

석사학위논문

대규모 언어모델(LLM)의 무기체계
전력화 적용방안 연구

2025년

한성대학교 국방과학대학원

국방전력학과

국방 AI 융합 전공

강명철

석사학위논문
지도교수 양병희

대규모 언어모델(LLM)의 무기체계 전력화 적용방안 연구

A Study on the Application of Large Language
Model(LLM) to Militarize Weapons Systems

2024년 12월 14일

한성대학교 국방과학대학원

국방 전력 학 과

국방 AI 융합 전공

강 명 철

석사학위논문
지도교수 양병희

대규모 언어모델(LLM)의 무기체계 전력화 적용방안 연구

A Study on the Application of Large Language
Model(LLM) to Militarize Weapons Systems

위 논문을 국방전력학 석사학위 논문으로 제출함

2024년 12월 14일

한성대학교 국방과학대학원

국방전력학과

국방 AI 융합 전공

강명철

강명철의 국방전력학 석사학위 논문을 인준함

2024년 12월 14일

심사위원장 김 홍 빈 (인)

심 사 위 원 김 두 형 (인)

심 사 위 원 양 병 희 (인)

국 문 초 록

대규모 언어모델(LLM)의 무기체계 전력화 적용방안 연구

한 성 대 학 교 국 방 과 학 대 학 원
국 방 전 력 학 과
국 방 A I 융 합 전 공
강 명 철

4차 산업혁명의 도래로 초거대 AI 시대가 시작되었다. 주변국에서 AI의 국방적용을 중요한 국정과제로 선정하여 강력히 추진하고 있다. 인구절벽 문제로 병력이 감소하는 우리 군에도 중요성이 더욱 커지고 있다.

빅데이터 분석기술이 AI에 활용된 GPT(Generative Pre-trained Transformer)가 등장하면서, 초거대 AI 서비스 가치와 중요성이 매우 높아졌다. 초거대 AI 대표적인 서비스가 생성형 AI다. 생성형 AI는 다양한 콘텐츠를 생성하는 AI 모델이다. ‘대규모 언어모델(LLM)’은 생성형 AI의 한 유형으로 텍스트 콘텐츠를 생성하며, 많은 생성형 AI는 LLM을 기반으로 발전한다.

LLM 기반, 생성형 AI시장 연평균 성장은 약 38%에 달하며 금융서비스, 의료 및 생명과학, 자동차 및 제조, 미디어 및 엔터테인먼트, 통신, 에너지 등 사회 전반의 다양한 분야에 활용된다. LLM은 텍스트와 더불어 이미지나 오디오와 같은 다양한 모달리티 데이터를 기반으로 훈련된 ‘대규모 멀티모달 모델(LMM)’로 발전하는 추세다. LLM 발전추세를 고려하면

활용 가능성이 무한하고 더욱 중요해질 것이다.

미래 전쟁 양상을 고려했을 때 전장 환경을 점진적으로 무인화, 자동화, 자율화하는 방향으로 개조해 나가야 함에 따라 지능화 무기체계를 획득하는 것은 중요한 사항이다. 대표적인 빅데이터 분석 기업인 ‘팔란티어 테크놀로지스(Palantir Technologies)’가 기업 및 군사용 애플리케이션을 위한 ‘인공지능 플랫폼(AIP)’을 출시했다. LLM을 기존 AI 및 머신러닝 기술과 통합함으로써 AIP는 국방 및 기업 등 다양한 분야를 위한 포괄적인 솔루션을 제공한다. 이처럼 LLM을 무기체계에 적용하려는 노력이 시작되었다.

LLM은 전장을 인식하고 정보수집 및 분석, 전략적 의사결정, 군사교육 및 시뮬레이션, 다국어 통신 및 번역 등을 가능하게 할 것이다. 또한 지능화 무기체계를 획득하기 위한 중요한 열쇠가 될 것이다. 따라서 LLM의 무기체계 적용은 중요한 문제이며 앞으로 국방 인공지능 패권을 둘러싼 경쟁에서 우위를 달성할 수 있는 핵심이 될 것이다. 본고는 LLM 즉, 최신기술이 적용된 무기체계 전력화(무기체계를 개발 또는 구매하여 소요군에 배치하는 활동)를 위한 방안을 도출하고자 다음과 같이 연구하였다.

우선, LLM 이론적 고찰을 시작으로 활용현황과 미래 전제 양상을 통해 중요성을 인식하고, 무기체계에 LLM이 적용된 사례를 제시했다. 사례를 통해 무기체계를 전력화할 때 제한사항을 도출하고 네 가지 측면에서 적용방안을 제시했다.

첫째, LLM 핵심기술 개발 및 인재양성 측면에서 국방기술기획서 4가지 중점기술에 기반한 ‘무기체계에 적용 가능한 LLM 기술’을 분석하였다. 이후 이러한 핵심기술을 개발하고 국방에 적용할 수 있도록 ‘체계적인 인재양성 방안’을 인재육성과 공감 형성 차원에서 제안하였다.

둘째, 무기체계 획득 측면에서 무기체계 내 내장형 소프트웨어와 SW 중심 무기체계 등을 중심으로 비교적 단기간(6개월~1년)에 획득할 수 있는 애자일 방식의 ‘SW 획득 프로세스’ 신설을 제안하였다. 또한 무기체계 획득과정에서 자유로운 ROC 수정을 위해 ‘ROC 핵심능력이 포함된 최저치와 최대치를 초기 단계에 설정하는 방안’을 제안하였다.

셋째, 무기체계 시험평가 측면에서 AI 무기체계에 적합한 ‘단계별 시험평가 방안(1단계: AI 모델 성능평가, 2단계: 실 운용환경 시험평가)’을 제안하였고, 이를 뒷받침해줄 관련 법령을 분석하고 보완 방향을 제안하였다. 또한 운영유지간 기술 진부화를 방지하기 위해 ‘AI 기반 무기체계의 유지관리 대상 및 관리범주 제도화 방안’도 제안하였다.

넷째, 무기체계 품질관리 측면에서 빅데이터 관리조직 편성, 무기체계 품질관리 가이드, 클라우드에 양자기술적용 등을 비롯해 ‘품질관리 업무 중심의 거버넌스 정립방안’을 제안하였다.

본 제안은 LLM의 무기체계 적용 가능성을 인식하게 할 것이다. 또한 LLM이 적용된 무기체계를 신속하게 획득하고 성능평가 이후 소요군이 품질 검증된 무기체계를 활용하는데 밑거름을 제공할 것이다.

【주요어】 생성형 AI, 대규모 언어모델(LLM), 멀티모달, 데이터, 무기체계

목 차

제 1 장 서 론	1
제 2 장 생성형 AI와 LLM 이론적 고찰 및 활용현황	5
제 1 절 생성형 AI와 LLM 이론적 고찰	5
제 2 절 LLM 활용현황	16
제 3 장 대규모 언어모델(LLM)의 무기체계 적용 제한사항	20
제 1 절 미래 전쟁 양상	20
제 2 절 LLM 적용 사례	23
제 3 절 LLM 적용 시 제한사항	26
제 4 장 대규모 언어모델(LLM)의 무기체계 적용방안	33
제 1 절 LLM 핵심기술 개발 및 인재양성 방안	34
제 2 절 LLM 기반의 무기체계 획득방안	44
제 3 절 LLM 기반의 무기체계 시험평가 방안	51
제 4 절 LLM 기반의 무기체계 품질관리 방안	60
제 5 장 결 론	66
제 1 절 연구내용 요약	66
제 2 절 추가 연구사항	67
제 3 절 결 언	68
참 고 문 헌	70
ABSTRACT	74

표 목 차

[표 1-1] 러-우 전에서의 인공지능 기술의 군사적 활용 분석	2
[표 2-1] 생성형 AI 모델 발전	13
[표 2-2] LLM 기술 특징	14
[표 2-3] LLM의 활용	16
[표 2-4] 멀티모달 기능이 적용된 LLM 상용화 서비스	18
[표 3-1] AIP 운영자 질문 및 솔루션	25
[표 3-2] 데이터 중요성(사례)	30
[표 3-3] LLM의 무기체계 적용 시 제한사항	32
[표 4-1] LLM의 무기체계 적용 시 고려사항	33
[표 4-2] 중점기술별 목표기술 (요약)	36
[표 4-3] 무기체계에 적용 가능한 LLM 기술	37
[표 4-4] 인공지능(AI) 인재양성 방안(핵심내용)	40
[표 4-5] 23년 교육 추진현황	42
[표 4-6] AI 실무교육 과정별 교육내용	42
[표 4-7] 신속시범사업 업무관리 지침 주요변경사항 (요약)	45
[표 4-8] ROC 수정과 진화적 획득의 법적 근거	46
[표 4-9] AI 무기체계 시험평가를 위한 조치사항	52
[표 4-10] 벤치마크 데이터셋 종류	55
[표 4-11] 운용요구서 관련 조항/운용요구서 서식(보완)	56
[표 4-12] 시험평가 관련 조항	57
[표 4-13] 시험평가 관련 내용 및 서식(보완)	58
[표 4-14] AI 유지관리 대상과 관리범주	59
[표 4-15] 무기체계 품질관리 가이드(평가항목 및 지표)	64
[표 5-1] 연구내용 요약 (기대효과)	66

그 립 목 차

[그림 1-1] 「국방혁신 4.0」 5가지 추진 중점	2
[그림 2-1] 기술 및 산업의 시대적 트렌드	5
[그림 2-2] 인공지능 > 머신러닝 > 딥러닝	7
[그림 2-3] 딥러닝 모델 구조	7
[그림 2-4] 딥러닝과 머신러닝의 차이점	8
[그림 2-5] 데이터 분할 개념	9
[그림 2-6] 트랜스포머 구조	10
[그림 2-7] 사전훈련과 미세조정	11
[그림 2-8] 딥러닝 언어모델 종류	12
[그림 2-9] 한국어 대형언어모델 사업	15
[그림 3-1] GIS-Arta 운용개념, 동작 화면	22
[그림 3-2] 우크라이나 전쟁에서 활약한 주요 군용 드론	23
[그림 3-3] AI 인력부족현황(18~22년), AI 특허 보유 기업	27
[그림 3-4] 연구개발절차와 ROC 결정·수정	28
[그림 3-5] 체계개발절차	29
[그림 3-6] 데이터 구축 프로세스 및 데이터 생애주기	31
[그림 4-1] 인공지능 기술 수준	34
[그림 4-2] 전 장병 AI·SW 생애주기 및 소양교육	41
[그림 4-3] 데이터 라벨링 전문교육 과정, 수료증	43
[그림 4-4] 일반소요 절차와 신속소요 / 시범사업 절차 비교	44
[그림 4-5] ROC 수정 현황 및 원인	46
[그림 4-6] ROC 고려요소 간 상충관계	47
[그림 4-7] IT 전력획득절차(독일), 적응형획득 Framework(미국) ·	48
[그림 4-8] 소프트웨어 획득절차(미국)	49
[그림 4-9] 소프트웨어 중심 무기체계 획득업무 프로세스 개선안	49
[그림 4-10] ROC 수정 개념 (ROC 최저·최대치 설정)	50
[그림 4-11] 구매사업 AI 무기체계 시험평가	52
[그림 4-12] 연구개발 사업 AI 무기체계 시험평가	54

