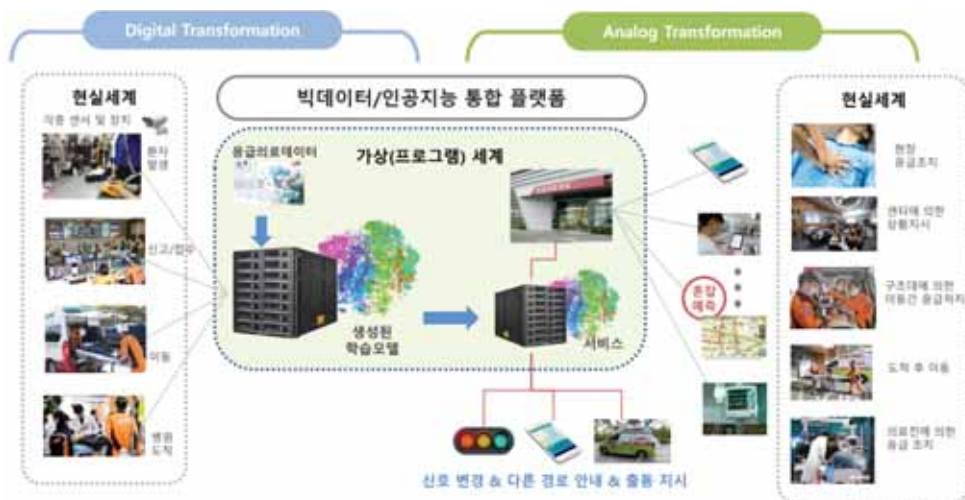
5) X-ray 및 응급환자처리 플랫폼

국방부는 딥러닝(Deep Learning) 기법을 활용하여 안과 원추각막 진단서비스를 구축 (의료 정보시스템)하였다. 군인들의 의료 정보시스템을 구축하고자 영상판독시스템, 다출처 영상 융합체계, 영상합성 생산 및 지원을 위한 응급환자처리 플랫폼을 구축하였다. 예로, 원추각막에 대한 의료 정보시스템은 원추각막에 대한 이미지를 데이터화하여, Fast R-CNN 알고리즘 적용으로 원추각막 유형을 식별하고 이미지를 탐지한다.



〈그림 III-7〉 X-ray 처리 플랫폼

또한, Digital Transformation과 Analog Transformation을 활용하여 응급환자 지원을 한다. Digital Transformation은 현실세계의 각종 센서 및 장치를 통해 환자 발생을 찾고, 신고/접수를 진행하고, 병원으로 이동 및 도착을 진행하여 응급환자를 처리한다. 이는 응급 의료데이터 수집을 하고, 생성된 학습모델을 통해 서비스를 제공한다. 서비스는 신호 변경 & 다른 경로 안내 & 출동 지시등의 서비스를 제공한다. Analog Transformation은 현실세계에서 현장 응급조치, 센터에 의한 상황지시, 구조대에 의한 이동간 응급처치, 도착 후 이동, 의료진에 의한 응급조치를 진행한다. 이를 통해 감시정찰, 지휘통제, 기동, 화력, 방호, 작전지속지원 등 다양하게 적용 및 활용이 가능하다.



〈그림 III-8〉 응급환자처리 플랫폼

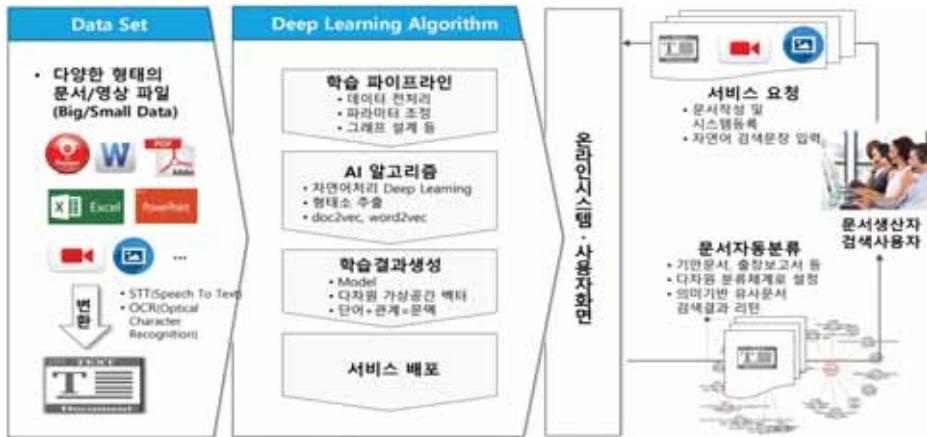
6) 전자문서 자동분류 플랫폼

국방부는 인공지능(AI) 기반 문서분류 자동화로 수작업 제거 및 업무에 필요한 정보검색 효율화를 추진하였다. 인공지능(AI)과 딥-러닝 알고리즘을 통해 기술도서 / 문헌 분류, 중요기록물 관리, 보고서 분류, 디지털 증거분석 자료 분류를 위하여 전자문서 자동 분류 플랫폼을 구축하였다.

Data Set, 딥러닝 알고리즘(Deep Learning Algorithm) 단계를 거쳐 온라인 시스템 / 사용자 화면에 제공하고, 온라인 시스템은 문서를 자동으로 분류하여, 문서 생산자 및 검색 사용자가 서비스를 요청할 시 사용자 화면에 제공한다.

Data Set 단계는 다양한 형태의 문서 및 영상 파일을 수집한다. 한글, 워드, ppt, excel, pdf, 이미지 파일, 영상파일 등의 모든 문서 및 영상파일을 수집 및 분석하여 STT (speech To Text), OCR(Optical Character Recognition)의 변환 단계를 거친다. 딥러닝 알고리즘(Deep Learning Algorithm)은 학습 파이프라인, AI 알고리즘, 학습결과생성, 서비스 배포 단계를 가진다. 학습 파이프라인에서는 데이터 전처리, 파라미터 조정, 그래프 설계 등의 작업을 진행한다. 데이터 전처리는 수집된 데이터를 분석하기 좋게 변형하고, 이를 토대로 파라미터 조정, 그래프 설계를 진행한다. 인공지능(AI) 알고리즘에서는 여러 종류의 문서 및 영상 파일에 대한 자연어 처리 딥러닝(Deep Learning)을 진행하고, 하나의 형태소를 추출한다. 이를 통해 doc2vec, word2vec의 자연어 처리과정을 진행한다. 학습결과생성은 각 추출된 데이터를 Model 화하고, 다차원 가상공간 벡터를 설정, 단어와의 관계를 통하여 문맥을 도출한다. 위 세 단계를 거쳐 수집되고 정제된 데이터를 온라인 시스템 / 사용자 화면에 배포한다.

온라인 시스템은 문서를 자동분류하며, 기안문서 및 출장보고서 등을 분류하며 다차원 분류체계로 설정하며 의미기반 유사문서 검색결과를 보여준다. 문서 생산자 및 검색 사용자가 서비스를 요청(문서작성 및 시스템 등록, 자연어 검색문장 입력)하면 도출된 검색결과를 사용자 화면에 서비스 제공한다.

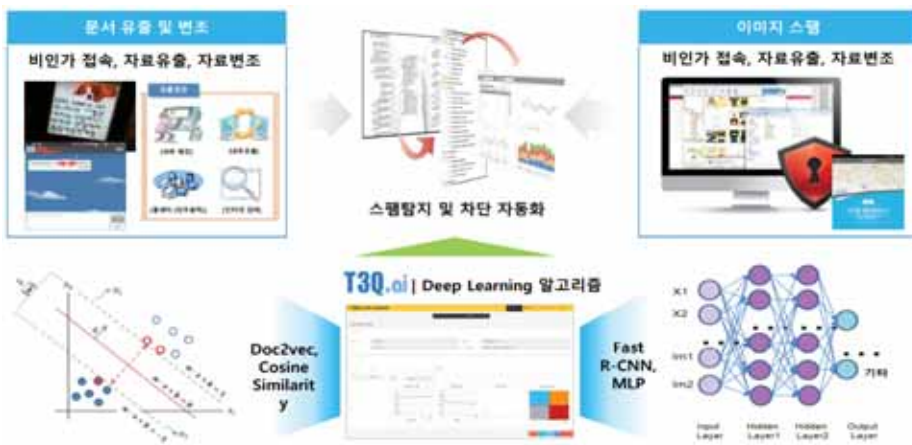


〈그림 III-9〉 전자문서 자동분류 플랫폼

7) 불법 스팸 식별 플랫폼

국방부는 인공지능망 모델개발 및 시스템 구축을 통한 비인가 접속, 자료유출 / 자료 변조 차단의 자동화를 구현하였다. 즉, 악성코드 분석, 정보유출 탐지 / 예측, 보안사고 탐지 / 분석체계 플랫폼을 구축하였다.

문서 유출 및 변조와 이미지 스팸을 방지하기 위해 비인가 접속 차단, 자료유출 차단, 자료 변조 차단시스템을 도입하였으며, 스팸탐지 및 정보 유출 차단 자동화를 구현하였다. 스팸탐지 및 정보유출 차단 자동화는 T3Q.ai / 딥러닝(Deep Learning) 알고리즘을 통하여 운영된다.



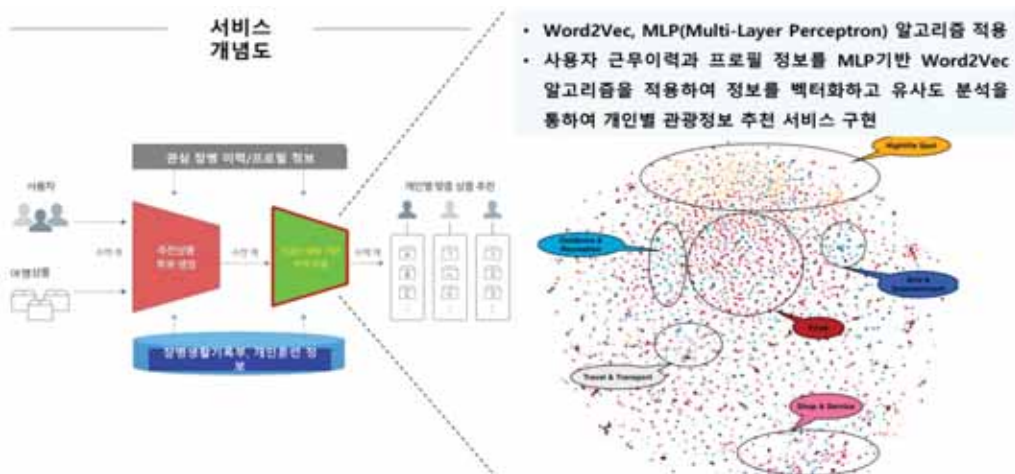
〈그림 III-10〉 불법 스팸(Spam) 식별 플랫폼

8) 장병성향 분석 플랫폼

국방부는 고객 성향분석을 위한 벡터화 및 다중신경망 기법을 적용하여, 맞춤형 장병 역량개발 서비스를 구축하였다. 즉, 병사들을 위한 병영상담, 맞춤형 리더십 역량개발, 맞춤형 개인 / 부대별 훈련체계 분석을 위하여 장병성향 분석 플랫폼을 구축하였다.

각 병사의 장병 생활기록부, 개인훈련정보를 통하여 각 개인에 맞는 훈련시스템 및 적응 프로그램을 진행하며, 개인별 맞춤 훈련을 추천한다. 또한, 각 부대별 훈련체계를 분석하여 적합한 훈련 방식, 전략 및 전술을 제공하여 효율적이고 적합한 훈련 시스템을 제공한다.

이는 인공지능망 기반으로 모델을 추천하며, Word2Vec, MLP(Multi-Layer Perceptron) 알고리즘을 적용한다. 병사의 근무이력과 프로필 정보를 MLP기반 Word2Vec 알고리즘을 적용하여 정보를 벡터화하고 유사도 분석을 통하여 개인별 맞춤 훈련체계 및 적응 프로그램 추천 서비스를 구현한다.



〈그림 III-11〉 장병성향 분석 플랫폼

9) 무인 잠수함 “씨 헌터”

미군과 미국방위고등연구계획국(DARPA)에서는 미국의 해군 전력 보강에 대한 대책 중 하나로 무인 잠수함을 개발하였다. 기존의 구축함으로는 대잠전 시행 시 하루 70만 달러(약 8억 3,300만원)의 비용이 소요되지만, 무인 잠수함을 활용할 경우 경우 1만~2만 달러(약 1,159만원~약 2,380만원)로 감소가 예상되고 있다. 〈그림 III-12〉에서와 같이 씨헌터(Sea Hunter)는 미국방위고등연구계획국(DARPA)의 ACTUV(AntiSubmarine Warfare Continuous Trail Unmanned Vesel) 프로그램을 통해 개발된 최초 무인 잠수함이다.

씨헌터는 2012년 탐색 개발을 시작으로 2014년 축소 모델의 실제 테스트를 진행하였으며, 2016년 4월 ‘씨헌터(Sea Hunter)’라는 이름으로 명명하였다. 개발사업자인 레이도스(Leidos)社에서는 2015년 초 13m 길이의 축소 모형 모델을 제작하여 미시시피주에서 테스트를 진행하였다.

미국방위고등연구계획국(DARPA)에서는 2010년부터 자율항행 무인수상 대잠전정(ACTUV, Anti-Submarine Warfare Continuous Trail Unmanned Vessel) 프로그램은 추진하였다. 이 사업은 적의 잠수함을 탐지하고 추적하기 위한 자동형 무인선박 기술개발 사업으로 전체 길이 40m, 무게 40톤으로 디젤 엔진 2개를 이용하여 발진하며, 장방형 모양에 선체 균형을 잡기 위한 한 쌍의 지지대를 배치하여 선체의 불안정성을 해소하였다. 3동선 선체로 디자인되어 안정성과 효율성, 속도를 모두 갖추었으며, 외양(外洋)에서도 잠수함의 추적이 가능하다. 또한, 자율항행시스템과 센서 등 다양한 소프트웨어와 자동 경고 방식 하드웨어를 탑재하여 다른 선박과의 충돌을 미연에 방지한다.

비밀리에 미국 영해에 침입하는 타국의 잠수함 탐지가 목적이며 별도의 무기는 탑재되어 있지 않다. 음향 항해 범위(SOund NAvigation Ranging), 즉 소나(Sonar)를 이용하여 저소음의 디젤 전기 잠수함을 자동으로 수천 km까지 추적하는 것이 가능하다. 2021년까지 서태평양 지역에 투입될 예정으로 잠수함에 투입되는 인력 및 구매 비용의 감소로 운영비용 절감이 예상되며 승무원의 교대가 필요 없기 때문에 잠수함 수색의 공백을 줄여주며, 입출항 빈도의 감소로 군사 작전의 효율성 향상도 기대되는 바이다.



〈그림 III-12〉 무인잠수함 “씨 헌터”

10) 인공지능(AI) 알고리즘으로 실종자를 수색하는 ‘쿼드콥터형 드론’

해마다 숲이나 산에서 사람이 실종되는 사례가 수십만 건 발생하고 있는 스위스는 산악 지역 복잡하고 넓은 특성으로 실종자의 조기 발견에 한계가 존재하였다. 이러한 문제점을

해결하고자 <그림 III-13>과 같이 드론을 활용하여 실종자 수색의 효율성을 높이고, 실종자 수색시스템을 고도화하기 위한 방안이 고려되었다.

산악지대에서 실종자를 수색하기 위한 인공지능(AI) 기반의 ‘쿼드콥터형 드론’은 스위스 취리히 대학과 이탈리아 델라스비제라 대학의 응용과학부, 남부 스위스 예술대학 연구자들이 공동으로 개발하였다. 연구진은 숲길을 자율적으로 인지하고 추적할 수 있는 소프트웨어를 개발하고 이를 드론과 결합하는 방식으로 드론의 활용범위를 산림과 같은 복잡한 지형까지 확대시킬 수 있었다. ‘쿼드콥터형 드론’은 카메라로 촬영된 숲길의 이미지를 인공지능(AI) 알고리즘을 통해 학습하였으며, 이를 기반으로 하여 실종자 위치를 파악하였다.

연구진은 헬멧에 장착된 카메라를 활용하여 스위스에 위치한 산림과 숲길의 이미지를 2만여장 촬영하고 지형 파악을 위한 데이터를 확보하였으며, 획득한 이미지를 드론에 내재된 딥 뉴런 네트워크 인공지능(AI) 알고리즘에 저장시켜 지속적으로 학습시킨 후 학습된 이미지를 분석하여 실종자 주변 환경에 대한 추적을 수행하였다. 현재까지 드론의 위치 추적능력은 약 85%의 정확도를 보이고 있으며, 이 결과는 사람의 정확도인 82%보다 약 3% 높은 수치이다.

딥 뉴런 네트워크(Deep Neural Network)는 경험을 통해 학습하는 인간의 뇌와 같이 복잡한 문제를 해결하기 위해서 경험을 통해 필요한 학습이 이루어지도록 설계된 컴퓨터 알고리즘의 일종으로 실종자를 식별하기 위해 드론 구조대에 실시간으로 해당 위치를 전송하여 신속한 구조 작업 구현을 가능하게 한다. 딥 뉴런 네트워크(Deep Neural Network)는 카메라로 촬영된 이미지 정보를 인공지능(AI) 알고리즘에 기반하여 학습능력을 통해 지속적으로 습득하고 학습함으로써 실종자의 정확한 위치가 빠른 시간에 식별이 가능하도록 하며, 실종자 수색과 구조 과정에 필요한 정보를 실시간으로 확보할 수 있어 구조대원들의 상황 판단 및 대처 능력 향상에 크게 기여한다.



<그림 III-13> 쿼드콥터형 드론

11) 인공지능(AI) 기술을 적용한 무인 항공기

미국, 유럽, 중국 등 주요국은 새로운 성장 동력이자 안전한 사회 구현을 위해 다음 <그림 III-14>과 같이 머신러닝(Machine Learning)을 활용한 데이터 기반 군사용 무인 항공기 기술 확보와 개발에 주력하고 있다. 미국 항공기 제조사 보잉의 CTO 존 트레이시도 과학기술의 발달로 항공기도 이제 날아다니는 컴퓨터가 되고 있다고 언급한 바 있다(서울대 강연, 2016. 4. 20).

미국방위고등연구계획국(DARPA)에서는 머신러닝(Machine Learning)을 기반으로 레이더 신호와 방해 프로파일 등에 효과적으로 대응할 수 있는 무인항공기의 개발을 추진하고 있으며, 미국 항공우주국(NASA)은 드론을 이용해 허리케인을 감시하려고 하며, 뉴욕시에서는 안전한 도시를 만들기 위해 드론으로 도심 전역을 살피겠다는 구상을 공개하였다. 중국은 2015년 8월부터 드론 개발 기술의 유출을 막기 위해 무인 항공기 기술을 금지시키고 있으며, 시속 12,240km 이상의 극초음속 드론을 개발하였다.

스위스, 프랑스 등은 안전에 필요한 항공 촬영과 데이터 작성이 필요한 분야에서 인공지능(AI) 무인 항공기를 이용하기로 하였다. 스위스는 페롯(Parot) 회사 고화질 카메라를 장착한 드론을 활용하여 광산 내부의 3D 지도를 제작하였으며, 이로 인해 광부들이 안전한 채굴을 할 수 있는 환경을 조성하였다. 프랑스는 EDF 에너지가 인공지능(AI) 기술이 탑재된 트림블(Trimble) 회사의 드론을 활용하여 핵발전소 건설을 위한 부지의 자료를 수집하고 있으며, 치안관리와 재해 예방, 수색, 사건현장 증거수집, 긴급 상황 대처 등 도시의 안전 관리 등 영역을 점차 확대하고 있다.

캐나다는 에드먼튼스에서 무인카메라를 장착한 드론을 도입하여 경찰이 교통사고 현장을 항공사진으로 촬영할 수 있도록하는 등 교통사고 현장조사에 직접 활용하고 있으며, 아랍 에미리트에서는 경찰 시스템 강화 및 긴급 상황 대처, 보안·안전 등 도시 정찰과 관리에 2010년부터 드론을 도입하여 활용하고 있다.

이처럼 이제 무인항공기는 인공지능(AI) 기술을 기반으로 향 후 군사 및 재난안전 등 안전한 사회를 구현하기 위해 핵심적인 역할을 수행할 것으로 기대되는 바이다. 이를 위해 무인 항공기에 대한 고도 및 용도 제한 등 제도가 보완된다면 보다 다양한 분야에서 활용이 확대될 전망이다.



〈그림 III-14〉 인공지능(AI) 기술 기반 무인항공기

12) 경비·보안 업무 수행 'K5'

미국 로봇 개발 스타업인 나이트 스코프(Knight scope)社에서는 방범용 로봇인 'K5'를 개발하였다(그림 III-15). 나이트 스코프의 공동 창업자인 윌리엄 산타나(Wiliam Santana)는 코네티컷주 초등학교에서 초등생 20명의 목숨을 앗아갔던 2012년 12월 총기난사 사건을 계기로 'K5'를 구상하게 되었다. 'K5'는 인구 이동이 많은 도심지와 쇼핑몰, 주차장 등 지역의 치안 업무를 보조하기 위해 광범위하게 사용될 것으로 기대하고 있다. 최근 들어 범죄행위가 더욱 다양화되고 지능화되면서 사회 안전 확보에 첨단기술과 장비를 활용한 과학적 대응체계의 중요성이 부각되고 있으며, 사회 안전망 구축을 위해 경비, 탐색, 범죄예방 등의 기능을 수행하는 치안 로봇 개발도 활발히 진행되고 있다.

'K5'는 카메라 및 각종 센서 등을 활용하여 순찰과 감시의 역할을 하고 있다. 고해상도 카메라를 활용해 주변을 실시간으로 감시하고 녹화할 수 있으며, 열감지기, 스피커, 냄새 탐지기 등을 갖춰 돌발적인 움직임이 포착되면 경비원을 호출하는 것이다. 2014년에 마이크로소프트(Microsoft)社에서는 4대의 'K5'를 도입하여 시설물 감시에 활용하고 있다.

또한 'K5'는 비디오 카메라, 모션 센서 등을 통해 획득한 데이터를 소셜미디어의 게시글과 비교 분석하여 범죄 위험수준에 대한 경고, 도난 차량의 위치파악, 지명수배자 검색 등을 수행할 수 있다. 'K5'는 1분에 약 30개의 차량 번호판을 판독하는 것이 가능하기 때문에 수배 중인 범죄자의 번호판이 감지되면 관련된 정보를 경찰에 전송해 추적업무에도 기여할 수 있으며, 센서를 통해 수집된 데이터는 소셜미디어의 게시글과 연관시켜 각종 범죄예방에 필요한 정보를 제공한다. 'K5'는 일정한 패턴이나 움직임에서 벗어난 정보가 식별되면 이를 스스로 학습해 상황 판단 능력을 제고 할 수 있는 자기학습 기능을 보유하고 있다. 'K5'가

수집한 데이터는 실시간 범죄 예측 네트워크 구축을 가능하게 하며, 센서를 통한 정확하고 신속한 대응으로 각종 사고 및 범죄의 조기 예방에도 기여한다. 다만, 로봇의 대체로 인한 사설 경비원의 일자리 감소 및 불특정 다수에 대한 감시체계 형성에 따른 사생활의 침해에 대한 우려도 공존한다.



〈그림 III-15〉 K5 방범용 로봇

13) 무인 자율 전투로봇

국방과학연구소가 구상 중인 ‘경 전투로봇’ 〈그림 III-16〉과 같이 원격 제어를 통해 임무를 수행하는 5t급 바퀴형으로 개발되고 있다. ‘경 전투로봇’은 지형 및 주행 정보를 사전에 입력한 뒤 원격으로 제어하면 스스로 경로를 분석하고 장애물을 피하면서 이동할 수 있는 기술이 적용된다.



〈그림 III-16〉 무인 경전투차량

특히 ‘경 전투로봇’은 적의 침투를 자동으로 탐지하여 경고하며 유사시에는 장착된 기관총으로 사격할 수도 있도록 개발된다. 양쪽으로 3개씩, 6개의 바퀴로 움직이며, 전면에 설치된 영상카메라로 통제소에서 전방에 있는 장애물이나 적을 실시간 확인할 수도 있다. 비무장 지대의 GP(소초)나 철책 경계 부대인 GOP(일반전초) 지역의 감시정찰, 기계화 부대의 수색 정찰용으로 우선 활용할 계획이며, 지뢰탐지나 화생방 탐지 등 다목적 용도로 활용될 수 있을 것으로 보고 있다.

이스라엘에서 개발한 무인지상 전투로봇(UGV) Guardium <그림 III-17>은 폭발물과 화학무기 탐지장치, 미사일 발사기, 기관총 등의 중무장을 하고 정찰 및 감시를 수행하며 103시간의 임무 수행이 가능하다. 2015년 중반 Guardium 플랫폼을 대체하는 Sergev UGV(완전 자율)을 도입하여 이스라엘 가자 지구 경계지역에 감시 정찰용으로 배치하였다. Sergev UGV(완전 자율) 인공지능(AI) 기능을 갖는 무인 자율 전투차량(로봇)은 목표지 자율 주행, 표적 자동식별, 자동 추적, 표적 정밀 타격, 화력 지원 등 다양한 유·무인 합동 임무를 수행할 수 있다.



〈그림 III-17〉 Guardium(Israeli UGV)

또한, 이스라엘 IAI사가 개발한 감시정찰 무인전투로봇 차량(UGV) RoBatle <그림 III-18>은 차량제어, 네비게이션, 자율주행, 센서 등으로 구성되어 있다. 모듈러 방식이며 작전에 따라 바퀴나 궤도의 선택이 가능하고 로봇 팔, 감시 센서, 원격제어무기, 레이더 등 탑재가 가능하다.

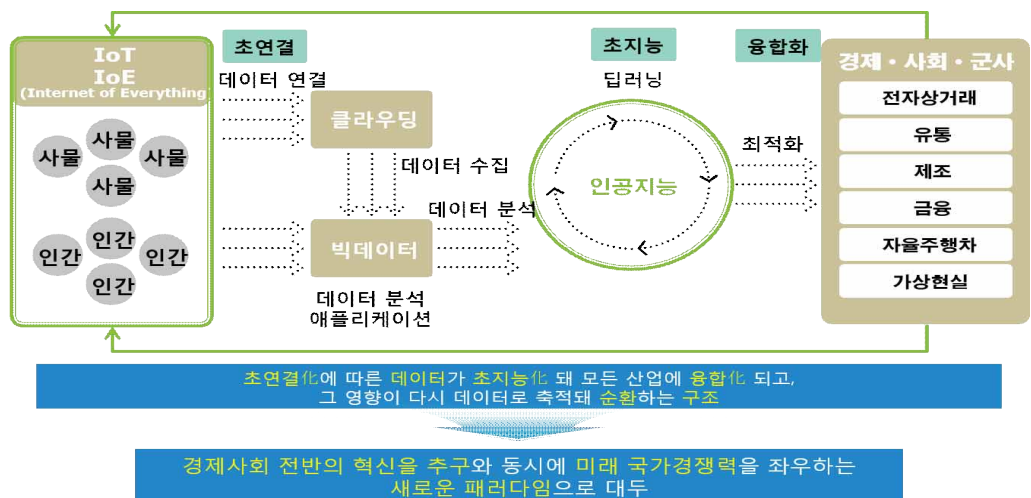


〈그림 III-18〉 RoBattle

2. 인공지능 시스템의 국방 분야 역할 및 실현

가. 인공지능(AI) 기술의 국방 분야 적용 필요성

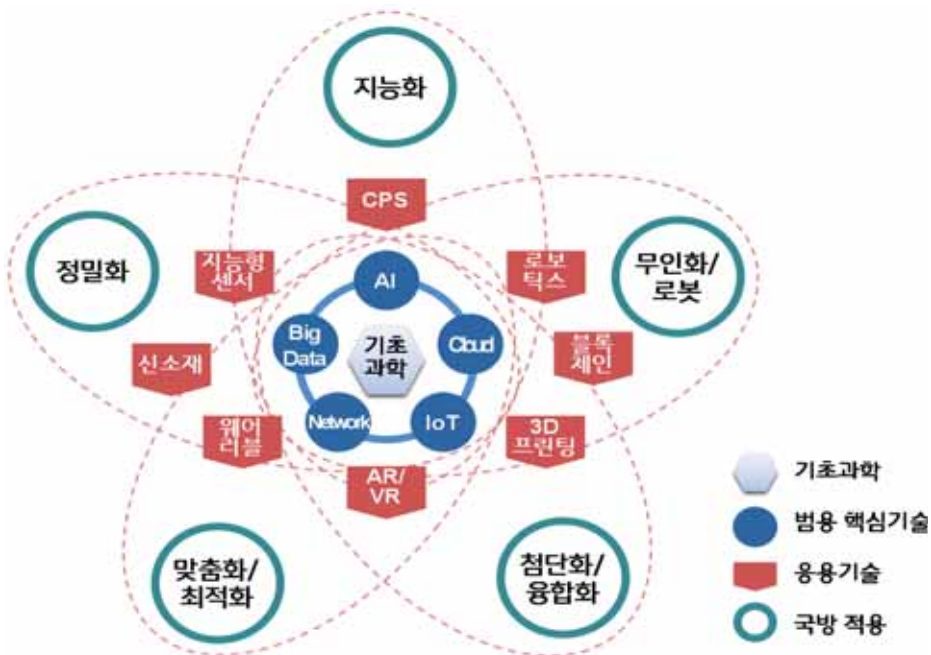
현 우리 군은 국가전환전략과 4차 산업혁명 스마트 국방혁신 추진계획을 연계한 첨단·과학화 군 건설과 국방운영의 효율화를 촉진하고자 하고 있다. 4차 산업혁명으로 정보통신기술(ICT)이 모든 산업으로 스며들면서 산업 생태계를 변화시키면서 제조·서비스 등 민간부문 뿐만 아니라 행정·국방 등 공공부문에 이르기까지 국가 인프라 시스템 개조 및 지능정보사회 실천전략으로 가고 있다.



〈그림 III-19〉 대한민국 국가 전환 전략(IDX)

4차 산업혁명 기반의 국방혁신 범위는 4차 산업혁명의 범용 핵심기술과 분야별 응용 기술을 활용하여, <그림 III-19>와 같이 국방 분야별 지능화, 무인화, 정밀화, 맞춤형, 첨단화 추구하고자 하고 있으며, 이를 위해서는『국가 전환 전략』및『국방혁신 추진계획』과 연계한 추진전략 필요하다.

즉, 국방개혁 2.0 추진과 연계하여 4차 산업혁명 핵심기술을 군 운용환경에 적용하여 ‘병력 위주의 양적 군 구조’에서 ‘정보·지식 중심의 질적 군 구조’로 전환되는 시대적 흐름에 대비해야 한다. 최신 정보통신기술(ICT) 신기술을 교육훈련, 경계작전, 장비관리 등 부대운영 전반에 적용하여 병력 감축, 부대 수 감소, 병영기간 단축에 따른 부대운영 공백 대비와 작전활동, 교육훈련 여건을 보장 필요하다.

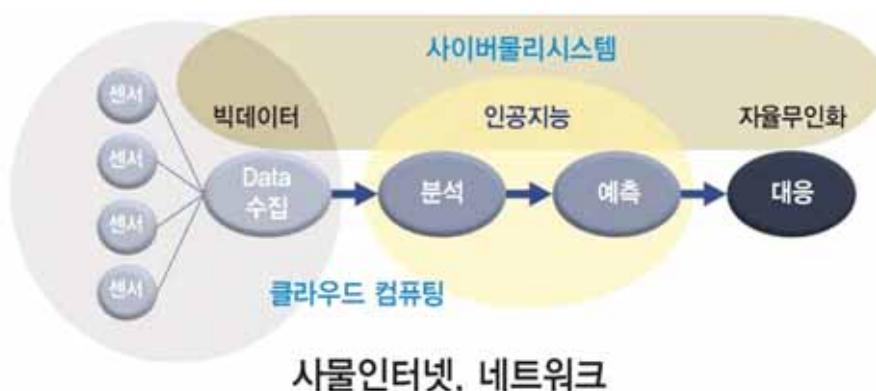


〈그림 III-20〉 국가 전환전략과 연계한 국방혁신 추진분야

이에 일환으로 4차 산업혁명 시대 초연결 육군 구축을 위한『첨단 ICT 신기술 軍 적용』 추진 계획과 연계한 통합적 관점의 스마트 부대 구축을 추진 중에 있으며, 4차 산업혁명 주요 핵심기술(AICBM¹³⁾) 기반의 스마트부대 구축을 통하여 경계 강화, 교육훈련 여건 보장 및 장병들의 안전·복지 증진, 국방자원(장비·물자·시설 등) 분야의 운영 및 관리

13) 4차 산업혁명의 대표적인 기술로서 AI(인공지능), IoT(사물인터넷), Cloud(기반 데이터 관리), Big Data (빅데이터), Mobile(모바일) 등을 통합하여 지칭

효율성 극대화하고자 하고 있다.



〈그림 III-21〉 4차 산업혁명의 핵심기술

미래창조과학부에서는 4차 산업혁명의 핵심기술로 인공지능(AI)+ICBM¹⁴⁾을 고려하고 있으며, 국방부에서도 이를 군사력 증강 및 국방경영개선에 활용하기 위해서 분야별로 연구를 진행하고 있다.

2016년 알파고와 인간의 바둑 대결을 지켜보며 사람들의 인공지능(AI)에 대한 관심과 충격이 증대하였다. 이처럼 4차 산업혁명 도래에 따른 인공지능(AI)과 자율주행, 데이터 사이언스 등의 기술 파급력은 사회적 충격뿐만 아니라 국가 간의 군사적인 불평등 격차를 심각하게 벌리고 있다. 4차 산업혁명의 파괴적 영향력은 1차 산업혁명보다 10배 더 빠르고, 300배 더 크고, 3,000배 더 강하다고 할 수 있다.

2012년 5월 미국 네바다(Nevada)주에서 스스로 운전이 가능한 무인 자동차(Driverless Car)에게 운전면허증을 발급하였으며, 현재는 상용화 수준(Lev. 4)에 근접하고 있다. 무인 자동차, 무인 항공기, 무인 로봇 등 다양한 분야에서 최근 전 세계적으로 선보이는 무인 장비들은 단순히 인간을 대신하는 기계가 아니라 사람처럼 스스로 인식하고 판단하는 기술을 바탕으로 하며, 이것이 바로 인공지능(AI)의 핵심기술이다.

과거 대부분 기술은 미 국방부에서 나왔다고 할 수 있으나 지금은 민간에서 더 많은 첨단기술들이 쏟아져 나오고 있다. 그 결과 미국과 경쟁국들 간의 기술적 격차가 급격하게 줄어들면서 그동안 미국이 누려왔던 기술적 우위의 강점 또한 상실되고 있다. 이를 만회하기 위한 전략이 제3차 상쇄전략(offset strategy)이며 이는 국방에 있어서 4차 산업혁명이라 할 수 있을 것이다.

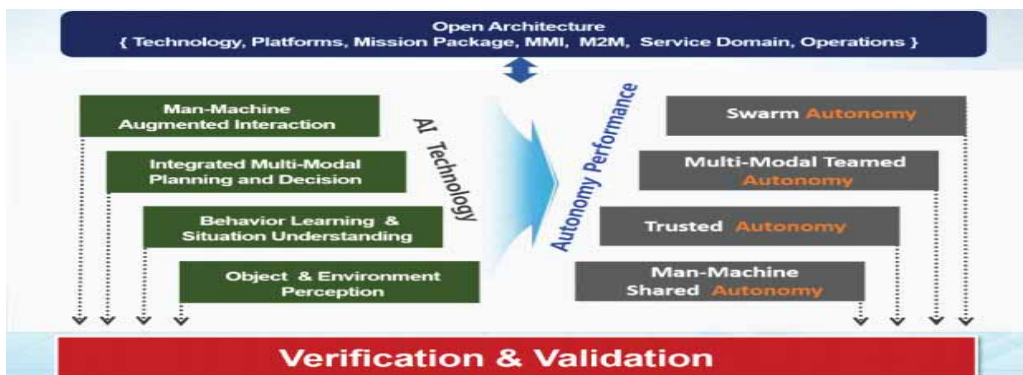
14) ICBM : 사물인터넷(IOT), 클라우드(Cloud)컴퓨팅, 빅데이터(BigData), 모바일(Mobile)

〈표 Ⅲ-2〉 상쇄전략 단계

구분	1차 상쇄전략	2차 상쇄전략	3차 상쇄전략
시기	1950년대	1970년대	2014년 ~
주도자	아이젠하워 대통령	브라운 국방장관	척 헤이글 국방장관
주 대상	소련	소련	중 + 러 + 다양한 적 상정
중점투자	전략 핵무기	정밀타력 유도무기	무인자율
작전개념	대량 보복	효율적 전력투사를 통한 공지전	효율적 협력을 통한 통합전
주요내용	1950년대 구상되었음 - 당시 유럽에 대한 구소련의 재래식 공격을 억제하기 위해 전략 핵무기의 능력을 발전시켰음	1970년대 발전되었음 - 구소련이 전략 핵능력을 보유함에 따라 새로운 억제력으로서 오차를 허용하지 않는 정밀유도무기를 개발	2016년부터 투자 하여 2030에 가시적 성과 예상 - 다양한 현-미래 위협에 효과적 대응 목표

제3차 상쇄전략의 핵심은 냉전시대와 달리 속도와 민첩성을 강조하고 있다. 혁신을 누가 더 빨리 하느냐에 따라 게임 체인저(Game Changer)가 되고 있으며, 변화를 주도하는 핵심기술에는 인공지능(AI)과 자율(AI & Autonomy), 사이버(Cyber), 로봇(Robotics), 데이터 사이언스, 전자전, 수중전 등이 포함된다. 전략식별은 최근 기술 및 학제간 융합과 Emerging 혁신기술기반 새로운 능력의 달성이 필요하며 궁극적으로 인공지능-자율화(AI-Autonomy)를 구현하는 것이다.

제3차 상쇄전략의 개념은 효과적, 경제적이며 상대방이 감당하기 불가능한 상쇄능력을 확보하는 것으로 궁극적인 토폴로지는 스웜(SWARM) 형태라 할 수 있으며, 이를 달성하기 위한 방법은 인공지능(AI)을 기반으로 하는 다수 자율무기의 융합(Teaming & Swarming)과 사람지능의 결합으로 달성할 수 있다. 아래 그림은 미 국방부의 3차 상쇄전략 기능 개념으로 결론적으로 자율화(Autonomy)라 할 수이다.



〈그림 Ⅲ-22〉 미국의 3차 상쇄전략 기능 개념

우리나라는 주적인 북한군과 잠재적인 경쟁국인 중국, 일본과 발생할 수 있는 갈등을 지속적으로 준비해야 한다. 전쟁을 수행하기 위한 전략이 병력 수, 무기 수준, 이를 운용할 수 있는 능력이라고 할 때 병력 수는 이미 고정되어 있기 때문에 무기 수준을 첨단화하여 병력 수의 열세를 만회하여야 할 것이다. 지금까지 첨단 무기는 동맹국인 미국의 도움을 받았다고 할지라도 앞으로의 첨단 무기는 인공지능(AI)을 기반으로 만들어지기 때문에 반드시 우리의 힘으로 만들어야 한다. 특히 인공지능(AI) 기술인 딥러닝(Deep Learning)은 반드시 데이터나 영상을 학습해야 되기 때문에 우리 영토에서 전투시 우리의 힘으로 만든 인공지능(AI) 기술로 우리나라의 지형을 토대로 수집된 데이터를 장병들이 사용한다면 우리가 항상 우세할 수 있을 것이다.

최근 IT 기술의 발전과 더불어 인공지능(AI)은 스마트 기기와 연결된 여러 분야에서 가시적인 성과를 나타내고 있으며, 국방부에서도 국방 분야의 인공지능(AI) 기술 적용을 위해 미래부 산하 지능정보추진단이 국방 분야에 우선 적인 사업추진을 통해 미래전장에 필요로 하는 여러 차세대 핵심기술을 연구개발로 추진 중에 있다.

따라서 이제는 군사력 증강, 국방경영개선 등의 국방 분야에서 인공지능(AI) 산업발전 및 기술개발을 위한 다양한 정책 마련과 정책을 실현하기 위한 지원 방안 마련이 필요한 시점이라고 판단되며, 특히 국방 분야에서의 인공지능(AI)을 활용과 적용하는 방안에 대한 연구가 반드시 필요하다.

나. 빅데이터(Big Data) 분석기술의 국방분야 역할 및 실현

빅데이터는 미국, 일본, EU 등 주요국들의 경우 이미 국가 차원에서 활용을 독려할 정도로 매우 관심이 높은 분야이며, 다양한 정책적 활용을 위해서 공공분야 및 민간분야에 까지 개방되어 가는 추세이다. 미국의 경우 빅데이터 이니셔티브를 통해 공공정책의 각 분야에 빅데이터 분석을 확산하여 국가적인 난제들을 해결하고 있으며, 최근 우리 정보에서도 정부 3.0 비전을 발표하면서 데이터 기반의 과학적 정책수립에 나서기 시작해 6대 분야에서 21개 빅데이터 관련 시범사업을 추진할 예정이다.

싱가포르는 2004년부터 '국가 위험관리시스템'을 구축하여 테러, 금융위기 등 국가차원의 위험·기회요인을 선제적으로 대응하고 있으며, 해상테러 의사결정 지원, 조류독감 위협 수준 평가 및 대응 방안 마련 등에 적극 활용하고 있다. 구글은 오바마 정부의 노후 차량 보상 프로그램의 호응도를 검색 통계방법을 이용하여 분석하여 정부 예산이 부족할 것이라는 것을 예측하였다. 이를 통해 미국 정부는 새 차 구입 수요에 대한 기존 예산을 뒤엎고 추가자금을 편성하였다. 이처럼 빅데이터는 국가와 기업적 차원에서 정책적으로

활용되며 긍정적 평가를 받고 있다.

국내에서는 2011년 중반부터 빅데이터에 관한 논의가 본격화되었으며, 2012년 말 ‘빅데이터 마스터플랜’을 통해 구체화되었다. 빅데이터 마스터플랜 안은 사회현안의 선제적 해결, 맞춤형 대국민 서비스, 데이터에 기반한 정책수립 지원, 빅데이터 신 성장동력 창출 등을 목표로 하고 있으며, 기반 조성을 위해 2017년까지 4개 영역 12개 세부과제를 정하고, 정부와 민간이 총 5,000억 원을 투입하였다. 권익위원회의 경우 2011년부터 각 부처의 온라인 민원정보를 수집하여 관리하고 분석하고 예측하는 민원정보 분석시스템을 구축하여 운영하고 있으며, 사회문제로 확산될 수 있는 민원을 사전에 파악하기 위해 주요 이슈에 대한 국민의 의견을 분석하고 경보, 예측하는 체계를 구축하였다.

국방 분야에서 빅데이터가 활용되기 위해서 선결해야 하는 과제들도 많다. 먼저 데이터를 활용할 수 있는 기반 조성이 필요하며, 활용전략과 정책도 수립해야 한다. 우리 군에서의 활발한 빅데이터 활용이 가시화될 것을 기대하며, 구체적인 활용방안에 초점을 두고 기술하고자 한다.

1) 빅데이터를 활용한 국방정보 분야의 각국 동향 예측

미군은 국방 분야에서 빅데이터의 활용을 위해 매년 2억 5,000달러 이상을 투자하고 있다. 이는 빅데이터의 국방 분야 활용 능력을 높이 평가하고 있다는 증거이며, 빅데이터가 국방 분야에서의 효과성을 입증했다는 것을 의미하기도 한다. 미군은 빅데이터를 잠재적인 위협 방어에 활용하고 있을 뿐만 아니라 방대하고 다양한 데이터를 분석하여 물리적인 공격뿐만 아니라 가상 세계의 사이버 공격에도 적극적으로 대비하고 있다.

미군은 정보 분석가를 활용하여 주기적으로 이메일과 휴대폰 사용기록, 언론 기사, 동영상, 음성대화 발췌 데이터를 분석하고 있다. 미군의 이러한 빅데이터 활용은 우리 군에도 많은 시사점을 주고 있다고 할 수 있다.

과거 2차 대전에서 당시 강한 전투력을 발휘하고 있던 독일군을 압박할 수 있었던 계기 중의 하나도 빅데이터의 패턴분석을 들 수 있다. 패턴 분석을 통해 수많은 숫자의 조합으로 이루어진 독일군의 암호를 해독할 수 있었으며, 이를 통해 상대의 전술을 역이용했던 연합군의 전술이 없었더라면 독일군의 U-boat는 연합군에 큰 위협요인이었을 것이다.

이와 마찬가지로 인터넷 상에서 매일 북한과 관련한 방대한 데이터가 생성되고 있는데, 이러한 데이터들을 수집하고 패턴을 정밀하게 분석한다면 북한의 군사적 행동에 대해 우리 군이 미리 예측하고, 충분한 대비를 할 수 있을 것이다. 실제로 북한의 군사기지나 주요 시설물들이 위치한 곳을 구글의 구글어스(위성 지도 프로그램)를 이용하여 찾아내어

이에 대한 정보를 공유할 수 있을 뿐만 아니라 북한의 주요시설 주변 부대 및 장비들의 이동을 분석하여 그들의 전술활동 반경과 핵실험 동향 등도 쉽게 파악할 수 있다. 최근 우려감이 높아지고 있는 EMP(전자기펄스)공격 분석을 위한 전자파 분석에도 빅데이터의 역할을 절대적으로 필요하다.

이러한 자료들을 기반으로 다양한 군사정보를 결합하고 정제 과정을 거쳐 분석한다면 신뢰성 있는 군사정보의 획득이 가능하다. 이렇게 획득된 정보는 시뮬레이션을 통해 적의 도발 징후가 일어나는 패턴이나 군사 동향에 대한 의미있는 정보를 재생하기 때문에 북한에 대한 우리 군의 전략우위를 통해 군사 작전에 크게 기여할 것이다.

2) 부대관리 측면에서 SNS 분석을 통한 군 홍보 및 CRM(Customer Relationship Management)

우리 군은 대외 이미지 향상을 위해 '진짜 사나이'와 같은 군 관련 프로그램, 다양한 민간 초청 부대개방 행사 등을 추진하고 있다. 군은 다양한 행사를 추진하며 국민에게 강하지만 친근한 군대의 이미지를 쌓아가기 위해 노력하고 있지만 예상치 못한 주변 반응으로 인해 예산과 인력 소모만을 초래하는 경우도 다수 발생하고 있다.

이에 육군에서는 홍보 효과를 극대화하기 위해 현재 빅데이터와 관련된 SNS 모니터링 분석 서비스를 도입하여 운영하고 있다. 육군 관련사항을 실시간으로 모니터링하고 여론의 동향을 파악하여 다양한 상황에 신속하게 대처하고 있으며 의도치 못한 불이익을 받지 않도록 모든 공보상황과 여론의 움직임을 주의깊게 파악하고 있다. 기존에는 주로 신문, 주·월간지 등 오프라인이나 방송으로 여론을 분석하였으나 현재는 트위터, 블로그, 카페, 페이스북 등 온라인 상에서의 주요 이슈와 논란이 되었던 모든 상황을 종합하여 분석하고 향후 언론 동향에 대해 미리 예측하기에 이르렀다. 현재 육군 정훈공보실에서 실시하는 대국민 여론조사는 온라인 여론조사, 그룹심층 토론(FGI), 빅데이터 분석을 포함한 종합적이고 구체적인 결과를 얻어내고 있다. 이는 홍보과에서 실시하고 있는 기획 홍보 및 홍보 활동의 분석에도 매우 유용하게 활용되고 있다. 또한, 자체 제작한 동영상이나 웹툰, 웹진 등 홍보활동에 대한 피드백을 특별한 절차없이 분석이 가능하며, 군 관련 프로그램에 대한 국민의 의견도 즉각적으로 얻을 수 있다.

특히, 2020년 국내 스마트폰 사용자 5천만을 넘는 시대에 군 홍보활동은 SNS 활용을 통해 이루어질 수 있다. 군의 수요자인 국민이 믿고 신뢰하는 군의 이미지 메이킹을 성공적으로 이끌어 냈을 때 바람직한 민군관계가 성립될 수 있을 것이다.

3) 군 보급품의 재고관리에 있어서의 빅데이터 활용

군수분야에서도 빅데이터를 활용할 수 있다. 우리 군은 해마다 약 8조 원이 넘는 예산으로 보급품을 유통하고 있지만, 군의 물류 시스템은 민간업체나 선진국에 비해 발전이 매우 미진하다. 기업의 물류환경은 사회와 기술 환경의 변화로 인해 고객 중심적이며 정보 중심적, 통합적 성격으로 점차 변화되고 있을 뿐만 아니라 기업 경쟁의 원천으로서 물류의 중요성이 더욱 부각되고 있다. 이미 많은 기업에서 빅데이터 자산관리시스템을 통해 자신들의 보유 자산을 전산화하는 작업을 진행하고 있으며, 성공적으로 안정궤도에 올려놓은 기업들은 전자상거래 및 물류와 유통경쟁에서 비교우위를 차지한 선두주자로 자리매김하였다.

이에 우리 군에서 물류환경에 적응하고 예산을 보다 효율적으로 사용하기 위해서는 이러한 물류 시스템에서의 빅데이터의 활용이 매우 필요하다. 군 유통관리의 목표는 최소의 물자로 최대의 국방력을 발휘하는 데 있으며, 이를 위해 필요한 물자를 필요한 장소와 시간에 신속하고 정확하게 보급하는 것이 최선의 방법이라 할 수 있을 것이다. 국방력 강화를 위한 필요물자들은 통상적으로 정확한 수요예측을 필요로 하며, 이러한 수요예측은 각종 데이터를 기반으로 정확성을 높일 수가 있을 것이다.

육군훈련소는 정확하고 신속한 피복 보급을 위해 유비쿼터스 기반 훈련체계를 구축하였으며, 훈련병이 측정장비에 올라가면 자동으로 신체 치수를 측정하는 시스템을 마련하였다. 측정 시스템에 의해 측정된 훈련병의 신체 치수는 전산화되며 자동으로 훈련소 인트라넷 서버에 저장되고, 저장된 훈련병의 신체 치수는 향후 보급품 분배에 있어 물류 시스템의 효율성을 높일 수 있는 빅데이터로 가치가 있을 것이다.

따라서, 우리 군에서도 기업과 같이 빅데이터 자산관리시스템을 적극 활용하여, 보급품이 적절한 시기에 보급되고 수리가 이루어지도록 효율화한다면 수월한 재고관리와 물류 시스템의 비약적 개선이 가능해질 수 있을 것이다.

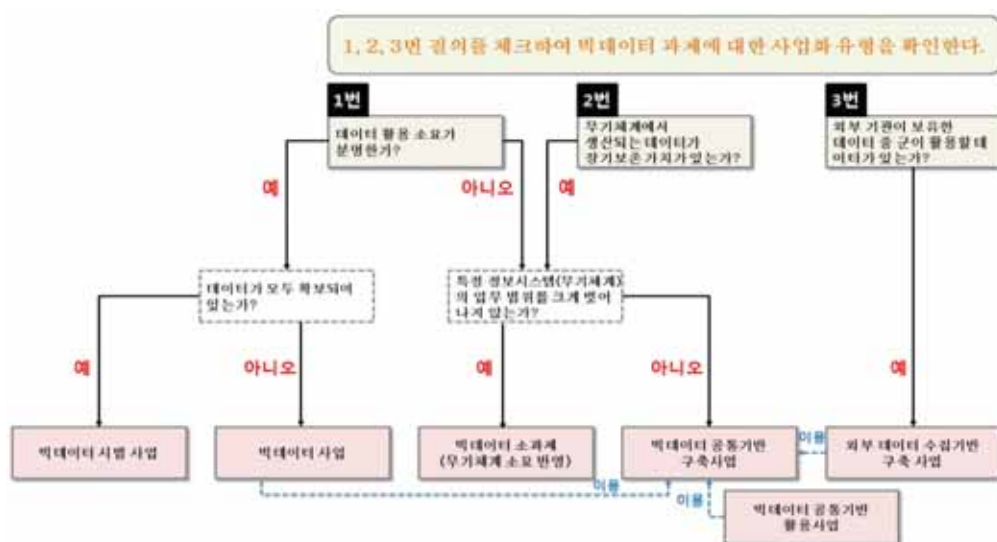
4) 빅데이터 도입 사업관리¹⁵⁾

우리 군의 데이터 관련 정보화 사업 분야로는 DB 구축, M&S, 그 외 신규 시스템 구축 또는 개선 사업 등이 있다. 하지만 빅데이터는 기존에 축적되어 있거나 수집 가능한 데이터를 2차적으로 분석하여 활용한다는 점에서 자료를 단순하게 DB화하는 DB 구축 사업과는 차별화 된다. 빅데이터는 예측 기능 측면으로 M&S와 특성이 유사하며, M&S 체계의 가상 입력 데이터 또는 산정지수 등을 빅데이터 또는 빅데이터 분석을 통해 산출

15) 김형주 외, 국방분야 빅데이터 활용 방안, 한국전략문제연구소, pp. 67~70, 2013. 11

되는 정보로 대체함으로써 산출되는 정보를 개선할 수 있다. 빅데이터 분석 또한 M&S 체계의 논리를 활용(참조)하여 설계가 가능하지만, 빅데이터 기술이 주로 불확실한 연관 관계를 다루기 때문에 논리체계가 없을 수 있다는 점은 반드시 유의하여야 할 것이다.

현행 국방 분야의 빅데이터 도입 절차는 ‘과제 발굴’, ‘과제 선정’, ‘사업계획 및 시행’ 등 크게 3단계로 정의되며, 업무부서나 업무담당자는 현재 발생하고 있는 문제, 업무 개선 사항, 필요한 예측 등을 인식하고 관련 데이터를 확인한 후 후보 과제를 발굴하고 있다. 하지만 빅데이터 전문 조직이 구성된다면 해당 조직 내에서 내부 데이터 현황과 흐름을 분석하고 외부 모범사례 등을 참조하여 보다 효과적으로 과제를 발굴할 수 있을 것이다. 이렇게 발굴된 과제로 국방 분야에 구현이 가능한 빅데이터 사업 과제를 선정하고 과제 선정 시 <그림 III-23>와 같은 기준에 따라 분류하여 사업 방식을 확정하고, 선정된 과제에 대해서는 사업화 당해 연도에 사업계획서를 작성하여 시행하여야 한다.



<그림 III-23> 빅데이터 사업화 분류 기준

<표 III-3> 빅데이터 사업화 유형

구 분	사업화 유형(방식)	설명
단일 업무 환경	빅데이터 시범사업	분석 논리와 데이터가 확보되어 소규모 투자(PC급 서버)로 가시적인 성과가 도출될 수 있는 사업
	빅데이터 사업	특정 분야에 업무 개선 또는 결과 데이터 산출 요구가 분명하여 단계별 신중한 추진이 필요한 사업(하나의 체계로 사업 추진) (사전 타당성 연구, 개념연구, HW도입, SW개발)

구 분	사업화 유형(방식)	설명
융합 환경	빅데이터 소과제	정보시스템 구축/개선/유지보수 사업 중 빅데이터 활용 관련 하위 과제
	무기체계 데이터 장기 저장 기반 소요 반영	무기체계 획득 시 해당 무기체계에서 생성되는 데이터를 장기 보존할 수 있는 기반에 대해 추가 소요 반영
	빅데이터 공통기반 구축사업	빅데이터 분석을 위한 데이터 수집 및 융합 인프라 구축사업 (대규모 부대/기관별 추진)
융합 환경	공통기반 활용사업	공통기반 등에 수집된 데이터를 활용하여 결과를 산출하는 SW개발 사업
	외부 데이터 수집기반 구축 사업	군 관련 외부 데이터 수집 저장 기반 구축 사업 (공통기반 연계를 통해 군내 데이터와 융합 활용)
기타	민간 사업	군 외부의 군 관련 데이터, 군에서 개방한 데이터를 융합 활용한 사업

다. ICT/IoT 기술의 국방분야 역할 및 실현

국방 분야의 경우, 미래 전장상황에 대비하고자 미국은 다양한 정보통신기술(ICT) 기술을 활용하여 통합관리체계 구축을 추진하고 있다. 미 육군은 개인 전투원과 무기체계를 하나의 사물인터넷(IoT) 네트워크로 연결하여 필요한 정보를 공유하고, 각 장비로부터 종합된 정보를 바탕으로 자동화된 결심지원체계 구축하고 있으며 미 공군은 탄도미사일방어 시스템을 중심으로 다수의 군사자원을 통합하고 최종적으로는 전 세계 군사자원을 통합이 가능하다고 판단하여 관련 연구를 진행 중에 있다. 미 DARPA(국방고등연구기획청)는 사물인터넷(IoT) 기술을 보안 네트워크에 적용할 수 있는 방안을 찾고 있으며, 방사능 물질이 들어있는 폭탄, 방사능 오염을 측정하기 위한 스마트폰형 소형 단말기 개발 등을 연구 중에 있다.

미 육군 연구소(U.S. Army Research Laboratory)의 kott 등은 사물인터넷 기술을 활용한 IoBT(전장 사물인터넷)를 정의하였다. IoBT는 말 그대로 전장 공간에서 흔히 이용 가능한 사물들을 상호 연결해 데이터를 수집·활용하는 것을 말한다. IoBT 환경이 구축 되면 초소형 센서 및 카메라를 통해 주변 환경의 데이터를 수집하고 머신러닝(Machine Learning) 기술을 적용하여 전장 상황을 지능적으로 인식하거나, 무인 항공기에 IoBT와 빅데이터, 인공지능(AI) 기술을 결합해 자율임무를 수행하는 등의 전장개념을 제시할 수 있다. 또한, 국방기술품질원이 발간한 ‘4차 산업혁명과 연계한 미래국방기술’에서는 첨단 기술의 도입, 군사적 위협, 미래 군 작전환경의 변화를 분석해 주목해야 할 사물인터넷(IoT) 관련 기술로 『지능형 전장환경 인지기술, 지능형 고신뢰성 사물연결기술, 생체신호 기반 원격제어기술, 내환경성 기반 지속적인 근접 통신 지원기술』을 제안했다. 이러한 기술을 기반으로 적의 동태를 파악할 수 있는 복합센서 기반의 지능형 무인 감시정찰체계와

이종의 통신자원 및 통신체계간 네트워크 환경을 지능적으로 인지·탐색해 초연결형 네트워크를 형성하는 최적의 C4I 체계를 구축할 수 있다. 사물인터넷(IoT) 기반 웨어러블 기기를 활용하면 병사의 병력 이력 추적, 체력관리, 훈련 중 응급체계 구축도 가능하다. 또한, 자동으로 총기·탄약 현황을 관리하는 위험·보안구역 관리체계, 공군 조종사의 피로 상태와 원인을 진단하고 이에 따라 출격시간을 조절하는 출격시간 조정체계 등 다양한 전력지원체계와 연계할 수 있다.

정보통신기술(ICT) 기반 기술 발달의 대표적인 참여형 콘텐츠 기술인 혼합(Mixed Reality)현실 기술은 인간의 인지능력을 현실과 가상공간에서 체험하고 감성으로 확장시키면서 오락, 문화, 교육, 의료 및 국방 등 다양한 분야에 제공되고 있다. 혼합(Mixed Reality)현실 기술은 사용자 웨어링(User Wearing) 형태로 인체에 착용하면 컴퓨팅 행위가 가능하게 되면서 체험 분야의 다양한 서비스로 확산되며, 정보의 이용 소통방식의 변화를 주도하고 있다¹⁶⁾.

정보화된 미래의 국방 응용 분야에서는 홀로렌즈 또는 HMD(Head Mount Display)를 어떻게 적용할 것인가에 대한 방안에 관심이 증가하고 있다. 대표적인 국방산업의 응용으로 현실세계의 지형지물을 전장에서 전자공간에 투사(Projection)하여 현실세계가 전자화된 제3의 공간이 있다. 즉, 전자공간 인식 및 증강(AR)현실을 통해 혼합(MR)현실 디바이스에서 플랫폼 응용기술을 활용하여 지능화된 주위환경인 건물, 도로, 나무 및 기상 정보 등으로 부터의 상황인지·분석 부문과 유기적으로 소통하여 다양한 정보기반 군사작전 전개를 구성할 수 있는 기초적 요소가 되는 ‘시·공간 식별에 대한 전자공간 인식을 위한 전술운용 시대’가 도래하고 있는 것이다¹⁷⁾¹⁸⁾.

다른 예로 군 장비 정비지원 및 교육을 위해 가상(VR)·증강(AR)·혼합(MR)현실 기술 기반으로 하여 현실 세계에 가상의 정보나 콘텐츠를 자연스럽게 병치하고, 인간의 감각과 인식을 더욱 확장시켜 정비응용 및 정비교육을 홀로렌즈 또는 HMD 등을 통해 지원하는 기술이다. 이 기술은 기존 정비지원 및 정비교육시스템과 운영관리시스템(Learning Management System: LMS)과의 연동을 통해 정비운영 다중 플랫폼 구축을 목표로 연구 진행 중에 있다. 첨단 방산 장비 제어를 위해 고위험·고속련 습득이 요구되는 상황에서 군 정비인력의 빈번한 교체는 고위험·고속련을 갖추기 어려운 현실이다. 따라서 방산장비

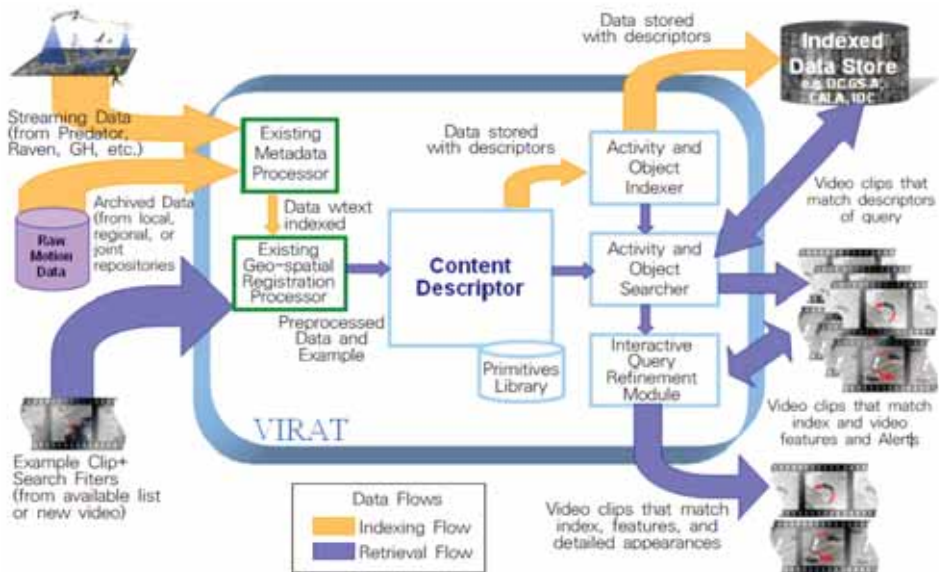
16) 방준성, 최은주, “증강현실(Augmented Reality) 국·내외 기술동향과 발전전망”, Emerging Issue Report 16, 한국과학기술정보연구원, 2017. 1.

17) 강진석, “전자공간을 위한 스마트폰기반 인터랙티브 혼합현실 기술 개발”, 중견연구자지원사업, 핵심연구, 2011.5.~2014. 4.

18) 강진석, “비정형 데이터마이닝에서 군 전술운용에 관한 연구”, 중견연구자지원사업, 도약연구(전략), 2014. 11.~2017. 10.

사용시 사고 발생 위험이 매우 높은 상황에서의 안전성을 확보하기 위해 가상정비 환경을 구축하여 정비지원과 교육과정을 진행하고 있다. 그 결과 단순 반복 훈련과정으로 해결되지 않는 고위험·고속력이 요구되는 고도화된 정비인력을 양성하고, 숙련되지 않은 인력이라 할지라도 쉽게 정비를 할 수 있는 시스템을 구축하여 실전에 활용할 수 있는 가능성을 보여주고 있다¹⁹⁾²⁰⁾.

미 국방부는 <그림 III-24>에서 보는 바와 같이 방위산업 분야에 비정형 데이터의 빅데이터 운용을 위해 연간 2억 5,000만 달러 이상을 투입하고 있다. ‘빅데이터 R&D 이니셔티브’ 사업의 일환으로 전투원 및 군 분석가의 전투 수행 능력을 배가시키기 위해 빅데이터 기술 연구에 주력하고 있다²¹⁾.



<그림 III-24> 미 방위고등연구계획국(DARPA)의 VIRAT 개발 프로젝트

미국방위고등연구계획국(DARPA)에서는 자율의사결정시스템, 전장상황 및 공간인식 기술을 개발하고 있으며, 대용량 데이터에서 특정 정보만을 탐지하는 기술 개발에 초점을 둔 ‘ADAMS’(The anomaly detection at multiple scales) 프로젝트를 추진하고 있다.

19) 강진석, “증강현실, 가상현실 또는 혼합현실 기반 군용 장비의 정비를 지원하는 서버, 방법 및 웨어러블 디바이스,” 특허등록 10-1874461-0000, 2018. 6.

20) 강진석, “증강현실에서 사례의 추론, 분류, 결정 기반 군용 장비의 정비를 지원하는 서버, 방법 및 웨어러블 디바이스,” 특허등록 10-1891992-0000, 2018. 8.

21) Defense Advanced Research Projects Agency

‘ADAMS’는 전장에서 발생할 수 있는 적의 위협요소를 사전에 찾아내는 전술 네트워크(Tactical Network) 운영방식으로 적군의 공격을 미리 차단하고, 방어가 가능한 기능을 제공한다. 그리고 위성영상이나 무인항공기(UAV)에서 촬영된 영상을 토대로 전장의 상황을 수집하여 추론과 내러티브를 통해 전장에서 펼쳐지고 있는 상황에 기초하여 위협요소를 검색하고 분석할 수 있도록 지원하고 있다²²⁾.

군사과학기술의 발전으로 인해 미래전은 다양한 전장 환경에서 전투원간의 상호운용성을 기반으로 한 네트워크 중심전(Network Centric Warfare)으로 변화하고 있다. 이는 전장에서 무기체계의 운영, 병사들의 기동성, 화력 지원에 있어서 다양하고 안전한 군사작전 지원을 목표로 하고 있으며, 통합적인 시스템을 통해 아군과 적군의 전술적 상황정보 즉, 병력이동, 지형·지물, 무기체계 등 전장공간에서 시공간적, 지리적, 물리적 요소를 오감을 활용하여 상호작용(Interactive)하며 체감할 수 있는 전투지휘체제로 발전하고 있다. 네트워크 중심전은 작전에 있어 군사력의 파괴보다 전투원 요소 간의 효과와 심리적 마비를 통한 전술 운용으로 변화할 것이며, 무기체계와의 연동을 통해 전투원 요소 간의 개별적인 플랫폼 운영이 아닌 네트워크 중심전으로 기동과 화력 그리고 전장의 상황인식 정보를 통한 상호작용 형태로 변화될 것이다.



〈그림 III-25〉 미 육군의 네트워크 중심전(Network Centric Warfare)을 위한 체계도

22) 미 국립연구재단(NSF)의 주요연구지원 프로그램, 2014. 12.

■ 소결론

- 인공지능(AI)에 대한 민간 기술은 웨어러블 로봇과 왓슨 등 의료, 무인 주행차량 등에 급속도로 성장하고 있는 추세이며, 이러한 인공지능(AI)은 미래 산업의 총아로 4차 산업혁명을 주도 할 것으로 예상
- 그러나 이러한 파괴적 상용기술(AI+ICBM)을 국방에 적용한 연구개발과 발전은 우리나라에 만 국한된 것이 아니며, 미국을 비롯한 일본, 중국 및 세계 각국에서 관심과 노력을 하고 있는 실정이기에 우리와 대립 관계에 있는 국가에서도 인공지능(AI)을 활용할 가능성이 매우 높다고 할 수 있음
- 우리의 경우 국방 분야에서 인공지능(AI) 활용을 위한 체계적인 연구개발은 미흡한 실정이며, 국방 분야 인공지능(AI)은 지능정보사회 추진단과 연계된 사업을 통해 사업계획을 수립하여 예산화하고 실증을 위해 추진하는 초기 단계에 있음
- 또한, 현재의 법규와 제도 및 환경이 인공지능(AI)에 적용된 융합(복합)체계를 획득하는 절차를 지원하지 못하고 규제를 받는 상황이 발생되고 있어, 이에 대한 관심과 개혁의 노력이 필요
- 국방 인공지능(AI) 활용을 위한 산·학·연·군이 연계된 전문가 및 소요군 내 인재 양성이 미흡하며, 인공지능(AI)의 기반이 되는 빅데이터 체계 축적 등의 준비도 부족한 상황임
- 특히, 군 체계의 특성상 창조적 개념과 설계 역량은 뒤쳐질 수 있는 바 이러한 인재와 기술력에 대해서는 외부 아웃소싱 등의 보완 제도 도입이 요구됨
- 빅데이터는 '21세기의 원유'라고 불릴 만큼 그 가치가 매우 높으며, 향후에도 이러한 빅데이터를 활용한 혁신적인 사례들이 많이 나올 것으로 예상되며, 미래에는 빅데이터라는 거대한 정보 속에서 새로운 정보기술력으로 발굴한 가치 있는 데이터들을 어떻게 정리하고 활용하느냐에 따라서 경쟁력이 결정지어질 것임
- 공공 및 민간분야 활용사례와 군에 적용할 수 있는 방안에 대해서 도출하면 다음과 같음
 - 빅데이터를 활용한 국방정보 분야의 각국 동향 예측 적용방안
 - 부대관리 측면에서 SNS 분석을 통한 군 홍보 및 CRM(Customer Relationship Management) 활용 방안
 - 군 보급품의 재고관리에 있어서의 빅데이터 활용방안
- 미래에 우리의 국방 정보력은 더욱 강화될 것이고, 그동안 직관과 통찰력에 의존해 부대관리를 해왔던 군 지휘관들도 과학적 부대관리 실현이 가능해질 것임
- 빅데이터의 긍정적 활용성과에도 불구하고 군의 특성상 무조건적인 빅데이터 기술 활용만을 주장할 수는 없으며, 이는 기술 활용에 앞서 군 조직의 특수성으로 인해 가볍게 여겨지기 쉬운 개인정보관리에 대한 지침이 마련되어야 하고, 향후 빅데이터 수집 및 활용범위의 확대와 함께 발생할 수 있는 정보제공 권한 및 소유권 문제, 그리고 군에서 가장 중요하게 다루는 군사보안 문제에 대한 대비책이 철저히 갖춰져야 함
- 빅데이터를 활용하고 있는 다양한 국가들의 사례와 우리 군에서 활용 중인 빅데이터 기술내용을 좀 더 구체적으로 포함시키지 못했지만 향후 연구에는 다양한 주변국들의 빅데이터 기술 활용사례들을 분석하여 빅데이터 기술의 긍정적 효과를 극대화할 수 있도록 제도적 장치 및 보안 문제 해결방법 등에 대해 논의가 필요함
- 선진과학화를 추구하는 대한민국 군이 빅데이터의 활용을 통한 발전 가능성을 무한히 증대시켜 더욱 가치 있는 미래 국가수호의 초석으로 자리매김 하기를 기대함

IV. 인공지능 기술분야별 활용방안 식별 및 과제도출

1. 인공지능 중점 추진과제별 활용 가능 분야

가. 인공지능(AI) 기술분야별 활용방안 식별 및 과제 도출

1) 인공지능(AI) 기술 동향

인공지능(AI)은 인간이 가진 지각, 학습, 추론, 자연언어 처리 등의 능력을 컴퓨터가 실행할 수 있도록 프로그램으로 구현하는 기술을 말한다. 인공지능(AI)은 기계학습(Machine Learning), 딥러닝(Deep Learning), 자연어 처리, 음성인식, 시각인식 등 첨단기술을 개발하는 방향으로 발전되고 있으며, 안전, 의료, 국방, 금융, 복지 등 다양한 응용 분야에서 특화된 소프트웨어와 머신러닝(Machine Learning), 클라우드, 고성능 컴퓨터 기술 등이 포함된다.²³⁾ 최근 인공지능(AI) 개발은 <그림 IV-1>과 같이 단순히 인지능력이 아니라 인지한 환경 속에서 최적의 답을 찾아내고, 여기에 스스로 수행한 학습결과를 활용하여 추론과 예측을 하며, 문제점을 스스로 발견하고 해결하는 행동 단계에 이르기까지 다양한 분야의 연구와 투자가 활발히 진행되고 있다. 이처럼 인공지능(AI)은 초기에 비해 많은 발전을 이루었으나 자율적인 상황 판단과 능동적인 행동을 기반으로 하는 인간의 지능을 완벽하게 구현하는 수준은 많은 한계를 갖고 있다.



<그림 IV-1> 인공지능(AI) 기술 구성

23) 과학기술정보통신부, “I-Korea 4.0 실현을 위한 인공지능(AI) R&D 전략”, 2018. 5.

위와 같은 제한사항을 극복하기 위해 오래 전부터 제안되어 온 수학·과학 분야의 이론과 모델링에 기반한 “인간처럼 계산(Computing like Human)”에서 “인간처럼 생각(Thinking like Human)”하는 지능을 구현하기 위해, 기존 인공지능망 구현 방식을 하드웨어, 소프트웨어적으로 고도화시키려는 노력과 기존 과학, 공학 분야의 연구가 아닌 신경과학(Neuroscience), 뇌과학(Brain Science)과 같은 분야의 연구를 기반으로 인공지능(AI)을 구현하려는 시도가 활발히 진행 중이다²⁴⁾.



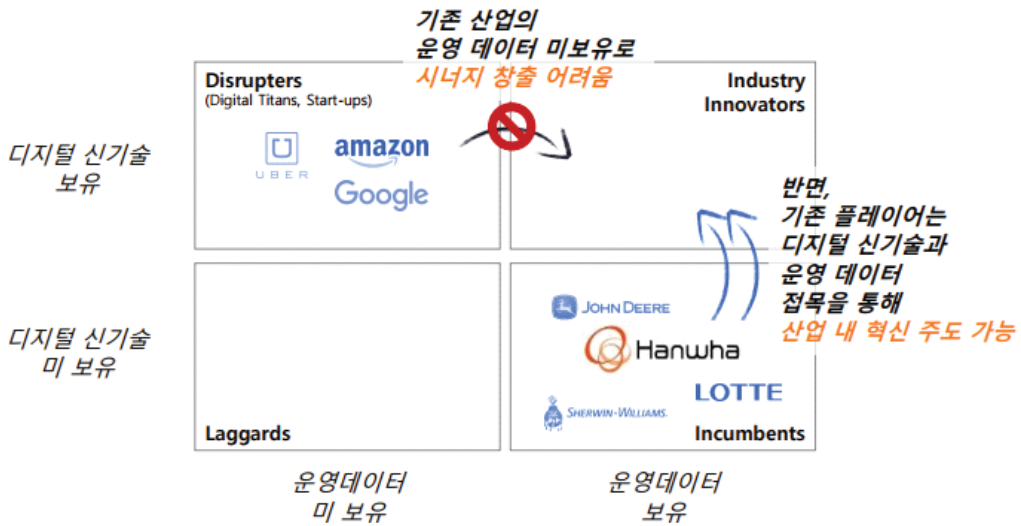
〈그림 IV-2〉 인공지능(AI) 기술의 발전 과정과 미래

2) 인공지능(AI) 기술 도입 전략

국방부는 인공지능(AI) 중점 추진과제별 활용 가능한 분야 식별 및 과제를 도출하여, 인공지능(AI) 시스템을 적용하고자 하는 요구과제별 사업계획의 구체화 가능 분석하고 있다. 현재 ‘인공지능(AI) 교관 개발’, ‘지능형 네트워크 트래픽 분석 및 조치도구 개발’, ‘전투 조종사용 인공지능(AI) 시뮬레이터 개발’ 3개 과제에 대한 운용개념과 이에 따른 적용 대상 인공지능(AI) 기술 등을 구체화 및 연구개발 진행 중에 있다.

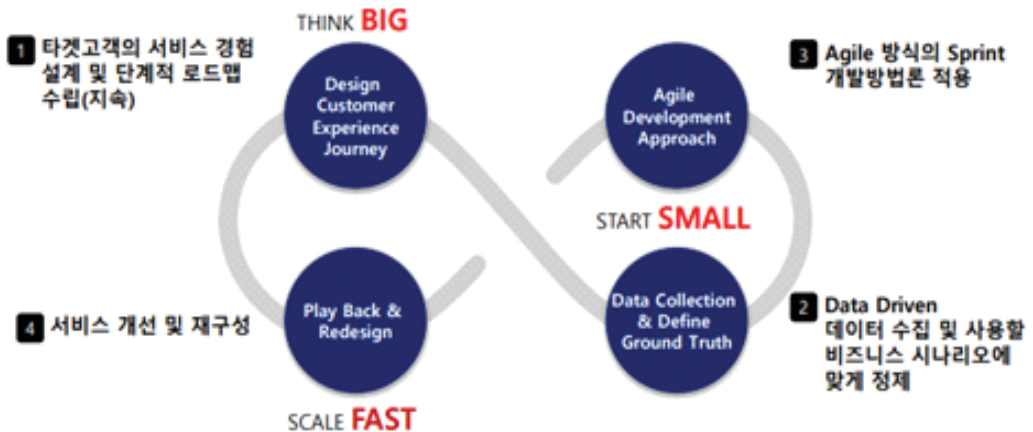
또한, 4차 산업혁명 기술을 산업별 터줏대감들이 주도할 것으로 믿는 이유는 혁신의 원천이 ‘Data’와 ‘Operation 경험’이기 때문이다. 따라서 기존에 군이 보유한 데이터와 운용 데이터의 접목을 통한 활용이 필요하다.

24) 이승훈, “최근 인공지능(AI) 개발 트렌드와 미래의 진화방향”, LG경제연구원, 2017. 12. pp. 30-31.



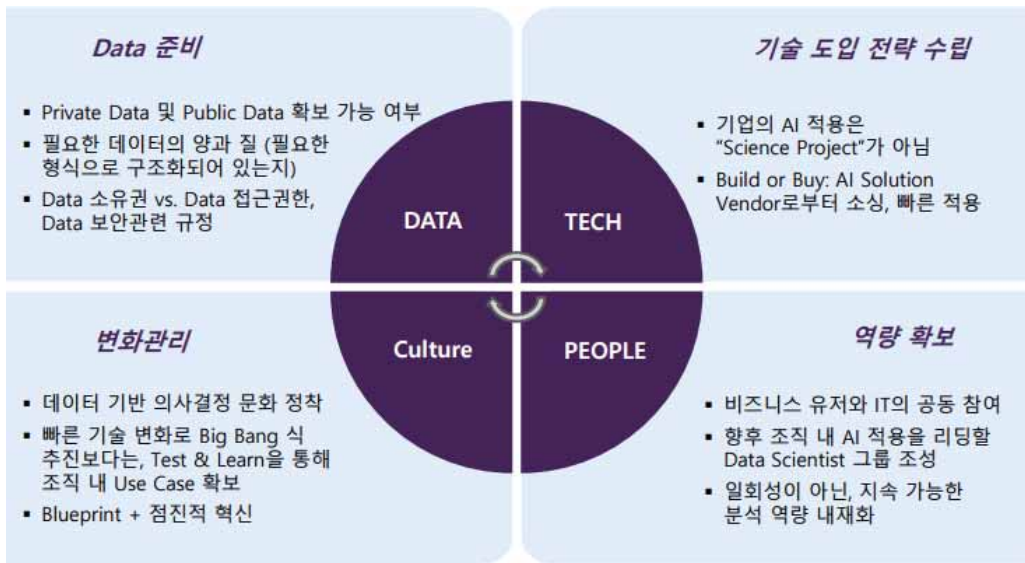
〈그림 IV-3〉 운용데이터 활용과 운용데이터의 접목 및 활용

이에, 빠른 기술 변화로 Big-Bang 식 추진보다는, Test & Learn을 통해 Use case를 점진적으로 혁신해 나가는 방법론을 채택해야 한다.



〈그림 IV-4〉 인공지능(AI) 도입 프로세스

즉, 인공지능(AI) 도입을 위해서는 충분히 필요한 데이터를 준비하고 기술 도입 전략을 수립하며, 데이터 기반의 의사결정 등 변화관리가 필요하며, 이에 필요한 역량 확보가 필요하다. 다음의〈그림 IV-5〉는 데이터 준비, 기술 도입 전략 수립, 변화 관리, 역량 확보 등 4개 분야의 인공지능(AI) 도입 전략을 제시하였다.



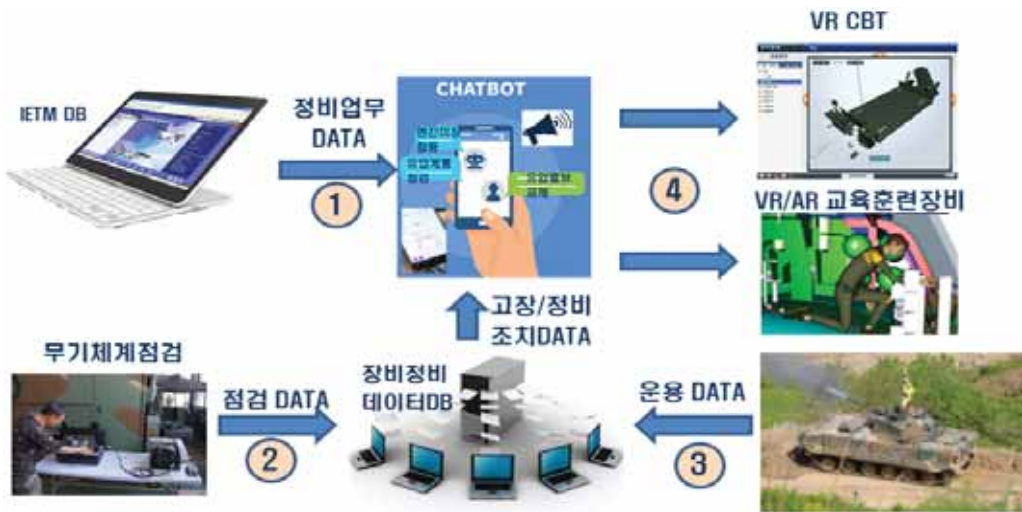
〈그림 IV-5〉 인공지능(AI) 도입 전략

다음의 〈그림 IV-6〉은 인공지능(AI)을 적용한 챗봇의 활용사례로 인공지능(AI) 기술교범 체계를 개발하는 방안을 예로 제시한 것이다.