[그림 4-13] 주요 AI 모델의 벤치마크 적용현황	55
[그림 4-14] 생성형 영상 DB 추가, 기존 DB 대비 개선 효과	60
[그림 4-15] 국방 지능형 플랫폼 사업 개요	61
[그림 4-16] 범용 AI 플랫폼과 특화 AI 플랫폼 특징 비교	62
[그림 4-17] 양자기술 분류	64
[그림 4-18] 양자 암호화 개념도	65
[그림 5-1] 미국 AI 관련 규제 수의 변화	69

제 1 장 서 론

제 1 절 연구배경 및 목적

24년 새해 첫날 “인공지능·인류 공존이 시작됐다.”¹⁾라는 인터넷 뉴스가 처음 눈에 띄었다. 삼성전자에서 대규모 언어모델(이하 ‘LLM’, Large Language Model)을 활용한 갤럭시 제품을 출시했다. ‘온디바이스 AI’는 개인 통역사를 둔 것과 같이 실시간으로 매끄러운 소통을 가능하게²⁾ 하는 등 이제 우리 삶은, 말 그대로 인공지능(이하 ‘AI’)³⁾과 함께 한다 해도 과언이 아니다.

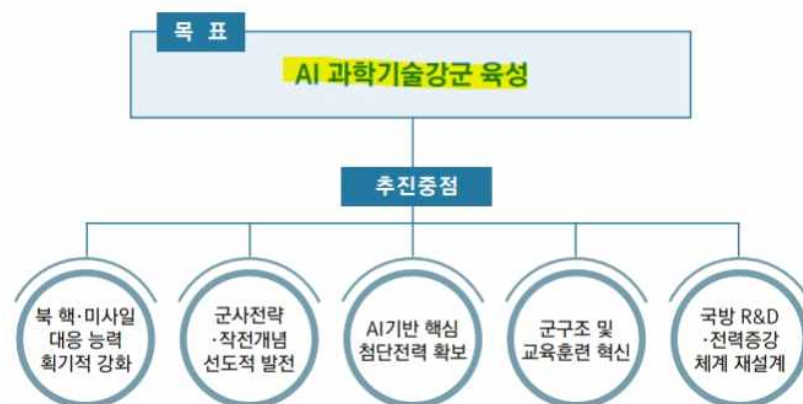
AI는 병력이 줄고 있는 우리 군에도 중요성이 더욱 커지고 있다.⁴⁾ 출산율이 0.7명까지 떨어져 외신들도 “한국이 소멸해 간다”⁵⁾, “0.78명에 불과한 한국의 합계출산율은 한국군의 가장 큰 적이 될 수 있다”고 보도했다.⁶⁾ 또한 러시아-우크라이나 전쟁에도 [표 1-1]과 같이 많은 부분 AI가 활용되었다.

-
- 1) 네이버 뉴스. (2024.1.1.). 인공지능·인류 공존이 시작됐다. <https://n.new.naver.com/article/030/0003169877?type=editn&cds=new_edit> (검색일: 2024.1.1.)
 - 2) 이러한 온디바이스 AI가 가능해진 이유는 거대언어모델(LLM) 때문인데 최근에 국내 통신사들이 범용 LLM 대신 특화 LLM으로 해외 시장 공략에 나서고 있다. (출처: 네이버 뉴스. (2023.11.9.). AI 입은 갤럭시S24, 통화하면서 실시간 통역해준다. <https://n.news.naver.com/article/092/0002310782?type=editn&cds=news_edit> (검색일: 2023.11.9.))
 - 3) 본 고에서는 인공지능(Artificial Intelligence: A.I)을 ‘AI’로 표기 단, 문맥상 필요한 경우 ‘인공지능’으로 표기했다.
 - 4) 최근 육군의 용연연구 결과에도 인공지능 중요성을 담고 있는 것을 고려해보면 우리 군에게 인공지능이 얼마나 중요한지 짐작할 수 있다. (출처: 대한민국육군발전협회. (2023.11). 『미래 육군 상비병력 절감방안 연구』)
 - 5) 네이버 뉴스. (2023.12.10.). 한국이 사라진다...전 세계 걱정거리 된 韓 저출산. <https://n.news.naver.com/article/448/0000439617?type=editn&cds=news_edit> (검색일: 2023.12.10.)
 - 6) 네이버 뉴스. (2023.12.31.). CNN 한국군, 새로운 적은 ‘저출산’...병력 유지 어려워. <https://n.news.naver.com/article/018/0005646681?type=editn&cds=news_edit> (검색일: 2023.12.31.)

[표 1-1] 러-우 전에서의 인공지능 기술의 군사적 활용 분석⁷⁾

분야	인공지능융합 기술 분야	적용 체계	비고(목적)
전투분야(피아 식별 / 실시간 정밀타격)	전투원 얼굴인식(SW) GIS Arta ⁸⁾	경계 감시 시스템 포병 사격통제+우버형 앱	개전초 적군 식별, 표적 3분 내 식별 가용 적정 포병부대로 타격
전투지원 및 전투근무지원	기계학습(ML)	공급망 관제 시스템	최적의 배치
사이버전	컴퓨터 디스플레이 장악, 사물인터넷(IoT)공격	러시아 컴퓨터시스템 전기 자동차 시스템	적의 지휘통제시스템의 사이버 공격
심리전	(Deep Fake) ⁹⁾ 기술 소셜 미디어에 콘텐츠	선전 및 홍보 컴퓨터 / 방송 시스템	통수권자의 항전 의지, 국민단결 전 세계 지원 호소
무인 자율 무기체계	영상처리 및 분석기술	UAV, 드론 체계 등	-

우리 군도 중요성을 인식하고 5가지의 추진 중점을 바탕으로 현 정부의 국방개혁안인 「국방혁신 4.0」(22.5.3.)을 강력히 추진 중이다. 궁극적으로는 ‘AI 과학기술강군 육성’이라는 목표를 정립하였다.



[그림 1-1] 「국방혁신 4.0」 5가지 추진 중점¹⁰⁾

7) 이정우, 김영인. (2023.11). 미래 AI 기반 디지털 전쟁에 대비하는 합동 AI Master Plan 발전방향. 『국방과 기술』, 537, 93.

8) GIS(Geographic Information System) Arta(Art for artillery), 직역하면 “지리정보시스템 - 포술” 정도로 번역 가능하며 여기서 “포술”이란 ‘적시적이고 정확한 간접사격이 보장될 수 있도록 사격 제원을 결정하고 장입하는 기술, 대포 방열 및 표적 위치결정, 사격제원 산출, 대포 및 탄약에 사격제원 장입 등의 제반 절차들’을 말한다.

9) 딥러닝과 페이크(가짜)의 결합어로 인공지능기술을 기반으로 한 가짜 이미지, 오디오, 비디오를 의미한다.

「국방혁신 4.0」 내용 중 AI가 약 34회나 언급된 것을 보면 그 중요성을 알 수 있다. AI의 국방적용은 주변국도 중요한 국정과제로 선정하여 강력히 추진하고 있다. 인공지능 기술개발과 자립화가 미래 국방력의 패권을 결정짓는 요소로 여겨지며 ‘인공지능 군비경쟁(AI Arms Race)¹¹⁾이라는 새로운 신조어를 만들어 내기도 했다.

AI 중 최근 가장 많은 주목을 받으며 활용되고 있는 ‘대규모 언어모델’ 중요성을 인식하였다. 국방 무기체계 적용 가능성을 전제로 앞으로 장병들이 활용하게 될 LLM의 올바른 이해가 필요하다. 또한 국방 무기체계 전력화에 도움이 되고픈 마음에 연구를 시작하였다. 본 연구로 LLM 즉, 최신기술이 적용된 무기체계 전력화 방안을 도출함으로써, 우리 군이 AI 분야를 선도하거나 추월하는 ‘Fast-Mover’로 변화할 수 있도록 밑거름을 제공하고자 한다.

제 2 절 연구 방법 및 범위

본 연구를 위해 사전 관련 논문, 기사, 사설 등 언론 및 인터넷에 공개된 자료를 수집하였다. LLM 기술 적용을 위해선 기술 고유한 특징을 이해하고 이를 적용할 수 있는 제도적 보완이 필요하다. 수집한 자료를 분석한 결과 한국군의 인공지능이라는 큰 범주의 발전을 위한 정책적이고 전략적인 방향에 관한 연구는 많은 전진을 보였다. 그러나 특정 기술에 국한된 세부적인 연구는 찾아보기 힘들었다.

따라서 LLM 이론적 고찰을 시작으로 활용현황과 함께 LLM의 중요성을 인식하고, LLM의 무기체계 적용사례 및 제한사항을 제시하였다. 이후 무기체계에 적용하기 위한 고려사항을 중심으로 무기체계 전력화를 위한 4가지 방안을 제시하였다.

10) 국방부. (2023.2.28.). 『2023_national_defense_brochure01』

11) 인공지능 군비경쟁(AI Arms Race): 과거 핵무기를 통해 억지력을 확보하려는 국제적 패권경쟁과 유사한 형태로 인공지능 기술의 선점을 통한 첨단 무기체계의 개발 경쟁을 의미함. (출처: 최근하, 오재진, 김영길. (2020). 미 국방부 및 육군의 인공지능(AI) 전략이 한국군에 주는 시사점. 『한국방위산업학회지』, 27, 42.

본 연구는 총 5장으로 구성하였다. 제1장은 서론으로 연구배경과 목적, 연구방법을 제시하고 제2장에서는 생성형 AI와 LLM 이론적 고찰을 통한 활용현황을 제시했다. 제3장은 LLM의 무기체계 적용 시 제한사항을 제시하고, 이를 토대로 제4장에선 무기체계를 전력화하기 위한 핵심기술 개발 및 인재양성, 무기체계 획득, 무기체계 시험평가, 무기체계 품질관리 측면에서 방안을 제안했다. 마지막 제5장은 결론으로 앞에서 다룬 내용을 바탕으로 연구내용 요약 및 추가 연구사항, 결론을 통해 마무리하였다.

제 2 장 생성형 AI와 LLM 이론적 고찰 및 활용현황

본 장은 생성형 AI와 LLM 이론적 고찰, 발전추세와 활용현황을 통해 LLM의 중요성을 기술하였다.

제 1 절 생성형 AI와 LLM 이론적 고찰

1) 초거대 AI 등장 배경 및 시사점

1760~1820년대 증기기관 기반의 기계화 혁명(1차 산업혁명)을 시작으로 전기에너지 기반 대량생산 혁명(2차 산업혁명)이 발생했다. 1970년대 이후 컴퓨터와 인터넷 기반의 지식정보혁명(3차 산업혁명), 2016년 이후 정보통신 기술(ICT) 융합 기반의 초지능 혁명(4차 산업혁명)이 도래했다.



[그림 2-1] 기술 및 산업의 시대적 트렌드

2017년 4차 산업혁명 위원회에서 3대 혁신 신산업으로 D.N.A(Data, Network, AI)를 설정하였다. 각 분야별 대책을 발표하면서 예산지원을 대폭 확대했으며 D.N.A 산업 육성 예산은 해가 지날수록 꾸준히 증가했다. 4차 산업혁명의 핵심인 빅데이터 분석기술은 기존 데이터베이스 관리 도

구 능력을 넘어서는 대량(수십 테라바이트)의 정형 데이터로부터 가치를 추출하고 결과를 분석하는 기술이다. 심지어 데이터베이스 형태가 아닌 비정형의 데이터 집합조차 포함한다.

2007년 아이폰이 출시되면서 정보의 폭발시대가 시작했고, 각종 데이터와 함께 2016년 AI가 대두되었다. 이후 빅데이터 분석기술이 AI에 활용된 생성형 AI GPT(Generative Pre-trained Transformer)가 등장하면서, 초거대 AI 서비스의 가치와 중요성이 매우 높아졌다.

사회 전반에 빅데이터 기반 AI 서비스가 확대되면서 국방 무기, 병무 행정, 작전, 보급, 우주 등 다양한 분야에서 AI 서비스를 위한 빅데이터 활용이 필요하다. 전술 데이터, 무기체계 현황, 식단정보, 군수품 조달정보, 항공 영상, 센서 데이터 등 국방의 빅데이터는 방위산업과 무기개발, 병영생활 개선, 국방 정보화를 위해 활용 가능할 것이다.

2) 생성형 AI와 LLM의 이해

MIT 테크놀로지 리뷰는 2023년 주목할 10대 기술 중 하나로 생성형 AI를 선정하였다.¹²⁾ 생성형 AI는 다양한 콘텐츠를 생성하는 AI 모델이다. 대규모 언어모델은 대규모 데이터셋으로 학습된 대규모 매개변수를 가진 언어모델로 문장에서 가장 자연스러운 단어 시퀀스를 찾아내는 딥러닝 모델이다. 즉, LLM은 텍스트 콘텐츠를 생성하는 생성형 AI의 한 유형이다. 또한 'GPT', 'HyperCLOVA X' 등 많은 생성형 AI 모델은 대규모 언어모델(LLM)을 기반으로 한다. 따라서 모든 생성형 AI는 LLM이 가장 중요하기에 LLM에 대한 이론적 고찰이 필요하다.

AI의 알고리즘은 1957년 로젠블랫에 의해 고안된 인공신경망의 한 종류인 ‘퍼셉트론’의 이해로부터 시작한다. 퍼셉트론의 발전과 새로운 개념의 등장으로 인공지능 범주는 [그림 2-2]와 같이 분류한다.

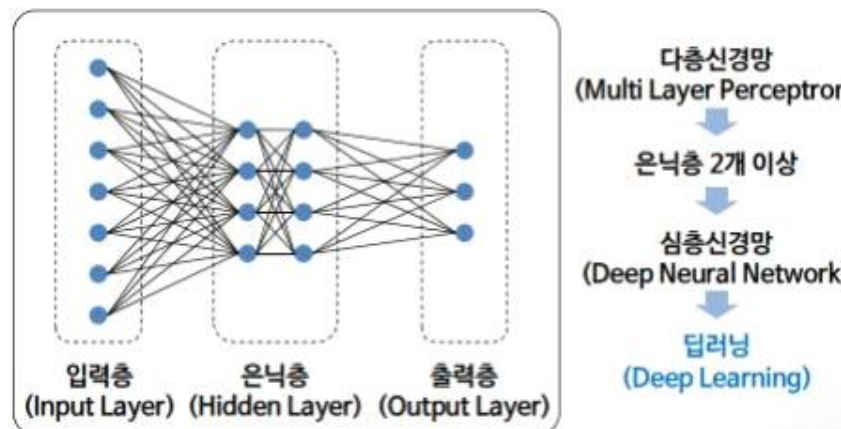
LLM은 딥러닝 범주에 속한다. 딥러닝은 심층신경망을 활용하여 인간이 가진 정보나 지식을 기계가 쉽게 학습하고 알고리즘으로 인식·추정·추

12) MIT Technology Review (2023.1.9.). AI that makes images: 10 Breakthrough Technologies 2023. <<https://www.technologyreview.com/2023/01/09/1064864/image-making-ai-10-breakthrough-technologies-2023/>> (검색일: 2024.11.8.)

론하는 기술이다. 그 구조는 [그림 2-3]과 같다.



[그림 2-2] 인공지능 > 머신러닝 > 딥러닝¹³⁾



[그림 2-3] 딥러닝 모델 구조

인공신경망에 기반을 둔 기계학습의 한 종류로, 여러 비선형 변환기법의 조합을 통해 많은 데이터로부터 특징들을 학습하는 기법이다. 인공신경망을 여러 겹 쌓은 것이 곧, 딥러닝이므로 보통 인공신경망과 구분하지 않고 사용하는 경우가 많다.

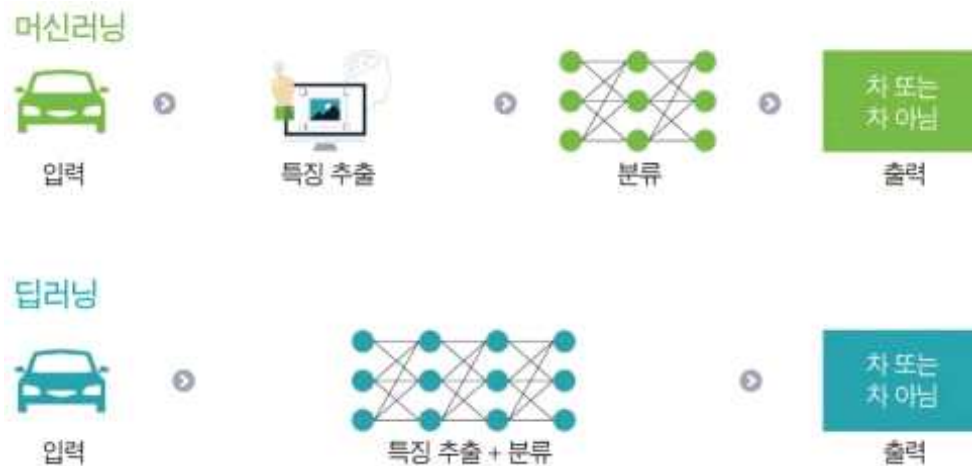
머신러닝이 정형 데이터에 적합한 것에 비해 딥러닝은 비정형데이터¹⁴⁾를 활용하는데 보통 ‘인지’와 관련된 문제를 잘 해결한다고 알려져 있다. 음성과 이미지인식, 자연어처리, 헬스케어 등 전반적인 분야에 활용되고

13) 국방전산정보원 빅데이터팀. (2019.5.1.). 『인공지능(AI), 머신러닝, 딥러닝』. 재인용

14) 데이터 유형은 정형 데이터, 반정형 데이터, 비정형 데이터로 분류하며 자세한 설명은 아래와 같다.

있다.

딥러닝이 일반적인 머신러닝과 큰 차이점은 [그림 2-4]와 같다. 예시와 같이 머신러닝은 특징추출, 분류, 차 여부 단계로 판정된다. 반면, 딥러닝은 특징추출+분류가 동시 자동으로 이루어진다.



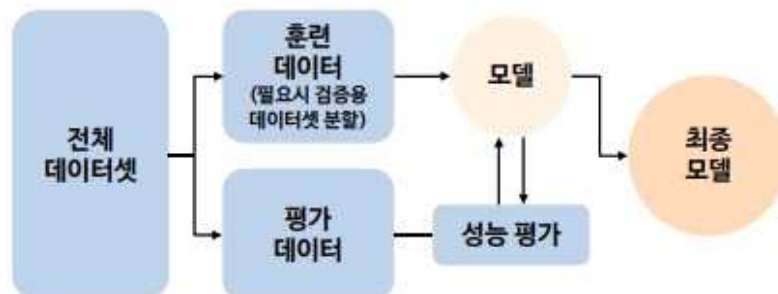
[그림 2-4] 딥러닝과 머신러닝의 차이점

딥러닝 모델이 성능확인 없이 실전에 투입되면 잘못된 결과를 초래할 가능성이 크다. 따라서 모델을 개발할 때 데이터 및 성능확인(품질관리와 시험평가)이 매우 중요하다. 모델을 학습시킨 훈련 데이터로 성능을 평가하면 그 모델은 당연히 좋은 성능이 나온다. 이런 이유로 전체 데이터를 훈련 데이터와 평가데이터로 나누며 그 개념은 [그림 2-5]와 같다.

훈련 데이터는 전체 데이터 중 가장 큰 데이터셋으로 구축용 데이터라고도 한다. 일반적으로 전체 데이터의 50%를 분할 한다. 평가데이터는 모델이 얼마나 적합한지 평가에 활용하고 일반적으로 전체 데이터의 20%를 분할 한다. 검증데이터는 모델의 미세한 오류를 평가할 때 활용되며 일반

구분	내용	예시
정형	·형태(고정된 필드)가 있고, 연산이 가능 ·주로 관계형 데이터베이스에 저장 ·데이터 수집 난이도가 낮고 처리가 쉬운 편	관계형 데이터베이스, 스프레드시트, CSV 등
반정형	·형태(메타데이터)가 있으며, 연산이 불가능 ·데이터 수집 난이도가 중간, 원하는 데이터를 추출하는 데이터처리 기술(파싱)이 요구	XML, HTML, JSON등 소셜데이터(트위터, 페이스북)영상, 이미지, 음성 텍스트 등
비정형	·형태가 없으며, 연산이 불가능 ·데이터 수집 난이도가 높고, 파일을 파싱하는 것 때문에 수집 데이터 처리가 어려움.	소셜데이터(트위터, 페이스북) 영상, 이미지, 음성, 텍스트 등

적으로 전체 데이터의 30%를 분할 한다. 딥러닝 모델은 다양한 품질 좋은 데이터가 많이 필요하며 데이터를 활용, 학습하고 검증될수록 모델의 성능이 향상된다.