〈그림 IV-6〉 인공지능(AI) 개발도구 활용(예)

〈그림 IV-7〉은 인공지능(AI) 기술교범을 확장하여 최초 전자식 기술교범의 데이터를 활용한 챗봇 형태의 서비스를 제공하는 예이다. 여기에는 실제 야전에서 발생된 정비 / 점검 데이터와 실제 야전 운용 데이터를 빅데이터로 축적하고, 운용한 데이터로 가공하여 정비서비스 챗봇에서 제공하여 지속적으로 현실적인 정비 가이드 서비스가 가능하도록 하는 인공지능(AI) 기술교범체계이다. 또한, 가상(증강)현실 데이터를 합성하여 챗봇과 증강현실(AR)로 정비를 경험하도록 하는 서비스를 제공하는 것을 예로 제시한 것이다.



〈그림 IV-7〉 인공지능(AI) 기술교범 서비스 활용(예)

나. 인공지능(AI) 기술분야별 활용분야 도출

1) 국방 무기체계 분야

국방부는 미래 전장환경의 변화에 대한 능동적인 대처와 최근 병력자원의 절벽 화에 대비하고, 무기체계를 지능화와 첨단기술을 활용할 훈련체계를 고도화하기 위해 인공지능(AI)을 활용한 시범사업을 진행하고 있다. 또한, 혁신적 국방 가치를 지속적으로 창출하기 위해 창의적인 과학기술을 융·복합하여 정보화 기반을 구축하는 데 역량을 집중하고 있다. 특히, 주변 강대국의 지능정보전 역량 강화로 인한 위협에 대응하기 위해 인공지능(AI) 역량을 확보하고, 이를 전력 소요창출과 핵심기동력으로 활용하기 위해 노력 중이다. 국방 분야에서는 다음의 〈표 IV-1〉에서 보는 것술 개발을 촉진시키는 미래 군사혁신의 과 같이 무기체계, 전력지원체계, 운영유지 등 전 분야에서 적용 및 활용이 가능할 것으로 판단²⁵⁾하고 있다.

〈표 IV-1〉 국방 무기체계 분야 인공지능(AI) 활용 분야

분 야	주요 내용
C4I	• 지능형 지휘결심지원체계, 인공지능(AI) 기반의 실시간 M&S 및 위게임 체계, 지능정보 센터, 초연결·초지능 네트워크 등
정보	• 지능형 군사정보관리체계(Smart MIMS), 지능형 사이버·전자전 공격/방호시스템 등
화력	• 인공지능(AI) 기술을 적용한 지능탄, 지능형 표적탐지 레이더, 지능형 사격지휘통제체계 등
기동	• 지능형 워리어 플랫폼, 인텔리전트 전투복, 인공지능(AI) 기반 자율 및 군집형 기동체계 등
방호	• 지능형 사이버 방호 시스템, 지능형 사이버전 수행 기술개발, 지능형 과학화 경계시스템, 지휘시설 및 무기체계의 지능형 방호체계 등
작전지속 지원	• 지능형 합성전장훈련체계(LVCG), KCTC와 연계한 인공지능(AI) 기반의 지휘결심지원체계, 인공지능(AI) 교관, 인공지능(AI) 기반의 훈련 시뮬레이터/전장훈련체계, 정비수요예측 시스템/탄약 저장관리체계, 지능형 물자보충/재고 관리체계, 지능형 안전관리 정보체계/원격치료 시스템, 인공지능(AI)기반의 인력획득 및 인사관리체계 등

최근 KAIST와 한화시스템은 국방 인공지능(AI) 융합연구센터를 개소하였으며, 인공지능(AI) 기반 지휘결심 지원체계, 대형급 무인 잠수정 복합항법 알고리즘, 인공지능(AI) 기반 지능형 항공기 훈련 시스템, 인공지능(AI) 기반 지능형 물체 추적 및 인식 기술 개발 등의 4개 과제를 우선적으로 선정하고, 기술자문, 인공지능(AI) 과제 발굴·연구, 상호 교류 및 교육 등을 추진 중에 있다. 육군에서는 2019년 초 인공지능(AI) 기술을 활용하여 초연결·초지능으로 상징되는 4차 산업혁명 시대의 군사혁신을 선도하기 위해 군 최초로 인공지능 연구 부서인 “인공지능(AI) 연구 발전처”를 창설하였다. 인공지능(AI) 연구 발전처는 인공지능(AI) 관련 컨트롤타워 구축, 국가 R&D 역량 활용, 빅데이터 구축, 군사혁신을 위한 동력(Driver) 마련을 목표로 하고 있다. 2019년에는 우선 군사용 인공지능(AI) 능력발전 비전·운영 개념을 조기 완성하고, 시범사업 계획 및 전력화 등 마스터플랜을 마련할 예정이다.

2) 의료 분야

최근 인공지능(AI) 기술을 이용하여 폐암, 폐질환, 유방암, 치매, 물리치료, 성조숙증 등과 같은 질환을 정확하고 빠르게 진단하거나 효과적인 치료가 가능한 보조 소프트웨어들이 속속 등장하고 있다. 이는 인공지능(AI)이 최신 논문, 과거 진료정보, 학술지 등의

25) 육군, “인공지능(AI) 연구 발전처”제공, 2019. 1.

정보를 스스로 학습하여 의사가 최적의 처방을 내리도록 보조하는 역할을 수행할 수 있기 때문이다. 인공지능(AI) 소프트웨어를 사용으로 질환에 대한 정확도는 높이고 진단하는데 들어가는 시간과 비용은 현저히 줄일 수 있으며, 환자는 최적화된 맞춤형 케어를 받을 수 있기 때문에 인공지능(AI)을 활용한 의료 및 헬스케어 적용 가치는 점점 증대되고 있다²⁶⁾.

MAM(Marketsandmarkets, 2016) 보고서에 따르면, 2015년 7억 1,300만 달러였던 인공지능(AI) 헬스케어 세계 시장규모가 2020년에는 75억 4,700만 달러로 크게 성장할 것으로 예상하고 있다. 국내 인공지능(AI) 헬스케어 시장도 17억 원(2015년)에서 256억 원(2020년)으로 증가하는 등 글로벌 시장의 연평균 성장률인 40%보다 높은 70.4%를 상회할 것으로 전망되고 있다. 인공지능(AI) 기술의 발달은 의료 및 헬스케어 산업에 혁신적이고 새로운 서비스를 보다 많이 창출할 것으로 예상된다.²⁷⁾

〈표 IV-2〉 의료 분야 인공지능(AI) 활용 분야

분 야	주요 내용
IBM	손이 물체를 만졌을 때 강도, 손의 떨림, 손톱 변형을 감지할 수 있는 손톱 센서를 개발하여 파킨슨병 징후 발견이 가능한 인공지능(AI) 종양학 의사 “왓슨 포 온콜로지”(Watson for Oncology)를 개발, 전 세계 대형병원 13곳에서 의사로 활약 중임
루닛	루닛 인사이트(Lunit INSIGHT for Mammography)는 유방암 진단 보조 소프트웨어로 영상 이미지를 입력하면 정확도 97%로 종양 악성 정도는 점수로 표기하며, 종양 위치는 히트-맵으로 표기가 가능함
텐센트	의료영상 분석 인공지능(AI) ‘미잉(MyIng)’을 개발하였으며, 수 백 여개 병원에 보급. 미잉은 당뇨병, 유방암, 식도암, 대장암 등을 진단할 수 있는 6개의 인공지능(AI) 시스템으로 구성됨
구글	알파벳의 생명과학 자회사인 베릴리(Verily)는 4년간 1만 명에 달하는 개인의 건강 상태를 면밀하게 추적하여 데이터를 축적하는 “프로젝트 베이스라인(Project Baseline)” 개시

3) 생활, 교육 분야

CES 2019에서는 “로봇 & 인공지능(AI)”전시관을 따로 마련하여 인공지능(AI)이 우리 생활과 보다 가까워졌음을 실감하게 하였다. 국내·외 글로벌 기업들은 이 곳에 각각의 전시관을 열어 인공지능(AI) 기술 자체가 아니라 자사의 어떤 제품에 인공지능(AI)이 탑재되었는지에 대해 많은 홍보를 하였다. 이제 인공지능(AI)의 적용은 우리에게 그리 새로운 일이 아니며, 우리 생활에 깊숙이 파고들고 있다. 인공지능(AI)과 관련한 글로벌 시장이

26) AIBRIL, “건강을 지키는 인공지능 AI와 헬스케어의 만남”, 2018. 10.

27) “헬스케어에 인공지능을 더하다”, 2018. 6., <https://skccblog.tistory.com/3712>

확대됨에 따라 각 국가 및 기업들은 인공지능(AI) 산업에 대한 투자를 더욱 강화하고 있다. 특히, 구글, IBM 등과 같은 글로벌 IT 업체들은 장기간 확보한 빅데이터와 패턴학습 기술을 접목하여 생활, 교육 및 게임 분야에서의 인공지능(AI) 기술의 상용화에 박차를 가하고 있다.

〈표 IV-3〉 생활 교육 분야 인공지능(AI) 활용 분야

분 야	주요 내용
레노버	중국 PC 업체 레노버가 인공지능(AI) 무인 매장 “레노버 러쿠 언맨드 스토어(LENOVO LECOO UNMANNED STORE)”를 개장, 얼굴 인식 만으로 구매부터 결제까지 모든 과정이 가능
삼성전자	인공지능(AI) 비서 ‘빅스비’를 향 후 스마트폰 뿐만 아니라 로봇, 냉장고, 스마트TV, 세탁기, 에어컨 등으로 적용 범위 확대 예정, 빅스비 비전(Vision) API를 추가로 공개, 서드파티 개발자가 더 자유롭게 많은 기능을 활용하게 될 전망
아마존	- 인공지능(AI) ‘알렉사’가 자사 뉴스 소식을 전하는 블로그를 통해 머신러닝(Machine Learning)으로 수 많은 뉴스 오디오 클립으로부터 낭독 기술을 배운 뒤 자체적으로 뉴스를 읽어줌 - 뉴스 진행자가 읽어주는 것 같은 뉴스 낭독 품질을 구현하기 위해 문자를 음성으로 바꿔주는 기술인 TTS(Text-to-speech) 기술에 머신러닝(Machine Learning)을 결합
구글	구글 딥마인드가 개발 중인 스타크래프트2 AI ‘알파스타’가 프로게이머에게 10대1로 압승
IBM	인간과 토론을 나눌 수 있는 클라우드 기반 인공지능(AI) 플랫폼 “스피치 바이 크라우드(Speech by Crowd)”를 개발, 파킨슨병과 관련된 데이터를 활용하여 효과적인 치료법을 추천할 수 있는 인공지능(AI) 모델 개발 예정
마이크로소프트	인공지능(AI) 및 클라우드 기술로 미래 자동차 기술 개발을 지원, 인공지능(AI) 플랫폼과 클라우드 BMW, 닛산, 볼보, 폭스바겐 등 세계 자동차 제조사들의 디지털 트랜스포메이션을 지원

4) 보안 분야

최근 사이버 공격은 신종 랜섬웨어, APT 공격 등과 같이 사이버테러로 불릴 만큼 공격 방법이 매우 고도화되고 있으며, 특히 인공지능(AI)을 접목한 지능형 공격도 증가하면서 피해 규모도 매년 증가하고 있다. 과거의 해킹 공격의 경우 자신의 능력을 과시하기 위한 사이버 공격이 많았으나 최근에는 산업의 발전과 함께 기업과 개인을 대상으로 한 악의적인 사이버 공격이 주를 이루고 있다. 따라서 4차 산업혁명 시대, 5G 시대에 산업 변화의 흐름에 따른 보안위협에 대처하기 위해서는 머신러닝(Machine Learning)과 같은 인공지능(AI)을 이용한 방어가 필수적이라고 볼 수 있다. 이를 위해 정보보안 관련 업체 중심으로 다음의 〈표 IV-4〉와 같이 구글의 딥마인드, IBM의 왓슨, 오픈 소스 인공지능(AI)

기술을 활용한 악성코드 분석, 위협탐지 및 예방, 취약점 분석 등이 활발히 진행하고 있으며, 국내·외 보안 업체에서도 인공지능(AI) 보안 솔루션 개발을 위해 많은 노력을 기울이고 있다²⁸⁾.

〈표 IV-4〉보안 분야 인공지능(AI) 활용 분야

분 야	주요 내용
구글	머신러닝(Machine Learning) 오픈소스 프레임워크인 '텐서플로(Tensor flow)'를 활용하여 하루에 1억 개 이상의 스팸 메일을 추가로 차단 이미지를 기반으로 한 메시지, 악성코드가 내용물에 숨겨져 있는 이메일, 새롭게 생성된 도메인으로부터 발송된 악성 메시지, 스팸이지만 볼륨이 낮아 정상 트래픽과 구분이 가지 않는 경우도 탐지 가능
와트릭스(Watrix)	최대 50미터 거리 내에서 체형과 걷는 방법을 통해 사람을 인식할 수 있는 '보행인식' 기술을 개발. 이 시스템을 활용하여 2020년까지 모든 시민들의 행동을 기반으로 개인 점수를 부여하여 전국적인 사회신용시스템을 도입할 계획
IBM	최근 증가하고 있는 랜섬웨어와 같은 개인에게 금전적인 피해를 주고 있는 사이버 범죄를 원천 봉쇄할 수 있는 클라우드 기반의 보안 위협 지능형 플랫폼 'X-Force Exchange'를 개발
시만텍	인공지능(AI)과 기계학습을 적용한 표적형 공격패턴 분석 기술 "시만텍 표적 공격 애널리틱스(Symantec Targeted Attack Analytics)"를 개발 기존 사이버 공격 분석 시 활용한 위협 탐지 기술과 머신러닝(Machine Learning)을 결합, 사이버 공격기법을 집중적으로 학습시켜 신속하고 월등한 대응력을 제공
아마존	머신러닝(Machine Learning)으로 AWS 계정을 완전히 보호하는 "아마존 가드듀티"를 개발, 정상적인 패턴을 벗어나는 모든 이벤트 식별 가능
파수닷컴	머신러닝(Machine Learning) 기술을 자사의 대표적 시큐어코딩 솔루션 '스패로우'에 적용. 개발단계부터 소스코드 상의 보안 약점을 정확하고 빠르게 제거하여 시간단축과 보안취약점 해결

4차 산업혁명 시대에 들어오면서 인공지능(AI)은 알파고 마스터(AlphaGo Master)와 같이 혁신적으로 발전한 알고리즘, 빅데이터, 클라우드, 컴퓨팅 파워 등이 서로 융·복합되어 실제로 산업 전반에 적용되어 다양한 현실 세계의 문제점을 해결하고 있다. 인공지능(AI)의 구현을 위해서는 인간과 유사하게 행동하는 컴퓨터 프로그램을 구현하는 학습방법인 머신러닝(Machine Learning)·딥러닝(Deep Learning)과 이것을 학습할 수 있는 막대한 양의 데이터와 컴퓨팅 파워가 필요하며, 데이터를 수집하는 사물인터넷(IoT) 뿐만 아니라 이를 분석하는 빅데이터 및 컴퓨터 용량을 제공하는 클라우드 기술, 이외에 자연어 처리 기술과 인식기술 등 다양한 기술개발이 필수적이다.

28) 박형근, “정보보안에서의 인공지능 도입 분야와 주요 사업자”, 2018. 8.

IBM은 2025년에 인공지능(AI) 산업이 2,000조 원에 이르는 시장을 창출할 것으로 내다보고 있으며, 맥킨지는 인공지능(AI)으로 인해 7,000조 원에 이르는 파급 효과가 창출될 것으로 전망하고 있다. 유엔 미래 보고서는 30년 내에 인공지능(AI)이 인간의 지능을 능가할 것이라는 전망을 내놓고 있다. 특히, 기존에는 인공지능(AI)이 어느 한 분야 전문가의 소유물이었다고 한다면 최근에는 인공지능(AI)과 관련된 연구결과물이 DeepMind, Open AI 등과 같은 오픈 소스 활성화를 통해서 제공되기 때문에 비전문가도 쉽게 이해하고 즉시 응용이 가능한 형태로 공개되기 때문에 보다 많은 사람들이 참여로 인공지능(AI)의 성능이 빠르게 향상되고 진화되고 있다. 수많은 글로벌 기업들은 다양한 연구 성과물을 자사 제품 개발과 서비스에 응용하여 상용화하고 있으며, 세계 각국에서도 인공지능(AI)과 관련된 다양한 정책을 수립하여 기술 주도권을 잡기 위해 노력을 하고 있다.

2. 인공지능을 적용한 사업화 및 구체화 가능성

가. 국내 인공지능(AI) 관련 기업 현황

국내 인공지능(AI) 관련 기술을 보유하고 있거나 비즈니스를 하는 기업 목록은 <표 IV-5>와 같다. 국내 기업의 주요 기술분야와 제품, 기술 수준을 활용하여 인공지능(AI) 적용 사업화가 가능할 것으로 예상된다.

<표 IV-5>국내 인공지능(AI) 관련 기업 현황

순	업체명	적용 기술	제품명(적용분야)	기술 수준
1	한글과 컴퓨터/ 한컴이터프리	언어(자연어처리)	지니톡	통 번 역
2	솔트룩스	기계학습·자연어처리	아담	(AI 플랫폼) 의료 / 상담
3	ETRI	언어(자연어처리)	엑소브레인	지식학습과 축적, 질의응답기술 (장학퀴즈 압승)
4	디오텍(셀빅AI)	언어(자연어처리)	셀비	문자/음성인식(제한된 텍스트 처리)
5	삼성전자	언어(자연어처리)	블링고	음성인식 (제한된 텍스트 처리)
6	LG전자	언어(자연어처리)	Q보이스	음성인식 (제한된 텍스트 처리)
7	마인즈 랩	자연어처리/기계학습	의료	의료녹취(제한된 텍스트 처리)
8	센티엔스	텍스트마이닝	금융	플랫폼 설계 중
9	네이버	대화희미분석	라운	챗봇(제한된 텍스트로 대화)
10		텍스트마이닝	파파고	통번역(4개국어 대화 가능)

순	업체명	적용 기술	제품명(적용분야)	기술 수준
11	루닛	기계학습	루닛	의료분야 딥 러닝(Deep Learning) 적용 (폐렴진단 정확도 증가)
12	센인트 시큐리티	기계학습	맥스	사이버 보안 탐색, 경보 기능
13	SK 텔레콤	음성인식/자연어처리	누구	(AI스피커) 음성인식 질의응답기술
14	가천대 길병원	기계학습	IBM 왓슨온콜로지	상용화 의료서비스 (정확한 암진단 처방)
15	다음카카오	기계학습	카카오	검색서비스 / 여행자 추천
16	SK플래닛	기계학습	전자상거래	유사상품 검색, 신용카드번호 자동 인식
17	엔시소프트	기계학습	게임	온라인 모바일 서비스
18	아이엔코프	기계학습	쇼핑몰 서비스	온라인 모바일 서비스
19	코노랩스	기계학습	모바일 스케줄러	저장스케줄 인식 가능
20	유비파이	자율주행	드론	장�물 회피기술 구현
21	솔리드웨어	기계학습	솔리드웨어	빅데이터 분석
22	노타	기계학습	소프트 키보드	이미지맵(가상 건반)

나. 국방 분야 실현 가능성

국내외 인공지능(AI) 관련 기술을 활용하여 국방 분야에서의 실현 가능성을 검토하며, 이미 많은 분야에서 무인 로봇과 같은 분야에서 도입이 되어 진행되고 있으며, 현재 진행되거나 향후 가능한 분야를 사례 중심으로 설명하고자 한다.

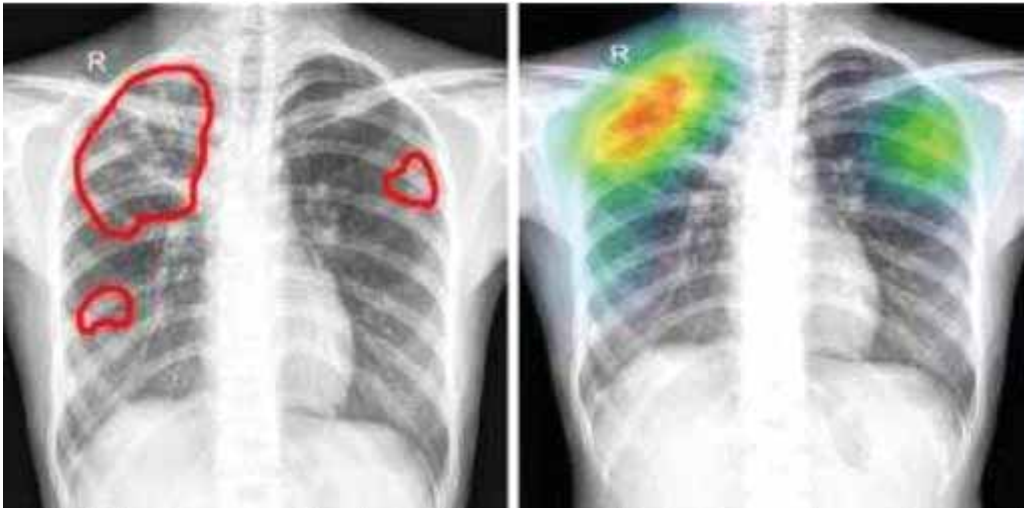
1) 의료 흉부진단 “루닛”

2013년에 설립된 루닛은 딥러닝(Deep Learning) 기반의 범용 이미지 인식 기술을 헬스케어 분야에 적용하는 의료영상 분석시스템을 연구 개발하고 있다. 루닛(옛 클디)은 이미지 인식관련 인공지능(AI) 기술을 통해 <그림 IV-8>과 같이 X-ray 등 초기 진단용 의료영상을 분석하는 기술을 보유하고 있다.

루닛은 전 세계 10대 인공지능(AI) 기업 랭킹인 ‘The AI 10’에 국내 기업으로는 유일하게 선정되었으며, 헬스케어 관련 기업들 중에서는 TOP 1, 의료 진단 AI 관련 기업들 중에서는 TOP 7에 오른 기업이다. 루닛은 2015년 인공지능(AI) 이미지 인식 대회인 ‘ILSVRC’에서 물체분류/위치추정 분야에서 5위에 올랐으며, 2016년 의료영상기술 학회인 ‘MICCAI 2016’에서 유방암 종양 확산 스코어 자동 판독 알고리즘 대회에서 세계 1위를

차지했다.

루닛은 개발 진행 중인 유방암, 폐질환 진단 기술에 대한 의학적 효용성을 객관적으로 입증하기 위해 협력 병원과의 임상 연구를 진행하고 있으며, 제품 상용화를 위해 식약처 의료기기 승인을 진행 중이다. 루닛은 ‘국방의료정보 빅데이터 분석체계 구축사업 연구용역’을 통해 흉부 엑스레이 영상 판독 지원시스템 부분의 연구용역을 진행하여, 대학병원과의 연구 경험을 노하우로 군에 최적화된 시스템을 위한 진단 프로세스를 개발하였다.²⁹⁾



〈그림 IV-8〉 루닛 인공지능(AI) 의료영상 판독 체계

2) ETRI “엑소브레인”

ETRI의 ‘엑소브레인’은 세계 최고인공지능(AI) 기술 선도라는 비전을 달성하기 위한 미래창조과학부 소프트웨어 분야의 국가 혁신기술 개발형 R&D 과제이다. ‘엑소브레인’은 자연어를 이해하여 지식을 자가 학습하며, 전문 직종에 취업 가능 수준으로 인간과 기계의 지식소통이 가능하면서 지식과 지능이 진화할 수 있는 SW를 개발하는 목표로 한다. 본 과제는 총 3단계에 걸쳐 10년간 수행되며 2013년 ~ 2017년 간에 1단계가 진행되었으며, 단계별 연구 진행 현황은 〈그림 IV-9〉와 같다.³⁰⁾

29) 출처 : https://www.lunit.io/ko/product/insight_cxr2/

30) 김현기, 엑소브레인 병렬형 과제 및 추진 현황, 한국전자통신연구원, 2018.8.13



〈그림 IV-9〉 엑소브레인 추진 로드맵

엑소브레인은 병렬형 4개 세부과제로 구성되어 있으며, 4개 세부과제의 연구결과물 통합을 통해 '지능진화형 엑소브레인 SW 개발'을 최종 목표로 하고 있다. 지능진화형 엑소브레인 SW는 자연어를 이해하여 지식을 자가 학습하며, 전문 직종에 취업 가능 수준의 인간과 기계의 지식소통이 가능한 지식과 지능이 진화하는 SW이다. 이를 위해 필요한 3대 핵심 기술은 인간 모사형 지능 기술, 자율학습 기반 지식 진화 기술, 문제 해결형 협업 기술 확보이다.

엑소브레인은 데이터를 분석하고, 언어를 처리하며, 판단 및 예측을 통해 백과사전, 뉴스기사 질의 응답과 같은 일반상식 질의 응답, 법률·특허분야 질의응답과 같은 전문직 의사결정, 금융·공공분야 지식상담과 같은 전문지식 컨설팅, 로봇·자동차·단말 탑재 형식의 탑재형 인텔리전스, 기업·공공 빅데이터 분석과 같은 빅데이터 인텔리전스 등을 통해 언어를 이해하고, 지식을 학습하여, 전문지식을 제공하는 언어지능 SW를 개발하는 사업이다. 엑소브레인 과제 수행을 통해 지능 진화형의 인공지능(AI) 원천기술 확보 및 기술선도, 전문가 문제해결 및 의사결정 지원 지식 컨설팅 제공, 정보통신기술(ICT) 융합 기반의 지능형 서비스산업 및 신시장 창출과 같은 성과를 기대하고 있다.

3) 인공지능(AI) “아담”

“아담”은 <그림 IV-10>과 같이 인간 두뇌 분석을 통한 인공지능(AI) 원천기술로 인공지능(AI)기술과 가상현실(VR) 및 증강현실(AR) 기술이 결합하여 발전된 사례로 유·무인 체계의 최적 이동경로 수립 및 원격지원, 임무수행 경로 사전 검증에 활용이 가능하다.

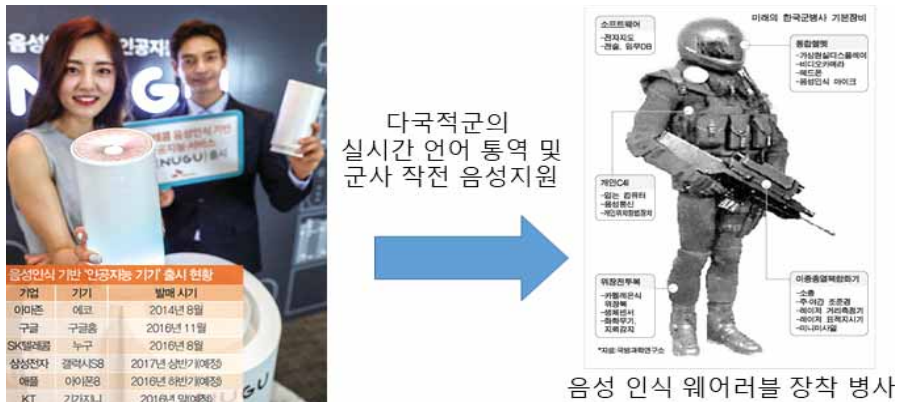
- ① 유·무인 무기체계 편대들의 시각화된 원격 지휘 통제
- ② 전장의 전투 원격 지휘 통제, 최적 전략, 작전 수립 지원
- ③ 가상전장 환경에서의 전투체험, 전투지휘 연습 등의 임무에 활용



<그림 IV-10> 인공지능(AI) 플랫폼 ‘아담’

4) 인공지능(AI) 비서 및 통번역 “누구” “파파고” “지니톡”

인공지능(AI) 비서 및 통번역 기술은 미래병사체계와 접목시켜 발전시켜야 한다. 다음의 <그림 IV-11>과 같이 무선 웨어러블 디바이스를 통해 원격지의 병사들에게 작전임무 수행 정보지 및 다국적군과의 작전 수행 시 실시간 언어 통번역 비서 역할 수행이 가능하다.



<그림 IV-11> 인공지능(AI) 비서를 미래병사에 적용 방안

또한, 다음의 <그림 IV-12>와 같이 무선 웨어러블 디바이스를 통해 미래 병사체계에 연동하여 작전임무수행 정보지원 및 다국적군과의 작전 수행 시 실시간 언어통역 비서 역할 수행이 가능하다.



<그림 IV-12> 미래병사에서의 활용 방안

5) 소부대 몰입형 훈련시스템(ETRI)

소부대 몰입형 훈련시스템은 <그림 IV-13>과 같이 보병 또는 특수작전임무를 수행하는 병사들이 도보로 이동하면서 임무수행 훈련을 할 수 있는 모의이동훈련 시뮬레이터(이하 ODM)를 구동하는 소프트웨어이다. 전 방향 이동지원 상호작용 소프트웨어 시스템은 다음과 같은 기능을 갖는다.

- ① 모의이동훈련 시뮬레이터 위에서 훈련자 이동시 충분한 체감 안정도를 유지할 수 있도록 실시간 정밀 제어
- ② 모의이동훈련 시뮬레이터 위의 훈련자 위치 및 자세를 인식
- ③ 분대급 전술 시뮬레이터 또는 상용게임과의 연동을 통하여 3D 가상현실 속 객체들과 탐지, 교전 등의 상호작용을 모의 가능

ODM(Omni-Directional Movement)은 걷거나 뛰는 등의 이동을 모의하는 장치로써 훈련자가 장치 위에서 실제 발을 내딛어 걷거나 뛰어서 이동을 실시하면 발바닥과 접촉하는 장치의 표면이 이동 반대 방향으로 움직임으로써 이동을 모의할 수 있게 된다. Omni-Directional은 모든 방향으로 이동할 수 있도록 만들어진 장치로 달리기와 걷기 등을 위한 트레드밀(Tread-mil)과 같은 개념으로 작동된다. 특히 병사들에게 실전과 같이 몰입감이 높은 가상훈련 환경을 제공하기 위해 개발된 기술로 훈련자의 자세와 위치를 실시간으로 추적한 정보를 기반으로 하여 군인들이 제한된 공간 내에서 처음 가보는 지형 지물 환경을 걷고 뛰면서 작전지역에 대한 사전 훈련이 가능하다.

또한, 사람의 자율신경계 반응에 의해 나타나는 생체·환경신호를 센싱·처리하여 심리 감성을 추론·처리하는 ‘심리감성 인지 및 처리기술’은 병사들의 신체적·정신적 상태를 인지·예측할 수 있어 군 복무 중 인사사고와 안전사고 등을 예방하는 ‘병영생활 관리시스템’으로도 충분히 활용이 가능하다.³¹⁾



<그림 IV-13> 소부대 몰입형 훈련시스템(ETRI)

31) 출처 : 테크월드뉴스(<http://www.epnc.co.kr>)

3. 무기체계별 인공지능 적용 가능 분야

가. 기동 분야

1) 전차 / 장갑차 / 전투차량

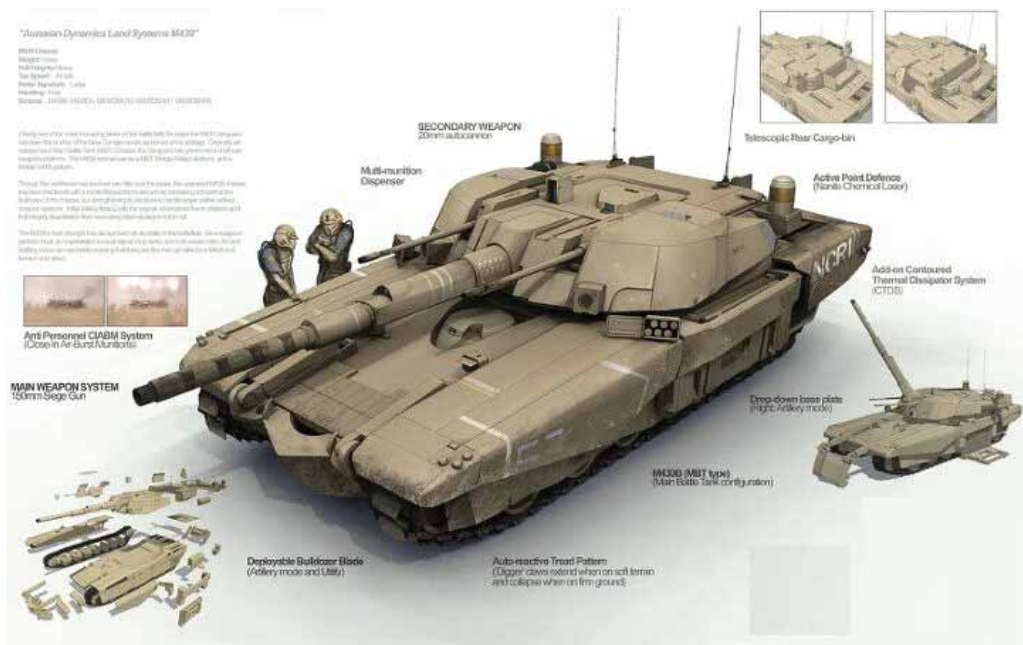
인공지능(AI) 전차는 맨-머신(M-M) 인터랙션(1000분의 5초 만에 전쟁터 정보 분석) 개념으로 “로봇전차가 인간 의사 결정권자들을 위한 정보를 수집하고 구성하는 것은 물론 인간-기계 간 네트워킹을 발전시키기 위해 고안된 새로운 세대의 인공지능(AI) 연구 결과와 일치한다”는 의미를 갖고 있다. 이에 따르면 첨단 알고리즘 바탕의 컴퓨터 기술은 이를 사용하지 않았더라면 모으기 힘든 데이터 풀(pool)을 모아서 몇 초 또는 몇 밀리(1밀리 = 1,000분의 1초) 안에 분리해 배포할 수 있다. 인공지능(AI)으로 구동되는 센서는 수신된 사진, 영상, 비디오 또는 데이터를 표면적으로 무제한인 기존 데이터베이스로 보내고 비교하며, 차이를 평가해 거의 실시간으로 분석해 준다. 다양한 인공지능(AI) 시스템은 가장 앞선 컴퓨터 처리 속도로 동시에 정보를 구성하고, 공유하고, 분석하는 작업을 수행한다. 그와 동시에 인간은 인식 능력을 통해 인간 고유의 많은 핵심 속성·재능·문제 해결 능력 등을 보여준다. 앞으로 향후 몇 년 내에 사람이 가진 능력과 기계 속성 간 결합 또는 합성이 빠르게 진화할 것으로 예상되며, 전투에 민감한 정보를 신속하고 효율적으로 전투 지휘관들에게 제공할 것으로 전망하고 있다.

예를 들어, 전방에서 운용되는 ‘윙맨(wingman)’ 로봇 차량은 자칫 감지에서 벗어날 수 있는 대상을 식별하고 지형·세부 항법 정보·해당 지역에서의 이전 임무 관련 데이터, 또는 알려진 위협 데이터베이스를 즉시 분석할 수 있다. 미 육군 연구소(Army Research Laboratory) 과학자 겸 엔지니어인 브랜든 페렐만 박사는 “사람보다 낫지는 않지만 사람과는 또 다른 AI 시스템을 갖게 된다. 이는 특정한 종류의 데이터를 처리하는 데 있어 더 빠를 수도 있고 더 효율적일 수도 있다. 이는 오늘날 우리가 일을 하는 방식과는 전혀 다른 방식으로 인간 팀원들과 협력해 위협에 대처할 것”이라고 말했다. 그는 “지휘자들은 차량 센서 패키지를 통해 목표물을 볼 수 있고, 목표물을 탐지하는 데 도움이 되는 표적인식 기술이나 어떤 종류의 인공지능(AI)이 있다면 지도에 목표물의 위치를 나타내는 전장표적 아이콘이 튀어나오는 것을 볼 수 있을 것”이라고 말했다.

인공지능(AI) 중심의 자율 탱크는 센서 감지에서 사격까지 시간을 크게 단축시켜 주기 때문에 전장 지휘관들이 빠르게 나타나고 움직이는 타겟이나 적의 공격에 재빠르게 대응하고 공격할 수 있게 해 준다. 페렐만 박사는 “이 탱크 도입으로 향후 군인이 하는 일,

즉 오늘날 하는 사격, 이동, 의사소통 등이 모두 달라질 것"이라고 말했다. 그는 "인간 대 인간 대응방식이 아닌 AI 팀과 함께 일하는 인간과 대응할 것이기 때문"이라고 설명했다. 그는 "드론(AI 탱크) 공격 자산을 더 많이 통합해 임무를 간소화할 수 있기 때문에 위험도가 높은 특정 작전에 필요한 병사의 수를 줄일 수 있다는 것"이라고 말했다.

미 육군은 2020년까지 미보병이 사용하고 있는 M113 보병장갑차를 인공지능화해 운영하기 위해 시제품을 선보일 예정이다. M113 장갑차는 유인과 무인으로 운영해 작전에 사용할 예정이다. 또한, 미군은 M113 장갑차를 대·중·소형으로 만들어 운영하는 것도 검토하고 있다. M113 무인장갑차는 기존의 장갑차를 이용한다는 점과 작전지역에서 적군에 대한 공격과 병력수송을 할 있다는 장점을 갖고 있다.



〈그림 IV-14〉 미군의 미래 인공지능(AI) 전차 개념도

- 화력 증대를 위해 인공지능(AI) 표적 추적 자동화, 유도화 지능탄 개발
- 사격통제장치 분야의 인공지능(AI) 표적 자동 추적장치(포탑 구동장치와 연계)
- 대전차 유도탄 방어를 위한 인공지능(AI) 방어체계(대전차 로켓 및 유도탄의 탐지, 추적, 요격)
- 전차 탑재형 인공지능(AI) 무인조종 자동화기(열 감지 및 자동 추적 사격)
- 기동성 향상을 위해 지형 조건에 따른 인공지능(AI)형 안정화 주행장치

- 생존성 향상을 위해 자동으로 오염도 측정 및 전차 내부 밀폐, 공기 정화 기능 개발

2) 전투장비

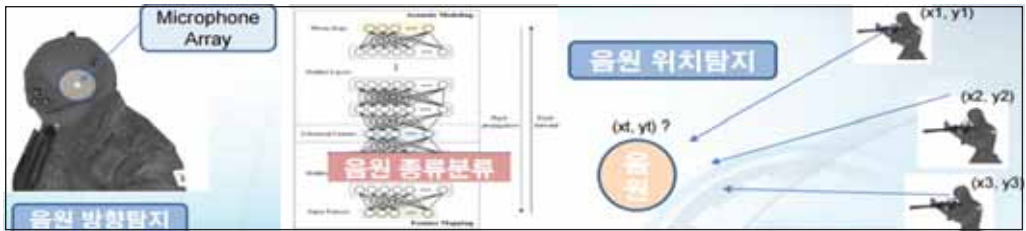
국방부는 인공지능(AI)과 빅데이터 등 첨단 정보통신기술(ICT)를 활용한 무기체계를 지능화하기로 했다. 이를 위해 군 위성, 정찰기, 무인기(UAV) 등 다양한 센서에서 수집된 영상정보를 통합하고 분석할 수 있는 ‘지능형 ICT 감시정찰 시스템’을 구축하여 장기적으로는 인공지능(AI) 기반의 지능형 지휘통제체계를 개발하고 전장 상황을 실시간으로 분석·공유하여 신속한 지휘통제를 보장할 것이라고 국방부는 설명하고 있다. 또한, 가상현실(VR)과 증강현실(AR) 기술을 다양한 분야에 적용해 훈련체계를 고도화할 방침이다. 군별 임무 특성을 고려하여 ‘특수작전 모의훈련체계(육군)’ ‘잠수함 승조원 훈련체계(해군)’, ‘기지작전 훈련체계(공군)’도 구축한다.

국방부 관계자는 “위험성이 높고 기술 숙련도가 높은 군 장비의 정비교육과 정비지원을 위한 시스템을 개발 중”이라며 “앞으로 군 차량 운전교육, 간호실습 등 군 요구를 반영해 콘텐츠 개발을 지속할 계획”이라고 전했다.

이외에도 진동·열상 감지 센서 기술을 활용한 침입탐지체계와 사물인터넷(IoT) 기반의 인원·장비·시설 원격 관리체계 구축, 이동 원격진료체계를 통해 초기 치료 골든타임 확보, 군 의료정보 빅데이터 분석체계 구축 등도 구축할 계획이다.³²⁾ 또한, 임무 지속형 개인 전투는 전투원이 미래 디지털 전장 환경에서 효과적으로 임무를 수행할 수 있도록 화기, 피복, 휴대품, 훈련, 치료 등에 첨단 기술을 적용해 개개인을 단위 무기체계화함과 동시에 지속적인 전투를 할 수 있도록 지원하는 기술 분야다. 개인전투체계용 웨어러블(wearable) 정보처리기술, 개인전투체계용 하지 근력 증강기술 등이 이에 속한다. 미래형 추진·플랫폼은 고출력 고성능 추진 시스템과 최적화된 형상 설계를 통해 지상·해상·수중·공중·우주 환경에서 초고속 기동 및 저피탐 능력을 고도화하는 기술 분야다. 초고속 수중 추진 기술, 해양 무인 고성능 추진 기술이 대표적인 기술로 꼽힌다.

- 자율표적획득장치 연구 : 음원 탐지 기반 적의 방향, 위치, 탐지정보 제공, 사격원점 등 표적/인원 등의 자율탐지, 인식, 위치등록, 추적 및 공유

32) 출처 : 에브리뉴스 EveryNews(<http://www.everynews.co.kr>)



〈그림 IV-15〉 자율 표적 획득장치 개념

자율상황인식, 의사결정 장치 연구 : 원시정보와 정보, 영상 기반의 자율인식정보 및 피아 작전 정보를 통합한 자율상황인식을 기반으로 인공지능(AI) 의사결정, 자율적, 반자율적 자산의 하무 임무에 할당



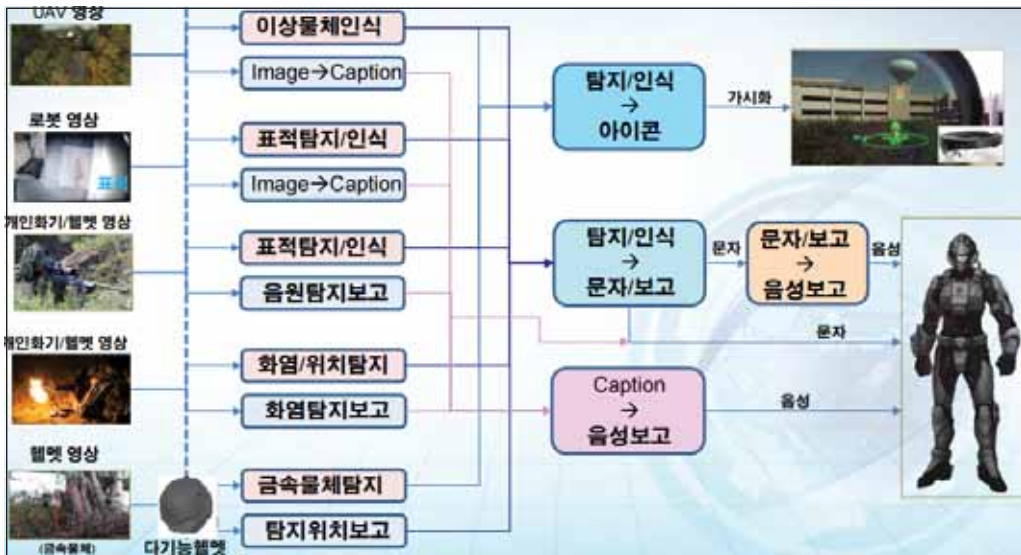
〈그림 IV-16〉 자율 상황인식 의사결정 장치 개념

계층별 자율상태인식 및 의사결정 : 인공지능(AI) 기반의 각 계층별 상태 인식과 임무 분할, 할당, 수행의 계획과 실행 상태를 전시



〈그림 IV-17〉 계층별 자율상태 인식/의사결정 개념

- Wearable 별 원시, 인식 정보 구분 및 활용
 - 위치 : 위치, 자세, 피로도, 맥박, 운동상태, 혈압 정보
 - 통합헬멧 : 정신상태, 영상/지형상태, 음원, 환경/표적인식, 수면 상태, 안구 지향 등
 - 병사컴퓨터 : 신체 자세, 온도 등 환경정보 등
 - 무장 : 자세정보, 상태정보, 사격상태, 영상정보, 표적정보 등
 - 통신 전시장치 : 적군 위치, 아군 위치, 명령정보, 통신상태 등
- 다양한 전시 기능 지원 MMI
 - UAV 영상(이상 물체 인식), 로봇 영상(표적탐지 인식), 개인화기 / 헬멧 영상(표적 탐지 인식, 화염/위치 탐지, 금속물체 탐지 인식)
 - 탐지 인식에 따른 보고(아이콘, 문자, 음성)



〈그림 IV-18〉 다양한 기능의 MMI 기능

- 지휘통제 체계화 : 전장정보 공유, 초소형 피아식별, 음성/데이터 통신
- 화력 자동화 : 사거리 증대, 이동표적 정밀타격, 초소형 미사일 장착 운용

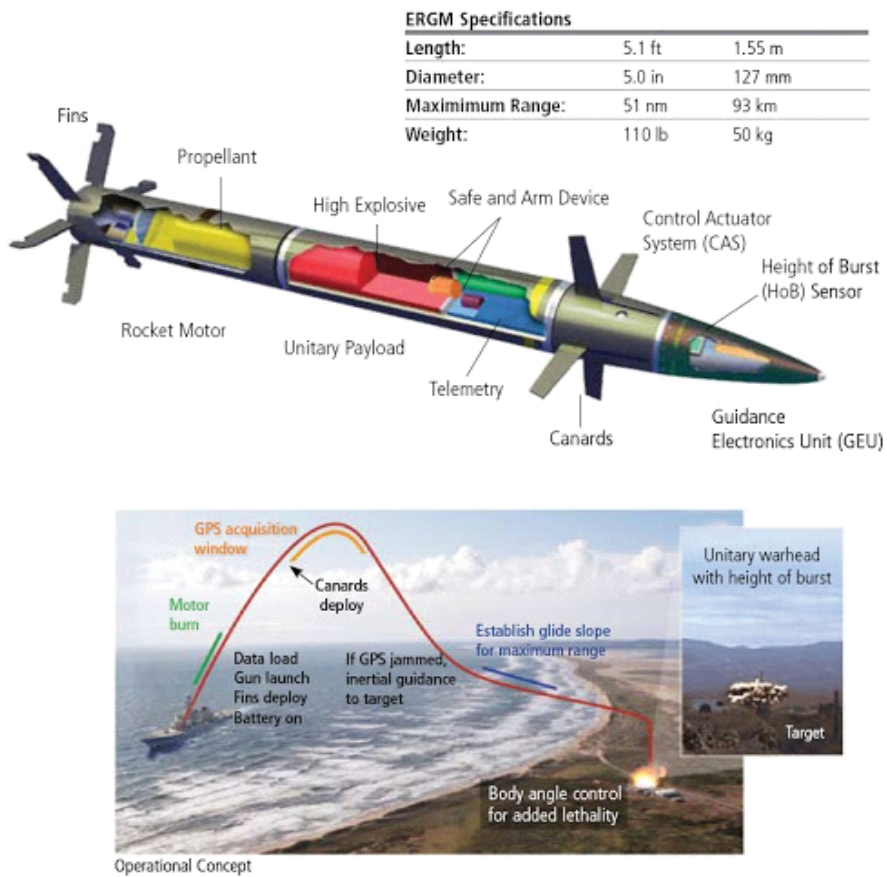


〈그림 IV-19〉 알고리즘과 인공지능(AI)가 지배할 미래 전쟁

나. 화력 분야

1) 포병 / 대화력 / 탄약 / 화생방

- 사표 자동 산출을 위해 공기 밀도 측정 및 고도, 온도, 풍속 등에 따른 변화 자동 계산, 사표 산출 프로그램 및 장치
- 화력 및 사거리 증대를 위해 인공지능(AI) 표적 추적 자동화, 유도화 지능탄 개발
- 기동성 향상을 위해 지형 조건에 따른 인공지능(AI) 안정화 주행장치
- 생존성 향상을 위해 자동으로 오염도 측정 및 전차 내부 밀폐, 공기 정화 기능 개발 여부
- 병커에서 원격조종 사격이 가능한 표적탐지, 추적, 자동 사격장치
- 병사의 안전을 위해 화기 자세에 따라 사격 가능 여부를 자동으로 제어하는 사격 안전장치
- 인공지능(AI) 교전 시스템 : 대테러전과 같은 근접전투에서 교전이 가능한 살상용 인공지능(AI) 교전체계
- 지능탄약 개발 활성화로 사거리 연장, 정밀 표적 타격



〈그림 IV-20〉 지능 탄약의 개념도 예

2) 공격 헬기

- 비행 중 사고 예방을 위하여 외부환경(풍속, 풍향, 기압, 추력, 기류)에 따라 비행 조종을 보조하는 인공지능(AI) 비행 지원 장치
- 조종사 헬멧을 지능화하기 위한 가시영상, 열영상, 가상현실 영상을 통합 제공하는 디바이스
- 대전차 유도탄 사격 후 회피 기능 향상을 위한 인공지능(AI) 추적 유도탄
- 비행 중 전력선 및 미확인 비행물체 탐지 및 회피를 위한 주변 탐지 레이더와 연동하는 인공지능(AI) 주위환경 탐지회피 장치
- 항공기 자동 조종 시스템
 - 항공기에 내장한 조종간과 스로틀을 직접 조작하는 로봇팔이 음성인식으로 작동하는 로봇팔 2개를 기본으로 태블릿을 결들인 항공기 자동 조종 시스템

- 운전석에 설치하면 부조종사 역할을 하며, 조종사는 조종을 맡긴 사이 기상 상황 확인이나 잠재적 문제가 없는지 여부를 모니터링 하거나 휴식을 취할 수 있음



〈그림 IV-21〉 항공기 자동 조종 시스템

- 인공지능(AI) 비행 자율주행 시스템
 - 항공 맵과 비행경로 지정으로 항공 경로를 지정하여 항공기가 자율비행을 통해 목적지까지 비행하며, 비행 중 발생하는 외란에 대응하여 비행하는 기능

다. 지휘통제·통신

1) 인공지능(AI) - 빅데이터 분석 정보체계 구축

- 전투지휘훈련 빅데이터 구축
- 인공지능(AI) 기반 스마트 인재관리 시스템 구축
- 지능형 해안감시체계 구축을 위한 인공지능(AI) 학습 모델
- 밀리터리 ImageNet 구축
- 장병 건강 및 체력 빅데이터 기반 맞춤형 모바일 체력관리 시스템 구축
- 슈퍼 컴퓨터와 인공지능(AI) 기술을 활용한 사격장 산불위험 예측 및 의사결정 지원체계
- 인공지능(AI) / 빅데이터 기반 해안감시체계 구축
- 빅데이터 기를 활용한 지상군(공군) 자원소요 분석모델 개선 및 성능개량 ISP
- 해군 지능형 가상군 모의기술 개발



〈그림 IV-22〉 빅데이터 기반 인공지능(AI) 전투 분석 모델 예

2) 인공지능(AI) 플랫폼

- 인공지능(AI) 및 인지 컴퓨팅 플랫폼 기반 의사 보조 시스템, 중요회의 의사결정 지원시스템, 자연어 이해 및 딥러닝(Deep Learning) 학습기능 등 다양한 인공지능(AI) 솔루션 개발 도구
- 인공지능(AI) 전술계획 수립체계
 - 다양하고 많은 방책의 비교가 가능하며 이렇게 선정된 방책과 우발계획 사이에 다양한 요소와 변수를 고려하여 위계임을 실행
 - 연관관계에 대해서 보다 객관적인 검증결과를 도출하여 방책 및 계획에 대한 검증의 속도가 향상되어 작전의 반응속도가 향상되고 효율적인 작전 수행 가능
- 교리 연구 시스템
 - 기존 훈련 축적 데이터 기반 인공지능(AI) 활용을 통해 직접적인 실기동 훈련 없이 다양한 계획들의 검증과 교리발전 소요를 사전에 식별 가능
- 한국형 제다이 클라우드
 - 인터넷이 끊기거나 어려운 환경, 인트라넷 환경에서도 동작하며, 지금껏 분리돼 있었던 최전선 및 전술적 영역의 데이터를 모두 저장할 수 있고, 이를 인공지능(AI)가 자료를 자동분류하고 분석을 수행

라. 무인화

로봇(Robots)은 체코어의 노동을 의미하는 단어인‘Robota’에서 기원한 것으로 사람과 유사한 감각(시각, 청각, 촉각 등) 및 판단 능력 또는 팔·다리와 같은 조작 및 이동성을 보유한 기계장치를 의미한다. 무인체계라는 용어는 일반적으로 탑승조작 없이 운용되는 로봇을 통칭하며 군사적 용도의 전투 또는 전투지원장비로 활용되는 로봇을 무인전투체계라고 지칭하고 있다. 국방 로봇·무인체계는 운용환경에 따라 지상(UGS, Unmanned Ground System), 해양(UMS, Unmanned Maritime System) 및 공중(Unmanned Aerial System) 무인체계로 구분할 수 있으며 로봇산업 전체 중에서 전문서비스 영역에 해당한다고 볼 수 있다.

전투에서 발생하는 대량의 인명손실은 부정적 여론을 조성하여 국가의 전쟁 수행 자체를 어렵게 할 수 있으며, 출생률 저하에 따른 인구절벽 현상으로 미래 확보 가능한 병력자원은 지속적으로 줄어들 것으로 전망되고 있다. 또한, 지상군의 세대별 책임지역이 확장됨에 따라 소부대의 근접전투시 단위 세대별로 분권화된 감시정찰, 지휘통제, 정밀타격 등의 능력이 요구될 것이다. 이런 측면에서 지상 로봇·무인체계는 치열한 근접전투가 벌어지는 위험지역에서 인명피해를 최소화하고 운용인력을 절감하며, 나아가 자율적인 임무 수행으로 인간 위주의 전투체계를 보완함으로써 세대별 전투 효과를 극대화할 수 있는 수단으로 필요성이 인식되고 있다. 하지만 현 지상 로봇·무인체계의 기술적 수준과 능력을 고려시 전투현장에서 충분한 기동성과 임무수행 능력을 발휘하기는 어려우므로 초기에는 전투원과 유인체계에 대한 보조수단으로 활용될 수 있다. 즉, 장시간 지루하고(Dull), 유해하며(Dirty), 위험한(Dangerous) 임무를 대신하는 차원에서 로봇·무인체계가 필요하며, 미래에는 자율화 및 군집 등 관련 기술들의 발전에 따라 전투원과의 협업 및 자율적인 임무수행으로 전투 효과를 극대화할 수 있을 것으로 전망할 수 있다.

국방 분야 적용을 위한 고려사항으로 첫 번째, 전장상황에서 전투원이 수행하는 본질적인 행위에 대해 어떤 부분을 로봇에게 맡기고 학습시켜 인공지능으로 대체할 것인지 세밀한 분석이 필요하다. 자율주행 차량에게 사람의 운전행위를 학습시키다 보니 ‘인지’ 알고리즘이 카메라에 찍힌 도로 영상에서도 도로 경계면에 집중하고 경계면의 굽어지는 정도에 따라 사람이 운전대를 돌리는 각도를 그대로 학습 하는 결과가 나타났다. 즉, ‘도로를 인지’하고 ‘핸들을 돌린다’는 운전이라는 행위의 본질적 요소를 찾아서 데이터화하고 이를 서로 연결하여 모델에 학습시킬 수 있었던 것이다.

두 번째, 인공지능을 학습하기 위한 신뢰성 있는 Big Data의 구축이 필요하다. 전투 행위 분석으로부터 정의된 본질적인 행위에 대해 입력(Input) 데이터와 입력에 관한 타겟

(Target)을 정하여 많은 수의 Data로 구축하는 것이 매우 중요하다. 잘못된 입력과 타겟을 구축하면 잘못된 모델이 만들어지게 되고 데이터가 너무 적으면 충분히 모델을 학습시킬 수 없기 때문이다. 세계의 주요 자율주행차 제조사들이 수년의 시간을 들여 수백 만 km의 주행데이터를 구축하고, 생성된 주행데이터를 모델에 학습시키는 과정을 보면 그 중요성을 알 수 있다. 이는 KCTC와 같은 과학화 전투체계 및 전투실험을 통해 Big Data를 구축하는 방안의 연구가 필요하다.

세 번째, 전투행위 데이터와 연계하여 전장환경에 대한 초정밀 기본데이터 구축이 필요하다. 한반도의 전장환경에 대한 세밀한 지형정보를 구축하고 그 위에 전투진지, 교통호, 전술도로, 고정 장애물 등의 전투시설 데이터를 정밀하게 구축하는 것이다. 이는 위성을 통해 확보된 한반도 전역의 수치표고모델(DEM, Digital Elevation Model) 및 수치표면 모델(DSM, Digital Surface Model)을 기반으로 정밀한 3D 지형도를 구축하고 항공 영상과 지상이동체의 3D LiDAR 스캐닝 영상을 조합하여 구축할 수 있다. 추가로 해당 지역을 담당하는 부대원과 장비들이 전술훈련이나 진지공사 등을 위해 거점단위로 활동하는 데이터(진지사진, 사경도사진, 이동빈도, 속도 등)도 Big Data화하여 구축이 필요하다. 이는 개발과정에 있는 로봇이나 무인체계가 테스트를 위해 실제 거점과 주변 지역에서 많은 테스트를 하여 그 결과가 축적되고 성능 개선을 위해 활용될 수 있도록 시스템을 갖추는 것도 의미한다.

이러한 과정을 요약하면 ‘전투행위 분석 → 전장환경 Big Data 구축(야외훈련) → 알고리즘 학습(Deep Learning) → 인공지능(AI) 성능향상 → 추가 Big Data 소요도출(야외훈련 필요성 도출)’의 순환구조 형성이 필요함을 의미한다. 즉, 인공지능 기술이 막연하게 전투 효과를 향상시켜 주길 기대할 수 없으며 우리는 전투행위의 본질을 더욱 면밀하게 분석하고 야외 훈련을 통해 발생시키고 축적하며 동시에 인공지능(AI) 알고리즘을 강화시켜 이것이 전투효과로 이어지도록 구조를 형성해야 한다는 것이다.

1) 인공지능(AI) 교전 전투 시뮬레이터

- 공중전투 시뮬레이션은 단위 시점에 미 공군 베테랑 교관의 의도와 행동을 선견적으로 분석해 대응하는 시뮬레이터
- 저비용 무인기 군집기술(LOCUST)과 인공지능(AI) 기술의 접목을 통해 상륙작전에서는 전투병의 상륙 대신 인공지능(AI)이 무장된 드론 떼에 대한 통합 전술작업 수행

2) 하이브리드 형태의 자율순항체계

- 수중과 수상에서 자율적으로 움직일 수 있으며, 대잠수함 작전, 수중 기뢰 탐지, 정찰 및 감시, 해저 탐험, 해안 대테러 작전 등의 임무를 수행
- 수중에 걸쳐 지속되는 감시 임무를 수행하기 위해 첨단 센서가 장착되어 임무 중 촬영한 정보를 초고화질로 관리자에게 전송



〈그림 IV-23〉하이브리드 형태의 자율순항체계 형상

3) 무인 합동 훈련체계

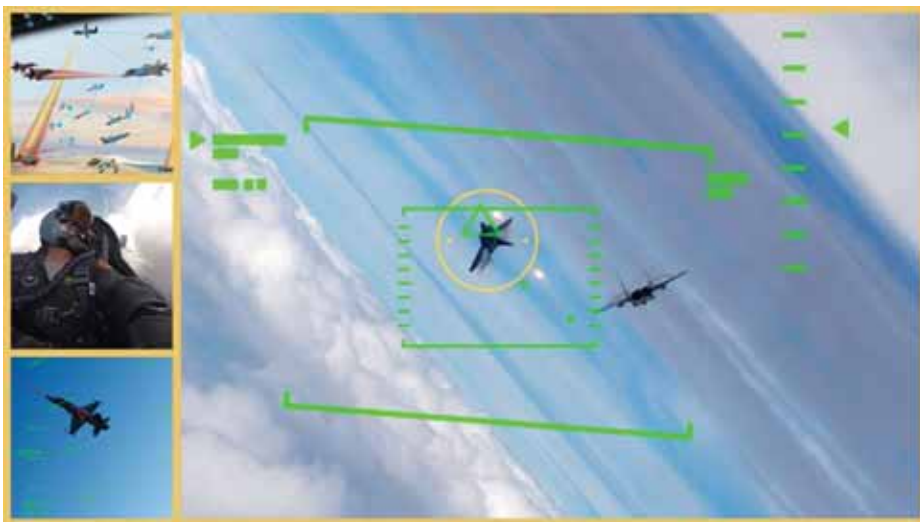
무인 합동 훈련체계는 드론이 서로 정보를 주고받는 합동무인훈련을 진행하는 것으로 항공·수중·지상 드론들이 서로 협력하여 작전을 수행하는 체계이다. 무인잠수정 작전을 통하여 합동 및 다국적 환경에서 기뢰대항책을 세우며 다양한 종류의 무인체계가 서로 정보를 교환하여 유인 지휘통제센터에 답신하는 훈련을 진행한다.



〈그림 IV-24〉유무인 합동 훈련체계

4) 인공지능(AI) 전투기 조종사

2020. 8. 20일(현지시간) 미국 국방성의 연구개발을 담당하는 미국 고등방위연구계획국(DARPA)이 18일부터 20일까지 주최한 알파도그파이트(AlphaDogfight) 모의 공중전 대회에서 헤론 시스템즈(Heron Systems)이 개발한 인공지능(AI) 알고리즘이 파이팅 팰콘(KF-16 Fighting Falcon)의 5가지 기본 전투기 기동 시나리오 시뮬레이션 전투를 통해 인간 F-16 조종사를 5-0으로 녹다운 시켰다고 전했다. 특히 현대전에서 전투기가 차지하는 위상을 생각했을때 이번 DARPA의 결과는 바둑에서의 알파고의 승리보다 더 다가오는 아주 무서운 결과이다. 영공에서 적의 행동에 신속하게 대응하기 위해 모든 영역의 대응 효과를 효율적으로 통합할 수 있는 새로운 AI 기술은 인간의 능력, 상상 이상으로 강력해질 것으로 예상된다.



〈그림 IV-25〉인공지능(AI) 전투 개념 시뮬레이터 영상

■ 소결론

- 국방부는 인공지능(AI) 중점 추진과제별 활용 가능한 분야 식별 및 과제를 도출하여, 인공지능(AI) 시스템을 적용하고자 하는 요구과제별 사업계획의 구체화 가능 분석하고 있음
- 현재 '인공지능(AI) 교관 개발', '지능형 네트워크 트랙픽 분석 및 조치도구 개발', '전투 조종사용 인공지능(AI) 시뮬레이터 개발' 3개 과제에 대한 운용개념과 이에 따른 적용 대상 인공지능(AI) 기술 등을 구체화 및 연구개발 진행 중에 있음
- 4차 산업혁명을 각 산업별 터줏대감들이 주도할 것으로 믿는 이유는 혁신의 원천이 'Data'와 'Operation 경험'이기 때문에 기존 군이 보유한 운용데이터 활용과 운용데이터의 접목과 활용이 필요하므로, 빠른 기술 변화로 Big-Bang 식 추진보다는 Test & Learn을 통해 Use case를 점진적으로 혁신해 나가는 방법론을 채택해야 함
- 인공지능(AI)을 기술을 적용한 국방 분야 활용 방안은 다음과 같음
 - C4I : 지능형 지휘결심지원체계, AI기반의 실시간 M&S 및 위계임 체계, 지능정보센터, 초연결·초지능 네트워크 등
 - 정보 : 지능형 군사정보관리체계(Smart MIMS), 지능형 사이버·전자전 공격/방호시스템 등
 - 화력 : 인공지능(AI) 기술을 적용한 지능탄, 지능형 표적탐지 레이더, 지능형 사격지휘통제체계 등
 - 기동 : 지능형 워리어 플랫폼, 인텔리전트 전투복, 인공지능(AI) 기반 자율 및 군집형 기동체계 등
 - 방호 : 지능형 사이버 방호 시스템, 지능형 사이버전 수행 기술개발, 지능형 과학화 경계시스템, 지휘 시설 및 무기체계의 지능형 방호체계 등
 - 작전지속지원 : 지능형 합성전장훈련체계(LVCG), KCTC와 연계한 AI기반의 지휘결심지원체계, 인공지능(AI) 교관, 인공지능(AI)기반의 훈련 시뮬레이터/전장훈련체계, 정비수요예측시스템/탄약 저장관리 체계, 지능형 물자보충/재고 관리체계, 지능형 안전관리 정보체계/원격치료 시스템, 인공지능(AI) 기반의 인력획득 및 인사관리체계 등
- 인공지능(AI)을 적용하여, 현시점 기준으로 사업화 및 구체화 가능성은 다음과 같음
 - 의료 흉부진단 : 국방의료정보 빅데이터 분석체계 구축사업 연구용역을 통해 흉부 엑스레이 영상 판독 지원시스템 부분의 연구용역을 진행하여, 대학병원과의 연구 경험을 노하우로 군에 최적화된 시스템을 위한 진단 프로세스를 개발
 - 지능진화형 엑소브레인 : 자연어를 이해하여 지식을 자가 학습하며, 인간과 기계의 지식소통이 가능한 지식과 지능이 진화하는 것으로, 언어를 처리하며 판단 및 예측을 통해 문제해결방안에 대한 참모 판단을 대체하고, 의사결정을 지원하는 시스템 개발
 - 인공지능(AI) 아담 : 인간 두뇌 분석을 통한 인공지능(AI) 원천기술로 인공지능(AI) 기술과 가상현실(VR) 및 증강현실(AR) 기술이 결합하여 발전된 사례로 유·무인 체계의 최적 이동경로 수립 및 원격 지원, 임무수행 경로 사전 검증에 활용 가능(유·무인 무기체계 편대들의 시각화된 원격 지휘 통제, 전장의 전투 원격 지휘 통제, 최적 전략, 작전 수립 지원, 가상전장 환경에서의 전투체험, 전투지휘 연습 등)
 - 인공지능(AI) 비서 : 무선 웨어러블 디바이스를 통해 원격지의 병사들에게 작전임무 수행 정보지원, 다국적군과의 작전 수행 시 실시간 언어 통역 비서 역할 수행이 가능
 - 소부대 몰입형 훈련시스템 : 훈련자가 모의이동훈련 시뮬레이터 위에서 이동을 실시할 때 충분한 체감안정도를 유지할 수 있도록 실시간 정밀 제어, 모의이동훈련 시뮬레이터 위의 훈련자 위치 및 자세를 인식, 분대급 전술 시뮬레이터 또는 상용게임과의 연동을 통하여 3D 가상현실 속의 객체들과 탐지, 교전 등의 상호작용을 모의 가능

- 무기체계별 인공지능(AI)을 적용 가능한 분야는 다음과 같다.
 - 기동분야(전차 / 장갑차 / 전투차량)
 - 화력 증대를 위해 인공지능(AI) 표적 추적 자동화, 유도화 지능탄 개발
 - 사격통제장치 분야의 인공지능(AI) 표적 자동 추적장치(포탑 구동장치와 연계)
 - 대전차 유도탄 방어를 위한 인공지능(AI) 방어체계(대전차 로켓 및 유도탄의 탐지, 추적, 요격)
 - 전차 탑재형 인공지능(AI) 무인조종 자동화기(열 감지 및 자동 추적 사격)
 - 기동성 향상을 위해 지형 조건에 따른 인공지능(AI)형 안정화 주행장치
 - 생존성 향상을 위해 자동으로 오염도 측정 및 전차 내부 밀폐, 공기 정화 기능 개발
 - 개인전투체계
 - 자율표적획득장치 연구 : 음원 탐지 기반 적의 방향, 위치, 탐지정보 제공, 사격원점 등 표적/인원 등의 자율탐지, 인식, 위치등록, 추적 및 공유
 - 자율상황인식, 의사결정 장치 연구 : 원시정보와 정보, 영상 기반의 자율인식정보 및 피아 작전 정보를 통합한 자율상황인식을 기반으로 인공지능(AI) 의사결정, 자율적, 반자율적 자산의 하루 임무에 할당
 - 계층별 자율상태인식 및 의사결정 : 인공지능(AI) 기반의 각 제대별 상태 인식과 임무분할, 할당, 수행의 계획과 실행 상태를 전시
 - Wearable 별 원인식 정보 구분 및 활용, 다양한 전시 기능 지원 MMI
 - 지휘통제 체계화 : 전장정보 공유, 초소형 피아식별, 음성/데이터 통신
 - 화력 자동화 : 사거리 증대, 이동표적 정밀타격, 초소형 미사일 장착 운용
 - 화력분야(포병 / 대화력 / 탄약 / 화생방)
 - 사표 자동 산출을 위해 공기 밀도 측정 및 고도, 온도, 풍속 등에 따른 변화 자동 계산, 사표 산출 프로그램 및 장치, 화력 및 사거리 증대를 위해 인공지능(AI) 표적 추적 자동화, 유도화 지능탄 개발
 - 기동성 향상을 위해 지형 조건에 따른 인공지능(AI) 안정화 주행장치
 - 생존성 향상을 위해 자동으로 오염도 측정 및 전차 내부 밀폐, 공기 정화 기능 개발 여부, 병거에서 원격조종 사격이 가능한 표적탐지, 추적, 자동 사격장치
 - 병사의 안전을 위해 화기 자세에 따라 사격 가능 여부를 자동으로 제어하는 사격 안전장치
 - 인공지능(AI) 교전 시스템 : 대테러전과 같은 근접전투에서 교전이 가능한 살상용 인공지능(AI) 교전 체계
 - 지능탄약 개발 활성화로 사거리 연장, 정밀 표적 타격
 - 지휘통제·통신 분야
 - 인공지능(AI) 구현을 위한 빅데이터 분석 정보체계 구축 : 전투지휘훈련 빅데이터, 인공지능(AI) 기반 스마트 인재관리 시스템, 지능형 해안감시체계 구축을 위한 인공지능(AI) 학습모델 등
 - 인공지능(AI) 플랫폼 : 인공지능(AI) 및 인지 컴퓨팅 플랫폼 기반 의사 보조 시스템, 중요회의 의사결정 지원시스템, 자연어 이해 및 딥 러닝(Deep Learning) 학습기능 등 다양한 인공지능(AI) 솔루션 개발 도구, 인공지능(AI) 전술계획 수립체계, 교리 연구 시스템 등
 - 무인화
 - 전투원과의 협업 및 자율적인 임무수행으로 전투 효과를 극대화하기 위해 '전투행위 분석 ⇒ 전장환경 Big Data 구축(야외훈련) ⇒ 알고리즘 학습(딥러닝, Deep Learning) ⇒ 인공지능(AI) 성능향상 ⇒ 추가 Big Data 소요도출(야외훈련 필요성 도출)'의 순환구조 분석시스템 개발
 - 인공지능(AI) 교전 전투 시뮬레이터, 하이브리드 형태의 자율순항체계, 무인 합동 훈련체계, 인공지능(AI) 전투기 조종사 등

V. 정책적 시사점 및 발전방향

1. 인공지능을 적용한 무기체계 획득을 위한 제도개선

4차 산업혁명이 전 세계의 이슈로 부상하면서 산업계의 패러다임이 바뀌는 대전환기가 올 것으로 전망되고 있다. 아직 4차 산업혁명에 대한 정의는 명확하지는 않지만, 컴퓨터 및 인터넷 기반의 3차 산업혁명 시대로에서 ‘초연결 지능사회’, ‘온라인과 오프라인의 융합(O2O)’ 등을 통해 기존 제품의 스마트화·플랫폼화·서비스화로 새로운 기술·제품·시장·서비스 창출을 가능하게 하여 산업계 전반의 효율성과 생산성이 크게 향상될 것으로 기대되고 있다.

방위산업 분야는 대규모 투자와 다양한 첨단기술들의 융·복합으로 국가안보와 국가 경제성장에 새로운 원천이 될 수 있는 잠재력을 가진 미래형 산업이라 할 수 있다. 역사적으로도 주요국들은 방위산업을 통해 4차 산업혁명의 기반이 되는 인터넷, GPS, 무인기, 로봇 등을 군사적 목적으로 개발하고 이를 민수 분야에 파급시켜 국가 신산업 육성과 경제성장에 활용되는 테스트-베드(Test-Bed)로서의 역할을 담당했다. 이에, 미래 국가경쟁력 우위 요소로서 잠재력이 높은 방위산업의 글로벌 경쟁력을 강화하여 국가안보 유지와 함께 국가 경제의 지속 성장을 견인하기 위한 발전전략 수립이 필요하다. 특히, 4차 산업혁명으로 방위산업 분야의 무기체계 첨단화·스마트화·융복합화·플랫폼화·서비스화가 확대되고 있어 이에 대응하기 위한 방위산업 경쟁력 강화 전략을 적극적으로 모색해야 할 시점이다.

조직 및 기능 획득의 예로 영국은 DE&S(Defence Equipment and Support)의 역할에 독립성 및 전문성을 보장함에 따라 이해관계 기관과의 의견 마찰 최소화와 DE&S 전문인력 양성을 위한 적극적인 투자가 이루어지고 있으며, 일본은 PM(Project Management) 중심의 총수명주기 차원의 사업관리로 무기와 장비가 폐기되기까지 전담하고 있다. 터키는 연구개발사업을 통한 획득업무만을 담당하며 해당 단위사업 관리조직은 탄력적으로 운용(한시적)되고, 획득업무는 소요 군에 인도 시까지 한정되어 운용하고 있다.

국방 연구개발 사업을 위한 획득의 예로 미국은 차별화된 연구개발 사업과 이에 연계한 개별 획득절차를 마련하였으며 전력화 지연을 방지하기 위해 연구개발 획득절차를 마련하고 업체의 연구개발 사업 참여를 유도하기 위한 다양한 제도(투자, 지원 등)를 추진하고 있다. 영국은 국내 연구개발보다는 국제 공동개발과 기존 무기체계의 성능개량 중심의 연구개발 사업을 추진하며, 국내 중견·중소 업체의 육성을 위한 연구개발 사업추진 등의

제도를 개선하고 있다. 이스라엘은 신무기 개발보다 기존 무기체계의 성능개량 중심의 개발사업 추진과 최첨단 무기체계의 핵심기술 개발에 집중적인 투자를 추진하고 있다.

민·군 기술협력 사업을 위한 획득의 예로 미국은 사업별 특성에 따른 별도 조직 및 규정 마련하였으며, 다양한 군 투자의 민·군 기술협력 사업추진을 시행하고 있다. 이스라엘은 적극적인 정부 투자에 의해 국내 업체의 참여를 유도하고 있으며, 산·학·연의 활발한 협력 연구개발 사업 마련의 정책을 시행하고 있다. 영국은 군과 산·학·연 간의 국방기술 이전 활성화를 통해 제도를 개선하고 있다.

구매사업을 통한 획득의 예로 호주는 FMS(Foreign Military Sale)를 위한 美 현지 전담조직을 운영하며, 싱가포르의 FMS 지위를 활용한 자국에 적합한 제도를 고안 및 적용을 추진하고 있다.

위와 같은 사례를 살펴보았듯이 우리 국방 분야에서도 획득 조직 및 기능에서 통합 또는 영역 분리를 통하여 업무추진에 있어 혼선 방지가 필요하며, 현 조직의 임무 및 역할을 효율적으로 수행할 수 있는 적정 인력 보충이 필요하다. 이를 위해 IPT(Integrated Product Team) 개념을 최초로 도입한 미국이나 프랑스의 운영형태를 주목할 필요가 있으며, 영국의 IPT도 벤치마킹의 대상으로 판단된다. 국방 연구개발 사업을 통한 획득에서 연구개발 사업추진 시 국내 기술 수준에 대한 명확하고 정밀한 검토 및 검증이 필요하며, 소요의 특성에 따른 차별적 연구개발 획득절차의 차별화를 통해 핵심기술이 확보된 상태에서 현 연구개발 획득절차 보다 간소화 할 수 있는 개별 절차가 필요하다. 민·군기술협력사업을 통한 획득에서 정부 차원의 다양한 투자 사업을 마련하고 업체를 포함하여 대학 및 연구기관 참여를 유도하고 사업별 특성을 고려한 개별 운영조직 및 규정이 필요하다. 특히 중대한 국가안보와 관련된 사업을 추진할 경우 국방부가 주도할 필요가 있다. 구매사업을 통한 획득에서는 FMS 구매를 효율적으로 운영하기 위해 외교적 관계 적용을 통하여 현 FMS 지위를 이용한 능동적 대처 방안을 미 정부에 제시할 필요가 있으며, 이스라엘 및 호주가 현지 FMS 및 상업 구매계약 전담조직을 운영하는 경우에서도 협상을 통해 구현할 필요가 있다.

4차 산업혁명 시대의 도래에 따라 사회적 변화에 적응하고 관련 기술을 활용하여 우리나라 방위산업의 경쟁력 향상을 위한 기본 방향을 제시하면 다음과 같다.

첫째, 4차 산업혁명 시대의 핵심기술을 방산 제품에 적극적으로 적용함으로써 방산 제품의 스마트화를 적극적으로 추진해 나가야 할 것이다. 둘째, 사물인터넷(IoT), 인공지능(AI) 등이 미개발 및 미적용된 분야에 대해서 민간 첨단기술들의 방위산업적용(Spin On)을 확대해 나가야 할 것이다. 셋째, 빅데이터를 활용한 방위산업의 디지털 플랫폼을 구축해 나가야 할 것이다. 넷째, 무기체계의 장기간 활용(20~30년)에 따른 방산 제품과 서비스

연계를 확대해 나갈 필요가 있다. 마지막으로, 4차 산업혁명 시대의 관련된 인프라 구축과 규제 해소에 집중해 나가야 한다. 규제 해소를 위해서는 방위산업의 진입장벽 완화를 위한 관련 제도개선이 무엇보다 필요하다.

4차 산업혁명 핵심기술들의 방위산업 분야 적용을 확대하기 위해서는 무엇보다 현존하는 다양한 진입장벽을 획기적으로 완화할 수 있는 방안은 다음과 같다.

첫째, 현행 방위산업의 독과점적 시장구조에 기인하는 높은 진입장벽의 완화가 필요하다. 4차 산업혁명 기술들이 방위산업 분야에 진입 확대를 위해서는 현행 방산물자지정제도의 획기적인 개선이 필요할 것으로 보인다. 우선 1,400여 종에 달하는 방산지정물자를 필요성, 전략·비닉 물자 여부, 민간기술력 수준 비교 등을 통해 재분류해야 할 것이며, 무기체계 완제품 외에 세부부품 단위까지도 방산물자로 지정하여 독과점적 지위를 보장하는 점에 대해서 완화할 필요가 있다. 특히, 주로 중소·벤처업체가 4차 산업혁명 기술력을 보유하고 있다는 점을 고려한다면, 현행 방산물자지정제도는 높은 진입장벽으로 작용할 가능성이 매우 크다고 판단되기 때문이다. 또한, 국내 대형 방산 업체들이 기존 무기체계 성능개량이나 신규 무기체계 개발에 4차 산업혁명 기술력을 보유한 중소·벤처 업체를 활용한다면 다양한 인센티브를 부여할 필요성도 있다. 있다. 정부에서 필요로 하는 4차 산업혁명 기술을 보유한 업체가 무기체계 개발 또는 성능개량에 참여할 경우에도 자금지원과 가점 인정 등이 고려되어야 할 것이다.

둘째, 4차 산업혁명 기술 적용간 군사보안 완화와 군사보안 완화가 필요하다. 인공지능(AI) 사업 부진 원인으로 '빅데이터 구축 등에 따른 과도한 군사보안 적용'으로 분석되었다는 점도 주목할 필요가 있다. 미국 GE사 보안담당자와의 인터뷰에서도 'Predix'라는 디지털 플랫폼 구축에 가장 큰 애로사항으로 미 국방성과의 군사보안 문제를 언급하였다. 이에 대해 해당 업체와 미 국방성간에 주기적인 회의를 통해 문제를 최소화하는 방안을 찾고 있는 것으로 파악되었다. 우선적으로 무기체계의 정비와 운영유지간 필요한 시스템 구축에 빅데이터 구축 등을 추진할 필요가 있다. 필요시에는 네이버, 다음 등 국내 관련 대형 업체와의 협력을 통해 시범사업 등을 추진할 수 있을 것이다. 이를 통해, 군사보안 관련 현안 문제들을 해소하고 군 사이버보안 역량을 강화할 수 있도록 중장기적인 대안 마련이 필요할 것으로 보인다.

셋째, 4차 산업혁명 위원회 내 방위산업분과 신설이 필요하다. 4차 산업혁명 위원회 내 방위산업 분과를 신설하는 문제 또한 검토해 볼 수 있을 것이다. 방위산업 분야는 전통적으로 기술혁신이 늦은 편이며, 제도·정책 발전도 더딘 분야이기 때문에 하루가 다르게 발전하는 4차 산업혁명 기술들을 방위산업 분야에 적용하기 위해서는 국방부와 방사청 등 관련 부처 역량만으로는 해결하기 힘든 문제가 있을 수 있을 것이다. 앞서 제시한

군사보안문제와 함께, 현행 독과점적 시장구조문제, 방산원가 제도에 따른 원가절감 유인 부족 문제와 정부소유의 지식재산권 문제 등 다양한 분야에서 4차 산업혁명 핵심기술들의 방위산업 분야 적용을 가로 막을 수 있을 것으로 예상되는 바이다. 이를 해결하기 위한 대안으로 정부 차원의 거버넌스(Governance)가 필요할 것으로 판단된다. 현재 국과심과 민군특위 등에서 4차 산업혁명 기술의 방위산업 분야 적용 확대를 위해 노력을 배가하고 있지만, 그럼에도 불구하고 정부 최고 수준의 컨트롤 타워가 존재할 필요가 있다. ‘4차 산업혁명 위원회’ 내에 방위산업 분과를 신설한다면 이러한 규제 해소와 범부처 협력의 중심 역할을 할 수 있을 것으로 판단된다.

넷째, 쌍방향 무기소요제기 시스템 구축이 필요하다. 4차 산업혁명 핵심기술력을 보유한 국내 업체가 방위산업에 진입하기 위해서는 현행 소요군 만의 일방적 소요제기 방식이 아닌 방산업체의 Bottom Up식 소요제기 방식의 병행으로 개발 예산 절감 및 업체투자 유도를 병행할 필요가 있다. 4차 산업혁명 시대 특징 중 하나로 수요자의 요구에 즉각적으로 대응하여 서비스 및 제품을 제공할 수 있는 ‘온-디맨드(On Demand)’ 경제를 활성화가 있기 때문이다. 이를 위한 필수조건 중 하나가 바로 수요자와 공급자 간에 적시적인 정보 공유체계를 마련에 있다. 이를 고려하여, 소요군에서 4차 산업혁명 기술 소요를 인터넷을 통해 공개하고, 이를 국내 방산업체와 4차 산업혁명 기술력을 보유한 민간업체들을 조사·분석하여 정부 주도 또는 정부-기업 간의 매칭 형태로 관련 사업들을 추진할 수 있을 것이다.

2. 중장기적인 인력양성 및 기술개발

2016년 세계경제포럼(WEF)에서 4차 산업혁명(The Fourth Industrial Revolution)이라는 개념이 등장한 이후 전 세계적으로 혁신 성장에 대해 강한 요구가 발생하고 있다. 특히, 알파고를 통해 널리 알려진 인공지능(AI)은 범용 기술로서의 특성을 가지고 있어서 보다 다양한 산업분야에 확산되어 사회·경제적 부가가치를 창출하고 있다. McKinsey 2018. 4)에 따르면 미국의 19개 전통 산업과 9개의 비즈니스 영역에서 인공지능(AI) 기술을 접목할 경우, 연간 3.5~5.8조 달러 규모의 경제적 효과 창출이 전망하고 있다.

주요국들은 4차 산업혁명의 핵심 동력이라고 할 수 있는 인공지능(AI)의 기술 선도를 위해 적극적인 투자를 하고 있지만, 전문 인력이 부족하여 인재확보 경쟁이 매우 치열하다. 국가·산업 분야를 막론하고 인공지능(AI) 전문가가 부족한 실정이며, 인공지능(AI) 선도국인 미국, 중국, 영국 등 국가들도 인공지능(AI) 경쟁력의 핵심인 우수 인재확보를 위한 대책을

마련하고 있다. 우리나라도 인공지능(AI) 육성 및 인력양성 정책을 추진하였으나 경쟁국 대비 기술력은 물론 전문인력의 양적·질적 수준은 여전히 미흡한 수준이며, 지능정보산업 발전전략(2016. 3), 지능정보사회 중장기 종합대책(2016. 12), 4차 산업혁명 대응계획(2017. 11) 등에서 인공지능(AI) 관련 정책들을 발표하였으나, 2017년 인공지능(AI) 기술력은 중국에 역전되는 등 경쟁국과의 기술 격차가 심화되고 있는 추세에 있다. 인공지능(AI) 전문인력 부족도 심각하여 삼성전자, LG전자 등 기업은 부족한 인공지능(AI) 인력 확보를 위해 미국, 캐나다 등 해외에 연구센터 설립하고 있는 실정이다.

이처럼 인공지능(AI) 시장규모 확대에도 불구하고 전 세계적으로 산업계에서 필요로 하는 인공지능(AI) 인제는 전 세계 인공지능(AI) 인재 규모는 20~30만 명 수준으로 절대적으로 부족한 상황이다. 향후 필요 인력 수요는 점차 확대되는 반면 인재육성 및 확보가 어려워 수급 불균형은 더욱 심화될 전망이다.



〈그림 V-1〉 국내외 AI 인재 현황

세계 인공지능(AI) 시장에서 필요한 인제는 100만명 정도로 추정하고 있으나 전 세계 인공지능(AI) 인재 규모는 약 30만 명(산업계 20만 명, 학계 10만 명)에 불과한 수준이다. 매년 인공지능(AI) 연구소를 갖춘 교육기관 367곳에서 인공지능(AI) 졸업생이 약 2만 명 배출되고 있으나, 수요에 비해 현저하게 부족한 실정이다. 글로벌 인공지능(AI) 인제는 상위 10개 국가에 60% 이상이 분포하며, 국내는 1.3%로 세계 15위 수준이다. 인공지능(AI) 고급인제는 대부분 미국, 중국, 유럽에 집중되어 있으며, 한국은 405명(1.8%)에 불과하는 등 인재 쏠림 현상이 심각하다³³⁾. 국내 인공지능(AI) 중소·벤처기업은 인공지능(AI)

인재난을 가장 시급한 문제로 인식하며, 기술력 한계 요인으로 자금보다 인재 부족을 최우선 과제로 꼽고 있는 실정이다.³⁴⁾

주요국의 인공지능(AI) 인재양성 정책 현황을 보면 전 세계 주요국은 인공지능(AI) 기술이 향후 국가경쟁력을 좌우할 것으로 인지하고, R&D의 근간이 될 인공지능(AI) 핵심인재 육성을 위해 범정부 차원의 대응 전략 수립하고 있다.

미국의 트럼프 정부는 인공지능(AI) R&D 전략 발표 및 인공지능(AI) 이니셔티브를 통해 인공지능(AI) 경쟁 우위 확보를 위한 기초교육 중심의 정부 정책 추진으로 2018년 백악관은 산·학·연이 참여한 인공지능(AI) 서밋회의에서 국가차원의 인공지능(AI) R&D 지원 및 교육강화, 규제 개선 등이 포함된 “모든 미국인을 위한 AI(AI for the American People)”를 발표하였다. 이어 대통령 산하 인공지능(AI) 특별위원회를 설치하고, 인공지능(AI) 글로벌 리더십 강화를 위한 국가전략 프레임 워크인 ‘The American AI Initiative’³⁵⁾를 발표하였다.



〈그림 V-2〉 미국의 AI 관련 정책 추진 현황

미국의 ‘인공지능(AI) 이니셔티브(2019)’에서의 인공지능(AI) 인재정책의 주요 내용은 다음과 같다.

- 직무훈련 및 재교육 : 정부 지원과 민간의 적극적 참여를 통해 고용 환경 급변에 따른 노동자를 보호하고 재교육 프로그램 확대 및 새로운 직무 개발
- 견습제 : 인공지능(AI) 초급 기술직 구직자와 고용주 간 상호 니즈를 충족할 수 있도록 ‘견습생³⁶⁾ 확대 TF’를 설립하고 필요 분야를 중심으로 확대
- STEM 교육 : 미래 STEM 인력 준비를 위해 미국 STEM 교육의 목표를 제시한 ‘연방 5개년 STEM 교육전략계획’을 발표하고 실행과제³⁷⁾ 추진

33) China AI Development Report, 중국 칭화대학 과학기술정책연구소(2018), Golbal AI Talent Report 2019.

34) '19 대한민국 인공지능(AI) 대상 수상자(중소·벤처 AI 우수기업 임원 21명)대상 설문 조사('19.11월)

35) American AI Initiative, 각 프로그램 웹사이트, IITP(2019), 연방정부의 AI R&D 우선 투자, AI 기술교육 제고, STEM교육 강화 등 포함

36) 견습제 제도는 높은 수준의 스킬 분야의 기업인력 수요 충족을 위한 유급 기반 실무 교육 프로그램

- R&D 인력 훈련 : 연방 주요 부처에서는 교육 연수, 펠로우십 등의 R&D 인력 훈련 프로그램을 통해 인공지능(AI) 교육 프로그램 지원 및 확대
- 일반적인 박사급 펠로우십의 경우 저명한 연구자들로 구성된 패널이 신청자 연구 계획서의 과학적 강점, 학술·연구실적, 추천서 등을 토대로 순위를 매겨 평가하여 통상 연구지원 기간 동안 평균 연 생활비는 연구자당 50,000~60,000달러에 추가로 여행비 5,000~ 10,000달러 지급

기관	프로그램명	지원 및 활동 내용
미항공우주국 (NASA)	NASA STEM Engagement	• 학생과 일반이 NASA의 탐험과 발견에 기여할 수 있는 기회 제공 • 학생들이 NASA 전문가, 콘텐츠 및 시설을 경험하게 함으로써 다양한 미래 STEM 인력 양성 기반 구축
국립과학재단 (NSF)	Graduate Research Fellowship Program(GRFP)	• 과학 엔지니어링 인력의 다양성과 경쟁력 확보를 위해 STEM 분야 우수 석박사급 학생을 대상으로 3년간의 연구 장학금 지원
국립표준기술 연구소 (NIST)	Graduate Student Measurement Science and Engineering(GMSE) Fellowship Program	• 박사급을 대상으로 한 측정 과학 엔지니어링 연구와 관련된 NIST 부설 연구소 랩 경험 축적 및 연구 자금 지원 • 국가물리과학컨소시엄(National Physical Science Consortium, NPSC)의 연구 지원 자금을 통해 프로그램 관리
	NRC Postdoctoral Research Associateships Program	• 국립학술연구위원회(NRC)와의 협력 하에 관리되는 전국 단위의 우수 포닥 프로그램을 지원하는 프로그램 • NIST의 주요 연구 도메인과 관련된 분야를 대상으로 함
	Professional Research Experience Program(PREP)	• STEM 분야의 학사/석사/포닥/박사급 연구원의 NIST 부설 연구소 랩 경험 축적 및 연구 자금 지원
국방부 (DoD)	National Defense Science and Engineering Graduate Fellowship	• 국방부 주력 STEM 분야와 관련된 박사학위 지원자를 대상으로 한 연구 자금 지원
에너지부 (DoE)	Computational Science Graduate Fellowship	• 고성능 컴퓨팅을 활용한 과학 및 엔지니어링 문제 해결 분야의 박사 학위 연구자 지원 • 펠로우십 이후 에너지부 소속 연구소 등 에너지 관련 연구 기관 진출

〈그림 V-3〉 미국 주요기관의 R&D 인력 연수 프로그램

중국은 인공지능(AI)을 국가 전략산업으로 지정하고 정부 주도의 교육과정 신설을 통해 인공지능(AI) 생태계 조성 및 중장기적인 대규모 인공지능(AI) 인력양성 정책을 추진하고 있다. 차세대 인공지능(AI) 발전계획(2017. 7)은 세계적 과학기술 강국 건설 및 혁신적인 인공지능(AI) 국가를 목표로 하며, 세부 전략으로 ‘고급 인공지능(AI) 인재 훈련 및 확보

37) 전략적 파트너십 개발 및 강화, 주요 STEM 분야 교육 촉진, 컴퓨터 리터러시 기반 구축, 투명성과 책임성 제고, 입각한 STEM 정책 운영 추진

추진’을 포함하며, 2030년까지 인공지능(AI) 핵심 산업 1조 위안, 연관 산업 10조 위안 규모의 시장육성을 추진 중에 있다. 대학 인공지능(AI) 혁신 행동계획(2018)은 차세대 인공지능(AI) 발전계획의 인력양성 방안을 실행하기 위한 교육부의 세부 계획으로 대학 등 고등 교육기관의 인공지능(AI) 기술혁신 및 인재양성에 대한 세부방안을 제시하고 있다.

구분	주요 내용
고급 AI 인재 영입을 위한 정책 실행	· 신경인지, 머신러닝, 지능형 로봇 등 분야 국제 전문가 영입 · ‘천인계획’과 같은 기존 인재 유치 프로그램들도 AI 인재 영입에 활용 · AI 인재 영입을 위한 기업체 및 연구기관 지원 정책 개선
AI 교육 체계 수립	· AI 분야 교과목 체계 개선 및 전공 신설, AI 전공 석박사 인력양성 · 수학, 물리학, 생물학 등 타 학문과 결합된 ‘AI+X’모델 추구 · 산·학·연 협력(AI 교육 체계 개발) 강화
단계	주요 내용
대학 학과목 개선	· AI와 컴퓨터, 양자, 신경과학, 수학, 경제학, 사회학 등 통합 강화 · 컴퓨터 공학 및 기술 교과목 내 AI 교과 개설
전문역량 강화	· 우수 공학자 교육 및 훈련 프로그램 강화, 대학생 인재 역량 강화 · AI와 타 학문 융합을 위한 ‘AI+X’ 모델 추진(20년 100개 복합전공 신설)
강의교재 개발 강화	· AI 분야 성과 및 자료들을 교육, 강의 자료로 활용 · AI 핵심 내용을 교재, 온라인 강의로 개발(20년 세계적 수준의 교재 및 온라인 강의 개발)
인력양성 강화	· 협동교육 체계 개선, 대학과 산업 간 협력 강화 · AI 단과대학, 연구소 설립 등 지원(~20년 50개)
보편적 교육 강화	· AI 공공 서비스 플랫폼 개발, 대학 내 비학위 AI 프로그램 개설 · 교수의 AI 초등학교 교육 지원, 초중고 교사 AI 교육 강화
국제 교류 협력 강화	· AI 분야 선진국 유학 장려 및 국가 장학금 지원 · UNESCO 중국 기업가정신 연맹을 통해 국제 교육 및 협력 강화

※ 출처: 中华人民共和国教育部(2018)

〈그림 V-4〉 중국의 차세대 인력양성계획과 주요 추진 내용

- 대학 인공지능(AI) 인재 국제양성계획(2018. 4)은 교육부와 인공지능(AI) 최고기술 보유국인 미국과 공동으로 인재를 양성하기 위한 정책 추진
 - 5년 내 인공지능(AI) 전공 교수 500명, 학생 5,000명
 - 中-美 대학 인공지능(AI) 교육 및 연구 교류협력을 위해 현직 대학교수를 선발 하여 무료 교육을 진행(교수 AI 육성반)하고, 교육과정 이수자는 향후 AI 분야 교원으로서 후학을 양성할 수 있도록 유도
 - 캠프(Camp) 프로그램을 운영하여 기계학습, 심층학습, 자연어 처리 교육 및 현실 응용문제를 해결할 수 있는 방안 모색

- 학술적·실전적 인공지능(AI) 훈련 프로그램, 학생 600여 명, 20개 이상 기업이 참여
- 세계적 수준의 해외 학자, 기업가, 전문 기술인재, 경영 인재 등을 영입하는 국가 프로젝트(2008) 천인 계획 추진
 - 핵심기술 발전, 첨단기술 산업 발전, 신흥학문 발전 추진을 위해 전략적으로 과학자와 리더급 인재들을 유치하고, 중국의 기술혁신 및 창업에 종사할 수 있도록 지원

일본은 인구 고령화 등 사회문제를 안고 있기 때문에 경제 활성화를 위해 인공지능(AI)을 적극 활용하는 정책을 추진하고 있으며, 인력양성을 필수 요소로 제시하고 있다.

- 인공지능(AI)정책 컨트롤 타워³⁸⁾로 총무성, 문부과학성, 경제산업성이 합동으로 ‘AI 기술전략회의’를 설치(2016)하고 내각부 종합과학기술 혁신회의(CSTI)가 의장을 담당
 - 이후 과학기술 관련 내각부 산하 협의체들의 기능을 합친 ‘통합혁신전략추진회의’를 설치(2018)하여, AI를 전략분야로 선정하고 CSTI가 전략 사령탑으로서의 기능을 수행
 - 통합혁신전략을 토대로 CSTI가 주축이 되어 인공지능(AI) 활성화와 인력양성 정책을 추진하고 있으며 주요 대학의 인공지능(AI) 인재 양성 본격화³⁹⁾



〈그림 V-5〉 일본의 AI 연구체계

38) 일본 총무성, “정보통신심의회 정보통신기술분과회의 117-2 회의록, KISTEP.

39) 주요 대학(도쿄 공대, 사이타마공대 등)은 '19년 4월 이후 AI 전문가 양성을 위한 학부·전공 개설

- 교육 초 과정에서 인공지능(AI) 역량을 배양시킬 수 있도록 단계적인 인력양성 정책을 추진
 - (일본 재흥전략) 범부처 차원에서 정보통신기술(ICT) 활용 극대화 전략 및 인공지능(AI) 중심의 대규모 국가 프로젝트(차세대 AI R&D 등) 필요성 제시(2016. 4)
 - (미래투자전략 2018) 국가적 경제성장 전략 수립을 위해 인공지능(AI) 시대에 대응하는 인재 육성 및 최적 활용방안을 포함(2018. 6)
 - 수리, 데이터 교육 강화, 인공지능(AI) 산·학·연계 교육 확대, 인공지능(AI) 스킬 표준화 등
 - (AI 기술전략 실행계획) 인공지능(AI) 기술전략을 구체화하기 위한 실행계획을 발표하고 장기적으로 부족할 것으로 예상되는 AI·IT 인재 확보 및 산·학·연 역할을 제시(2018. 8)
 - 첨단 인공지능(AI) 인재 연 2~3만 명 육성 및 일반 IT 인재 15만 명 육성 추진
 - (통합혁신전략추진회의) 과학기술 혁신을 목표로 하는 ‘통합혁신전략’을 발표하고 정책적 집중 강화 분야로 AI를 선정(2018. 9, 2019. 3)
 - 일본 전체 대학생(50만 명) 대상으로 인공지능(AI) 기초교육 실시, 인공지능(AI) 전문인재 25만 명 양성, 재직자(2천 명) 대상 인공지능(AI) 실무교육 추진, 교육 인프라 개선 등 인공지능(AI) 중심으로 교육 개혁
- 인공지능(AI) 전략은 전 국민을 대상으로 하는 인공지능(AI) 교육과 인재양성에 대한 정량적 수치 제시(2019.3)
 - 초·중·등 교육은 보다 많은 국민이 인공지능(AI) 기술을 활용할 수 있는 역량을 키울 수 있도록 인공지능(AI)의 기반이 되는 STEM 교육과 컴퓨터 프로그래밍 편성
 - 인공지능(AI) 전문 인재라 할 수 있는 대학 교육에서는 연간 25만 명(일본 전체 대학생 수의 50%) 양성을 목표로 하며, 세계 수준의 인재는 연간 2천 명, 최고급 인재는 연간 100명을 양성한다는 계획

영국은 인공지능(AI) 전문인력 양성을 위해 2017년부터 세 가지 인공지능(AI) 인재양성 정책을 추진⁴⁰⁾하고 있다.

40) 한국보전사업진흥원(2019), SPRi(2019)

정책 명	인재양성 정책 내용
영국 AI 산업 발전 (‘17.10.)	• AI 전문인력 공급 개선을 위한 6가지 권고사항 제시 - AI 관련 교육 및 멘토링, AI 석사과정 금전 지원(300명), 비전공자의 AI 전공 전환 지원, AI 박사과정 200개 추가 개설 - AI MOOC 개설 지원 및 STEM 교육 실시, AI 전문가 연구 지원
산업-전략-AI분야 합의안 (‘18.4.)	• AI 인재양성의 정부 정책안 : 2025년까지 최소 1,000개의 정부 자원 박사과정을 확보하여 고급인재 양성 및 산학협력 확대, 비자 제도 개선을 통한 글로벌 고급인재 확보 • 산업계의 AI 인재양성 : 청소년 AI 교육을 통해 진로 탐색 프로그램 운영, AI Council 운영
영국의 AI : 준비, 의지, 가능성 (‘18.4.)	• 영국 상원 AI 특별위원회는 AI 발전을 위해 25억 파운드 기금을 조성 • AI 인재양성 방안 - 숙련된 AI 개발자 양성 : AI 박사과정 확대, 단기 비학위 프로그램 - 다양한 인재 영입 : 여성, 소수인종 등

〈그림 V-6〉 영국의 AI 인재 양성 정책

프랑스는 인공지능(AI) 인재양성 및 연구확산을 위한 기초교육 강화, 인공지능(AI) 윤리 교육추진, 생태계 구축 등 기반 마련을 위한 정책 방향 수립하고 있다.

- (프랑스 AI) 프랑스 고등교육연구 혁신부는 인공지능(AI) 정책 보고서를 통해 인공지능(AI) 연구확산 및 인공지능(AI) 인재양성정책을 제안⁴¹⁾(2017. 3)
- (AI의 함의 : 국가와 유럽의 전략) 인공지능(AI) 인재양성 및 연구혁신, 인공지능(AI)로 인한 노동시장 변화에 대한 정책방향을 제안(2018. 3)

우리나라의 인공지능(AI) 인재양성 정책 현황을 보면 다음과 같다.

- ‘인공지능(AI) R&D 전략’을 통해 구체적인 인공지능(AI) 인재양성 목표와 추진전략을 구체화하며 본격적인 인공지능(AI) 인재양성 정책⁴²⁾ 시작(2018. 5)

정책 명	인재양성 정책 내용
AI 연구 혁신	• 학제 간 및 범유럽 AI 연구소 구축 • 프랑스 인재 유출 방지 및 해외 인재 유입 촉진 방안 마련 및 AI 고급 전문가 양성 • 산학 교류 확장 및 프로젝트 장려 • AI 분야 연구자 공무원 임명 • 스타트업 기업 창립 장려
노동시장 변화 대응	• AI 전문가 양성 및 노동 구조 변화 대응을 위한 공공 연구소 설립 • 초중등 교육과정의 창의교육 강화 • 대학교육 내 AI 관련 커리큘럼 및 교육과정 신설 • 수학 및 정보통신기술 과목 교육 강화

〈그림 V-7〉 한국의 AI 인재 양성 정책

41) 초·중·고 인공지능(AI) 관련 교육과정 개설, 인공지능(AI) 교육 생태계 구축을 통한 융합 연구추진, 국가 차원의 인공지능(AI) 교육 자료 발간, 교육부 내 인공지능(AI) 관련 부서 및 공무원 양성

42) IITP(2018)

구 분	학 력	2018	2019	2020	2021	2022	합계
수급차	초 급	24	96	125	186	240	671
	중 급	77	296	393	556	726	2,048
	고 급	702	1,177	1,394	1,803	2,167	7,268
	합 계	802	1,569	1,902	2,555	3,133	9,986

학교	내용	개원시기	정원('20년 현재)
고려대	과기부 AI대학원 지원사업 선정	'19년 9월	50명(석박사포함)
성균관대	과기부 AI대학원 지원사업 선정	'19년 9월	50명(석박사포함)
KAIST	과기부 AI대학원 지원사업 선정	'19년 9월	60명(석박사포함)
포항공대	과기부 AI대학원 지원사업 선정	'20년 3월	50명(석박사포함)
GIST	과기부 AI대학원 지원사업 선정	'20년 3월	50명(석박사포함)
연세대	AI석사과정 신설, 과기부 AI대학원 지원사업 선정	'19년 석사과정 개설 '20년 대학원 개원예정	50명(석박사포함)
UNIST	과기부 AI대학원 지원사업 선정	'20년 9월 예정	40명(석박사포함)
한양대	과기부 AI대학원 지원사업 선정	'20년 9월 예정	40명(석박사포함)
서울대	데이터사이언스 대학원	'20년 3월	55명(석사 40, 박사15)
중앙대	AI대학원 개원 예정	'20년 신입생 모집 예정	00명
서강대	컴퓨터공학과 내 AI석사과정 신설	'20년 3월학과 신설 예정	00명

주) 초급 : 전문대 + 기능대 + 산업대, 중급 : 4년제 대학, 고급 : 대학원(석·박사)

〈그림 V-8〉 한국의 AI 인세 수급 현황 및 대학원 현황

- 또한, '인공지능(AI) 국가전략'에서는 '세계 최고의 인공지능(AI) 인재양성 및 전 국민 인공지능(AI) 교육'을 추진 전략으로 제시하며, 고급인재와 융합인재 육성뿐만 아니라 전 국민 대상 인공지능(AI) 교육을 실시할 수 있도록 교육 체계 변화 추구(2019. 12) - 인공지능(AI) 인재상을 구체화함으로써 맞춤형 인재양성 프로그램 추진⁴³⁾
- 이에 세계 수준의 연구역량을 갖춘 인공지능(AI) 석·박사급 고급 인재를 양성하여 인재 부족 현상을 완화하고 미래 인공지능(AI) 경쟁력을 강화하기 위한 인공지능(AI) 대학원 사업 추진
- SPRi는 2018년부터 2~22년까지 누적 9,986명의 수급차가 발생할 것으로 조사하였으며, 그 중 석·박사급 고급 인재 부족은 7,268명(73%)으로 가장 시급한 과제로 부각

43) AI 고급인재 : AI 난제 해결, 새로운 모델과 알고리즘 개발, 'AI 전문인재' : AI 플랫폼, 시스템 개발, 'AI 실무인재' AI Tool, SW를 산업분야에 응용(AI+X), '일반 국민' AI 소양 (이용 역량, 윤리·인문 소양)

- 인공지능(AI) 대학원은 2019년에 5개 대학(KAIST, 고려대, 성균관대, 광주과학기술원, 포항공대)이 선정되었으며, 2020년에는 3개 대학(연세대, 울산과학기술원, 한양대)이 선정
 - 선정 대학에는 최고 수준의 인공지능(AI) 알고리즘·시스템 등을 설계·개발할 수 있는 최고급 전문가를 양성할 수 있도록 5년에서 최대 10년간 연 20억 원을 지원
 - 이를 통해 인공지능(AI) 특화 커리큘럼 개발⁴⁴⁾, 인공지능(AI) 전문교원 확보(2019년 78명, 2020년 91명), 해외 연구교류 등 인공지능(AI) 전문교육 체계를 마련

전 세계 인공지능(AI) 인재 규모는 약 20~30만 명으로 추정되나, 산업계에서 요구하는 인공지능(AI) 인재 규모는 100만 명으로 현 공급 수준으로는 인재 수요를 충족할 수 없기 때문에 향후 수급 불균형에 따른 산업 생태계 혼란을 최소화하기 위해서는 인재 양성방안 마련이 반드시 필요하다.⁴⁵⁾ 미국, 중국, 일본 등 주요국은 인공지능(AI) 인재확보에 국가적 역량을 집중하고 있으며, 인공지능(AI) 인재확보를 위한 경쟁은 더욱 치열해질 것으로 예상됨에 따라 우리나라도 국가 차원에서 전략적 대응이 그 어느 때보다 필요한 시점이다.⁴⁶⁾ 최근 코로나 19 여파로 해외 인재 영입 등이 어려워지면서 국내 인공지능(AI) 인재 양성의 필요성 및 중요성 더욱 부각되고 있다.⁴⁷⁾ 특히, 인공지능(AI) 핵심인재(h-index 상위 10%)는 소수 국가에 집중되어 있어 인공지능(AI) 격차 해소를 위한 석·박사급 고급인력 양성 체계 구축 및 질적 고도화가 필요하며, 핵심 인재가 포진한 국가는 인공지능(AI) 전문가 양성 및 고용, 기술혁신 주도권을 가질 것으로 예상되며 그렇지 못한 국가와의 격차가 점차 심화될 전망이다.

우리나라가 추진하고 있는 ‘인공지능(AI) 대학원’ 사업은 사업이 종료되는 2031년까지 약 3,600명 정도의 석·박사 인재를 배출함으로써 인공지능(AI) 고급인재 부족 해소에 기여 할 것으로 예상⁴⁸⁾된다. 도입기인 인공지능(AI) 대학원의 질적 고도화 및 성과확산을 위해서는 체계적인 커리큘럼 개발, HW·SW 인프라 확충, 실증적 교육 연구 협업 환경 구축, 교원확보, 글로벌 네트워크 활성화 등 추가적인 프로그램 추진이 필요하다.

또한, 인공지능(AI)에 대한 사회적 수용성(Public Acceptance) 향상을 위한 보편적 교육 확대로 재능 있는 인재가 모여 세계 최고의 인공지능(AI) 인재로 성장할 수 있는 토양을 마련하기 위해서 초·중·고 단계부터 인공지능(AI) 지식을 습득하기 위한 STEM

44) 기계학습, 딥러닝 등 AI 분야 특화교육 과정('19년 선정 대학의 경우 총 208개 과목)을 개발·편성

45) 국내 AI 인력 수급차(SPRi) : '18년~22년 누적 9,986명 부족

46) 중국('18~'22년내 AI교수 500명, 학생 5,000명 육성 목표), 일본(AI응용인재 年 25만명 양성 목표), 영국(민·관 협력 AI인재 양성 추진) 등

47) “사실상 신규채용 제로” 코로나禍 AI인력가뭄 최악(아시아경제, '20.6.30)

48) '19년 5개 선정, '20년 3개, '21년 2개 대학 선정 가정

교육 강화, MOOC 개발, 인공지능(AI) 비학위 프로그램 개설 및 기존 인공지능(AI) 인재의 재교육 등 사회 전반에서의 인공지능(AI) 활용 능력 제고를 위한 교육 프로그램 확충이 필요할 것이다.

3. 인공지능 R&D 정책과 연계한 협의체 구성방안

인공지능(AI) R&D 전략의 실행력 확보를 위해 ‘인공지능(AI) 전략협의체’ 구성·운영을 통해 추진체계 마련이 필요하며, 협의체 구성은 복지, 산업, 행안, 국방 등 정부부처 공무원(실국장급)과 민간위원(산·학·연 전문가)으로 구성하며, 위원장은 과학기술정보통신부 2차관으로 하여 분야별 전략이 연계·통합 관리될 수 있도록 인공지능(AI) 전략 협의체의 하위 분과로 기술·인재·기반 분과 운영이 필요하다. 협의체의 역할로는 중점 과제 추진 상황, 기술·정책 환경 변화에 따른 R&D 전략 및 목표 재점검, 기술-인재-기반 분야의 핵심과제 세부 추진전략을 마련한다. 협의체의 운영은 분기별 1회 운영을 원칙으로 하되, 기술-인재-기반 분과별로 안건 수시 논의가 필요하다.



〈그림 V-9〉 인공지능(AI) 전략 협의체

‘인공지능(AI) 전략협의체’ 구성·운영을 통해 미래 대비를 위한 선도적인 인공지능(AI) R&D 투자를 강화하여, 기술 역량의 조기 확보와 시장 선점에 기여하고, 대형 공공특화 프로젝트를 통해 시장을 주도할 수 있는 기술 개발을 촉진하는 등 공공영역에서 대규모 혁신이 촉발되며, 고위험 차세대 기술 분야에 대해 중장기 관점에서 투자함으로써 불확실성이 높은 미래에 유연하게 대응할 수 있는 역량 제고가 가능하다. 또한, 최고급 인공

지능(AI) 연구자와 고급 융합형 전문 인재풀을 확충하고 AI 인재의 양과 질 확보에 역량을 결집하여 인공지능(AI) 핵심 차세대 원천기술을 개발할 수 있는 고급 연구인력을 양성하며 세계적 선도 연구자급 역량을 강화한다. 핵심기술 및 데이터를 개방하고 공유하며, 연구자와 기업 간의 교류와 협력이 활성화 될 수 있도록 인공지능(AI) 연구환경을 조성하고 인공지능(AI) 개발에 필요한 기계학습용 데이터, 컴퓨팅 파워, 오픈 API가 원활히 개방 활용 되는 체계를 구축한다.

이를 통해 자율적 경쟁과 협업이 가능한 인공지능(AI) 기술혁신의 장이 마련되고, 경제 사회적 난제들을 해결하여 국민 삶의 질 향상에 기여할 수 있을 것이다.

4. 인공지능 플랫폼 구축방안

가. 인공지능(AI) 플랫폼의 개념

1) 플랫폼의 전통적 개념

플랫폼(Platform)이라는 용어는 ‘기차’와 같은 이동 수단을 통한 교역과 유통을 중계하는 공간으로 16세기부터 사용되어 왔으며, 최근에는 그 의미가 특정 장치나 시스템 등에서 이를 구성하는 기초가 되는 틀 또는 골격을 지칭하는 용어로 정보통신기술(ICT) 및 제조 등 다양한 분야에서 사용되고 있다. 플랫폼에 대한 논의는 다양하게 진행되고 있으며, 정보통신기술(ICT) 관점으로는 “컴퓨터 시스템의 기본이 되는 특정 프로세서 모델과 하나의 컴퓨터 시스템을 바탕으로 하는 운영체제”, 또는 “어떤 소프트웨어가 제공하는 환경”을 의미한다는 인식⁴⁹⁾도 공존하고 있다.

그러나 이러한 정보통신기술(ICT) 기술 공간으로서의 플랫폼에 대한 인식과는 별개로, 최근에는 급격하게 비즈니스 전략으로서의 플랫폼에 대한 관심이 더욱 커지고 있다. 이는 기존의 사회질서를 파괴하며 혁신적 공간으로서의 가치를 시장에서 증명한 ‘4인방(Gang of Four)’인 ‘구글, 애플, 아마존, 페이스북’의 역할에 기인한 것으로 볼 수 있을 것이다. 플랫폼은 ① 4인방을 비롯한 우버, 에어비엔비 등 플랫폼을 통해 수익을 확대하거나 거대 기업으로 급성장하는 현상이 나타나고 있으며, ② 정보통신기술(ICT) 기술의 진화로 플랫폼 구축 및 활용을 수월하게 할 수 있다. ③ 제품, 서비스의 수명주기가 단축됨에 따라 저비용 요구와 최단기간에 새로운 제품, 서비스를 생산해야 하는 요구가 증가하고 있으며, ④ 학문과 산업 영역의 경계를 무너뜨리는 융복합화에 대한 요구가 증가하면서 융복합을

49) 최상복, “산업안전대사전”, 골드, 2004. 5.

효과적으로 중계하기 위한 매개 공간의 필요성이 절대적으로 커졌기 때문이다.

이러한 플랫폼은 기업 측면에서 단기간에 투자 대비 높은 성과를 제공할 수 있는 “레버리지 효과”를 비롯하여, 비즈니스 모델 구축의 기회 등을 제공할 수 있어야 하며, 효과를 달성하기 위해서는 관련 기술들이 유기적으로 융합·구성되어 있어야 할 뿐만 아니라 해당 기술들을 이용한 목적 달성을 위한 효과적인 프로세스와 경험이 동시에 구현되어 있어야 할 것이다. 플랫폼이 급부상된 이유는 플랫폼의 활용을 통해 기업이 얻는 가치의 측면에서 설명될 수 있으며, 인공지능(AI) 플랫폼의 정의는 물리적 관점, 활용 프로세스 관점, 논리적 관점의 3가지 측면으로 플랫폼 구성요소를 인식할 수 있을 것이다.

2) 구성요소에 기반한 인공지능(AI) 플랫폼의 정의

인공지능(AI) 플랫폼은 다양한 관점에서 인식 및 사용되고 있으나, 3가지 요소에 대한 고려가 충분히 이루어진 정의는 찾아보기에는 제한되었다. 대표적인 인공지능(AI) 플랫폼 개념을 다음과 같은 관점에서 인공지능(AI) 플랫폼의 정의를 접근하고자 한다.

물리적 관점에서 인공지능(AI) 서비스를 구축하기 위해서는 해당 서비스의 개발 자원 및 배포 자원(서버)들의 통합적인 관리(버전 관리, 형상 관리)와 환경제공(딥러닝, Deep Learning 개발 환경), 그리고 자원 모니터링 등의 기능이 제공되어야 한다. 이러한 기능들이 물리적 관점에서 플랫폼의 구성요소로 정의할 수 있다.

활용 프로세스 관점에서 인공지능(AI) 서비스 구축에 필수적인 기계학습 과정은 일반적으로 “데이터 준비 - 교육(훈련) 데이터 생성 - 기계학습 모델 생성 및 훈련 - 검증”과 같은 단계를 거치게 된다⁵⁰⁾. 이처럼 각 프로세스를 효과적으로 실행할 수 있는 인터페이스의 제공은 기계학습에 대한 숙련도가 낮은 개발자들의 서비스 구축에 대한 진입 장벽을 낮추어 플랫폼 활용 기회를 높여줄 수 있을 것이다. 또한, 잘 알려진 오픈소스 기반의 딥러닝(Deep Learning) 라이브러리들을 추천하고 최신 버전을 관리하여 제공하는 기능은 이러한 프로세스의 품질을 높여주는 필수 요소이다.

논리적 관점에서 기계학습에 사용되는 다양한 알고리즘들을 내장하고 있는 기계학습 프레임 워크의 준비는 인공지능(AI) 플랫폼의 활용성과 품질을 높여주는 중요한 요소이다.

따라서 인공지능(AI) 플랫폼은 다음과 같이 정의될 수 있다. “인공지능(AI) 플랫폼은 다양한 사업 영역의 사용자가 원하는 인공지능(AI) 서비스 구축에 활용될 수 있는 다양한

50) 산업통상자원부, 제9차 산업핵심기술개발사업 RFP, “빅데이터 기반 AI의 산업특화 활용을 위한 개발형 AI 클

추상화 수준의 기계학습 라이브러리(또는 인터페이스)들을 제공하며(논리적 관점), 해당 라이브러리들을 활용한 효과적인 서비스 구축 프로세스를 인터랙티브하게 실행할 수 있는 기능(활용 프로세스 관점) 및 효과적인 자원 관리를 통한 데이터 준비, 개발, 검증 및 배포를 지원(물리적 관점)하는 관련 소프트웨어, 라이브러리, 서비스 인프라 스택의 유기적 집합이다.”

3) 인공지능(AI) 플랫폼의 활용 면에서의 특성

인공지능(AI) 플랫폼의 정의에서는 인공지능(AI) 플랫폼의 활용 면에서 다음과 같은 특성을 포함하고 있다.

가) 다양한 사업 영역

IBM, 마이크로소프트, 구글, 아마존 등과 같은 글로벌 기업들이 범용 인공지능(AI) 플랫폼 개발을 통해 치열하게 경쟁하고 있으며, 자사 플랫폼 제공 기술과 서비스들의 품질을 고도화하고 있다. 그럼에도 불구하고, 이들 범용 플랫폼이 갖는 규모적인 특성과 도입 비용 등의 문제, 제공되는 기술 및 서비스들의 추상화 수준에 따른 애플리케이션 개발 비용 등의 문제점들이 예전부터 꾸준히 인지되어 왔다. 인공지능(AI) 산업계에서는 이러한 문제의식에 대응하기 위해 금융·보험, 법률, 디자인, 제조, 교통, 의료, 세무·회계 등 다양한 분야에 특화된 산업 특화 플랫폼의 개발 및 발표가 이루어지고 있다.

이와는 독립적으로, 각 산업 분야에서 공통적으로 요구되는 서비스 영역에 의한 플랫폼 분류 가이드 라인도 제시되고 있으며, 챗봇이나 CRM, 마케팅, 결제, SEO(Search Engine Optimization), 텍스트 분석(text analytics) 등의 영역들을 포괄하고 있다.⁵¹⁾

나) 서비스 인프라 스택

일반적으로 인공지능(AI) 플랫폼은 설치형(on-premise) 또는 클라우드 시스템을 통한 서비스 제공형으로 서비스 인프라 스택이 준비될 수 있으며, 각 서비스 인프라 스택은 각각의 상황에 따라 장단점을 갖는다. 또한, 서비스 인프라 스택은 각 기업이나 기관의 지능화 대상이 되는 데이터의 특성 및 보안에 대한 인식 등에 따라 도입 전략 시 매우 중요한 판단 기준이 되고 있다.

51) PAT Research, “Top 15 Artificial Intelligence Platforms,,” 2018. 7. 15.

나. 인공지능(AI) 플랫폼 도입을 위한 전략

가트너는 2019년까지 시장 주도 기업(Market-Leading Companies)의 30%가 인공지능(AI) 플랫폼 서비스에 의해 수입이 감소할 것이라고 예측하였는데, 이는 인공지능(AI) 플랫폼 도입 전략이 인공지능(AI) 기술을 도입하고자 하는 기업 입장에서 매우 중요하다는 것을 추론할 수 있게 한다⁵²⁾. 자사의 인공지능(AI) 플랫폼인 Rage를 설명하는 리포트에서, 가트너는 기업이 해결하고자 하는 문제(Business Opportunity), 문제 해결을 위한 비즈니스 프로세스 변환(Business Process Transformation), 유사한 문제 해결 기술의 검색, 90일 이내의 문제 해결 가능성 등을 포함한 10개의 질문들을 인공지능(AI) 플랫폼 선택(Shopping for Enterprise AI) 문항으로 제시하고 있으며, 이는 Rage 플랫폼 설계 철학과도 깊은 관계가 있다⁵³⁾. 가트너의 Rage 플랫폼은 인공지능(AI) 플랫폼 정의의 관점에서 볼 때 논리적 관점과 활용 프로세스적 관점을 중점적으로 구현되었다. 또한, 공통 서비스별 분류에 특화된 플랫폼으로 분류될 수 있으며, 이러한 플랫폼의 선택을 위해 플랫폼 도입을 위한 주요 고려사항들에 대해 제시하였다.

인공지능(AI) 플랫폼 도입 전략 수립과 인공지능(AI) 플랫폼 도입의 필요성에 대해서는 다음과 같은 6가지 측면들(데이터 부문 2개, 서비스부문 2개, 엔지니어 및 조직 부문 각 1개)에 대한 분석을 통하여 필요성에 대해서 정의하였다.

- ① (데이터 1) 지능화 대상이 되는 데이터의 특성: 기업의 인공지능(AI) 기술 도입 필요성은 보유하고 있는 경쟁력(노하우)을 지능화하고자 하는 의지에서 비롯되는 경우가 많으며, 일반적으로 경쟁력은 축적되어 있는 데이터에 기반하고 있다. 따라서, 인공지능(AI) 플랫폼 도입 시에는 지능화 대상이 되는 데이터의 특성에 대해 점검할 필요가 있으며, 이를 위해 ① 변환 과정을 거쳐서 지능 구축을 위한 훈련데이터(training data)로 효율적인 변환이 가능한지 ② 보유 데이터가 충분치 않아서 기업의 경험에 기반한 훈련데이터 구축을 새롭게 수행할 필요가 있는지에 대해 확인해야 한다. 또한, 훈련데이터의 준비 또는 신규로 수집되는 과정을 지원해줄 수 있는 도구나 프로세스 및 컨설팅 수준 등에 대한 검토를 반드시 수행해야 한다.
- ② (데이터 2) 인공지능(AI) 서비스 관련 데이터의 특성: 산업별 특성 및 문화에 따라 인공지능(AI) 서비스 관련 데이터(훈련데이터 및 서비스 실행 과정에서 수집 및 축적되는 데이터)는 인공지능(AI) 기술을 도입하고자 하는 기업과 기관에서

52) 60 second marketer, "157 Artificial Intelligence Platforms to Help You to Grow Your Business," 2018. 1. 24.

53) Gartner, "The Road to the Enterprise AI," 2018.

외부 전송이 어려운 경우들이 존재한다. 이런 경우 설치형(On-Premise) 인공지능(AI) 플랫폼에 대한 검토가 우선적으로 이루어져야 한다.

- ③ (서비스 1) 구축 대상 인공지능(AI) 서비스의 규모: 인공지능(AI) 서비스는 기업 내 관련 부서에서 이용하기 위해 구축되는 경우도 있고, 불특정 다수의 사용자들을 위해 구축되는 경우도 있다. 구축 내용에 따라 요구되는 서버 자원의 규모가 달라진다. 인공지능(AI) 서비스 개발 및 운영에 필요한 서버 자원(GPU, 메모리 등)의 경우는 고가인 경우가 많으므로 이러한 자원의 효과적인 관리기능 지원이 인공지능(AI) 플랫폼에서 어떻게 이루어지고 있는지 확인해야 한다.
- ④ (서비스 2) 구축 대상 인공지능(AI) 서비스의 특성: 의료, 금융, 법률 등의 산업 분야에서는 서비스 특화 지능(service-defined intelligence)을 이미 제공하는 산업 특화 인공지능(AI) 플랫폼들이 다수 존재하고 있다. 그러나, 서비스 특화 지능을 보유하고 있지 않은 인공지능(AI) 플랫폼인 경우라도 제공되는 도구들을 이용하여 해당 특화 지능 구축이 가능할 수 있다. 예를 들어, 보험 상품을 판매하는 챗봇을 구축하려는 경우, 일반적인 챗봇 기술을 제공하는 플랫폼을 도입하여 개발을 진행할 수도 있으며, 보험 상품을 위한 전문 챗봇 기술을 제공하는 플랫폼 도입도 검토할 수 있는데, 이때 서비스 구축 기간, 인력 및 비용 등 비즈니스 환경 요인들에 의해 영향을 받게 된다.
- ⑤ (엔지니어) 플랫폼 도입 기업 / 기관에서 보유하고 있는 인공지능(AI) 기술 담당 그룹의 특성: 인공지능(AI) 플랫폼들이 제공하고 있는 서비스들을 플랫폼 도입 기업이 보유하고 있는 인공지능(AI) 기술 그룹의 기술 숙련도, 담당 업무의 전문성(기획, 개발 등) 및 기업의 인공지능(AI) 기술 및 서비스 관련 로드맵 등에 의해 검토해야 한다. 기술 그룹의 숙련도가 낮고, 기획 및 관리 영역 경험과 역량이 높은 그룹을 보유하고 있는 경우라면 활용 프로세스적 관점이 잘 지원되고, 제공되는 라이브러리들의 추상화 수준 및 특성에 대해 더욱 세심한 검토가 필요할 것이다.
- ⑥ (조직) 인공지능(AI) 서비스 관련 기술의 내재화 요구사항: 플랫폼을 도입하고자 하는 기업이 구축 대상 인공지능(AI) 서비스의 개발 및 유지 보수를 내재화하여 자체적으로 실행하고자 하는 계획을 수립하였다고 한다면 도입 플랫폼에서 제공되는 기술 지원 수준과 라이선스 사항 등의 검토가 매우 중요할 것이다. 대부분의 상용 인공지능(AI) 플랫폼의 경우에 추상화 수준이 높은 서비스 라이브러리들(예: 자연어 처리 기술(개체명 인식), 감성 인식, 주제 분류, 문서 요약 등)은 훈련 가능한 수준의 딥러닝(Deep Learning) 코드를 제공하는 경우도 있지만

구축된 심층신경망(Deep Neural Net)의 내부 구조는 공개하지 않는 경우가 있기 때문이다(예: IBM의 Watson NLU 등).

다. 인공지능(AI) 플랫폼 도입 방안

가트너는 2019년까지 스타트업들이 경쟁력 있는 비즈니스 솔루션(Disruptive Business Solution)으로 아마존, 구글, IBM, 마이크로소프트를 추월할 수 있을 것이라고 예측하고 있으며, 2020년까지 20%의 기업들이 인공지능(AI) 개발과정을 모니터링하는 인력들을 전담으로 배치시킬 것이라고 예측하였다. 이러한 가트너의 예측은 치열한 인공지능(AI) 기술 시장을 이끌어나가는 주체로서 재빠른 움직임과 독창적이고 폭발적인 개발력을 가진 소규모 스타트업들의 역할에 대한 기대감이며, 많은 기업들이 인공지능(AI) 기술을 도입할 때 플랫폼에 대한 중요성에 대해 인식될 것이라는 측면에서 주목할 수 있다.

국외 인공지능(AI) 플랫폼 업체들은 클라우드 중심의 범용성과 산업 특화 영역에서 글로벌 기술 리더십을 갖고 있기 때문에 경쟁력과 차별성을 갖기 위해 국내에서도 인공지능(AI) 플랫폼에 대한 구성요소 중심의 정확한 개념 인식과 중요성에 대한 공유 확산이 필요하다. 또한, 4차 산업혁명 시대의 핵심 동력원인 인공지능(AI) 플랫폼에 대한 관심과 투자가 이루어져야 할 것이다.

4차 산업혁명 시대가 도래하면서 GE, Google 등 글로벌 대기업을 중심으로 '디지털 플랫폼' 구축을 적극적으로 추진하고 있다. 이는 4차 산업혁명이 단순한 제품 성능개량이나 공장 자동화, 업무 효율화 및 생산성 향상 이상의 의미를 가지고 있기 때문이라고 할 수 있다. ICBM + AI 등과 같은 4차 산업혁명 기술을 활용하여 제품개발로부터 제조, 판매, 서비스에 이르는 기업 전반에 걸쳐 비용 절감 또는 새로운 부가가치 창출 과정을 이해해야 한다. 이를 통해 제품 및 이와 관련된 서비스를 만들어냄으로써 새로운 비즈니스 모델을 창출해 나갈 것으로 예상된다.

현재 방산 분야에서는 인공지능(AI) 분야의 적용이 다른 분야보다 매우 높은 수준을 기록하고 있으며, 아울러, 8대 무기체계 분야에서도 다른 분야보다 인공지능(AI) 구축 수요가 많은 것으로 조사되었다. 방산 분야의 무기 및 제품 개발과 성능개량, 관련 지원 및 운영유지 시스템 구축에 인공지능(AI) 기반의 4차 산업혁명 기술을 적극적으로 활용할 수 있는 방안에 대한 모색도 필요할 것으로 보인다. 이를 위해 무기체계별 인공지능(AI) 구축 소요를 식별하고 이에 대한 우선순위를 고려하여 맞춤형 디지털 플랫폼을 구축해 나가야 할 것이다. 해외 사례에 대한 벤치마킹으로 수요가 많고 비용 절감 효과가 큰 무기체계 사업을 선별, 시범사업을 추진할 필요도 있다. 미 GE사가 추진하고 있는

‘군용기 운용 정비 능력 향상을 위한 디지털 플랫폼 구축사업’등이 좋은 사례이다. 또한, 국내 인공지능(AI) 관련 업체와의 공동 플랫폼 구축 사업을 추진하는 것도 필요하다. 더 나아가, 미국 GE사 등 디지털 플랫폼 구축을 추진 중인 업체와의 공동연구개발 투자 사업 추진도 필요할 것으로 판단된다.

■ 소결론

- 인공지능(AI)을 적용한 무기체계 획득을 위한 제도개선
 - 무기체계 완제품 외에 세부부품 단위까지 방산물자로 지정되어 독과점적 지위를 보장하는 점에 대해서는 이를 크게 완화. 즉, 4차 산업혁명 기술력을 보유한 업체들이 중소벤처 업체임을 고려할 때, 현행 방산물자지정제도는 높은 진입장벽으로 작용할 가능성이 매우 크다고 판단됨.
 - 정부에서 필요로 하는 4차 산업혁명 기술을 보유한 업체가 무기체계개발 또는 성능개량에 참여할 경우, 이에 대한 자금지원과 가점 인정 등이 고려
 - 무기체계의 정비와 운영유지간 필요한 시스템 구축에 빅데이터 구축 등을 추진. 즉, 필요하다면, 네이버, 다음 등 국내 관련 대형 업체와의 협력을 통해 시범사업 등을 추진하고 이를 통해, 군사보안 관련 현안 문제들을 해소함과 아울러, 군 사이버 보안역량을 강화하는 중장기적인 대안 마련이 필요
 - 4차 산업혁명 위원회 내 방위산업분과 신설 필요. 이는 정부 차원의 거버넌스(Governance)가 필요
 - 쌍방향 무기소요 제기 시스템 구축으로 국내 방산업체와 4차 산업혁명 기술력을 보유한 민간업체들이 조사, 분석하여 정부 주도 또는 정부-기업간 매칭 형태로의 관련 사업들을 추진
- 중장기적인 인력양성
 - 인공지능(AI) 인재 수급 불균형에 따른 산업 생태계 혼란을 최소화하기 위한 인재양성 방안 마련이 필요. 즉, 인공지능(AI) 인재확보를 위한 전세계 경쟁이 더욱 치열해질 것으로 예상됨에 따라 우리나라도 국가 차원의 전략적 대응이 그 어느 때보다 필요한 시점임
 - 인공지능(AI) 핵심인재(h-index 상위 10%)는 소수 국가에 집중되어 있어 인공지능(AI) 격차 해소를 위한 석·박사급 고급인력 양성 체계 구축 및 질적 고도화가 필요
 - ‘인공지능(AI) 대학원’ 사업은 사업이 종료되는 ’31년까지 약 3,600명 정도의 석·박사 인재를 배출함으로써 인공지능(AI) 고급인재 부족 해소에 기여할 것으로 예상되지만, 도입기인 인공지능(AI) 대학원의 질적 고도화 및 성과확산을 위해서는 체계적인 커리큘럼 개발, HW·SW 인프라 확충, 실증적 교육 연구 협업 환경 구축, 교원확보, 글로벌 네트워크 활성화 등 추가적인 프로그램 추진이 필요
 - 인공지능(AI)에 대한 사회적 수용성(Public Acceptance) 향상을 위한 보편적 교육 확대, 세계 최고의 인공지능(AI) 인재로 성장할 수 있는 토양 마련을 위해서 초·중·고 단계부터 인공지능(AI) 지식을 습득하기 위한 STEM 교육 강화, MOOC 개발, 인공지능(AI) 비취위 프로그램 개설 등 사회 전반에서의 인공지능(AI) 활용 능력 제고를 위한 교육 프로그램 확충이 필요
- 인공지능(AI) R&D 정책과 연계한 협의체 구성
 - 인공지능(AI) R&D 전략의 실행력 확보를 위해 ‘인공지능(AI) 전략 협의체’구성 및 운영체계 마련
 - 협의체 구성은 복지, 산업, 행안, 국방 등 정부부처 공무원(실국장급)과 민간위원(산·학·연 전문가)으로 구성하며, 위원장은 과학기술정보통신부 2차관으로 하여 분야별 전략이 연계·통합 관리될 수 있도록 인공지능(AI) 전략 협의체의 하위 분과로 기술·인재·기반 분과 운영이 필요

- 협의체의 역할로 중점 과제 추진상황, 기술·정책 환경 변화에 따른 R&D 전략 및 목표 재점검, 기술-인재-기반 분야의 핵심과제 세부 추진전략을 마련
- 인공지능(AI) 플랫폼 구축
 - 물리적인 관점 : 인공지능(AI) 서비스를 구축하기 위해서는, 해당 서비스의 개발 자원 및 배포 자원(서버)들의 통합적인 관리(버전 관리, 형상 관리)와 환경 제공(답러닝, Deep Learning 개발 환경), 그리고 자원 모니터링 등의 기능이 제공
 - 활용 프로세스 관점 : 인공지능(AI) 서비스 구축에 필수적인 기계학습 과정은 일반적으로 “데이터 준비 - 교육(훈련) 데이터 생성 - 기계학습 모델 생성 및 훈련 - 검증”과 같은 단계로 각 프로세스를 효과적으로 실행할 수 있는 인터페이스의 제공
 - 논리적 관점 : 기계학습에 사용되는 다양한 알고리즘들을 내장하고 있는 기계학습 프레임 워크의 준비
 - 인공지능(AI) 플랫폼 도입 전략 수립을 위해서는 인공지능(AI) 플랫폼 도입의 필요성에 대한 6가지 질문들(데이터 부문 2개, 서비스부문 2개, 엔지니어 및 조직 부문 각 1개)에 대해 점검해보는 것이 필요

VI. 결론

기술 발전에 따른 미래전의 변화에 따라 수행될 미래전은 과학기술 발전에 따른 네트워크 기반 전쟁(NCW) 수행이 예상되며, 초국가적·비군사적 위협에 대비한 대테러전 및 대국 지전이 필요며, 감시·정찰-정밀타격-요격-방호 능력 구축이 필요하며, 4차 산업혁명 시대의 급변하는 새로운 기술 여건과 북한 핵 도발로 국가 안보 상황은 날로 위중해지고 있는 것이 현실이며, 미래전을 대비한 신개념 무기체계를 선도적으로 개발할 수 있도록 국가기술력을 총 결집하는 등의 혁신적 발전이 요구되는 시점이다.



〈그림 VI-1〉 4차 산업혁명시대의 미래전 모습

더불어, 국방 분야에서는 전장에서 아군 전투원의 피해를 최소화하면서 전투효율성과 효과를 극대화하려는 노력으로 미래의 작전환경에 대비한 중요한 화두로 인식되고 있다.

이를 위해 4차 산업혁명 기술을 적용한 첨단화되고 무인화된 무기체계가 중요한 대안 중 하나로 손꼽히고 있다. 이는 인공지능(AI) 기술을 기반으로 물리적 한계를 극복하고 자율성과 협업 능력을 강화하는 방향으로 나가고 있다.

이에 국가 국방 R&D 체제의 혁신을 강력하고 시급히 추진하여 4차 산업혁명 특히 인공지능(AI) 분야에서 국방 연구개발 체질을 강화하는 것이 필요하며, 국방연구개발은 국가안보를 책임지는 하나의 커다란 축으로 실질적인 무기체계를 개발하고 생산·배치하여 국방력을 개선·증강하고 안으로 내수 활성화와 수출을 통한 국가적인 이익 창출을 통하여 경제에 기여하며, 국가 과학 발전에 중요한 역할을 수행할 수 있을 것이다. 또한, 인공지능(AI) 국방과제 발굴을 통하여 민·군 기술 활용 극대화가 필요하며, 국가의 기술력 결집을 시킬 수 있는 R&D 혁신의 기반 토대를 마련해야 할 것이다. 즉, 국가 R&D와 국방 R&D 공동 기획 과제 제시와 신기술 상호 활용 추진을 통해 국가 기술의 개방적 활용 기회 마련하고, 인공지능(AI) 과제 발굴에 따라 정부 출연 연구소의 최신 등장 기술이 국방에 기여할 수 있도록 국방 분야 전문 연구기관 협업 기회 제공해야 한다.



〈그림 VI-2〉 민·군 협력 R&D 체계

인공지능(AI) 국방 분야 활용방안 연구를 통해 앞서 제시된 방안 들을 기반으로 과제 화하여 창의적이고 도전적인 국방 R&D 연구 기회의 마련이 가능하였다. 즉, 인공지능 (AI) 관련 신개념, 신기술 아이디어를 국방에 적용토록 관련 우수 인력을 영입하여 수행 하는 개방형 연구로의 발전 가능성이 있다. 또한, 미래 운용개념 개발과 신무기·신기술 융합을 위한 원천핵심기술 연구 가능성(예산 확대 필요)을 보여 주었으며, 고난이도 연구 개발에 대하여 창의적이고 도전적인 연구개발을 유도하는 기회 제공하였다.



〈그림 VI-3〉 위리어플랫폼 및 원격 로봇(예)

인공지능(AI) 국방 분야 활용방안 연구를 통해 기존의 무기체계에 인공지능(AI) 기술을 접목하는 방법으로의 발전을 통해 세부 분야별 지속적 발전이 가능한 국방 R&D 개발 근간 마련 기회 제공하였다. 즉, 인공지능(AI) 관련 과제 연구 및 방안 제시를 통해 기존의 무기체계 성능개량을 유도하고 지속 발전 가능한 연구개발 선진화를 통해 최소 예산 투입만으로 국방력 향상에 기여에 기대되며, 인공지능(AI) 과제 발굴을 통하여 분야별 기술 진부화를 방지하는 최소 예산의 성능개량 연구 활성화가 기대된다. 더불어 개념연구 등 운용의 혁신과 빅데이터, AI, IOE 등 기술혁신을 동시에 지속적으로 추구할 수 있는 기회가 예상된다.



〈그림 VI-4〉 이스라엘 개발 근거리 대공방어체계 예)

인공지능(AI) 국방 분야 활용방안 연구를 통해 국가가 유지, 발전시켜야 할 기술분야의 정책적 투자 기회를 마련하고, 지속적으로 투자를 통해 발전시킬 수 있는 단초를 제공하였으며, 그 분야는 다음과 같이 제시한다.

- 인공지능(AI)을 국가가 전략적으로 유지, 발전시켜야 하는 분야로 육성 추진 기회로 활용

- 인공지능(AI) 기술과 같이 기술적 위험도가 크고 대규모 투자가 필요한 분야의 육성 기회로 활용
- 민·군이 국가 예산을 활용하여 동시에 참여하여 기술 개발능력이 취약하거나 경제성이 없는 분야에 적극적인 연구 기회로 활용이 가능

〈참고 문헌〉

- 국가정보화전략위원회(2013), “빅데이터를 활용한 스마트 정부 구현”.
- 고숙자, 정영호(2012), “국민건강 미래예측 시스템 구축 방안,” 한국보건사회연구원, 『보건 복지포럼』, 통권 193호, p. 46.
- 김형주 외, 국방분야 빅데이터 활용 방안, 한국전략문제연구소, pp. 67~70, 2013. 11.
- 방준성, 최은주, “증강현실(Augmented Reality) 국·내외 기술동향과 발전전망”, Emerging Issue Report 16, 한국과학기술정보연구원, 2017. 1.
- 강진석, “전장공간을 위한 스마트폰기반 인터랙티브 혼합현실 기술 개발”, 중견연구자지원 사업, 핵심연구, 2011.5. ~ 2014. 4.
- 강진석, “비정형 데이터마이닝에서 군 전술운용에 관한 연구”, 중견연구자지원사업, 도약 연구(전략), 2014. 11. ~ 2017. 10.
- 강진석, “증강현실, 가상현실 또는 혼합현실 기반 군용 장비의 정비를 지원하는 서버, 방법 및 웨어러블 디바이스,” 특허등록 10-1874461-0000, 2018. 6.
- 강진석, “증강현실에서 사례의 추론, 분류, 결정 기반 군용 장비의 정비를 지원하는 서버, 방법 및 웨어러블 디바이스,” 특허등록 10-1891992-0000, 2018. 8.
- 미 국립연구재단(NSF)의 주요연구지원 프로그램, 2014. 12.
- 과학기술정보통신부, “I-Korea 4.0 실현을 위한 인공지능(AI) R&D 전략”, 2018. 5.
- 이승훈, “최근 인공지능(AI) 개발 트렌드와 미래의 진화방향”, LG경제연구원, 2017. 12.
- 육 군, “인공지능(AI) 연구 발전처”, 2019. 1.
- AIBRIL, “건강을 지키는 인공지능 AI와 헬스케어의 만남”, 2018. 10.
- “헬스케어에 인공지능을 더하다”, <https://skccblog.tistory.com/3712>, 2018. 6.
- 박형근, “정보보안에서의 인공지능 도입 분야와 주요 사업자”, 2018. 8.
- 김현기, 옛소브레인 병렬형 과제 및 추진 현황, 한국전자통신연구원, 2018. 8. 13.
- 최상복, “산업안전대사전”, 골드, 2004. 5.
- 산업통상자원부, 제9차 산업핵심기술개발사업 RFP, “빅데이터 기반 AI의 산업특화 활용을 위한 개발형 AI 클러스터 구축
- 국경완, 4차 산업혁명 시대 인공지능을 활용한 군사적 적용방안, 합참지, 2018.
- 최현준, 국내외 인공지능 동향과 국방 활용 방안, 한국통신학회지 34(11), 2017, pp. 53-59.
- 김형철, “ICT표준화 전략맵”, 한국정보통신기술협회(TTA), 2018. 10. pp19-21.
- 주영대, “미국의 인공지능(AI) 개발전략과 시사점”, 한국산업기술평가관리원(KIET), p. 32. 2016. 12.

- 과기정통부, “데이터·AI경제 활성화 계획”, 관계부처일동, pp. 2-3, 2019. 1.
- 과기정통부 보도자료, “데이터·인공지능(AI) 경제 활성화의 이정표 제시”, 2019. 1.
- 아웃소싱타임스, “뛰는 중국 걷는 한국, 중국 인공지능(AI) 인재 한국의 7배”, 2019. 1.
- AIBRIL, “건강을 지키는 인공지능 AI와 헬스케어의 만남”, 2018. 10.
- “헬스케어에 인공지능을 더하다”, <https://skccblog.tistory.com/3712>, 2018. 6.
- 행정안전부, “2019년 지능형 정부를 주도할 핵심기술 선정”, 2019. 1. 28.
- 국경완, “4차 산업혁명 시대 인공지능을 활용한 군사적 적용방안”, 합참지, 2018. 12.
- 박형근, “정보보안에서의 인공지능 도입 분야와 주요 사업자”, 2018. 8.
- 윤장우, “인공지능 관련 기술과 정책동향 및 시사점”, 한국전자통신연구원(ETRI), pp. 13-14, 2015. 7.
- 최은수, “인공지능의 습격...인간을 어디까지 위협할까?”, 매일경제, 2016. 3.
- 헤럴드경제신문, “중국의 AI 굴기, 미국도 추월했다”, 2019. 2.
- 중소벤처기업부, “중소기업 기술로드맵(2018~2020, AI/빅데이터)”, pp. 18-24., 2017. 1.
- 심혜정, “우리기업의 인공지능(AI)을 활용한 비즈니스 모델”, 국제무역연구원, 2018. 3.
- 경향신문, “군 AI는 워리어 플랫폼·드론봇 전투체계의 선행 핵심기술”, 2018. 12.
- 권 현, “인공지능기반 지상 로봇·무인체계 발전방향제안”, 2020. 10.

McKinsey Global Institute(2011), Big data: The next frontier for innovation, competition, and productivity.

Yiu, C.(2012), The big data opportunity: making government faster, smarter and more personal.

PAT Research, “Top 15 Artificial Intelligence Platforms”, 2018. 7. 15.

60 second marketer, “157 Artificial Intelligence Platforms to Help You to Grow Your Business,” 2018. 1. 24.

Gartner, “The Road to the Enterprise AI,” 2018.

AGCO, “AGCO innovations in manufacturing with glass“, 2017.

Badler, N., Erignac, C., Vincent, P., Sanchez, E., Wampler, J., Ianni, J., 2000, Design Concepts for Automating Maintenance Instructions, Air Force Research Laboratory Technical Report (AFRL-HE-WP-TR-2000-0088)

Christopher Volpe, VirtualHaptic Validation for Service Manual Generation, GE Global Research Center Cnet, “Here’s what Apple’s doing to get you excited about AR,” 2018. 6. 18.

- Drew, Dennis M. and Snow, Donald M., Making Strategy: An Introduction to National Security Processes and Problems, Alabama: AIR UNIV MAXWELL AFB, 1988.
- Dror, Yehezkel, Public Policymaking Reexamined, New Brunswick.: Transation Inc., 1983.
- Freeman, Linton C. (ed.) Social Network Analysis: Data, mathematical models and graphics; Vol. 2, The Structure of Social Groups; Vol. 3, The Structure of Social Positions; Vol. 4, Antecedents and Consequences of Network Structure, LA, London: Sage, 2008.
- Hansen, Derek. Shneiderman, Ben. and Smith, Marc A., Analyzing Social Media Networks with NodeXL: Insights from a Connected World, San Francisco: Morgan Kaufmann Publishers Inc., 2010.
- Hanggeun Shim, Jaekyung Yang and Myoungjin Choi (2018), A Study on the Virtual Reality Interface Integrated Logistics Support System, International Journal of Advanced Science and Technology, Vol. 112, March, 2018, pp. 33-42 ISSN 2005-4238(Scopus, Australia)
- Jeff Wampler, Service Manual Generation: An Automated Approach too Maintenance Manual Development, 16th Human Factors in Aviation Maintenance Symposium, April 2-4, 2002.
- Lasswell, Harold D. and Kaplan, Abraham., Power and society, New Haven: Yale University Press, 1970.
- MIT Technology Review, "NASA is using HoloLens AR headsets to build its new spacecraft faster", 2018. 10. 9.
- Qualcomm, "Qualcomm Reveals the World's First Dedicated XR Platform," 2018. 5. 29.
- Wccfttech(2016), Nvidia Shows Off Near Eye Light Field VR Headset at VR Los Angeles 2016, Virtual Reality Without The 'Motion Sickness'.
https://www.lunit.io/ko/product/insight_cxr2/
- 테크월드뉴스(<http://www.epnc.co.kr>)
- 에브리뉴스 EveryNews(<http://www.everynews.co.kr>)

현대전에서의 사이버전 워게임 연구

국방대학교 교수 **강 동 수**아주대학교 교수 **이 민 우**

- I. 연구 개요
- II. 현대전에서의 사이버전과 워게임
- III. 사이버 워게임 사례분석 및 시사점
- IV. 한국군을 위한 사이버 워게임 활용 방안
- V. 결론

요 약

우리가 개발한 다양한 컴퓨팅 기술과 네트워크화된 사이버공간과 우주공간은 우리의 생활방식이 되고 있다. 다양한 컴퓨팅 환경은 무기체계를 지능화하고 네트워크화된 사이버공간과 확장된 우주 공간은 전쟁 방식에 변화를 줄 것이며, 우리는 이에 대한 준비가 필요하다.

우리는 일상생활에서 이러한 사이버공간을 매일 사용하고 있다. 때로는 이동할 때 들어 가기도 하고 걸어 다니면서 이용할 정도로 일상생활에서 차지하는 비중이 크다. 이러한 사이버공간은 미래의 전장으로 다영역작전(MDO: Multi Domain Operation)의 한부분으로 분류된다. 즉, 물리공간 작전과 사이버공간 작전이 함께 사용되는 전장인 것이다.

사이버전의 선진국인 미국은 사이버전이 미래의 국가 안보와 국가 전략에 미치는 영향력을 알고 2006년부터 국가 수준의 사이버 워게임을 수행하고 있다. 이와 별개로 다영역작전을 수행하는 무기체계의 획득 과정에서 사이버 워게임의 한 형태인 사이버 테이블 탑(CTT: Cyber Table Top)을 적용하여 사이버 위협을 감소시키기 위한 지침을 가지고 있다.

하지만, 국내에서는 독립적으로 사이버전을 워게임의 형태로 수행할 수 있는 모델,

프레임워크에 대한 연구가 아직은 미진한 상황이다. 사이버작전사령부에서는 사이버전에 대한 위계임을, 방위사업청에서는 무기체계 획득을 위한 사이버 테이블 탑을 적용하는 방안을 검토할 필요가 있어 본 연구에서는 미국의 사이버 위계임 모델 사례를 분석하고, 사이버 위계임 적용 필요성을 설명하고 한국군의 사이버 위계임 모델 적용 방안과 무기체계 획득 시 사이버 위계임 적용 방안을 제안한다.

현재의 위성통신망은 전 세계 모든 지역에서 하늘만 볼 수 있으면 통신이 가능한 환경을 만들고 있다. 전 지구적 환경인 우주와 사이버공간이 전장영역으로 기능하는 것이다. 그러므로, 사이버공간을 포함하는 다영역작전 수행능력이 미래 전쟁의 승패를 좌우할 것이며, 이를 위해 무기체계 개발과 획득에 대한 사이버 테이블 탑 활용이 필요하며 이는 다영역 시험평가와 같은 역할을 할 것이다.

I. 연구 개요

제1절 연구배경 및 목적

1. 연구배경

군사분야에서 위계임은 전쟁 계획 수립에 있어서 매우 중요한 역할을 해오고 있다. 위계임은 전장의 안개(Fog of War)로 표현되는 충분하지 않은 정보에 대한 지휘관의 의사결정에서의 어려움을 해소하는데 유용한 도구이다. 이 때문에 비단 군사 활동에서만 아니라 비즈니스 활동 영역에서도 위계임이 사용된다.

미래 전장에서는 지상, 해상, 공중, 우주, 사이버공간을 모두 아우르는 다영역작전(MDO: Multi Domain Operation)이 수행된다. 미래 전장은 물리공간 작전과 사이버공간과 우주공간 작전이 함께 사용되는 하이브리드 전장이 될 것이다.

사이버전의 자타공인 선진국인 미국은 사이버전이 미래의 국가 안보와 국가 전략에 미치는 영향력을 간파하고, 지난 2006년부터 통상 2년마다 국가 수준의 사이버 위계임을 수행하고 있다. 이와 관련하여 미 국방부는 다영역작전에 사용되는 무기체계의 획득 과정에서 사이버 위계임의 한 형태인 사이버 테이블 탑(CTT: Cyber Table Top)을 적용하여 사이버 위협을 감소시키기 위한 지침을 무기획득 과정에 마련하였다.

하지만, 국내에서는 독립적으로 사이버전을 위게임의 형태로 수행할 수 있는 연구가 아직은 미진한 상황이다. 그래서 사이버작전사령부에서는 사이버전에 대한 위게임을, 방위사업청에서는 무기체계 획득을 위한 사이버 테이블 탑을 적용하는 방안을 검토할 필요가 있다.

본 연구는 미국의 사이버 위게임 모델 사례를 분석하고, 사이버 위게임 적용 필요성에 관한 시사점을 도출하여 한국군의 사이버 위게임 모델 적용 방안과 무기체계 획득 시 사이버 위게임 적용 방안을 제안한다.

2. 연구 목적

전쟁의 양상이 변화되면서 사이버전 작전계획 수립을 위한 사이버공간에 대한 전장정보 준비(IPB: Intelligence Preparation of the Battlefield) 활동을 비롯하여 효과적인 작전 수행을 위한 활동들에 대한 개념연구들이 많은 사이버전 선진국에서 수행되고 있다. 국내에서도 국군사이버작전사령부가 창설된 후 사이버작전 수행에 필요한 관련 개념들이 연구되면서 사이버 위게임에 대한 관심이 증가하고 있다.

본 연구는 먼저 사이버 위게임의 프레임워크와 대표적인 사이버 위게임 사례들을 분석한다. 사이버 위게임은 기존 전쟁 연습과 관련하여 미래전에 필수적인 활동이며 물리공간과 사이버공간의 복합적인 특성을 가지고 있다. 사이버위게임 프레임워크와 사례 분석이 이러한 복합적인 특성들을 이해하는데 도움이 된다. 이를 통해, 한국군의 사이버 위게임 모델 적용 방안을 마련하기 위한 시사점과 활용 방안을 도출하고자 한다.

다음으로 사이버 위게임을 한국에 적용할 수 있도록 사이버위게임 방안과 무기체계 획득시 시험평가 적용방안 도출한다. 이는 사이버 위게임 계획 수립 및 추진을 위한 참고자료이면서 국방 사이버보안 능력 강화를 위한 관련 정책 도출, 체계와 기술 도입 및 연구개발 추진 방향 설정에 활용이 가능할 것으로 기대한다.

제2절 연구범위 및 방법

연구범위는 연구 과제를 더욱 목표 지향적으로 연구를 수행하기 위해 중점 연구 분야를 크게 3가지로 구분하였다.

- 현대전에서의 사이버전과 위게임
 - 사이버공간의 등장과 전쟁의 변화
 - 사이버전의 등장과 사이버 위게임의 역할

- 사이버 워게임 사례분석 및 시사점
 - 미 DHS의 Cyber Storm 분석
 - 미 HSSEDI Cyber Wargaming Framework 분석
- 한국군을 위한 사이버 워게임 활용 방안
 - 미 DoD CTT 분석과 사이버 워게임 활용 방안
 - 무기체계 획득 과정에서 사이버 워게임 적용

연구방법은 선행연구 자료를 분석하고 기술동향과 대응방안을 도출한다. 연구방법은 다음과 세 가지로 구분 된다.

- (방법1) 관련 선행연구 자료 분석
- (방법2) 기술동향 분석 및 대응 방안 도출
- (방법3) 전문가 자문 및 토의

II. 현대전에서의 사이버전과 워게임

제1절 사이버공간의 등장과 전쟁의 변화

1. 사이버공간의 발견

현대전에서는 비전통 안보위협 중 하나인 사이버 전쟁이 수행되고 있다. 앨빈 토플러(1928-2016)의 저서 전쟁과 반전쟁(War and Anti-War)의 언급처럼 역사를 통해서 인류의 전쟁 방식은 인류가 일하고 생활하는 방식을 투영해 왔듯이 사이버공간에서의 생활이 일반화된 현재의 생활 방식은 곧 현대 전쟁에 투영되고 있다.

우리가 접하고 있는 공간은 자연적으로 존재하는 것(God-made)과 인위적으로 만들어진 것(Man/Woman-made)으로 구분될 수 있다. 지상, 해상, 공중, 우주는 전자로 보는 것이 자명하다. 또한, 전자기 스펙트럼(Electro magnetic Spectrum)도 자연에 존재하는 공간임이 1862년 맥스웰(Maxwell)의 예측과 1987년 헤르츠(Hertz)의 실험에 의해 확인되었다.

1969년에 미국의 4개 대학에서 패킷 스위칭 네트워크(Packet Switching Network)가 처음 ‘연결’되면서 ‘인터넷(Internet)’이 만들어졌다. 앞서 등장한 컴퓨터가 인터넷에 접속되면서 새로운 공간이 만들어진 것이다. 이후 1970년대의 암호혁명 시기를 지나면서 1990년대부터 인터넷 붐이 일어나고 이들을 이용하는 정보전에 이어 사이버전이 전쟁사에 등장하게 되었다.

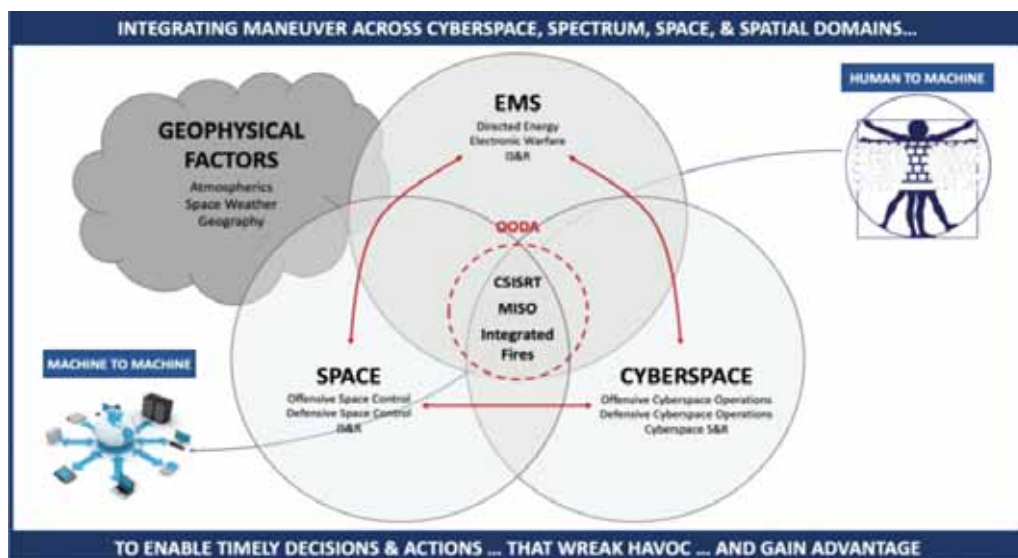
사이버전은 물리전과 결합된 하이브리드 전(Hybrid Warfare)으로도 불리는데, 러시아의 게라시모프 독트린(Gerasimov Doctrine)은 사이버공간을 본격적으로 전쟁의 영역으로 활용하는 것을 보여주는 사례이다.

군사 전략가들은 사이버공간을 지상, 해상, 공중, 우주와 더불어 새로운 전장으로 발견한 것이다. 이러한 사이버공간을 이용하고, 사이버공간에서, 전쟁을 수행하기 위해, 미국을 비롯한 많은 나라에서 사이버사령부를 창설하고 사이버전 전투원을 양성하며 사이버공간에 대한 교리적인 연구를 통해 전쟁 수행 개념들이 발전하고 있다.

군사작전에서 기동은 적군에 대해 우군이 방어와 공격에 우세한 기회를 가질 수 있는 위치를 차지하기 위한 부대의 이동, 무기의 배치를 의미한다. 이러한 기동이 사이버공간에도 적용될 수 있다. 미 국방부에서는 사이버공간도 기동(maneuver)의 대상으로 보고 있는데, <그림 1>은 미 해군에서 사이버공간을 기동의 대상으로 다루는 다영역작전 개념을 보여 준다.

기술적으로 볼 때 사이버공간은 인위적으로 만들어진 공간이지만, 군사적으로 보면 새롭게 발견된 공간이다. 단 물리공간과 달리 사이버공간에서의 기동은 물리공간과 다른 특성을 갖는다. 예를 들어 컴퓨터와 네트워크의 속도로 기동하며, 전기적인 신호에 의해 지속적으로 기동하고, 신체에서뿐만 아니라 우주 공간까지도 기동할 수 있다.⁵⁴⁾

54) G.Conti, D.Raymond, “On Cyber: Towards an Operational Art for Conflict”, 2017.



〈그림 1〉 사이버공간을 포함하는 다영역에서의 기동 개념

* 출처 : Navy Cryptologic & Cyber Warfare Community Vision, US Navy, 2019

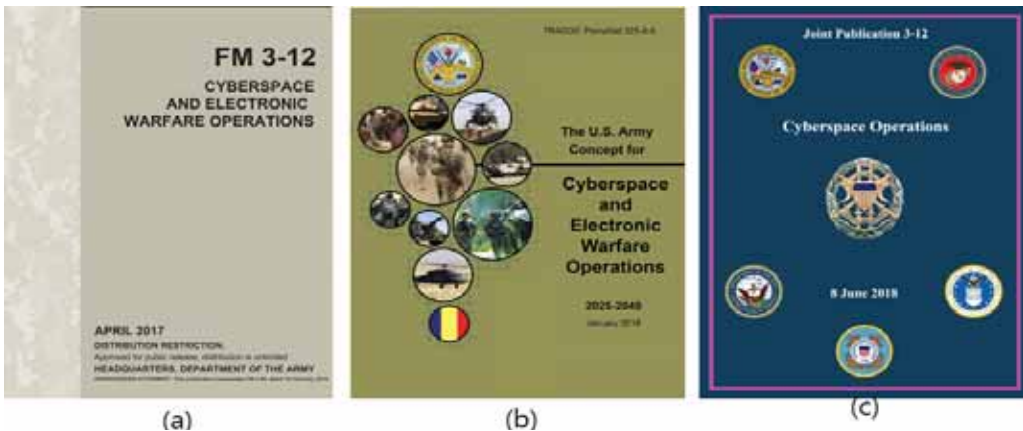
2. 사이버전의 등장

사이버전은 인터넷을 비롯한 가상현실세계(사이버공간)에서 다양한 공격수단을 이용하여 적의 정보체계를 교란, 거부, 통제, 파괴하는 등의 공격과 이를 방어하는 활동을 가리킨다.⁵⁵⁾ 또는, 국가 또는 그 요원이 자국의 이익을 위해 인터넷 등 사이버 공간에서 정보기술을 이용하여 타국을 대상으로 적대적 행위를 가하고, 이에 대하여 사이버공간에서 정보 기술을 방어하는 일련의 전쟁양상으로 정의되기도 한다.⁵⁶⁾

앞서 살펴봤듯이 미국은 사이버공간을 군사력을 투사하기 위한 전투 기동 공간, 즉 지상, 해상, 공중, 우주와 함께 전장 공간으로 정의하고 있다. 이를 위해 미군은 합동교리를 비롯하여 각 군에서 사이버공간을 활용하는 작전교리를 〈그림 2〉와 같이 정립하고 있다. 특히, 육군은 사이버전을 전자전과 결합한 사이버공간 및 전자전 작전으로 발전시키며 다영역작전 개념에 적용하고 있다.

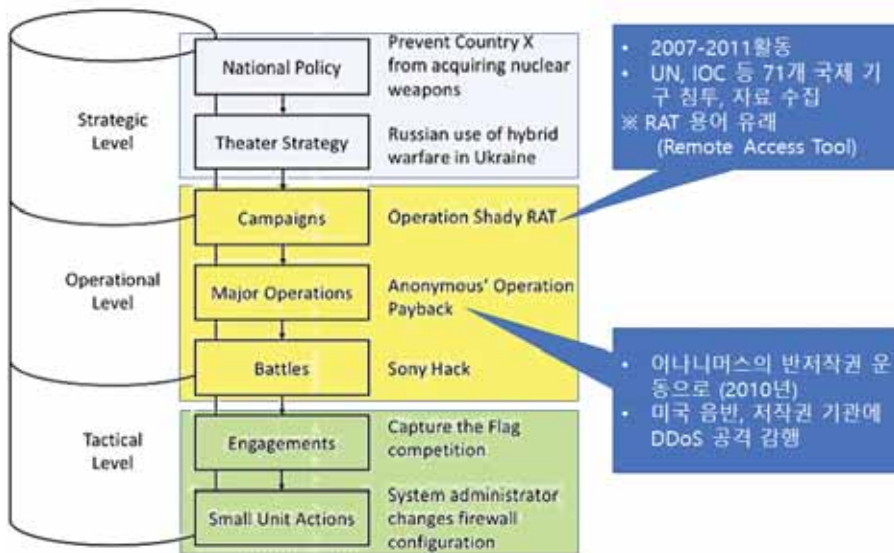
55) 사이버전 용어사전, 국군사이버사령부, 2018.