[그림 2-5] 데이터 분할 개념

딥러닝 알고리즘은 대표적으로 컨볼루션 신경망(CNN, Convolutional Neural Network), 순환 신경망(RNN, Recurrent Neural Network), 생성형 적대 신경망(GAN, Generative Adversarial Network), 트랜스포머(Transformer)¹⁵⁾ 등 다양하다. 지금도 최신 모델들이 SOTA(State Of The Art)¹⁶⁾에 탑재되고 있다. 이처럼 사회 속에서 AI 기술발전 속도는 매우 빠르게 증가하며, 트렌드도 빠르게 변화되고 있다.

현재 개발된 LLM은 대부분 ‘트랜스포머(Transformer)’¹⁷⁾ 알고리즘에

15) 본 장은 LLM을 이해하기 위해 딥러닝 원리 및 개념을 다루었다. 딥러닝 대표적인 알고리즘 및 모델에 대한 개념은 아래 참조.

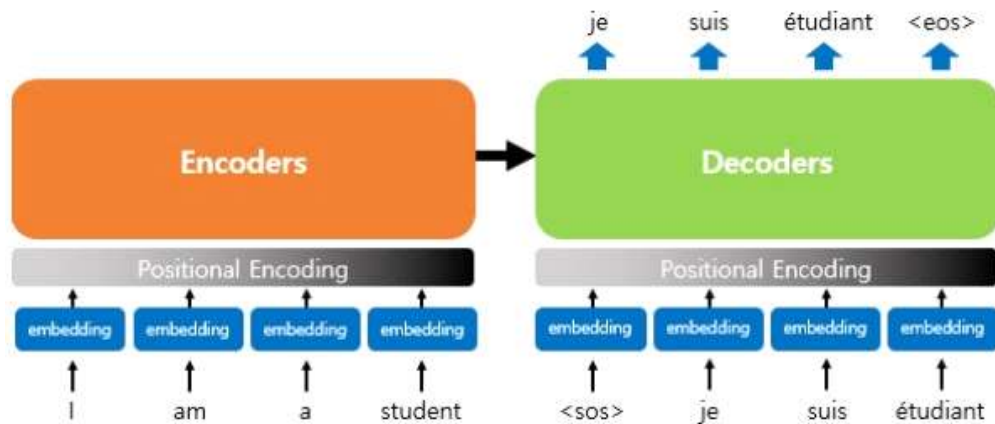
구분	내용	활용
CNN	사람의 시각인지 과정을 모방해서 인공신경망에 필터링 기법에 적용한 것, 이미지와 같은 2차원 데이터를 분석하는 심층신경망 방법론	자율주행차, 이미지·텍스트·사운드·비디오 인식 및 식별
RNN	순차적이며 반복적인 데이터를 학습하는데 특화된 알고리즘으로 내부가 순환구조로 이뤄져 있는 인공신경망	자동번역, 단어 의미 판단, 이미지 캡션 생성 등 자연어 처리 분야
GAN	생성자(Generator)와 식별자(Discriminator)라는 신경망 2개가 서로 경쟁(Adversarial)하면서 학습하는 생성 모델	이미지 생성, 합성, 음악 위조품 생성 분야
Transformer	구글의 2017년 논문(Attention is All You Need)에 처음 등장하였고 지금까지 개발된 모델 중 가장 새롭고 강력한 성능을 보유	문장 속 단어와 같은 순차 데이터 내의 관계를 추적해 맥락과 의미를 학습

16) 현재 최고 수준의 결과를 가진 최신 딥러닝 모델로 가장 정확도가 높은 모델을 의미하며, SOTA에 탑재되어 있다. (출처 : <http://paperswithcode.com/sota>)

17) 구글(Google)의 2017년 논문(Attention is All You Need)에 처음 등장했으며, 지금까지 개발된 모델 중 가장 새롭고 강력한 성능을 보여주며, ‘트랜스포머 AI’라 불리면서 머신러닝 생태계의 혁신을 주도하고 있다.

의해 학습된 것으로 이해가 필요하다. AI 발전에 가장 큰 걸림돌은 대량 데이터를 처리하는 것이 어렵다는 점이었다. 하지만 2017년 구글이 발표한 ‘트랜스포머’ 알고리즘이 이를 가능하게 했다. 번역작업을 예로 설명하면, 트랜스포머 이전에 사용한 순환신경망(RNN)은 번역할 때 바로 앞뒤 단어와 상관관계만 순환적으로 고려했기 때문에 문장이 길어지면 오류가 늘었다. 반면 트랜스포머는 전체 문장에서 한 단어가 다른 모든 단어와 연관 관계를 수학적으로 계산해서 결과 값을 찾아냈다. 또한 여러 인코더를 쌓아 올린 ‘Multi-Headed Attention’ 방식으로 대량데이터를 순차가 아니라 병렬로 처리할 수 있게 해 학습속도가 대폭 향상되었다.

앤비디아 발표에 따르면 트랜스포머 이전 AI 모델이 학습할 때 사용하는 연산능력이 2년 동안 8배 증가했다면, 트랜스포머 이후 2년 동안 275배 성장했다고 밝힌 바 있다. [그림 2-6]은 트랜스포머를 구조화한 것으로 인코더 블록과 디코더 블록을 여러 개 쌓아서 인코더 부분과 디코더 부분을 생성하는 구조다.



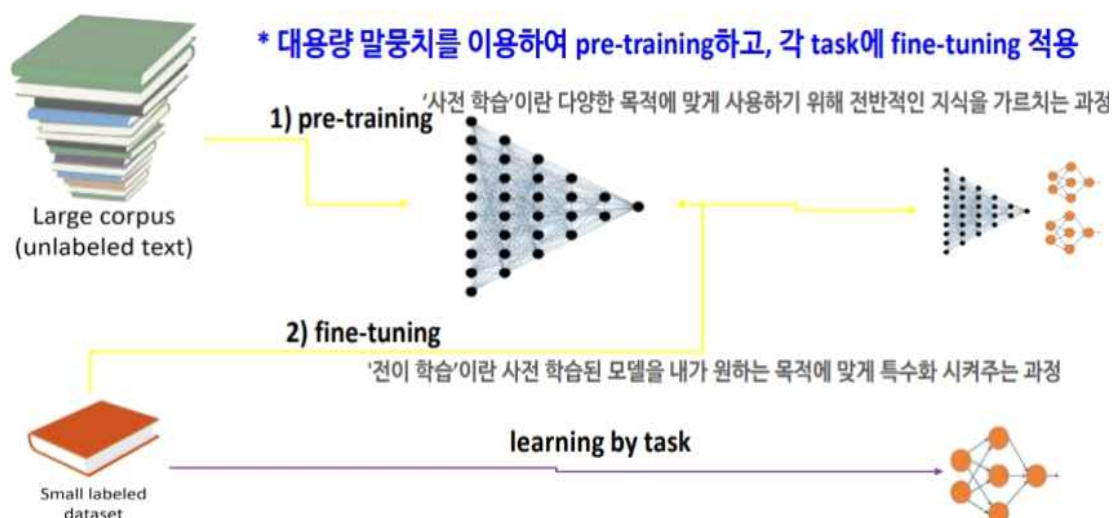
[그림 2-6] 트랜스포머 구조¹⁸⁾

데이터를 행렬 형태로 한 번에 입력하면 Positional Encoding을 통해 단어의 상대적 위치정보를 입력한다. 문장 내 다른 위치에 있는 단어들을 보고 힌트를 받아 현재 목표 위치 단어를 더 잘 인코딩할 수 있게 하는 Self Attention 과정을 거친다.

LLM은 효과적인 개발과 활용을 위해 사전훈련(pre-training)과 미세

18) 국방기술진흥연구소. (2022.1.16.). 『미래국방 2030 기술전략(요약본)』, 22.

조정(fine-tuning)이라는 두 가지 중요한 과정이 사용된다. 사전훈련은 대규모 데이터셋을 활용해 모델을 훈련하는 것으로 이 단계의 목적은 모델이 언어 기본구조와 패턴을 학습하는 것이다. 이 과정에서 모델은 수백만 개 문장과 문서를 분석해 언어의 광범위한 측면을 학습한다. 미세조정은 모델을 특정 목표나 작업에 맞게 조정하는 것이다. 사전 훈련된 모델이 일반적인 언어이해능력을 갖추었다면, 미세조정으로 더 특화된 지식과 기능을 습득한다. 이 단계에서는 비교적 작은 크기의 특화된 데이터셋을 사용해 추가로 학습한다.



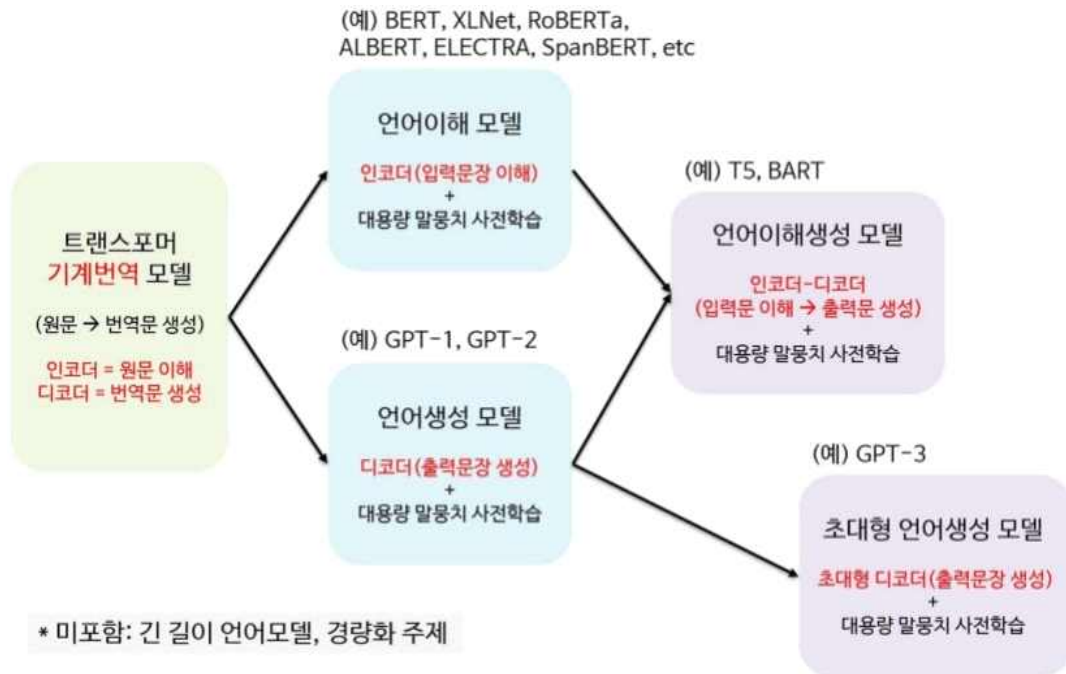
[그림 2-7] 사전훈련과 미세조정

사전훈련과 미세조정으로 특화된 기능을 습득하더라도 사용자 요구에 따라 결과는 달라진다. 사용자가 입력하는 내용 즉, 질문을 프롬프트(Prompt)¹⁹⁾라고 한다. 프롬프트 엔지니어라는 직업이 탄생하기도 했다. 많은 기업이 효과적인 모델 사용으로 업무 생산성을 높이기 위한 것에 기인한 것이다.