56) 사이버전 개론, 오명호 등, 2017.



〈그림 2〉 미군의 사이버전 관련 작전교리

- (a) 미 육군의 FM 3-12 (2017년), (b) 미 육군의 TRADOC (2018년),
(c) 합동교범 JP 3-12 (2018년)



〈그림 3〉 전쟁의 수준 관점에서 바라본 사이버전

* 출처 : G. Conti, D. Raymond, "On Cyber", 2017.

클라우드비즈의 전쟁의 수준(level of war) 관점에서 바라본 사이버전 개념은 〈그림 3〉과 같다. 전술적 수준에서는 사이버전은 CTF(capture the flag)와 같은 사이버 기술 경연 대회, 사이버 인프라 관리와 같은 단위 부대의 임무가 이뤄진다. 작전적 수준에서는 일련의 사이버 공격 활동의 집합으로 구성되는 캠페인(campaign)의 형태가 나타난다. 대표적인

사례로는 2011년에 발견된 Shady RAT, 어나니머스(Anonymous)의 반저작권 운동, Sony 엔터테인먼트에 대한 사이버 공격을 들 수 있다. 전략적 수준에서는 국가수준의 지원을 받는 사이버전 부대의 활동이 나타난다. 이것은 국가의 사이버안보 전략에 따른 전략적 활동, 군사적 전구(theater)를 대상으로 하는 사이버전 작전으로 수행된다.

제2절 사이버전과 워게임

1. 사이버 워게임의 등장

인류사에서 전쟁의 역사가 오래된 것처럼, 워게임은 긴 역사를 가지고 있다. 전통적으로 군대에서의 워게임은 전쟁에 대한 계획(planning), 평가(assessment), 훈련(training)을 목적으로 사용된다.

〈표 1〉은 워게임의 역사를 보여준다.⁵⁷⁾ M.B Caffrey 교수는 1차 세계대전 이후 근 현대의 전쟁 워게임이 등장한 것으로 본다. 1차와 2차 세계대전 이후 냉전시기에 워게임의 프레임워크가 정립되면서 기법이 발전하였다. 운용분석(OR: Operation Research)이 발전하면서 의사결정에 관한 수학적, 통계적 모형들이 워게임에 적용된 것도 이 시기이다. 반세기 정도의 시간을 두고 워게임이 발전을 해오다 미국의 9/11 테러를 기점으로 전쟁의 양상이 크게 변화되기 시작하면서 또다시 워게임의 변화에 큰 획이 그어졌다. 더욱이 컴퓨터 네트워크가 군사부분에서 차지하는 비중이 크게 높아지면서 사이버 위협은 전쟁의 또 다른 변화를 가져다준 요인이 되었다. 앞에서 살펴봤듯이 사이버 위협은 사이버공간을 전쟁의 또 다른 영역으로 발견하게 만들어준 역할을 하게 된 것이다.

〈표 1〉 워게임의 역사(미 해군 전쟁대학의 M. B. Caffrey Jr.)

Prehistory to 1913	: The Rise of Modern Wargaming
1905-1945	: Wargaming and the World Wars
1946-1989/1991	: Wargaming in the Cold War
1990s-2001	: Wargaming after the Cold War
2001-2011	: Post-9/11 Wargaming
2012-2016 and Beyond	: Wargaming in Transition

57) M.B.C.Jr, On Wargaming. Newport, Rhode Island: Naval War College Press, 2019.

전쟁의 양상이 사이버공간을 포함하는 다영역작전으로 발전하면서 사이버전을 대상으로 하는 사이버 위게임에 대한 연구와 사례가 증가하고 있다. 사이버 위협이 민간 영역에서도 그 영향과 위험이 커지면서 민간 영역에서 사이버 위게임에 대한 관심과 활용이 증가하고 있다.⁵⁸⁾ 특히 사이버 위게임의 필요성은 해킹, 랜섬웨어(ransomware), 피싱(phishing) 공격과 같은 사이버 위협의 증가와 관련이 있다. 군사 영역에서는 사이버공간을 이용하는 사이버 테러의 증가, 드론을 이용한 공격과 같이 전통적인 물리전에서 사이버/전자전으로의 변화가 일어나고 있다.

보통 사이버 위게임의 다음과 같은 역할로 사용되고 있다. 그것은 사이버 위협에 대해 조직에서 사용 중인 보안 통제의 적절성을 평가하고 사이버 방어 업무를 수행하는 운영자, 운영 부서의 능력을 향상시키는 데 사용되는 기술이자 도구의 역할로 사용된다.

이러한 전쟁의 양상이 변화하면서 사이버전의 복잡성으로 인해 사이버 위게임의 필요성이 군사 분야에서도 크게 증가하고 있다. 작전적 관점에서의 사이버 위게임은 작전 운영요원들에게 사이버 위게임 시나리오를 적용함으로써, 훈련 참여자들의 상호작용 능력을 향상시키고, 사이버 위게임의 시나리오를 반복 수행함으로써 발생 가능한 공격 기술을 개발하고, 이에 악용되는 요소들을 식별함과 동시에 조직과 시스템의 운영자들의 공격 대응능력을 평가하여, 충분한 대응을 위해 필요한 능력을 발견하고 능력을 향상 시키는데 사용되는 훈련 도구로 사용될 수 있다.

민간 분야이든 군사 분야이든, 그리고 물리전이든 사이버전이든 상관없이, 위게임은 조직의 경영진 또는 지휘부가 조직의 운영 목표를 달성하는데 직면한 위협을 이해하는데 가장 이상적인 방법이라고 볼 수 있다.

2. 사이버 위게임의 개념

가. 사이버 위게임의 활용 분야

사이버 공격에 대한 현재 능력의 효과성을 평가하고, 계획 목적의 잠재적인 추가 또는 변경 활동을 시험하며, 사이버 공격에 의한 시스템의 위험을 식별하는데 필요한 경험을 제공하기 위해, 사이버 위게임은 능력 평가(assessing capabilities), 계획(planning), 훈련(training), 그리고 위험 식별(risk identification)에 활용된다.

능력 평가는 조직에서 사용 중인 네트워크와 시스템 구조의 강점과 약점을 식별하는

58) David E. O’Gorman, “Military, Business and Cyber Wargaming: A Redteaming Perspective”, Amazon.com, 2nd ed. 2017.

활동이다. 평가 대상으로는 방어체계의 기술, 프로세스, 절차이다. 이들에 대한 평가는 모사된 환경(simulated environment)에서 이뤄지며 사이버 공격에 대한 현재의 방어 능력을 평가하는 것에 집중한다. 모사된 환경에서 수행되므로 최소한의 위험으로 의미 있는 결과(lessons learned)를 얻게 된다. 위게임이 수행된 다음에는 공격에 대한 방어 임무를 수행한 대항군에 대한 검토(review)가 이뤄지는데 이 과정에서 시스템 방어를 위한 보다 효과적인 대응책들을 발견할 수 있다. 이 때문에 위게임은 위게임 과정보다 사후 검토 과정이 전체의 성과를 좌우한다고 볼 수 있다. 이러한 사후 평가를 하지 않는다면 현재 능력에 대한 객관적으로 전반적인 평가 기회를 놓치는 것이다. 위게임의 사후 평가는 실제 피해를 보지 않고 효과적인 대응책을 발견하기 위한 절호의 기회가 된다.

계획은 위게임에 의해 현재 능력을 평가함으로써 미래 계획 수립에 필요한 자료를 얻는 활동이다. 현재 환경에서 미래에 적용 할 기술 능력을 예측하고, 기술의 적용 방법과 이에 대한 개선, 그리고 전략 변경을 위한 판단 자료를 얻는 것이다. 예를 들어 새로운 기술이나 구상 중인 기술을 현재 능력을 모사하는 위게임 환경에 모델링함으로써 실제적인 사이버 공격 시나리오를 통해 적용해 보는 것이다. 새로운 기술들을 적용하기에 앞서 변경이 필요한 사항들을 모방(emulating)하여 사이버 공격 환경에 적용하거나, 효과와 영향을 모사(simulating)하여 실제 시간, 노력, 자본의 투입을 대체해 볼 수 있다. 이것은 실제 장비가 없거나 사용이 어려운 경우 가상의 입력과 출력을 사용하는 것이다. 이러한 모방과 모사를 통해 실제 비즈니스 기능⁵⁹⁾ 환경을 변화시키지 않더라도 사전에 발생 가능한 위험을 식별 할 목적으로 위게임을 수행하는 것이다.

훈련은 현실의 운용자들에게 가상으로 실제의 경험을 체험시킴으로써 운용 능력을 숙달 하고 대처능력을 향상시키는 활동이다. 사이버 위게임 이외에도 컴퓨터 기반의 훈련(CBT: Computer- based training)과 교관 중심의 강의(instructor-led seminar), 또는 사이버보안 인증시험을 통해서도 수행될 수 있다. 하지만 이 방법들은 사이버 위게임의 실제적인 이벤트를 제공하지 않아 실제 환경의 경험을 가질 수 없다. 실제 사이버 공격 상황에서는 실시간으로 공격 상황에 직면함으로써 상당 수준의 스트레스가 가해지기 때문에 실전적인 경험을 위해서는 모사된 환경에서의 훈련이 필요하다. 사이버 위게임의 시나리오가 이러한 역할을 하게 된다. 현실감 있는 이벤트 발생으로 실제적인 수준의 스트레스를 경험 하며 훈련 대상자는 집중과 관심도를 극대화 할 수 있다. 즉 잘 구성된 이벤트에 의한 훈련으로 훈련 대상자들은 실제 상황을 체험할 수 있다. 이러한 연습을 통해 운영자들을

59) 비즈니스 기능(business function): 조직의 운영 목표를 달성하기 위한 프로세스 활동의 집합을 의미한다. 사용자, 프로세스, 응용 프로그램, 정보 자산이 포함된다. 은행을 예로 들면 전술적 수준에서는 온라인 뱅킹 거래 프로세스, 전략적 수준에서는 인수 합병 프로세스를 생각해 볼 수 있다.

훈련시키고 지휘 체계의 프로세스를 관찰할 수 있다. 이러한 과정 속에서 운영자들의 능력에 대한 강점과 약점을 동시에 평가하고 필요한 경우 기술 향상을 위한 지원과 스스로의 학습 필요성을 자각하도록 유도할 수 있다.

시스템 위험 식별은 사이버 위게임의 가장 중요한 측면이다. 여기에서 위험 식별이란 조직 전반에 걸친 범위를 대상으로 하며 비즈니스 기능의 복원력(resiliency)을 훼손하는 요소를 의미한다. 국가적인 수준에서 보면 국가기반시설(CI: Critical Infrastructure)에 관련된 기관들에 미치는 위협이 시스템의 위협으로 나타나게 되는 것과 같다. 사이버 위게임시 고려되어야 할 시스템 위험에 미치는 영향은 다음과 같다.

첫 번째로는 기술의 다양성 부족으로 특정 제품의 성능 저하 시 대응이 제한되는 상황이다. 예를 들어 오픈 소스 소프트웨어와 운영체제의 취약점의 경우에는 개발자나 업체가 보완책을 제공할 때까지 자체적으로 대응할 수 있는 방법이 제한되어 위험도가 증가하게 된다. 두 번째는 제3자 기관에 대한 의존성 증가로 조직의 독립성이 저하되는 상황이다. 세 번째는 “상호지원계획”을 통한 다른 협력 기관과의 협력이 실패하는 상황이다. 네 번째는 조직 내의 효과적인 소통 부족과 불명확한 책임 부여에 따른 위기 대응 및 의사결정이 지연되는 상황이다. 다섯 번째는 공격 행위에 대한 피해 저감 대책을 개발하는데 필요한 자료가 부족하거나 잘못된 정보가 제공되는 상황이다. 이러한 상황들이 고려되어 시스템 위험 식별이 이뤄져야 한다.

나. 사이버 위게임의 유형

19세기의 독일의 베르노이(J. D. Vernois) 장군은 위 게임을 두 가지 유형으로 구분하였다. 첫 번째 유형은 지휘, 통제, 통신의 C360) 절차에 대한 것으로 이것은 스크립트(script) 형태로 수행된다. 두 번째 유형은 레드팀이 블루팀을 공격하는 자유공방전 형태로 수행된다.

이에 반해 현대의 사이버 위게임은 세 가지로 구분된다. 첫 번째는 조직의 비즈니스 프로세스 중심의 테이블 탑(table-top)⁶¹⁾이다. 명칭의 의미에서 보듯이 과거 전통적인 전쟁 연습 분야에서 사용되어온 방식이다. 두 번째는 기술 중심의 레드 팀잉(red-teaming)이다. 레드팀(red-team)에 의한 모의 공격을 활용하는 방식이다. 세 번째는 테이블 탑과 레드 팀잉의 중간 형태인 복합형(composite)이다.

테이블 탑 유형은 방어팀만 사용하여 일방향으로 진행된다. 조직의 경영진 또는 지휘부 수준의 시나리오를 사용한다. 위게임 수행 간 실제 대응군의 활동은 없으며 위게임 참가자는

60) Command, Control, Communication

61) 테이블 탑(table-top)은 전장 환경을 모사하는 미니어처(miniature)를 설치하는 모래 상자에서 유래되었다.

사전에 정의된 시나리오와 이벤트에 대응하여 위계임을 수행한다. 수행 방법은 수작업 또는 자동화 시스템이 사용될 수 있다.

레드팀 유형은 방어팀과 공격팀을 사용하는 양방향으로 진행된다. 일방향으로 진행되는 테이블 탑에 비해 현실 상황에 더욱 가까우며 실재적인 수행이 가능하다. 공격팀은 직접 공격을 수행하는데 인간에 의해 이뤄지거나 자동화된 도구를 사용할 수도 있다. 자동화 도구를 사용하는 경우에는 동일한 유형과 수준으로 반복적인 공격이 가능하기 때문에 방어팀의 대응을 정형적으로 분석하는데 유리하다. 공격의 대상의 대상이 되는 시스템⁶²⁾은 실험실 환경의 장비, 연습 전용 장비, 또는 실제 운영 환경이 될 수 있다. 방어팀은 공격팀의 활동을 발견하도록 공격을 저지하도록 노력해야 한다.

복합 유형은 테이블 탑 유형에 비해 기술적인 요소를 적용할 수 있고, 레드팀 유형에 비해 비용과 노력의 투입을 절약할 수 있다. 다시 말해 비즈니스 기능 중심의 위계임과 사이버 방어 기술 중심의 위계임의 간극을 메우는 중간 수준의 유형이다. 비즈니스 프로세스와 모사된 기술을 결합한 형태로 볼 수 있다. 모사된 기술을 이용해서 공격에 대한 방어팀의 대응 수준의 자율성을 조정하고 조직 차원에서는 경영진의 의사결정의 수준을 조정 할 수 있다. 예를 들면 비즈니스 프로세스의 운영 중단이나 사용자 접속 제한 등을 활용하면서 위계임을 진행하게 된다.

다. 사이버 위계임의 주요 요소

사이버 위계임은 위계임의 범위, 비즈니스 기능, 시스템 환경, 방어적 사이버 기술과 자세, 위협, 시나리오에 의해 정의되며, 위계임의 범위(scope)는 연습 목적에 따라 결정된다. 조직에서는 최고경영진, 경영진, 관리자, 스텝 수준에서 선정하게 되고, 시스템에서는 네트워크 범위로 결정할 수 있다. 예를 들어, 조직 전체가 위계임의 대상이 될 수 도 있고, 하위 부문 중에서 주요 인프라만을 대상으로 할 수도 있다. 위계임에 포함되는 네트워크와 IT 자산의 범위는 해당 비즈니스 조직의 범위에 의해 결정하는 것이 적합하다. 왜냐하면 현재 조직에서 비즈니스 기능과 IT 기능은 분리되는 것보다는 비즈니스 임무 수행의 일부로 IT가 포함되어 있는 비중이 크기 때문이다.

비즈니스 기능(Business Function)은 조직의 임무 달성을 위한 프로세스와 활동들의 집합을 의미한다. 사이버 위계임을 활용하는 목적은 단순히 사이버 취약점을 식별하는

62) 정보기술(information technology) 시스템을 의미한다. 이러한 IT 시스템은 사이버 위계임에서 중요한 요소가 되는데, 시스템 환경에 따라 공격 전략, 공격 메커니즘이 영향을 받기 때문이다. 시스템의 예로는 네트워크 장비, 사용자 단말, 응용 시스템, 데이터 서버, 네트워크 토폴로지, 외부 네트워크와의 인터페이스 등을 생각해 볼 수 있다.

것에 있는 것이 아니고 사이버 취약점에 대한 위협이 비즈니스 기능에 미치는 영향과 그 위협을 식별하는 것에 있다. 앞에서 본 범위의 규모에 상관없이 비즈니스 기능은 어떤 방식으로든 사이버 위게임에 반영되어야 한다.

시스템 환경(System Environment)은 조직의 비즈니스 임무 달성에 사용되는 IT 자산을 의미한다. 네트워크, 시스템, 응용체계 뿐만 아니라 데이터도 그 대상이 될 수 있다. 시스템 환경은 사이버 위게임 유형을 결정하는데 중요한 요소가 된다. 테이블 탑 유형에서는 경영진이나 지휘부를 대상으로 하기 때문에 시스템 환경은 고수준의 추상화된 상태로 제시될 수 있다. 레드팀 유형에서는 기술과 운영자를 대상으로 하기 때문에 실제 시스템 또는 모사된 환경이 제시되어야 한다.

방어적 사이버 기술과 자세(Posture)는 현재 조직이 가지고 있는 방어 능력과 수준에 영향을 미친다. 사이버 위게임 결과가 실제 상황과 관련성이 높은 산출물이 나오려면 IT 환경에 적용된 보안 기능이 잘 고려되어야 한다. 예를 들어 네트워크 분리, 방화벽 구성, 단말기 보안 설정, 인증 및 접근 통제 정책, 탐지 센서와 모니터 도구 등이 실제 상황을 반영하여 위게임에 적용되어야 한다. 방어 기술은 네트워크 경계선 뿐 아니라 내부 네트워크와 시스템의 보안 능력을 포함해야 한다. 이것은 내부자 위협과 보안 경계선의 구분이 모호해지는 상황을 반영하기 위함이다. 위게임은 경계선 침투를 대상으로 할 수도 있고 이미 경계를 넘어 다양한 수단을 통해 침입한 상황에서 내부망에서 활동하는 위협을 대상으로 수행될 수도 있다.

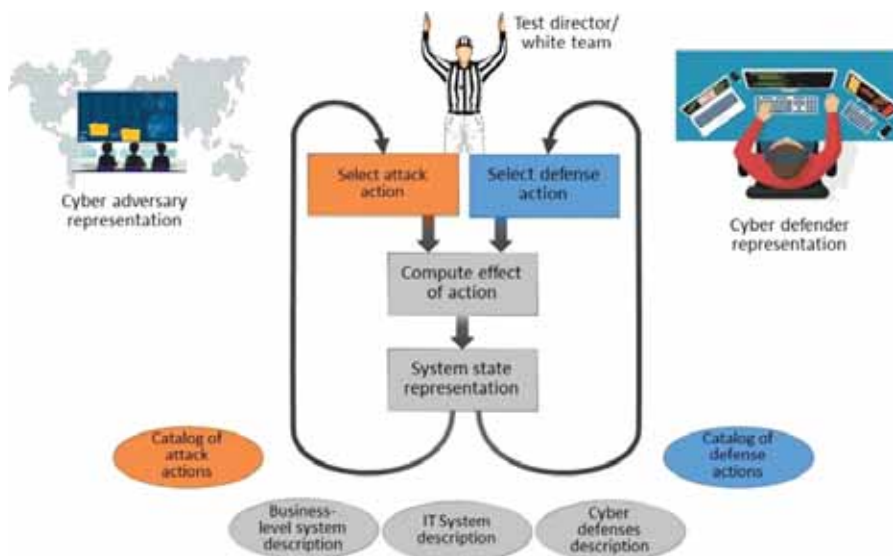
위협(Threat)은 사이버 위게임에서 효과적인 사이버 위게임의 산출물을 얻기 위해서는 조직의 IT 시스템 환경을 공격 표적으로 하는 공격자의 유형을 먼저 정의하고 이들의 목표와 능력을 구체화하는데 중요한 역할을 한다. 위협 모델은 모든 것을 경험한 것으로만 만들 수는 없다. 아직 경험해보지 못했던 적대적인 활동과 환경을 제시하되 실제로 그러한 위협을 얼마나 잘 대응할 수 있는지를 탐색하는 것이 중요하기 때문이다. 이 때문에 위협을 과소평가하거나 과대평가하는 것으로는 효과적인 위게임 산출물을 얻기 어렵다.

시나리오(Scenario)는 위게임 참가자가 경험하고 대응해야할 특정 상황을 제시하는 것이다. 예를 들면, 비즈니스 관점에서 어떤 일이 발생하는가? 공격자는 누구인가? 공격의 표적이 되는 자산은 무엇인가? 공격의 목적은 무엇인가? 이와 같이 위게임의 전반적인 흐름을 제시하는 이야기 형태가 될 수 있다. 이외에도 다른 조직에 대한 사이버 공격의 결과를 제시하거나 사이버 공격과 관련해서 조치된 행동, 언론이나 위협 정보의 출처를 통해 보고되는 정보, 공격자의 공격이 좌절되는 경우 대체 공격을 추구하는 방법에 대한 예상 등과 같이 추가적인 정황을 제시할 수도 있다.

제3절 사이버 워게임 참조 모델과 프레임워크

1. 사이버 워게임 참조 모델

사이버 워게임의 개념을 가시적으로 표현한 것이 사이버 워게임 참조 모델이다. 사이버 워게임 참조 모델을 활용하면 사이버 워게임의 구성 요소를 명확하게 이해할 수 있고 각각의 특성을 가시적으로 볼 수 있다. 사이버 워게임 참조 모델은 사이버 워게임을 어떤 유형 (테이블 탑, 레드 팀 등)으로 진행할지, 그리고 레드 팀으로 진행할 경우 훈련 환경이 실제 환경인지 또는 테스트 환경 인지 를 가시적으로 보여준다. <그림 4>는 사이버 워게임을 위한 프로세스 흐름과 각각의 주요 구성 요소들을 보여주는 개념적 참조 모델이다.



〈그림 4〉 사이버 워게임 참조 모델

* 출처 : David B. Fox, Catherine D. McCollum, Eric I. Arnoth, Darrell J. Mak, "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context", HSSDI, 2018.

2. 사이버 워게임 프레임워크

워게임에 있어서 프레임워크는 워게임 시나리오를 구성하는 기본 틀을 제공한다. 참조 모델과 함께 이러한 틀을 통해서 사이버 워게임의 구성 요소들을 명확하게 구분할 수 있다. 먼저 어떤 유형의 사이버 워게임을 적용할 것인지, 예를 들어 테이블 탑, 레드 팀 또는 중간 수준의 복합 유형 중에서 적합한 것을 선택하게 된다. 또 프레임워크는 사이버 워게임의 윤곽을 그리는데 활용된다. 어떤 기술과 프로세스를 사용할 것인지, 연습 플랫폼과 환경, 비즈니스 프로세스 모델, IT 시스템, 사이버 방어 시스템, 시스템의 현재 상태, 공격자와 방어자가 수행하는 작업의 영향을 볼 수 있는 가시화 자료 등이 포함된다.

기존의 워게임에 사용되는 프레임워크로는 군사분야에서는 WCK(Wargame Construction Kit)가 잘 알려져 있다. WCK는 미 해군 전쟁 대학(NWC: U.S. Naval War College)의 워게임 개발에 관한 강의 교재로 개발된 테이블 탑 유형의 워게임 프레임워크이다.⁶³⁾ 워게임 규칙, 시나리오, 지형 모델, 테이블 탑 진행에 필요한 도구들이 포함되어 있어서 맞춤형의 워게임을 만들 수 있도록 구성되어 있으나 사이버전 요소에 대한 개발이 필요하다.

민간분야에서는 사이버전 요소가 포함된 워게임 프레임워크로는 Cisco사의 Cyber Range, Unisys사의 cyber resilience wargame service⁶⁴⁾, PwC의 Game of Threats⁶⁵⁾ 등 많은 보안 업체에서 자체 개발한 것들이 알려져 있다. 하지만 대부분이 업체 자산으로 공개되어 있지는 않다.

미국 HSEDI(Homeland Security Systems Engineering & Development Institute)⁶⁶⁾에서는 2018년에 사이버 워게임 프레임워크 연구 보고서를 발간하였다. 이 프레임워크는 주요 기반시설 중에서 금융 서비스 부분에 대한 위협 모델과 사이버 워게임 프레임워크를 다루고 있다. 특히 기존의 테이블 탑 유형과 레드팀 유형의 복합 유형을 제시하고 있다.

63) P. P. Perla, et al., "Wargame-Creation Skill and the Wargame Construction Kit", Sanitized Version, CNA, 2004.

64) http://assets.unisys.com/Documents/Global/POVPapers/POV_170029_CyberResilienceServicesUnderstandingPotentialThreats.pdf

65) <https://www.pwc.co.uk/issues/cyber-security-services/game-of-threats.html>

66) HSEDI는 DHS(Department of Homeland Security)의 예산지원을 받는 FFRDC (Federally Funded Research and Development Center)의 하나이다. HSEDI는 "Next Generation Cyber Infrastructure (NGCI) Apex Cyber Risk Metrics and Threat Model Assessment"를 수행

〈표 2〉 사이버 워게임 구성요소별 프레임워크와 플랫폼 적용 예시

Wargame elements	Scripted (Card/ Tabletop)	Process Based Multipath	Simulated	Emulated	Live Exercise
Attack Step Selection	Script	Cyber Gym Maelstrom		BRAWL ¹³ Rapid7 (Metasploit)	Metasploit Human red team
Defense Step Selection	Script	Cyber Gym Maelstrom	CALDERA		Human blue team
State Change Evaluation / Execution	Disclose result	DECIDE			
Testbed	SimSpace	DECIDE		LARIAT KALI Linux BRAWL	NCR BSides
Attack Vocabulary	ATT&CK (Windows)	ATT&CK (Windows)	ATT&CK (Windows)		Armitage ¹⁴
Defense Vocabulary		Maelstrom	STIX CAR CAPEC CyBOX ¹⁵ CALDERA		
System	N/A	N/A		LARIAT KALI Linux	Real hardware and application execution

테이블 탑 유형은 경영진과 지휘부에 초점을 맞추었기 때문에 기술적인 구체성 보다는 의사결정 프로세스를 관찰하는데 적합하다. 실재 시스템을 연동할 필요가 없기 때문에 비용이나 운영에서 부담이 적다. 레드팀 유형은 공격 기술과 방어 기술에 초점을 맞추었기 때문에 실무진의 참여에 의한 운영자들의 능력 평가와 기술 수준 향상에 적합하다. 하지만 실재 시스템과 많은 장비, 시뮬레이션 등이 필요하기 때문에 비용 부담이 크다. HSSEDI에서 제시하는 복합 유형은 이러한 양 끝단의 특징들을 잘 조화하는 형태이다. 물론 워게임의 목적에 따라 테이블 탑, 레드팀 복합 유형을 선정하는 것이 바람직하다. 〈표 2〉는 사이버 워게임을 구성하는 요소에 대해 현재 알려져 있는 프레임워크와 플랫폼들을 적용한 예를 보여주고 있다.⁶⁷⁾

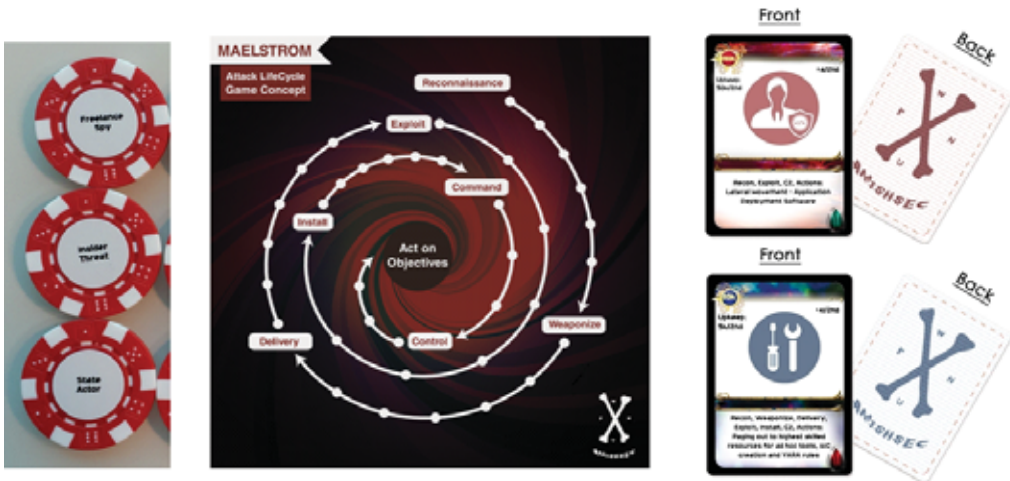
III. 사이버 워게임 사례분석 및 시사점

제1절 사이버 워게임 기술

1. 사이버 워게임 플랫폼

67) David B. Fox, Catherine D. McCollum, Eric I. Arnoth, Darrell J. Mak, "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context", HSSEDI, 2018.

본 절에서는 해외에서 사용되고 있는 대표적인 주요 사이버 위게임 플랫폼을 살펴본다. 여기에서 살펴볼 사이버 위게임 플랫폼은 DECIDE(Distributed Environment for Critical Infrastructure Decision-Making Exercises), Maelstrom, Cyber Gym, SimSpace 이다. 미국 Norwich 대학의 첨단연구센터인 NUARI (Norwich University Advanced Research Institute)에서 개발한 테이블 탑 유형의 위게임 플랫폼이다. 뒤에서 살펴볼 미국의 국가 수준의 사이버 위게임인 Cyber Storm에 사용되는 것으로 알려져 있다.⁶⁸⁾



〈그림 5〉 Maelstrom의 구성품 예시(왼쪽부터 보드 게임 칩, 게임 보드, 게임 카드).

Maelstrom은 Lockheed Martin사의 Cyber Kill Chain을 보드 게임 형태로 개발한 것이다. 공격팀과 방어팀으로 나누어 네트워크 공격을 방어하는 방식으로 게임이 진행된다. 2016년 Defcon 24에서 발표되었고 Github에 게임에 필요한 설명서와 인쇄가 가능한 게임 카드가 공개되어 있다.⁶⁹⁾

Cyber Gym는 이스라엘 기업인 Cyber Gym에서 개발한 사이버 위게임 플랫폼이다. 주로 유럽과 영국의 금융 기관에서 사이버 위게임을 위한 교육 플랫폼으로 활용되고 있다. 고객사의 요구에 따라 사이버 방어 및 공격 시나리오를 맞춤형으로 조정하고 모의 공격을 통해 훈련을 진행한다. 앞에서 살펴봤던 사이버 프레임워크에 따라 구성되어 있으며 레드팀, 블루팀, 화이트팀으로 나누어 위게임을 진행한다.⁷⁰⁾

68) <http://nuari.org/>

69) <https://github.com/maelstromthegame/defcon24/>

70) <https://www.cybergym.com/>

2. 사이버 워게임 자동화 공격 도구

사이버 워게임에서 공격팀은 사람 또는 자동화 도구를 사용한다. 사람으로 구성된 공격팀은 구성원들의 실력과 상황에 따라 공격 능력이 변화될 수 있다. 하지만 동일한 공격에 대한 방어 능력을 향상시키는 것을 목적으로 할 경우, 공격팀의 능력 변화는 방어팀에 대한 정량적 평가를 어렵게 만드는 요인이 된다.

따라서 반복적이고 정형화된 공격자 모델이 필요한데 이때 반복 가능한 자동화 도구가 일련의 공격자 기술을 실행하여 공격팀의 역할을 할 수 있다. 이 때문에 사이버 워게임에서 자동화 공격 도구는 중요한 역할을 한다. 자동화 공격 도구는 공격 모사(adversary emulation) 기능을 갖고 있다. 이것의 목표는 사이버 공격을 모사하고 이를 자동화하여 방어 활동을 반복적으로 수행하면서 결국 방어 능력을 향상시키는 것이다.

Persistence - Registry autorun keys - Scheduled Task - Services Privilege Escalation - Weak service perms - Weak service file perms - Unquoted paths (Path interception) Defense Evasion - Scripting - Timestomping Credential Access - Credential Dumping Lateral Movement - Remote File Copy - Windows Admin shares - Pass the Hash - PsExec	Discovery - Remote System Discovery - Local Network config - Registry - Account - System information - Processes/services - System Owner - Permission Group - Files Execution - PowerShell - Scheduled Task - WMI - SC (service controller) Exfiltration - HTTP/S

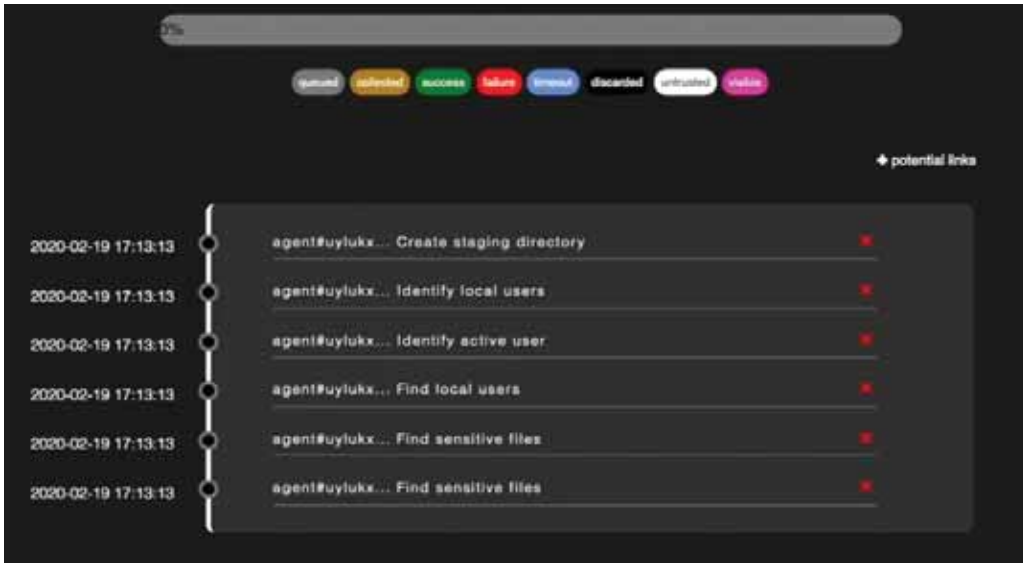
〈그림 6〉 CALDERA에서 모사 가능한 공격 유형 예시

대표적인 공개 도구는 MITRE에서 개발한 CALDERA(Cyber Adversary Language and Decision Engine for Red Team Automation) 이다.⁷¹⁾

CALDERA는 MITRE에서 개발한 사이버 인텔리전스 도구를 사용한다. 예를 들어

71) <https://github.com/mitre/caldera/>

ATT&CK는 공격 유형을 위협 모델로 분류한 프레임워크이다. 또 CAR(Cyber Analytics Repository)⁷²⁾는 사이버 공격 유형에 대한 분석 보고서를 제공한다. <그림 6>은 ATT&CK을 참고하여 CALDERA에서 모사가 가능한 공격 유형을 예를 보여준다.



<그림 7> CALDERA의 모의 공격 화면 예시

CALDERA는 자동화 공격 도구로서 공격의 유형을 정하고 나면, 공격 수행은 자체의 의사 결정 알고리즘에 의해 수행된다. CALDERA의 의사 결정 알고리즘은 지능적으로 공격 옵션을 선택하여 공격 유형의 전술적 목표를 달성하도록 개발되어 있다. <그림 7>은 CALDERA의 모의 공격 화면 예시이다.

제2절 사이버 워게임 사례

1. Cyber Storm

사이버 스톰(CS: Cyber Storm)은 미국 국토안보국(DHS: Department of Homeland Security)의 국가사이버보안처(NCSD: National Cyber Security Division)에서 주관하는

72) <https://car.mitre.org>.

국가 수준 사이버 워게임으로서 국회의 요청에 따라 2006년부터 실시되고 있다. 2012년을 제외하고는 2006년부터 격년제로 실시되고 있다. 연방 정부 기관, 주 정부, 업체들의 참여를 활성화해서 사이버 공격의 기술적 요소뿐만 아니라 유관기관 사이에서 종합적인 대응 훈련을 하며 정보공유 파트너십을 강화하고 있다. 훈련 결과는 다음 훈련에 반영함으로써 지속적으로 국가적인 대응 역량을 향상시키는 것을 목적으로 한다.

〈표 3〉 DHS Cyber Storm Series

- Cyber Storm I (Feb. 6-10, 2006)
- Cyber Storm II (Mar. 10-14, 2008)
 - * 5 eyes와 연합 연습, 개별 대응 능력과 리더십 의사 결정
- Cyber Storm III (Sep. 27-Oct. 1, 2010)
 - * 국가 차원의 프레임 워크 대응 중점, NCCIC⁷³⁾의 운영 시험
- Cyber Storm IV (Nov. 2011-Jan. 2014)
 - * 2011년 ~ 2014년, 15개의 단위 연습을 수행
- Cyber Storm V: (Mar. 7-11 2016)
 - * 1000명 이상의 분산 활동, 상업 및 건강 관련 부문 추가
- Cyber Storm VI: (Mar. 2018)

〈표 3〉에 요약되어 있는 CS의 주요 사항들을 보면 참여 규모가 점진적으로 확장되는 것을 알 수 있다. CS은 미국뿐만 아니라 다른 국가도 참여할 수 있는데 CS IV에서는 11개국이 참여하였다. CS는 시나리오를 기반으로 진행되며 사이버 공격은 실제 체계를 사용하지 않고 모사(emulation) 된다.⁷⁴⁾ 시나리오는 국가의 주요기반시설을 대상으로 한다. 3일간의 훈련 기간 동안 국가의 지원을 받는 사이버 위협 세력에 의한 국가전산망, 전력망, 금융망 등에 대한 기반시설 공격 시나리오를 기반으로 진행된다.

73) NCCIC (National Cybersecurity and Communications Integration Center): DHS의 CISA (Cybersecurity and Infrastructure Security Agency) 소속의 국가 사이버보안과 통신 통합 센터이다. 기존의 US-CERT, ICS-CERT, NCC 등이 하나로 통합되었다.

74) 모사(emulation)는 실제 체계를 사용하지 않고 실제 체계에서와 유사한 결과 값을 대신 사용하는 방법이다. 이에 반해 모의(simulation)는 실제 체계를 사용하여 그 출력 결과를 사용하는 방법이다.

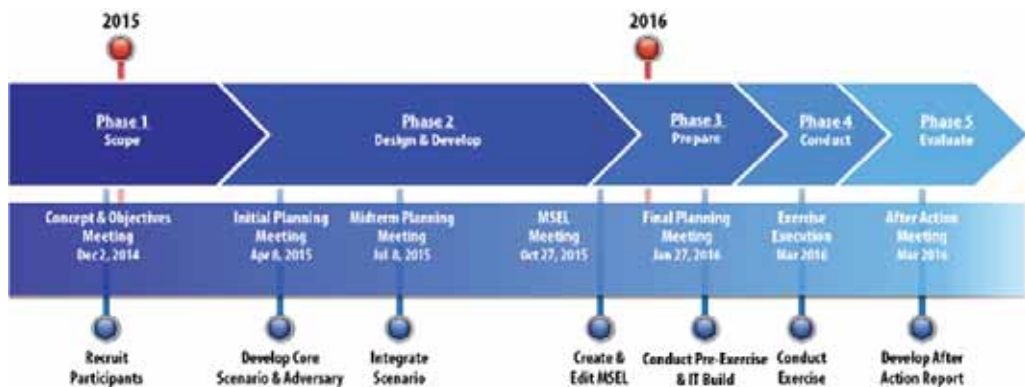


〈그림 8〉 Cyber Storm IV 사후분석 보고서와 안내표지

CS 사이버 위게임의 특징 중 하나는 위협 인식 수준과 정보 공유 능력, 그리고 TTP 대응 절차를 향상 시키는 것이다. 즉 기술적 대응뿐만 아니라 정책적 판단에 대한 대응도 주요 훈련 항목이 된다. 예를 들어 소셜미디어를 통해 선거에 영향을 미치는 가짜뉴스를 판별하고 대응하는 절차 등을 살펴보게 된다. CS에서는 각 참여 기관들의 사이버 위협에 대한 대응 능력을 시험하기 위하여 사이버 공격의 잠재적인 영향에 대한 준비, 보호, 대응 절차를 모니터 한다. 사이버 테이블 탑의 유형으로 진행되기 때문에 전략적 의사결정 과정을 시험한다. 특히 정보 공유 관계의 유효성을 중점적으로 분석하는데, 각 기관에서 사이버 위협 정보를 공유하는 수단과 프로세스가 그 대상이 된다.

〈그림 9〉는 2016년에 수행된 CS V의 프로세스를 보여준다. 앞에서 살펴본 사이버 위게임 프레임워크와 유사하지만 준비에 매우 많은 시간이 소요되었음을 볼 수 있다. 실제 CS 연습이 2016년 3월에 수행되었는데, 개념과 목표 정립은 2014년 1월부터 시작되었고, 이후 1년여의 기간 동안 계획과 훈련 시나리오를 구체화하였다. CS V에는 10개 연방 기관, 32개 주, 45개 업체, 22개의 협력 기관, 그리고 해외 12개국의 총 1200여명 이상의 인력이 참여하여 역대급 규모로 수행되었다.⁷⁵⁾ 실제 연습은 2016년 3월 7일부터 11일까지 4일간 진행되었다. 연습이 종료된 이후에는 평가 단계가 시작된다. 사후분석 보고서는 일반 내용들은 모두 인터넷으로 공개되고 있다.

75) CS V에 참석한 아시아 국가는 일본이 유일하다.



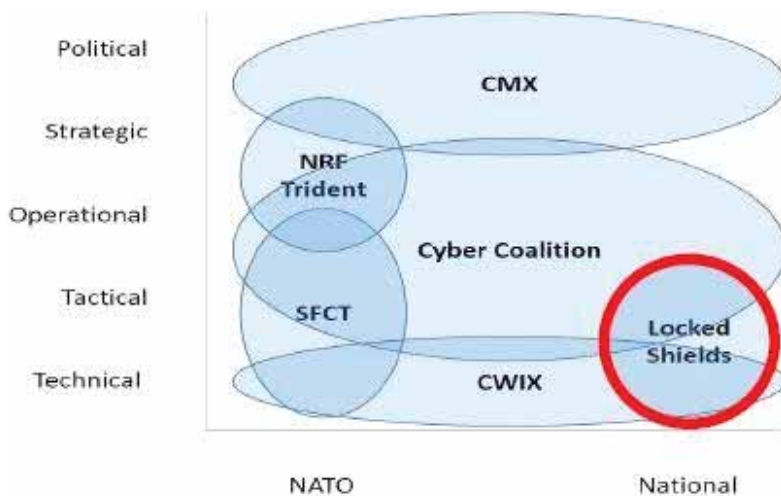
〈그림 9〉 Cyber Storm V의 5단계 프로세스

* 출처 : Cyber Storm V: After Action Report, Homeland Security, 2016.

2. Locked Shields(LS), Crossed Swords(XS)

에스토니아는 사이버전 역량 강화를 목적으로 연합 사이버 워게임인 Locked Shields (LS)와 국제 사이버 컨퍼런스인 CyCon을 개최하고 있다. 이중에서 LS는 실시간 공격에 대한 협력을 통한 방어 중심 훈련으로서 2012년부터 매년 에스토니아에 있는 NATO CCDCOE(Cooperative Cyber Defense Center of Excellence)에서 주관하며 에스토니아 탈린에서 개최된다. NATO CCDCOE 회원국의 민·관·군 보안전문가들이 참여하여 사이버 위협에 대한 대응 준비태세를 점검하고 서로의 실력을 겨루는 국제 사이버 방어 훈련으로 사이버 공격에 대한 기술적 대응 외에도 언론·법·전략, 사이버 공격에 대한 포렌식 대응 등의 능력을 종합적으로 평가하고 있다. LS는 〈그림 10〉과 같이 전술적, 기술적 수준의 사이버 워게임이다.⁷⁶⁾

76) 조성림, “NATO 사이버연습, 우리도 참여할 수 있어”(http://kookbang.dema.mil.kr), 2019.



〈그림 10〉 Locked Shields의 사이버 워게임의 유형

* 출처 : 조성림, “NATO 사이버연습, 우리도 참여할 수 있어” (<http://kookbang.dema.mil.kr>), 2019.

〈표 4〉 Locked Shields 연혁 (2012~2019)

Exercise	Number of Blue Teams (BTs)	Nations represented in Blue Teams	BT size cap	VMs per team	Persons involved
Baltic Cyber Shield 2010	6	3 + NATO	10		< 100
Locked Shields 2012	9	9 + NATO	10	~25	250 +
Locked Shields 2013	10	9 + NATO	12	34	~ 250
Locked Shields 2014	12	14 + NATO	16	50	300
Locked Shields 2015	15	16 + NATO	16	~75	400
Locked Shields 2016	20	19 + NATO	16	~75	550 +
Locked Shields 2017	20	19 + NATO	∞	120	~ 800
Locked Shields 2018	22	20+NATO+EU	∞	150	1000
Locked Shields 2019	23	21+NATO+EU	∞	150	1200

〈표 4〉는 2012년부터 2019년까지 시행된 LS 연혁이다.⁷⁷⁾ 대한민국은 국가보안연구소에서 참여하고 있지만 국방 기관에서는 참여하고 있지 않다. 우리나라와 같은 NATO

77) 강정민, “사이버 훈련의 이해”, 국가보안기술연구소, NetSec-KR 2020, 2020.

비회원국은 CCDCOE의 운영위원회의 동의를 거쳐 기여국가(CP: Contributing Nation /Participated) 자격으로 참여가 가능하다.

LS의 운영 조직은 앞서 살펴본 사이버 위게임 프레임워크 참조모델과 같이 5개 팀으로 구성되어 있다. 화이트 팀은 시나리오, 그린 팀은 인프라, 옐로우 팀은 상황 인식, 레드 팀은 사이버 공격, 블루 팀은 방어를 담당한다. 블루팀은 가상사설망(VPN: Virtual Private Network)으로 LS에 참여한다.

Crossed Swords(XS)도 CCDCOE에서 주관하는 사이버 위게임으로 2016년부터 매년 실시하고 있는 XS는 사이버공격을 수행하는 레드 팀에 대한 기술 중심의 위게임이다. 레드 팀에 특화된 기술적 연습에 초점이 맞추고 있어서 TTTP(Techniques, Tools, Tactics, Procedures)를 평가한다.

제3절 DoD CTT (Cyber Table-Top)

현대 무기체계는 첨단 기술을 활용하면서 네트워크 중심의 IT 환경에 대한 의존성이 증가하고 있다. 이러한 추세에 따라 무기체계의 사이버 위협 취약성에 대한 위협은 증가하고 있다. 이에 따라 미 국방부(DoD: Department of Defense)는 무기체계 획득 과정 속에 사이버 테이블 탑(CTT: Cyber Table Top) 프로세스를 적용하고 있다.⁷⁸⁾

CTT는 NIST SP 800-30 'Guide for Conduction Risk Assessments'에서 제시하는 임무기반 사이버 위협 평가(MBCRA: Mission-Based Cyber Risk Assessments) 방법의 하나이다. 여기에서 MBCRA는 DoDI 8510.01 'RMF for DoD IT'의 위협 평가 기법이다.

미 국방획득대학 (DAU: Defense Aquisition University)에서 정립한 사이버보안 및 획득 생명주기 통합 도구(CALIT: Cybersecurity & the Acquisition Lifecycle Integration Tool)에서는 CTT를 다음과 같이 정의한다. 첫째, 경량화 되어 있고 비용이 저렴하며 지속적으로 집중적인 위게임 연습으로서 대화와 소통으로 진행되며 시스템에 대한 실제 사이버 공격을 포함하지는 않는다. 둘째, 사이버 공격이 무기체계 시스템에 미치는 영향을 연습을 통해 알아가는 탐색 과정이다. 셋째, 방어팀과 공격팀의 양방향 절차에 집중한다. 넷째, 무기체계 프로그램 관리자, 엔지니어, 시험평가 요원에게 조치 가능한 정보⁷⁹⁾를 제공하여 사이버 위협이 임무 수행에 미치는 영향을 조치할 수 있도록 돕는다.

이와 같이 CTT는 무기체계 획득의 MBCRA의 관점에서 임무에 영향을 미치는 사이버

78) The Department of Defense Cyber Table Top Guidebook", DoD, 2018.

79) 조치 가능한 정보(actionable information)가 의미하는 것은 무기체계 체계 획득 과정 속에서 통제해야 할 위험 요소들을 비용 대비 효과성 측면에서 실제 조치할 수 있는 사항들을 제공해야 한다는 점이다.

위험에 대한 조치 가능한 정보를 제공하는 것이 목표이다. 여기에서 조치 가능한 정보라는 것은 무기체계 획득과정에서 비용과 효과 대비 합리적인 조치가 가능한 대안을 결정하는데 필요한 정보로서, 취약점, 취약점을 악용하는 방법, 그리고 그 취약점이 임무 수행에 미치는 영향 평가 결과를 포함한다. 이러한 정보는 무기체계 획득 사업의 PM(program manager), 정보시스템 보안 담당관(ISSM: Information System Security Manager), ISSE와 같은 주요 책임자 뿐 아니라 체계 개발에 관련된 시스템 엔지니어, 시험평가 요원들에게 제공된다.

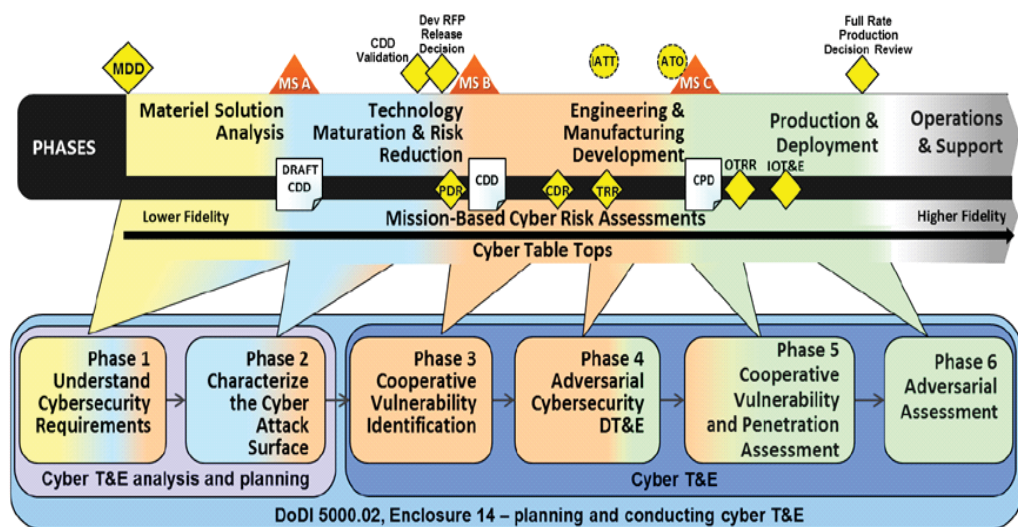
CTT는 지적 전쟁 게임과 같은 위게임의 형태로써 무기체계에 대한 사이버 위협을 분석하고 실행 가능한 대응 전략을 수립하기 위한 일련의 의사결정 참고자료를 얻는 것을 목표로 한다. CTT의 연습과 분석은 잠재적인 사이버 보안 취약점의 위험 식별과 이해를 용이하게 한다.

CTT에서 도출된 내용은 무기체계에의 위협을 감소(reduce), 완화(mitigate), 대응(counter)을 위한 조치들을 결정하는데 참고 된다. 이러한 정보를 통해 제한된 자원을 더 효과적으로 할당하고, 사이버 위협 환경에서 성공적으로 임무를 수행할 수 있는 시스템을 개발하는데 기여한다.

CTT는 알려진 정보, 또는 알 수 있는 정보를 기반으로 잠재적인 취약성을 예상하고 관련 위협을 활용하는 공격 세트를 활용한다. 따라서 공격자가 시스템에 할 수 있는 완전하고 포괄적인 공격 시나리오를 모두 활용하지는 않는다.

CTT의 궁극적인 목표는 사이버 공간에서 적대세력이 무엇을 목표로 하는 것인지를 예측하는 것이 아니고, 작전 임무의 성공에 중대한 영향을 미칠 수 있는 시스템과 그 능력을 파악하는 것이다. 다시 말하면 공격자 관점에서 공격자의 의도를 예측하고 결정하는 것이 매우 어렵기 때문에, 시스템 관점에서 가장 악용될 수 있는 취약점이 무엇인지, 이 취약점에 대한 위협은 무엇인지, 그래서 공격이 성공할 경우 어떤 위협을 얻게 되는지를 이해하는 것이 CTT의 궁극적인 목표가 된다.

이 때문에 인텔리전스(intelligence)를 활용하게 되는데, 현실적으로 충분한 인텔리전스를 획득하는 것이 어렵지만 CTT를 수행하는데 있어서 인텔리전스의 역할은 매우 중요하다. 따라서 인텔리전스와 CTT의 효율성과의 간극을 줄이기 위해서는 반복적인 피드백 활동이 필요하다. 예를 들어 CTT를 활용해서 공격 표면(attack surface)의 우선순위를 지정하거나, 알려져 있는 공격자의 능력 또는 의도를 이해하기 위한 활동이 필요하다.



〈그림 11〉 NIST SP 800-30의 MBCRA

* 출처 : DODI 5000.02, Enclosure 14.

〈그림 11〉에서 볼 수 있듯이, CTT는 사이버위협 시험&평가 절차에 포함되어 있다. DoD의 무기체계 획득 생명 주기는 Phase 1에서 Phase 6까지 6단계로 구분이 되는데, CTT는 모든 생명 주기에서 활용된다. 그리고 CDD, CPD가 완성되는 시점별로 3개의 마일스톤(MS: milestone)이 지정되어 있는데, CTT는 이들 마일스톤별로 활용 목표를 수립하는데 기준자료가 된다.

MS A에서는 사이버보안, 사이버 생존성, 작전적 회복 요건을 검토한다. MS B에서는 사이버공격 표면(cyber-attack surface)를 분류하고 이것을 MS C에서 취약점 평가에 적용한다. MS C 이후에는 지속적 관찰(continuous monitoring)을 수행한다.

무기체계에 대한 CTT 활용은 다음 장에서 자세히 살펴보도록 하겠다.

제4절 분석과 시사점

이 장에서는 사이버 위게임의 프레임워크를 분석하고 대표적인 사이버 위게임 사례들을 살펴보았다. 사이버 위게임의 프레임워크는 미 DHS의 후원으로 수행된 HSSEDI의 보고서를 참고하였으며, 국가 수준의 사이버위협 대응 역량 향상을 목적으로 하는 미국 DHS의 사이버 스톰, 국제 사이버 협력 강화를 위한 에스토니아의 Locked Shields를 살펴보았다.

첫째, 사이버 위게임은 위게임의 목적에 따라 다양한 분야에서 적용되어 발전되고 있음을 알 수 있었다. 특히 군사적인 측면에서는 물리공간에서의 물리전과 사이버공간의 사이버전의 하이브리드 융합 형태로 발전하고 있다. 그러므로 미래전에서 사이버 위게임은 필연적인 역할을 하게 될 것이다. 사이버 위게임 프레임워크는 각 기관의 위협 관리 활동에 따라 사이버 위게임이 효과적으로 수행되도록 적절하게 적용되어야 할 것이다. 즉 기술 환경이 사이버 공격으로부터 받을 영향과 그 위험을 통제할 수 있도록 세부적인 사항들이 테일러링(tailoring)되어야 한다.

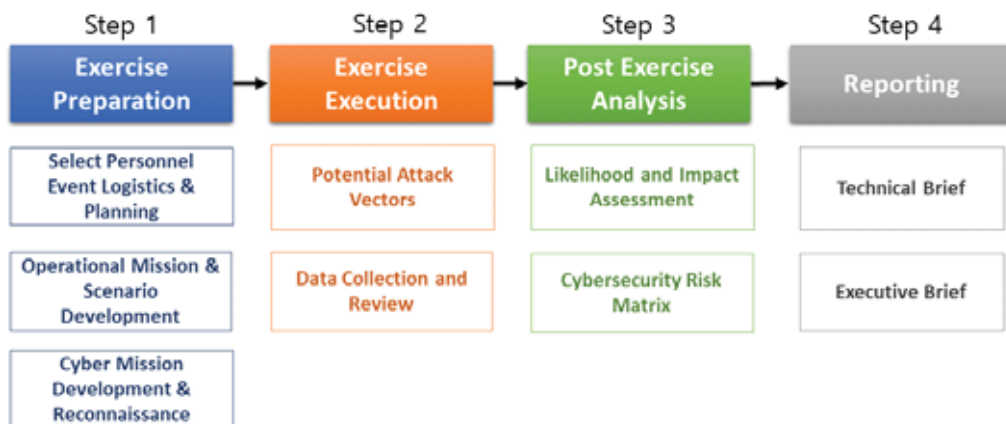
둘째, 무기체계 획득에서 활용되는 사이버 위게임의 역할이다. 무기체계에서 정보통신 기술이 차지하는 비중과 외부 네트워크와의 의존도가 증가함에 따라, 무기체계는 사이버 공간에서의 임무 수행 범위가 넓어지고 있다. 이 때문에 무기체계의 획득과 시험평가 단계에서 사이버공간에서의 대응 능력과 복원 능력을 검토하고 확인해야 할 필요가 있다. 이와 같이 사이버 위게임은 전쟁 연습뿐만 아니라 무기체계의 획득과 시험평가에 적용되고 있는 추세이다.

다음 절에서는 무기체계의 사이버보안 위협을 획득단계에서 통제하기 위한 미국 DoD의 사이버 테이블 탐과 한국군을 위한 사이버 위게임 활용 방안을 제시하고자 한다.

IV. 한국군을 위한 사이버 위게임 활용 방안

제1절 DoD CTT의 활용

DoD CTT는 무기체계 획득 책임자에게 다영역에 접한 무기체계에 대한 사이버보안 개념을 제공함으로써 사이버공간을 전쟁의 영역 중 하나로 인식하는 데 도움을 준다. 본 절에서는 DoD CTT를 국방분야에 활용하기 위해 필요한 내용들을 살펴본다. CTT는 <그림 12>과 같이 4단계로 구성된다. 1단계는 연습 준비, 2단계는 연습 시행, 3단계는 사후 분석, 4단계는 결과 보고를 수행한다. 각 단계에서 CTT 활용을 위해 어떤 준비가 필요한지 하나씩 살펴본다.



〈그림 12〉 CTT Process

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

1. (1단계) 연습 준비

1단계에 필요한 시간은 보통 30~60일이다. 이 단계는 임무영향평가(Mission Impact Assessment)를 위한 준비 단계이면서, 발생가능성평가(Likelihood Assessment)를 위한 방법론이 정의된다.

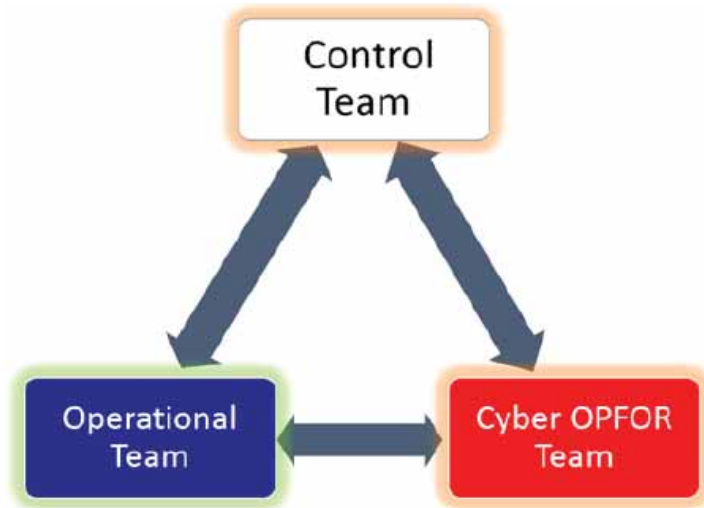
이 단계에서는 CTT 수행을 위한 팀 구성원을 선발하고 팀의 임무와 수행 가능한 시나리오를 정의하며, CTT 대상에 대한 사전정찰을 수행하기 위해 관련 문서들을 수집하고, CTT 수행 계획과 그 결과로서 얻게 되는 산출물들을 정의하고 구체화한다.

1.1. 팀 구성

CTT 수행팀은 통제팀(control team), 작전팀(operational team), 사이버공격팀(cyber opposing force team)으로 구분된다. 통제팀은 CTT 수행을 주관하며 CTT 수행에 필요한 물자를 지원한다. 작전팀은 사이버방어 임무를 위해 대부분의 CTT 활동을 수행한다. 사이버공격팀은 CTT 2단계인 연습 시행에서 주로 활동하는데, 이 팀의 리더는 1단계에서 정찰, 계획/임무 할당을 위해 다른 팀들과의 사전 협조를 수행한다.

통제팀은 CTT 목표 달성을 위한 일정을 관리하며, 연습 계획을 수립한다. 이를 위해 팀 구성원 사이에서 지속적인 의사소통이 필요하다. 통제팀의 구성은 팀 리더, CTT 관리자,

작전팀 리더, 사이버공격팀 리더, 그리고 서기로 이뤄진다. 그리고 CTT 수행에 필요한 기술 자문을 위한 주제별 전문가 그룹(subject matter expert, SME)을 활용한다. 예를 들면 개발시험 책임자, 시험평가 실무 책임자, 시스템 개발담당 엔지니어, 그리고 해당 분야에서 작전 경험이 있는 현역 군인 또는 예비역, 사이버보안 전문가를 활용한다.



〈그림 13〉 CTT의 팀 구성

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

작전팀은 CTT에서 사이버방어 임무를 수행한다. 이를 위해 사전계획 수립, 사후 보고, 시스템에 대한 유지보수 활동을 하며, CTT를 위한 시스템 확보, 시험계획 수립에 관여한다. 작전팀은 사이버방어 임무 수행에 필요한 기술적 이해와 작전적 이해를 갖고 있어야 한다. 기술적으로는 시스템 설계, 인터페이스, 통신 경로, 데이터 흐름 등에 대한 지식이 필요하다. 작전적으로는 시스템의 임무와 그 역할, 사이버공격의 TTP, 시스템의 현재능력과 목표능력을 알고 있어야 한다. 이러한 역할은 해당 작전을 수행하는 현역 군인, 군무원 또는 DT와 OT 담당자, 시스템 운영자, 임무에 관련된 무기와 전술 담당자, 시스템 개발 및 정비 담당자, 사이버보안 서비스 제공자(CSSP: Cyber Security Service Provider), 정보시스템 보안 담당관(ISSM) 등이 적합하다.

사이버공격팀은 CTT에서 공격 임무를 수행한다. 통상적으로 4~8명으로 구성되는 것이 효과적이다 다양한 잠재적인 공격 기회를 구현할 수 있도록 광범위한 분야의 인력으로 구성한다. 예를 들어, 공격과 방어, 사이버보안 테스트, 사이버전 작전 요원 등으로 구성

된다. 공격을 수행하기 위해 사이버공격팀원들은 CVE(Common Vulnerabilities and Exposures), CAPEC (Common Attack Pattern Enumeration and Classification), CWE (Common Weakness Enumerations), NVD(National Vulnerabilities Database) 등을 활용하여 알려진 SW 취약점, 공격 패턴에 대한 정보를 활용할 수 있어야 한다. 이러한 역할은 정부로부터 인증 받은 공격팀, 민간에서 인증 받은 윤리적 해커(CEH: Certified Ethical Hackers), 사이버 개발 시험 및 분석 전문가, 사이버 경찰대, 상호운용성 기술자, 사이버 보안 서비스 제공자(CSSP), 네트워크 보안 전문가 등이 수행한다.

CVE	CWE-659 (C++)																		
CVE-2016-4018 (Latest version of National Vulnerability Database (NVD)) A Security Rating is the information vulnerability software receives as a result of inspection. Description: The Data Processing Agent (aka DP Agent) in SAP makes does not properly restrict access to service functionality, which allows remote attackers to bypass authentication, gain privileges, and conduct unspecified actions without the need for authentication via SAP Security Note 2207462. References: Advisories are provided for the convenience of the reader to help distinguish between vulnerabilities, but they do not intend to be exhaustive. • HACKERS: SAP's Critical Patch Program Shows How Open Source Can Be Used To Control Software Development State: Entry Ignored 2016-09-14 CVSSv2 Score: The entry creation date thus reflect when the CVE ID was proposed or reserved, and does not necessarily indicate when the vulnerability was discovered, stated with the affected products, publicly disclosed, or updated in CVSS. Assigned (CVE-2016-4018) Vendor (Language) Committers (Language) Impacted (Language) N/A This is an entry in the CPE/CSS, which distribution access for security products. OpenSource CVE Symbols and Metadata: Submit... You can also search by reference using the CPE database. See More Information: cve.mitre.org	CWE-659: Weaknesses in Software Written in C++ Subpages List View XML Zip Weaknesses in Software Written in C++ View All CVE Count Impact Date Status Draft View Data View Objective: This view [8] covers issues that are found in C++ programs that are not common to all languages. View Filter: <code>/Applicable_Families/{Language_Name}C++</code> View Metrics <table> <tr> <th>Total</th><th>CWE's in this view</th><th>Total CWE's</th></tr> <tr> <td>IDs</td><td>0</td><td>out of 1004</td></tr> <tr> <td>Vendors</td><td>0</td><td>out of 33</td></tr> <tr> <td>Categories</td><td>3</td><td>out of 244</td></tr> <tr> <td>Weaknesses</td><td>81</td><td>out of 719</td></tr> <tr> <td>Compound Elements</td><td>1</td><td>out of 8</td></tr> </table> Total 85(Category 3, Weakness 81, Compound Element 1)	Total	CWE's in this view	Total CWE's	IDs	0	out of 1004	Vendors	0	out of 33	Categories	3	out of 244	Weaknesses	81	out of 719	Compound Elements	1	out of 8
Total	CWE's in this view	Total CWE's																	
IDs	0	out of 1004																	
Vendors	0	out of 33																	
Categories	3	out of 244																	
Weaknesses	81	out of 719																	
Compound Elements	1	out of 8																	

〈그림 14〉 CVE와 CWE 예시

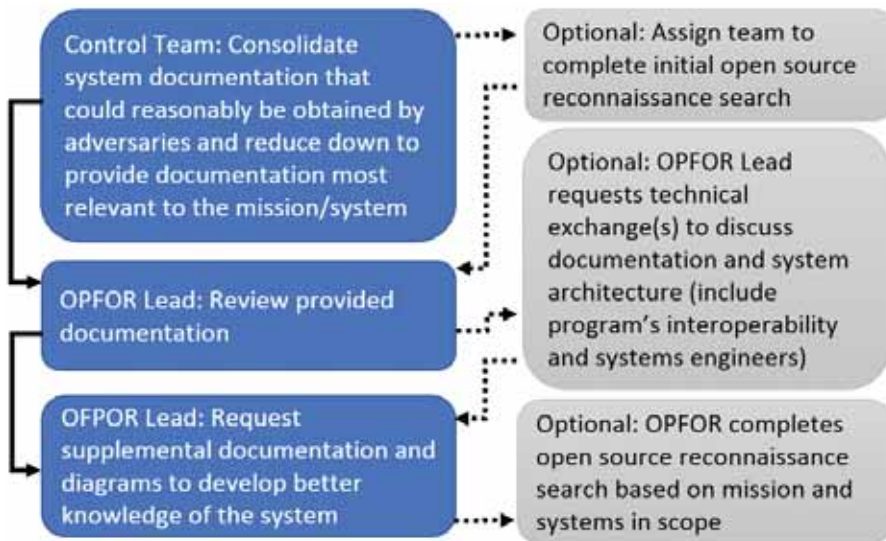
1.2 작전 시나리오

작전 시나리오는 CTT의 배경을 설명하는 역할을 한다. 1단계(연습 준비)에서부터 3단계(사후 분석)까지 작전 전반에 걸쳐 영향을 줄 수 있는 현실적인 조건과 상황을 제시한다. 주요 고려사항으로는 작전영역, 작전일정, 작전기간, 기상, 가정사항이다. 이 중에서 작전기간은 가능하면 하나의 단위임무(task)에 맞춰 너무 길지 않도록 구분한다. 작전기간이 너무 길면 사전에 식별하지 못한 사이버공격, 사이버 취약점이 발견될 수 있기 때문이다.

공격임무는 무기체계의 임무 수행을 방해하는 사이버공격팀의 역할이다. 가정사항에 따라 사이버 공격 임무 수행을 위한 TTP 범위를 지정하고 공격자의 수준을 맞춰 사이버 공격팀의 활동을 제한한다. 이를 위해서는 시스템 정찰 정보, 사이버 무기의 수준, 네트워크의 접속 권한, 미사일과 전자전과 같은 복합전 등이 고려될 필요가 있다.

1.3 시스템 정찰

1단계(연습 준비)에서는 시스템에 대한 정찰 활동을 수행한다. 시스템 정찰 활동과 주요 문서화 절차는 <그림 15>에 나타나 있다. 통제팀에서는 시스템 정보를 얻을 수 있는 문서들을 취합한다. 이때 접근할 수 있는 정보의 수준은 공격자 수준에서 충분히 확보할 수 내용들을 담고 있어야 한다. 공격팀에서는 제공된 문서들을 검토하고 필요한 추가 정보들을 요구해야 한다. 작전팀에서도 대상 시스템을 충분히 이해할 수 있는 정보들을 요구하고 공개출처정보(OSINT: Open Source Intelligence)를 활용하여 시스템이 본래의 임무를 수행하는 기능들을 잘 이해하여야 한다.



〈그림 15〉 1단계(연습 준비) - 시스템 정찰 절차

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

1.4 초기임무영향 방법론

초기임무영향 방법론은 위협 매트릭스를 문서화 한 것으로서, 모든 사이버 공격에 대하여 각각의 임무가 받는 영향성을 일관성 있게 평가하는 방법을 제시하는데 사용된다. 통제팀이 1단계(연습 준비)에서 개발하고, 작전팀이 2단계(연습 시행)에서 구체화하며, 다시 통제팀이 3단계(사후 분석)에서 완성 시킨다.

Impact	Mission Impact	Data Loss (MEF)	System Performance (MEF)	Delay (Operational Mission)
1	Fully Mission Capable	No data compromised	System Performance Not Impacted	Less than 5 Minutes
2	Partial to Fully Mission Capable	Public Access Level	System Performance Marginally Impacted	Greater than 5 Minutes and less than 30 Minutes
3	Partially Mission Capable	FOUO	Partial Loss of Functionality	Greater than 30 Minutes and less than 1 Hour
4	Non to Partially Mission Capable	FOUO/New Technology	Major Loss of Functionality	Greater than 1 Hour, less than 2.5 Hours
5	Non-Mission Capable	Classified	System Performance Severely Impacted/ Total Loss of Functionality	Greater than 2.5 Hours

〈그림 16〉 임무영향 방법론 표기 예시

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

1.5 발생 가능성 평가 방법론

발생 가능성 평가 방법론은 통제팀이 1단계(연습 준비)에서 개발하고 사이버공격팀이 2단계(연습 시행)에서 활용한다. 여기에서는 2차원의 평가요소가 사용된다. 하나는 공격 비용(attack cost)으로 공격을 수행하는데 투입되는 노력의 수준을 의미한다. 또 다른 하나는 공격 성공 가능성(attack success likelihood)으로서 해당 공격 기술의 활용 가능성을 의미한다. 알려져 있는 공격 기술들은 CAPEC(Common Attack Pattern Enumeration and Classification) 데이터베이스를 활용한다.

Attack Cost/ Level of Effort				Attack Success Likelihood		
				Rarely works	Sometimes works	Always works
				Low	Medium	High
				Occasionally works		Always works
Nearly anyone can build: Nascent – Limited threat	Low cost to develop	Exists today	Easy to develop	3 Example: Network DoS	5 Example: Flash implant delivered via website/email	
Criminal level organization can build: Moderate threat	Medium cost to develop	Many can develop				
Nation state organization can build: Advanced threat	High cost to develop	Few can develop	Hard to develop	1 Example: RF inject of malware into sensor or radio	3 Example: Supply chain implant in HW or firmware	

〈그림 17〉 발생가능성평가방법론 적용 예시

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

2. (2단계) 연습 시행

CTT 프로세스의 2단계(연습 시행)는 통상적으로 3-5일이 소요되며, 킥오프 미팅(1-1.5일), CTT 시행(1~3일), 그리고 데이터 수집과 검토(1-1.5일)로 구성된다.

2.1 킥 오프 미팅

CTT 시행을 위해 준비를 개시한다. CTT의 방법론과 시행 목표를 참여자에게 교육하는데, CTT 시작 2~4주 전에 미리 개최하여 작전 시나리오, 공격임무를 구체화하고, 분석 대상이 되는 시스템에 대한 환경 정보를 제공한다. 작전팀과 사이버공격팀이 본격적으로 구성되며 각각 분리된 장소에서 착수 준비를 진행한다. 작전팀은 임무영향방법론 활용법을 숙지하고 연습 계획 문서를 최신화하며 임무의 이해도를 향상시킨다. 공격팀은 발생빈도평가방법론 활용법을 숙지하고, 공격 프로세스를 이해하고 TTP를 포함하는 공격 방법을 구체적으로 논의하게 된다.



〈그림 18〉 CTT 팀 사이의 협업 관계

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

2.2 CTT 시행

CTT는 작전팀과 사이버공격팀 사이에서 의사소통을 통해 진행되는 고도의 상호작용 연습이다. 이 때문에 CTT 진행자와 각 팀의 리더 사이의 소통을 위해 긍정적이고 우호적인 환경을 조성하는 것이 매우 중요하다. CTT 시행을 관찰하고 기록하는 서기(note taker)가 핵심 논의 사항을 포착하도록 하는 것도 중요하다. 서기의 기록 자료는 3단계(사후 분석)에서 CTT의 의미있는 산출물을 만드는 데 가장 중요한 자료가 되기 때문이다. 따라서 서기는 CTT 시행 기간 동안 모든 정보를 정확하게 수집하기 위해 CTT 시행 중에 해당 팀에게 질문을 할 수 있고 필요하다면 진행을 일시 중지하도록 요청할 수도 있다.

2.3 데이터 수집과 분석

CTT에서 데이터 수집은 서기에 의해 이뤄진다. 서기는 시스템, 사이버공격팀의 정보 흐름을 파악하고, 사이버공격팀이 사용하는 TTP, 그리고 다른 구성원들이 상호작용에 사용하는 전반적인 사항들을 관찰하고 정보를 수집한다. 서기가 수집한 자료에는 기밀성을 갖는 것도 포함되며, 전자적 자료, 수기 자료 등 모든 형태가 대상이 된다. 이러한 자료들은

원시 데이터(raw data)로 불리며, 3단계(사후 분석)에서 가공되어 통합 처리된다.

데이터 분석은 CTT 시행 기간 동안 일일단위로 이뤄진다. 하루 동안 계획된 일정을 검토하여 공격이 얼마나 이뤄졌고, 얼마나 남았는지 등 작전팀과 사이버공격팀 사이의 진행 상황을 평가한다. CTT 마지막 날에는 3단계(사후 분석)을 준비하기 위한 미팅 시간을 갖는다.

3. (3단계) 사후 분석

CTT 시행이 완료되면 수집된 데이터와 이에 대한 검토 사항을 가지고 사후 분석을 실시한다. 3단계(사후 분석)은 30~90일이 소요되는데 CTT 프로세스 중에서 가장 많은 노력이 필요한 단계이다. 주요 활동으로는 데이터 종합, 초기 분석, 공격 평준화, 위험 매트릭스 완료, 최종 위험 분석이 있다.

3.1 데이터 종합

CTT 시행 결과 산출된 원시 데이터를 데이터 분석가가 검토하여 분석 표(analysis table)로 정리하는 과정이다. CTT 시행 중에 만들어진 사이버공격팀의 분석표가 통합된 자료이며 이 분석표는 CTT의 핵심 산출물이 된다. 통상적으로 데이터 분석가에 의한 데이터 종합 과정은 3주 정도가 소요된다. 이렇게 종합된 분석표는 이후 3번의 미팅을 진행하면서 초기 분석, 공격 평준화/위험 매트릭스, 최종 위험 분석 순으로 정형화되어 간다.

3.2 초기 분석

분석표의 첫 3개 열을 작성하는 과정이다. 각 열은 사이버 공격, 각 행은 해당 공격에 대한 정보를 의미한다. 각 열에 부여된 ID는 위험 매트릭스에서 제시된 사이버 공격(cyber-attack)을 의미한다.

이 과정에서 분석가들은 각 열의 사이버 공격을 검토하며 추가 또는 보완되어야 하는 정보를 식별하고, 관련성이 높은 사이버 공격들은 묶어서 그룹핑하는 작업을 하게 된다. 예를 들어 사이버 킬체인의 단계별로 묶거나, 공격 대상이 되는 표적 시스템 또는 작전 임무의 단계별로 그룹핑을 한다.

	OPFOR				Control Team/ OPFOR		Operational Team	
ID	Goal	Attack Method Attack Description	Assumptions	When in the Mission Timeline	Possible System Effect (IF)	Attack Result (THEN)	Mission Effect (IF)	Mission Impact (THEN)
M1A1V1								
M1A1V2								

〈그림 19〉 초기 분석 과정에서 사용되는 분석표의 양식

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

3.3 공격 평준화

초기 분석 이후, 분석표의 가운데 6개 열을 작성하는 과정이다. 초기 분석 과정을 거쳐서 만들어진 분석표를 재검토하고, 각 공격에 대한 임무의 효과, 그리고 임무 영향을 재평가한다. 그 결과에 따라 사이버 공격에 대한 임무의 영향과 결과값을 재조정 할 수 있다.

분석가들은 임무 영향을 작전 시나리오의 가정 상황에 따라 결정을 할 수 있는데, 예를 들어 항공모함의 항공기 발사 장치에 사이버 공격이 발생하는 상황에 대해서, 가정 상황이 전시인지 또는 평시인지에 따라 임무 영향은 다르게 평가할 수 있다.

Analysis Team					
Numerical Mission Impact and Consequence	Attack Cost / Level of Effort	Attack Success Likelihood	Numerical Likelihood	Analysis of numerical Likelihood factoring in access methods. Put new (or unchanged) likelihood value from N.	Final Risk Assessment coordinates

〈그림 20〉 공격 평준화 과정에서 사용되는 분석표의 양식

* 출처 : The Department of Defense Cyber Table Top Guidebook”, DoD, 2018.

3.4 최종 위험 분석

최종 위험 분석은 분석표의 마지막 3개 열을 작성하는 과정이다. 이 과정에서는 이제까지 만들어진 분석표와 위험 매트릭스를 최종 점검하게 된다. 여기에서 위험 매트릭스는 CTT 결과를 가시적으로 보여주는 역할을 하며 기술 검토 결과에 대한 요약이 된다.

Analysis Team and System Test			
Capabilities or Mitigations		Recommendations	Questions, RFIs, Further Analysis
In Place Today	Planned for the Future		

〈그림 21〉 최종 위험 분석 과정에서 사용되는 분석표의 양식

* 출처 : The Department of Defense Cyber Table Top Guidebook", DoD, 2018.

Capabilities or Mitigation 열은 각 공격의 능력과 해당 공격에 대한 대응 방법을 설명한다. Recommendation 열은 각 공격에 대한 권고 사항이 제시된다. 권고 사항은 시험 필요(test), 수용 또는 보류(accept or hold), 추가 분석 필요(further analysis)로 구분한다. 이 중에서 '시험'은 특정 공격 사례에 관련된 위험 수준을 결정하기 위해 시험이 필요함을 의미한다.

즉, 해당 무기체계에서는 '시험'으로 권고된 사이버 공격 유형을 시험하는 것이 필요하다는 의미이다. '수용 또는 보류'는 해당 공격 유형의 위험이 낮거나, 그것이 미치는 임무 영향도를 알 수 없거나, 대응이 불가능한 경우를 의미한다. '추가 분석 필요'는 추가 조사를 통해 최종 판단이 필요함을 의미한다.

LIKELIHOOD (Y)	5	Very Low	Low	Moderate	High	Very High
	4	Very Low	Low	Moderate	High	Very High
	3	Very Low	Low	Moderate	Moderate	High
	2	Very Low	Low	Low	Low	Moderate
	1	Very Low	Very Low	Very Low	Low	Low
		1	2	3	4	5
		IMPACT (X)				

〈그림 22〉 위험 매트릭스

* 출처 : NIST SP 800-30 Rev. 1

위험 매트릭스는 <그림 22>와 같이 NIST SP 800-30 Rev.1을 기반으로 작성한다. X축은 임무 영향도, Y축은 발생 빈도를 각각 수치적으로 나타낸다.

4. (4단계) 보고

CTT 프로세스의 마지막 단계인 4단계(보고)는 3단계(사후 분석) 결과에서 도출된 분석표를 가지고 이제까지 식별된 사이버 보안 위험, 그리고 권고 사항의 우선 순위를 결정한다. 모든 위험 관리는 비용 대비 효과성을 고려하므로 우선 순위 결정은 중요한 의사결정의 자료가 된다.

보고 단계는 그 대상과 내용에 따라 CTT 수행에 대한 전반적인 기술적 브리핑, 고위 지도부를 대상으로 CTT의 주요 사항을 보고하는 지휘부 보고로 구분된다.

제2절 무기체계 획득에 대한 CTT 적용

CTT는 전통적인 위계임은 아니다. 지휘부와 전투원이 사이버전 영역에 대한 이해를 임무의 관점에서 증진하도록 돕는 역할을 한다. 또한, 무기체계 시험평가 프로그램⁸⁰⁾에서 개발과 시험 자원을 잘 할당하도록 돕는 역할을 한다. 그러므로, CTT는 무기체계 획득 프로그램에 전체에 걸쳐 사용될 수 있다. 이를 통해 효율적이고 효과적인 사이버 보안 시험평가 전략을 계획할 수 있다.

1. DoD 무기체계 시험평가

미 국방부는 무기체계에 사이버 보안을 실현하기 위해 국방획득체계, 위험관리 프레임워크(RMF: Risk Management Framework), 사이버보안 시험평가체계를 통합하여 운영하고 있다⁸¹⁾.

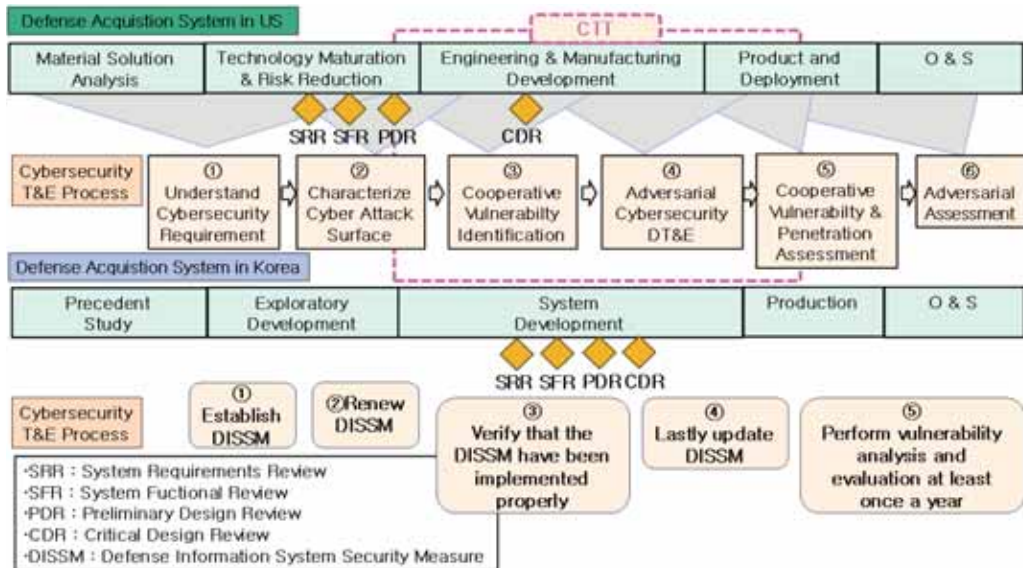
Cybersecurity T&E Process는 총 6단계로 수행된다. 1단계는 사이버보안 요구사항 이해로써, 가능한 모든 대상 시스템 관련 문서를 살펴서 사이버보안 요구사항을 이해하는 단계이다. 2단계는 사이버 공격표면 식별단계로써 공격자가 시스템을 악용할 수 있는

80) 여기에서 프로그램(program)은 프로젝트(project)의 집합을 의미한다.

81) Cybersecurity and the Risk Management Framework. Department of Defense.
<http://slideplayer.com/slide/4575411>

공격표면을 식별하는 단계이다.

3단계는 협업을 통한 취약점 식별단계로써 시험, 분석, 수정, 재시험 과정을 통해 시스템 개발 전반에 걸쳐 사이버보안 취약점을 식별하는 단계이다. 4단계는 적대적 사이버 보안 개발시험평가 단계로써 앞서 산출된 취약점 분석·평가 보고서, 보안평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템의 시험평가를 수행하는 단계이다. 5단계는 협업을 통한 취약점 평가 및 침투평가로써 취약점이 발생할 수 있는 환경을 구축하여 사이버위 게임과 같이 시험평가를 진행하고 대상 시스템에 적용된 사이버보안 정도를 파악하는 단계이다. 끝으로 6단계는 공격 위험도 평가로써 공인된 취약점 침투 테스트 팀이 앞 단계에서 도출된 사이버 위협에 대한 대응방안을 평가한다. 이러한 사이버 보안 시험절차는 <그림 23>과 같다.



〈그림 23〉 미국과 한국의 무기체계 사이버보안 시험평가 절차 비교

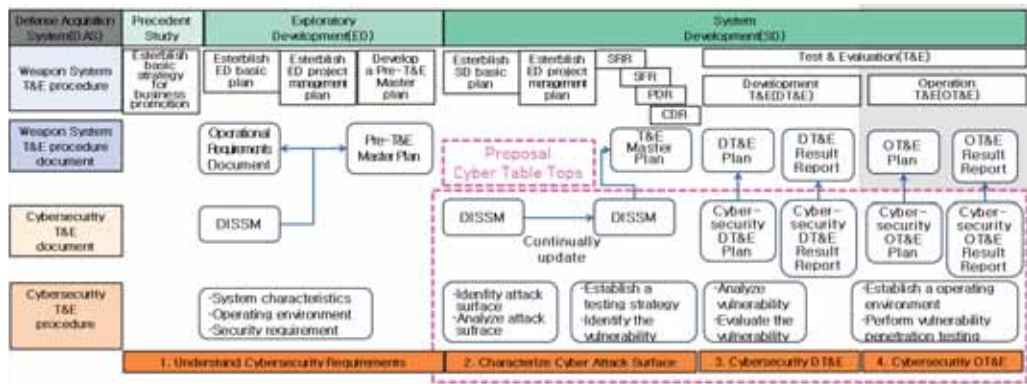
* 출처 : 홍해선 등 “사이버 테이블 탑을 활용한 무기체계 시험평가 방안 제안”, 한국정보통신학회 춘계학술대회, 2020.

2. 한국군의 무기체계 획득 절차에 CTT 적용

한국군의 무기체계 획득 환경에 CTT를 적용하기 위한 방안을 살펴본다. 이를 위해 국내 무기체계 국내 무기체계 시험평가 프로세스의 변화를 최소화하면서 무기체계 시험평가와 ‘국방정보시스템 보호대책서’의 간극을 메울 수 있는 사이버보안 시험평가체계가

필요하다.

먼저 사이버보안 시험평가체계를 <그림 24>와 4단계로 제안한다. 세부적인 사이버보안 시험평가 프로세스는 다음과 같다.



<그림 24> 한국군 무기체계 획득에 CTT 적용 방안

* 출처 : 홍해선 등 “사이버 테이블 탑을 활용한 무기체계 시험평가 방안 제안”, 한국정보통신학회 춘계학술대회, 2020.

(1단계) 사이버보안 요구사항 이해

가능한 모든 대상 시스템 관련 문서를 통해 무기체계 운영개념 이해와 사이버보안 요구사항을 이해하는 단계로 ‘국방정보시스템 보호대책서’를 작성하는 단계이다.

(2단계) 사이버 공격 취약점 식별

공격자가 시스템을 악용할 수 있는 공격표면을 식별하고, 보호전략을 수립하는 단계로서 ‘국방정보시스템 보호대책서’를 발전시키고, ‘시험평가기본계획서’에 사이버보안 항목이 구체적으로 반영시키는 단계이다.

(3단계) 사이버보안 개발시험평가

이 전 사이버보안 취약점 분석·평가 보고서, 보안평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템에 대한 사이버보안 시험평가를 수행하는 단계로서 평가결과는 무기체계 개발시험평가 결과에 반영한다.

(4단계) 사이버보안 취약점 운용시험 평가

취약점이 발생할 수 있는 환경을 임의로 구축하여 사이버위게임을 통해 시험평가를 진행하며, 이를 통해 대상 시스템에 적용된 사이버보안 정도를 파악하는 단계이다. 평가 결과는 무기체계 운용시험평가 결과에 반영한다.

또한, 실질적인 무기체계 사이버보안 능력검증을 위해 전력발전업무훈령 제12조 무기체계 시험평가지 사이버 테이블 탑을 적용할 필요가 있다. 이러한 사이버보안 검증과정은 무기체계 도입 후 운용 간 보완해야 하는 문제점을 사전에 식별, 개선하게 하고 보완 비용과 노력을 최소화하도록 가능하게 할 것이다. 현재 국내 무기체계는 체계개발 단계에서 일부 사이버취약점 평가를 위해 모의침투 시험(Penetration Test)을 수행하고 있으나, MBCRA 개념이 적용된 CTT 유형이 보다 적합할 것이다.

사이버 위게임 중 사이버 테이블 탑 유형인 CTT는 미국의 무기체계 획득 절차에 적용되고 있다는 것을 참고하여 한국군의 국방획득체계의 무기시험평가에 적용하는 방안을 살펴보았다. CTT를 적용한 사이버보안 시험평가 프로세스는 무기체계 개발단계에서 사이버보안 요구사항 파악을 통해 시험평가 수행을 준비하고, 사이버 취약점 식별과 취약점 완화대책을 실질적으로 수행하기 위해 임무기반 사이버위협 평가에 활용될 수 있다.

실질적 무기체계 운용환경과 유사한 환경에서 공격자 입장에서 취약점 침투 테스트를 수행하고 대상 시스템의 사이버 보안정보를 평가하여 무기체계 시험평가 결과에 반영할 필요가 있다. 이러한 실질적 취약점 식별 및 평가과정은 무기체계의 사이버보안 능력을 강화하는데 기여할 것이다.

V. 결론

사이버공간은 복합 전장으로 현대전의 형태를 변화시키고 있다. 전쟁의 양상이 달라지는 것이며 이에 따른 전쟁 연습을 위한 사이버전 프레임워크와 참조 모델에 대한 연구가 시급한 시기이다. 본 연구에서는 사이버 위게임의 다양한 자료를 조사하여 사이버 위게임 프레임워크, 참조 모델, 플랫폼, 주요 사례들을 살펴보았다.

사이버 위게임은 기존의 전쟁 연습과 연계하여 조직의 비즈니스 임무 및 프로세스에 대한 경영진/지휘부의 대응 능력, 그리고 실무진의 방어 기술 수준을 평가하는데 매우 유용한 기술이자 도구임을 확인하였다. 따라서 사이버 위게임을 기존 전쟁 연습과 연계하기 위한 노력과 시행을 지속 추진하는 것이 필요하다.

먼저 DoD CTT를 국방분야에 활용하기 위해 필요한 내용들을 살펴보았다. DoD CTT는 무기체계 획득 책임자에게 다영역에 접한 무기체계에 대한 사이버보안 개념을 제공함으로써 사이버공간을 전쟁의 영역 중 하나로 인식하는 데 도움을 준다.

그리고, 효과적인 사이버 보안 시험평가 전략을 계획할 수 있도록 CTT 적용을 제안한다. CTT는 전통적인 위게임은 아니지만 지휘부와 전투원이 사이버전 영역에 대한 이해를 임무의 관점에서 증진하도록 돕는 역할을 한다. 또한, 무기체계 시험평가 프로그램에서 개발과 시험 자원을 잘 할당하도록 돕는 역할을 한다. 그러므로, CTT는 무기체계 획득 프로그램에 전체에 걸쳐 사용될 수 있을 것이다.

사이버공간을 포함하는 다영역작전 수행능력이 미래 전쟁의 승패를 좌우할 것이다. 이 때문에 사이버공간을 포함하는 다영역에서 작전을 수행해야하는 첨단 무기체계 개발과 획득에 대한 CTT 활용은 국내 독자 기술의 무기체계 개발이 확대되는 현 시점에서 필요한 것이다. 규격 검사 수준의 SW 신뢰성 시험평가, C4I체계 중심의 보안성 평가 외에 무기체계에 대한 전반적인 위험관리 프레임워크를 적용하는 차원에서 사이버 위 게임을 활용하는 것을 제안한다. 다영역작전을 위한 다영역 시험평가와 같은 역할을 할 것이다.

〈참고 문헌〉

- 강동수, 무기체계 지능화 전쟁 패러다임 변화에 준비 필요, 국방일보, 2020.
- Dongsu Kang, "Bridging North and South Korea in Cyberspace", RINSA Forum, 2019.
- Junhyeong Choi, Dongsu Kang. (2019). Prioritizing Maintenance of Naval Command and Control System Using Feature Selection. 한국컴퓨터정보 학회논문지, 24(11), 219-228.
- HJ Kim, D.S. Kang, A Design of Risk-based Security Threat Assessment Process for Fighter-Aircraft Airworthiness Security Certification, KIPS Transactions on Software and Data Engineering, 2019.
- SI Son, DS Kang, A Test Case Generation Method for Data Distribution System of Submarine, KIPS Transactions on Software and Data Engineering, Vol.8, No.4 pp.137~144, 2019.
- Dongsu Kang, "A classification method of commonality and variability for mobile services," International Journal of software engineering and its applications(IJSEIA), Vol.10, No.3, pp.119-129, 2016.
- Colbert, E.J., A. Kott, and L.P. Knachel, The game-theoretic model and experimental investigation of cyber wargaming. The Journal of Defense Modeling and Simulation, 2018. (0): p. 1548512918795061.
- Colbert, E.J., D. Sullivan, and A. Kott, Cyber-Physical War Gaming. Journal of Information Warfare, 2017. 16(3): p. 119-133.
- Colbert, E.J., et al., Modeling Cyber Physical War Gaming. 2017, US Army Research Laboratory Aberdeen Proving Ground United States.
- Consulting, K., CYBERSECURITY GAMES: BUILDING TOMORROW'S WORKFORCE. 2016, Katzcy Consulting.
- Curry, J. and N. Drage, Developments in State Level Cyber Wargaming, in Proceedings of the 11th International Conference on Security of Information and Networks. 2018, ACM: Cardiff, United Kingdom. p. 1-6.
- Deloitte. 2014. "An introduction to cyber war games," CIO Journal, September 22, 2014. <http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/>

- Dobson, G.B., et al., R-EACTR: A Framework for Designing Realistic Cyber Warfare Exercises. 2017, CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States.
- DoD, The Department of Defense Cyber Table Top Guidebook. 2018.
- Domingo, A. and M. Parmar. Functional Analysis of Cyberspace Operations. in MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). 2018. IEEE.
- Fox, D.B., et al., Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic. 2018.
- Fox, D.B., et al., Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions. 2018.
- Fox, D.B., et al., Enterprise Threat Model Technical Report. 2018.
- Haggman, A., Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education. 2019, University of London.
- Kick, J., Cyber exercise playbook. 2014, MITRE CORP BEDFORD MA.
- Kyeong-Ho, K., et al., A Study on Control System Cyber Security Education & Training Method. Journal of the Korea Institute of Information Security & Cryptology, 2019. 29(3): p. 645-656.
- Matthew B. Caffrey Jr., "On Wargaming; How Wargames Have Shaped History and How They May Shape the Future," Naval War College Press, 2019.
- MITRE, ATT&CK Enterprise, MITRE, Editor. 2018.
- Nichols, J. Cyber Wargaming: Lessons Learned Influencing Security Stakeholders. in Blackhat. 2017.
- Perla, P.P., et al., Wargame-Creation Skills and the Wargame Construction Kit. 2004, Dec.
- U.S. DHS, Cyber Storm I Exercise Report, 2006.
- U.S. DHS, Cyber Storm II Exercise Report, 2008.
- U.S. DHS, Cyber Storm III Exercise Report, 2010.
- U.S. DHS, Cyber Storm IV Exercise Report, 2015.
- U.S. DHS, Cyber Storm V Exercise Report, 2016.
- U.S. DHS, Cyber Storm VI Exercise Report, 2018.
- 홍해선, 이민우, "사이버 테이블 탑을 활용한 무기체계 시험평가 방안 제안", 한국정보통신학회 춘계학술대회, 2020.
- CALIT(Cybersecurity & the Acquisition Lifecycle Integration Tool) Ver 3.1, DAU, 2018.

하드웨어 보안기술의 적용을 통한 국방사이버보안 연구

국방대학교 교수 이 수 진

- I. 연구개요
- II. 하드웨어 기반 사이버보안 기술
- III. PUF 기술
- IV. PUF 기반의 국방 사이버보안 강화 방안
- V. 결론

요 약

일반적으로 소프트웨어는 다양한 보안취약점을 내포하고 있으며, 운영체제 등의 기반 소프트웨어가 가지는 보안취약점에 의해 각종 사이버위협에 노출되기도 한다. 소프트웨어를 기반으로 하는 사이버보안 도구 역시도 해당 도구 자체의 보안취약점이 아닌 운영체제의 취약성이나 연계된 다른 소프트웨어의 보안취약성으로 인해 손쉽게 무력화되는 경우가 허다하다. 소프트웨어를 기반으로 구현된 대표적인 사이버보안 도구인 암호 역시도 예전에는 최선의 사이버보안 대책으로 각광받았지만, 현재는 사이버보안 도구로서의 위상을 서서히 상실하고 있다.

이러한 문제를 해결하기 위해 최근에는 하드웨어를 기반으로 사이버보안을 구현하려는 움직임이 활발하게 전개되고 있다. 하드웨어 기반의 사이버보안은 기본적으로는 소프트웨어로 구현된 사이버보안 도구들을 하드웨어로 대체하는 개념이기도 하지만, 하드웨어가 제공하는 고유한 특성을 기기 인증 및 암호 생성 등의 사이버보안에 활용하는 개념이기도 하다.

본 연구는 현재 국방영역에 광범위하게 적용되고 있는 소프트웨어 기반의 사이버보안

도구들이 잠재적으로 가질 수 있는 한계를 극복하면서, 하드웨어를 기반으로 보다 강력한 국방 사이버보안을 구현할 수 있는 방안을 도출하기 위해 진행되었다. 연구의 진행을 위해 우선적으로 하드웨어 기반 사이버보안의 개념과 적용 사례를 살펴보고, 최근 들어 하드웨어 기반 사이버보안 구현의 핵심 기술로 떠오르고 있는 PUF와 관련된 연구동향을 고찰하였다. 그리고 국방영역에서 PUF 기술을 기반으로 사이버보안을 강화할 수 있는 대상을 국방 사물인터넷과 드론봇 전투체계로 설정하고, 해당 체계에서 사이버보안을 강화할 수 있는 방안을 제시하였다.

국방 사물인터넷에 대해서는 PUF 기술을 기반으로 안전한 통신 채널을 구성하는 기반이 되는 비밀키 설립 기법을 제안하였고, 드론봇 전투체계와 관련해서는 기반 네트워크가 될 수 있는 4G LTE 및 5G 상용 정보통신 기술의 보안취약점을 해결하는데 초점을 두고 PUF 적용 방안을 제안하였다. 또한 드론봇 전투체계가 군집드론의 형태로 운영될 경우 안전하게 자율적인 통신망을 구성할 수 있도록 PUF 기술을 활용하는 방안도 제안하였다.

본 연구를 통해 제안된 기법들은 현재까지 국방에서 최선의 사이버보안 대책이라 여겨왔던 암호를 대체하면서 보다 경량화된 형태의 사이버보안 구현을 통해 해당 체계의 사이버보안을 충분히 강화할 수 있을 것으로 판단된다. 그러나 하드웨어를 기반으로 사이버보안을 구현하기 위해서는 정책적 차원에서의 검토가 선행되어야만 한다. 소프트웨어를 기반으로 하는 사이버보안 도구들은 CC 인증과 같은 공식적인 검증 절차를 통해 안전성과 성능이 검증된 이후 군에 도입되지만, 하드웨어를 기반으로 하는 사이버보안 도구에 대해서는 CC 인증뿐만 아니라 아직 적용할 수 있는 구체적인 지침이나 제도가 없는 상황이다.

미국을 비롯한 주요 국가들은 이미 소프트웨어 기반 사이버보안 구현의 한계점을 깊이 인식하고, 하드웨어를 기반으로 하는 사이버보안 구현을 집중적으로 연구하고 있다. 학계를 중심으로 다양한 응용 기법들이 제시되고 있으며, 산업계에서는 설계 단계에서부터 하드웨어를 기반으로 하는 사이버보안을 구현한 제품들을 출시하고 있다. 그리고 4차 산업혁명의 핵심 기술 중 하나인 사물인터넷은 하드웨어 기반의 사이버보안이 가장 필요한 분야로 인식되고 있다. 따라서 우리 군도 소프트웨어 기반의 사이버보안 구현만을 고집할 것이 아니라, 하드웨어를 기반으로 사이버보안을 효율적으로 구현할 수 있는 방안에 대해 연구를 시작해야만 한다. 그리고 하드웨어 기반 사이버보안 도구를 국방영역에 적용하기 위한 정책적 차원의 준비도 시작해야 할 것이다.

I. 연구개요

1. 연구배경 및 목적

일반적으로 소프트웨어는 사이버보안 구현과 하드웨어의 동작 성능 등에 영향을 미칠 수 있는 크고 작은 보안취약점을 내포하고 있으며, 그러한 보안취약점이 완벽하게 제거된 소프트웨어를 찾는 것은 거의 불가능하다. 또한 대부분 소프트웨어는 원활한 서비스 제공을 위한 동작상의 오류 제거에 주력하면서 개발이 진행되는 경향이 강하기 때문에, 사이버보안 기능이 기본적으로 탑재된 소프트웨어를 기대하는 것도 쉽지 않다. 또한, 개발 과정에서 취약점이 발견되고 제거되기보다는 배포되고 사용되는 과정에서 취약점이 발견되는 경우가 빈번하다.

사이버 위협이 날로 심각해지면서 그 필요성이 증대하고 있는 사이버보안 시스템도 유사한 문제점을 안고 있다. 현재 광범위하게 사용되는 상용 사이버보안 제품들은 대부분 소프트웨어를 기반으로 제작되었으며, 운영체제 등 다른 소프트웨어의 도움이 필수적이기 때문에 소프트웨어 취약성으로 인해 발생하는 문제를 완전하게 배제하는 것이 불가능하다. 특히 사이버보안의 핵심적인 수단으로 간주되며 국방을 비롯한 다양한 분야에서 인증이나 접근통제 등을 위해 널리 활용되고 있는 소프트웨어 기반의 암호화는 암호 프로토콜 자체의 취약성이 아니라 프로토콜을 구현한 소프트웨어 및 해당 소프트웨어가 운용되는 환경에 내재된 취약성으로 인해 다양한 위협에 노출되고 있다.

네트워크 사이버보안의 핵심이라 할 수 있는 침입차단시스템과 침입탐지시스템 역시도 소프트웨어로 구현된 도구이기 때문에 다양한 위협에 직면하고 있다. 침입차단시스템의 경우 정당한 트래픽으로 가장하여 유입되는 악성트래픽을 차단하기가 불가능하며, 침입탐지시스템은 탐지규칙 업데이트가 적절하게 이루어지지 않으면 새롭게 출현하는 사이버 공격을 탐지할 수 없다. 바이러스 백신도 침입탐지시스템과 동일한 문제점을 안고 있다. 바이러스 탐지 엔진의 지속적인 업데이트가 진행되지 않으면 하루가 다르게 발전하는 악성코드로부터 시스템을 보호할 능력을 상실하게 된다. 그리고 엔진 업데이트 과정에서 악성코드가 내포된 업데이트 파일이 배포될 경우에는 조직의 네트워크 및 시스템 전체가 위협에 처할 수 있다. 2016년 발생한 국방망 해킹사건이 바로 대표적인 사례에 해당한다고 볼 수 있다. 즉 소프트웨어 기반의 사이버보안 도구들은 운용환경에서 필수적으로 존재하는 운영체제의 취약성 또는 소프트웨어 제작 과정에서 내포되는 결함 등으로 인해 본래의 기능을 제대로 수행하지 못하게 되면서 보호해야 할 대상뿐만 아니라 조직 전체를

위험에 빠뜨릴 수도 있다.

이러한 소프트웨어 기반 사이버보안 도구가 가지는 문제점을 해결하기 위한 대안으로 최근 중요성이 부각되고 있는 접근방법이 바로 하드웨어 기반의 사이버보안 구현이다. 하드웨어 기반의 사이버보안 기술은 하드웨어 자체가 가지는 고유하면서 모방할 수 없는 특성을 이용하여 네트워크에 접속하는 기기를 인증하거나 접근을 통제하고, 중요 정보의 보호에 사용할 암호 코드를 생성하는 방식을 취한다.

소프트웨어 기반 사이버보안 기술이 한계에 직면하게 되면서 출현한 하드웨어 기반 사이버보안 기술은 다양한 형태로 구현 및 적용되고 있으며, 그 중 대표적인 형태가 바로 물리적 복제방지 기술을 의미하는 PUF (physical unclonable function, 이하 PUF)이다. PUF는 반도체 제조과정에서 발생하는 공정오차를 이용하여 특정 입력(challenge)에 대응하는 고유한 출력값(response)을 생성하는 시스템을 의미한다. 동일한 작업공정을 거치더라도 똑같은 공정오차를 가지는 반도체를 생산하는 것은 거의 불가능하다는 특성을 이용하여 구현되는 PUF는 작은 칩의 형태로 간단하게 구현할 수 있어 전력 소모율이 낮고, 생산단가도 저렴하다. 또한 별도의 메모리에 생성되는 출력값을 저장할 필요가 없기 때문에 PUF 칩을 내장한 기기는 복제 또는 유출이 불가능한 고유한 ID 값을 가질 수 있게 된다. 그리고 이러한 PUF의 특성을 활용하여 암호 코드 생성, 기기 인증 등을 안전하게 수행할 수 있도록 지원한다.

본 연구에서는 하드웨어 기반 사이버보안 기술의 대표적인 형태인 PUF를 활용하여 소프트웨어 기반 사이버보안 기술의 한계를 극복하고 국방 사이버보안을 강화할 수 있는 방안을 중점적으로 연구한다.

본 연구의 목표는 다음과 같이 요약된다.

- ① 소프트웨어 기반 사이버보안 기술의 한계를 극복하기 위해 최근 들어 활발하게 연구되고 있는 하드웨어 기반 사이버보안 기술의 개념을 살펴보고, 연구동향을 정리한다.
- ② 국방분야 및 민간분야에서의 하드웨어 기반 사이버보안 기술 적용사례들을 조사하여 분석하고, 그 결과를 바탕으로 우리 국방에서 하드웨어 기반 사이버보안 기술을 적용할 영역을 식별한다.
- ③ 하드웨어 기반 사이버보안 기술을 대표하는 PUF를 활용하여 국방분야에서 추진하고 있는 주요 사업 및 체계의 사이버보안을 강화할 수 있는 방안을 도출한다.

2. 연구범위 및 방법

본 연구는 하드웨어 기반 사이버보안 기술의 국방분야 적용방안 제시를 목표로 한다. 그러나 학술적 차원에서 하드웨어를 기반으로 사이버보안을 구현하기 위해 연구되는 접근 방법은 상당히 다양하여 모든 방법론에 대해 국방 적용방안을 다루는 것은 불가능하다. 따라서 본 연구에서는 하드웨어 기반 사이버보안 기술을 구현함에 있어 최근 그 활용도가 증대되고 있는 PUF만을 연구의 대상으로 설정하여 국방분야 적용방안을 모색한다.

그리고 국방분야 사이버보안 강화에 CC 인증의 개념이 부재한 하드웨어 기반의 사이버보안 기술을 적용하기 위해서는 반드시 법·제도적 측면에서의 개선이 선행되어야 하나, 본 연구에서 법·제도적 측면에서의 개선 소요는 다루지 않는다. 기술적 측면에 국한하여 PUF의 국방분야 적용방안을 모색하고, PUF의 적용을 통해 얻을 수 있는 사이버보안 강화 효과 검증에 중점을 두고 연구를 수행한다.

현재까지 국방분야에서는 하드웨어 기반 사이버보안 기술의 적용을 공식적으로 검토한 사례가 없으며, 대부분의 정책부서 근무자들도 개념 자체가 생소할 것으로 판단된다. 따라서 하드웨어 기반 사이버보안기술의 개념에 대한 이해를 돕기 위해 다양한 하드웨어 기반 사이버보안 기술에 대한 조사를 우선적으로 진행한다. 이어서 본 연구의 핵심 적용 대상인 PUF에 대해 기 발표된 논문과 산업계의 보고서 등을 통해 기술개발 동향을 조사한다.

PUF의 국방분야 적용과 관련해서는 현재 구축을 고려하거나 또는 기 구축되어 운용 중인 체계 및 서비스 중 PUF의 적용을 통해 사이버보안을 강화할 수 있는 최적의 대상을 선정하고, 구체적인 적용방안을 기술한다.

II. 하드웨어 기반 사이버보안 기술

디지털화된 시스템 및 서비스에 대한 의존도가 높아지고 각종 기기의 연결성이 획기적으로 증대됨에 따라 과거에 일반적으로 적용되었던 소프트웨어 기반의 사이버보안 기술은 점점 한계에 직면하고 있다. 그와 동시에 하드웨어 기반 사이버보안 기술에 대한 관심이 증대되고 있으며, 하드웨어로 인해 발생 가능한 취약점을 근본적으로 해결하기 위한 기술들이 지속적으로 개발되고 있다.

본 장에서는 소프트웨어를 기반으로 사이버보안 문제를 해결하고자 했던 과거의 접근 방법이 왜 한계에 부딪히게 되었는지를 우선적으로 살펴보고, 그에 대한 대안으로 중요성이

부각되고 있는 하드웨어 기반 사이버보안 기술의 개념과 장점을 간략하게 정리한다. 이어서 하드웨어 기반 사이버보안 기술은 최근 연구동향을 정리하고, 실질적인 적용사례의 분석을 통해 시사점을 도출한다.

1. 소프트웨어 기반 사이버보안 기술의 한계

새로운 응용프로그램과 그를 기반으로 하는 디지털 서비스가 활발하게 개발되고 있지만, 디지털 환경에서 유통되는 각종 정보에 대한 사이버보안과 서비스를 제공하는 시스템의 무결성 및 안전성이 보장되지 않을 경우에는 성공적인 서비스 제공 자체가 불가능해진다.

과거에는 디지털 기기에서의 인증을 수행하기 위한 목적으로 소프트웨어 기반 솔루션을 적용하려는 시도가 주를 이루었다. 그러나 불행하게도 소프트웨어에 기반하는 사이버보안 솔루션은 몇 가지 중요한 약점을 내포하고 있다. 우선 기본적으로 소프트웨어는 문자로 작성된 코드이기 때문에, 사이버 공격자가 읽고 분석하면서 자신의 의도에 맞게 수정하는 것이 가능하다. 어떤 디지털 기기가 공격자에 의해 수정된 소프트웨어로 재프로그래밍 되는 경우에는 그 기기에서 수행되는 인증 프로세스와 시스템 무결성이 무력화될 수 있다.

소프트웨어의 재프로그래밍에 의한 취약성 발생은 1930년대 앨런 튜링에 의해 제안되었고 현대 컴퓨팅 기기의 이론적 모델이 된 ‘튜링머신(Turing machine)’이 가지는 개방성과 적응성에서 비롯되었다고 볼 수 있다. 현대의 모든 컴퓨팅 장치는 프로그래밍 할 수 있는 스마트한 기계라는 튜링머신의 개념을 기반으로 만들어졌다. 그러나 사이버보안의 관점에서 튜링머신을 재프로그래밍되지 않도록 잠그는 것은 불가능하다고 알려져 있다. 그리고 컴퓨팅 장치에서 핵심 기능을 담당하는 CPU도 프로그램에 의해 동작하는 하나의 튜링머신이기 때문에, 악의적인 기능을 수행하는 악성코드가 CPU 재프로그래밍에 성공하기만 하면 사이버공격도 성공할 수 있다.

소프트웨어 기반 사이버보안 솔루션들이 가지는 또 다른 심각한 약점은 디지털 기기가 생산되어 유통되고 사용되는 전 과정에 걸쳐 안전하지 못한 방식으로 저장되는 비밀키가 노출될 수 있다는 점이다. 일반적으로 소프트웨어 기반 사이버보안 시스템에서 사이버 공격자는 중요한 동작이나 핵심 정보 보호를 위해 사용되는 비밀키를 다양한 방법으로 알아낼 수 있다. 암호 알고리즘에 적용된 비밀키를 추측함에 있어 가장 흔하게 사용되는 기법은 1998년 Paul Kocher에 의해 처음으로 소개된 전력분석공격(power analysis attack)이다.⁸²⁾ 처음 소개되었을 당시에는 암호 알고리즘이 동작하는 과정에서의 전력 소비 패턴을

82) P. Kocher, J. Jaffe, and B. Jun, “Introduction to Differential Power Analysis and Related

하나 또는 소수만 수집하여 분석하더라도 비밀키를 추출하는 것이 가능할 정도로 취약성이 심각하였다. 이후 전력분석공격에 대응하기 위한 기술들이 개발되면서 전력분석공격은 보다 고도화된 형태로 진화하게 되었고, 최근에는 원격에서 전력 소비 패턴을 관찰하여 핵심 정보를 추출하는 공격기법까지 등장하였다. 그러나 안타깝게도 현재까지 전력분석 공격에 완벽하게 대응할 수 있는 기술은 제시되지 못하고 있다.

마지막으로 소프트웨어 기반의 사이버보안 솔루션은 사이버공격자가 물리적으로 접근할 수 있는 구성 요소가 없는 경우에만 보호를 제공할 수 있다. 즉, 외부에서 물리적 수단을 이용해 디지털 기기에 접근할 수 있다면 소프트웨어 기반의 사이버보안 솔루션은 무용지물이 될 수 있다. 이러한 이유로 최근 들어서는 소프트웨어 기반 사이버보안 솔루션이 기기 인증, 시스템 무결성 보장 등을 위한 대안으로 고려되는 경향이 점점 감소하고 있다.

2. 하드웨어 기반 사이버보안 기술의 개념 및 필요성

하드웨어 기반 사이버보안의 핵심은 소프트웨어 기반의 사이버보안 도구를 해당 기능을 수행하는 전용 하드웨어로 대체하거나 또는 하드웨어가 제공하는 고유의 특성을 활용하여 각종 조작이나 오동작 유발 행위로부터 보호함으로써 보다 강력한 사이버보안을 구현하는 것이다.

전술한 바와 같이 소프트웨어는 설계 및 구현 과정에서 결함이나 취약성이 포함될 가능성이 크고, 운용환경에서 동작하는 과정에서도 공격자에 의해 수정되거나 변조되어 악의적 행위를 수행할 수 있다. 특히 운영체제 자체에 보안취약점이 존재한다면, 어떠한 소프트웨어도 보호받을 수 없으며, 사이버보안 기능을 수행하는 소프트웨어 역시도 운영체제의 취약성으로 인해 본래의 기능을 수행할 수 없게 된다. 그러나 하드웨어를 기반으로 구현된 사이버보안은 수정이나 변조가 용이하지 않으며, 신뢰할 수 있는 컴퓨팅 환경을 시스템의 가장 낮은 계층에서 구축할 수 있도록 지원하기 때문에 훨씬 견고한 사이버보안의 구현이 가능해진다.

사이버보안의 구현은 설계 단계에서부터 고려되어야 하며, 가장 기초적인 계층에서부터 사이버보안의 구현이 시작되어야 한다. 시스템을 구성하는 요소들의 계층구조에서 소프트웨어는 가장 상층부에 속한다. 따라서 하위 계층에서 안전성이 보장되어야만 소프트웨어가 안전하게 동작할 수 있다. 이러한 이유로 하드웨어 기반 사이버보안의 구현을 통해 '신뢰의

Attacks," Cryptography Research, 1998.; P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Advances in Cryptology - CRYPTO '99, 1999.

기반(Root of Trust)'을 시스템 스택의 최하위 계층(칩 수준에서의 사이버보안 구현)으로 옮겨갈수록 시스템의 안전성은 더욱 높아질 수 있다.

이렇듯 하드웨어 기반 사이버보안 기술은 소프트웨어 기반 사이버보안 기술에 비해 많은 장점을 제공하지만, 국방분야에서 사이버보안을 강화하기 위한 연구들은 대부분 소프트웨어를 기반으로 하는 접근방법들을 대안으로 제시하였다. 최근 들어 하드웨어 기반 사이버보안 기술을 대표하는 형태인 PUF 기술을 일부 체계에 적용하여 기기에 대한 인증을 강화하고 암호 코드를 생성하여 활용하는 방안 등이 제시되기 시작했지만, 국방분야에 광범위하게 적용되고 있는 소프트웨어 기반의 사이버보안 기술이 가지는 한계점을 극복하기 위해서는 하드웨어 기반 사이버보안 기술에 대한 보다 폭넓은 연구가 반드시 필요하다.

3. 연구 동향

최근 10년 동안 사이버보안 대책을 제시한 주요 연구들을 살펴보면 하드웨어를 기반으로 하는 사이버보안 구현이 주 관심사로 부각되는 분야는 스마트폰이나 스마트 홈 구축에 사용되는 각종 스마트 기기 및 사물인터넷 기기 등을 포함하는 모바일 시스템, 특정한 기능을 수행하기 위해 다른 장치에 내장되는 디지털 기기 등을 포함하는 임베디드 시스템, 메모리 반도체, 그리고 집적회로(IC) 설계 분야 등이다. 본 절에서는 이러한 분야들에서 사이버보안 문제를 해결하기 위해 학술적 차원에서 논의된 선행 연구의 결과를 간략하게 정리한다.

가. 모바일 시스템

최근 들어 모바일 기기 또는 스마트 기기의 사용이 급속도로 확산됨에 따라 그러한 환경을 겨냥하는 사이버공격도 기하급수적으로 증가하고 있다. 그러나 모바일 환경에서 사용되는 기기는 많은 취약점을 안고 있어 각종 사이버공격에 손쉽게 노출될 수 있는 반면, 사이버보안을 구현하는 것은 용이하지 않다는 문제점을 안고 있다. 이러한 문제를 해결하기 위해 신뢰할 수 있는 하드웨어 플랫폼을 구현하여 기기에 장착하고 사이버보안을 제공하려는 시도가 활발하게 진행되고 있다.

Z. Shen 등은 신뢰할 수 있는 컴퓨팅 플랫폼을 모바일 기기에 장착하여 인증 및 자격 증명 관리를 수행함으로써 사이버보안을 강화하는 기법을 제안하였다.⁸³⁾ A. P. Fournaris

83) Z. Shen and X. Wu, "An Improved Security Method for Mobile Agent System by Using Trusted Computing Platform," International Conference on Intelligent Computation Technology and

역시 모바일 기기에 신뢰성을 보장할 수 있는 하드웨어 장치를 부착하여 유연한 사이버 보안을 구현하는 방법을 제시하였다.⁸⁴⁾

H. Ju 등은 모바일 기기에 장착하면 입출력 인터페이스를 통해 사이버보안 기능을 제공할 수 있는 보안 칩 구현 방안을 제시하였다.⁸⁵⁾ A. Maruaisap 등은 차량에서 광범위하게 적용되고 있는 CAN(Controlled Area Network)의 사이버보안을 강화하기 위한 방안으로 하드웨어 기반의 암호키 생성을 제안하였다.⁸⁶⁾ J. Milosevic 등은 모바일 기기를 설계하는 과정에서 마주할 수 있는 도전과제들을 제시하면서 각종 물리적 공격을 완화하기 위해 하드웨어 설계 과정에서 구현할 수 있는 대책들을 제안하였다.⁸⁷⁾

사물인터넷에 연결되는 각종 기기들은 대부분 네트워크 연결 능력만을 강조하면서 개발되는 경향이 강해 사이버보안 측면에서는 상당히 취약할 수밖에 없다. 특히 스마트 홈 구현을 위해 활발하게 사용되고 있는 소형 센서 장치들은 사이버보안 기능을 탑재하지 않은 경우가 대부분이라 외부 사용자가 통제권을 확보할 수도 있고, 센서를 통해 수집되는 각종 정보들이 외부로 유출될 수도 있어 개인정보보호 차원에서 큰 문제점으로 지적되고 있다.

S. Ray 등은 모바일 시스템 및 사물인터넷 기기의 보안취약점을 설계 관점에서 검토하였다. 기기에 장착되는 대부분의 SoC(System-on-Chip)는 자동화된 도구를 사용하여 설계되고 있어 기능과 사이버보안 사이의 균형을 유지하려는 경향이 강해지기 때문에 보안취약점이 발생한다고 지적하였다.⁸⁸⁾ A. Syed 등은 디지털 신호 처리 전용 사물인터넷 기기에서 처리되는 각종 정보를 수집하기 위해 하드웨어 트로이목마 형태로 삽입될 수 있는 스파이 장치를 Xilinx FPGA를 활용하여 하드웨어 기반으로 탐지할 수 있는 방안을 제시하였다.⁸⁹⁾

사물인터넷 기기의 보안을 강화하기 위해 암호를 적용하여 인증을 실시하고 수집 및 전송되는 각종 정보를 암호화하는 방안들도 지속적으로 연구되었다. 그러나 대부분의 연구들은 소프트웨어로 암호 알고리즘을 구현하여 사물인터넷 기기에 탑재하고, 인증과

Automation, 2010.

84) A. P. Fournaris, "Toward Flexible Security and Trust Hardware Structures for Mobile-Portable Systems," IEEE Latin American Transactions, Vol. 10, No. 3, 2012

85) H. Ju, Y. Kim, Y. Jeon and J. Kim, "Implementation of a Hardware Security Chip for Mobile Devices," IEEE Transactions on Consumer Electronics, Vol. 61, No. 4, 2015.

86) A. Maruaisap and P. Kumhom, "A Hardware-Based Security Scheme for In-Vehicle CAN," International Computer Science and Engineering Conference (ICSEC), 2016.

87) J. Milosevic, A. Ferrante and F. Regazzoni, "Security Challenges for Hardware Designers of Mobile Systems," Mobile Systems Technologies Workshop, 2015.

88) S. Ray and J. Bhadra, "Security Challenges in Mobile and IoT Systems," 29th IEEE International System-on-Chip Conference (SOCC), 2016.

89) A. Syed and M. Lourde R., "Hardware Security Threats to DSP Applications in an IoT network," IEEE International Symposium on Nanoelectronic and Information Systems, 2016.

암호화 및 복호화에 사용되는 키는 기기의 비휘발성 메모리에 저장하는 방식을 채택함으로써 인해 보안대책 자체가 무력화되고 암호키가 노출될 수 있다는 문제점을 안고 있다. 이러한 문제를 해결하기 위해서 M. A. Bahnasawi 등은 각종 암호 알고리즘을 하드웨어 칩으로 구현하여 성능 비교 실험을 실시한 후, AES 암호 알고리즘이 사물인터넷 환경에 가장 적합한 알고리즘이 될 수 있다고 주장하였다.⁹⁰⁾

나. 임베디드 시스템

A. Puraghily 등은 임베디드시스템의 전력과 처리능력 제한 때문에 소프트웨어 기반의 보안 메커니즘을 적용하는 것은 효율성이 떨어진다고 주장하였다. 그리고 임베디드시스템에 설치된 운영체제와 각종 응용프로그램의 비정상적인 동작을 감지하기 위한 하드웨어 기반의 모니터링 기법을 제안하였다.⁹¹⁾

L. Fiorin 등은 임베디드시스템의 운영체제로 주로 사용되고 있는 리눅스에 적용 가능한 FPGA 기반의 하드웨어 보안 플랫폼을 제안하였다.⁹²⁾ S. Wang 등은 임베디드시스템에 저장된 프로그램을 안전하게 보호하기 위해 하드웨어 기반의 모니터링 기법을 제안하였다.⁹³⁾ S. Lukacs 등은 알려진 모든 커널 루트킷 공격을 탐지함으로써 휴대용 시스템과 임베디드 장치를 보호할 수 있는 하드웨어 기반의 강제 보안 메커니즘을 제시하였다.⁹⁴⁾

하드웨어 기반의 사이버보안 기술이 가장 활발하게 연구되고 있는 분야는 부채널 공격(side channel attack)에 대한 대응기법을 연구하는 분야라고 할 수 있다. 기기 내의 특정 장치가 동작하면서 발생하는 누수 정보를 분석하여 암호키 혹은 중요 정보를 획득하는 공격방법을 의미하는 부채널 공격은 하드웨어가 동작하는 과정에서 일정한 형태의

90) M. A. Bahnasawi, Kh. Ibrahim, A. Mohamed, M. Kh. Mohamed, A. Moustafa, K. Abdelmonem, Y. Ismail and H. Mostafa, "ASIC-Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications," 28th International Conference on Microelectronics (ICM), 2016.

91) A. Pouraghily, T. Wolf and R. Tessier, "Hardware Support for Embedded Operating System Security," IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2017

92) L. Fiorin, A. Ferrante, K. Padarnitsas and F. Regazzoni, "Security Enhanced Linux on Embedded Systems: a Hardware-accelerated Implementation," 17th Asia and South Pacific Design Automation Conference, 2012.

93) X. Wang, Q. Shen, P. Du, R. Zhang, W. Wang, L. Li, B. Xu and H. Ji, "Hardware-Assisted Monitoring for Code Security in Embedded System," IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing, 2015

94) S. Lukacs, A. V. Lutas, D. H. Lutas and Gh. Sebestyen, "Hardware Virtualization Based Security Solution for Embedded Systems," IEEE International Conference on Automation, Quality and Testing, Robotics, 2014.

패턴이 관찰된다는 점을 이용하는 공격기법이다. 그리고 일정한 패턴을 관찰하기 위해 가장 광범위하게 사용되는 방법이 전력분석공격이며, 그 외에도 고의로 오류를 주입하여 기기에서 발생하는 각종 신호를 수집하여 분석하기도 한다. 암호화 측면에서의 부채널 공격은 암호 알고리즘이 작동하는 과정을 통해 관찰할 수 있는 소요 시간, 소비 전력, 방출하는 전자기파, 심지어는 소리를 통해서 암호키를 추출하는 공격이다. 이러한 부채널 공격은 소프트웨어를 기반으로 하는 사이버보안 기술로는 방어가 거의 불가능하여 대부분 추가적인 하드웨어의 장착을 통해 동작과정에서 발생하는 정보에 임의의 값을 추가하거나 시간을 불규칙하게 만들고 전력 소비를 일정한 패턴을 가지도록 조정하는 방법 등이 사용되고 있다. 최근에서 반도체 칩에서 발생 가능한 오작동으로부터 신속한 복구가 가능하도록 설계 단계에서부터 하드웨어적인 보안대책을 추가하는 추세이다.

다. 메모리 반도체

비휘발성 메모리(Non-volatile memorie)는 저장된 데이터가 계속 유지된다는 기본 특성 때문에 휘발성 메모리보다 더 공격하기 쉬운 대상이다. 따라서 비휘발성 메모리의 보안을 강화하기 위한 대책들이 상당히 활발하게 진행되었다.

S. Kan 등은 하드웨어 트로이목마가 비휘발성 메모리에 저장된 데이터의 위치를 예측하기 어렵게 만듦으로써 SRAM의 보안성을 강화하기 위해 메모리의 데이터 위치를 재매핑하는 방법을 제안하였다. 그리고 위치 재매핑 시 발생할 수 있는 오류 및 성능저하 문제를 최소화하는 대책도 동시에 제안하였다.⁹⁵⁾

Wiersema 등은 재구성이 가능한 시스템에서 메모리 액세스를 확보하기 위해 액세스 모니터와 교정 운반 하드웨어(공식 런타임 검증 기법)의 조합을 제안하였다.⁹⁶⁾ 메모리 시스템의 보안을 강화하기 위해, Neagu와 Sebestyen 등은 데이터 충돌 기술과 정보 엔트로피 모델을 채택하였다.⁹⁷⁾

비휘발성 메모리와 관련해서는 CPU에 인접해 있는 캐시에 비밀키나 중요한 정보가 계속 저장된다는 점을 악용하여 공유 캐시에 대한 불법적인 접근을 통해 정보를 탈취하는

95) S. Kan, M. Ottavi and J. Dworak, "Enhancing Embedded SRAM Security and Error Tolerance with Hardware CRC and Obfuscation," IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), 2015.

96) T. Wiersema, S. Drzevitzky and M. Platzner, "Memory Security in Reconfigurable Computers: Combining Formal Verification with Monitoring," International Conference on Field-Programmable Technology, 2014.

97) M. Neagu and Gh. Sebestyen, "Increasing Memory Security through Data Scrambling and Information Entropy Models," 15th IEEE International Symposium on Computational Intelligence and Informatics, 2014.

공격과 캐시 접근 시간이나 접근 패턴 등을 분석하여 비밀키를 유추하는 공격 등에 대비하기 위해 다양한 하드웨어 기반의 대응기법들이 제시되었다.

라. 집적회로

집적회로(IC)는 하드웨어 자체이기 때문에 집적회로의 사이버보안을 다루는 문제는 하드웨어를 기반으로 사이버보안을 강화하는 문제와 직결된다. 집적회로에 대한 공격은 주로 위조를 통한 모조품 생산, 역공학을 통해 집적회로에 적용된 핵심기술 유출 또는 비밀키 추출 등이 주를 이루고 있으며, 그러한 공격에 대응하기 위한 대책은 주로 집적회로의 설계 변경을 통한 대응에 초점을 맞추고 있다.

G. Gayathri 등은 집적회로의 위조, 역공학 공격 및 핵심기술 유출 등에 대응하기 위해 난독화를 적용하여 집적회로의 보안을 강화하는 방법을 제안하였다.⁹⁸⁾ 집적회로 내에 여분의 비밀키를 추가로 내장하고 은폐시킨 후, 은폐된 비밀키를 이용하여 각종 정보를 암호화시킨다. K. Shamsi 등은 CMOS 이외의 새로운 장치가 집적회로에 사용되는 경우 새로운 공격이 가능해진다는 문제를 지적하고, 새로운 장치를 집적회로에 적용할 경우 설계과정에서 고려해야 할 사항을 제시하였다.⁹⁹⁾

J. Dofe 등은 3차원 구조를 가지는 집적회로를 겨냥하는 보안위협을 식별하고, 역공학을 이용하는 공격을 더욱 어렵게 만들기 위해 3차원 구조를 가지는 network-on-chip에서 난독화를 구현하는 방법을 제시하였다.¹⁰⁰⁾ 그리고 P. Gu 등도 3차원 집적회로에서 사이버보안 대책을 구현하는데 적용 가능한 다양한 설계기법을 제시하였다.¹⁰¹⁾

대부분의 집적회로는 설계 과정 또는 완성된 이후에 올바르게 동작하는지를 확인하기 위한 목적으로 시험기능(test point)을 포함하고 있다. E. Moghaddam 등은 그러한 시험기능을 활용하여 역공학 공격이나 집적회로 복제 및 중요 정보 탈취 등에 대응하기 위한 하드웨어 차원의 사이버보안 강화 방안을 제시하였다.¹⁰²⁾ D. Fujimoto 등은 상용 디지털

98) G. Gayathri, T. Thangam, M and Kasthuri, "An Efficient Logic Obfuscating Strategy for Hardware Security Using SIC Generator," International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.

99) K. Shamsi, W. Wen and Y. Jin, "Hardware Security Challenges Beyond CMOS: Attacks and Remedies," IEEE Computer Society Annual Symposium on VLSI, 2016.

100) J. Dofe, Q. Yu, H. Wang and E. Salman, "Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs," International Great Lakes Symposium on VLSI (GLSVLSI), 2016.

101) P. Gu, Sh. Li, D. Stow, R. Barnes, L. Liu, Y. Xie and E. Kursun, "Leveraging 3D Technologies for Hardware Security: Opportunities and Challenges," International Great Lakes Symposium on VLSI (GLSVLSI), 2016.

102) E. Moghaddam, N. Mukherjee, J. Rajski, J. Tyszer, J. Zawada, "On Test Points Enhancing Hardware Security," IEEE 25th Asian Test Symposium, 2016.

기기에서 부채널공격에 대응하기 위해 칩상에서 발생하는 전력 노이즈를 활용하는 방법을 제시하였다.¹⁰³⁾

4. 적용사례

본 절에서는 하드웨어를 기반으로 사이버보안의 구현을 시도했던 대표적인 사례들을 소개한다.

가. Trusted Platform Module(TPM)

TPM은 칩 외부에서는 접근할 수 없는 기기 내부의 안전한 메모리에 비밀키를 저장한 후, 암호화 연산을 장치 내부에서만 수행하도록 설계된 하드웨어 칩을 의미한다. TPM 내부에서 암호화된 데이터는 TPM 내부에서만 복호화가 가능하며, 다양한 정보를 수집하여 유효성을 비교한 후 시스템 사용 여부를 통제하기 때문에 정보 유출 방지뿐만 아니라 시스템의 불법적인 사용까지도 차단할 수 있다는 장점을 가지기 때문에 다양한 분야에서 활발하게 적용되고 있다.

인피니온은 2011년부터 구글의 크롬 기반 운영체제를 실행하는 장치의 사이버보안 강화를 위한 하드웨어 장치인 TPM을 생산하고 있다. 인피니온 TPM은 주로 인터넷에 접속하여 웹 기반 애플리케이션을 사용하기 위해 컴퓨터 장치를 사용하는 사람들에게 빠르고 간단하며 안전한 사용환경을 제공하기 위해 고안된 구글 크롬북 보안 아키텍처의 핵심 요소이다. TPM의 설계에 적용된 핵심 개념은 ‘심층 방어(depth in defense)’라고 불리며, 이를 통해 악성코드에 대해 다양한 수준에서의 보호 기능을 제공한다.

인피니온은 새롭게 개발되는 응용프로그램을 광범위하게 지원할 목적으로 보다 다양한 기능과 인터페이스를 추가하면서 TPM의 구조를 개선하고 있다. 사이버보안 측면의 업그레이드가 가능한 포괄적인 소프트웨어 스택을 TPM에 포함시킴으로써 단순히 크롬 사용자의 인터넷 사용환경 보호를 넘어서서 IT 산업뿐만 아니라 임베디드 시스템, 스마트폰, 통신 장비, 산업 자동화 시스템 또는 자동차에서도 사이버보안 관련 기능을 수행할 수 있도록 진화하고 있다.

103) D. Fujimoto, M. Nagata, Sh. Bhasin, J. Danger, “A Novel Methodology for Testing Hardware Security and Trust Exploiting OnChip Power Noise Measurement,” The 20th Asia and South Pacific Design Automation Conference, 2015.

나. 자동차의 사이버보안 강화를 위한 HSM(Hardware Security Module)

자동차 역시 하드웨어 기반의 사이버보안 기술 적용이 급증하고 있는 응용 분야로서, 자동차에서 운용되고 있는 특정 응용프로그램에서 요구하는 보안 수준에 맞춰 설계된 하드웨어 기반의 사이버보안 기능이 이미 자동차 내부에 광범위하게 적용되어 있다. 예를 들어, AURIX 제품군의 마이크로컨트롤러는 SE (Security Hardware Extensions) 또는 HSM(Hardware Security Module) 등과 같은 특수 기능 블록을 포함하고 있다. 컨트롤러에 내장된 HSM은 메시지에 전자서명을 포함시키거나 완전히 암호화시키는 등의 방법을 통해 다른 마이크로컨트롤러들과 안전한 통신을 수행한다. 또한, 바이러스 및 트로이목마 등에서 비롯되는 공격을 방지하고 자동차 내부 장치들에 대한 무단 접근을 차단하기 위해 마이크로컨트롤러를 안전하게 부팅시키는 데에도 사용할 수 있다.

자동차가 다른 차량이나 인프라와 통신을 수행하는 것이 가능해지면서 점점 더 연결성을 가지는 컴퓨팅 장치로 전환되고 있다는 사실을 고려하면, TPM은 자동차에서 사용하는 소프트웨어의 업데이트 중 해커, 사이버 공격자 또는 각종 악성 프로그램으로부터 자동차의 통신 인터페이스를 보호함에 있어 필수 불가결한 존재가 될 것임은 분명하다. 그리고 자동차 내부에서 사용되는 각종 장치 및 상호 연결되는 구성 요소들을 조작, 공격, 오작동 유발 행위 등으로부터 보호하기 위한 강력한 안전 및 보안기술이 종합적으로 적용되어야만 사물인터넷과 같은 새로운 연결 기술의 구현이 가능해질 것이다. 최고의 보안 수준 구현은 보안성이 강화된 하드웨어를 필요로 하며 소프트웨어 기반의 사이버보안 기술만으로는 불가능하기 때문에, 보안성이 강화된 하드웨어는 필수적인 요소이다.

다. 인텔사의 vPro Platform¹⁰⁴⁾

vPro는 기업에서 사용되는 PC를 각종 사이버 위협으로부터 보호하기 위한 목적으로 강화된 보안기능을 탑재하여 특별히 제작한 하드웨어 기반의 플랫폼으로서, 하나의 플랫폼을 통해 성능 및 사이버보안 관리가 모두 가능하다.

운영체제 수준에서 사이버보안을 구현하기보다는 운영체제 이하 계층에서 사이버보안을 구현하는 접근방법을 채택하였기 때문에, 하드웨어, 펌웨어 및 소프트웨어 전반에 대해 강력한 보호를 제공할 수 있다. 그리고 관리 측면의 효율성도 충분히 고려하였기 때문에 IT 관리자가 원격 접속을 통해 보안 패치를 설치하거나 공격을 당한 PC를 복구하는 것도 가능하다. 실행 중인 응용프로그램을 보호하고 메모리에 저장되는 데이터는 안전하게 저장 및 관리되도록 지원하며, 원격에서 CPU 모니터링을 통해 사이버공격 징후를 탐지하는

104) <https://www.intel.com>

고급 위협탐지기능도 탑재하고 있다.

또한, 인텔사는 2020년 2월 개최된 RSA 컨퍼런스를 통해 강력한 메모리 암호화 지원, 칩 수준인 FPGA에서의 사이버보안 기능 구현 등을 골자로 하는 새로운 하드웨어 기반의 사이버보안 기술을 발표한 바 있다.¹⁰⁵⁾

라. 애플사의 Secure Enclave¹⁰⁶⁾

애플사 역시 하드웨어 수준에서 사이버보안의 기반이 마련되어야 소프트웨어도 안전하게 사용할 수 있다는 확신을 가지고, 애플 기기에 사이버보안 기능이 내장된 실리콘 칩과 시스템에 대한 사이버보안을 제공하기 위한 CPU를 탑재하였다.

Secure Enclave라고 불리는 사이버보안을 전담하는 보조 프로세서는 맥 OS의 안전한 시동, 안전한 데이터 암호화 및 생체 인증 등의 기능을 주로 수행한다. 운영체제의 안전한 시동을 통해 소프트웨어의 최하위 계층에서 조작행위가 수행되는 것을 방지하고, 신뢰할 수 있는 소프트웨어만 로드되도록 한다. 그리고 iOS 및 iPadOS 기반 기기에서는 칩 제조 단계에서 Boot ROM이라 불리는 변경이 불가능한 코드를 이용하여 사이버보안의 기반을 구축하였다. 사이버보안 기능을 전담하는 T2 칩이 장착된 맥 컴퓨터에서는 T2 칩 자체가 신뢰할 수 있는 사이버보안의 기반을 제공한다.

마. ARM사의 TrustZone¹⁰⁷⁾

ARM의 TrustZone 프로세서는 프로세서가 작업을 처리하는 영역을 일반영역과 보안 영역으로 구분하고, 중요한 작업은 보안영역에서 처리하는 Trusted Execution Environment (TEE) 기술을 적용하여 설계된 프로세서로서, 삼성전자의 KNOX 등을 포함하여 다양한 모바일 기기 및 임베디드 시스템에서 활용되고 있다.

바. SSITH(System Security Integration Through Hardware and Firmware)

SSITH 프로그램은 하드웨어 및 펌웨어를 통해 시스템 보안을 통합함으로써 일반적인 악의적 행위로부터 디지털 시스템을 안전하게 보호하기 위해 2017년 미국 국방부 산하의 방위고등연구계획국(DARPA, Defense Advanced Research Program Agency)이 출범

105) <https://www.securityweek.com/intel-announces-new-hardware-based-security-capabilities>

106) <https://support.apple.com/ko-kr/guide/security/secf020d1074/web>

107) ARM, "ARM Security Technology-Building a Secure System using TrustZone Technology", (http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf)

시킨 프로그램이다. SSITH 프로그램의 핵심 목표는 디지털 시스템에서 사용하고 있는 응용 소프트웨어의 안전성을 보장하기 위해 보안패치에만 의존하던 기존 관행에서 탈피하여 취약점이 직접적으로 발생하는 디지털 장치 내의 하드웨어 요소에 초점을 맞춰 하드웨어 취약점을 해결하는 것이다.¹⁰⁸⁾

DARPA는 SSITH 프로그램을 통해서, 특정한 취약점에 국한되지 않고 소프트웨어를 통해 악용할 수 있는 모든 형태의 취약점으로부터 디지털 시스템을 보호하기 위한 하드웨어 보안 아키텍처 및 그와 연계된 설계 도구를 개발하고 있다. 그리고 특히 버퍼 오류, 정보 누출, 시스템 내의 자원 관리, 수치 오류, 코드 주입, 암호연산 오류, 승인, 권한 및 접근 등을 포함하여 공통 보안약점(CWE, Common Weakness Enumeration)¹⁰⁹⁾ 프로젝트 및 NIST에 의해 식별된 하드웨어 보안취약점에 초점을 맞추고 대책 개발을 추진 중이다.

DARPA는 2020년 6월, 사이버보안 전문가들을 초빙하여 SSITH 프로그램의 취약점을 찾기 위한 버그 바운티(bug bounty) 프로그램인 FETT(Finding Exploits to Thwart Tampering) 프로그램을 시작하였다. 국방부 산하의 국방디지털서비스국과 클라우드 보안 업체인 Synack이 협력하여 2020년 7월부터 9월까지 진행될 예정인 FETT 프로그램에는 SRI 인터내셔널, 케임브리지 대학교, 매사추세츠 공과대학교(MIT), 미시간 대학교, 록히드 마틴 등에 소속된 연구원들이 참여하고 있으며, DARPA에서 개발한 SSITH 하드웨어 보안 체계에 침투하여 취약점을 찾고자 노력하고 있다. 이러한 과정을 통해 공격 소프트웨어가 어떤 행위를 시도하는지에 대한 정보를 획득하고 하드웨어에 제공함으로써 하드웨어 자체가 능동적 방어를 수행하는 주체가 되도록 만드는 것이 FETT 프로그램의 최종 목표라 할 수 있다.¹¹⁰⁾

108) DARPA 홈페이지, <https://www.darpa.mil/program/ssith>(검색일: 2020. 8. 21)

109) MITRE에서는 공통취약점 리스트인 CVE(Common Vulnerabilities and Exposures)와 보안약점 리스트인 CWE(Common Weakness Enumeration)를 모두 제공하고 있다. 취약점(vulnerability)은 공격자가 시스템 또는 네트워크에 접근하기 위해 직접적으로 사용할 수 있는 소프트웨어에 내재된 실수(mistake)를 의미하며, 보안약점(weakness)은 취약점으로 연결될 수 있는 오류(error)를 의미한다. 즉 보안약점이 보다 포괄적인 개념이며, 보안약점 중에서 공격자가 사이버공격에 악용할 수 있는 약점이라면 취약점 리스트에도 포함된다. 그러나 악용할 수 없는 약점이라면 취약점으로 분류되지 않는다. 2005년부터 제공되기 시작한 CVE에 이어 보안약점 리스트가 추가로 작성 및 제공된 이유는 다소 광범위하게 분류를 수행한 CVE만으로는 사이버보안업계의 요구사항을 충족시킬 수 없었고 보다 상세한 분류 기준이 필요했기 때문이다.(출처: <https://cwe.mitre.org/about/faq.html>)

110) <https://www.darpa.mil/news-events/darpa-finding-exploits-to-thwart-tampering>

III. PUF 기술

1. 개요

PUF는 반도체 제조 과정에서 발생하는 공정오차를 이용하여 특정 입력값(Challenge)에 대해 임의의 출력값(Response)을 생성하는 시스템을 의미하며, 다른 PUF에서 동일한 출력값을 생성하는 것은 불가능하다.¹¹¹⁾ 그리고 특정 입력값에 대한 출력값을 예측하는 것이 불가능하다는 ‘예측 불가능성’, 동일한 출력값을 생성하는 PUF를 복제하는 것이 불가능하다는 ‘복제 불가능성’의 특징을 가진다.¹¹²⁾

PUF의 예측 불가능성은 PUF가 장착된 기기의 유일성을 보장할 수 있는 수단이자 임의의 값을 생성하는데 사용되었던 난수 생성 장치를 대신할 수 있을 것으로 평가하고 있다.¹¹³⁾ 또한 PUF를 통해 생성된 값은 전압이나 온도 등의 환경적 요인에 영향을 받지 않으면서 외부로부터의 추가적인 정보 주입 없이 오로지 하드웨어 공정오차에 의해서만 생성되기 때문에 무결성을 보장하기 위한 수단으로도 많이 활용되며, 소프트웨어-하드웨어적으로도 안전한 것으로 평가하고 있다.¹¹⁴⁾

이러한 PUF는 작은 chip의 형태로 간단하게 구성되며, 기존 비휘발성메모리(Non-Volatile Memory, 이하 NVM) 대비 적은 면적과 전력 소모율을 갖는다. 그리고 PUF 자체는 별도의 메모리에 저장이 불필요하다.¹¹⁵⁾¹¹⁶⁾

PUF의 성능을 평가하는 지표는 <표. 1>에서 보는 바와 같다.¹¹⁷⁾¹¹⁸⁾¹¹⁹⁾

111) 백종학, 신광조, “PUF 기술을 활용한 보안칩 기술 개발과 그 응용 분야,” 전자공학회지, 7월, 2016.

112) 변진옥, “PUF 기반 RFID 인증 프로토콜의 효율적설계에 관한 연구,” 정보보호학회논문지, 제 24권, 제5호, pp. 987-999, 2014.

113) C. W. O'Donnell, G. E. Suh, and S. Devadas, “PUF Based Random Number Generation,” MIT CSAIL CSG Technical Memo 481, 2004.

114) J. Zhang, B. Qi, and G. Qu, “HCIC: Hardware-assisted Control-flow Integrity Checking,” IEEE Internet of Things Journal, pp. 1-14, 2018.

115) Wei Liang, “Study on PUF based secure protection for IC design”, Microprocessors and Microsystems, Vol.45, pp. 56-66, 2016.

116) B. Habib, “A comprehensive set of schemes for PUF response generation”, Microprocessors and Microsystems, Vol.51 pp. 239-251, 2017.

117) M. Barbareschi, “A PUF-based hardware mutual authentication protocol”, J. Parallel Distrib. Comput. 119 (2018) 107-120

118) Minseo Kim, “A Chaotic Entropy Source based PUF Design for Secure IoT Platform”, Journal of Semiconductor Technology and Science 19(1), pp. 124-128, 2019.

119) Paik Jong Hak, “Development of Secure Chip Technology Using PUF Technology and Its Applications”, The Magazine of the IEEE 43(7), pp. 59-67, 2016.

〈표 1〉 PUF 성능 평가 지표

지표	설명
신뢰성	환경의 변화(전압, 온도 등)가 발생하더라도 동일한 출력값을 생성할 수 있어야 한다.
무작위성	단일 반도체 제조공정에서 생산되었다 해도 동일한 입력값에 대해 서로 다른 출력값을 가져야 한다.
예측 불가능성	한 쌍 이상의 CRP(Challenge and Response Pair)를 이용하여 임의의 입력값에 대한 출력값을 알아낼 수 없어야 한다.
균일성	생성된 출력값에서 0, 1의 분포가 균일해야 한다.(1:1)

2. PUF의 형태

가. Weak PUF와 Strong PUF

PUF는 처리할 수 있는 입력값(Challenge)의 크기에 따라서 ‘Weak PUF’와 ‘Strong PUF’로 분류한다. Weak PUF는 적은 수의 입력값만을 처리할 수 있고 특별한 경우에는 하나의 입력값만을 지원하기도 한다. Strong PUF는 제한된 시간 내에 모든 CRP(Challenge-Response Pair)에 대한 완전한 측정이 불가능할 정도로 충분히 많은 입력을 처리할 수 있다. 즉 Strong PUF는 충분히 많은 CRP를 가진다.¹²⁰⁾¹²¹⁾ 그러나 처리 가능한 입력값의 수가 PUF의 성능을 의미하는 것처럼 인식되는 경향이 있어 PUF 표준인 ISO/IEC 20897-1에서는 각각 ‘Confined PUF’와 ‘Extensive PUF’로 표기하여 분류하고 있다.¹²²⁾

• Weak PUF(Confined PUF)

Weak PUF는 회로 혹은 하드웨어가 제조과정에서 가지게 되는 ‘지문(fingerprint)’의 일부를 직접 디지털 값으로 변환하는 PUF로 생각할 수 있으며, 다음과 같은 특성을 가진다.¹²³⁾

- 하나 또는 소수의 CRP만을 가진다. 가질 수 있는 CRP의 범위는 제조과정에서 적용된 구성 요소의 수에 따라 선형적으로 달라질 수 있다.
- 지문을 직접 디지털화하여 만든 Challenge에 대해 항상 동일한 출력값을 생성하기

120) Paik Jong Hak, 앞의 논문.

121) Jae-min Choi, “Design and Implementation of a Low Power Chip with Robust Physical Unclonable Functions on Sensor Systems”, Journal of Sensor Science and Technology Vol. 27, No. 1, pp. 59-63, 2018.

122) ISO/IEC 2nd CD 20897-1, July 2018.

123) C. Herder, M. Yu, F. Koushanfar and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial”, Proceedings of the IEEE, Vol. 102, No. 8, August 2014.

위해 환경적인 조건에 영향을 받지 않으며, 다중 판독에 대해서도 안정성을 가진다.

- 입력값에 대한 출력값은 예측할 수 없으며 제조과정에서 기기나 회로에 적용된 변동성(구성 요소의 수나 구성방식 등)에 따라 크게 달라진다.

이러한 Weak PUF의 극단적인 사례로는 전원을 켜올 때 SRAM의 상태를 들 수 있다. SRAM을 구성하는 셀은 대칭적인 형태를 가지지만, 제조과정에서 적용된 변동성에 따라 전원이 켜졌을 때 각 셀이 가지는 값("1" 또는 "0")은 달라진다. 이러한 현상이 SRAM 전체에 걸쳐 무작위로 발생하면서 전원이 켜졌을 때 각각의 SRAM을 유일하게 식별할 수 있는 고유 지문이 생성된다.¹²⁴⁾ 만약 Response가 전체 SRAM의 상태에 의해 구성되면, 입력은 전원을 켜는 행위 자체가 되며 CRP는 단 하나만 생성된다.

일반적으로 Weak PUF는 적은 수의 CRP만 가지기 때문에, 이러한 쌍들은 안전하게 관리되어야만 한다. 하나의 CRP만 가지는 경우 그 CRP가 노출되면 어떤 장치라도 PUF를 모의하는 것이 가능해진다. 이러한 이유로 Weak PUF는 암호키 생성 과정에 적용하기에 적합하다.

- Strong PUF(Extensive PUF)

Strong PUF는 많은 물리적 구성 요소가 Challenge 생성에 관여하기 때문에 매우 많은 수의 Challenge를 가진다. 때문에 Weak PUF보다 훨씬 강력한 보안 기능을 제공할 수 있으며, 다음과 같은 특성을 가진다.¹²⁵⁾¹²⁶⁾¹²⁷⁾¹²⁸⁾¹²⁹⁾¹³⁰⁾

- 많은 Challenge를 가지기 때문에 공격자가 상당한 시간 동안 물리적으로 PUF를

124) P. Layman, S. Chaudhry, J. G. Norman, and J. R. Thomson, "Electronic fingerprinting of semiconductor integrated circuits," (6,738,294), September 2002.

125) C. Brzuska, M. Fischlin, H. Schroder and S. Katzenbeisser, "Physical Unclonable Functions in the Universal Composition Framework," CRYPTO 2011.

126) U. Ruhrmair, H. Busch and S. Katzenbeisser, "Strong PUFs: Models, Constructions and Security Proofs. In A.-R. Sadeghi, P. Tuyls (Editors): Towards Hardware Intrinsic Security: Foundation and Practice," Springer, 2010.

127) U. Ruhrmair, S. Devadas and F. Koushanfar, "Security based on Physical Unclonability and Disorder," In M. Tehranipoor and C. Wang (Editors): Introduction to Hardware Security and Trust. Springer, 2011.

128) U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas and J. Schmidhuber, "Modeling Attacks on Physical Unclonable Functions," ACM CCS 2010.

129) U. Ruhrmair, J. Solter and F. Sehnke, "On the Foundations of Physical Unclonable Functions," Cryptology ePrint Archive, 2009:277, 2009.

130) U. Ruhrmair, J. Solter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson and S. Devadas, "PUF Modeling Attacks on Simulated and Silicon Data," IEEE Transactions on Information Forensics and Security (IEEE T-IFS), 2013.

점유하고 있더라도 모든 CRP를 완전하게 파악할 수는 없다.

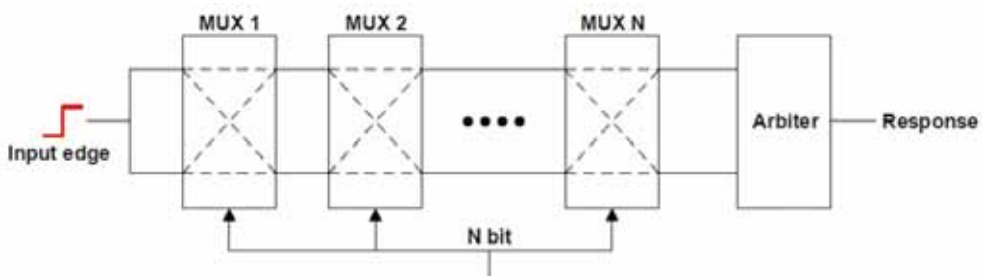
- 공격자가 CRP의 상당 부분을 알아냈다 하더라도 알려지지 않은 다른 CRP를 추론하거나 예측할 수 없다.
- 일반적으로 Strong PUF는 CRP를 생성하는 인터페이스에 자유롭게 접근할 수 있다고 가정한다. 따라서 Strong PUF를 물리적으로 소유하고 있는 공격자는 임의의 Challenge를 적용하여 그에 상응하는 Response를 생성할 수 있다.

나. Mismatch-based PUF와 Physical-based PUF

또 다른 분류 방법은 반도체 내부의 회로소자 동작에 따른 오차를 이용하는 mismatch-based PUF와 물리적 특성을 이용한 physical-based PUF가 있다. 먼저, mismatch-based PUF에는 Arbiter, RO, Butterfly 등 다수의 PUF가 존재하나, 본 연구에서는 가장 대표적인 형태인 Arbiter PUF만을 간단히 소개하고, physical-based PUF는 VIA PUF에 대해서만 살펴본다.

• Arbiter PUF

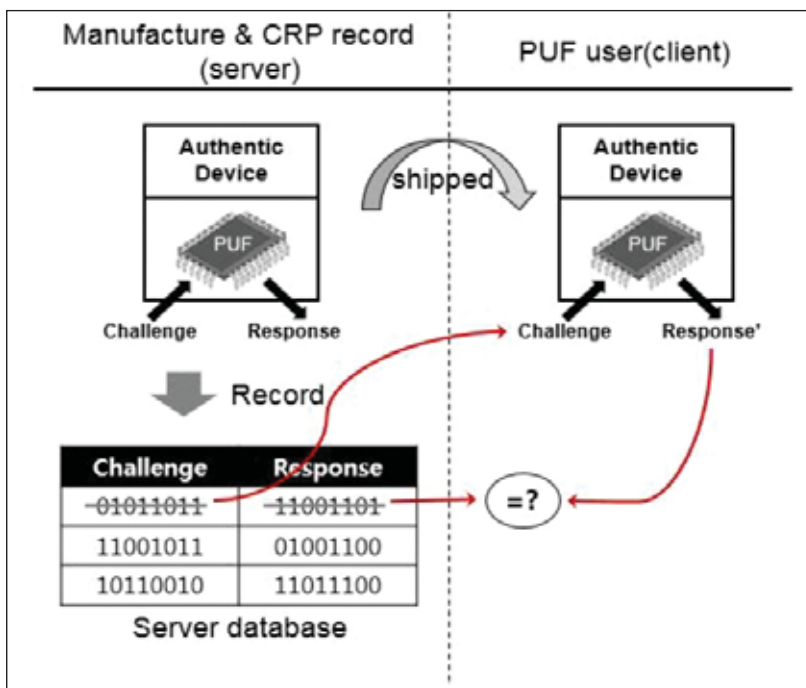
Arbiter PUF는 공정 변이에 의해 발생하는 게이트의 지연(delay) 차이를 이용한다. N개의 멀티플렉서 쌍으로 구성되는 Arbiter PUF는 <그림 1>에서 보는 바와 같이 설계상 동일한 거리를 갖는 두 개의 경로로 N bit의 입력 신호를 보내면 달라지는 멀티플렉서의 연결과 공정 편차에 의해 지연시간이 발생한다. 그리고 Arbiter 회로는 신호가 도착하는 순서에 따라 1, 0의 값을 Response로 출력한다.¹³¹⁾



<그림 1> Arbiter PUF의 구조

131) 임순일, "Enhancing reliability of Physically Unclonable Function(PUF) using counter", 성균관대학교 석사학위논문, 2018

이러한 과정을 통해 Arbiter PUF는 N 비트의 입력에 대해 2N개의 CRP를 생성할 수 있기 때문에 Strong PUF로 분류되며, IoT 기기의 인증을 위한 수단으로 활발하게 사용되고 있다. <그림 2>에서 보는 바와 같이, 우선 칩 제조자는 PUF를 작동시켜 생성되는 CRP를 인증서버에 등록하고, PUF 칩이 내장된 모듈 운용 단계에는 등록된 Challenge 중 하나를 사용자에게 보내어 Response를 받아 등록된 CRP와 대조하여 인증한다. 그리고, 사용된 CRP는 OTP(One Time Password)처럼 삭제하여 보안 위협을 감소시킨다.¹³²⁾¹³³⁾



〈그림 2〉 Strong PUF를 이용한 인증

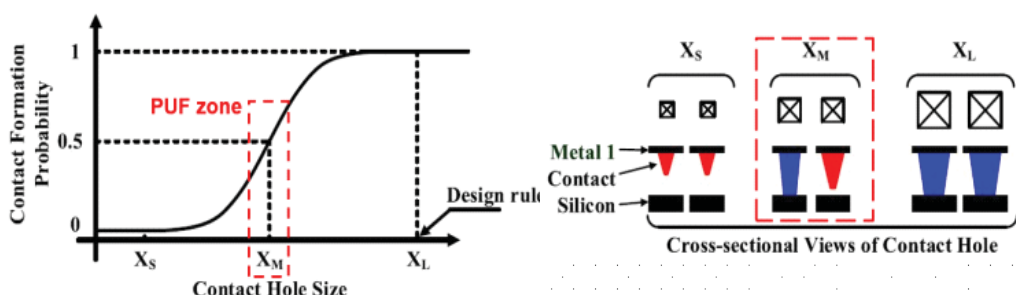
- VIA PUF

VIA는 전도성인 인접 메탈 레이어를 연결하기 위한 반도체 제조공정으로 두 레이어의 연결을 위해 구멍(hole)을 뚫게 되고, 구멍의 크기에 따라 레이어 연결 여부가 결정된다. VIA PUF는 이러한 VIA가 형성될 확률을 기반으로 임의의 예측하기 불가능한 값을 생성하는 PUF이다.

132) Mario Barbareschi, 앞의 논문.

133) 인순일, 앞의 논문.

일반적으로 VIA가 항상 형성되는 것을 보장하기 위한 크기를 설계 규칙으로 정하고, 이것을 X_L 이라고 했을 때 이보다 작아지면 VIA가 형성이 되지 않을 수도 있다. <그림 3>의 우측에서 보는 바와 같이 연결된 부분은 0, 단락된 부분은 1이 된다. 왼쪽 그래프에서 보는 것처럼 구멍의 크기를 고의적으로 X_M 으로 설정하였을 때 1과 0의 분포가 균일해져 PUF의 특성 중 하나인 균일성을 만족하게 된다.¹³⁴⁾ (이후의 연구에서는 $X_L = 0.25\mu\text{m}$, $X_M = 0.19\mu\text{m}$ 시 1과 0의 비율이 1:1이 됨을 밝혔다.¹³⁵⁾).



<그림 3> VIA Hole 크기에 따른 연결 확률

기존 mismatch-based PUF의 한계점을 여러 가지 측면에서 보완할 수 있는 VIA PUF가 가지는 장점은 다음과 같다.

- 기존 PUF는 회로 구성 소자가 운용 환경(온도, 입력전압 등)에 영향을 받아 동일 Challenge에 대해 동일한 Response를 출력하지 못할 수 있어 신뢰성, 균일성 측면에서 불리하다. 반면 VIA PUF는 메탈 재질의 레이어의 물리적 연결 여부와 관련이 있으므로 실온의 환경에 영향을 받지 않으며, 이는 국제반도체표준협약기구(JEDEC)의 신뢰도 평가에서 확인되었다.¹³⁶⁾¹³⁷⁾
- 환경적 영향으로 동일 Challenge에 대해 항상 동일한 Response를 출력하지 못할 수도 있다는 문제점을 개선하기 위해 회로기반 PUF는 오류 정정코드(error correction code) 기반의 후처리가 필요하다. 즉 오류 정정을 위해 별도의 하드웨어가 필요하게 되어 PUF 원본 데이터를 노출시킬 수 있는 여지가 발생한다. 그리고 입력 전력, 크기, 비용의 측면에서 불리하다는 단점이 존재하는데, VIA는 환경에 영향을 받지 않으므로 기존 PUF의 단점을 보완할 수 있다.¹³⁸⁾

134) ICTK, KR open patent, 10-2013-0019 358, 2013. 2.

135) Paik Jong Hak, 앞의 논문.

136) Paik Jong Hak, 앞의 논문.

137) Mario Barbareschi, 앞의 논문.

- Arbiter PUF와 같은 Strong PUF는 인증 시 단말기와 인증서버 간 주고받는 여러 쌍의 CRP를 학습하여 향후의 CRP값을 유추해 내는 머신러닝 기반의 공격기법에 취약하다는 점이 입증되었다.¹³⁹⁾
- 회로 소자를 이용한 PUF는 소자의 상태 변화 시 전력의 소모량이 증가하여 DPA (Differential Power Analysis)같은 부채널 공격에 취약하고, 칩 내부 버스의 분석을 통해 비밀키를 유추해 내는 Probe 공격 등에 취약할 수 있으나, VIA PUF는 회로 소자에 의한 비밀키 생성이 아닌 의도된 물리적 공정에 의한 무작위 값 생성으로 DPA 공격 방어에 우수하며, 수만에서 수십만 개의 게이트 칩 내부에서 PUF 셀을 찾아내어 VIA의 단락 여부를 관찰하는 것은 거의 불가능에 가깝기 때문에 Probe 공격의 방어도 용이하다.

3. PUF 기반의 사이버보안 구현 사례

PUF가 가지는 무작위성, 예측 불가능성 및 복제 불가능성 등의 특성으로 인해 PUF는 하드웨어 기반 사이버보안 기술에서 독보적인 위치를 선점하고 있다. 최근 사물인터넷을 위한 사이버보안 강화에서 특히 인증 분야에 PUF 기술이 가장 활발하게 적용되고 있고, 필요한 경우에만 유일한 비밀키를 생성하여 이용할 수 있도록 지원하는 저비용 기술로도 각광을 받고 있다.