LLM은 트랜스포머 알고리즘에 의해 학습되며 사전훈련과 미세조정이란 전문적인 기술과정이 필요하다. 또한 모델로부터 원하는 결과를 얻기 위해서 프롬프트에 대한 전문성도 필요하다.

19) 프롬프팅은 대규모 언어 모델(LLM: Large Language Model)에서 모델이 응답을 수행하도록 하기 위한 프롬프트(Prompt)를 작성하여 입력하는 과정 (네이버 지식, 검색일: 2024.2.10.)

앞에서 설명한 LLM(딥러닝) 언어모델의 종류는 [그림 2-8]과 같다.



[그림 2-8] 딥러닝 언어모델 종류

트랜스포머 모델은 인코더 원문이해와 디코더 번역문 생성 두 가지 기능으로 언어이해모델(BERT, XLNet 등)과 언어생성모델(GPT-1, 2 등)로 구분한다. 그리고 두 가지를 모두 가능하게 하는 언어이해생성모델(T5, BART 등)과 대규모데이터를 기반으로 한 초대형언어생성모델(GPT-3)로 구분할 수 있다. 최근 많은 기업에서 대규모 언어모델에 초점 두고 개발하는 이유는 사전 학습된 모델을 다양한 분야(산업군)에서 특정한 용도로 사용할 때 좋은 성능을 기대할 수 있는 장점 때문이다. 이는 미세조정처럼 모델에 적은 양의 데이터를 공급해 집중적으로 특정한 애플리케이션에 맞춰 훈련 시키는 프로세스기술 덕분이다.

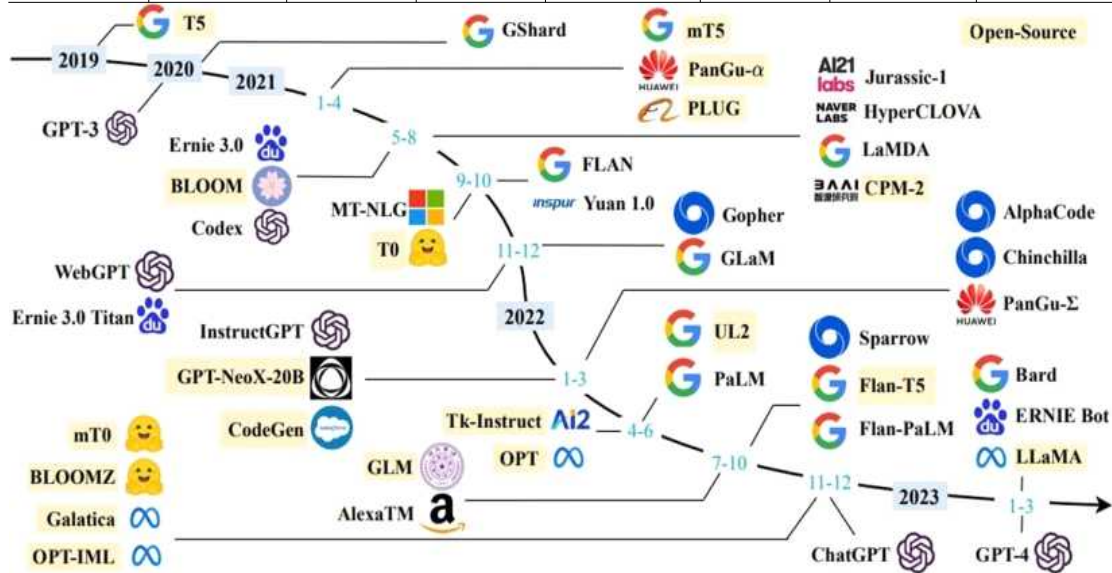
LLM기반, 생성형 AI 모델은 하나 이상 대용량 학습말뭉치와 함께 많은 매개변수, 즉 가중치가 필요하다. [표 2-1]과 같이 매개변수는 매년 새로운 모델 발전과 함께 증가하고 있다.

매개변수가 많아질수록 모델을 학습시킬 GPU 성능 고도화가 필요하다. GPU는 그래픽 연산을 빠르게 처리해 모니터에 결과 값을 출력하는 연산 장치다. AI 모델을 학습시킬 때 복잡한 연산과 데이터를 빠르게 처

리하기 위한 기술이 필요한데, GPU는 AI 모델 학습에 이상적인 도구로 반드시 필요한 시스템이다.

[표 2-1] 생성형 AI 모델 발전

구분	2018	2019	2020	2022	2023	2024	
모델	엘모(ELMo)	GPT-2	GPT-3	팜(PaLM)	GPT-4	라마2(Llama2)	GPT-4o
매개변수(개)	9,360만	16억	1,750억	5,400억	1조 7,600억	70, 130, 700억	10조



LLM기반, 생성형 AI가 발전하고 있지만, 한계도 있다. 첫째, 비용문제다. LLM은 언어 데이터를 처리하는 기본 단위 토큰(Token)을 기준, 사용량을 측정한다. 단어, 문자, 또는 문장 일부를 포함하고 일반적으로 영어보다 한글로 서비스할 때 더 많은 토큰이 사용되며 이는 비용과 연관된다. 대표적인 예로 Open AI의 GPT-4는 약 7,800만 달러, 구글의 Gemini Ultra는 1억 9,100만 달러 상당의 컴퓨팅 비용이 소요되었다.²⁰⁾ 둘째, 신뢰성 문제다. 무분별한 데이터로 학습된 모델은 편향된 답변을 출력하며, 모델이 출력한 내용의 사실 확인이 어렵다.²¹⁾ 또한 없는 사실을 만들어

20) HAI(Stanford Institute for Human-Centered Artificial Intelligence). (2024). AI Index Report 2024 Chapter 3.

21) IT WORLD . (2024.8.26.). 생성형 AI의 한계...점점 명칭해지는인공지능의 미래. <<https://www.itworld.co.kr/news/348359>> (검색일: 2024.10.27.)

내기도 하는데, 이를 환각(Hallucination)이라고 한다. 환각은 수집된 데이터품질이 저조할수록 발생할 확률이 높다.

지금까지 이론적 고찰을 바탕으로 LLM 기술 특징을 정리하면 다음과 같다.

[표 2-2] LLM 기술 특징

특징	내용
전문적인 기술영역	트랜스포머 알고리즘에 의한 구현(사전훈련, 미세조정)
기술발전 속도가 빠름	매개변수가 증가(CPU 성능 고도화)하며, 모델 진화 빠름
데이터 학습을 통해 성능향상	다양한 데이터로 학습하고 검증될수록 성능이 향상됨
다양한 품질 좋은 데이터 필요	데이터품질에 따라 환각 현상, 편향성 발생

LLM은 딥러닝 범주에 속하며 AI 기술과 유사한 특징을 가진다. 첫째, 전문적인 기술영역이다. 대부분 트랜스포머 알고리즘에 의해 학습된 모델이며, 활용을 위해선 사전훈련과 미세조정 단계가 필요하다. 또한 원하는 답을 얻기 위해 전문적인 프롬프트 기술도 필요하다. 따라서 이를 구현하기 위한 전문가가 필요하다. 둘째, 기술발전 속도가 빠르다. GPU 성능 고도화와 함께 매개변수 증가로, 매년 새로운 모델이 개발되면서 진화속도가 빠르다. 셋째, 다양한 품질 좋은 데이터 학습을 통해 성능이 향상된다. 데이터셋으로 사전 훈련되는데 데이터셋은 웹 페이지, 책, 기사, 소셜 미디어 게시물 등 다양한 출처에서 수집된 텍스트 데이터로 구성된다. 다양한 데이터로 학습하고 검증될수록 성능이 향상되나, 때로는 환각 현상 및 편향된 답변을 출력하기도 한다. 따라서 데이터품질이 중요하다.

3) LLM 발전

현재 LLM은 모두 언어모델이다. 하지만 우리 두뇌의 정보전달은 90% 이상이 시각정보며, 유지하는 메시지 양 95% 이상이 비디오 형태다. 따라서 새로운 언어시각모델 필요성이 대두되고 있다. 그 움직임이 최근(24년 5월) 오픈 AI에서 출시한 새로운 ‘자비스’ 같은 모델인 GPT-4o(omni)다.

기존 챗 GPT와 여러 차원에서 차이가 있는데 특히, 여러 데이터 형식

을 처리할 수 있는 멀티모달(multi modal) 기능을 꼽을 수 있다. 텍스트와 이미지뿐 아니라 오디오까지 확대해 음성소통이 가능해졌다. 기존 어색한 기계 음성에서 영화 ‘아이언맨’ AI 비서 ‘자비스’나 영화 ‘HER’ ‘사만다’와 같이 감정 표현이 자연스럽게 진화했다.

개발자는 텍스트를 사용해 대부분 LLM을 훈련 시키지만, 일부는 텍스트뿐만 아니라 이미지나 오디오와 같은 다양한 모달리티 데이터를 기반으로 훈련 시킨다. 다양한 모달리티 데이터로 사전 학습된 초대형 딥러닝 모델 즉, 대규모 멀티모달 모델(이하 ‘LMM’, Large Multimodal Model)로 발전하는 추세다.

국내에도 멀티모달 중요성을 인식하고 한국어 대형언어모델(LLM) 사업을 수행 중이다. 개념은 [그림 2-9]와 같다.