인증은 통신을 수행하는 당사자들의 신원을 확인하는데 있어 필수적인 암호학적 수단이다. 그리고 인증을 안전하게 수행하기 위해서는 신원정보를 복제나 추측 등이 어렵도록 복잡하게 만드는 것이 중요하다. 이러한 측면에서 최근들어 기억장치에 신원 정보를 저장하기 보다는 기기의 구조 자체에 내장될 수 있도록 해주는 PUF가 주목을 받고 있으며, 다양한 분야에서 많은 응용 방안들이 제시되었다.

특히 PUF는 보안 EEPROM 및 기타 고가의 하드웨어가 없이도 인증정보를 안전하게 저장할 수 있다.¹⁴⁰⁾¹⁴¹⁾ 이는 디지털 메모리에 비밀키를 저장하는 대신 PUF가 집적회로의 물리적 특성에서 비밀키를 도출하기 때문에 가능한 일이다. 전력 사용 측면에서도 EEPROM

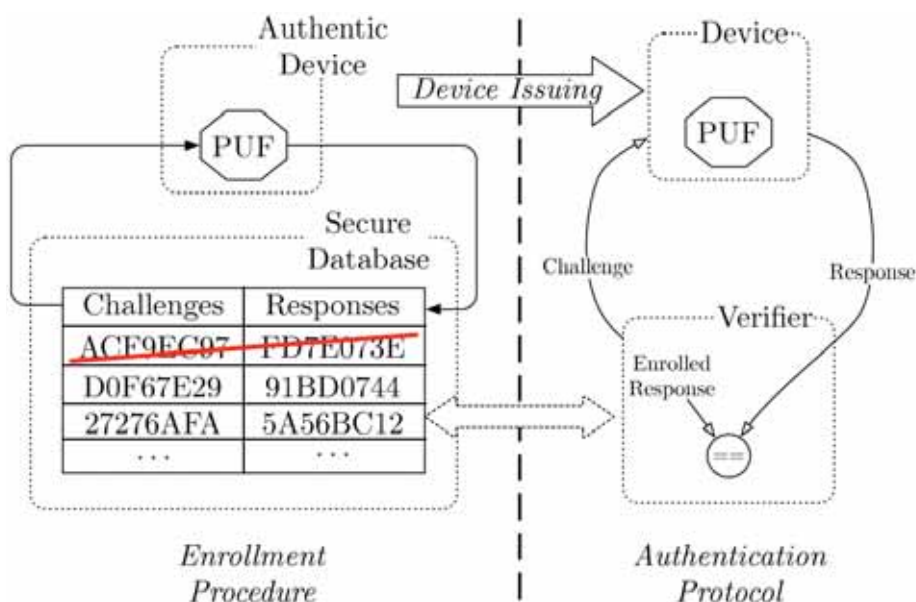
138) 인순일, 앞의 논문.

139) Wei Liang, "Study on PUF based secure protection for IC design", Micro-processors and Microsystems Vol. 45, pp. 56-66, 2016.

140) B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in Proc. 9th ACM Conf. Comput. Commun. Security (CCS), pp. 148-160, 2002.

141) U. Rührmair, S. Devadas and F. Koushanfar, "Security based on physical unclonability and disorder," Introduction to Hardware Security and Trust, M. Tehranipoor and C. Wang, Eds. New York, NY, USA: Springer-Verlag, pp. 65-102, 2012.

이나 RAM 기반의 대책보다는 적은 전력을 사용하며, PUF를 사용하는 응용프로그램은 SHA 해시알고리즘이나 공개키암호 알고리즘을 이용할 때 필수적인 고가의 암호화 전용 하드웨어가 불필요하다. 이러한 PUF 기술을 활용하여 인증을 수행하는 기본적인 절차는 <그림 4>에서 보는 바와 같다.



<그림 4> PUF의 Challenge-Response를 활용한 인증 절차

PUF를 기반으로 특정 기기에 대한 인증을 수행하기 위해서는 우선 해당 기기에 내장된 PUF에 Challenge-Response 쌍을 포함하고 있는 CRP 테이블이 생성되어야 하며, 생성된 CRP 테이블은 안전한 저장소에 보관되어야 한다. 이러한 과정은 기기 등록 과정에서 이루어진다. 이후 PUF를 장착한 기기가 네트워크 접속 등을 위하여 인증을 요청하면, 인증을 담당하는 측에서는 CRP 테이블에 저장되어 있는 특정한 Challenge 값을 해당 기기에 전송하고, 인증을 요청한 기기는 전송받은 Challenge를 이용하여 Response를 생성한다. 생성된 Response를 인증 담당에게 전송하면 인증 담당은 전송받은 Response가 CRP 테이블에 저장된 값과 일치하는지를 확인하여 일치하면 인증이 완료 되는 순으로 진행된다.

Y. Alkabani 등은 PUF에서 생성되는 Response 값을 활용하여 기기의 고유 ID를 생성하는 방안을 제시하였고¹⁴²⁾, J. Bringerr 등은 PUF를 기반으로 스트림 암호의 비밀키를

142) Y. Alkabani, F. Koushanfar, N. Kiyavash, and M. Potkonjak, "Trusted integrated circuits:

보호하는 방안을 연구하였다.¹⁴³⁾ 이종훈 등은 보안 USB를 인증하는 과정에서 PUF 기술을 접목하여 보안성을 강화하는 방안을 제시하였다.¹⁴⁴⁾ S. Park 등은 Public PUF를 기반으로 하드웨어에서의 응답 생성 시간의 차이를 이용하는 인증모델인 PUFSec를 제안하였다.¹⁴⁵⁾

정진우 등은 PUF 기술을 활용하여 5G EPS-AKA를 기반으로 무선망을 구성할 경우 초기 인증을 강화할 수 있는 방안을 제시하였고¹⁴⁶⁾, Huang 등은 무선 센서네트워크에서의 그룹키 분배방안을 제시하였다.¹⁴⁷⁾

T. Gu 등은 지문 기반 인증을 통해 장치 스푸핑공격을 방지할 수 있는 사물인터넷 보안통신 프레임워크를 제안하였다.¹⁴⁸⁾ 김수민 등은 다양한 사물인터넷 기기가 운용될 IoT 환경에 적용 가능한 PUF 기반의 키관리 및 인증 강화 기법을 제시하였다.¹⁴⁹⁾

4. 국방 영역에서의 PUF 기술 적용 분야 식별

하드웨어 기반 사이버보안 기술의 대표적인 형태이며, 최근 들어 다양한 분야에서의 적용이 가시화되고 있는 PUF를 활용하여 국방영역에서 사이버보안 강화를 도모할 수 있는 분야로는 다음과 같은 2가지 대상 체계를 선정하였다.

- 국방 사물인터넷(M-IoT)

대한민국 국방부는 지난 2015년 5월, 국방 IoT 사단 ‘NCW-K’ 구축방안을 확정하고, 2016년부터 시범 사업을 실시한다는 계획을 발표하였다.¹⁵⁰⁾ 육군은 2015년 6월 육군

A nondestructive hidden characteristics extraction approach,” Lecture Notes in Computer Science, Springer-Berlin, vol. 5284, pp. 102-117, 2008.

143) J. Bringerr, H. Chabanne, T. Icart, “On physical obfuscation of cryptographic algorithms,” vol. 5922 of Lecture Notes in Computer Science, Springer-Verlag, pp. 88-103, 2009.

144) 이종훈, 박정수, 정승욱, 정수환, “PUF 기반의 보안 USB 인증 및 키 관리 기법”, 한국통신학회논문지 Vol.38B, No.12, 2013.

145) S. Park, S. Lim, D. Jeong, J. Lee, J. Yang, H. Lee, “PUFSec: Device Fingerprint-based Security Architecture for Internet of Things,” In Proceedings of the IEEE Conference on Computer Communications, Atlanta, GA, USA, 1-4, pp. 1-9, May 2017.

146) 정진우, 이수진, “5G 인증 및 키합의 프로토콜(5G-AKA)의 보안취약점과 PUF 기반의 보안성 향상 방안”, 융합보안논문지, 19(1), pp. 3-10, 2019.

147) M. Huang, B. Yu, and S. Li, “Puf-assisted group key distribution scheme for software-defined wireless sensor networks,” IEEE Communications Letters, Vol 22, no.2, pp. 404-407, 2018.

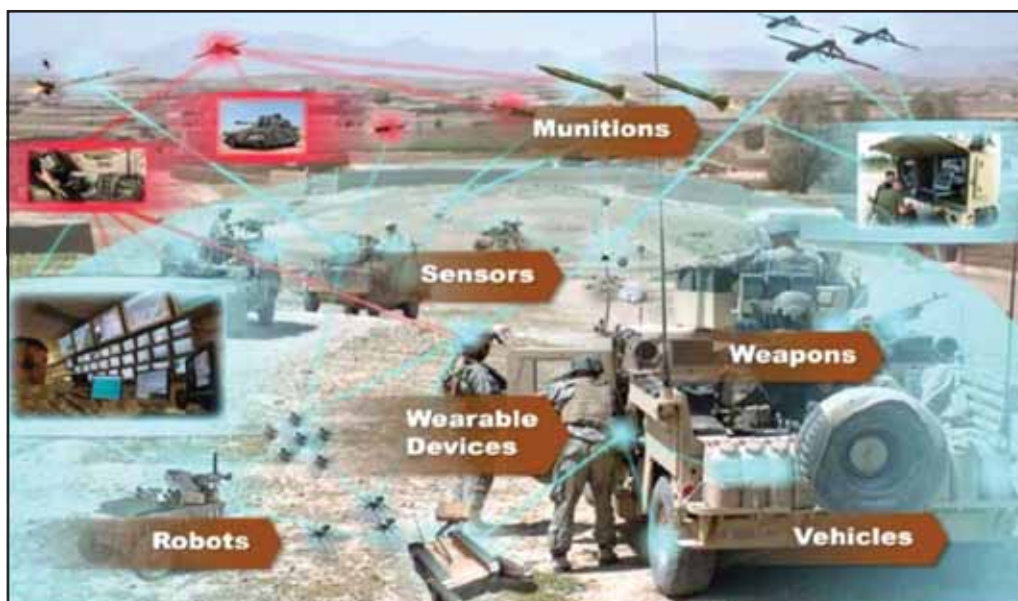
148) T. Gu, P. Mohapatra, “BF-IoT: Securing the IoT Networks via Fingerprinting-Based Device Authentication,” In Proceedings of the IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Chengdu, China, pp. 254-262, October 2018.

149) 김수민, 이수진, “M-IoT 환경에서 PUF 기술을 활용한 안전한 통신채널 구성 기법”, 융합보안논문지, 19(5), pp. 107-118, 2019.

150) 디지털타임스, 『국방부, IoT 사단 만든다』, 2015. 5. 25.

훈련소를 테스트베드로 하여 스마트 훈련병 관리체계를 구축하는 사업을 시작하였고, 공군도 같은 해에 조종사 헬스케어 시스템 구축을 시작하여 12월 헬스케어 캡슐을 시범 운영하기 시작하였다. 2016년 3월에는 수도군단에 센서 기반의 주둔지 방호 및 스마트 부대관리를 지원하는 국방 사물인터넷 기반 플랫폼 체계를 구축하였다. 적 예상 접근로에 지진동 센서를 설치해 조기경보가 가능해졌고, 드론을 활용하여 울타리 순찰을 실시함으로써 경계 능력도 보강하였다. 총기·탄약에는 센서를 부착하여 입출고 현황관리를 자동화하고, 병사들에게 지급된 스마트폰을 활용하여 실시간 상황전파 및 효율적인 병력관리가 가능하도록 하였다.¹⁵¹⁾

미국을 비롯한 주요 국가도 사물인터넷 기술을 국방에 적용하여 혁신을 시도하고 있다. 미군의 경우 사물인터넷 기술을 기반으로 <그림 5>에서 보는 바와 같이 전장의 모든 요소를 연결하는 IoBT(Internet of Battlefield Things) 구축을 추진하고 있다.¹⁵²⁾



〈그림 5〉 IoBT 구축 개념도

향후 군사 분야에서는 작전, 병력관리, 무기체계 및 지휘통제체계(C4I) 등 다양한 영역에 걸쳐 사물인터넷 기술이 점차적으로 확대 적용되면서 IoBT 형태로 발전해 나갈 것임은 충분히 예측 가능하다. 그리고 사물인터넷 기술을 기반으로 한 제반 요소들의 연결은 미래

151) 국방일보, 『‘All-IP’ 통합 네트워크로 유선, 무선, 위성 넘나든다』, 2017. 4. 10.

152) <https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt>

전장에서의 우위를 보장해 줄 것이며, 전장이 아닌 일반업무 영역에서는 국방경영 효율화와 혁신적인 국방운영이 가능해지는 등 사물인터넷 기술의 국방 적용을 통해 얻을 수 있는 효과는 상당히 크다. 그러나 사물인터넷 환경 구축에 있어 결코 간과할 수 없는 부분이 바로 사이버보안이다. 사물인터넷 환경에서 네트워크로 연결되는 다양한 종류의 기기들에 대해 상당수는 데이터 센싱 및 통신능력 확보가 우선시되고 있는 반면에, 보안에 대한 고려는 상대적으로 미흡하여 많은 취약점을 안고 있다.

Business Insider는 2018년 기준으로 100억 개의 사물인터넷 기기가 인터넷에 연결되어 있으며, 2025년에는 640억 개 이상의 기기가 연결될 것으로 전망하고 있다. 그리고 보안전문가들은 사물인터넷에 연결되는 기기의 수가 급증하면 보안취약점도 더욱 다양한 형태로 나타날 것이고, 피해는 더욱 심각해질 것이기 때문에 효율적인 보안대책 수립의 필요성을 강조하고 있다. 국방부가 스마트 국방 구현을 위해 구축을 추진하는 국방 사물인터넷(M-IoT)도 연결되는 기기의 종류와 수량이 증가할수록 다양한 사이버보안 위협에 직면하게 될 것이다. 연결성을 강조할 수밖에 없는 국방 사물인터넷 환경에서는 하나의 기기라도 사이버 위협에 노출될 경우 인접한 기기뿐만 아니라 기반구조까지 위협에 노출되고 전력 손실로까지 이어질 수 있기에 보안대책에 관한 연구는 기술의 적용과 함께 반드시 병행되어야 한다.

사물인터넷 보안과 관련된 대부분의 연구는 사이버보안을 사물인터넷 기술발전과 활성화를 위한 최우선 과제로 지목했다. 그러나 사물인터넷 환경의 특수성과 연결되는 기기의 자원제약적 특성으로 인해 다른 형태의 네트워크에 적용했던 보안기법들을 직접 적용하기는 어려우며, 복잡하고 많은 연산이 요구되는 보안대책을 적용하기도 쉽지 않다.

이에 본 연구에서는 스마트 국방의 최우선 선결 과제라고 할 수 있는 국방 사물인터넷을 구축 및 운용하는데 필수적으로 요구되는 보안대책을 구현하기 위해, 물리적으로 복제 불가능한 기능(PUF)을 이용하여 다양한 이기종 기기들을 고유하게 식별 및 인증하고, 비교적 적은 연산량에 의해 대칭키를 생성하여 안전한 통신채널을 구성하는 방안을 제안하고자 한다.

• 드론봇 전투체계

육군이 지상작전 패러다임의 변화를 위한 핵심 전력인 5대 게임 체인저(Game changer) 중 하나로 고려하고 있는 드론봇 전투체계는 보안성과 안전성을 제대로 확보하지 않고 전력화를 진행하게 된다면, 적으로부터 노출되기 쉬운 드론의 특성상 다양한 공격에 취약해질 수 있다. 이미 2008년도에 미군이 운용하는 프레데터 드론이 이라크 무장단체의 해킹 공격에 의해 기밀영상이 그대로 유출된 사례가 있으며, 2011년에 무인 스텔스 RQ-170이 스푸핑 공격을 당해 이란 정부에 납치되면서 최첨단 기술이 유출되는 사건도

발생한 바 있다.

본 연구에서는 드론봇 전투체계의 기반 네트워크가 상용 이동통신 기술인 4G 또는 5G 네트워크가 될 것임을 가정하고, PUF 기반으로 드론봇 전투체계의 사이버보안을 강화할 수 있는 방안을 제안하고자 한다

상용 통신기술은 빠른 속도에 초점을 두고 있기 때문에 다양한 보안취약점을 가지고 있는 것으로 알려져 있다. 4G LTE 네트워크의 경우에는 EPS-AKA의 취약점으로 인해 사용자 장치인 UE의 IMSI 노출 및 복제, 사용자 위치 노출, 중간자 공격, Race-Condition 공격 등이 가능하다. 5G 네트워크의 경우에는 5G-AKA의 취약점으로 인해 USIM 복제 및 탈취를 이용한 공격, Race-Condition 공격, 중간자에 의한 메시지 연결 공격 등에 가능하다. 이에 본 연구에서는 PUF를 기반으로 우리 군이 이미 적용했거나 적용을 고려하고 있는 상용 이동통신 기술의 보안취약점을 해결하면서 드론봇 전투체계의 사이버보안을 강화하는 방안을 제안한다.

또한 드론봇 전투체계 운용 시 다수의 드론을 동시에 운용하는 군집드론의 필요성이 증대되고 있음을 고려하여, 다수의 드론이 자율통신망인 FANET을 안전하게 형성할 수 있도록 PUF 기반의 안전한 라우팅 프로토콜을 제안한다.

IV. PUF 기반의 국방 사이버보안 강화 방안

1. PUF를 이용한 국방 사물인터넷의 사이버보안 강화 방안

현재의 국방사물인터넷 환경은 각종 센서를 통해 정보를 수집하고 가공 및 분석하여 업무에 활용하는 일반적인 사물인터넷의 모습을 크게 벗어나지 않고 있다. 그러나 <그림 5>에서 보는 바와 같이 제반 전장 요소들이 모두 사물인터넷 기술을 기반으로 통합 연결 될 경우, 보다 다양한 형태의 통신이 나타날 수 있다. 본 연구에서는 미래지향적 관점에서 각종 센서 장비나 무기체계, 지휘통제체계 등이 모두 사물인터넷 기술을 기반으로 연결된 국방 사물인터넷 환경을 가정하고, PUF 기술을 활용하여 안전한 통신 채널을 구성할 수 있는 방안을 제안한다.

국방 사물인터넷 환경에 적용 가능한 PUF 기반의 안전한 통신 채널 구성기법은 다음과 같은 원칙을 적용하여 설계한다. 우선 공개키 기반 암호가 아닌 대칭키 기반 암호를 사용한다. 공개키 기반 암호가 대칭키 기반 암호에 비해 암호학적 강도가 높아 보다 강화된

사이버보안을 구현할 수는 있지만, 공개키 암호를 적용하기 위해서는 공개키 인증서를 검증하기 위한 인증서서가 존재해야만 한다. 그러나 전장 환경에서 인증서서가 항상 온라인으로 연결 가능함을 보장할 수 없다. 또한 사물인터넷에 연결되는 기기 중 센서와 같은 기기들은 연산능력이 제한되어 공개키 암호를 이용하는 것이 제한될 수도 있다. 둘째, 사물인터넷 환경에서 대칭키 기반 암호를 이용하기 위해 제안된 기존 접근방법들은 대부분 통신에 사용할 대칭키의 설립을 위해 초기 보안키 또는 마스터키의 사전 공유를 전제로 하고 있다. 그러나 초기 보안키나 마스터키가 통신 채널 형성 초기에 노출될 경우 이후에 생성되는 모든 대칭키가 노출될 위험에 처하게 된다. 따라서 본 연구에서는 초기 보안키 또는 마스터키의 공유를 배제한다. 셋째, 통신에 사용할 대칭키를 생성하여 전송하는 과정에서 노출되는 위험을 제거하기 위해 모든 키는 각 기기 내부에서 생성한다. 마지막으로 국방 사물인터넷 환경에서 다양한 형태의 통신이 발생할 수 있음을 고려하여 통신을 실시하는 대상과 목적에 따라 변경하여 사용할 수 있도록 다중키 구조를 적용함으로써, 단일키 장기 사용에 우한 노출 위험 증가를 제거한다.

사물인터넷 환경에서 운용되는 각각의 기기들을 관리하기 위해서는 대부분 관리서버를 운용한다. 본 연구에서는 그러한 관리서버를 통신에 활용한 대칭키를 생성하는데 사용한다. 그리고 국방 사물인터넷 환경에서 나타날 수 있는 통신의 형태에 따라 사용할 비밀키를 다음과 같이 세 가지로 구분하며, 사이버보안 대책의 기술을 위해 사용되는 표기법은 <표 2>에서 보는 바와 같다.

- ① 개인키 : 개별 기기들이 저장하는 비밀키로서, 관리서버와의 안전한 통신을 수행하기 위해 사용하는 비밀키(서버에서 특정 기기에 대한 정보수집 명령 하달 및 수집된 정보의 서버 전송, 특정 타격체계에 대한 명령 하달 및 수행 결과 전송 등)
- ② 일대일키 : 기기 간 일대일 통신에 사용되는 비밀키로서, 센서와 센서 혹은 무기체계와 지휘통제체계 간 통신 등 국방 사물인터넷 환경에서 운용되는 개별 기기들이 정보 및 상황 공유 간 안전한 비밀통신을 수행하기 위해 사용하는 비밀키
- ③ 그룹키 : 특정 관리서버의 관할 하에서 운용되는 기기들 전체가 비밀통신을 수행하기 위해 사용하는 비밀키(전체 기기가 공유해야 할 명령을 관리서버가 하달할 경우 또는 특정 기기가 수집한 정보를 전체 기기가 공유해야 할 경우의 정보 전송 등)

가. 사물인터넷 기기 도입 및 등록

국방 사물인터넷에서 운용할 모든 기기는 PUF 칩을 장착한 상태로 도입한다. 군 인증 센터에서는 도입된 사물인터넷 기기에 대해 고유한 식별자를 부여한 후 장착된 PUF의

Challenge-Response 값을 측정하여 CRP 테이블을 생성하고 기기의 식별자와 함께 저장한다. 이후 개별 부대에서 운용할 사물인터넷 기기가 결정되면 인증센터는 해당 기기와 함께 CRP 테이블을 각 운용부대로 배부한다. 운용부대는 기기를 수령한 후 부대 관리 서버에 기기의 고유식별자와 CRP 테이블을 등록하고, 사물인터넷 환경에서 해당 기기를 운용할 준비를 한다.

〈표 2〉 표기법

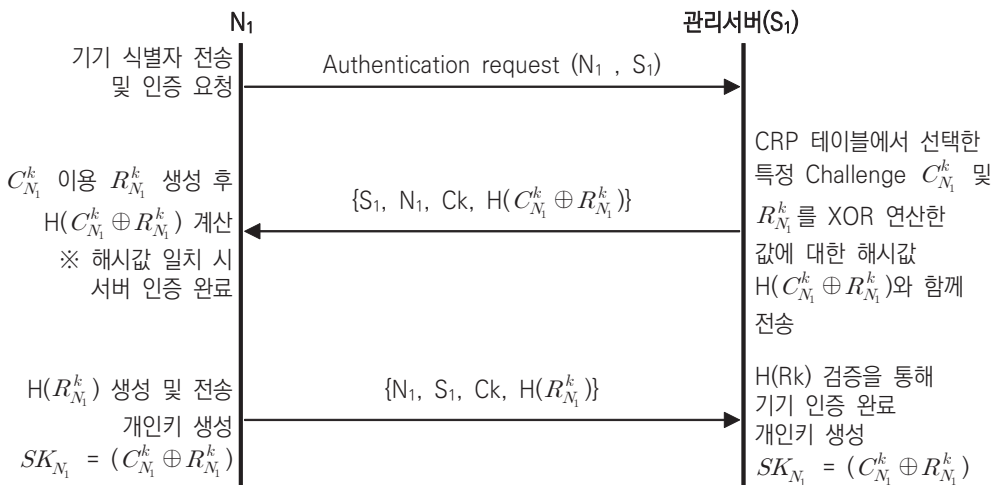
표기법	의 미
S_i	사물인터넷 기기 관리용 서버의 식별자
N_i	사물인터넷 기기의 고유 식별자
$H()$	일방향 Hash 함수
$C_{N_i}^k$	N_i 기기에 장착된 PUF에 입력되는 k 번째 Challenge
$R_{N_i}^k$	N_i 기기에 장착된 PUF에서 k 번째 Challenge에 의해 출력되는 k 번째 Response
SK_{N_i}	N_i 기기의 개인키
PK_{N_i, N_j}	N_i 기기와 N_k 기기가 공유하는 일대일키
GK	동일한 관리서버에 의해 관리되는 기기 간 비밀통신용 그룹키
e_{N_i}	그룹키 생성을 위해 각 기기에 제공되는 특정 지수
ACK	메시지 정상 수신 후 발송자에게 전송하는 확인 메시지

나. 기기 초기 인증 및 개인키 생성

운용부대 관리서버에 등록이 완료된 사물인터넷 기기가 네트워크에 최초로 접속하기 위해서는 인증과정이 먼저 진행된다. 각 기기는 〈그림 6〉에서 보는 바와 같이 자신의 식별자(N_i)를 관리서버로 전송하면서 초기 인증을 요청한다. 인증요청을 수신한 관리서버는 이전에 저장한 N_i 기기의 CRP 테이블에서 특정한 Challenge 값($C_{N_i}^k$)을 선택하고, 그에 대응되는 Response 값($R_{N_i}^k$)을 XOR 연산한 결과의 해시값 $[H(C_{N_i}^k \oplus R_{N_i}^k)]$ 을 계산하여 함께 N_i 기기로 전송한다.

N_i 기기는 전송받은 $C_{N_i}^k$ 를 PUF의 입력으로 사용하여 대응하는 $R_{N_i}^k$ 를 생성한 후 해시값 $[H(C_{N_i}^k \oplus R_{N_i}^k)]$ 을 계산하여 전송받은 해시값과 비교함으로써 인증 요청에 응답한 관리서버가 정당한 서버인지를 검증한다. 정당한 서버인지를 확인한 이후에는 $H(R_{N_i}^k)$ 를 생성하여 관리서버로 전송하고, 관리서버는 전송받은 해시값을 자신이 생성한 해시값과 비교하여

등록된 기기인지를 검증한다. 이러한 과정을 거쳐 기기와 관리서버 간의 인증이 완료되면 양측에서는 인증에 사용되었던 Challenge 값($C_{N_1}^k$)과 Response 값($R_{N_1}^k$)를 XOR 연산하여 비밀통신에 사용할 대칭키(SK_{N_1})를 설립한다. 다른 기기들도 이와 동일한 절차를 거쳐 관리서버와의 통신에 사용할 개인키를 설립하여 기기에 저장하면 관리서버는 모든 기기와 개별적인 비밀통신을 수행할 수 있게 된다.



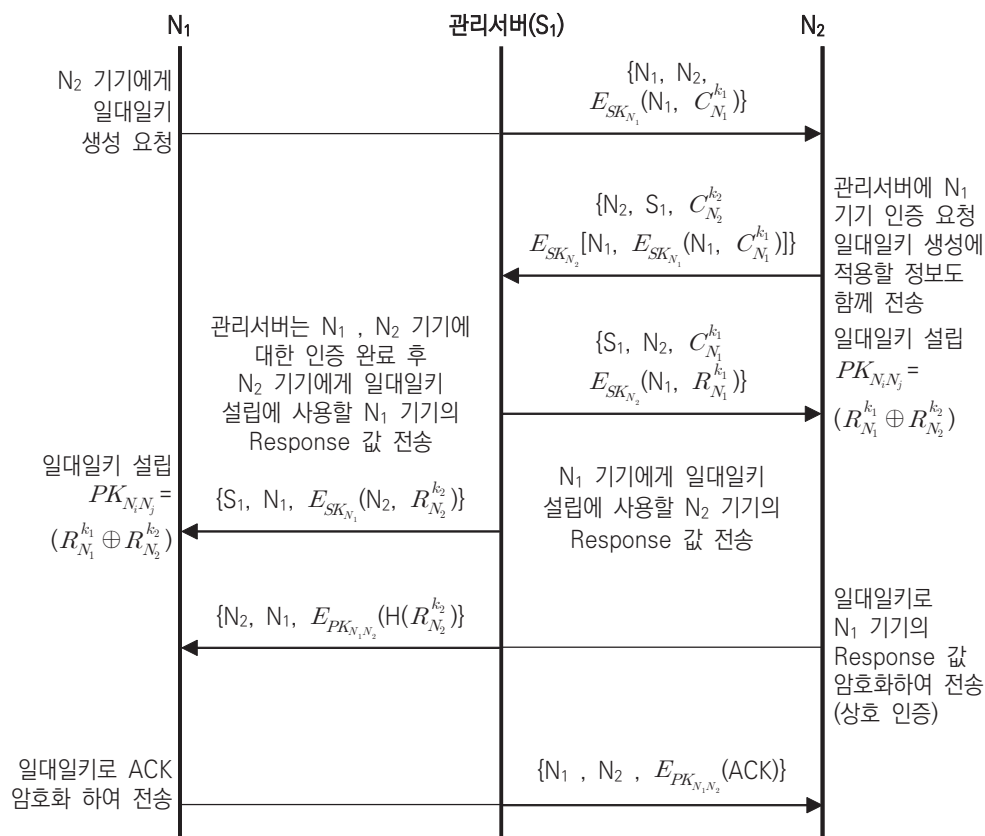
〈그림 6〉 기기 인증 및 개인키 설립 절차

다. 기기 간 비밀통신을 위한 일대일키 생성

일대일키 생성 절차는 특정 기기(N_2)와 비밀통신을 수행하고자 하는 기기(N_1)에 의해 개시되며, 일대일키의 설립은 기기 상호 간 정보 교환을 통해 진행되는 것이 아니라 관리서버를 통해 진행된다. 그러나 관리서버가 일대일키를 직접 생성하는 것은 아니며, 일대일키 설립을 원하는 기기들에 대한 인증을 수행한 후 각 기기에서 일대일키를 설립하는데 필요한 정보를 전송해주는 역할만 수행한다. 즉 일대일키의 설립은 관리서버에서 전송받은 정보를 이용하여 개별 기기에서 이루어진다.

〈그림 7〉에서 보는 바와 같이, N_1 기기가 N_2 기기와 비밀통신을 원할 경우 N_1 기기는 N_2 기기에게 일대일키 설립을 요청하는 메시지를 자신의 개인키로 암호화하여 전송한다. 전송되는 메시지에는 차후 N_2 기기가 일대일키 설립을 위해 사용할 Response 값에 대응하는 Challenge 값이 포함된다. 요청을 접수한 N_2 기기는 일대일키 설립을 요청한 N_1 노드가 등록된 기기인지 검증하기 위해 관리서버에 확인을 요청한다. 이 때 N_1 기기로부터 전송받은 메시지를 자신의 개인키로 암호화하고, N_1 기기가 일대일키 설립에 사용

할 자신의 Response 값에 대응되는 Challenge 값을 선택하여 함께 전송한다.



〈그림 7〉 기기 상호 간 일대일키 설립 절차

관리서버는 N_2 기기로부터 수신한 메시지를 N_2 기기의 개인키를 이용하여 복호화하면서 N_2 기기가 등록된 기기임을 확인하고, 이어서 일대일키 설립을 요청한 N_1 기기까지 공유 개인키를 통해 복호화하여 등록된 기기임을 확인하면, N_2 기기에게 일대일키 설립에 사용할 N_1 기기의 특정 Response 값을 N_2 기기의 개인키로 암호화하여 전송한다. N_1 기기에게도 동일한 절차에 의해 일대일키 설립에 사용할 N_2 기기의 특정 Response 값을 개인키로 암호화하여 전송한다. 관리서버로부터 상대 기기의 Response 값이 포함된 메시지를 수신한 기기들은 자신의 개인키로 복호화한 후 일대일키를 각자 설립한다. 각 기기에서의 일대일키 설립이 완료되면 N_2 기기는 일대일키 설립이 안전하게 완료되었는지를 확인할 목적으로 상호인증을 시도한다. 생성된 일대일키를 이용하여 N_1 기기의 Response 값에 대한 해시값을 암호화하여 보낸다. N_2 기기로부터 메시지를 수신한 N_1

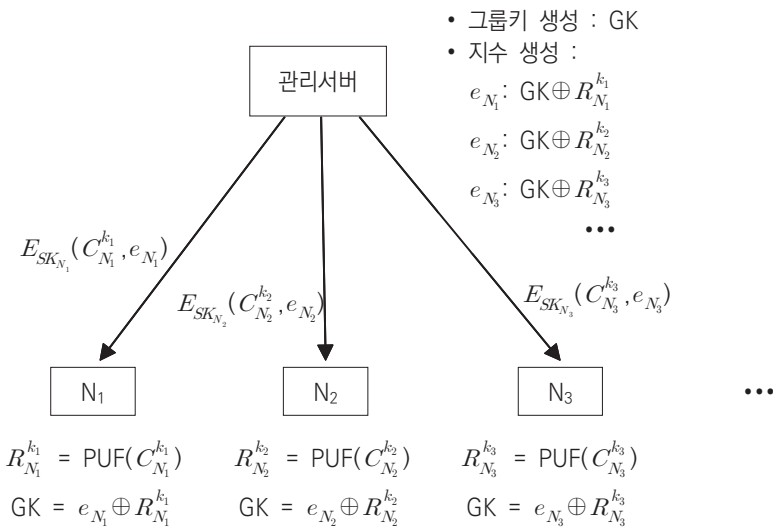
기기는 복호화에 성공하고 해시값 검증이 완료되면 일대일키 설립이 완료되었음을 알리는 ACK 메시지를 일대일키로 암호화하여 N_2 기기에게 전송함으로써 일대일키 설립이 완료된다.

라. 그룹 비밀통신을 위한 그룹키 생성

부대 관리서버가 관리하는 모든 사물인터넷 기기들이 공통적인 명령을 수신해야 하거나 상황인식을 공유하기 위해 특정 정보를 전체에게 전파해야 할 경우에 사용하는 그룹키는 <그림 8>에서 보는 바와 같은 절차에 의해 설립된다.

먼저 관리서버는 전체 기기가 공유할 그룹키 GK를 생성하고, 이어서 각 기기에서의 그룹키 생성에 사용될 지수 정보를 생성한다. 각 기기의 CRP 테이블에서 임의의 Response 값을 선택하여 그룹키와 XOR 연산한 후 생성된 지수 정보를 생성하고, 지수 정보 생성 시 사용된 Response 값에 대응되는 Challenge 값과 함께 각 기기와 공유하고 있는 개인키를 이용 암호화하여 전송한다.

개별 기기에서는 관리서버로부터 전송받은 메시지를 복호화한 후, Challenge 값을 이용하여 그룹키 생성에 사용할 Response 값을 생성한다. 그리고 함께 전송받은 지수 정보와 XOR 연산하여 그룹키를 개별적으로 생성한다. 이러한 과정을 거치면 관리서버 관할 하에 운용되는 모든 기기들은 그룹키 GK를 공유하게 된다.



<그림 8> 그룹키 설립 절차

이상과 같은 절차를 거쳐 설립된 개인키와 일대일키, 그리고 그룹키를 향후 상황 및 목적에 맞게 사용하면 국방 사물인터넷 환경에서 소통되는 모든 통신과 정보를 안전하게 보호할 수 있다.

기존 사물인터넷을 위해 제안되었던 기존 접근방법들은 대부분 공개키와 대칭키 암호를 동시에 사용하기 때문에 연산능력이 제한되는 사물인터넷 기기에 적용하는 것이 쉽지 않다. 또한 공개키의 유효성을 검증하기 위한 인증서버가 항상 온라인에 존재해야만 정상적인 동작이 가능하다. 그러나 본 연구에서 제안하는 접근방법은 칩 수준에서 생성되는 유일한 정보를 이용하여 상황과 목적에 맞게 사용할 수 있는 대칭키를 간단한 연산만을 사용하여 설립할 수 있기 때문에 자원제한적인 특성을 가지는 사물인터넷 기기에 적용하는 것이 전혀 문제가 없다.

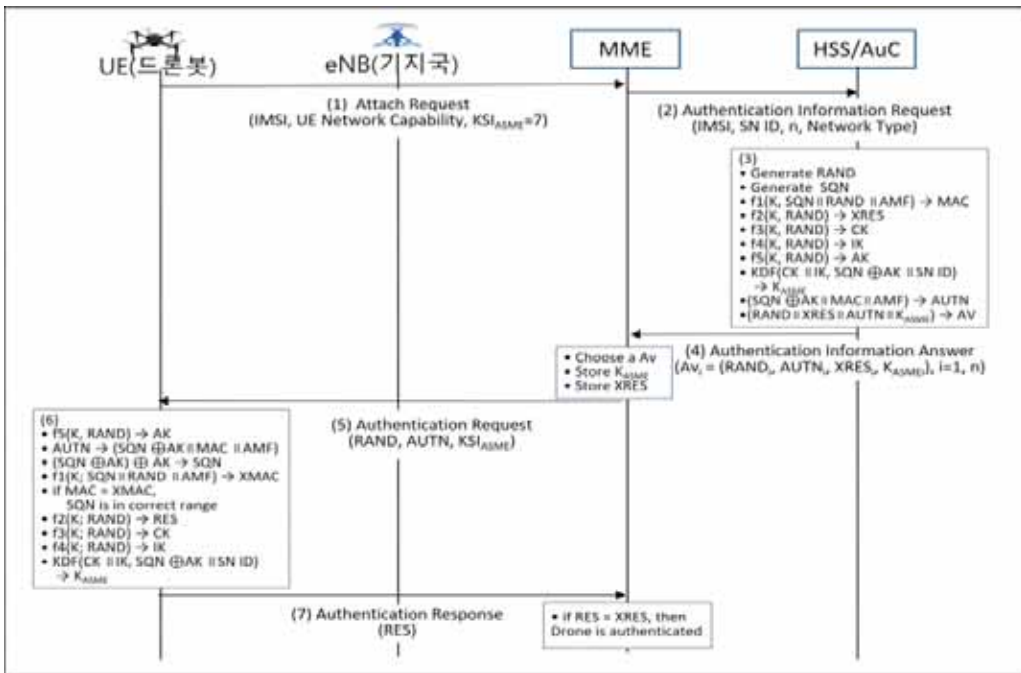
대칭 비밀키의 생성에 있어서도 제안하는 기법은 모든 비밀키가 개별 기기에서 유일하게 생성할 수 있는 PUF의 Response 값을 활용하여 직접 생성하기 때문에 비밀키의 노출을 원천적으로 배제할 수 있고, 공격자가 전송되는 정보를 이용하여 비밀키를 생성하는 것도 불가능하기 때문에 안전성 측면에서 기존 접근방법들보다 월등하게 우수하다고 할 수 있다.

2. PUF를 이용한 드론봇 전투체계 사이버보안 강화 방안

■ 4G LTE 기반 드론봇 전투체계에서의 인증 강화 방안

4G LTE 네트워크를 기반으로 드론봇 전투체계가 운용됨을 가정할 때, 드론봇은 지상 통제소와의 통신을 개시하기 위해 먼저 <그림 9>에서 보는 바와 같은 상호인증 및 키 합의 절차를 수행해야만 한다.¹⁵³⁾ 이 때 드론봇은 4G LTE 네트워크에서 주로 사용되는 개인용 스마트폰과 동일한 방식으로 네트워크 접속을 시도하기 위해 부대 도입 후 등록 과정에서 LTE K와 IMSI(International Mobile Subscriber Identity)가 저장된 USIM(Universal Subscriber Identity Module)을 장착한다. 그리고 해당 정보는 LTE 네트워크에서 직접 인증을 담당하는 HSS/AuC(Home Subscriber Server/Authentication Center)에도 등록된다.

153) 정진우, 이수진, "LTE 기반 드론봇 전투체계를 위한 PUF를 활용한 개선된 인증 및 키합의 절차", 군사과학기술학회 추계학술대회, 2018.



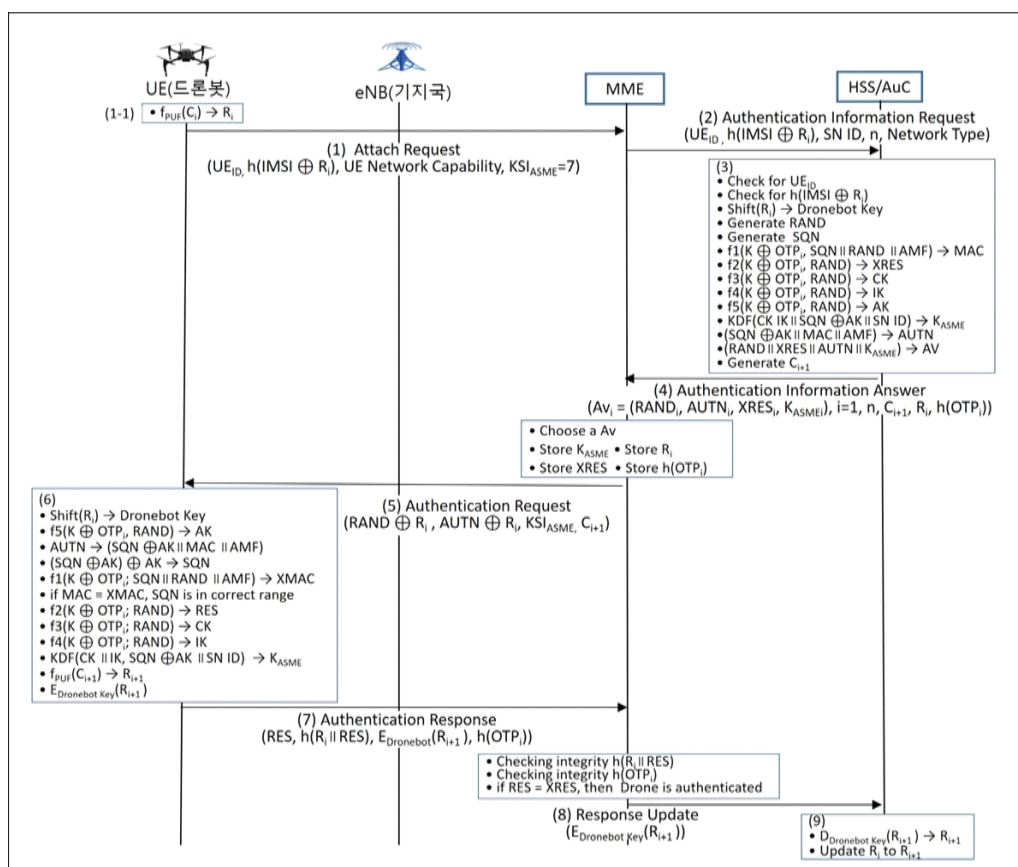
〈그림 9〉 4G LTE 네트워크 기반의 드론봇 인증 절차

도입 후 등록이 완료된 드론봇이 LTE 네트워크에 접속하기 위해 최우선적으로 실시되는 인증과정에서 발생 가능한 보안취약점과 사이버공격은 다음과 같이 정리할 수 있다.

우선 4G LTE 네트워크에서는 USIM에 저장된 IMSI가 드론봇을 구별하기 위한 유일한 식별자로 사용되고, 차후 인증에 사용되는 모든 비밀키는 USIM에 저장된 LTE-K를 이용하여 추가로 생성한다. 따라서 드론봇에 장착된 USIM을 물리적으로 탈취하거나 복제할 경우 아군이 드론봇 전투체계 네트워크에 정상적인 드론봇으로 가장하여 접속할 수 있게 된다. 그리고 동일한 USIM을 두 대의 드론봇이 동시에 사용하는 상황에서 지상의 통제소가 탈취 사실을 제대로 인지하지 못할 경우에는 동일한 ‘경쟁조건에 의한 공격’까지도 수행 가능하다. 둘째, 드론봇이 MME (Mobility Management Entity)에게 ‘Attach Request’ 메시지를 전달하는 과정에서 드론봇의 IMSI가 평문으로 무선을 통해 전송됨으로 인해 도청 등에 의해 손쉽게 노출될 수 있다. 셋째, USIM에 저장된 LTE-K가 인증과정 전반에 걸쳐 계속해서 사용되기 때문에, 유출 및 노출 위험이 상존한다. 그리고 LTE-K가 노출될 경우에는 이후 진행되는 모든 인증과정을 무력화시킬 수 있다. 넷째, HSS/AuC에서 생성한 인증벡터(Authentication Vector, 이하 AV)를 MME에서 전송하는 과정(절차 ④)에서 K_{ASME} 가 IMSI와 연계되지 않고 전송되기 때문에, 드론봇에 잘못된 보안키가 연결

될 가능성도 존재한다. 다섯째, MME가 HSS/AuC로부터 전송받은 AV 중 하나를 선택하여 Authentication Request 메시지로 드론봇에 전송하는 과정((절차 ⑤)에서 RAND와 AUTN이 평문으로 전달되기 때문에 탈취하여 재전송공격을 수행할 수 있다. 여섯째, 인증이 실패할 경우 전송하는 'Authentication Failure' 메시지를 탈취하여 재전송함으로써 드론봇 전투체계 네트워크 내에 존재하는 모든 드론봇의 IMSI와 위치 정보를 수집할 수도 있다.

이상과 같은 4G LTE 네트워크의 문제점을 해결하기 위해 제안하고자 하는 PUF 기반의 개선된 인증 절차는 <그림 10>에서 보는 바와 같다. 제안하는 개선된 인증 절차에서는 일회용 비밀번호를 생성할 수 있는 OTP를 추가로 활용한다.¹⁵⁴⁾



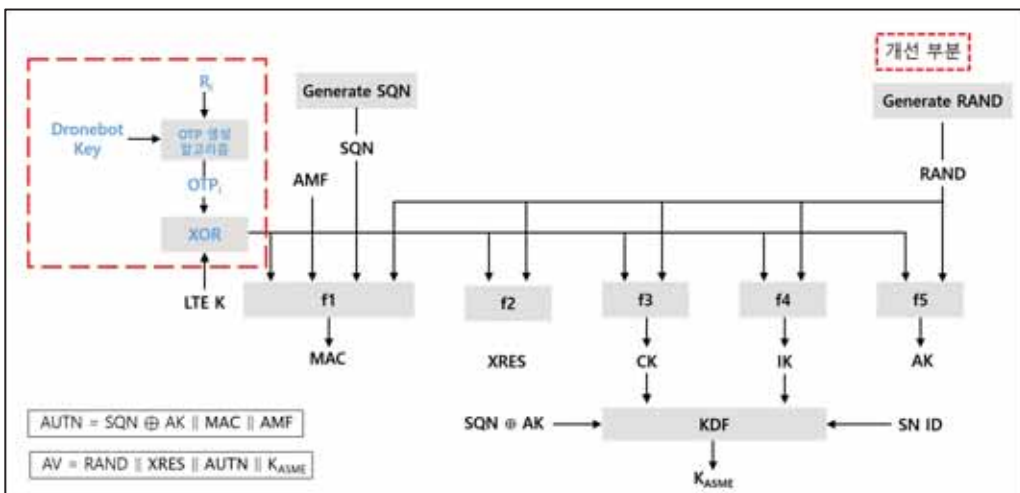
<그림 10> PUF와 OTP 기반의 개선된 인증 절차

154) 제안하는 기법은 2020년 4월 한국통신학회 논문지 게재된 공동연구논문의 내용을 제정리한 것임.(윤상열, 이수진, "PUF-OTP를 활용한 LTE 기반 드론봇 전투체계의 인증 강화방안", 한국통신학회 논문지 45(4), pp. 756-766, 2020. 4.)

드론봇을 HSS/AuC에 등록하는 절차는 기존 LTE 네트워크에서의 절차와 동일하며, 드론봇에 장착한 PUF를 이용하여 생성한 Response 값 R_0 과 드론봇에 부여된 고유 식별자인 UEID를 추가로 등록한다. 개별 드론봇에는 인증을 처음 실시할 때 사용할 Challenge 값 C_0 만을 저장한다.

인증 준비 단계에서 드론봇은 필드 배치 전 저장한 Challenge 값 C_0 를 이용하여 Response 값 R_0 를 생성한다.(1-1) 그리고 UEID와 IMSI 및 R_0 를 XOR 연산한 값의 해시값을 포함하는 Attach Request 메시지를 생성하여 MME로 전송한다.(1) 드론봇으로부터 Attach Request 메시지를 전송받은 MME는 Authentication Information Request 메시지를 생성하여 HSS/AuC로 전송한다.(2)

MME로부터 드론봇 인증에 필요한 정보를 요청받은 HSS/AuC는 해당 드론봇이 정당한 드론봇인지를 확인하기 위해 UEID와 해시값을 검증한다. 이어서 R_0 에 대해 시프트(Shift) 연산을 수행하여 OTP 입력으로 사용할 드론봇 키(Dronebot Key)를 생성한다.(3) 이러한 과정을 거쳐 생성된 드론봇 키를 이용하여 HSS/AuC에서 키를 생성하는 절차는 <그림 11>에서 보는 바와 같다. 기존 인증 절차에서는 LTE-K가 계속적으로 사용되어 노출 위험이 상존하였으나, 제안하는 개선된 절차는 인증이 실시될 때마다 변경된 값을 이용하여 키를 생성하기 때문에, 단일 키의 장기적인 사용에 의해 키 노출 위험을 사전 배제할 수 있다.

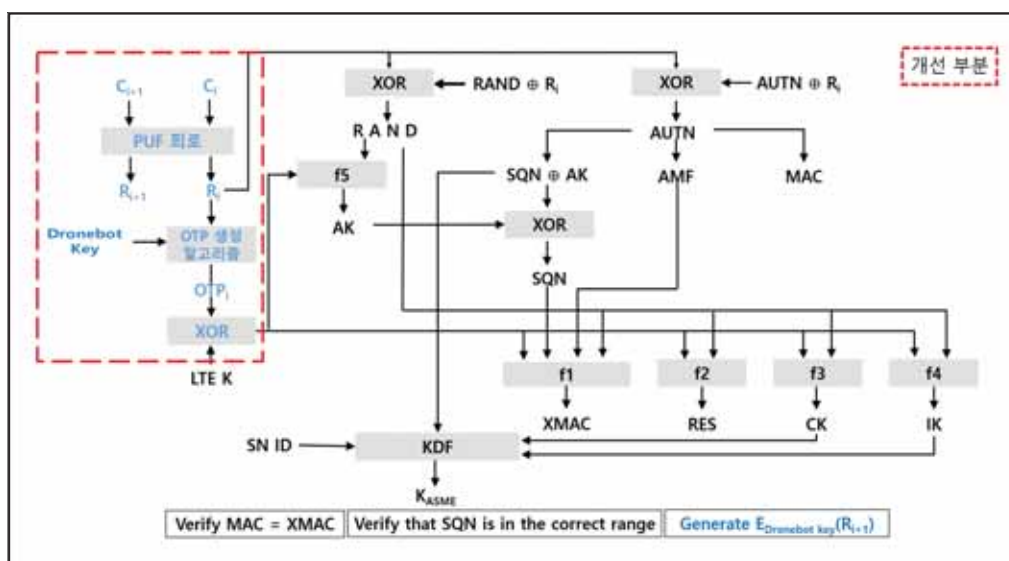


<그림 11> PUF와 OTP를 활용한 개선된 키 생성 절차

HSS/AuC는 인증 벡터(AV_i)를 생성하여 MME로 전송한다. 이때 인증 벡터에는 드론봇이 다음 인증과정에서 사용할 Challenge 값 C_1 과 MME에서 드론봇이 사용하는 OTP를

인증하기 위한 해시값 $H(OTP_0)$ 이 포함된다.(4) 인증 벡터들을 전달받은 MME는 그 중 하나의 벡터를 선택하여 벡터에 포함된 정보를 저장한다. 그리고 Authentication Request 메시지를 생성하여 드론봇에게 전송한다. 이 때 드론봇만이 유일하게 생성할 수 있는 Response 값인 R_0 가 RAND 및 AUTN과 XOR 연산 후 메시지에 포함된다.(5)

MME로부터 Authentication Request 메시지를 수신한 드론봇은 전송받은 정보를 활용하여 <그림 12>에서 보는 바와 같은 절차를 통해 인증에 사용할 키를 생성한다.(6) 키 생성을 완료한 드론봇은 RES 등의 인증 정보를 포함하는 Authentication Response 메시지를 생성하여 MME에 전송한다.(7) MME는 HSS/AuC에서 전송받은 R_0 및 RES를 사용하여 드론봇이 전송한 정보에 대한 무결성을 검증한 후, 차후 인증에 사용할 갱신된 Response 값인 R_1 을 암호화하여 HSS/AuC에 전송한다.(8)



〈그림 12〉 PUF와 OTP를 활용하는 드론봇 내에서의 키 생성 절차

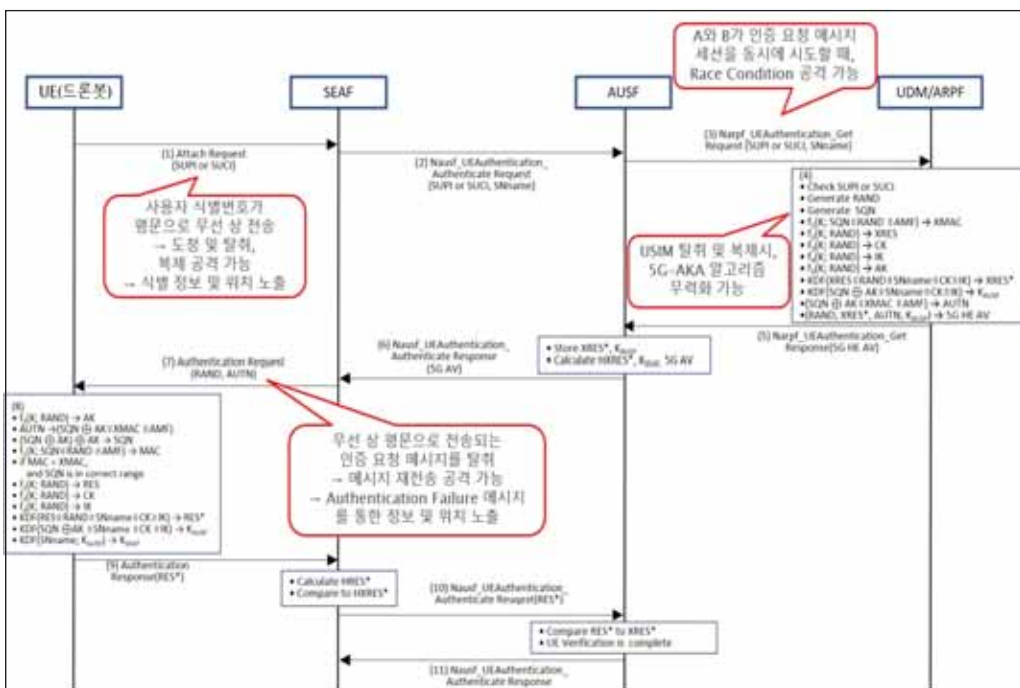
■ 5G 기반 드론봇 전투체계에서의 인증 강화 방안

2020년 상용화되어 본격적인 서비스가 시작된 5G 네트워크는 4G LTE 네트워크보다 20배 이상 빠른 서비스가 가능하며 지연은 120배 이상 감소하여, 향후 다양한 응용 분야에서 기반 네트워크로 활용될 것이며, 국방영역에서도 앞서 설명한 국방 사물인터넷 또는 드론봇 전투체계 운용을 위한 기반 네트워크로 활용 가능하다.

5G 네트워크는 4G LTE 네트워크에 비해 사이버보안 측면에서도 많은 부분이 개선되었다. 평문으로 전송되었던 식별자를 암호화하고, 공개키 기반 암호를 추가로 적용하는

등 기존 보안취약점을 제거하기 위해 다양한 노력이 진행되었으나, 현재까지도 기기 인증과 관련된 일부 구간에서의 통신은 여전히 알려진 공격에 취약하다는 문제점을 안고 있다. 본 절에서는 육군의 드론봇 전투체계가 5G 네트워크를 기반으로 운용됨을 가정하고, 발생 가능한 보안취약점을 제거할 수 있는 PUF 기반의 사이버보안 대책을 제안한다.

5G 네트워크를 기반으로 드론봇 전투체계가 운용됨을 가정할 때, 드론봇은 지상통제소와의 통신을 개시하기 위해 먼저 <그림 13>에서 보는 바와 같은 상호인증 및 키 합의 절차를 수행해야만 하며, 인증 과정에서 다양한 보안취약점이 발생할 수 있다.

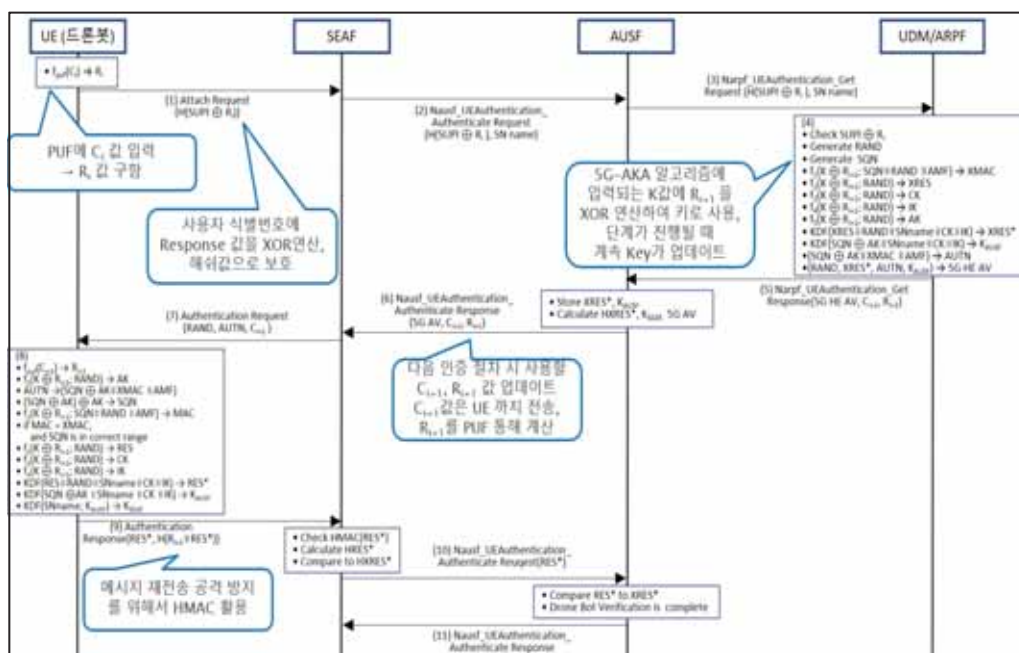


〈그림 13〉 5G 네트워크를 기반으로 한 드론봇 인증 절차 및 보안취약점

전술한 바와 같이 4G LTE 네트워크에서는 IMSI를 무선으로 평문 전송하기 때문에 전송과정에서 노출될 가능성이 상존하였다. 5G 네트워크에서는 이러한 문제를 해결하기 위해 IMSI에 해당하는 SUPI(Subscription Permanent Identifier)를 암호화하여 생성한 SUCI(SUBscription Concealed Identifier)를 전송한다. 그러나 USIM 내부에는 인증 수행에 필요한 모든 정보가 포함되는 것은 동일하기 때문에 USIM 물리적 탈취 및 복제에 의한 인증 과정 무력화는 배제하기 힘들다. 또한 공격자가 인증을 시작하는 드론봇이 SEAF로 전송하는 Attach Request 메시지를 도청하면 SUCI를 획득하는 것도 가능해진다.

이 경우 공격자가 획득한 SUCI를 재전송하면 경쟁 조건이 발생하면서 잘못된 인증 정보가 연결되어 문제가 발생할 수 있다.

Attach Request 메시지를 도청한 공격자는 동일 드론봇이 차후에 인증 요청을 할 경우 위치를 파악할 수 있으며, 'Authentication Request' 메시지를 획득하는 것도 가능해진다. 이런 과정을 통해 획득한 메시지를 인근에 위치한 드론봇에게 재전송할 경우에는 메시지를 수신한 드론봇들이 오류 메시지를 보내게 되고, 공격자는 오류 메시지를 전송한 드론봇들의 위치를 파악할 수 있다. 이러한 문제를 해결하기 위한 PUF 기반의 개선된 인증 절차는 <그림 14>에서 보는 바와 같다.



〈그림 14〉 PUF 기반의 개선된 인증 절차

- 군집드론 운용을 위한 자율통신망 형성 간 PUF 기반의 보안 강화방안

현재 가장 일반적인 형태의 드론 운용 방식은 단독 드론이 지상통제소와 1:1로 통신을 실시하면서 조종하는 방식이다. 그러나 최근 들어 다수 드론을 동시에 운용하는 군집드론의 필요성이 대두되면서, 군집드론 운용을 위한 통신방식에 대한 연구가 활발하게 진행되고 있다.

군집드론 운용을 위해서는 기존 지상통제소에서 개별 드론을 통제하던 방식에서 벗어나 드론들이 상호 자율적으로 네트워크를 구성하고 통신을 수행하는 자율통신망의 구성이

필요하며, 최근 그 대안으로 떠오르고 있는 기술이 바로 FANET (Flying Ad Hoc Networks) 기술이다. 본 절에서는 FANET 기술을 기반으로 군집드론을 운용함에 있어 네트워크에 참여하는 드론들이 안전하게 자율통신망을 구성할 수 있도록 보장하기 위해 PUF 기술을 적용한 안전한 라우팅 프로토콜을 제안하고자 한다. 대상이 되는 라우팅 프로토콜은 FANET 환경에서 활용되는 대표적인 Reactive 방식의 라우팅 프로토콜인 AODV와 DSR 프로토콜로 설정하였다.

가. PUF 기반의 안전한 AODV 라우팅 프로토콜¹⁵⁵⁾

제안하는 기법을 기술하기 위해 사용되는 표기법은 <표 3>에서 보는 바와 같다. 그리고 드론을 등록하는 과정은 전술한 과정과 유사하다. 생산업체를 통해 PUF가 장착된 드론이 군으로 도입되면 군 인증센터에서는 각 드론에 고유 식별자를 부여하고, 드론별로 1,000개 이상의 Challenge-Response 쌍을 생성하여 CRP 테이블을 구성한다. 드론 운용부대는 인증센터로부터 드론을 인수받으면서 각 드론의 ID와 CRP 테이블을 함께 전달받아 지상통제소(Ground Control Station, 이하 GCS) 내의 안전한 관리서버에 저장한다. 지상통제소는 군집드론에 참여할 드론들을 결정하고, 각 드론별로 Challenge-Response 한쌍을 임의로 선택하여 군집드론용 CRP 테이블을 생성하여 군집드론에 참여하는 모든 드론에 저장한다. 이 때 모든 드론은 자신의 Response 값을 저장하지 않고 Challenge 값만을 저장한 상태에서, 필요한 경우 저장된 Challenge 값을 이용하여 Response 값을 생성한다.

<표 3> 표기법

S	출발지 드론의 IP 주소
D	목적지 드론의 IP 주소
BC_{id}	RREQ 메시지의 식별자
D_i	드론의 고유 식별자
$C_i^{D_i}$	드론 D_i 에 저장된 Challenge 값
$R_i^{D_i}$	드론 D_i 에 저장된 Response 값
s_n	출발지 드론의 시퀀스 번호(Sequence number)

155) 제안 내용은 2020년 9월 한국컴퓨터정보학회 논문지계 게재된 공동연구논문의 내용을 제정리한 것임.
(박윤길, 이수진, “군집드론을 위한 PUF기반의 안전한 FANET 라우팅 프로토콜”, 한국컴퓨터정보학회 논문지 25(9), pp. 81-90, 2020. 9.)

d_n	목적지 드론의 시퀀스 번호(Sequence number)
h	홉 수(Hop Count)
lifetime	설정된 경로의 유효 시간
Key_{D_i, D_j}	드론 D_i 와 D_j 가 사용할 임시 비밀키
ACK	확인 응답 메시지
CRP_{pre}	기존 드론들이 저장하고 있는 CRP 테이블
CRP_{New}	새로운 드론이 추가된 갱신된 CRP 테이블

경로 발견단계에서 경로 탐색을 원하는 드론은 다음과 같은 RREQ(Route Request) 패킷을 생성하여 네트워크 내로 브로드캐스트한다. BC_{id} 는 패킷이 재전송될 때마다 순차적으로 증가한다.

$$\{S, D, BC_{id}, s_n, d_n, h\}$$

원본 AODV 프로토콜의 RREQ 패킷은 어떠한 정보도 보호되지 않은 상태에서 전송되기 때문에, 공격자가 중간에서 시퀀스 번호나 홉수 등의 조작을 통해 경로 설정을 방해하는 것이 얼마든지 가능하다. 그리고 특정 드론의 ID를 가장하여 웜홀 또는 블랙홀을 만들어 패킷을 중간에서 가로채거나 모든 패킷을 거처가게 만드는 것도 가능해진다. 이러한 문제를 해결하기 위해 PUF가 적용되어 개선된 RREQ 패킷은 다음과 같이 구성된다.

$$D_s, \{S, D, BC_{id}, E_{R_i^{D_s}}(s_n, d_n, h)\}$$

최초 경로 발견 과정을 개시한 출발지 드론은 자신의 ID(D_s)와 함께 자신의 Response 값($R_i^{D_s}$)으로 s_n, d_n, h 등의 핵심 정보를 암호화하여 브로드캐스트한다. 이러한 RREQ 패킷을 수신한 중간드론(D_k)은 필드 배치 전에 저장했던 CRP 테이블에서 출발지 드론의 Response 값을 확인하여 암호화된 RREQ 패킷을 복호화한 후 정보의 위변조 여부를 검증한다. 검증 결과 이상이 없으면 홉 수를 증가시킨 후 자신의 Response 값 $R_i^{D_k}$ 로 암호화하여 네트워크로 다시 브로드캐스트한다.

$$D_k, \{S, D, BC_{id}, E_{R_i^{D_k}}(s_n, d_n, h+1)\}$$

경로 발견 단계에서는 RREQ 패킷이 브로드캐스트되지만, 경로 설정 단계에서는 다음과 같은 RREP(Route Reply) 패킷이 발견된 경로를 따라 출발지 드론까지 유니캐스트된다. 유니캐스트되는 RREP 패킷에는 출발지 및 목적지 드론의 IP 주소만 포함되며, 설정되는 경로가 언제까지 유효할지를 결정하기 위한 lifetime이 포함되어 있다.

$$\{S, D, d_n, h, lifetime\}$$

이러한 RREP 패킷 역시도 포함된 정보를 보호할 수단이 강구되어 있지 않기 때문에 각종 위변조 공격에 취약하다. 따라서 RREP 패킷에 대해서는 매 홉마다 임시 세션키를 생성하여 시퀀스 번호와 홉 수 정보를 보호한다. 임시 세션키는 RREP 패킷을 전송하는 드론에서 패킷을 수신받을 드론에게 CRP 테이블에서 선정된 임의의 Challenge 값 3개를 선정하여 전송하고, 수신 드론은 전송받은 3개의 Challenge 값에 대응하는 Response 값 3개를 추출하여 XOR 연산함으로써 생성한다.

$$\{S, D, E_{Key_{D_n, D_k}}(d_n, h), lifetime\}$$

설정된 경로가 통신 장애 또는 중간 드론의 기능 장애 등으로 인해 단절된 경우에는 RERR(Route Error) 패킷이 경로에 포함된 드론들에게 유니캐스트되며, 포함되는 정보는 다음과 같다.

$$\{D, d_{n+1}, h\}$$

RERR 패킷의 경우에도 공격자에 의해 위변조됨으로써 정상적인 드론들 간의 연결을 강제로 종료시키거나 경로 발견 단계를 재수행하도록 강요할 수 있는 정보가 포함되어 있다. 따라서 이러한 정보를 보호하기 위해 수정된 RERR 패킷의 형태는 다음과 같다.

$$\{E_{key_{D_n, D_k}}(D, d_{n+1}, h)\}$$

전장상황에서 소형 드론이 운용되는 도중에 공격자에게 탈취되거나 기능 장애, 배터리 부족 등으로 군집드론에서 제외될 경우에는 차후 원활한 작전수행을 위해 새로운 드론을 투입하여 군집드론을 재구성해야 한다. 이 경우 신규 드론이 이륙하여 군집드론 네트워크에 자율적으로 참여하는 절차는 다음과 같다.

- ① 군집드론에 포함된 특정 드론 D_d 가 군집드론에서 이탈
- ② D_d 와 인접하여 상황을 관찰할 수 있는 드론 D_3 이 D_d 의 갑작스러운 이탈로 인한 경로단절을 인지하고, RERR 패킷을 경로상의 모든 드론에게 전송
- ③ 지상통제소에서는 D_d 를 대체할 신규 드론 D_{41} 을 준비하고, 임무를 수행 중인 기존 드론들이 저장하고 있던 CRP 테이블(CRP_{pre})에 D_{41} 의 CRP를 추가한 CRP_{New} 를 생성 및 저장시킨 후 이륙시켜 군집드론에 합류. 이 때 군집드론에서 이탈한 D_d 의 CRP는 차후 임무 복귀시를 대비해 삭제하지 않고 그대로 저장하여 유지한다.
- ④ D_{41} 은 CRP_{pre} 테이블에 저장되어 있는 모든 Response 값을 XOR 연산하여 임시 세션키 $E_{key_{41}} = R_{20}^{D_s} \oplus R_7^{D_1} \oplus \dots R_1^{D_{40}}$ 을 생성하고, 생성된 세션키를 이용하여 CRP_{New} 테이블을 암호화한 후 전체 드론에게 브로드캐스트한다.
- ⑤ 암호화된 새로운 CRP 테이블을 수신한 각 드론은 자신의 CRP 테이블에 저장된 모든 Response 값과 자신의 Responsr 값을 XOR 연산하여 임시 세션키를 생성한 후 수신한 새로운 CRP 테이블을 복호화하여 저장한다.

제안하는 PUF 기반의 안전한 AODV 라우팅 프로토콜에서 CRP 테이블은 아주 중요한 역할을 담당하기 때문에 안전하게 보호되어야 한다. 일반적으로는 CRP 테이블은 공개키 암호를 사용하여 암호화하는 방법도 고려해 볼 수 있지만, 자원이 제한되는 소형 드론의 특징 상 공개키 암호에 의한 보호는 과도한 오버헤드를 발생시키고, 드론의 배터리 사용 시간을 감소시킬 수 있다. 따라서 CRP 테이블 역시도 PUF의 Response 값을 이용하여 암호화한다. 각 드론은 자신의 Challenge 값을 가지고 있기 때문에, 해당 Challenge 값을 이용하여 생성된 Response 값을 이용하여 대칭키 암호 기반으로 CRP 테이블을 암호화하여 보호할 수 있다. 그리고 공격자가 드론 탈취 후 PUF에 Challenge 값을 강제로 주입하여 Response 값을 추출하고자 할 경우 방어할 수 있는 기법은 이미 상용화되어 있기 때문에, 물리적으로 복제가 불가능하고 임의 생성도 불가능한 Response 값을 이용한 CRP 테이블 암호화는 충분한 보호대책으로 작용할 수 있다.

나. PUF 기반의 DSR 라우팅 프로토콜

DSR 라우팅 프로토콜의 경로 발견단계에서 출발지 드론(D_s)은 자신의 라우트 캐시에서 목적지 드론 D_d 에 대한 경로를 검색하고, 경로가 존재할 경우에는 해당 경로를 활용하여 패킷 전송을 실시한다. D_d 까지의 경로가 라우트 캐시에 존재하지 않을 경우 D_s 는 RREQ 패킷에 자신의 주소를 추가한 후 전체 드론(D_i)에게 브로드캐스트한다. 이를 수신한 중간 드론 D_i 들은 라우트 캐시 내에 D_d 까지 경로가 존재할 경우 해당 경로를 추가하여 D_s 에게 RREP 패킷을 전송한다. 경로가 존재하지 않으면 RREQ 패킷에 자신의 주소를 추가하여 다음 D_i 에게 전달한다. 이러한 과정을 통해 전달되는 DSR 라우팅 프로토콜의 RREQ 패킷 구성은 다음과 같다.

$$D_s, (Type(RREQ), S, D, U_{id}, Path)$$

암호화 또는 어떠한 보호대책도 적용되지 않은 RREQ 패킷을 AODV 라우팅 프로토콜에서와 마찬가지로 각종 위변조 공격에 취약하다. 따라서 전송되는 정보를 보호해야 하며, PUF를 적용하여 수정한 RREQ 패킷의 구성은 다음과 같다.

$$D_s, [Type(RREQ), S, D, E_{R_i^{D_s}}(U_{id}, Path)]$$

RREQ 패킷을 수신한 D_d 는 $Path$ 에 저장된 모든 D_i 의 주소를 자신의 라우트 캐시에 저장하고, 해당 경로로 D_s 에게 RREP 패킷을 전송한다. 패킷은 RREQ 패킷 구성과 동일하며, $Type$ 이 RREP로 변경된다. RREP 패킷 전송 시 D_d 는 특정 $C_i^{D_d}$ 에 대한 고유한 $R_i^{D_d}$ 값들을 활용하여 이전 홉 드론과 임시 세션키를 설립한 후 $U_{id}, Path$ 을 암호화하여 다음과 같이 전송한다.

$$[Type(RREP), S, D, E_{key_{D_d, D_s}}(U_{id}, Path)]$$

경로 관리단계에서 중간 드론에 의해 전송되는 RERR 패킷의 구성은 다음과 같으며, 이러한 RERR 패킷 역시도 앞서 설명한 절차와 동일한 임시 세션키 설립 과정을 거친 후 생성된 세션키를 이용하여 암호화한다.

$$D_i, \{Type(RERR), S, D, U_{id}, Path\} \Rightarrow [Type(RREP), S, D, E_{key_{D_d, D_s}}(U_{id}, Path)]$$

라우팅 프로토콜의 보안을 위해 제시된 기존 대책들은 대부분 자원이 제한되는 드론에 적용하기에는 다소 무리가 따르는 공개키 암호를 기반으로 하고 있다. 또한 대칭키도 병행하여 적용하고 있기는 하지만, 대칭키를 설립하는 과정에서 비밀키가 노출될 가능성이 상당히 높다. 그러나 PUF 기반의 대책은 경량화된 대칭키 암호만을 사용하며, 생성되는 비밀키가 노출될 가능성은 없다. 따라서 소형 드론에 적용하기에 적합한 사이버보안 대책이라고 할 수 있다.

V. 결론

국방에서의 사이버보안 구현은 현재까지 소프트웨어를 중심으로 진행되어 왔고, 하드웨어를 기반으로 하는 사이버보안 구현에 대해서는 크게 논의된 바가 없었다. 그러나 암호를 비롯한 소프트웨어 기반의 사이버보안 도구들은 최근 들어 다양한 사이버위협에 직면하면서 한계를 보이고 있으며, 그러한 한계를 극복하기 위해서 하드웨어 기반의 사이버보안 구현이 주요 연구주제로 부각되고 있다.

본 연구에서는 다양한 하드웨어 기반 사이버보안 기술 중 물리적 복제 방지 기술로 지칭되는 PUF 기술을 중심으로 국방영역에 하드웨어 기반 사이버보안 기술을 적용하는 방안을 제시하였다. PUF 기술의 적용을 통해 사이버보안을 강화할 수 있는 대상으로는 비교적 경량화된 사이버보안 기술의 적용을 필요로 하는 국방 사물인터넷과 드론봇 전투체계를 선정하였다.

국방 사물인터넷은 현재 제반 전장 요소들을 모두 포함하는 IoBT의 개념으로 확장되고 있는 추세이며, 하드웨어 기반의 사이버보안 적용이 가장 필요한 영역이다. 이에 본 연구에서는 PUF 기술을 기반으로 국방 사물인터넷 환경에서 안전한 통신 채널을 구성할 수 있는 방안을 제시하였다. 드론봇 전투체계는 4G 및 5G 상용 기술을 기반으로 운영됨을 전제하고, 기존 상용 통신망이 가지고 있는 취약점을 해결하기 위한 PUF 적용 방안을 제시하였다. 또한 최근 필요성이 증대되고 있는 군집드론을 효율적으로 운용하기 위해서는 안전한 자율통신망 형성이 필수적임을 고려하여, FANET 환경에 적용되는 대표적인 라우팅 프로토콜의 보안성을 강화하는 방안을 제안하였다.

본 연구는 국방영역에서 하드웨어 기반 사이버보안 기술 적용 가능 분야를 식별하고, 개략적인 적용방안을 도출하는데 중점을 두었기 때문에, 제시된 사이버보안 대책을 적용하기 위해서는 추가적인 연구가 필요하다. 그러나 하드웨어 기반의 사이버보안 구현은 선택이 아닌 필수로 전환되고 있다. 따라서 본 연구의 결과를 바탕으로 국방영역에서도 하드웨어 기반 사이버보안 기술에 대한 연구가 보다 활발하게 진행되기를 기대해 본다.

〈참고 문헌〉

- 이종훈, 박정수, 정승욱, 정수환, “PUF 기반의 보안 USB 인증 및 키 관리 기법”, 한국통신학회논문지 Vol.38B, No.12, 2013.
- 변진욱, “PUF 기반 RFID 인증 프로토콜의 효율적설계에 관한 연구,” 정보보호학회논문지, 제 24권, 제5호, pp. 987-999, 2014.
- 백종학, 신광조, “PUF 기술을 활용한 보안칩 기술 개발과 그 응용 분야,” 전자공학회지, 7월, 2016.
- 정진우, 이수진, “LTE 기반 드론봇 전투체계를 위한 PUF를 활용한 개선된 인증 및 키합의 절차”, 군사과학기술학회 추계학술대회, 2018.
- 임순일, “Enhancing reliability of Physically Unclonable Function (PUF) using counter” 성균관대학교 석사학위논문, 2018.
- 정진우, 이수진, “5G 인증 및 키합의 프로토콜(5G-AKA)의 보안취약점과 PUF 기반의 보안성 향상 방안”, 융합보안논문지, 19(1), pp. 3-10, 2019.
- 김수민, 이수진, “M-IoT 환경에서 PUF 기술을 활용한 안전한 통신채널 구성 기법”, 융합보안논문지, 19(5), pp. 107-118, 2019.
- 윤상열, 이수진, “UF-OTP를 활용한 LTE 기반 드론봇 전투체계의 인증 강화방안” 한국통신학회 논문지 45(4), pp. 756-766, 2020.
- 박윤길, 이수진, “군집드론을 위한 PUF기반의 안전한 FANET 라우팅 프로토콜”, 한국컴퓨터정보학회 논문지 25(9), pp. 81-90, 2020.
- P. Kocher, J. Jaffe, and B. Jun, “Introduction to Differential Power Analysis and Related Attacks,” Cryptography Research, 1998.; P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” Advances in Cryptology – CRYPTO ‘99, 1999.
- Z. Shen and X. Wu, “An Improved Security Method for Mobile Agent System by Using Trusted Computing Platform,” International Conference on Intelligent Computation Technology and Automation, 2010.
- A. P. Fournaris, “Toward Flexible Security and Trust Hardware Structures for Mobile-Portable Systems,” IEEE Latin American Transactions, Vol. 10, No. 3, 2012
- H. Ju, Y. Kim, Y. Jeon and J. Kim, “Implementation of a Hardware Security Chip for Mobile Devices,” IEEE Transactions on Consumer Electronics, Vol. 61, No. 4, 2015.

- A. Maruaisap and P. Kumhom, "A Hardware-Based Security Scheme for In-Vehicle CAN," International Computer Science and Engineering Conference (ICSEC), 2016.
- J. Milosevic, A. Ferrante and F. Regazzoni, "Security Challenges for Hardware Designers of Mobile Systems," Mobile Systems Technologies Workshop, 2015.
- S. Ray and J. Bhadra, "Security Challenges in Mobile and IoT Systems," 29th IEEE International System-on-Chip Conference (SOCC), 2016.
- A. Syed and M. Lourde R., "Hardware Security Threats to DSP Applications in an IoT network," IEEE International Symposium on Nanoelectronic and Information Systems, 2016.
- M. A. Bahnasawi, Kh. Ibrahim, A. Mohamed, M. Kh. Mohamed, A. Moustafa, K. Abdelmonem, Y. Ismail and H. Mostafa, "ASIC-Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications," 28th International Conference on Microelectronics (ICM), 2016.
- A. Pouraghily, T. Wolf and R. Tessier, "Hardware Support for Embedded Operating System Security," IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2017
- L. Fiorin, A. Ferrante, K. Padarnitsas and F. Regazzoni, "Security Enhanced Linux on Embedded Systems: a Hardware-accelerated Implementation," 17th Asia and South Pacific Design Automation Conference, 2012.
- X. Wang, Q. Shen, P. Du, R. Zhang, W. Wang, L. Li, B. Xu and H. Ji, "Hardware-Assisted Monitoring for Code Security in Embedded System," IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing, 2015
- S. Lukacs, A. V. Lutas, D. H. Lutas and Gh. Sebestyen, "Hardware Virtualization Based Security Solution for Embedded Systems," IEEE International Conference on Automation, Quality and Testing, Robotics, 2014.
- S. Kan, M. Ottavi and J. Dworak, "Enhancing Embedded SRAM Security and Error Tolerance with Hardware CRC and Obfuscation," IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), 2015.

- T. Wiersema, S. Drzevitzky and M. Platzner, "Memory Security in Reconfigurable Computers: Combining Formal Verification with Monitoring," International Conference on Field-Programmable Technology, 2014.
- M. Neagu and Gh. Sebestyen, "Increasing Memory Security through Data Scrambling and Information Entropy Models," 15th IEEE International Symposium on Computational Intelligence and Informatics, 2014.
- G. Gayathri, T. Thangam, M and Kashuri, "An Efficient Logic Obfuscating Strategy for Hardware Security Using SIC Generator," International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.
- K. Shamsi, W. Wen and Y. Jin, "Hardware Security Challenges Beyond CMOS: Attacks and Remedies," IEEE Computer Society Annual Symposium on VLSI, 2016.
- J. Dofe, Q. Yu, H. Wang and E. Salman, "Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs," International Great Lakes Symposium on VLSI (GLSVLSI), 2016.
- P. Gu, Sh. Li, D. Stow, R. Barnes, L. Liu, Y. Xie and E. Kursun, "Leveraging 3D Technologies for Hardware Security: Opportunities and Challenges," International Great Lakes Symposium on VLSI (GLSVLSI), 2016.
- E. Moghaddam, N. Mukherjee, J. Rajske, J. Tyszer, J. Zawada, "On Test Points Enhancing Hardware Security," IEEE 25th Asian Test Symposium, 2016.
- D. Fujimoto, M. Nagata, Sh. Bhasin, J. Danger, "A Novel Methodology for Testing Hardware Security and Trust Exploiting OnChip Power Noise Measurement," The 20th Asia and South Pacific Design Automation Conference, 2015.
- C. W. O'Donnell, G. E. Suh, and S. Devadas, "PUF Based Random Number Generation," MIT CSAIL CSG Technical Memo 481, 2004.
- J. Zhang, B. Qi, and G. Qu, "HCIC: Hardware-assisted Control-flow Integrity Checking," IEEE Internet of Things Journal, pp. 1-14, 2018.
- W. Liang, "Study on PUF based secure protection for IC design", Microprocessors and Microsystems, Vol.45, pp. 56-66, 2016.
- B. Habib, "A comprehensive set of schemes for PUF response generation", Microprocessors and Microsystems, Vol.51 pp. 239-251, 2017.
- M. Barbareschi, "A PUF-based hardware mutual authentication protocol", J. Parallel Distrib. Comput. 11(9), pp. 107-120, 2018.