[그림 2-9] 한국어 대형언어모델 사업

외부지식 및 메모리를 통한 효율적인 언어모델, 열린 지식기반 언어모델에서 대형 멀티모달 언어 지식모델로 발전을 도모하고 있다. 한글로 영상제작이 가능하고 시각/문자가 동시에 인식되며 이미지로부터 문서 요약, 줄거리로부터 비디오생성 등 다양한 기능이 가능해진다.

LMM은 데이터 양식과 애플리케이션 및 작업 측면에서 LLM과 차이점이 있다. LLM은 이미지나 오디오와 같은 비텍스트 데이터를 처리하지 않

는다. 텍스트 데이터처리와 생성에 특화되어 있으며, 주로 대규모 텍스트 말뭉치로 훈련받아 다양한 맥락에서 인간 언어를 이해하고 생성에 능숙하다. 반면 LMM은 텍스트, 이미지, 오디오, 비디오, 때로는 감각 데이터와 같은 다양한 유형의 데이터 입력 또는 양식을 이해하고 처리하도록 설계되어 있다. 애플리케이션 및 작업 면에서 LLM은 기사작성, 언어번역, 질문에 답변, 문서 요약, 텍스트 기반 콘텐츠생성 등 텍스트와 관련된 작업을 중심으로 이루어진다. 하지만 LMM은 멀티모달 특성으로 다양한 데이터 유형의 정보를 이해하고 통합해야 하는 작업에 적용할 수 있다.

제 2 절 LLM 활용현황

LLM은 복잡한 언어이해가 가능하고, 언어생성능력이 뛰어나며, 자동번역 및 다국어처리, 감정분석 및 의견 마이닝에 특화되어 있다. [표 2-3]과 같이 여러 분야에 활용된다.

[표 2-3] LLM의 활용

활용 분야	내용	비고
금융서비스	챗봇, AI 비서(응답)	복잡한 언어이해 언어생성 자동번역 및 다국어처리 감정분석 및 의견 마이닝
의료 및 생명과학	새로운 단백질 서열 생성, 신약 및 희귀질환 연구	
자동차 및 제조	부품 설계, 제조 프로세스 최적화, 결함 식별	
미디어 및 엔터테인먼트	콘텐츠제작, 창조(음악, 게임 등), 수익증대	
통신	서비스 개선, 네트워크 성능 최적화	
에너지	효율적인 에너지 사용, 절약, 안전성 향상	

첫째, 금융서비스 분야에 활용된다. 생성형 AI 성능과 비용효율을 활용해 비용을 절감하면서 더 나은 서비스를 제공할 수 있다. 대화용 봇으로 제품추천 및 고객 문의에 응답을 생성하여 고객서비스를 개선할 수 있고, 대출 승인 신속처리, 신용카드 및 대출사기를 신속하게 탐지한다. 투자회

사는 저렴한 비용으로 금융자문을 제공할 수 있다.

둘째, 의료 및 생명과학 분야에서 생성형 AI로 항체, 효소, 백신 설계 및 유전자치료를 위한 특정한 특성을 가진 새로운 단백질 서열을 생성하여 신약 탐색 및 연구를 가속화 할 것이다. 또한 인공 환자 의료데이터 생성이 가능하며, AI 모델훈련으로 희귀질환 연구에도 적용할 수 있다.

셋째, 자동차 및 제조 분야에서 기계부품설계를 최적화하고 일반적인 고객 질문에 빠르게 응답하여 더 나은 고객서비스를 제공할 수 있다. 또한 제조 프로세스를 최적화하여 비용을 절감하고 특히, 데이터테스트용 가상 데이터를 생성하여 결함을 식별하는데 적용할 수 있다.

넷째, 미디어 및 엔터테인먼트 분야는 생성형 AI로 기존보다 훨씬 적은 비용과 시간으로 고품질 참신한 콘텐츠제작이 가능하고 새로운 음악 장르를 창조할 수 있다. 개인화된 콘텐츠와 광고를 제공하여 고객 경험을 개선하고 수익을 증대시키며, 게임회사는 새로운 게임 및 아바타 제작에 도움이 될 것이다.

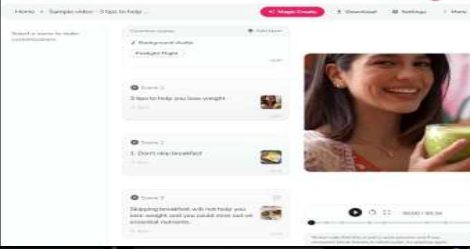
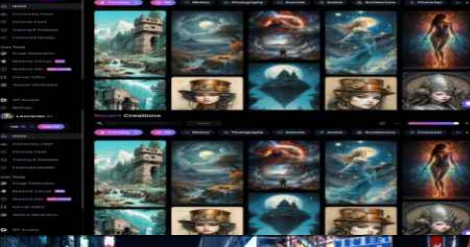
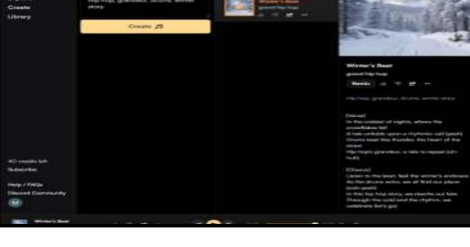
다섯째, 통신 분야에서는 생성형 AI로 실제 사람과 같은 대화 에이전트를 통해 고객서비스를 개선하고 네트워크 데이터를 분석하여 해결방법을 제안, 네트워크 성능을 최적화할 수 있다.

여섯째, 생성형 AI는 복잡한 데이터 분석, 패턴인식, 예측 및 최적화를 포함하는 에너지부문에 적합하다. 고객데이터 분석, 사용패턴식별, 에너지 효율 프로그램으로 고객서비스를 개선하여 에너지를 절약하고 운영현장 안전을 높여 줄 것이다.

위에서 제시한 것 외에도 다양한 분야에 활용할 수 있으며 언어모델에 멀티모달 기능이 추가된다면 그 활용성은 무한할 것이다. 멀티모달이 적용된 LLM 상용서비스를 정리하면 [표 2-4]와 같다.

본 서비스들은 텍스트 콘텐츠를 생성하는 Text to Text(T2T)에서 벗어나 멀티모달 기능이 추가되어 텍스트나 이미지, 비디오, 음성, 음악 등 다양한 형태로 입·출력이 가능하다. 대규모 멀티모달 모델이 어떤 형태로 출력이 가능하든 결국 텍스트를 기반한 LLM이 필수적이다.

[표 2-4] 멀티모달 기능이 적용된 LLM 상용화 서비스

서비스	관련 이미지	비고
Midjourney https://midjourney.com		텍스트/이미지 → 이미지/비디오
Fliki https://app.fliki.ai		텍스트 → 음성/비디오
Gen-2 https://app.runwayml.com		텍스트/이미지/비디오 → 음성/이미지/비디오
Leonardo.AI https://app.leonardo.ai		텍스트/이미지 → 이미지/애니메이션/비디오
Sora https://openai.com/sora		텍스트 → 비디오
SUNO https://app.suno.ai		텍스트 → 오디오(음악)

LLM에 기반한 생성형 AI GPT는 스위스 투자은행 UBS에 따르면 2023년 1월 기준으로 전 세계적으로 한 달에 1억 명의 사용자가 찾는 서비스가 되었다. 오픈 AI의 DALL-E2는 150만 명의 사용자가 매일 200만 개 이상의 이미지를 생성하고 있으며, 스테빌리티(Stability)사의 스테이블 디퓨전(Stable Diffusion) 사용자는 하루 100만 명 이상이라고 알려졌다.²²⁾ 2023년 생성형 AI 시장규모는 2022년 대비 약 8배 증가한 252억 달러에 달했으며 2030년에는 1.6조 달러(한화 약 2,000조)에 달할 것으로 전망되고 있다.²³⁾ 연평균 성장은 약 38%에 달한다. LLM 기술력은 일정 수준 이상으로 발전되고 그 활용성이 무한한 상황이다. 이제 LLM을 어떻게 활용할지 철저하게 ‘아이디어 싸움’이 관건이 될 전망이다. 이러한 이유에서 LLM은 AI 분야에서 중요한 요소이며 이를 무기체계에 적용하기 위한 노력은 국방 분야에서 인공지능 패권을 둘러싼 경쟁에서 우위를 달성할 수 있는 핵심이 될 것이다.

22) 김대환, 고은진. (2023.7.31.). 생성형 AI 기술을 활용한 국방 무기체계 개발. 『국방과학기술플러스』, 261, 20~27.

23) HAI. (2024.), Chapter 6.

제 3 장 대규모 언어모델(LLM)의 무기체계²⁴⁾

적용 제한사항

최근 인공지능(AI)기술의 급속한 발전과 사회 제반 활발한 응용을 배경으로 세계 각국이 AI 등 4차 산업혁명 기술을 활용한 군사혁신 경쟁을 본격화하고 있다. KIDA에서 연구한 “(인공)지능 시대 한국의 국방력 건설 방향”에서 이와 같은 글로벌 안보 상황에 대응하기 위해서는 AI 등의 기술을 적극 활용, 국방 제 영역(무기, 조직, 작전, 인재)에서 군사혁신을 이룸으로써 새로운 유형의 국방력 즉, ‘지능화 국방력’을 건설할 필요가 있음을 제안하였다. 따라서 본 장에서는 위 자료를 바탕으로 미래 전쟁 양상을 통해 지능형 무기체계를 위한 LLM 필요성을 기술하였다. 이후 LLM의 무기체계 적용사례와 제한사항을 제시하였다.

제 1 절 미래 전쟁 양상

AI 및 빅데이터 등 4차 산업혁명 기술발전과 사회 제반 영역 응용확대 추세 속에 군사영역에서도 초 지능화, 초 융합화, 네트워크화 현상이 점차 뚜렷해지고 있다. 이에 따라 향후 작전공간과 전투력 생성방식에 큰 변화가 예상된다.

우선 미래에는 기술발전으로 전쟁승리에 영향을 주는 작전공간이 대폭 확대되고 이들 사이 상호연계와 통합성이 크게 높아질 것이다. 구체적으로 기존 전통영역 작전공간은 신홍영역을 점차 포함하는 방향으로 발전하고 이들 사이 상호연계는 한층 심화 될 것이다. 그리고 이들 영역은 2050 년경에는 완전히 통합될 가능성이 있다. 이처럼 미래에는 다 영역에서 작전이 수행될 가능성이 크다.

24) 전장에서 전투력을 발휘하기 위한 무기와 이를 운용하는데 필요한 인원, 장비, 부품, 시설, 소프트웨어, 종합군수지원요소, 전략, 전술, 훈련 등 제반 요소를 통합한 체계 (출처: 육군본부. (2022.12.31.). 『기준 0-3 군사용어』, 67.)

둘째, 미래에는 AI 등 4차 산업혁명 기술 발달로 기존 정보화 전쟁이 고도로 발전한 지능화 전쟁이 본격화할 전망이다. 지능화 전쟁은 새로운 지능화 네트워크 정보시스템에 기초해 지능화 무기체계와 이에 상응하는 작전방법을 이용해 육·해·공·우주, 전자기·사이버, 인지 영역에서 진행되는 합동 전력의 통합전쟁으로 정의할 수 있다. 지능화 전쟁은 정찰 및 지휘 통제 등 개별 작전요소의 지능화 단계를 거쳐 점차 작전(전역), 전략 차원으로 고도화되면서 2050년경 본격적인 무인 로봇 전쟁 시대가 도래할 것이다.

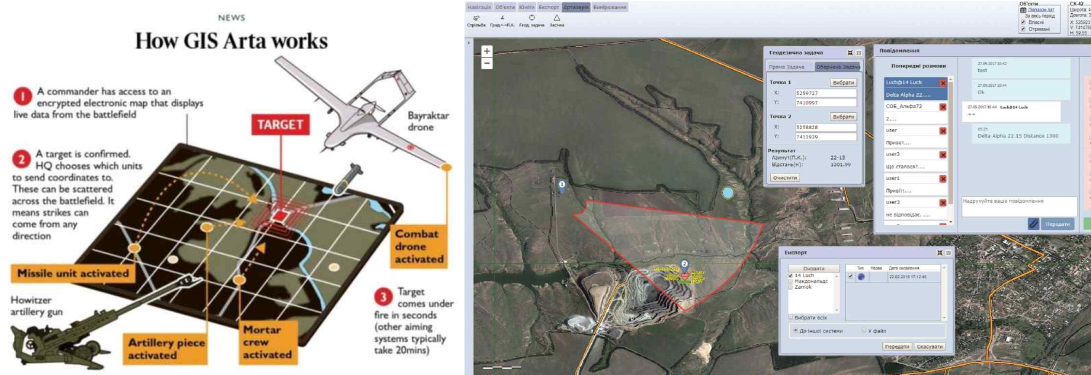
이러한 전쟁 양상에서 아군 지능화 수준이 뒤쳐질 경우 전투력 창발(emergence)이 적시에 이뤄지지 않거나 상대방 작전행동의 불확실성을 줄이는 데 실패함으로써 전쟁에서 불리한 상황에 빠지게 될 것이다.

이에 미국과 중국 등 주요국 동향을 놓고 볼 때 지능화 국방력은 지능화 무기체계, 지능화 군 조직, 지능화 작전, 지능화 군사 인재 등으로 구성할 필요가 있다고 위 연구에서 제안하고 있다. 그중 본 연구와 관련된 지능화 무기체계는 지능형 C4ISR, 정밀유도 무기 시스템과 같이 지능기술(AI), 로봇기술 등 4차 산업혁명 기술을 적극적으로 국방영역에 투입하면서 전장 환경을 점진적으로 무인화/자동화/자율화하는 방향으로 개조해 나가야 함을 시사한다.

최근 전쟁사례를 보았을 때도 전쟁 양상변화를 잘 알 수 있다. 우선, 러-우 전쟁에서는 대표적으로 ‘GIS-Arta’와 ‘드론’ 운용이 있다. 러-우 전쟁 중 세베르스키 도네츠크 전투 시 GIS-Arta 활약이 돋보였는데, 러시아군 부교가 설치되고 3분의 2 이상의 병력이 도강에 성공한 직후 해당 지역의 정확한 GPS 좌표와 대전차 무기로 무장한 소규모 특수부대의 화력 유도, 장거리 화력 투사가 가능한 포병의 정밀사격으로 러시아군을 공격하였다.

기동부대의 기습과 포병의 장거리 정밀포격, 대전차 로켓·미사일부터 유탄발사기, 박격포 등 다양한 무기로 무장한 우크라이나군 전투부대들이 마치 순번을 정한 것처럼 질서정연하게 공격과 후퇴를 반복하였다. 이는 GIS-Arta를 활용해 별도의 작전 회의나 협조 없이 정확한 전장 정보를

실시간으로 확인하고, 전투상황에 맞춰 최적 시간과 장소에서 러시아군을 공격한 덕분이었다.²⁵⁾



[그림 3-1] GIS-Arta 운용개념, 동작 화면

[그림 3-1]과 같이 GIS-Arta는 탑승객과 가장 가까운 곳에 있는 운전자를 자동으로 연결해 주는 우버(Uber) 앱처럼 표적 주변에서 가자 가깝거나 가장 효율적인 무기를 보유한 부대에 화력지원 혹은 직접공격을 명령한다. 즉, 표적처리과정 중 표적을 식별하고 지휘관 요망효과에 부합한 가장 적합한 무기체계를 선정하여 공격방법을 결정하는데, 이러한 결심과정에 AI를 활용하여 수행한다.

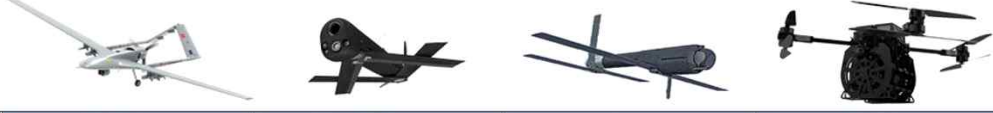
이를 통해 일반적으로 현대화된 군대가 전선에서 적을 식별하고 포병이나 공군전력으로 공격하기까지 20분 안팎의 시간이 걸리지만, GIS-Arta는 최소 30초에서 2분 이내로 단축함으로써 신속한 표적획득과 타격이 가능하다. 이러한 AI와의 협업으로 세베르스키 도네츠크강 전투에서 우크라이나군이 입은 피해는 경미한 반면 러시아군은 73대 이상의 전차와 장갑차, 1,500명가량의 병력을 잃은 것으로 추정되고 있다.²⁶⁾

이와 더불어 다양한 ‘드론’도 활용되었다. 우크라이나는 20여 종(정찰 15종, 공격 5종)의 드론을 운용한 것으로 분석된다. 2014년 돈바스 전쟁의 교훈을 기초로 다양한 드론을 전력화(자체 개발 12종)하였고, 미국·터키·폴란드·중국 등 해외 도입 8종을 함께 운용하였다. 서방국가에서도 ‘TB-2’, ‘Switchblade’ 등 공식·비공식적으로 드론을 지원한 것으로 알려

25) 국방일보. (2022.5.30.). 도네츠크 강 건너던 러 대대급 병력 전멸 ‘일등공신’.

26) 강명철. (2023. 7.). 우크라이나-러시아 전쟁 간 포병 운용 분석. 『전투발전』, 166, 202.

졌다. 러시아는 13여 종(정찰 10종, 공격 3종)의 드론을 운용한 것으로 분석된다.²⁷⁾



이름	바이라타르 TB2	스위치 블레이드 LMAMS	파닉스 고스트	리볼버 860
제조국	튀르키예	미국	미국	대만
제조사	바이카르	에어로바이런먼트	에이펙스 에어로스페이스	드론스비전
특징	▶최고 속도 시속 220km ▶최대 150kg 무기 적재 ▶중급 드론 대비 높은 가성비	▶자폭형 드론, 일명 '가미카제 드론' ▶최대 속도 시속 161km ▶대인용 '300' 모델 무게 2.5kg으로 휴대 가능 ▶1기당 약 6000달러(약 814만원)로 높은 가성비	▶자폭형 드론, 일명 '가미카제 드론' ▶제조사美 국방부 모두 지원 함구 ▶비행 가능 시간 6시간 이상	▶60mm 박격포탄 8개 장착 ▶25~40분간 최대 20km 비행

[그림 3-2] 우크라이나 전쟁에서 활약한 주요 군용 드론

이스라엘 하마스 무력충돌에서도 드론을 활용하여 이스라엘 감시탑을 파괴하거나, 이스라엘군이 로봇을 활용하여 지하 통로를 정찰하는 등 유·무인 복합으로 전쟁이 수행됨을 알 수 있다. 이처럼 최근 전쟁에서도 점진적으로 무인화/자동화/자율화하는 방향으로 전쟁 양상이 변화되고 있다.

미래전 수행방식에서 가장 큰 영향을 미치게 될 기술은 인공지능이 될 것이며, 로봇은 인간의 육체를 대신하면서 인간 전투원과 지능형 군사 로봇과 협업으로 전쟁이 수행될 것이다. 인간과 로봇협업에서 가장 중요한 것은 '상호의사소통'이며 이러한 모든 활동, 능력은 무인 무기에 탑재된 컴퓨터 인공지능(LLM) 수준에 따라 결정될 것이다. 따라서 LLM의 무기 체계 적용 문제는 '지능화 무기체계'에서 중요한 요소이다.

제 2 절 LLM 적용 사례

대표적인 빅데이터 분석 기업인 '팔란티어 테크놀로지스(Palantir Technologies)'가 기업 및 군사용 애플리케이션을 위한 '인공지능 플랫폼(AIP)'을 출시했다. 이 플랫폼은 Open AI의 GPT-4 또는 Google의 BERT와 같은 대규모 언어모델의 기능을 독점 소프트웨어와 결합하여 국

27) 교육사령부. (2022.7.12.). 러시아-우크라이나 전쟁 전훈분석 및 전투발전 방향 토의

방 기관 및 기업 고객에게 책임감 있고 효율적이며 규정을 준수하는 AI를 활용할 수 있도록 지원한다. LLM을 기존 AI 및 머신러닝 기술과 통합함으로써 인공지능 플랫폼은 국방 및 기업 등 다양한 분야를 위한 포괄적인 솔루션을 제공한다.

AIP는 기밀 네트워크부터 전술적 디바이스에 이르기까지 모든 네트워크에 대규모 언어모델과 AI를 배포할 수 있다. 이러한 과정에서 가드레일(guardrail)²⁸⁾을 구현하여 통제, 관리 및 신뢰를 높인다. 운영자와 AI가 플랫폼에서 조치를 위하면 AIP는 안전한 디지털 운영 기록을 생성한다. 이러한 기능은 군에서 책임감 있고 효과적이며 규정을 준수하는 AI를 배포하는 것에 필수적이다.