- Paik Jong Hak, "Development of Secure Chip Technology Using PUF Technology and Its Applications", *The Magazine of the IEEE* 43(7), pp. 59-67, 2016.
- Jae-min Choi, "Design and Implementation of a Low Power Chip with Robust Physical Unclonable Functions on Sensor Systems", *Journal of Sensor Science and Technology* Vol. 27, No. 1, pp. 59-63, 2018.
- ISO/IEC 2nd CD 20897-1, July 2018.
- C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial", *Proceedings of the IEEE*, Vol. 102, No. 8, August 2014.
- P. Layman, S. Chaudhry, J. G. Norman, and J. R. Thomson, "Electronic fingerprinting of semiconductor integrated circuits," (6,738,294), September 2002.
- C. Brzuska, M. Fischlin, H. Schroder and S. Katzenbeisser, "Physical Unclonable Functions in the Universal Composition Framework," *CRYPTO* 2011.
- U. Ruhrmair, H. Busch and S. Katzenbeisser, "Strong PUFs: Models, Constructions and Security Proofs. In A.-R. Sadeghi, P. Tuyls (Editors): *Towards Hardware Intrinsic Security: Foundation and Practice*," Springer, 2010.
- U. Ruhrmair, S. Devadas and F. Koushanfar, "Security based on Physical Unclonability and Disorder," In M. Tehranipoor and C. Wang (Editors): *Introduction to Hardware Security and Trust*. Springer, 2011.
- U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas and J. Schmidhuber, "Modeling Attacks on Physical Unclonable Functions," *ACM CCS* 2010.
- U. Ruhrmair, J. Solter and F. Sehnke, "On the Foundations of Physical Unclonable Functions," *Cryptology ePrint Archive*, 2009:277, 2009.
- U. Ruhrmair, J. Solter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson and S. Devadas, "PUF Modeling Attacks on Simulated and Silicon Data," *IEEE Transactions on Information Forensics and Security (IEEE T-IFS)*, 2013.
- ICTK, KR open patent, 10-2013-0019 358, 2013. 2.
- W. Liang, "Study on PUF based secure protection for IC design", *Microprocessors and Microsystems* Vol. 45, pp. 56-66, 2016.
- B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Security (CCS)*, pp. 148-160, 2002.

- U. Ruhrmair, S. Devadas and F. Koushanfar, "Security based on physical unclonability and disorder," Introduction to Hardware Security and Trust, M. Tehranipoor and C. Wang, Eds. New York, NY, USA: Springer-Verlag, pp. 65-102, 2012.
- Y. Alkabani, F. Koushanfar, N. Kiyavash, and M. Potkonjak, "Trusted integrated circuits: A nondestructive hidden characteristics extraction approach," Lecture Notes in Computer Science, Springer-Berlin, vol. 5284, pp. 102-117, 2008.
- J. Bringerr, H. Chabanne, T. Icart, "On physical obfuscation of cryptographic algorithms," vol. 5922 of Lecture Notes in Computer Science, Springer-Verlag, pp. 88-103, 2009.
- S. Park, S. Lim, D. Jeong, J. Lee, J. Yang, H. Lee, "PUFSec: Device Fingerprint-based Security Architecture for Internet of Things," In Proceedings of the IEEE Conference on Computer Communications, Atlanta, GA, USA, 1-4, pp. 1-9, May 2017.
- M. Huang, B. Yu, and S. Li, "Puf-assisted group key distribution scheme for software-defined wireless sensor networks," IEEE Communications Letters, Vol 22, no.2, pp. 404-407, 2018.
- T. Gu, P. Mohapatra, "BF-IoT: Securing the IoT Networks via Fingerprinting-Based Device Authentication," In Proceedings of the IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Chengdu, China, pp. 254-262, October 2018.

최신 북한의 미사일 기술진전과 위협

육군협회 연구원 김 황 록

육군협회 연구원 신 동 호

- I. 서론
- II. 최신 북한의 미사일 고도화와 위협 분석
- III. 북한 미사일 위협 종합 및 전망
- IV. 북한 미사일 대응전략
- V. 결론

요 약

김정일 시대는 스커드-B/C, 스커드-ER 및 노동미사일 등 3종을 보유 하였으나, 김정은 시대에는 11종을 새롭게 추가적으로 개발하여 총 14종의 탄도미사일을 보유하게 됐다. 신형 11종은 전략미사일 7종, 전술미사일 4종이다.

전략미사일은 신형 백두산엔진을 자체적으로 개발하여 화성계열 중거리탄도미사일(IRBM)과 대륙간탄도미사일(ICBM)을 완성했으며, 추정 다탄두용 화성-16형은 시험발사 이전에 공개했다. 또한 새로운 고체연료와 콜드론칭 기술을 개발하여 수중플랫폼에서의 잠수함발사탄도미사일(SLBM) 비행시험과 지상플랫폼에서의 탄도미사일인 북극성-2형 시험발사에 성공했다. 이어서 북극성-3형 SLBM도 수중바지선에서의 시험발사에 성공(2019.10)했고, 3개 이상의 발사관을 갖춘 신형 3천톤급(북극성-3형)과 4-5천톤급(북극성-4형) 잠수함을 건조 중이다.

전략미사일은 미국의 알래스카, 괌, 하와이는 물론 미 본토를 직접 위협할 수 있는 중·장거리탄도미사일로써 총 7종(화성-12/14/15/추정16, 북극성-2/3형/4형)으로 모두 신형무기체계이다. 이로써 김정은 시대 북한은 미국의 영토와 미국민을 직접 위협 또는 직접 공격할 수 있는 『직접억제력』을 추가로 확보했다.

전술미사일은 3종의 기보유 스커드와 스커드-ER 및 노동미사일에 핵탄두장착 능력과 정확도를 향상시키는 기술 진전(고도화)이 있었으며, 신형 고체연료추진제를 사용하는 4종의 이스칸데르형·에이태킴스형·대구경 및 초대형방사포를 추가로 개발했다. 특히 신형 전술미사일은 스커드와 노동미사일과는 다르게 모두 연속발사가 가능한 다련장이며, Pull-Up 요격회피 비행기술 및 30~50km의 저고도 비행으로 한미의 탐지 및 요격을 어렵게 하는 위협을 가지게 됐다. 이러한 전술미사일은 한국군, 주한미군 그리고 주일미군 및 주일 유엔사 후방기지를 모두 위협할 수 있게 되어 유사시 한국과 일본을 완벽하게 인질로 삼을 수 있는 『간접억제력』을 향상시켰다.

이러한 북한 미사일 위협에 대한 대응방안을 정책적인 방안과 군사적인 방안으로 구분하여 연구하였다.

정책적인 대응으로 먼저, 북핵·미사일 위협 관련 긴밀한 한미정보공조 및 공동정보판단이 필요하다. 북핵·미사일 위협의 실체를 보는 한미의 시각에 차이가 나면 북한과의 비핵화 협상전략에도 균열이 생기기 때문이다. 또한 유사시 한미공동대응태세에 허점이 생겨 북한에게 억제력을 상실하고 도발의 빌미를 제공함은 물론 적시에 대응할 수 없기 때문이기도 하다. 두 번째, 긴밀한 정보공조와 정보판단에 따른 연합대비태세가 유지되어야 하며, 세 번째, 미국의 핵 확장 억제력 강화 및 한미연합첨단전력의 적시적 SC를 실시해야 한다는 점을 제안했다. 북한이 핵 무력을 고도화하는데 성공하고, 고도화된 핵 무력에 대한 과신과 상응하는 요구조건에 대한 불만으로 군사적 행동을 하지 못하도록 하는 지속적인 메시지 전달 노력이 필요하다.

다음은 군사적인 대응방안으로, 첫째, 한미동맹 군사력을 활용한 방법으로 가장 현실적이고 즉각 적용 가능한 방안이다. 이는 핵미사일에 대응 가능한 전략무기를 한반도에 상시 배치하는 방안과 북한 핵 미사일에 대응하기 위해 배치한 사드를 활용하는 방안이다. 추가적으로 고려할 수 있는 방안은 미국의 전술핵 재도입이다. 핵에는 핵으로 북한의 핵 공격을 억제하기 위한 전략으로 북한이 핵으로 대한민국을 공격할 경우, 대한민국에 배치된 미국의 전술 핵무기들에 의해 몇 배의 보복을 당해 결국 북한이 멸망케 된다는 확실한 인식을 심어주어 아예 사용할 생각을 하지 못하도록 하는 것이 근본 목적이다.

둘째, 한국 자체적으로 군사적 대응태세를 갖추는 것이다. 이를 위해 한국군은 전략표적 타격체계를 전력화 중이다. 전략표적 타격체계는 북한의 핵미사일 위협을 단계별로 구분하여 대응하는 체계로 북한의 핵미사일 사용임박 단계 시 선제타격 하겠다는 개념이다. 두 번째는 한국형 미사일 방어체계(KAMD)체계 구축으로, 북한이 미사일을 발사할 경우

패트리어트나 천궁 등을 운용하는 부대에 요격명령을 하달하여 날아오는 미사일을 공중에서 파괴하는 개념이다. 세 번째, 압도적 대응개념은 북한이 금지된 행위를 감행하게 되면 즉각적이고 강력하게 군사적인 응징정보복을 하겠다는 작전개념이다. 마지막으로 스텔스 드론, LAMD, 극초음속 곡사포 등 4차 산업혁명 첨단기술을 적용한 군사력 첨단화 방안을 제시했다.

북한 핵 미사일 위협을 분석하고 대응방안을 연구한 결과, 아래와 같은 시사점을 정리할 수 있었다.

첫째, 핵미사일 체계를 구축한 북한은 한국 및 한국 내 주한미군을 볼모로 하는 간접 억제력으로 군사적 도발을 감행할 가능성이 높다. 그래서 한국과의 관계는 위장평화 및 통일전선 책동에 불과할 수밖에 없다는 것이다. 책임전가와 도발명분을 확보하는데 한국 만큼 호재가 없는 것이 북한의 입장이자 현실이다. 핵무기를 보유한 인도-파키스탄 간 카길 전쟁 같은 우발상황에 대비해야 한다.

둘째, 북한 미사일의 위협에 대응하여 긴밀한 정책적 대응을 해야 한다는 것이다. 군사적 대응은 많은 비용과 희생을 감수해야 하는 최종 선택이며 먼저 정책적으로 국제적인 공조를 통해 북한 핵미사일 개발을 억제하고 핵 기술 유입 루트를 차단하여 스스로 포기하도록 하는 정책이 바람직하다.

셋째, 북한 미사일의 위협에 따른 실질적인 대응 군사력 건설은 아무리 강조해도 지나치지 않다. 북한미사일에 대응하기 위한 전력을 구축하는 마스터플랜을 갖고 추진해 나가야 한다. 최종적으로 결국 북한이 스스로 핵미사일을 포기할 수 있도록 다각적인 노력을 해가야 할 것이다.

I. 서론

제1절 연구배경과 목적

김정은 집권 10여년 사이 북한의 미사일 기술은 급속도로 고도화됐다. 과거 김일성·김정일 시대와 비교 시 김정은 시대 북한의 미사일 기술은 다종화, 정밀화되었으며 핵탄두 투발능력도 갖추게 됐다.

2011년 12월 김정일 위원장의 사망으로 권력을 승계한 김정은은 집권 초기인 2012년

4월 13일 이른바 장거리미사일 발사를 시작으로 2020년 3월까지 약 60여 회 80여 발의 탄도미사일을 발사했고, 특히 스커드급 이상 탄도미사일에는 소형화된 핵탄두를 장착할 수 있을 정도로 기술이 향상됐다.

위협면에서도 김일성·김정일 시대 북한의 미사일은 스커드 및 노동미사일인 단거리탄도미사일(SRBM) 위주 실전사격 능력을 보유했지만 김정은 시대 북한은 중거리탄도미사일(IRBM)과 대륙간탄도미사일(ICBM)을 개발하여 미국의 영토까지 직접 핵탄두를 운반할 수 있는 위협으로 확대됐다고 평가했다.

따라서 본 연구의 목적은 김정은 시대의 미사일 기술 고도화 진전내용과 변화된 위협을 상세하게 분석하여 김정은 시대 북한의 미사일 위협 고도화 전략을 도출함으로써 우리의 대응전략을 점검하는 등 정책적 함의를 제시하는 데 있다.

제2절 연구범위와 방법

1. 연구범위

먼저 본 연구는 북한의 최신미사일 기술 진전과 위협을 분석하기 위하여 첫째, 김정은 시대 전 과정을 망라(2012.1-2020.10)하여 연구기간으로 설정하였다.

둘째, 미사일 기술의 진전 정도는 김정일 시대와 김정은 시대의 차이점 비교를 통해 변화된 정확도와 신형 제원에 기초하여 객관성 있게 분석한다.

셋째, 핵경제 병진노선인 ‘핵 무력 고도화 5개년 계획’을 시작으로 유형별 세 가지 트랙으로 구분하여 북한 미사일 고도화 과정의 특징과 기술 진전을 분석한다.

넷째, 미사일 분류는 북한의 입장에서 전략, 전술 미사일 분류 기준을 적용하여 설명한다.

다섯째, 위협 분석 및 대응전략을 제시하는 것으로 전략 미사일 위협 및 대응 방안은 핵 투발 수단으로서의 능력과 위협으로 위협의 범위 및 피해 효과, 위협별 대응전략을 제시한다. 미사일 위협 분석에 따른 대응전략은 정책적, 군사적인 대응방안을 제시한다.

2. 연구방법 및 구성

본 연구를 진행하는 방법은 북한 언론매체에서 공개한 자료, 국방부, 국방대, 국방과학

연구소 등 군 과 군 출연기관에서 공개한 자료를 이용하였으며, 인터넷, SNS, 클라우드 등 민간 자료를 활용하는 문헌연구 방법을 적용했다.

선행연구에 대한 분석은 학위논문 및 관련 학술지, 정책연구 등에 대한 분석으로 기 제안된 연구에 대한 분석을 하였다. 관계 기관 자문은 군 관련 기관 및 연구소인 ADD, KIDA 등과 민간연구소, 학교, 민간연구단체 등의 공개된 자료와 세미나 등에서 발표된 자료를 활용하였고 한국군의 대응전력 수준 평가를 위해 전문가를 대상으로 하는 SPND 평가 툴을 이용하였다.

본 연구의 구성은 아래의 <표 1-1>과 같다.

<표 1-1> 연구 구성 체계

서 론		
연구배경	연구목적	연구구성
북한의 미사일 기술 분석		
미사일 고도화	전략미사일 기술	전술미사일 기술
미사일 위협종합		
위협 종합		고도화 전략전망
대응전략		
정책적 대응	군사적 대응	대응전략 평가

II. 최신 북한의 미사일 고도화와 위협 분석

제1절 김정은 시대 미사일 고도화 로드맵

북한은 김정은 정권 집권 첫해인 2012년부터 핵무력 고도화를 본격적으로 시작했다. 아래 <그림 2-1>에서 보는 바와 같이 김정은 정권의 북한은 핵무력 고도화를 위한 전략적 구상을 세 가지 트랙으로 설정하고 로드맵을 수립했다.¹⁵⁶⁾



〈그림 2-1〉 김정은 정권의 핵·미사일 고도화 로드맵

먼저 트랙#1은 새로운 백두산엔진을 개발, 화성계열 IRBM 및 ICBM을 완성하는 이른바 5개년개발 기본계획이다. 트랙#2는 새로운 북극성계열 SLBM을 완성하는 계획으로 무기체계 특성상 트랙#1 보다 장기적인 개발계획(약8-10년)이었다. 트랙#3은 새로운 단거리 전술미사일 고도화 계획으로 트랙#1, #2 개발 과정에서 미국의 압박과 제재에 대응하는 역할을 하면서 선(先) 트랙#1 기본계획 완성 이후에 집중적으로 완성하는 개발계획이었다.

김정은은 이러한 전략적 구상을 실현하기 위해 집권 이후 전 국가적 역량을 집중했다. 2013년 3월 당 전원회의에서 ‘경제·핵건설 병진로선’을 채택, 연쇄적인 핵실험으로 핵무기를 소형화하고 다양한 신형 핵탄두(미사일)를 개발하는데 성공함으로써 마침내 2017년 11월 29일 핵무력 완성을 선언했다. 핵무력 완성을 김정은이 선언한 이유는 미 본토를 직접 위협할 수 있는 트랙#1 기본형 개발을 1차적으로 완료하여 핵무력에 의한 대미·대남 직·간접억제력과 협상력이 강화됐다고 판단했기 때문이다. 그 결과 2018년 4월 20일 김정은은 당 전원회의를 개최하여 ‘병진로선’에서 ‘경제총력 집중로선’으로 전략적 전환을 선언하고 고도화된 대미·대남 직·간접 핵·미사일 억제력과 강화된 협상력으로 남북 및 북미 정상회담에 나서게 됐다.

사상 최초의 북미 정상회담은 2018년 6월과 2019년 2월 2회에 걸쳐 성사됐으나, 하노이

156) 본 연구에서 ‘핵무력(핵미사일) 고도화’란 ‘다종의 핵탄두(Pu/HEU)를 소형화하고, 소형화된 핵탄두를 장착할 수 있는 다양한 운반수단인 탄도미사일을 보유한 기술적 진전의 상태’로 정의한다. 단, 탄도미사일 중 신형 전술미사일 4종은 핵탄두 운반능력이 아직 검증되지 않은 것으로 평가했다. 연구목적상 김정은 정권에서 ‘핵무력(핵미사일)’용어는 문맥에 따라 핵탄두 장착이 가능한 운반수단인 ‘미사일’과 같은 의미로도 사용한다.

2차 정상회담에서 협상이 결렬됨에 따라 북핵 비핵화 국면은 교착국면으로 전환됐다. 하지만 하노이 노딜 이후 북한은 그동안 은밀히 진행해왔던 트랙#3을 2019년 5월부터 공개 및 과시했다. 이후 북한은 최소 4종의 새로운 단거리 전술미사일을 2020년 3월말까지 약 11개월 동안 16차례 시험발사를 통해 완성하고, 실전배치에 들어갔다. 트랙#2는 2019년 7월부터 김정은이 현장지도를 통해 신포조선소에서 건조된 대형 3천톤급 잠수함을 공개하면서 신형 전략무기의 전력화가 임박했음을 과시했다. 이러한 신형 전술미사일과 잠수함 건조활동으로부터 북한이 비핵화 협상과정에서도 트랙#2와 트랙#3의 핵투발수단을 지속적으로 고도화한 사실이 확인됐다.¹⁵⁷⁾

제2절 전략미사일 기술 고도화 및 위협

북한은 탄도미사일을 전략미사일(‘전략탄도로켓트’¹⁵⁸⁾)과 전술미사일(‘전술탄도로켓트’)로 분류한다.¹⁵⁹⁾ 전략미사일은 다시 ‘중장거리탄도로켓트’(IRBM)와 ‘대륙간탄도로켓트’(ICBM)로도 구분한다. 김정은 시대 개발한 전략미사일 중 화성계열 미사일은 화성-12/14/15형/추정16형, 북극성계열 미사일은 북극성-2/3/4형¹⁶⁰⁾이 포함된다. 전술미사일은 기보유 스커드계열 미사일과 노동미사일, 그리고 소위 북한판 신형 이스칸데르형(KN-23/19-1)·에이태킴스형(KN-24/19-2)·초대형방사포(KN-25/19-5)¹⁶¹⁾ 등을 포함한다.

1. 화성계열 전략미사일 고도화 및 위협

1.1 신형 백두산 대출력 엔진 시험

김정은 시대 북한은 백두산 엔진(구소련제 RD-250엔진을 개조)을 새로 개발하여 화성-12형 IRBM과 ICBM인 화성-14형 및 화성-15형 등 3종의 중·장거리 탄도미사일을 각각

157) 트랙#1 및 트랙#2는 2020년 10월 10일 당창건 75주년 열병식에서 공개한 추정 화성-16형인 「신형 ICBM」과 「북극성-4형」이 은밀하게 개발 및 기술적 진전이 있었다는 사실이 추가적으로 확인됐다.

158) 북한은 ‘탄도미사일’을 ‘탄도로켓트’라고 부르며, 구소련이나 중국 등 공산권 국가들이 미사일을 ‘로켓트’라고 부른 데서 기인했다.

159) 북한은 ‘전술탄도로켓트’를 ‘전술유도무기(탄)’라고도 부른다.

160) 북극성-1형은 2/3/4형을 만들기 위한 ‘시험용 미사일’로 평가했다.

161) 방사포는 미사일로 분류하지 않지만, 북한식 대구경방사포나 초대형방사포는 유도기술을 적용하여 비행 기술이 탄도미사일과 구분이 어려울 정도로 고도화되어 전술미사일에 포함하여 설명했다. 참고로 한국 합참 정보본부는 2019년부터 시험발사한 북한의 신형 전술미사일에 대구경방사포를 포함하였으며, 발사 순서대로 19-1, 2, 3, 4, 5 명칭을 부여하였다.

시험발사하여 성공했다. 백두산엔진은 북한이 2016년 4월 최초로 엔진연소시험 결과를 공개적으로 발표하고 관련제원과 사진을 보도하여 실체가 구체적으로 확인됐다. 다음 <표 2-1>은 김정은 참관 하에 북한이 엔진시험을 성공적으로 진행했다고 공개한 내용이다.¹⁶²⁾

<표 2-1> 북한의 신형 ICBM용 대형엔진 시험 공개내용

구 분	북한 공개내용
1차 시험 (2016.4.9)	“짧은 기간 연구제작 … 시험에서 완전 성공 놀라운 기적 창조 … 새로 설계·제작한 발동기의 기술적 특성들을 평가 목적 … 또 다른 형태의 핵공격을 할 수 있는 확고한 담보 마련
2차 시험 (2016.9.20)	“새형 정지위성 운반로켓용 대출력발동기 지상분출시험 … 새로 개발한 대출력발동기는 단일발동기로써 추진력 80tf, 지상분출시험을 통하여 추진력을 포함한 발동기의 기술적 지표들이 정확히 도달
3차 시험 (2017.3.18)	“지난 시기 발동기들보다 비추진력 높은 대출력발동기를 완전히 우리식으로 새로이 연구 제작 … 다른 나라 기술을 답습하던 의존성 완전히 뿌리뽑고 … 새로운 탄생 선포한 역사적 대사변 … 김정은이 ‘3.18혁명’이라 언급”

* 출처 : 『조선중앙통신』, 2016년 4월 9일; 2016년 9월 20일; 2017년 3월 19일. 저자 작성.

2016년 4월 1차 시험 발표내용은 “백두산엔진”을 북한이 새롭게 설계 및 제작한 이후 기술적 특성 작동상태만을 평가하는 엔진시험에 성공했다”고 주장했다. 9월 20일 2차 시험간 엔진시험시는 실제 추력과 연소시간을 점검하기 위해 80tf(톤포스)/80t 무게 밀어 올리는 추력)로 약 200여 초(3분 20초) 동안 연소시키면서 기술적 지표와 계통들의 상태를 확인한 것을 알 수 있다.



<그림 2-2> 2·3차 백두산엔진 시험 비교

* 출처 : 『조선중앙통신』, 2016년 4월 9일; 2017년 3월 18일. 저자가 작성.

162) “새형의 대륙간탄도로켓 대출력발동기 지상분출시험 대성공,” 『조선중앙통신』, 2016년 4월 9일; 2016년 9월 20일; 2017년 3월 19일.

최종 3차 시험을 실시한 2017년 3월 18일에는 <그림 2-2>와 같이 주엔진 옆에 보조엔진 4개를 추가 장착하여 엔진연소시험을 성공한 뒤 이를 다시 공개함으로써 단계적으로 기술적 진전의 성과를 과시했다.

1.2. 화성-12형(IRBM) 시험발사 및 실거리 발사

북한은 2017년 3월 18일 새로운 대출력 3차 엔진시험에 성공한 뒤 불과 2개월 만인 5월 14일 평북 구성에 위치한 방현 비행장에서 김정은 참관하 새로운 화성-12형 중거리 탄도미사일의 시험발사에 성공한다.¹⁶³⁾

다음날인 5월 15일 북한은 보도매체를 통해 “금번 시험발사는 위력이 강한 대형중량 핵탄두 장착용 새형의 중장거리 전략탄도로켓의 전술·기술적 제원 및 기술적 특성들을 확증하는데 목적 … 가혹한 재돌입환경 속 조종전투부의 말기유도특성 및 핵탄두폭발체계 동작 정확성을 확증”하였다고 주장했다. 그러면서 김정은이 “후손만대에 물려줄 고귀한 국보인 ‘주체탄’에는 피어린 결사전을 벌려온 로켓부문 일군들과 과학자, 기술자들의 영웅적 투쟁사가 깃들어있다”고 감사의 표시를 전했다며 공개했다.¹⁶⁴⁾

다음 <그림 2-3>과 같이 북한이 공개한 화성-12형 발사사진의 엔진분사형태를 분석한 결과 3월 18일 신형 ICBM용 3차 대형엔진 시험 시 식별됐던 4개의 보조엔진이 동일하게 확인됐다.



<그림 2-3> 3차 신형 대출력 엔진시험과 화성-12형 엔진 비교

* 출처 : 『로동신문』, 2017년 3월 19일; 2017년 5월 15일. 저자가 작성.

163) 김황록, 「김정은 정권의 핵·미사일 고도화와 미국 상대하기」(블루리본, 2020), pp. 208-209.

164) “주체적 핵강국건설사에 특기할 위대한 사변 지상대지상중장거리전략탄도로켓 화성-12형 시험발사 성공,” 『로동신문』, 2017년 5월 15일; “김정은, 화성-12형 개발자들과 기념사진, 축하연회 마련,” 『로동신문』, 2017년 5월 20일.

사진자료 분석을 통해 국내외 전문가들은 화성-12형 미사일이 이른바 ‘3.18혁명’이라고 공개했던 백두산 엔진을 이용한 1단 추진동체로 평가했으며, 북한이 주장한 최대고각 최대고도(2,111km)를 감안시 정상각도로 발사할 경우 약 5,000km를 비행할 수 있는 IRBM으로 분석했다.¹⁶⁵⁾

시험발사 이후 화성-12형은 8월과 9월 북태평양상 2회의 실거리 위협발사를 거쳐 실전 배치에 들어갔다. <표 2-2>는 2017년 화성-12형 발사현황이다.

〈표 2-2〉 화성-12형 발사 현황

구 분	장 소	발수	거리(km)	탄착	고도(km)
4.5	함남 신포	1	실패		
4.16	함남 신포	1	실패		
4.29	평남 북창	1	실패		
5.14	평북 방현	1	787	동해	2,110
8.29	평양 순안	1	2,700	북태평양	550
9.15	평양 순안	1	3,700	북태평양	770

1.3. 화성-14형(ICBM) 시험발사

신형 화성-12형 시험발사 성공 이후 북한은 불과 50여 일 후인 7월 4일 미국 독립 기념일에 평북 방현 일대에서 화성-14형 ICBM 시험발사에 성공한다. 화성-14형은 1단 형인 화성-12형을 2단형으로 길이와 두께를 확대 제작한 사거리 약 10,000km 이상의 ICBM이다. 이는 미국 서부지역까지 도달할 수 있는 위협 사거리다.¹⁶⁶⁾

7월 5일자 노동신문은 “7월 4일 새롭게 연구개발한 대륙간탄도로케트 화성-14형 시험 발사 성공적 진행”했다면서 김정은이 “올해 안에 미국 본토 타격능력 보여 줄 대륙간탄 도로케트 시험발사를 반드시 단행할 확고한 의지 지니고 진두에서 직접 조직 지휘 … 대형 중량 핵탄두 장착 가능한 대륙간탄도로케트를 짧은 기간에 우리식으로 새로이 설계 제작”했다면서 “이번 시험발사는 새로 개발한 탄소복합재료로 대륙간탄도로케트 전투부침두(표적탄두 부분)의 열견딤특성과 구조안정성을 포함한 재돌입전투부의 모든 기술적 특성을 최종 확증하는데 목적두고 진행 … 예정된 비행궤도 따라 최대고도 2,802km까지 상승비행,

165) 대한민국 국방부, 『2018 국방백서』(서울: 국방부, 2017), p. 26.

166) 김항록, 앞의 책, pp. 210-211.

거리 933km 동해 공해상 설정된 목표수역 정확히 타격 ... 1계단 대출력발동기 시동 및 차단특성 재확증 ... 2계단발동기 시동 및 차단특성, 작업특성을 확증 ... 최대 가혹한 재돌입 환경조건속 말기유도 특성 및 구조안정성 확증 ... 특히 재돌입간 전투부에 작용하는 수 천℃ 고온과 가혹한 과부하, 진동조건에서도 전투부침두 내부온도 25-45℃의 범위에서 안정 유지, 핵탄두 폭발 조종장치 정상작동”했다고 공개했다.¹⁶⁷⁾

북한이 화성-14형 ICBM 발사에 성공했다고 발표한 4일(현지시각) 미국의 아침 방송은 북한 ICBM이 미국을 위협한다는 뉴스로 도배됐다. PBS와 CBS 등은 ‘긴급뉴스’로 북한 ICBM의 사거리에 알래스카가 들어온다는 그래픽을 내보내며 서부의 샌프란시스코까지 사정권에 포함될 것을 우려했다. CNN은 “트럼프 행정부의 선택지가 많지 않다”며 군사적 옵션을 사용할 가능성에 대해 언급하기도 했다. 월스트리트저널(WSJ)과 워싱턴포스트(WP) 등도 북한의 ICBM 시험발사 성공 주장을 온종일 인터넷판 톱뉴스로 다뤘다. 북한의 과거 미사일 도발 때와는 차원이 다른 보도 행태였다. 미국은 1962년 쿠바 미사일 위기 이후 55년간 중국·러시아 등을 제외하고 적대국의 핵미사일 사정거리에 든 적이 없었다. 폭스뉴스는 “불량(rogue) 정권 중 최초로 북한이 ICBM을 손에 넣었다”며 “이란도 이렇게 다양하고 높은 수준의 미사일을 보유하고 있지 않다”고 보도했다. 안보 전문가인 브루스 벡톨(Bruce Bechtol) 엔젤로주립대 교수는 미국의 소리(VOA) 방송에서 “이번의 ICBM 발사는 기존 판세를 바꿀 수 있는 게임 체인저가 될 수 있다”고 주장했다.¹⁶⁸⁾

트럼프 행정부 외교·안보팀은 7월4일이 휴일임에도 불구하고 워싱턴과 뉴욕 UN본부에서 긴급회의를 열어 대응책을 논의하고 북한의 화성-14형 ICBM 발사 주장을 공식 확인하면서 모든 수단을 동원해 강력하게 대응할 것임을 천명했다. 렉스 틸러슨(Rex Tillerson) 국무 장관은 성명에서 “미국은 북한의 ICBM 발사를 강력하게 규탄한다”라며 사실상 ICBM 발사를 공식 인정했다. 틸러슨 장관은 “북한의 ICBM 발사로 미국과 세계에 새로운 위협이 고조되고 있다”라며 “미국은 북한의 핵무장을 절대로 받아들이지 않을 것”이라고 강조하면서 국제사회의 동참도 주문했다.¹⁶⁹⁾

또한 7월 5일 니키 헤일리(Nikki Haley) UN주재 미국 대사는 5일 긴급 소집된 UN 안보리 회의에서 “우리가 가진 여러 능력 중 하나가 막강한 군사력이다. 사용해야 한다면 그것(군사력)을 사용할 것”이라며 4일 틸러슨 장관의 성명보다 더 강도가 높고 내용도 구체적으로 언급하는 등 미국의 강경한 분위기를 반영했다.¹⁷⁰⁾ 그리고 미국은 화성-14형

167) 「로동신문」, 2017년 7월 5일.

168) “쿠바 미사일 후 55년만의 본토 위협...신경 곤두선 미국,” 『조선일보』, 2017년 7월 6일; https://news.chosun.com/site/data/html_dir/2017/07/06/2017070600273.html(검색일: 2020년 8월 1일).

169) “미 국무 “강력한 조치로 北 ICBM 책임 물을 것” 『연합뉴스』, 2017년 7월 6일; <https://www.yna.co.kr/view/MYH20170706000700038>(검색일: 2020년 8월 1일).

발사에 대응해 7월 8일 B-1B 전략폭격기 ‘랜서’ 2대를 한반도 상공에 긴급 전개한 후 처음으로 공개적인 정밀유도폭탄 실탄폭격훈련을 했다. 미국의 장거리 전략폭격기가 한반도 상공에서 공개적으로 실탄폭격훈련을 한 것은 최초사례다.¹⁷¹⁾

한편, 북한은 7월 28일 자강도 무평리 지역에서 최대고각사격으로 2차 시험발사에 성공한다. 7월 29일 북한은 언론매체를 통해 2차 시험발사는 “최대정점고도 3,724.9km까지 상승, 거리 998km를 47분 12초간 비행 … 재돌입환경에서 유도 및 자세조종이 정확하게 진행 … 수천℃ 고온에서도 전투부의 구조적 안정유지 … 핵탄두폭발 조종장치 정상동작 확증” 되었으며, 김정은이 “오늘 굳이 우리가 최대사거리 모의시험발사 진행한 것은 미국에 엄중한 경고 … 이 정도면 미국의 정책입안자들이 우리나라를 감히 건드리는 날에는 무사할 수 없을 것임을 제대로 이해했을 것”이라고 보도했다.¹⁷²⁾ 또한 “한 달도 안 되는 짧은 시일 안에 거의 1,000km나 더 상승하는 대륙간탄도로켓을 제작 완성했다”라며 스스로 단기간에 추가 발사할 수 있는 능력을 과시하기도 했다.¹⁷³⁾ <표 2-3>은 화성-14형 시험발사 현황이다.

<표 2-3> 화성-14형 ICBM 시험발사 현황

구 분	1차 시험발사	2차 시험발사
일 시	2017.7.4. 09:00	2017.7.28. 23:04
장 소	평북 구성시 방현비행장	자강도 전천군 무평리 (북중 접경지역 인접)
최대고도(km)	2,802	3,724
거리(km)	933	998

화성-14형 2차 발사는 1차 장소인 방현 일대로부터 약 130km 떨어진 자강도 전천군 무평리 일대였다. 예상치 못한 장소였고, <그림 2-4>처럼 발사 시간도 한밤중이었다. 당시 북한은 기습발사를 위해서 발사장소 및 미사일 관련 징후를 노출하지 않으려고 기만활동을 했다. 북한이 미국을 직접 위협할 수 있는 ICBM급인 화성-14형의 2차 발사간 그 동안 한 번도 시험발사한 적이 없었던 자강도 무평리를 선택한 데 주목해야 한다. 자강도

170) “미, 중력 비토할테면 하라, 우리 길 간다…군사오피스 공개 거론,” 『조선일보』, 2017년 7월 7일; https://news.chosun.com/site/data/html_dir/2017/07/07/2017070700153.html(검색일: 2020년 8월 1일).

171) “다시 날아온 ‘죽음의 백조’…첫 실탄 폭격훈련,” 『조선일보』, 2017년 7월 10일; https://news.chosun.com/site/data/html_dir/2017/07/10/2017071000156.html(검색일: 2020년 8월 1일).

172) “화성-14형 2차 시험발사 단행,” 『로동신문』, 2017년 7월 29일.

173) “민족사적인 대승리를 안아온 금지드높이 연속공격 앞으로,” 『로동신문』 2017년 7월 31일.

무평리는 북중 접경지역에서 약 50km 이내의 인접지역으로 북한의 중요 군사시설들이 위치한 지역이다. 미국이 발사징후가 있는 북한의 미사일 이동식발사차대(TEL)를 선제공격하기 어려운 중국과 인접한 민감한 지역에 위치한 북한의 TEL을 공격시 중국의 심각한 반발을 가져올 수 있을 경고했다. 김정은 정권은 1차 시험발사에 성공한 화성-14형 ICBM을 북중 국경 인접지역에서 다시 2차 발사를 감행함으로써 미국 본토를 기습적으로 공격할 수 있다는 능력을 의도적으로 과시한 것이다.¹⁷⁴⁾



〈그림 2-4〉 화성-14형 2차 시험발사 장면

* 출처 : 『조선중앙통신』, 2017년 7월 29일.

화성-14형 2차 시험발사에 대해 미 트럼프 대통령과 틸러슨 국무장관은 이를 연속 성명과 트위터로 북한을 비난했다. 북한 도발이 ‘레드라인(금지선)’에 도달하면서 워싱턴 포스트(WP) 등 미국 언론들과 싱크탱크들은 북한과 거래한 모든 나라를 경제적으로 보복하는 ‘이란식 경제제재’를 요구했다. 마이크 폼페이오(Michael Pompeo) 미 중앙정보국(CIA) 국장은 “최근 북한에 대한 비밀공작 등 다양한 작전을 들여다보고 있다”고 언급했고, 해리 해리스(Harry Harris) 미 태평양사령관도 “군사적 선택지도 준비할 것”이라고 언급했다. 미 의회도 격앙됐다. 공화당 폴 라이언(Paul Ryan) 하원의장은 28일 성명을 내고 “김정은 정권은 자신들의 행동에 대가를 치러야 한다”라고 했다. 과학자 단체인 ‘참여과학자모임’의 데이비드 라이트(David Wright) 선임연구원은 “정상 각도로 날아간다면 로스앤젤레스와 덴버, 시카고 등도 사정권에 들어간다”라고 주장했다.¹⁷⁵⁾

미국의 대통령과 고위인사, 의회 그리고 전문과학자들이 북한 화성-14형의 위협과 북한의

174) 김황록, 앞의 책, pp. 214-215.

175) 김황록, 앞의 책, pp. 215-216.

ICBM 기술적 진전을 인정한 것이다.

1.4. 신형 화성-15형(ICBM) 시험발사

화성-14형 ICBM 2차 시험발사(7.28)를 기점으로 북한은 약 4개월, 6차 ICBM장착용 핵탄두실험(9.3)을 기점으로는 약 3개월이 경과된 11월 29일 새벽 2시 48분에 평남 평성에서 또다른 신형 ICBM인 화성-15형 시험발사에 성공한다.¹⁷⁶⁾ 북한은 공화국 정부성명을 통해 “당의 정치적 결단과 전략적 결심에 따라 새로이 개발한 대륙간탄도로켓트 화성-15형 시험발사가 성공적으로 진행되었다”면서 “미국본토 전역을 타격할 수 있는 초대형 중량급 핵탄두장착이 가능하며 … 지난 7월 화성-14형보다 훨씬 우월한 무기체계로써, 목표한 로켓트 무기체계 개발의 완결단계에 도달한 가장 위력한 대륙간 탄도로켓트로 … 최대정점고도 4,475km까지 상승, 거리 950km를 53분 간 비행, 조선동해 공해상의 설정된 수역 정확히 탄착” 되었다며金正은이 “비로소 국가 핵무력 완성의 역사적 대업이 실현됐다고 선포했다”고 주장했다.¹⁷⁷⁾

〈표 2-4〉 화성-14형과 화성-15형 주요제원 비교

구 분	화성-14형	화성-15형
엔진 / 추진제	백두산엔진 1개 (보조엔진 4개)	백두산엔진 2개 (노즐 2개, 짐벌엔진)
	액체	액체
추진체(동체)	2단형	2단형
이동식발사대 (TEL)	8축	9축
사거리 (해당지역)	약 10,000km	약 13,000km
	하와이, 미 서부	미 동부 등 전지역
주요 특징	화성-12형 엔진에 1단계 확대 및 2단체를 추가한 ICBM	백두산엔진 2개를 클러스터링한 완전히 새로운 엔진을 장착한 ICBM

* 출처 : 대한민국 국방부. 『2018 국방백서』(서울: 국방부, 2018). 저자가 작성.

전문가들의 분석에 의하면, 〈표 2-4〉처럼 화성-15형은 총 2단형 추진동체로 구성된 미사일이다. 1단동체는 2개의 백두산 엔진을 클러스터링한 노즐 2개의 짐벌엔진이고, 2

176) 김황록, 앞의 책, p. 224.

177) “새형의 대륙간탄도로켓트 시험발사 성공,” 『로동신문』, 2017년 11월 29일.

단체는 화성-14형 미사일의 2단계보다 크기가 확장된 형태의 ICBM으로써(사거리 약 13,000km) 미국 전 지역을 타격할 수 있는 것으로 평가됐다. 특히 화성-12형이나 14형의 1단계 엔진인 백두산엔진 1개의 추력이 80tf(톤포스)인 반면 화성-15형의 추력은 백두산 엔진 2개를 클러스터링함으로써 화성-14형 추력 대비 2배 이상이 증가하여 더 무거운 탄두를 더 멀리 운반할 수 있게 되었다. 또한, 엔진 2개의 노즐이 움직이면서 방향을 조정하는 방식인 이른바 짐벌 시스템으로 화성-12형이나 14형과는 완전히 다른 새로운 형태의 미사일로 평가됐다.¹⁷⁸⁾

한편, 북한은 11월 29일 노동신문을 통해 “짧은 기간에 자체의 힘으로 우리식 9축 자행발사대차를 만들어냈다”고 밝혔는 바, 이 주장의 실체를 공개된 사진에서 확인할 수가 있었다. 과거 북한은 8축형 이동식 차량을 중국으로부터 수입에 의존했지만, 만약 9축 차량인 화성-15형의 이동식발사차량(TEL)을 북한이 직접 제작 또는 개조했다면 미국이 추적하기 어려워 북한이 미국을 공격하는 데 제약이 사라진 것이나 다름없다고 제프리 루이스(Jeffrey Lewis) 연구원은 주장했다.¹⁷⁹⁾ 다음의 <그림 2-5>처럼 9축의 이동발사차량 4대에 실린 화성-15형은 2018년 2월 8일 북한군 창건 열병식에서 식별되어 화성-15형을 본격적으로 생산하는 정황으로 분석했다.¹⁸⁰⁾



<그림 2-5> 화성-15형 발사(2017.11.29) 및 열병식 참가(2018.2.8)

* 출처 : 「로동신문」, 2017년 11월 29일; 「조선중앙TV」, 2018년 2월 8일.

178) “북한 ICBM 기술 세계 3, 4위 수준,” 『주간동아』, 2017년 12월 19일; <http://weekly.donga.com/List/3/all/11/1159979/1>(검색일: 2020년 9월 9일).

179) “화성-15형 실은 9축 자행발사대차가 주목받는 이유,” 『민플러스』, 2017년 12월 4일; <http://www.minplusnews.com/news/articleView.html?idxno=4128>(검색일: 2019년 6월 17일).

180) “미 군사전문가 ”북, 9축 이동식발사차량 본격 생산 정황,” 『민플러스』, 2018년 2월 15일; <http://www.minplus.or.kr/news/articleView.html?idxno=4599>(검색일: 2020년 9월 9일).

북한의 화성-15형 ICBM발사에 대해 미국은 28일(현지시각) 북한의 도발 2시간 만에 대통령과 국무장관, 국방장관 등 외교안보팀 핵심 관계자의 압박 성명을 내놓았다. 트럼프 대통령은 기자들에게 “우리가 처리할 것”이라며 “대북정책 기조는 아무것도 변하지 않았다. 우리는 매우 진지한 접근법을 가지고 있고, 이 문제를 심각하게 여기고 있다”고 언급했다. CNN은 “트럼프 대통령이 북한 김정을 ‘리틀로켓맨’이라고 조롱하지도 않고 ‘화염과 분노’ 같은 격한 발언도 하지 않았다”라고 전했다. 이 자리에 함께한 매티스 국방장관도 “북한이 ICBM을 발사했다”라며 “앞서 발사한 어떤 미사일 보다 높은 고도까지 올라갔다”고 말했다. 그러면서 “북한이 세계 모든 곳을 위협할 수 있다”고 했다.¹⁸¹⁾

미국의 대통령과 국방장관이 북한의 화성-15형 ICBM 능력이 미국과 전 세계를 위협할 정도로 심각하게 인식하고 있다는 점을 잘 보여주고 있는 방증자료이다.

한편 화성-15형 공개사진을 본 미국 전문가들은 다음 <표 2-5>에서와 같이 북한의 미사일이 기술적인 면에서 큰 발전이 있었고, 과거보다 위협이 훨씬 커질 것이라는 점에 동의했다.¹⁸²⁾

<표 2-5> 화성-15형 시험발사 이후 美전문가 평가

구 분	평 가 내 용
위즈먼 (핵무기확산방지 연구센터 연구원)	북한미사일로써 크다는 수준이 아니라 일반적 기준에서도 매우 큰 미사일이다. 화성-14형에 비해 2단 추진체(동체) 너비가 훨씬 넓다. 이정도 크기의 미사일 만들 수 있는 나라는 많지 않다.
데이비드 슈멜러 (David Schmeler, CNS 연구원)	북한 주장을 심각하게 받아들여야 한다. 어제 미사일 시험은 핵폭탄 무게와 같은 모형탄두를 장착해 실시했을 것으로 보인다. 보조엔진 없이 두 개의 엔진을 탑재한 것으로 보인다. 북한에서 보지 못했던 것으로 큰 변화이다.
조셉 버뮤데즈 (Joshep Bermudez, 38노스 선임연구원)	화성-15형의 앞부분이 더 뭉툭해졌다. 이는 재진입기술의 진전으로 보인다.

또한 다음의 <그림 2-6>처럼 북한은 화성-12형과 14형 백두산엔진에 보조엔진(Vernier Engine/버니어엔진)을 달았다. 보조엔진은 탄도미사일의 방향을 조정하는 엔진으로써 내부설계가 복잡하고, 한정된 연료를 보조엔진에 사용하기 때문에 사거리가 상대적으로 줄어드는 단점이 있다. 하지만 북한은 화성-15형에는 가장 최신 기술인 짐벌(Gimbal)

181) “트럼프 北 미사일 발사에 “우리가 처리할 것”, 『한국일보』, 2017년 11월 29일; <https://www.hankookilbo.com/News/Read/201711290749784848>(검색일: 2020년 9월 9일).

182) “‘화성-15형’ 사진 본 美전문가들 “정말 큰, 신형 미사일”, 『노컷뉴스』, 2017년 12월 1일; <https://www.nocutnews.co.kr/news/4885886>(검색일: 2020년 9월 10일).

엔진을 적용했는데 이는 엔진배기구(노즐)의 각도를 조절해 미사일의 비행방향을 조정하는 시스템이다. 화성-15형은 두 개의 백두산엔진을 클러스터링한 짐벌엔진을 적용하였는데 두 개의 배기구(노즐)가 움직여서 방향을 조정함으로써 추력손실을 줄여 사거리를 늘리고 정확도도 높일 수 있었으며, 미사일 구조가 버니어엔진체계 보다 상대적으로 단순해 생산 기간도 단축할 수 있는 장점을 가진 진전된 기술을 확보했음을 보여주었다.¹⁸³⁾

구 분	화성-12형 & 화성-14형	화성-15형
실험사시 엔진연소 장면		
엔진구조		
특징	· 백두산 엔진 1개와 보조엔진 4개를 결합 · 백두산 엔진 추진력 80ft(톤포스) · 엔진 1개만으로 500kg 탄두를 최대 5,000km 운반 가능	· 백두산 엔진 2개를 클러스터링한 짐벌엔진 · 짐벌엔진을 사용한 화성-12·14형에 비해 사거리·정확성 증대

〈그림 2-6〉 엔진시험 기술분석을 통한 화성-12/14/15형 평가

국제사회에서는 화성-15형을 두고 ‘게임체인저’란 말도 나왔다. 미국을 포함한 국제사회는 화성-15형 위협의 실체에 대해 인정하고 싶지 않겠지만 화성-15형이라는 ICBM은 상당히 위협적이라고 인식 및 평가하고 있었다. 이 때문에 허버트 맥매스터(Herbert McMaster) 백악관 국가안보보좌관은 “북한과 전쟁 가능성이 매일 커지고 있다”고 경고했으며, 린지 그레이엄(Lindsey Graham) 상원의원은 “의회가 선제타격을 논의해야 한다”고 주장했다.¹⁸⁴⁾

1.5. 신형 ICBM(추정 화성-16형) 시험발사 없이 공개

북한은 2020년 10월 10일 자정을 기해 실시한 당 창건 75주년 열병식에서 다음 〈그림 2-7〉처럼 신형 ICBM을 공개했다. 공개된 신형 ICBM은 기존의 화성-15형(길이 약

183) 김황록, 앞의 책, p. 208.

184) “북한 ICBM 기술 세계 3, 4위 수준,” 『주간동아』, 2017년 12월 19일; <https://weekly.donga.com/3/all/11/1159979/1>(검색일: 2020년 9월 10일).

21m/직경 약 2.2m) 보다 길이가 길고(약 25m) 직경이 넓어졌다(약 2.5m). 이동형 발사대는 화성-15형의 9축 18륜 대비 11축 22륜으로 확인됐다. 탄두모양과 형태를 고려 시 다탄두(2-3개 탑재 가능)형 ICBM으로 전문가들은 분석했다. 신형 ICBM은 2단형으로써, 1단 엔진은 백두산엔진 4개를 클러스터링한 것으로 보이며, 2단엔진은 백두산엔진 1개 정도의 추력으로 사거리 확대보다는 다탄두 탑재를 위한 증가된 탄두중량 운반 목적으로 보인다.

시험발사 없이 공개했기 때문에 향후 미국의 대응에 따라 협상력을 강화하기 위한 발사 카드로 사용할 것으로 분석되며, 세부 제원은 한미가 공동으로 평가 중에 있다.



〈그림 2-7〉 추정 화성-16형인 신형 ICBM 공개 사진

* 출처 : 「조선중앙TV」, 2020년 10월 10일.

2. 북극성 계열 전략미사일 고도화 및 위협

2.1 북극성-1형 SLBM 사출 및 비행시험

김정은 정권의 북한이 SLBM을 개발하고 있다는 사실은 2014년 9월 14일 국회 국방위원회 질의에 대한 우리 합동참모본부의 답변에서 처음으로 공식 확인됐다.¹⁸⁵⁾ 합동참모 본부는 이날 국회 국방위원회 진성준 의원실에 제출한 자료에서 “현재까지 북한이 잠수함에 미사일을 탑재해 실제 운용하고 있다는 첩보는 없으나 최근 북한 잠수함의 미사일 탑재

185) 김황록, 앞의 책, p. 182.

가능성이 일부 식별되어 한미 공조 아래 정밀 분석 중”이라고 밝혔다.¹⁸⁶⁾ 38노스는 2014년 11월 4일 보도에서 “북한이 신포조선소 일대에서 새로운 시험장을 건설하기 시작하여 2014년 4월에 완성됐다”며 2014년 7월 24일에 인공위성으로 촬영한 67m급 잠수함 영상을 게재한 바 있다.¹⁸⁷⁾ 이 잠수함이 북한의 ‘고래급’ 잠수함이다.¹⁸⁸⁾ 북한은 2015년 5월 9일 김정은이 참관한 가운데 고래급 잠수함에서 ‘북극성’으로 명명된 SLBM을 수중 사출 및 수면에서 로켓점화까지 성공한 장면을 보도했다. 이후 2016년 8월 최종 시험 발사까지 약 10여 차례 진행한 시험발사 현황은 다음 <표 2-6>과 같다.

〈표 2-6〉 북한의 SLBM 사출 및 비행시험 현황

구 분		장 소	내 용	비고
2015년	1.23	신포조선소	수중 사출시험	
	5. 8	신포 근해	수중 사출시험	김정은 참관
	11.28		비행시험(실패 추정)	
	12.21			
2016년	8	신포 근해	비행시험(실패 추정)	김정은 참관
	3.16	신포조선소	지상 사출시험(추정)	
	4.23	신포 근해	비행시험(약 30km 비행)	
	7. 9		비행시험(약 10km 비행)	
	8.24		비행시험(약 500km 비행)	김정은 참관

2015년 5월부터 북한은 SLBM 사출 및 비행시험 내용을 의도적으로 공개했다. 2014년에는 주로 육상 및 수중(바지선)에서 사출시험을 실시하고, 2015년부터 신포급 잠수함에서 본격적으로 수중발사를 통한 사출 및 비행시험을 실시했다.¹⁸⁹⁾

2015년 5월 9일 북한은 보도를 통해 김정은 참관 하에 전략잠수함 수중시험발사가 진행됐다고 최초로 보도했다. 북한 매체인 조선중앙방송은 “시험발사를 통하여 함내소음

186) “북 잠수함 기지서 탄도미사일 수직발사관 식별,” 『연합뉴스』, 2014년 9월 14일; <https://www.yna.co.kr/view/MYH20140914003900038>(검색일: 2020년 9월 25일).

187) Joseph S. Bermudez Jr, “The North Korean Navy Acquires a New Submarine,” 38 NORTH, 19 October 2014; <https://www.38north.org/2014/10/jbermudez101914/>(검색일: 2020년 9월 25일).

188) 고래급 잠수함은 길이 67m, 배수량 2,000톤, 발사관 1개를 탑재한 최초의 SLBM 탑재 잠수함이다. 북한은 1993년 3개의 SLBM 발사관을 갖춘 러시아제 G급(골프급) 잠수함 수척을 고철로 수입, 미사일 발사장치와 관련 기술 및 부품 일부를 입수해 역설계 방식으로 건조한 것으로 알려졌다. 신포급 잠수함이라고도 불리는 동 잠수함은 시험용 잠수함으로써 2016년 8월 최종 비행시험 이후 현재는 미활동 중이다. 새롭게 건조 중인 것으로 추정되는 약 3천톤급의 잠수함으로 대체될 것으로 보인다.

189) 김황록, 앞의 책, p. 184.

준위, 발사반충력, 탄도탄의 수면출수속도, 자세각 등 전략잠수함에서의 탄도탄 수중발사가 최신 과학기술적 요구에 완전히 도달했다는 것이 검증 확인되었다며, “당 중앙의 전략적 기도에 맞게 전략잠수함에서의 탄도탄 수중발사기술을 완성한 … 위훈을 높이 평가하고 … 우리식의 공격형 잠수함에서 탄도탄을 발사할 수 있게 된 것은 인공위성을 쏘아 올린 것에 못지 않는 경이적인 성과이며 … 실전배비되면 적대세력들의 뒤통수에 언제 터질지 모르는 시한탄을 매달아 놓는 것으로 … 임의의 수역에서 … 마음 먹은 대로 수중작전을 진행할 수 있게 되었다”고 김정은이 강조한 내용을 보도했다.¹⁹⁰⁾

이후 약 1년 가까이 수차례 비행시험을 거쳐 2016년 4월 24일 북한은 다시 김정은 참관 하 시험발사한 위협내용을 공개한다. 조선중앙통신은 “핵공격 능력을 비상이 강화해 나가는 길에서 커다란 의의를 가지는 탄도탄 수중시험발사의 눈부신 성공을 또 다시 이룩 … 최대 발사심도에서의 탄도탄 냉발사체계 안정성과 새로 개발한 대출력고체발동기를 이용한 탄도탄의 수직비행체제에서의 비행동력학적 특성, 계단열분리의 믿음성, 설정된 고도에서 전투부핵기폭장치의 동작정확성을 입증하는데 목적을 두고 진행 … 완전히 확증, 공고화 … 수중발사기술을 보다 높은 수준에서 훌륭히 완성 … 역사적인 당 7차대회를 앞두고 경이적 성과”라고 김정은이 강조한 내용을 포함해 보도했다.¹⁹¹⁾ 2015년 대비 액체 추진제에서 고체추진제로 연료를 대체하고 이른바 콜드런치 방법¹⁹²⁾으로 가상 핵기폭장치 작동 시험을 병행한 것을 강조했다.¹⁹³⁾

약 4개월 뒤인 8월 24일, 다음 <그림 2-8>과 같이 북한은 김정은이 참관한 가운데 핵무력 고도화 기간 중 북극성-1형인 SLBM의 마지막 비행시험을 단행했다. 수중에서 발사된 탄도미사일은 약 500km 거리로 날아가 일본의 방공망식별구역에 낙하한다. 다음날인 8월 25일 북한은 언론매체를 통해 김정은의 핵무력 고도화 계획 및 전략적 의도를 파악할 수 있는 몇 가지 주요한 내용을 다음과 같이 주장했다. “지난해 5월 전략잠수함 탄도탄의 수중시험발사를 성공시키고 불과 1년도 못되는 기간에 비행시험단계에 진입하는 빠른 속도를 과시한데 이어 오늘 또다시 보다 높은 단계의 탄도탄 수중시험발사에서 성공함으로써 우리의 핵무력 고도화에서 커다란 군사적 진보를 이룩했다”라며 김정은이 “이번 전략잠수함 탄도탄 수중시험발사는 성공 중의 성공, 승리 중의 승리라며 … 오늘 발사한 탄도탄의 시험결과를 통하여 우리가 핵공격 능력을 완벽하게 보유한 군사대국의 전열에

190) “전략잠수함 탄도탄 수중시험발사에서 완전 성공,” 『조선중앙방송·로동신문』, 2015년 5월 9일.

191) “전략잠수함 탄도탄 수중시험발사 또다시 대성공,” 『로동신문』, 2016년 4월 24일.

192) 콜드런치(Cold Launch)란 수중에서 미사일이 점화되는 핫 런치(Hot Launch)와 달리 SLBM이 물 밖으로 나와 점화되는 방식을 의미한다. 콜드런치 방식의 장점은 핫 런치 방식 대비 소음이 작고 설계구조가 단순하며, 은폐성이 뛰어나다.

193) 김항록, 앞의 책, pp. 185-186.

들어섰다는 것이 현실로 증명 ... 미국이 아무리 부인해도 미 본토와 태평양작전지대는 손아귀에 ... 미국과 추종세력들이 이번 시험발사를 걸고들며 또 무슨 고리타분한 수작을 ... 우리의 불굴의 정신력과 무궁무진한 힘을 절대로 과소평가하지 말아야 한다 ... 제재와 봉쇄, 압박의 쇄사슬을 끊고 어떻게 무섭게 솟구쳐 오르는가를 세계 앞에 똑똑히 보여줄 것 ... 핵무기병기화사업에 더욱 박차를 ... 동시에 운반수단 개발에 총력을 집중할 것을 강조”했다고 보도했다.¹⁹⁴⁾



〈그림 2-8〉 북한의 SLBM 비행시험 공개 사진

* 출처 : 『조선중앙통신』, 2016년 8월 25일.

8월 24일 북극성-1형 비행시험에 성공한 북한은 3개 이상의 발사관을 장착해 SLBM을 발사할 수 있는 신형 3천톤급 이상의 잠수함 건조에 들어갔다.¹⁹⁵⁾ 고래급(신포급) 잠수함이 1개의 발사관만을 갖춘 시험용 잠수함이었기 때문에 새로운 SLBM용 잠수함이 필요했던 것이다.

194) “주체조선의 핵공격능력의 일대 과시 경애하는 김정은동지의 지도밑에 전략잠수함 탄도탄수중시험발사가 성공적으로 진행되었다,” 『조선중앙통신』, 2016년 8월 25일.

195) 김정은이 북한 정권수립 70주년인 2018년 9월 9일까지 잠수함발사탄도미사일(SLBM) 발사관을 2-3개 갖춘 신형잠수함을 제작하도록 당 간부에게 지시했다고 도쿄신문이 26일 보도했다. 김정은이 이만건 당 부위원장(군수공업부장)에게 성공하면 동상을 세워주겠다는 말을 들었다는 북한 소식통의 발언도 소개했다. “김정은, SLBM 3발 장착 잠수함 만들라” 『중앙일보』, 2016년 8월 27일; <https://news.joins.com/article/20510908> (검색일: 2019년 6월 29일); 북한이 SLBM의 발사관 2-3기를 갖추고 장시간 잠행이 가능한 신형 잠수함 개발을 진행해 건조작업이 80%에 달했다는 정보가 있다고 도쿄신문이 2017년 9월 14일 보도했다. “북한, SLBM 발사관 2-3기 갖춘 신형잠수함 완성 임박,” 『MK뉴스』, 2017년 9월 14일; <https://www.mk.co.kr/news/politics/view/2017/09/618085/> (검색일: 2020년 9월 29일).

2.2 북극성-2형 MRBM 시험발사 성공 및 실전배치 돌입

북한은 2017년 2월 12일, <그림 2-9>처럼 김정은 참관 하에 북극성-2형인 고체추진제 준중거리지대지탄도미사일(MRBM)을 시험발사했다. 트럼프 행정부가 들어선 이후 32일 만에 북한의 첫 탄도미사일 발사이다. 북극성-2형은 2016년 8월 시험발사에 성공한 SLBM을 지대지용으로 개량한 신형 MRBM이다. 신형 고체연료 엔진이 장착된 새로운 탄도미사일인 북극성-2형은 지상의 무한궤도형 이동식발사차량(TEL)에서 발사됐다.¹⁹⁶⁾

2월 13일 북한은 언론매체를 통해서 김정은이 “지난해 8월 전략잠수함 탄도탄 수중 시험발사에서 이룩한 성과에 토대하여 사거리를 연장한 지상대지상탄도탄으로 개발”을 지시했다며 “새로운 전략무기체계를 불과 6개월이라는 짧은 기간에 완성하는 놀라운 기적을 창조”했다고 보도했다. 또한 “핵탄두 장착이 가능한 조종전투부 분리후 … 재돌입구간에서 자세조종과 유도, 요격회피기동 특성 등을 검증 … 수중과 지상 임의 공간에서 가장 정확하고 신속하게 전략적 임무를 수행할 수 있게 됐다”고 강조했다.¹⁹⁷⁾



<그림 2-9> 북한의 북극성-2형 시험발사 장면

* 출처 : 『조선중앙통신』, 2017년 2월 13일.

5월 21일, 북한은 김정은이 참관한 가운데 북극성-2형을 또다시 발사했다. 북한 매체들은 “5월 22일 북극성-2형 중거리전략탄도미사일 시험발사에 성공했다”면서 “김정은이 실전

196) 김황록, 앞의 책, p. 190.

197) “지상대지상중거리전략탄도탄<북극성-2>형 시험발사에서 완전성공 경애하는 최고령도자 김정은동지께서 새 전략무기시험발사를 현지에서 지도하시였다,” 『조선중앙통신』, 2017년 2월 13일.

배치를 승인하고 대량생산을 지시했다”고 밝혔다. 지난 2월 첫 발사에 이어 3개월 만에 추가 시험발사에 성공하고 전력화에 들어갔다는 의미다.¹⁹⁸⁾

조선중앙통신 등 북한 관영매체들은 “금번 발사를 통해 리대식(무한궤도식) 자행발사대 차량의 냉발사, 단 분리특성, 대출력 고체발동기의 믿음성과 정확성이 입증됐고, 핵조종 전투부에 설치된 촬영기의 영상자료로 자세조종체계의 정확성도 더 명백히 검토됐다”면서 대기권에서 촬영한 지구 사진을 공개했다.¹⁹⁹⁾ 북극성-2형 발사현황은 다음 <표 2-7>과 같다.

<표 2-7> 북한의 북극성-2형 시험발사 현황(2017년)

구 분	장소	발수	거리	탄착	비고
2.12.07:55	평북 구성 방현비행장	1	500km	동해	김정은 참관
5.21.16:59	평남 북창	1	500km	동해	김정은 참관

북극성-2형의 궤도형 이동식발사대는 차륜형보다 산악지역 등 야지 주행 능력이 뛰어나다. 고체추진제 사용은 연료 및 산화제 주입시간이 필요 없기 때문에 은밀성과 기동성, 생존성과 기습발사 능력이 매우 우수하다. 따라서 지상에서 선제 기습타격은 물론 미국의 제1격 으로부터 주한 및 주일미군 기지 보복능력도 획기적으로 향상됐다.²⁰⁰⁾

2.3 북극성-3형 SLBM 수중 사출시험 성공 및 신형 잠수함 건조

북한은 수중발사 잠수함탄도미사일인 북극성-1형을 개발하는 과정에서 지대지미사일인 북극성-2형을 새롭게 만들어 내는 치밀함과 기술적 능력을 보여줬다. 2016년 8월 시험용 잠수함(고래급/2천톤)에서 발사한 SLBM이 500km 비행에 성공함으로써 그해 말부터 신포 조선소에서 약 3천톤급 잠수함 건조를 시작했다. 약 3년이 경과된 2019년 7월 23일 다음 <그림 2-10>처럼 김정은은 참관 하 북한은 북극성-3형 SLBM을 발사할 수 있는 신형 3천 톤급 잠수함 건조 모습을 관영매체를 통해 공개했다.

198) 김황록, 앞의 책, p. 191.

199) “전략탄도탄 북극성-2형 시험발사에 또다시 성공,” 『조선중앙통신』, 2017년 5월 22일.

200) 김황록, 앞의 책, p. 192.



〈그림 2-10〉 신형 3천톤급 잠수함 공개 사진

* 출처 : 『조선중앙통신』, 2019년 7월 23일.

7월 23일 조선중앙통신은 김정은이 새로 건조한 잠수함을 둘러보고 “작전 전술적 제원, 무기 전투체계를 구체적으로 요해”했다면서 “잠수함이 각이한 정황 속에서 당의 군사전략적 기도를 관철할 수 있게 설계, 건조된 데 대하여 커다란 만족을 표시 … 잠수함 이용 및 수중작전에 대한 당의 전략적 구상”에 대해 설명했다면서 이 잠수함이 동해 작전수역에서 임무를 수행할 것이며 작전배치를 목전에 두고 있다고 밝혔다.²⁰¹⁾

2016년 8월 북극성-1형 비행시험 성공 이후 약 3년 만에 3천톤급 대형 잠수함 건조 모습을 과시한 것이다.

SLBM 발사관은 3개로 분석됐다. 최후병기로 알려진 잠수함은 상대방에게 노출하지 않는 것이 상식이지만 북한 역사상 SLBM용 잠수함 건조 사실을 처음으로 공개한 것은 매우 이례적이다. 미국에게 제재를 해제하고 협상에 나오라는 핵무력 과시 목적으로 공개했을 가능성이 높다. 또한 미국과 비핵화 협상 과정에서도 잠수함을 건조해 온 사실은 비핵화 의지의 진정성이 없었음을 보여주는 이중적 행동으로 확인되기도 했다. 불과 한 달도 채 지나지 않은 지난 6월 30일 김정은 위원장과 트럼프대통령이 판문점에서 회동한 직후 나온 김정은의 첫 군사행보이기 때문이다.

10월 2일 북한은 북미 실무협상을 앞두고 동해상으로 신형 잠수함발사탄도미사일인 북극성-3형 시험발사에 성공했다고 다음 〈그림 2-11〉처럼 수중발사사진을 공개했다. 조선중앙통신은 10월 3일 “조선민주주의인민공화국 국방과학원은 2019년 10월 2일 오전 동해 원산만 수역에서 새형의 잠수함탄도탄 ‘북극성-3형’ 시험발사에 성공적했다”고 밝혔다.

201) 「조선중앙통신」, 2019년 7월 23일.

이날 발사한 미사일은 1발로써 최대 고도 910km, 비행거리는 약 450km로 탐지됐다. 실제 위협 사거리는 2,000km를 훨씬 초과할 것으로 분석됐다.



〈그림 2-11〉 북한의 북극성-3형 시험발사 성공 공개사진

* 출처 : 『조선중앙통신』, 2019년 10월 3일.

2.4 신형 북극성-4형 SLBM 시험발사하지 않고 공개

한편, 2020년 10월 10일 당창건 75주년 열병식에서 북한이 공개한 북극성-4형은 다음 〈그림 2-12〉처럼 북극성-3형보다 길이와 직경이 약간 커진 것으로 확인되어 신형 4-5천 톤급 잠수함용으로 추정되고 있다. 신형 북극성-4형 SLBM 세부제원은 한미가 공동으로 평가에 들어 간 것으로 알려졌다.



〈그림 2-12〉 신형 북극성-4형 열병식 공개사진

* 출처 : 『NEWSIS』, 2020년 10월 11일.

이로써 북한은 북극성-3형의 신형 잠수함(완성 직전) 비행시험, 북극성-4형의 수중사출 시험(바지선) 및 신형 잠수함(건조 중) 비행시험 단계, 그리고 전력화 단계가 아직 남아 있다.²⁰²⁾

제3절 전술미사일 기술 고도화와 위협

북한의 전술미사일은 스커드 B/C('80년대), 노동미사일('90년대), 스커드-ER('05), 스커드-ER 개량형('16), 이스칸데르형('19), 에이태킴스형('19-'20)으로 발전했다. 대구경 방사포도 300мили('13-'16)에서 400мили('19), 그리고 600мили 초대형방사포('19-'20)로 진화되면서 전술미사일과 유사한 탄도와 유도장치가 고도화됐기 때문에 미사일의 범주로 분류할 수 있게 됐다. 김정은 시대 들어서는 스커드-ER 개량형부터 본격적으로 성능개선이 이루어졌는데 정확도가 향상되고 사거리가 연장됐다. 이러한 새로운 신형 단거리 전술미사일들은 2019년 5월에서 2020년 3월사이 모두 시험사격에 성공하여 김정은 지시에 의거 실전배치에 돌입했다.

1. 스커드 및 노동미사일 기술 고도화와 위협

김정은 시대 들어 북한은 기(既) 보유했던 스커드와 노동미사일의 핵탄두 투발능력과 정확성을 크게 향상시킨 것으로 분석된다. 2013년 2월 3차 핵실험으로 인한 북미 간의 핵전쟁 소동 국면(3-5월)을 거친 후 북미관계는 잠시 소강상태를 보이는 듯 했지만 2014년부터 김정은이 다시 전략군 예하 탄도미사일부대 현장지도를 통해 스커드와 노동미사일의 실전 타격능력을 점검하면서 고도화가 본격적으로 진행됐다. 김정은은 이미 보유하고 있는 단거리 및 중단거리 탄도미사일의 핵투발 능력과 유도성능 개선으로 정확도 향상을 위한 고도화에 노력을 집중하면서 그 과정을 의도적으로 공개했다. 이 시기는 김정은 정권이 신형 화성계열(IRBM·ICBM) 및 북극성계열(SLBM) 엔진과 동체를 은밀히 설계하고 제작했던 시기이기도 했다.²⁰³⁾

북한은 1960년대 중반부터 미사일 개발 프로그램에 인력과 자원을 투입해 왔다. 1976년 스커드-B를 이집트로부터 도입하고 역설계를 통해 스커드 미사일을 자체적으로 생산하는데 성공했고, 이를 개량(B/C: 사거리 300/500km)하여 1988년에는 야전에 작전

202) SLBM 개발 4단계는 지상사출 → 수중사출 → 비행시험 → 전력화 단계다.

203) 김황록, 앞의 책, p. 152.

배치를 완료했다. 1990년대에는 사거리 1,300km인 노동미사일, 2000년대 들어서는 스커드 개량형인 사거리 약 1,000km인 스커드-ER을 각각 개발해 야전에 작전배치를 완료했다. 스커드-B/C는 한반도를, 스커드-ER과 노동미사일은 일본 전역까지 위협하는 북한의 탄도 미사일이다. 한국지역에는 주한미군이, 일본지역에는 주일미군과 UN사 후방기지가 있다. 북한에게는 주요 타격목표들이다. 이러한 스커드와 노동미사일을 기반으로 북한은 대포동 1호를 2006년과 2009년에, 대포동 2호를 2012년과 2016년에 소위 위성(은하/광명성)이라 주장하며 발사했다. 대포동미사일 1단동체는 노동미사일 엔진을 클러스터링했고, 2단 동체는 스커드미사일을 사용한 것으로 알려졌다. 그리고 대포동미사일 발사로 축적된 단분리 기술로 김정은 시대인 2017년 말 북한은 미사일 개발 시작 이래 약 40여 년 만에 ICBM 개발에 성공했다. 결국 스커드 및 노동미사일은 북한 미사일의 개발 기술과 독자적 미사일 제조 기술 축적의 원천이었다.²⁰⁴⁾

그런데 북한이 1, 2차 핵실험 전후나 위기조성 시마다 주기적으로 실제 발사훈련을 했던 스커드 및 노동미사일은 탄두의 크기나 무게 면에서 소형화된 핵탄두를 장착하여 운용하기에 가장 용이한 미사일이다. 김정은 정권의 북한이 3차 핵실험 이후 핵탄두를 소형화했다고 빈번하게 주장하는 이유 중의 하나가 기(既) 보유 중인 스커드 및 노동미사일에 핵탄두를 가장 먼저 장착하여 자신들의 핵무력 고도화를 압박할 것으로 예상되는 미국의 강압을 억제할 수 있는 수단으로도 활용했다고 분석했다.²⁰⁵⁾

〈표 2-8〉은 김정은 시대 스커드 및 노동미사일 발사현황이다. 2012-2013년도에 북한이 탄도미사일을 발사한 사례는 식별된 바 없다.

〈표 2-8〉 김정은 시대 스커드/노동미사일 발사 현황

구 분	계	2014	2015년	2016년	2017년
스커드	24발	11발	2발	6발(ER)	5발(ER)
노 동	4발	2발		2발	

2. 신형 ‘이스칸데르형’ 미사일 기술 고도화와 위협

소위 신형 이스칸데르형 미사일(북한은 ‘신형 전술유도무기(탄)’라고 언급)은 2019년 5월 4일부터 〈그림 2-13〉처럼 본격적으로 식별되기 시작했다. 이 시기는 하노이 2차 북미 정상회담에서 협상이 결렬되고 북미간 기싸움이 벌어지던 비핵화협상 교착국면의 초기이다.

204) 김황록, 앞의 책, pp. 152-153.

205) 김황록, 앞의 책, p. 153.

북한매체는 4일 오전에 원산 호도반도 일대에서 240미리 방사포와 300미리 방사포를 포함하여 신형전술유도무기를 발사했다고 5일 보도했다. 합참은 신형 전술유도무기는 2발로써 최대 240km 비행, 고도는 약 30km로 추정했다.



〈그림 2-13〉 김정은 시대 북한판 이스칸데르형 미사일 발사 장면

* 출처 : 『조선중앙통신』, 2019년 5월 4일.

이어서 북한은 2019년 5월 9일(2차), 7월 25일(3차), 8월 6일(4차) 등 총 3차례의 추가 시험발사를 거쳐 최종적으로 4차 내륙발사에서 정밀타격에 성공하고 김정은이 관련자들과 기념촬영을 했다고 조선중앙통신이 보도했다. 발사현황은 다음 〈표 2-9〉와 같다.

〈표 2-9〉 김정은 시대 신형 전술유도무기(‘이스칸데르’형) 발사 현황

구 분	1차	2차	3차	4차
일시/장소	5.4/호도반도	5.9/평북구성	7.25/호도반도	8.6/황남과일
발 수	2	2	2	2
비행거리(km)	240	420, 240	600, 600	450, 450
고도(km)	미포착, 30	40, 40	50, 50	37, 37
속도(마하)	미포착, 5.9	6.4, 4.9	6.5, 6.9	6.9, 7.4
비 고		내륙 발사		내륙 발사

〈표 2-9〉처럼 신형 이스칸데르형 전술유도무기는 저고도로 마하 6이상의 빠른 속도로 최대 600km를 비행할 수 있는 능력을 과시했다. 북한지역에서 한반도 전 지역을 위협할

수 있는 사거리와 정확성을 향상시켰음은 물론 Pull-up 상승비행 기술도 새롭게 개발한 것으로 분석되어 한미연합군의 요격이 매우 제한될 것으로 평가했다.

북한의 조선중앙통신은 8월 7일 1일전 김정은이 참관한 가운데 신형 전술유도탄 위력 시위발사를 했다고 보도했다. 매체는 “서부의 작전비행장에서 발사된 전술유도탄 2발이 북한의 평양권 지역 상공과 중부의 내륙지대 상공을 비행하여 동해상의 설정된 목표점을 정밀타격했다”고 공개했다. 또한 김 위원장이 “위력시위발사를 성공적으로 단행한 국방 과학 부문 간부, 과학자, 군수노동계급을 만나 기념사진을 찍었다”고 전했다. 이번 발사 참관에 다수의 당 부위원장들이 참석하고 기념촬영까지 했다는 점에서 동 무기체계 개발은 완성되어 실전배치 작업에 들어간 것으로 전문가들은 평가했다.²⁰⁶⁾

3. 신형 ‘에이태킴스형’미사일 기술 고도화와 위협

북한판 에이태킴스형 미사일²⁰⁷⁾은 2019년 8월 10일, 8월 16일 그리고 2020년 3월 21일 세 차례 시험발사했으며, 2020년 3월 21일 발사 성공을 마지막으로 실전배치에 들어갔다. 특히 북한 조선중앙통신은 2020년 3월 22일 김정은이 전날 이뤄진 전술유도 무기 시범사격을 참관했다며 무한궤도형 이동식 발사차량(TEL)에서 발사되는 유도무기 사진을 <그림 2-14>처럼 공개했다.



<그림 2-14> 김정은 시대 신형 에이태킴스형 미사일 발사 공개 사진

* 출처 : 『조선중앙통신』, 2019년 8월 17일; 2020년 3월 22일.

206) 「조선중앙통신」, 2019년 8월 7일.

207) 북한은 ‘새무기 체계’ 또는 ‘전술유도무기’로 부름.

북한은 “시범사격에서 서로 다르게 설정된 비행궤도와 각각특성, 유도탄의 명중성 및 탄두 위력이 뚜렷이 과시됐다”고 밝혔는 바, 이는 2발을 발사하기 전에 서로 다르게 제원을 설정하고 정점고도를 지나 목표물 인접 상공까지는 폴업 기동(pull-up/상승 및 활강)을 했을 가능성이 높은 것으로 분석됐다. 이는 미사일이 종말단계에서 변칙 기동함으로써 패트리엇나 샤드로 요격하기가 쉽지 않다는 것을 보여주고 있다. 북한은 무수단 남단에 위치한 알섬을 명중하는 사진을 공개함으로써 미사일에 내장된 첨단 유도장치인 시커(seeker) 성능도 과시하고자 의도했다. 이러한 북한의 단거리미사일 유도장치 개발 및 정확도 향상 노력은 이미 지난 2016년부터 김정은의 지시에 의거 본격적으로 추진한 것으로 분석했으며,²⁰⁸⁾ 실전배치에 들어간 것으로 평가했다. 3차에 걸친 북한판 에이태 킴스형 전술미사일 시험발사 현황은 아래 <표 2-10>과 같다.

<표 2-10> 김정은 시대 신형 전술유도무기(‘에이태킴스’형) 발사 현황

구 분	1차(2019년)	2차(2019년)	3차(2020년)
일시/장소	8.10/함남 함흥	8.16/강원 통천	3.21/평북 선천
발수	2	2	2
비행거리(km)	430	230	410
고도(km)	48	30	50
속도(마하)	6.1	6.1	6.1(추정)
비고			내륙 발사

4. 신형 초대형 방사포 기술 고도화와 위협

300미리 방사포는 김정은 집권 이후 2013년부터 시험발사를 시작했다. 우리군에서는 북한이 2016년-2017년 사이에 작전배치했을 것으로 추정하고 있다. 김정은 정권은 300미리 방사포 기술을 토대로 2019년부터 400미리 대구경방사포와 600미리 초대형방사포를 연속적으로 개발, 마침내 2020년 3월말 국방과학원의 시험발사를 마지막으로 실전 배치에 들어갔다.

북한은 2019년 8월 24일 신형 초대형방사포를 함남 선덕비행장에서 발사한 이후, 9월 10일 개천(평남), 10월 31일 순천비행장(평남), 11월 28일 연포비행장(함남), 2020년 3월

208) 2017년 5월 29일 원산일대에서 스커드-ER 개량형 시험사격시 김정은 위원장이 “지난해(2016년) 지시한 적의 함선을 비롯한 해상과 지상의 임의의 바늘귀 같은 개별목표를 정밀타격할 수 있는 새로운 정밀조종 유도체계를 도입한 우리식의 주체무기를 탄생시키는 성과를 이룩했다”고 언급한 내용을 공개한 데부터 확인 되고 있다. 『조선중앙통신』, 2017년 5월 29일.

2일 원산(강원), 3월 9일 선덕(함남), 3월 29일 원산(강원)에서의 시험발사를 마지막으로 실전배치에 돌입했다. 특히 2020년 3월 30일 북한 관영매체는 전일 발사한 발사체가 초대형방사포 시험사격이었다고 보도했다. 당 기관지인 노동신문은 “국방과학원에서 조선인민군 부대들에 인도되는 초대형 방사포의 전술 기술적 특성을 다시 한번 입증하는데 목적을 두고 시험사격을 진행했다”면서 “시험사격은 성공적이었다”고 주장했다.²⁰⁹⁾



포토출

북한 화보집에 실린 초대형방사포 시험사격

(서울=연합뉴스) 북한 외국문출판사가 '김정은 시대' 무기 개발과 군사지도 모습을 담은 화보집을 펴냈다. [외국문출판사 화첩 캠퍼] 2020.11.24
[국내에서만 사용가능. 재배포 금지. For Use Only in the Republic of Korea. No Redistribution]
nkphoto@yna.co.kr

〈그림 2-15〉 김정은 시대 신형 초대형 방사포 발사장면 공개사진

* 『연합뉴스』, 2020년 11월 25일.

합참은 3월 29일 오전 6시 10분경 원산 일대에서 북동쪽 해상으로 발사된 단거리탄도 미사일로 추정되는 2발의 발사체가 포착됐으며 비행거리는 약 230km, 고도는 약 30km로 탐지했다고 밝혔다. 북한매체는 김정은이 불참했지만 리병철 당 부위원장 등 당 중앙위 군수공업부 간부들과 장창하, 전일호 등 국방과학연구부문 간부들이 지도했다고 보도했다. 당시 리병철이 “초대형 방사포 무기체계를 작전배치하는 사업은 국가방위와 관련한 당 중앙의 새로운 전략적 기도를 실현하는 데서 매우 중대 사업”이라고 언급한 것처럼 신형 초대형 방사포는 매우 위협적인 무기체계다. 왜냐하면 금번 발사 이후 북한이 공개한 초대형 방사포의 발사관은 4련장, 5련장, 6련장 등 다양한 형태로써 발사간격이 20초로 현저히 단축되었음이 확인되어 위협이 현저하게 증가했다고 분석됐기 때문이다.²¹⁰⁾ 짧은 시간에 연속발사하고 기존의 장사정포(240RL/170SP)와 단거리 미사일 등을 혼합하여 이른바

209) 「로동신문」, 2020년 3월 30일.

210) 북한은 10월 10일 열병식에서 4련장, 5련장, 6련장 등 3종의 초대형방사포를 보여줬다.

‘섞어쓰기’를 할 경우에는 요격이 거의 불가하다. 사거리 또한 신장되어 평택 주한미군 기지도 초대형 방사포의 밀집 포격에 매우 취약해진 것도 드러났다. 다음의 <표 2-11>는 북한의 초대형 방사포 시험발사 현황이다.

<표 2-11> 김정은 시대 신형 초대형 방사포 발사 현황

구분		장소	발수/련장	비행거리(km)	고도(km)	발사간격
1차	2019. 8.24	함남 선덕	2/4련장	380	97	17분
2차	9.10	평남 개천	2/4련장	330	50-60	19분
3차	10.31	평남 순천	2/4련장	370	90	3분
4차	11.28	함남 연포	2/4련장	380	97	30초
5차	2020. 3.2	강원 원산	2/4련장	240	35	20초
6차	3.9	함남 선덕	3/4련장	200	50	20초-1분
7차	3.29	강원 원산	2/6련장	230	30	20초

<표 2-11>에서와 같이 초대형 방사포 시험사격은 총 7차에 걸쳐 진행되었으며, 고도가 30-50km로 대폭 낮아졌음을 확인할 수 있다. 또한 발사간격도 20초로 짧게 단축되었고 연발사격 능력도 향상되어 한미연합군의 요격을 어렵게 하려는 북한의 분명한 의도가 확인됐다. 이스칸데르형이나 에이태킴스 미사일과 유사하게 이러한 초대형 방사포도 기존의 방사포와 장사정포 그리고 신형 단거리 전술미사일과 혼합되어 이른바 ‘섞어쓰기’를 한다면 한국군과 주한미군의 미사일 요격체계를 무력화하는데 매우 위협적인 북한군의 재래식 전술무기체계가 아닐 수 없게 됐다.

한편, 북한은 2020년 10월 10일 당창건 75주년 열병식에서 발사관 4개형, 5개형, 6개형 등 3종의 초대형방사포도 공개했다. 따라서 2019년 두 차례에 걸쳐 시험발사(7.31/8.2) 했던 400mm 대구경방사포라 알려진 북한주장 ‘신형대구경조종방사포’는 북한이 600mm 초대형방사포를 개발하는 중간과정으로 평가했다. 또한 본 연구에서는 2015년경에 개발을 완료한 대구경 300mm 방사포도 정확도 향상과 저고도 탄도를 고려하여 김정은 시대에 새로 개발한 신형 전술미사일 범주에 포함하여 분류했다.

Ⅲ. 북한 미사일 위협 종합 및 전망

제1절 김정은 시대 미사일 기술과 위협 종합

앞 장에서 살펴본 바와 같이 김정은 정권의 북한은 핵탄두를 장착하여 투발할 수 있는 전략 및 전술미사일을 다음의 <표 3-1>에서 보는 바와 같이 현저하게 기술적 진전을 이루었다고 종합평가해 볼 수 있다.

<표 3-1> 김정은 시대 전략 및 전술미사일 고도화 위협 종합

구 분	김 정 일		김 정 은	비 고
	핵무기 소형화 미달성		핵무기 소형화 + 미사일 장착	핵무기 병기화
전 술	SR BM	스커드-B/C 노동 스커드-ER	스커드-B/C, 노동, 스커드-ER ①이스칸데르형 ②에이태킴스형 ③300미리 방사포 ④600미리 초대형방사포 * 발사관 3종(4, 5, 6련장)	기보유 3종 + 신형 4종 추가 완성. TEL, 정확도, 저고도, 사거리 확대
전 략	MR, IR, ICB M	무수단 (*시험발사 미 실시) KN-08 (*시험발사 미 실시) *기만용 장비	①고체추진 북극성-2형 (지대지) ②화성-12형 ③화성-14형 ④화성-15형 ⑤추정 화성-16형(다탄두) *시험발사 미 실시	고체, TEL, 기습타격력 향상 백두산엔진(액체), TEL * 미 본토 타격력
			⑥북극성-3형(잠대지) ⑦북극성-4형(잠대지) *시험발사 미 실시	수중 은밀성, 고체, 발사관 3개 이상 잠수함 *세컨스크라이크/게임체인저
	SLB M			

※ 미사일 총 14종(既 3종 + 新 11종) = 전술 7종(既 3종, 新 4종) + 전략 7종(新 7종)

기보유 3종(스커드·노동계열)과 신형 화성·북극성계열 미사일은 핵탄두장착 능력 보유

김정일 시대는 스커드-B/C, 스커드-ER 및 노동 미사일 등 3종을 보유했지만 김정은 시대에는 무려 11종을 추가적으로 새롭게 개발하여 총 14종의 미사일을 보유하게 됐다. 신형 11종은 전략미사일 7종, 전술미사일 4종이다.

전략미사일은 신형 백두산엔진(러시아제 RD-250개량)을 자체적으로 개발하는데 성공함으로써 이를 기초로 화성계열 중거리탄도미사일(IRBM)과 2종의 대륙간탄도미사일(ICBM) 시험발사에 모두 성공했다. 단지 추정 화성-16형은 시험발사 없이 2020년 10월

10일 당창건 75주년 열병식에서 공개했다(트랙#1). 또한 새로운 고체연료와 콜드론칭 기술을 개발하여 수중플랫폼(시험용 고래급 잠수함)에서 잠수함발사탄도미사일(SLBM) 비행시험과 지상플랫폼에서 탄도미사일인 북극성-2형 시험발사에도 성공했다. 이어서 북극성-3형 SLBM도 수중바지선에서 시험발사에 성공(2019.10)했고, 3개의 발사관을 갖춘 신형 3천톤급 잠수함과 최근 공개한 북극성-4형 SLBM용 3-4개 이상의 발사관을 갖춘 4-5천 톤급 잠수함의 진수도 목전에 두고 있다(트랙#2). 트랙#1, #2의 전략미사일은 미국의 알래스카, 괌, 하와이는 물론 미 본토를 직접 위협할 수 있는 중·장거리탄도미사일로써 총 7종(화성-12/14/15/추정16형, 북극성-2/3/4형)²¹¹⁾으로 모두 신형무기체계이다. 이로써 김정은 시대 북한은 미국의 영토와 미국민을 직접 위협 또는 직접 공격할 수 있는 『직접억제력』을 확보하게 됐다.

한편, 전술미사일은 3종의 기(既) 보유 스커드, 스커드-ER 및 노동미사일에 핵탄두장착 능력과 정확도를 향상시키는 기술적 진전(고도화)이 있었으며, 신형 고체연료추진제를 사용하는 4종의 이스칸데르형·에이태킴스형·대구경 및 초대형방사포를 추가로 개발하여 완성했다(트랙#3). 트랙#3에서 특히 신형 전술미사일은 스커드와 노동미사일과는 다르게 모두 연속발사가 가능한 다련장이며, Pull-Up 요격회피 비행기능 및 30-50km의 저고도 비행으로 상대의 탐지 및 요격이 제한되는 위협을 가지게 됐다. 이러한 전술미사일은 한국군, 주한미군 그리고 주일미군 및 주일 유엔사 후방기지를 모두 위협할 수 있게 됨에 따라 유사시 한국과 일본을 완벽하게 인질로 삼을 수 있는 『간접억제력』을 추가로 향상시켰다.

제2절 김정은 시대 핵·미사일 고도화 전략 전망

김정일 시대 미사일 전력은 단거리인 스커드와 개량형인 스커드-ER 그리고 노동미사일이 주전력이었다. 당시에는 미사일에 장착할 수 있는 핵탄두 소형화 기술도 완성하지는 못했다. 그래서 김정일 시대 북한의 미사일 위협은 단순히 한국군이나 주한미군 그리고 주일 미군 기지를 위협하는 재래식 무기체계로써 북미관계 측면에서 볼 때는 이른바 『간접 억제력』 수준만을 보유했었다고 평가할 수 있다.

그러나 김정은 시대에 들어와 북한은 4차례의 추가적인 고강도 핵실험으로 핵탄두를 소형화했고, 이를 무기화(병기화)²¹²⁾하는 전략적·전술적 운반수단인 탄도미사일을 모두

211) 추정 화성-16형 ICBM과 북극성-4형은 시험발사를 하지 않았기 때문에 시험발사 가능성이 있으며, 시험 발사에 성공해야만이 실제 보유여부를 판단할 수 있음을 밝혀둔다.

212) 김정은 시대 들어 북한은 『핵무기병기화사업』을 2회에 걸쳐 김정은이 직접 현지도했다고 공개했다. 1차 핵무기병기화사업은 2016년 3월 9일 원구형 핵장치를 김정은 사진과 함께 공개했고, 2차 핵무기병기화

고도화함에 따라 기존의 대미 『간접억제력』 보유 위주의 미사일전략에서 과감하게 탈피하여 미국을 직접 공격할 수 있는 대미 『직접억제력』을 추가로 확보하게 됐다.

여기서 『직접억제력』의 함의는 미본토를 직접 공격할 수 있는 핵투발 능력을 갖춘 다양한 전략미사일인 군사적 수단의 추가 확보라는 의미 이외에도 정치·전략적으로 협상에서 유리한 고지를 점유하고 핵보유국 지위를 인정받으려는 북한의 대(大)전략임에 유의해야 한다.

김정은 정권은 선대인 김정일 정권에서 물려받은 대미 『간접억제력』만으로는 결코 미국을 상대할 수 없다는 점을 인식했기 때문에 기존의 현상을 타파하기 위해 미국을 직접 공격할 수 있는 전략미사일을 추가적으로 개발하여 확보함으로써 미국과 대등한 입장에서 핵협상력을 제고시키고자 했다. 미국이 한국이나 중국의 반대로 북한을 쉽게 공격할 수 없다는 점과 미국이 사활적 이익으로 여기는 영토와 국민을 치명적인 취약점으로 북한이 이용함으로써 김정은 정권의 북한은 미국과 대등한 위치에서 전략적 관계를 설정하려는 현상변경의 전략을 전개하고 있다.

그 결과 2018과 2019년 두 차례의 북미정상회담 과정에서 나타났듯이 김정은 정권의 북한은 몸 값을 키운만큼의 대가나 보상을 요구하고 있으며 과거 대비 상수의 입장이 되었다는 것이 작금의 현실이다. 다만 북미간의 비핵화 협상국면 교착 이후 지속적인 제재의 영향 이외에도 설상가상 세계적인 코로나-19 팬데믹 현상이 북한의 충격적인 행동을 지연시키고 있을 뿐이다. 더욱이 비핵화 협상기간에도 불구하고 북한은 추정 화성-16형과 북극성-4형까지 최근 당창건 75년 기념 열병식에서 추가로 공개했다. 자신들의 요구가 관철되지 않을 때 북한은 대외 책임전가와 군사적 도발로 현상을 변경시킬 수 밖에 없는 상황에 직면해 있다. 북한이 처한 경제발전과 핵보유국 간의 양립할 수 없는 딜레마를 극복하기 위해서는 긴장조성과 도발이라는 선택지 외에는 답이 궁색한 것이 북한체제의 속성이다.

미국 대선 결과 바이든이 당선되었으며 새로운 미 행정부가 출범하는 시기까지 북한은 내부를 계속 추스려야 한다. 그리고 8차 당대회를 통해 충격적인 돌파를 시도할 준비를 지속하고 있다²¹³⁾. 향후 예상되는 정면돌파 과정에서 첫 상대는 이미 진행 중인 한국이다.²¹⁴⁾ 다양한 핵투발수단을 완성한 북한이 협상력을 최고조로 높이고 판을 키우기

사업은 2017년 9월 3일 6차 핵실험 직후 장구형 핵장치와 김정은 사진 그리고 화성-14형 핵탄두 설계도를 동시에 공개했다. 북한 핵개발 역사에서 『핵무기병기화사업』 활동은 최초로써 이는 ‘소형화한 핵탄두를 미사일에 장착할 수 있는 무기화’를 의미한다.

213) 북한 8월 29일 제7기 6차 당 전원회의에서 내년 1월 제8차 노동당 대회 개최를 결정했다고 보도했다. 『조선중앙통신』, 2020년 8월 20일.

214) 북한이 지난 6월 16일 개성에 위치한 수백 억짜리 연락사무소를 폭파한 사실이 이를 실증하고 있다.

위해서는 한국 및 한국내 주한미군을 볼모로 하는 간접억제력으로 군사적 도발을 감행할 가능성이 가장 높다. 핵을 가진 북한에게는 유혹을 끄는 위협대상이다. 일종의 조커식 도발카드다. 그래서 한국과의 관계는 위장평화 및 통일전선전략 일환의 책동에 불과할 수밖에 없다. 책임전가와 도발명분을 확보하는데 한국이나 주한미군을 호재로 삼을 수밖에 없는 것이 북한의 입장이자 현실이다. 핵무기를 보유한 인도-파키스탄간 「카길전쟁」 사례처럼 사실상 핵무기를 보유한 북한이 자신들의 요구가 관철되지 않을 때에는 미국의 대한(對韓) 핵확장억제력의 취약점(세부적 이행 계획이 미흡하다는 점)을 이용하여 대남 재래식 군사도발을 감행할 수 있다는 ‘안정불안정 역설’이론²¹⁵⁾이 한반도에서 적용될 가능성에 철저히 대비해야 한다.

IV. 북한 미사일 대응전략

제1절 개 요

국방부는 2020년 8월10일 국방중기계획을 발표하면서 2021년부터 5년간 300조 7,000억원을 투입하겠다는 방침을 밝혔다. 수백조원에 달하는 예산은 한국형 장사정포 요격체계(아이언돔) 개발 등에 관련한 예산에 투입될 예정이다.

지난 30여 년 동안 북한 핵미사일 문제는 계속하여 국제사회의 안보이슈로 주목을 끌고 있다. 시간이 길어질수록 북한이나 대한민국은 상호평화와 번영을 공유할 기회를 잃게 될 것이다. 이러한 측면에서 국방부의 이번 발표는 그나마 다행스런 대비방안이 되겠으나 북한의 위협변화를 고려한 체계적인 전력화가 필요하다.

초대형방사포나 대구경조종방사포는 휴전선에서 멀리 떨어진 지역에서도 발사가 가능하다. 사실상 평양-원산 이남 지역 전체를 사전에 제압해야 하는데, 이는 쉽지 않은 과제다. 북한 장사정포를 공격전에 파괴한다고 해도 예방적 타격과 선제공격의 경계가 모호하다는 점에서 선불리 행동에 옮기지 못하다가 장사정포 공격을 받을 경우 요격체계가 제대로 작동하기 힘들 수도 있다²¹⁶⁾.

215) 국제정치학에 ‘안정-불안정의 역설’(stability-instability paradox) 이론이 있다. 이는 핵무기를 가진 국가간 갈등 해소를 위해 핵무기를 사용하는 전면전쟁은 자제하지만, 낮은 수준의 재래식 무력사용으로 국지도발을 통한 갈등을 해소하려는 가능성은 오히려 높아진다는 이론이다. 대표적인 사례는 1999년 인도와 파키스탄 간에 발생한 인도령(領) 카슈미르지역의 카길(Kargil War)전쟁이다. 이 전쟁은 파키스탄이 핵개발 완료 후 국지전을 통해 국제사회의 관심을 끌어 모아 자국의 이익을 취하려고 인도에 대한 선제공격으로 시작된 전쟁이다. 핵무기 사용없이 전쟁은 종료됐다.

따라서 북한이 개발한 전략적, 전술적 미사일들의 기술적 특징과 위협을 분석하여 정반합의 원리에 따라 대응논리를 구현하여 무기체계를 체계적으로 전력화하도록 해야 한다.

북한은 핵문제 해결을 위한 협상과정에서 지속적으로 벼랑 끝 전술을 구사하고 있다. 북한 입장에서 핵미사일은 대한민국과의 군사력 경쟁에서 우위를 차지할 수 있는 핵심 군사력이자 정권을 보장하는 보루이고, 또한 ‘사회주의 강성대국’ 유지의 실천수단이기 때문에 북한은 핵을 보유하려는 의지가 월등히 강하다는 점을 직시해야 할 것이다.

한국과 미국 등 국제사회는 북한 핵 폐기를 목표로 많은 협상을 추진해왔으며 핵 폐기에 관해 모종의 합의를 이끌어내기도 하였다. 그러나 합의사항이 구체적으로 이행되지 않고 지금까지의 노력이 결실을 보지 못하고 있는 점을 감안할 때 국가 정책적, 전략적 차원의 노력과 함께 군사적 대응전략을 구체화할 시점으로 판단된다. 핵무기의 가공할 파괴력과 핵사용을 전제로 하는 북한의 전략을 고려 시 이러한 비대칭 전력에 대응 가능한 방안을 수립하고 실천해야 할 필요성은 더욱 절실했다. 이에 본 연구는 북한의 미사일 위협에 대비할 수 있는 정책적 대응방안과 군사적 대응방안을 제시했다.

제2절 정책적 대응방안

1. 북핵·미사일 위협 관련 긴밀한 한미정보공조 및 공동정보판단

북핵·미사일 위협에 대한 정밀분석과 유사시 핵무력의 운용양상에 대한 한미간의 실질적인 정보공조와 정보판단이 긴요한 시기이다. 북핵·미사일 위협의 실체를 보는 한미의 시각에 차이가 나면 북한과의 비핵화 협상전략에도 균열이 생기기 때문이다. 또한 유사시 한미공동대응태세에 허점이 생겨 북한에게 억제력을 상실하고 도발의 빌미를 제공함은 물론 적시에 대응할 수 없기 때문이기도 하다.

김정은 정권의 핵무력 고도화 위협의 실체, 전략적 목표 및 의도, 위협양상을 한미간에 긴밀하게 공조 및 판단하는 것으로부터 북핵·미사일 위협을 해결하려는 실마리가 풀릴 것이다. 정부는 정부대로, 정보기관은 정보기관대로 각자 하도록 되어 있는 책임을 질려는 자세부터 가져야 한다. 「탑다운 ↔ 바텀업(Top-down ↔ Bottom-up)」의 양방향 소통이 필요한 시기다. 그리고 정보와 정책의 관계가 조화를 이루어야 할 시기다. 북핵문제 해결의 목표는 전략적·당파적이지 않으면서 진정한 한반도의 평화와 안보를 지향해야 한다.

216) 세계일보 인터넷판 : <https://www.segye.com/newsView/20200814520289>, 2020. 8. 16.

2. 국제적 공조와 한미공동 대응전략 수립

북한의 강점은 회피하고 취약점은 활용해야 만이 북한과 같은 특수체제로부터 얻어낼 수 있는 효과를 극대화할 수 있다.

이제 북한의 강점은 실존하는 핵무기를 보유했다는 것이다. 그것도 미 본토까지 위협 가능한 다탄도 운반수단까지를 보유하고 있으며, 미국과 한국을 위협하는 수단은 요격이 어려운 위협으로 더욱 고도화되어 있음에 유의해서 북한의 사용 위협이나 의지를 확실하게 억제해야 한다. 억제의 방법은 도발할 경우 더 많이 잃는다는 것을 북한이 스스로 인식토록 하는 전략을 개발해야 한다. 또한 북한체제의 필사적인 항전의지도 적절하게 관리되어야 하는 전략 개발도 필요하다.

북한의 취약점은 경제와 외교적 제재에서 나타나고 있다. 국제적 공조가 필요한 사안이기도 하다. 특히 북 중 국경지역이나 동서해 해상에서 이루어지는 밀거래나 중국의 지원이 북핵 비핵화나 도발에 어떤 영향을 주고 있는지를 세부적으로 분석하고 중국의 적극적 동참을 유도하는 전략이 필요하다. 동아시아 핵도미노 현상을 막기 위해서도 중국의 동참을 유도해야 한다.

북한 핵의 완전한 비핵화 이전까지는 긴밀한 한미공조와 연합방위태세가 더욱 필요하고, 한미가 같은 목소리와 같은 전략으로 북핵 비핵화를 리드해야 한다. 특히 우리는 핵이 없기 때문에 더욱 그렇다.

3. 북한의 미사일 기술 교류 원천 차단을 위한 외교노력 강구

2020년 9월 미국은 북한의 미사일 개발에 협조하는 국가와 단체에 대해 경고 메시지를 보냈다. 미국 대선을 2개월 앞둔 상황인지라 돌발 상황을 막기 위한 관리용이라는 해석도 있지만 모두 19장으로 이뤄진 이 문건은 북한의 미사일 개발에 협조하지 말라는 경고로 이루어져 있다. 북한의 핵무기 확산 활동에 대응하려는 미국의 관련 법 조항을 따라, 법을 어길 경우 UN 등 국제사회에서의 제재가 가해질 수 있다는 내용을 담고 있다²¹⁷⁾.

북한 미사일에 사용되는 주요 부품 목록을 비롯하여 미국의 제재를 받는 북한 인사 및 기관의 명단도 들어 있다. 특히 “북한은 기초적인 부품을 얻기 위해 중국이나 러시아와 같은 해외 설립 기업들과 합작하기도 한다”며 중국과 러시아를 직접 거론하기도 했다. 미국이 중·러에게 북한 미사일 개발에 대한 경고를 내놓은 것은 처음이다. 북한의 불법적인

217) mbc헤드라인뉴스, “북 탄도미사일 협조말라”, 2020.9.2.

선박 이용이나 사이버 적대행위 등에 대해서는 꾸준히 경고를 했지만, 미사일 개발과 조달을 문제로 삼진 않았었다.

미 국무부는 “북한의 탄도미사일 역량 확대가 국제 사회에 중대한 위협이 되고 있다”며 “부주의하게라도 북한 미사일 조달에 지원했다가 제재 대상이 될 수 있다는 점을 알고 있기를 촉구한다”고 주의보 발령의 배경을 설명했다.

하지만, 현지 언론은 북미간 협상이 교착상황에 빠진 상태에서 오는 2020년 11월 열리는 미국 대선에 앞서서 미사일 발사 등 대미 무력시위를 경고하는 트럼프 대통령의 메시지로 해석된다고 했다. 미국의 주의보 발령으로 북한의 미사일 개발을 막겠다는 의지가 확연히 드러났기 때문에 오히려 북한이 강하게 반발할 가능성도 제기했다.

북한 탄도미사일 기술교류는 김정일 시대로 거슬러 올라간다. 1998년에 북한은 당시 개발한 노동1호 기술을 파키스탄에 제공하게 된다. 북한은 파키스탄에 노동1호 기술 이전을 해주고 파키스탄은 북한에 핵 관련 기술을 이전하게 되는데, 구체적으로 우라늄 농축 기술과 원심분리기 제작이 가능한 설계도 및 부속품과 완제품까지 북한으로 이전하게 된다.



〈그림 4-1〉 북한의 국제 핵 밀거래 네트워크

* 출처 : 인터넷블로그 (<https://blog.naver.com/notenter9/221210221828>, 2018. 2월)

핵기술을 가지고 있는 파키스탄은 핵탄두를 운반할 미사일 기술이 필요했으며 북한은 핵 기술이 필요하여 서로의 이해타산이 맞았던 것이다. 이슬람권인 파키스탄의 핵무기

투발기술을 전수함으로써 이슬람권에 핵 무기화를 주도한 북한은 이란과 리비아, 시리아에도 핵관련 기술을 제공했으며 말레이시아에는 생산공장까지 만들기도 하였다.

이 당시 제공된 기술은 주로 스커드 계열의 기술이었으나 이후에 제공된 노동1호 미사일 기술은 의미가 매우 달랐다. 사거리가 1,000km가 넘는 미사일은 전략무기로서의 역할을 하여 이 지역의 힘의 균형을 깨기에 충분하였다.



〈그림 4-2〉 이란의 샤하브-3 (노동1호 미사일)

* 출처 : 인터넷블로그 (<https://blog.naver.com/notenter9/221210221828>, 2018. 2월)

이란이 도입한 북한의 노동1호 미사일(샤하브-3)은 이스라엘을 위협하는 수준 이상의 중동 전체에 영향력을 행사하게 됐다. 이러한 미사일 네트워크는 북한과 파키스탄의 핵 기술을 연결하는 매개체가 되었던 것이다. 북한에 핵기술을 제공한 압둘 칸은 자신의 조국에서는 영웅이었으나 가장 위험한 분쟁지역인 한반도에 핵 구름을 드리게 한 원흉이기도 하다.

이제는 단순한 위협 수준을 넘어서 실질적인 위협이 되어버린 북한의 장거리 미사일의 핵 투발기술은 어느 나라도 범접할 수 없는 고도의 기술이 되었다. 그러나 미사일의 핵심 기술에 들어가는 중요 부품이나 원료 중에서 해외에서 도입할 수 밖에 없는 것들은 결국 북한에 제공하는 루트를 차단하면 된다는 것이다. 미국정부가 전 세계를 상대로 북한에 미사일 기술관련 제공을 금지하는 경고를 한 것은 매우 시의 적절한 조치다.

한미동맹의 협조차원으로 지금까지 이루어진 북한의 미사일 관련 기술 교류 루트를 분석하고 전 세계가 공식적으로 대응하는 모습을 보인다면 머지않아 북한의 미사일 부품들은 수명을 다할 것이고 결국은 핵협상 테이블로 유도하는 요인이 될 것이다.

제3절 군사적 대응방안

한국에서는 북한 미사일과 핵에 대해 연구가 이루어지고 있다. 본 연구에서는 학술지에 게재된 논문들 중에서 군사적 대응 논리를 제기한 연구들을 종합하여 이를 본 연구의 큰 축인 북한 미사일에 대한 군사적 대응 방안을 위한 논리의 근거로 적용하였다.

박훈희(2018)²¹⁸⁾는 북한 핵미사일 위협과 관련 있는 4대 강대국들의 이해관계를 주제로 연구했다. 중국과 러시아는 미국과 일본이라는 태평양 세력에 대응하기 위한 최전방의 완충지대 역할자로서 북한이 필요한 입장으로 인식했고, 따라서 북한의 핵미사일 위협을 방관하고 있다고 보았다. 또한 미국과 일본은 북한의 핵미사일 위협이 현실화되자 보다 공세적이고 적극적으로 억제하려는 입장이라고 평가했다. 또한 대한민국은 핵에 의한 피해 확률이 가장 높은 당사자로서 북한이 핵미사일로 대한민국을 공격하지 않도록 강한 억제력을 구축해야 한다고 주장하였다. 그러면서 현실적으로 북한의 핵미사일 위협에 대한 한국의 자력만으로 대응하기 제한됨에 따라 현실적인 방책으로 미국의 맞춤형 확장억제 전력을 활용하는 방안과, 장기적으로는 대한민국 자체의 억제전력을 구축하는 방안을 대안으로 제시했다.

차경재(2018)²¹⁹⁾는 핵무기는 반인륜적인 대량 살상무기로 전 세계적으로 감축하려고 노력하기 때문에 북한의 핵미사일에 대해 동일하게 핵미사일을 사용해서는 안된다고 주장한다. 그러면서 오늘날 첨단 재래식 무기는 비록 핵무기 위력만큼은 아니더라도 핵무기보다 안전하고 유용하게 핵무기 자체를 무력화시킬 수 있다는 강점을 활용하는 논리를 제시했다. 그는 한국형 미사일 방어체계(KAMD: Korea Air and Missile Defense, 2006년)와 한국형 킬체인(Kill Chain, 2013)에 이어 북한의 5차 핵실험 이후에는 대량응징보복(KMPR: Korea Massive Punishment and Retaliation)을 포함한 한국형 3축 체계²²⁰⁾를 대안으로 제시하고 있다.

이밖에도 임정섭(2020)²²¹⁾은 NATO식 전술핵을 재배치 하는 등 고강도 군사조치를 미국과 적극 논의할 필요가 있다고 주장하며 특히 북한 정권의 핵전쟁 방지를 위해 핵 시설에 선제적 군사공격을 실행할 수 있는 군사력을 가져야 한다고 주장하기도 하였다.

이와 같은 연구들을 종합하면 개략 두 가지 연구로 종합이 된다. 첫 번째는 한미동맹이라는 큰 틀에서의 군사력 활용 측면의 대응과 두 번째는, 한국군 자체적으로 가져야 할

218) 박훈희, '북한 핵미사일 위협에 따른 대응방안 연구' 한성대학교 석사학위논문, 2018.

219) 차경재, '북한 핵 미사일 위협에 대비한 한국형 3축 체계 연구', 충남대박사학위논문, 2018.

220) 한국군은 3축 체계를 핵·WMD 대응체계로, 킬체인을 전략표적타격, 대량응징보복을 압도적 대응으로 용어를 바꾸기로 하였다('킬 체인' '대량응징보복' 과격한 용어 사라진다, 한겨레, 2018.12.10.).

221) 임정섭, '북한의 군사위협 변화에 관한 연구', 한성대학교 석사학위논문, 2020.

대응 능력에 대한 방안 제시이다. 이에 대한 구체적인 대응 논리를 다음과 같이 정리했다.

1. 한미동맹 군사력 활용

한미 양국은 2016년 10월 한미 간 맞춤형 억제전략을 적용하기 위한 의도에서 북핵에 대비, 한반도상 미국 전략무기를 상시로 순환 배치하는 방안을 검토하기로 합의했다. 미국 전략사령부는 통제전력과 부대를 한반도에 순환배치 할 전략무기로 판단하고 있고, 이러한 자산들은 핵무기를 탑재할 수 있는 능력이 있다.

따라서 한미동맹 군사력 활용방안 중 첫 번째로 고려할 대상은 미국의 전략자산이다. 미군의 전술핵 투발이 가능한 전략폭격기는 다음 <그림 4-3>과 같다.

 B-52	 B-2	 B-1B
길이 / 폭 / 높이 48m / 56.4m / 12.4m	20.9m / 52.1m / 5.2m	44.5m / 41.8m / 10.4m
최대 속도 마하 0.95	마하 0.95	마하 1.25
최대 항속거리 1만6,000 km	1만2,000 km	1만2,000 km
탑승인원 6명	2명	4명
특징 및 주요 탑재무기 · 1950년대 실전 배치 · 핵폭탄, 정밀유도폭탄과 공중 발사 순항미사일 등 최대 271 탑재	· 스텔스기, 1990년대 실전 배치 · 핵폭탄, 재공16발, GPS형 JSOW 16발, 500파운드급 JDAM(GBU-30) 80발, 2천파운드급 JDAM(GBU-32) 16발 등 최대 221 탑재	· B-52 대체용으로 개발, 1980년대 실전 배치 · 핵폭탄, GBU-31, GBU-38, GBU-54 정밀 유도폭탄 등 최대 561 탑재

<그림 4-3> 미국의 전략폭격기

* 출처 : 연합뉴스, 2016년 9월 11일.

B-1B 폭격기는 2시간이면 광에서 한국까지 비행이 가능하다. 1회에 2,000파운드(약 900kg)급 합동정밀직격탄 24발, 비유도재래식 폭탄 84발 적재가 가능하다. 스텔스의 대명사인 B-2 폭격기는 적의 레이더에 포착되지 않는 기술인 스텔스'를 이름으로 명명하여 알려진 폭격기로 적진에 침투해 핵폭탄을 투발할 수 있다. '성층권의 요새'라는 B-52 폭격기는 1952년 첫 비행을 시작으로 베트남전에서 용탄 폭격으로 이름이 알려졌고, 이라크전(1990년)과 아프간전(2000년)에 배치되어 명성을 확인한 미국의 전략무기이다.

현존 최강의 전투기인 F-22 랩터는 지구상의 모든 전투기의 제왕으로 불리며, 가장 발전된 전투기 기술의 집합체로 '초절정 병기'로 불려지고 있다. 1997년에 첫 비행을 시작으로 2014년 IS사령부를 파괴한 실전경험이 있으며 뛰어난 스텔스 성능으로 지상공격과

전자전을 위한 장비도 탑재되어 있다. 이 밖에 한반도에 가장 먼저 도착이 가능한 항모로는 대륙간탄도미사일(ICBM)로 무장한 핵잠수함 ‘펜실베이니아호’와 핵 항공모함 ‘로널드 레이건호’ 등이 있다²²²⁾.

두 번째로 고려할 수 있는 자산은 아래 <그림 4-4>와 같은 고고도 미사일 방어체계(THAAD)를 활용하는 것이다.



<그림 4-4> THAAD 요격시스템과 구성

* 출처 : 좌(조선미디어, 2016년 8월 15일), 우(뉴시스, 2016년 7월 8일)

미국의 고고도 미사일 방어체계(THAAD)²²³⁾는 지난 1987년 개발된 소련 전역탄도 미사일에 대한 대응책으로 미국 육군 전략방어사령부에 의해 수행된 대기권 탄도미사일 상층방어 연구에서 시작된 것으로 알려지고 있다. 걸프전 시 미군의 패트리엇(Patriot)는 이라크의 알 후세인(Al Hussein)과 스커드(Scud) 탄도미사일 요격에 성공하기도 하였지만, 패트리엇은 특정 지점만을 방어하는 방공무기체계로 개발되어, 광범위한 지역방어가 불가능했다. 또한 요격고도가 10~20km로 탄도미사일 요격이 제한적이었으며, 높은 고도에서 핵탄두가 폭발할 경우 대응이 불가능하다. 이 때문에 패트리엇 요격고도 보다 더 높은 고도에서 광범위한 지역을 방어할 수 있는 탄도미사일 방어체계 필요에 따라 새롭게 개발되었다. 중국의 반대를 무릅쓰고 한반도에 사드배치를 배치한 이유는 북한 미사일이 대한민국 영토 내에서 폭발하는 것을 사전에 예방하기 위함이다. 작전 절차를 살펴보면, 인공

222) 포커스뉴스, 2016년 1월 13일.

223) 고고도 미사일 방어체계(THAAD : Terminal High Altitude Area Defense) : 공중에서 미사일을 탐지·요격하는 시스템으로 기존 방어체계(패트리엇)는 고도 20km 이내에서 요격 가능하지만, 고고도 미사일 방어체계는 150km 상공까지 요격 가능하다.

위성을 활용하여 북한 미사일 공격 징후를 탐지하며, 미사일이 발사되면, AN/TPY-2 레이더를 이용하여 추적하고, 사거리 도달 시 사드포대가 적정고도(100~150km)에서 요격하게 된다. 현재 전력화 배치되어 있어 가장 실효성 있는 대응방안이라 할 수 있다.

세 번째 고려할 수 있는 자산은 미국의 전술핵이다. 북한이 핵 보유국이 되었고 대한민국이 비핵국인 상황 속에서 국가생존 차원에서 제일 긴급하게 추진하여만 할 대책은 북한이 보유한 핵무기를 사용하지 못하도록 억제하는 일이다. 그러기 위해 가장 중요하고 순발력 있게 취할 수 있는 조치는 1991년 12월, 북한의 기만에 의해 서명하고 지금까지 농락당하고 있는 소위 “한반도 비핵화에 관한 공동선언”을 조속하게 무효화하고, 한국에서 철수된 미국의 전술 핵무기들을 다시 환원 배치하는 것이다²²⁴⁾.

그러나 전술핵 재도입 방안은 부정적인 의견도 있다. 이들의 입장은 미국의 핵 비확산 정책과 상충되며 중국의 반발과 국가안보의 대미의존 심화, 국내 반대세력 의 부정적인 의견을 꼽고 있다. 이 중 가장 큰 영향력은 미국의 핵 비확산 정책과 상충되는 면이긴 하나, 최근 북한의 미사일 개발이 지속되면서 미국입장에서 북한 미사일 위협에 대한 대응책이 필요하고, 이를 위해 한반도 전술핵 재배치 방안에 대해 재고할 사항으로 대두되고 있기에 어느 정도는 극복할 수 있는 가능성이 있다. 미국 전술 핵무기 재도입은 예상하는 대로 긍정적인 요소와 부정적인 요소가 있다. 이들 주장과 제안 가운데 가장 중요한 주장과 가치는 대한민국의 생존이다. 대한민국이 없다면 모든 다른 가치들도 의미가 없다. 논의되는 모든 가치와 주장은 우선적으로 대한민국의 생존이 전제되어야 하는 것이다.

2. 한국군 자체 군사적 대응태세 구축

이론적으로 완벽한 미사일 방어체계 구축은 현실적으로 어려움이 있다. 특히 핵미사일은 단 한발이라도 방어망을 뚫으면 미사일방어 시스템을 무의미하게 할 만큼 큰 피해를 줄 수 있다. 이러한 우려는 북한의 핵미사일이 실전배치 될 경우 더 증폭될 것이다.

또한 이론적으로 완벽한 미사일 방어체계가 가능할 수 있는 상황이 오더라도 방어체계를 구축하기까지는 긴 공백이 발생할 것이다. 따라서 한국군 자체 군사적 대응전력은 첫 번째로 북한 미사일 공격에 대응하여 미사일 방어 연장선에서 대응 가능한 개념이 전략표적 타격이다²²⁵⁾.

전략표적 타격은 북한의 핵 위협을 단계별로 구분하여 대응하는 개념이며, <그림 4-5>과 같이 핵 사용임박 단계에서 선제타격을 가하겠다는 것이다. 전략표적 타격은 북한의

224) 송대성, 「우리도 핵을 갖자」(서울 : 기파랑, 2016), pp. 136-137.

225) 김도훈, “북한의 핵·미사일 위협과 군사적 대응전략에 관한 연구”, 조선대학교 대학원 석사학위논문, 2017, pp. 64-65. 본 연구에서는 길제인을 변경된 용어를 사용하여 전략표적 타격으로 기술

핵미사일을 탐지하고 추적하며 타격하는 일련의 단계로 구성된 시스템으로 미사일 지상 시설 표적탐지 1분, 표적지 좌표식별 1분, 타격에 사용될 무기 선정과 발사 결심에 3분 등 과정을 5분 안에 마치고 최소 25분 안에 선제타격을 하겠다는 개념이다.

북한의 방사포와 탄도미사일은 미국을 공격하기 위한 IRBM(중거리 탄도미사일)과 ICBM(대륙간 탄도미사일)과는 달리 발사 준비가 간편하고 단시간 가동되므로 사전에 발사 징후를 탐지하기가 어렵다. 우리 군이 도입한 F-35A 스텔스전투기는 화성-15형과 같은 대형 ICBM미사일의 경우, 징후를 포착하고 발사되기 전 북한 영공에 침투하여 발사위치 추적 후 파괴하는 것이 가능하다. 한국군 미사일 사령부의 현무-2a/b 탄도미사일은 몇 분 만에 즉각 발사 가능해 선제공격을 사전에 차단이 가능하다.



〈그림 4-5〉 전략표적 타격 개념

하지만 방사포나 탄도미사일은 반응시간이 빨라 대응이 매우 어렵다. 아무리 빠른 시간에 공격징후를 인지를 해도 F-35A 전투기가 무기를 장착하고 이륙준비에 상당한 시간이 걸리나 방사포나 탄도미사일이 먼저 발사준비를 마칠 수 있기 때문이다. 그러나 북한의

신형 전술 탄도미사일은 현재 개발 초기단계로 사거리는 짧으면서 그 가격과 비용이 많이 든다는 점이다. 신속한 발사가 가능한 고기동 발사대와 고체 연료, 위성 항법장비 등을 구비하는데 소요되는 비용이 ICBM을 만드는 것보다는 적게 소요되나 이런 단거리 미사일은 대량으로 갖추어야 전략적인 용도로서의 가치가 있다. 따라서 이들을 대량으로 구비하기 위해서는 수조 원 이상의 예산이 소요되므로 북한의 현 상황에서 생산에 한계가 있다고 할 수 있다.

한국군이 최근 시험발사에 성공한 전술지대지유도탄(KTSSM :Korea Tactical Surface to Surface Missile)은 개전초 북한의 170mm자주포와 240mm방사포, 300mm방사포 등의 장사정포 궤도를 파괴하고 스커드 미사일 기반시설을 무력화하기 위한 무기체계이다. 현무-2나 현무-4(가칭)와 같이 북한 전역을 타격하기 위한 것이 아닌 단거리 표적용이다.

한국군의 전술지대지유도탄 KTSSM은 GPS 유도기술을 사용하여 북한 장사정포 진지를 선제 타격이 가능한 핵심 전력이다. 최대사거리 120km로 낙하 시 지하 콘크리트 방호벽을 관통할 수 있다. 동일한 발사대에서 수초 이내에 4발 발사가 가능하는 등 단시간에 대량으로 목표를 파괴할 수 있다. 전술지대지유도탄은 KTSSM- I, KTSSM- II 등 2가지 버전으로 개발되고 있다. 먼저, KTSSM- I은 고정형 발사대에서 발사하는 침투관통형 열압력탄을 사용한다. KTSSM- II는 이동형 발사대에서 발사되는 침투관통형 열압력탄(블록- I) 뿐만 아니라 고풍탄(블록- II)도 운용이 가능하도록 제작됐다.

2017년 육군본부에 대한 국정감사에서 당시 육군참모총장은 “북한의 비대칭 위협을 최단 시간 내 무력화하고 일거에 전장의 판도를 바꿀 수 있도록 육군 전략 개념을 발전시키고 이를 구현할 수 있는 치명적인 전력을 확보할 것”이라며 전술지대지유도탄 KTSSM을 대표적인 무기로 공개했다.



〈그림 4-6〉 대한민국전술지대지유도탄(KTSSM) 비행모습

* 출처 : <https://blog.naver.com/rgm84d/222002014231>

두 번째로 한국군은 ‘한국형 미사일 방어체계(KAMD : Korea Air and Missile Defense)’ 개념을 2010년대에 정립하여 탄도미사일 방어체계를 구축한다는 계획을 구체화 하였다. 북한이 미사일을 발사할 경우 조기경보위성과 공중조기경보통제기, 해상의 이지스 구축함, 지상의 그린파인레이더 등이 탐지하여 탄도유도탄작전통제소(AMD-cell)로 탄도 미사일 공격정보를 전송하고, 작전통제소는 이 정보를 분석해 패트리엇나 천궁 등을 운용하는 부대에 요격명령을 하달하여날아오는 미사일을 공중에서 파괴하는 개념이다. 한국군은 작전 환경 및 여건의 특수성, 재원의 제한 등을 고려하여, 종말단계 하층(고도 10~30km)방어 중심으로 KAMD를 구축하고 있는데 센서체계는 Green Pine 레이더와 이지스 구축함의 SPY-1 레이더와 연동하며 요격체계는 PAC-2/-3, SM-2와 연동하고 이들은 지휘통제소인KAMD-cell 및 美 TMO-cell과 연동이 가능하도록 구성되어 있다.



〈그림 4-7〉 한국형 미사일 방어체계(KAMD)

〈그림 4-7〉은 2021~2025년 국방중기계획에 포함된 전력을 바탕으로 구성한 한국형 미사일방어체계의 구성도이다. KAMD가 성공하기 위한 요건 중 하나는 적의 표적(미사일)을 발견 및 식별, 추적하고, 타격결과를 평가할 수 있는 공중정밀 감시정찰 능력이 매우 중요

하다. 한국군은 이러한 능력을 확보하기 위해 2025년까지 군사용 정찰위성과 중고도 무인 정찰기 등을 추가로 전력화할 예정이다.

북한 탄도미사일의 비행 고도 변경과 초고속 비행 제어 능력은 선진국의 최첨단 기술로 쉽게 얻을 수 있는 기술이 아니다. 그러나 발사 각도를 낮추어 사드의 최소 요격고도인 40km 미만으로 비행할 수 있다는 평가는 위협분석에서 충분히 이루어졌으므로 이에 대비하여 북한의 신형 전술 탄도미사일 요격이 가능한 국산 지대공미사일인 천궁-2 PIP이나 미국 레이시온사가 제작한 패트리엇 PAC-3 MSE의 추가 도입이 필요한 이유이기도 하다²²⁶⁾.

세 번째로 고려할 수 있는 방안은 압도적 대응개념이다. 압도적 대응개념은 적이 금지된 행위를 감행하게 되면 즉각적이고 강력하게 군사적인 응징보복을 하겠다는 작전개념이다. 이는 북한의 핵무기 등 대량살상무기 사용을 응징보복이 두려워 사전에 포기하게 하여 공격당하기 전에 사전 차단한다는 군사대응책이다. 한국군의 압도적 대응개념은 2016년 9월 북한의 5차 핵실험 이후 북한 전쟁지도본부를 포함한 북한의 지도부를 제거하기 위해 개념을 발전시키고 있다. 현재 한국군이 보유하고 있는 탄도 및 순항미사일 능력으로도 북한군 도발 시 상당수준의 응징보복이 가능한 수준이다. 앞으로 최적화된 발사체계와 대용량 고성능 탄두 등을 개발하고 신편 된 특수임무여단과 함께 응징보복 능력을 극대화할 예정이다. 만약 북한이 핵무기와 화학무기 등 대량살상 무기를 이용하여 대한민국 국민이나 군을 공격하게 되면 응징보복을 한다는 것이다. 현재까지 압도적 대응개념은 개념발전 단계에 있다. 군에서는 압도적 대응개념을 조만간 군사조치를 실행할 수 있는 작전계획 수준으로 구체화할 것이라고 하였다²²⁷⁾.

위에서 제시한 세 가지는 아래 <표 4-1>과 같은 계획으로 전력화가 진행될 예정이다.

<표 4-1> 핵·WMD 대응체계 사업 및 예산

구 분	예 산	추진사항
2014년	1조 1,199억 원	- 전략표적 타격 : 425사업, HUAV, MUAV, 타우러스, 전술지대지유도무기 전력화 등 - KAMD : 탄도탄조기경보레이더-Ⅱ 도입, 철매-Ⅱ 성능개량, 패트리엇 성능개량 및 도입 등 - 압도적대응 : 특수작전용 UAV, CH/HH-47D 개량 등 * 일부예산은 전면전 등과 중복 계상, 북한 핵·미사일 위협에 대비한 플랫폼 전력은 별도 편성
2015년	1조 3,509억 원	
2016년	1조 5,695억 원	
2017년	2조 1,359억 원	
2018년	2조 2,735억 원	

* 출처 : 국방부, “국방예산 보도자료”(2014~2018)

226) 비즈한국, 2019.5.7. <https://post.naver.com/viewer/postView.nhn?memberNo=30808112&volumeNo=19816117>.

227) 김도훈, “북한의 핵·미사일 위협과 군사적 대응전략에 관한 연구”, 조선대학교 대학원 석사학위논문, 2017,

마지막 네번째로 다양한 4차 산업혁명의 첨단 과학 기술을 접목한 대응이다. 북한의 신형 전술 탄도미사일과 방사포를 제거하기 위해 개발 중인 드론 무기들을 활용한 타격 체계를 적용할 필요가 있다. 국방과학기술연구소(ADD)는 체공형 스텔스 타격체계라는 전술용 드론을 개발 중이다. 이 드론의 크기는 작으나 내부에 자탄을 탑재하여 비무장지대(DMZ) 북쪽의 장사정포를 공격하고 자폭하는 스마트 자탄 기능을 갖추었다. 비슷한 크기의 자폭 드론보다 동시에 여러 표적 공격이 가능하며 레이더에 잘 포착되지 않는다.

다만 이 스텔스 전술 타격체계는 아직 양산이 확정되지 않았고, 휴전선 근처의 북한 방사포를 공격하는 것으로 만들어져 있어, 향후 본격 개발과 양산에 들어갔을 때 근거리 저가형, 중거리 침투공격형, 그리고 KF-X와 같은 항공기 탑재 후 장거리 침투형 등 여러 버전으로 개발한다면 지금의 공대지 미사일, 유도폭탄보다 훨씬 효과적으로 북한의 전술 탄도미사일을 요격할 수 있다(김민석, 2020).²²⁸⁾

이 밖에도 전방에서부터 차례로 방어를 한다 해도 결국 내 눈 앞으로 날아오는 단 한발의 미사일이라도 막지 못하면 그 피해는 매우 심각하다. 특히 최근에 등장한 북한판 이스칸데르 미사일 등 전술미사일 4종세트는 Pull-up 상승기동을 한다. 이동하는 중간 단계에서 레이더 포착을 최소화하고 요격단계에서 상승하여 공격하는 방식으로 이미 위협분석에서 문제점을 제기하였다. 이러한 미사일의 기동을 맨 끝단에서 저지, 격파하는 능동방어 체계가 필요하다.

이러한 개념을 실현하기 위한 무기체계는 2018년 소요 결정된 ‘장사정포 요격체계 (LAMD: Long-range Artillery Missile Defense)’이다. 이는 발사대에 탑재된 유도로켓을 이용하여 적 장사정 포탄(240mm, 300mm 방사포)을 파괴시키는 고정밀 요격체계이다. 미국은 유사 무기체계인 MHTK(Miniature Hit to Kill : 초소형 직접타격) 개발하여 실전 배치 중이다. LAMD 무기체계는 이스라엘 아이언돔 개념을 적용한 ‘한국형 아이언돔’ 형태로 개발이 될 것이다.



〈그림 4-8〉 이스라엘 아이언 돔

* 출처 : 인터넷 블로그(<https://blog.naver.com/liu1995/221376049568>)

228) 비즈한국, 2019.5.7. <https://post.naver.com/viewer/postView.nhn?memberNo=30808112&volumeNo=19816117>.

최근 ‘2021-2025 국방중기계획’에 한국형 아이언 돔인 장사정포 요격체계 개발 계획이 반영되었다. 아이언 돔은 대공 미사일이다. 돔 형태로 만들어지는 방공망 전역에 대한 요격 시스템이라 붙여진 이름이다. 저고도로 날아오는 로켓포나 박격포탄, 미사일을 방어 하기에 적합하다.

군은 국방중기계획을 통해 “한국형 아이언 돔을 통해 장사정포 위협으로부터 수도권 및 핵심 중요시설을 방호할 것”이라고 밝혔다. 군은 2020년대 중반부터 2030년까지는 아이언 돔을 전력화한다는 계획이다.

군은 북한 장사정포에 대해 대(對) 화력전을 통해 대응이 가능하다고 한다. “장사정포를 막을 체계가 군에 없다는 이야기들이 나오는데, 사전에 공군 전력으로 포병들이 갭도에서 나올 때부터 징후를 식별해 포를 발사하기 전에 우리 군이 보유한 미사일로 진지를 타격해 무력화시킬 수 있다”며 “보다 완벽하게, 2중 3중으로 방어체계를 갖추기 위해 아이언 돔을 개발하는 것”이라고 하였다.

전술미사일 4종세트 등이 실전에 대량으로 배치되기 전에 이들을 막을 대응체계인 장사정포 요격체계를 빠른 시간에 실전배치하여 다층방어체계를 구축해야 한다.

제4절 대응전략 평가

북핵·미사일 위협에 대해 정책적, 군사적 대응방안에 대해 살펴보았다. 위협에 대한 대응은 지나친 대안이 있을 수 없다. 한 국가가 총력을 기울여 적어도 국민과 국토에 대한 안전을 보장한다는 것은 현 정치를 책임지는 자들의 몫이다.

그러나 최소한 관련분야에서 이를 연구하는 연구자들은 올바른 정책대안을 제안할 수 있어야 한다. 모든 가능성을 열어두고 제안하여 그것을 성사시킬 수 있는 국력과 여건이 되었을 때 전체를 채워가야 한다. 그럼에도 불구하고 현재 우리의 문제는 그것을 채울 마스터 플랜이 매우 미흡한 실정이다. 이번 기회에 큰 그림을 그릴 수 있는 대안을 제시할 수 있다면 본 연구는 그 의미를 더할 것이다.

북한 미사일에 대한 현재의 위협과 앞으로의 전망을 토대로, 이 장에서는 북한 미사일 대응 방안을 제시하였다.

정책적 대응방안에 대한 평가는 일반적인 수준에서도 개략적인 평가가 가능하겠으나 군사적 대응방안은 기술 수준에 대한 평가가 필요하므로 SPND(Service-Platform-Network-Device) 분석²²⁹⁾방법을 적용하여 평가하였다. 재구성한 질문지를 이용하여

229) IoT 오픈 플랫폼 기반 스마트시티분야 서비스 사례집(2018. 9), 한국정보통신산업연구원, pp. 60-60.

국내 최고의 방산업체인 H사의 해당분야 임직원 18명을 대상으로 전문가 설문을 실시하고 이를 종합하여 아래 <표 4-2>로 제시하였다. SPND기법은 최신기술이나 아직 구현되지 않은 기술에 대해 전문가들의 설문을 통해 해당 사업의 진행정도를 평가하는 방법으로 적용되고 있다. 전문가들은 해당 항목에 대해 1~7까지 기술 구현의 정도를 낮은 점수에서 높은 점수 순으로 체크하여 의견을 제시하면 분석자는 이를 종합하여 평가를 하게 된다. 종합결과 A는 즉각 적용이 가능한 수준이며 B는 구체적인 실현계획에 반영된 수준, C는 개념정립 수준으로 평가할 수 있다. 이 방법은 단순히 무기체계의 기술적 수준을 전문가의 개략적인 평가로 대응 수준을 평가한 것이다. 북한의 미사일에 대한 대응 능력 평가는 북한의 미사일 운용환경 변화에 따라 매우 민감하며 한국의 대응체계 또한 다양한 시나리오로 고려해 볼 수 있다. 이러한 시나리오는 군사 작전적 배경을 고려하여 기술적 운용능력을 평가하는 방법이 보다 과학적이다. 그러나 본 연구는 단순히 제시된 위협에 대해 포괄적인 대응면에서 볼 때, 한국군의 기술적인 수준을 해당 전문가를 통해 평가함으로써 막연하게 대응수준에 대한 논의 보다는 보다 구체적인 기술수준을 제시함으로써 부족한 분야를 인식하고 대응능력을 확보해야겠다는 논리적 전개를 충족하기 위한 방법으로 SPND 기법을 사용하였다.

<표 4-2> SPND(Service-Platform-Network-Device) 평가 결과

① 전략표적 타격체계에 대한 평가

구분			수준						
유형	분류	세부분류	C			B		A	
			1	2	3	4	5	6	7
S	개념의 구현정도	국가수준 완성도		1	4	5	7	1	
		세계 정책 및 기술수준 비교		1	1	10	5	1	
P	플랫폼 구현 수준	국가 수준 플랫폼 구성			7	6	5		
		세계수준 플랫폼 구성		1	6	5	4	2	
N	세계적인 네트워크	국가수준 네트워킹			5	8	5		
		세계수준 네트워킹			6	3	6	3	
D	디바이스 완성도	개념수준			4	4	8	1	
		연구개발 진행과정			3	11	4		
		체계완성			8	7	3		
합				3	44	59	47	8	
수준별 합산				47			106		8

* 글로벌 경쟁력이 가장 높은 미국을 기준, 1이 가장 낮고 7이 가장 높음.

* 표 출처 : 중장기 ICT 기술정책방향, 한국정보통신산업연구원, 2018.

② 한국형미사일방어체계(KAMD)에 대한 평가

구 분			수 준						
유형	분류	세부분류	C			B		A	
			1	2	3	4	5	6	7
S	개념의 구현정도	국가수준 완성도			5	7	4	2	
		세계 정책 및 기술수준 비교		1	3	7	2	4	
P	플랫폼 구현 수준	국가 수준 플랫폼 구성			5	7	6		
		세계수준 플랫폼 구성			4	7	6	1	
N	세계적인 네트워크	국가수준 네트워킹		1	2	10	5		
		세계수준 네트워킹		1	8	3	4	1	1
D	디바이스 완성도	개념수준		1	4	5	8		
		연구개발 진행과정		2	4	8	4		
		체계완성		1	5	7	5		
합				7	40	61	44	8	1
수준별 합산			47			105		9	

* 글로벌 경쟁력이 가장 높은 미국을 기준, 1이 가장 낮고 7이 가장 높음.

③ 압도적 대응개념에 대한 평가

구 분			수 준						
유형	분류	세부분류	C			B		A	
			1	2	3	4	5	6	7
S	개념의 구현정도	국가수준 완성도			5	7	6		
		세계 정책 및 기술수준 비교			7	8		3	
P	플랫폼 구현 수준	국가 수준 플랫폼 구성		1	3	11	3		
		세계수준 플랫폼 구성			6	5	4	2	1
N	세계적인 네트워크	국가수준 네트워킹		1	3	10	4		
		세계수준 네트워킹			7	5	3	2	1
D	디바이스 완성도	개념수준			5	8	5		
		연구개발 진행과정			6	10	2		
		체계완성			8	7	3		
합				2	50	71	30	7	2
수준별 합산			57			101		9	

* 글로벌 경쟁력이 가장 높은 미국을 기준, 1이 가장 낮고 7이 가장 높음.

④ 4차산업 첨단기술 적용에 대한 평가

구 분			수 준						
유형	분류	세부분류	C			B		A	
			1	2	3	4	5	6	7
S	개념의 구현정도	국가수준 완성도			6	6	5	1	
		세계 정책 및 기술수준 비교			7	7	1	3	
P	플랫폼 구현 수준	국가 수준 플랫폼 구성		1	3	10	4		
		세계수준 플랫폼 구성			6	6	6		
N	세계적인 네트워크	국가수준 네트워크		1	2	10	5		
		세계수준 네트워크			6	4	7	1	
D	디바이스 완성도	개념수준		1	5	8	3	1	
		연구개발 진행과정			8	9	1		
		체계완성		3	10	3	2		
합				6	53	63	34	6	
수준별 합산			59			97		6	

* 글로벌 경쟁력이 가장 높은 미국을 기준, 1이 가장 낮고 7이 가장 높음.

⑤ 한국의 군사적 대응방안 종합 평가

대응방안	평 가			비 고
	C	B	A	
전략표적 타격체계	47	106	8	B
한국형미사일방어체계(KAMD)	47	105	9	B
압도적 대응개념	57	101	9	B
4차산업 첨단기술 적용	59	97	6	B

전문가 설문결과 대체적으로 군사적 대응방안은 B수준으로 구체적인 실현계획에 반영된 수준으로 평가되었다. <표 4-2>의 ⑤를 보면 B수준이라도 4차산업 첨단기술 적용은 아직 개념정립단계로 더욱 관심을 갖고 발전시켜야할 분야로 평가된다.

한국이 많은 국방예산을 투자하여 북한의 무력에 대응할 군사력 건설을 하고 있으나 북한 미사일에 대한 대응능력은 아직 실전에 즉각 대응할 준비가 되지 않고 있다. 즉, 언제라도 공격이 가능한 북한 핵 미사일 위협에 대해 순수한 한국군사력 대응 수준은 계획단계에 머물고 있다는 평가가 된다. 한미동맹 군사력의 도움이 없이는 즉각적인 대응이

제한되는 실정이다.

정책적 대응방안을 포함하여 전반적인 북한 미사일 대응방안을 종합 평가하면 아래 <표 4-3>과 같다.

북한미사일 대응에 대한 종합적인 평가를 한다면, 즉각 대응 가능한 수단이 4종, 계획 중인 방안이 5종, 개념수준이 1종이다. 이 중에서 즉각 가능한 군사력은 한미공조를 통한 정보 및 군사력에 의한 대응으로 아직까지 한국군은 독자적인 북한 핵 미사일 대응수준을 갖추지 못하고 있음을 알 수 있다. 따라서 독자적인 방어능력을 갖추기 위한 군사력 건설을 앞당기고, 최소한 독자적인 능력을 갖추 때까지 한미동맹을 굳건히 하여 대응해 가는 것이 북한 핵미사일에 대한 최상의 대응방안임을 알 수 있다.

<표 4-3> 북한 미사일 위협에 대한 대응방안 종합 평가

구 분		내 용	상 태
정책적 대응방안		① 북핵·미사일 위협 관련 긴밀한 한미정보공조 및 공동정보판단	A
		② 국제적 공조와 한미 공동 대응전략 수립	A
		③ 북한의 미사일 기술 교류 원천 차단을 위한 외교노력 강구	B
군사적 대응 방안	한미 동맹 군사력	① 미군 전략자산(B-2, B-52, F-22, 도널드 레이건호, 펜실바니아호)	A
		② 고고도미사일방어체계(THAAD) 활용	A
		③ 미군의 전술핵 재배치	C
	한국 군사력	① 전략표적 타격체계 구축	B
		② 한국형미사일방어체계(KAMD) 구축	B
		③ 압도적 대응개념 구현	B
		④ 스텔스 드론, LAMD, 극초음속 곡사포 등 4차 산업혁명 첨단기술을 적용한 대응	B

* A : 즉각 적용 가능한 상태 B : 실현계획에 반영된 수준

C : 개념정립 수준

V. 결론

제1절 연구 결과

김정일 시대는 스커드-B/C, 스커드-ER 및 노동미사일 등 3종을 보유 하였으나 김정은 시대에는 11종을 새롭게 추가적으로 개발하여 총 14종의 탄도미사일을 보유하게 됐다. 신형 11종은 전략미사일 7종, 전술미사일 4종이다.

전략미사일은 신형 백두산엔진(러시아제 RD-250개량)을 자체적으로 개발하는데 성공 함으로써 이를 기초로 화성계열 중거리탄도미사일(IRBM)과 대륙간탄도미사일(ICBM) 시험 발사에 모두 성공했다. 또한 새로운 고체연료와 콜드론칭 기술을 개발하여 수중플랫폼 (시험용 고래급 잠수함)에서의 잠수함발사탄도미사일(SLBM) 비행시험과 지상플랫폼에서의 탄도미사일인 북극성-2형 시험발사에 성공했다. 이어서 북극성-3형 SLBM도 수중바지선에서의 시험발사에 성공(2019.10)했고, 3개의 발사관을 갖춘 신형 3천톤급 잠수함과 북극성-4형인 3-4개 이상의 발사관을 갖춘 신형 4-5천톤급 잠수함이 건조 중인 것으로 분석되고 있다.

전략미사일은 미국의 알래스카, 괌, 하와이는 물론 미 본토를 직접 위협할 수 있는 중·장거리탄도미사일로써 총 7종(화성-12/14/15/추정16형, 북극성-2/3/4형)으로 모두 신형 무기체계이다. 이로써 김정은 시대 북한은 미국의 영토와 미국민을 직접 위협 또는 직접 공격할 수 있는 『직접억제력』을 확보하게 되었다.

전술미사일은 3종의 기보유 스커드와 스커드-ER 및 노동미사일에 핵탄두장착 능력과 정확도를 향상시키는 기술 진전(고도화)이 있었으며, 신형 고체연료추진제를 사용하는 4종의 이스칸데르형·에이태킴스형·대구경 및 초대형방사포를 추가로 개발하여 완성했다. 특히 신형 전술미사일은 스커드와 노동미사일과는 다르게 모두 연속발사가 가능한 다련장이며, Pull-Up 요격회피 비행기능 및 30-50km의 저고도 비행으로 상대의 탐지 및 요격이 제한되는 위협을 가지게 됐다. 이러한 전술미사일은 한국군, 주한미군 그리고 주일미군 및 주일 유엔사 후방기지를 모두 위협할 수 있게 되어 유사시 한국과 일본을 완벽하게 인질로 삼을 수 있는 『간접억제력』을 향상시켰다.

이러한 북한 미사일 위협에 대응하여 먼저 정책적 대응방안으로, 첫째, 북핵·미사일 위협 관련 긴밀한 한미정보공조 및 공동정보판단을 제안하였다. 북핵·미사일 위협의 실체를 보는 한미의 시각에 차이가 나면 북한과의 비핵화 협상전략에도 균열이 생기기 때문이다. 또한 유사시 한미공동대응태세에 허점이 생겨 북한에게 억제력을 상실하고 도발의 빌미를

제공함은 물론 적시에 대응할 수 없기 때문이기도 하다.

둘째, 긴밀한 정보공조와 정보판단에 따른 연합대비태세가 유지되어야 하며 셋째, 미국의 핵 확장 억제력 강화 및 한미연합첨단전력의 적시적 SC를 실시해야 한다는 것이다. 북한이 핵무력을 고도화하는데 성공하고, 고도화된 핵무력에 대한 과신과 상응하는 요구조건에 대한 불만으로 안정불안정 역설에 따른 군사적 행동을 하지 못하도록 지속적인 메시지 전달 노력이 체계적으로 관리되어야 한다.

다음은 군사적 대응방안을 제시하였다.

첫째, 한미동맹 군사력을 활용한 방법이다. ① 미국 전략자산을 활용하는 방안으로 전략 무기를 한반도에 상시 배치하는 것이다. 미국 전략사령부는 예하 부대와 통제전력들을 한반도에 순환배치를 하게 될 전략무기로 판단하고 있고, 이 자산들은 핵무기를 운영할 수 있는 능력을 보유하고 있다.

② 미군이 배치한 고고도 미사일 방어체계(THAAD)를 활용하는 방법이다. 한반도에 사드를 배치한 이유는 북한의 핵미사일이 대한민국 영토 상공에서 폭발하는 것을 사전에 예방하기 위함이다. 작전절차를 살펴보면, 인공위성을 활용하여 북한 미사일 공격 징후를 탐지하며, 북한 미사일 발사 후에는 AN/TPY-2 레이더를 이용하여 추적하고, 사거리 도달 시 사드가 이를 적정고도(100~150km)에서 요격하게 된다. 현재 전력화 배치되어 있어 가장 실효성 있는 대응방안이다.

③ 미국 전술핵 재도입이다. 이 방안은 북한의 핵공격을 억제하기 위한 전략으로 북한이 핵미사일로 대한민국을 공격할 경우, 대한민국에 배치된 미국의 전술 핵무기에 의해 몇 배의 보복을 당해서 결국 북한이 멸망케 된다는 확실한 인식을 심어주어 아예 사용할 생각을 하지 못하도록 하는 것이 근본목적이다. 예측이 어려운 북한정권이라도 자멸하는 행위를 선택하지는 않을 것이다. 미국의 전술 핵무기 재배치는 이러한 위협과 공포에 처한 상황에 대한 균형을 기한다는 장점을 갖고 있다.

둘째, 한국군 자체 군사적 대응태세를 갖추는 것이다. 이를 위해 ① 전략표적 타격체계를 전력화 중이다. 전략표적 타격체계는 북한의 핵미사일 위협을 단계별로 구분하여 대응하는 체계로 북한의 핵미사일 사용임박 단계시 선제타격 하겠다는 개념이다. 이를 위해 한국군은 북한의 신형 전술 탄도미사일 요격이 가능한 국산 지대공미사일인 천궁-2 PIP이나 미국 레이시온사가 제작한 패트리엇 PAC-3(MSE)의 추가 도입을 추진하고 있으며, 북한 장사정포 진지를 선제 타격이 가능한 '킬체인'의 핵심 전력인 전술지대지유도탄 KTSSM 등을 전력화 하고 있다.

② 한국형 미사일 방어체계(KAMD)로 대비하고 있다. 북한이 미사일을 발사할 경우 조기경보위성과 공중조기경보통제기, 해상의 이지스구축함, 지상의 그린파인레이더 등이

탐지하여 탄도유도탄작전통제소(AMD-cell)로 탄도미사일 공격정보를 전송하고, 작전 통제소는 이 정보를 분석해 패트리엇나 천궁 등을 운용하는 부대에 요격명령을 하달하여 날아오는 미사일을 공중에서 파괴하는 개념이다.

③ 압도적 대응개념이다. 이는 적이 금지된 행위를 감행하게 되면 즉각적이고 강력하게 군사적인 응징정보복을 하겠다는 작전개념이다. 이는 북한의 핵무기 등 대량살상무기 사용에 응징정보복이 두려워 사전에 포기하게 하여 공격당하기 전에 사전 차단한다는 군사대응책이다. 압도적 대응개념은 북한 정권이 한국군의 대량응징정보복 계획만으로도 극도의 공포와 충격을 느끼고 핵미사일을 사용하지 못하게 억제하는 개념이라고 할 수 있다. ④ 스텔스 드론, LAMD, 극초음속 곡사포 등 4차 산업혁명 첨단기술을 적용한 대응방안을 제시하였다.

제2절 시사점 및 정책제안

본 연구는 다음과 같은 시사점과 정책제안을 할 수 있다.

첫째, 핵미사일 체계를 구축한 북한은 미국 대선을 앞두고 내부를 추스르고 있다. 그리고 충격적인 돌파를 시도할 준비를 지속하고 있다는 것이다. 향후 예상되는 첫 상대는 이미 진행 중인 한국임으로 다양한 핵 투발수단을 완성한 북한이 협상력을 최고조로 높이고 판을 키우기 위해서는 한국 및 주한미군을 볼모로 하는 간접억제력으로 군사적 도발을 감행할 가능성이 가장 높다. 그래서 한국과의 관계는 위장평화 및 통일전선전략 일환의 책동에 불과할 수 밖에 없다는 것이다. 책임전가와 도발명분을 확보하는데 한국만큼 호재가 없는 것이 북한의 입장이자 현실인 것이다. 핵무기를 보유한 인도-파키스탄간 카길 전쟁 같은 우발상황에 대비해야 한다.

둘째, 북한 미사일의 위협에 대응하여 정책적 대응방안을 제시하였다. 군사적 대응은 많은 비용과 희생을 감수해야 하는 최종 선택이며 먼저 정책적으로 국제적인 공조를 통해 북한 핵미사일 개발을 억제하고 핵 기술 유입 루트를 차단하여 스스로 포기하도록 하는 정책이 바람직하다.

셋째, 북한 미사일의 위협에 따른 군사적 대응으로 현재까지는 주로 외교·정치적인 대응방안 위주로 진행한 것이 사실이나 김정은 집권이후 도약적으로 발전한 북한 미사일의 위협과 능력을 분석하고, 북한의 미사일 위협을 극복하기 위한 실질적인 군사적 대응방안을 열거하고 이를 평가 하였다. 각 방안별로 SPND 분석척도를 만들어서 전문가에 의한 평가를 종합 분석한 결과 한국군의 북한미사일에 대한 대응책은 많은 노력을 통해 향상되고 있으나 전반적으로 B수준으로 아직까지 실전에 적용한 수준은 부족하고 계획단계에 머무르고

있음을 알 수 있었다. 북한 미사일 위협을 구체화하고 위협별로 대응 시나리오를 만들어 위기조치 계획에 포함해야 하며 위협에 대응하기 위한 대응 전력은 그때 그때 일시적으로 대응하는 수준으로 전력화하면 비용도 많이 들고 효과도 떨어지게 된다. 따라서 북한 미사일에 대응하는 마스터플랜을 세우고 기초부터 차근차근히 구축해 나가서 결국 냉전 시대에 소련이 미국의 스타워즈 계획에 포기하고 탈냉전으로 간 것처럼 북한이 스스로 핵미사일 구축을 포기할 수 있도록 대응전력을 선제적으로 구축 해 가야 한다.

제3절 연구의 한계점과 향후 연구 방향

본 연구는 시사점도 많으나 아래와 같은 한계점도 있다.

첫째, 본 연구는 북한에서 보도하는 자료들과 국내 보도 자료, 연구자료 등 문헌연구에 치중할 수 밖에 없었다. 추후 심도 있는 연구를 위해 실제 현장에 종사한 탈북 과학자나 접촉이 가능한 중·러 과학자 등으로부터 지속적인 첩보 보강을 통해 보다 실질적인 검증이 요구된다.

둘째, 북한 미사일에 대한 학술적 연구가 미흡하다. 특히 미사일의 기술적 분석 자료가 미흡하여 이를 정책적 연구에 적용하기가 제한된다. 기술에 대한 보호와 정보유출 방지로 인한 한계로 생각되어진다. 공개된 자료는 부족하고 학술연구는 많이 미흡한 상태로 이 분야에 대한 공개된 논의가 활성화 되고 학술적인 연구가 병행될 필요가 있다.

향후에는 군과 민간학술 연구기관이 함께 연구된 자료들을 토대로 기술적 분석과 위협 분석, 대응방안에 대한 실질적이고 적용 가능한 대안이 제시될 수 있기를 기대한다.

〈참고 문헌〉

1. 단행본

- 국방대학교. (1985). 『방위학 개론』, 서울 : 국방대학교.
- 국방대학교. (1993). 『억제전략의 이론과 실제』, 서울 : 국방대학교.
- 국방부. (2014). 『국방백서 2014』, 서울 : 국방부.
- 국방부. (2017). 『국방백서 2019』, 서울 : 국방부.
- 권태영 외. (2014). 『북한 핵·미사일 위협과 대응』, 성남 : 북코리아.
- 공성진 외. (2008). 『한국 안보전략 2008-2013』, 서울 : 시대정신.
- 김황록. (2020). 『김정은 정권의 핵·미사일 고도화와 미국상대하기』, 서울 : 블루리본.
- 비피기술거래. (2017). 『사드배치가 한반도에 미치는 경제분석보고서』, 전주 : 비피 타임즈.
- 송대성. 『우리도 핵을 갖자』, (서울 : 기파랑, 2016), pp. 136-137.
- 전성훈. (2004). “억지이론과 억지전략에 대한 소고”, 『전략연구 통권 제31호』, 서울 : 한국 전략문제연구소.
- 정영태. (2017). “북한의 핵·미사일 위협과 우리 군의 대비태세”, 『합참 제73호 가을호』, 서울 : 합동참모본부.
- 조홍제. (1993). 『미사일 방어와 한국의 선택』, 서울 : 한누리미디어.
- 한국정보통신산업연구원. (2018). 『IoT 오픈 플랫폼 기반 스마트시티분야 서비스 사례집』, pp. 60-60.
- 한응섭. (2007). “미국의 맞춤형 억제전략과 북한의 핵위협 해소방안”, 『국방연구 제50권 제2호』, 서울 : 국방대학교.
- 함형필. (2007). “북한의 고농축우라늄 핵개발 상황과 우리의 대응방향”, 『국방정책연구 2007년 겨울』, 서울 : 한국국방연구원.
- 홍용표. (1999). 『북한의 미사일 개발전략』, 서울 : 통일연구원.

2. 논문

- 김도훈. (2017). “북한의 핵·미사일 위협과 군사적 대응전략에 관한 연구”, 조선대학교 정책 대학원 석사학위논문.
- 김영태. (2013). “북한의 핵위협에 대한 한국의 대응전략”, 경기대학교 대학원 석사학위논문.
- 김황록. (2020). “김정은 정권의 핵무력 고도화와 우리의 대응방향”, 한국국가정보학회 2020 하계학술회의.

- 박훈희. (2018). ‘북한 핵미사일 위협에 따른 대응방안 연구’ 한성대학교 석사학위논문.
- 염규현. (2011). “북한 핵문제 대응방안에 관한 연구”, 한성대학교 국방과학대학원 석사학위논문.
- 임정섭. (2020). ‘북한의 군사위협 변화에 관한 연구’, 한성대학교 석사학위논문.
- 정병호. (2007). “북핵 실험 이후 북한의 군사구조의 지속성과 변화”, 서울 국방대학교.
- 채수민. (2013). “북한 탄도미사일 개발전략 연구”, 북한대학원대학교 석사학위논문.
- 차경재. (2018). ‘북한 핵 미사일 위협에 대비한 한국형 3축 체계 연구’, 충남대박사학위논문.
- 최정우. (2013). “북한의 탄도미사일 개발에 관한 연구”, 동국대학교 대학원 석사학위논문.
- 황현식. (2013). “북한의 핵실험에 따른 군사적 대응전략 연구”, 한성대학교 국방과학대학원 석사학위논문.
- Joseph S. Bermudez Jr, “The North Korean Navy Acquires a New Submarine,” 38 NORTH, 19 October 2014; <https://www.38north.org/2014/10/jbermudez101914/>

3. 언론보도

〈한국〉

- 연합뉴스, 2020년 11월 25일.
- 조선일보, 2017년 7월6일.
- 연합뉴스, 2017년 7월6일.
- 조선일보, 2017년 7월7일.
- 조선일보, 2017년 7월10일.
- 한겨레신문, 2017년 11월30일.
- 주간동아, 2017년 12월19일.
- 민플러스, 2017년 12월4일, 2018년 2월15일.
- 한국일보, 2017년 11월29일.
- 노컷뉴스, 2017년 9월10일.
- 주간동아, 2017년 12월19일.
- 연합뉴스, 2014년 9월14일.
- 중앙일보, 2016년 8월27일.
- 세계일보, 2020. 8월16일.
- 포커스뉴스, 2016년 1월13일.
- mbc 헤드라인뉴스, 2020년 9월2일.
- 조선미디어, 2016년 8월15일.

뉴시스, 2016년 7월8일.
비즈한국, 2019년 5월7일.

<북한>

조선중앙TV, 2020년 10월 10일.
로동신문, 2017년 3월 19일; 2017년 5월 15일.
조선중앙통신, 2016년 4월 9일; 2017년 3월 18일.
로동신문, 2017년 7월 29일.
로동신문, 2017년 7월 31일.
로동신문, 2017년 11월 29일.
조선중앙방송, 로동신문 2015년 5월 9일.
로동신문, 2016년 4월 24일
조선중앙통신, 2016년 8월 25일.
조선중앙통신, 2017년 5월 29일.
조선중앙통신, 2020년 8월 20일.

4. 기타

네이버 지식백과, <http://terms.naver.com/>
인터넷블로그 (<https://blog.naver.com/notenter9/221210221828>, 2018. 2월)
인터넷블로그 (<https://blog.naver.com/notenter9/221210221828>, 2018. 2월)
인터넷 블로그(<https://blog.naver.com/liu1995/221376049568>)

〈Abstract〉

Hwang rok, Kim

Dong ho, Shin

The Kim Jong-il era had three types of missiles: Scud-B/C, Scud-ER and Rodong missiles, but during the Kim Jong-un era, 11 new types of ballistic missiles were developed, bringing the total number of ballistic missiles to 14. The new 11 types are seven strategic missiles and four tactical missiles.

The strategic missile developed its own new Baekdusan engine and completed the Hwasung Intermediate-Range Ballistic Missile (IRBM) and Intercontinental Ballistic Missile (ICBM), and the presumed Dartanduyong Hwasong-16 was unveiled before the test-firing. It also succeeded in developing new solid fuel and cold-drone technology to test submarine-launched ballistic missiles (SLBM) on underwater platforms and to test-fire the North Star-2 type, a ballistic missile on ground platforms. Subsequently, the North Star-3-type SLBM succeeded in test-firing a submarine (2019.10) and is currently building a new 3,000-ton (Polaris-3) and 4-5, 000-ton (Polaris-4) submarine with three or more launch tubes.

Strategic missiles are medium and long-range ballistic missiles that can directly threaten the U.S. mainland, as well as Alaska, Guam, Hawaii, and the U.S. All seven types (Hwasong-12/14/15/estimated 16, North Star-2/3/4), which are all new weapons systems. As a result, North Korea has secured additional direct deterrence against U.S. territory and direct attacks on the American people.

Tactical missiles had advanced technology to improve the ability and accuracy of nuclear warheads on three types of holding Scuds, Scud-ERs and Rodong missiles, and developed four additional Iskander, ATK, Daegu, and large-scale radars using the new solid fuel propellant. Unlike Scud and Nodong missiles, the new tactical missile is a multiple launch site, and the full-up interceptor flight technology and low-altitude flight of 30 to 50 kilometers have made it difficult for South Korea and the U.S. to detect and Japan.

The tactical missiles could threaten both the South Korean military, the U.S. Forces Korea and the U.S. military in Japan and the U.N. base in Japan, enhancing indirect deterrence to take South Korea and Japan completely hostage in case of emergency.

The countermeasures against these North Korean missile threats were studied by dividing them into policy and military measures.

In a policy response, the government first proposed close South Korea-U.S. intelligence cooperation and joint intelligence judgment on North Korea's nuclear and missile threats. If South Korea and the U.S. differ in their views on the reality of North Korea's nuclear and missile threats, their strategies for denuclearization negotiations with the North will also be cracked. It is also because the South Korea-U.S. joint response posture is flawed in case of an emergency, thereby losing deterrence and providing an excuse for provocations, as well as being unable to respond in a timely manner. Second, it suggested that the combined readiness should be maintained by close intelligence cooperation and intelligence judgment, and third, that the U.S. should strengthen its deterrence against nuclear expansion and implement timely SCs of South Korea-U.S. advanced forces. Continuous message delivery efforts should be systematically managed to prevent North Korea from succeeding in upgrading its nuclear force and engaging in military action with dissatisfaction with its overconfidence in advanced nuclear force and corresponding requirements.

The following are military countermeasures, first of all, the most realistic and immediately applicable measures using the ROK-U.S. military forces. The plan calls for the permanent deployment of strategic weapons capable of responding to nuclear missiles on the Korean Peninsula and the use of THAAD deployed to counter North Korea's nuclear missiles. An additional option to consider is the reintroduction of tactical nuclear weapons by the U.S. military. The fundamental purpose of nuclear weapons is to instill a clear perception that if North Korea attacks the Republic of Korea with

nuclear weapons, it will be retaliated by multiple times by U.S. tactical nuclear weapons deployed in the Republic of Korea, which will eventually lead to North Korea's destruction, so that the North will not think about using them at all.

Second, the South Korean military has its own military response posture. For this purpose, the Kill-Chain system is being developed first. The Kill Chain is a system that responds to North Korea's nuclear and missile threats step by step, and the concept is to launch a preemptive strike in the event of North Korea's nuclear and missile use. The second is the Korean-style missile defense system (KAMD), which is designed to destroy incoming missiles in the air by issuing an interception order to troops operating Patriot or Heavenly Palace if North Korea launches a missile. Third, the concept of KMPR is an operational concept that if an enemy carries out prohibited acts, it will immediately and forcefully retaliate against the military. Finally, it proposed advanced military capabilities by applying advanced technologies of the fourth industrial revolution such as stealth drones, LAMDs, and ultra-high-speed curved artillery.

After analyzing the North Korean nuclear missile threat and studying countermeasures, we were able to summarize the implications below.

First, North Korea, which has established a nuclear and missile system, is likely to carry out military provocations with indirect deterrence, which is based on South Korea and the U.S. forces stationed in South Korea. Therefore, Korea's relations with South Korea are nothing but camouflage peace and maneuvering of the united front. North Korea's position and reality are that there are no more favorable factors than South Korea in securing a cause for responsibility and provocation. We must prepare for contingencies such as the Kagil War between India and Pakistan, which has nuclear weapons.

Second, it is necessary to take a close policy response in response to the threat posed by North Korean missiles. Military response is a final choice that requires a lot of cost and sacrifice, and a policy of first curbing North

Korea's nuclear and missile development through policy international cooperation and blocking the flow route of nuclear technology into its own hands is desirable.

Third, it cannot be overemphasized to prepare for a substantial military response to the threat of North Korean missiles. The government should have a master plan to build electricity to counter North Korean missiles. In the end, the government should make policy efforts and build counter-power to help North Korea give up its nuclear and missile programs on its own.