또한 운영자가 질문을 제기할 때 LLM은 공개 및 기밀 소스 전반에서 통합된 실시간 정보를 사용한다. 데이터는 자동으로 태그가 지정되고 분류 표시로 보호되며, AIP는 개인의 권한, 역할 등 보안수준을 고려 LLM이 조직 내 접근할 수 있는 부분을 제한한다.²⁹⁾

팔란티어는 새로운 플랫폼 데모 영상에서 전투가 벌어지는 지역에서 AIP를 어떻게 활용할 수 있는지 강조했다. 이 시나리오는 동유럽지역을 감시하던 작전 요원이 국경 근처에 모이는 적군을 감지하는 내용이다. AIP는 신속하게 상황을 평가하고 잠재적 위협에 효과적으로 대응하기 위한 전략적 행동방침을 제안했다. 주목할 만한 사례는 적 T-80 주력 전차가 있는 전장 상황을 신속하게 분석하고 세 가지 잠재적 행동방침을 생성한 후 선택한 작전계획을 통해 위협을 효율적으로 무력화시키는 능력을 보여준 것이다.

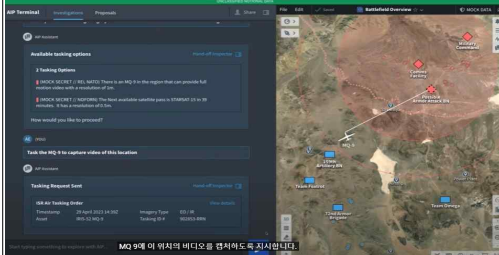
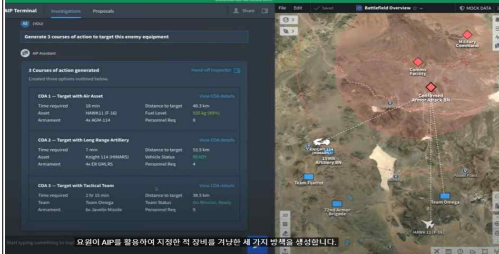
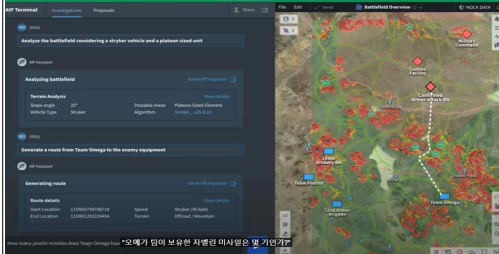
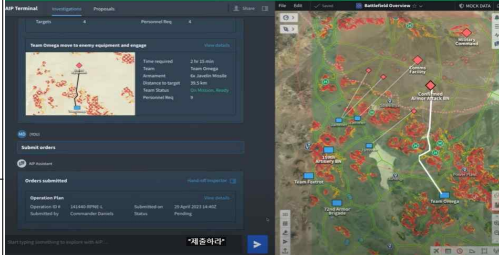
이러한 과정에서 AIP는 대규모 언어모델을 활용하여 운영자가 질문하고, 신속한 솔루션을 제공하는데 그 과정을 정리하면 [표 3-1]과 같다.

28) guardrail : 물리적인 방화책이 아니라, AI 시스템의 작동을 통제하고 관리하며 신뢰성을 보장하기 위한 일련의 정책, 절차, 안전장치 등을 의미한다. 이는 AI가 예상치 못한 방식으로 작동하거나 오작동하지 않도록 하고, 사용자가 시스템을 올바르게 사용할 수 있도록 돕기 위한 조치들이다. 이러한 가드레일은 AI의 책임감 있는 사용과 규정 준수를 보장하는 데 필수적이다.

29) 장사정 정밀화력체계 과학기술그룹. (2024.7.5.). 팔란티어 기업 및 군사용 인공지능 플랫폼 발표. 『화력전투발전 군사과학기술개발 동향』, 24-16, 1~7.

먼저 아군으로부터 30Km 떨어진 지역에 군사 장비가 집결되어 있다는 정보를 받으면 표적식별을 위한 질문을 한다. 질문을 바탕으로 AIP는 근처에 드론을 배치하여 영상을 수집하는 옵션을 제시하고 지시에 따라 적 T-80 주력 전차가 포착된 사진을 전송한다.

[표 3-1] AIP 운영자 질문 및 솔루션³⁰⁾

구분	질문을 통한 작전계획 수립	솔루션
표적 식별	① “보다 자세한 내용을 보여줘~” ② “이 위치에 대해 1M 이상의 해상도로 새 이미지를 작업” ③ “MQ 9에 이 위치의 비디오를 캡처 하도록 지시”	 MQ 9에 이 위치의 비디오를 캡처하도록 지시합니다.
방책 선정	④ “지정한 적 장비를 표적으로 타격하기 위한 방책 세 가지를 생성해줘” ⑤ “이 세 가지 방책을 지휘관에게 보고해 검토를 요청하라” ⑥ “제 3호 방책의 실행을 승인한다.”	 요청이 AIP를 활용하여 지정한 적 장비를 겨냥한 세 가지 방책을 생성합니다.
계획 수립	⑦ “스트라이커 전차와 소대규모의 부대를 고려하여 전장을 분석하라” ⑧ “오메가 팀의 위치에서 적 장비까지 이동경로를 생성하라”	 “오메가 팀이 보유한 재블린 미사일 몇 기인가?”
계획 시행	⑨ “오메가 팀이 보유한 재블린 미사일은 몇 기인가?” ⑩ “우선순위가 높게 검증된 통신표적에 각각 재머를 할당하라” ⑪ “작전계획을 요약해라”, “제출하라” ⑫ “재밍 작전을 실시하라”	 “제출하라”

이후 세 가지 방책을 요구하고 AIP가 제시한 방책을 지휘관에게 보고해 검토를 통해 선정된다. 이때 지휘관 의사결정을 지원하기 위해 각 방책에 대한 주요정보를 강조 표시하여 제시한다.

30) YOUTUBE. (2023.4.26). Palantir AIP | Defense and Military. <https://www.youtube.com/watch?v=XEM5qz_HOU> (검색일: 2024.7.16.)

지휘관이 결심한 방책의 작전계획 수립을 위해 AIP는 가장 근접한 아군부대(오메가 팀)를 확인하고 작전계획을 수립한다. 우선 전장 분석 및 최적 경로판단을 위한 질문을 수행한다. AIP는 자동화된 지형분석모델이 기존 모든 지리 공간정보를 처리 후 부대 기동성을 파악한다. 이후 부대 구성을 기반으로 동선을 연산하며 지형 횡단 가능 여부에 따라 최적 경로를 제안하고, 오메가 팀이 보유한 무장에 대한 정보도 제공한다. 다음은 재머작전을 위해 AIP는 검증된 모든 적 통신 노드를 자동으로 식별하고 교란 기능이 있는 노드와 서로 연결하여 결과를 제시한다. 작전계획이 수립되면 지시를 받고 작전계획을 제출한다.

전자전 담당관이 통신 교란 작전을 시작하고 아군 지상군이 작전 위치로 이동하면 적 장비를 파괴할 수 있게 승인되고 작전이 진행된다. 이 모든 과정이 운영자에 의한 간단한 질문과 지시로 수행된다.

CEO 겸 공동 설립자인 알렉스 카프(Alex Karp)는 성명에서 “인공지능 플랫폼(AIP)을 통해 기존 플랫폼에서 직접 대규모 언어모델과 함께 기존 머신러닝 기술의 성능을 활용할 수 있게 될 것”이라고 말했다. 이처럼 팔란티어의 국방용 인공지능 플랫폼은 대규모 언어모델(LLM)이 군 조직의 중요한 임무 결정에 어떻게 도움을 줄 수 있는지를 보여주는 첫 번째 중요한 사례다.

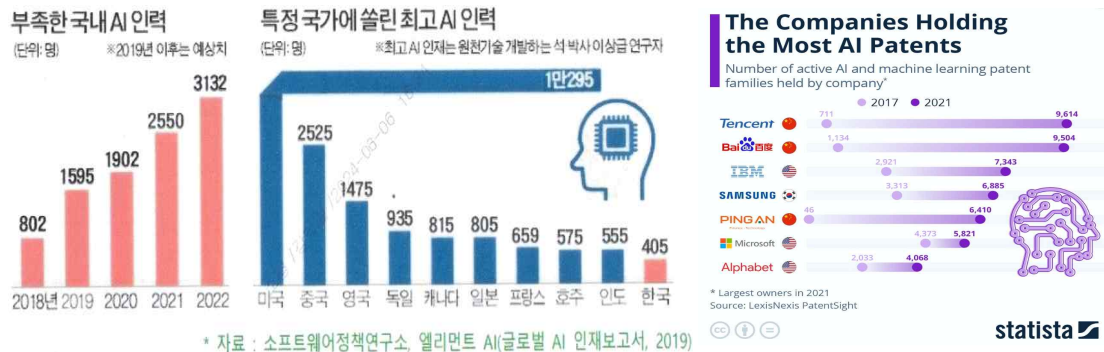
LLM이 모달리티 데이터를 활용하면서 발전하고 있기에 그 확장성은 무한할 것이며, 가까운 미래에는 국방 전 분야에서 LLM이 활용되고 있을 것이다.

제 3 절 LLM 적용 시 제한사항

1) 핵심기술 개발을 위한 전문가 및 공감 부재

앞선 사례 ‘AIP’ 등 LLM을 무기체계에 적용하는 것은 전문적인 기술 영역으로 전문가 양성이 필수적이다. 미국, 영국, 중국, 러시아, 독일 등 주요국에서는 국방 AI 전략적 우위를 강화하기 위해 AI 인력양성에 총력을 다 하고 있다. [그림 3-3]과 같이 특정 국가에 AI 전문인력이 집중되

있고 특히 건수도 비례함을 알 수 있다.



[그림 3-3] AI 인력부족현황(18~22년), AI 특허 보유 기업³¹⁾

각 군 AI·빅 데이터 분야 석사급 전문인력은 전군에 30명(육군 7명, 해군 6명, 공군 17명)에 불과하며, 전문가 부족은 AI 확산에 장애 요인으로 작용하고 있다.³²⁾

최근 중국 스마트폰을 홍보하던 직원이 전직 ‘삼성맨’ 이었다는 기사³³⁾는 많은 교훈을 준다. 전문인력을 양성해도 관리되지 않으면 개인 이익을 추구하는 등 조직 인력 및 기술유출이라는 결과를 초래한다는 것이다.

국내 AI 인력 필요성이 기하급수적으로 증가함을 보았을 때 군내에도 AI 전문 인력양성은 중요하며 전문 인력이 유출되지 않도록 하는 것 또한 중요한 사안임이 분명하다. 따라서 인재양성과 공감 형성을 위한 최적화된 교육제도가 필요하며, 인재양성을 기반으로 LLM 관련 핵심기술이 개발되어야 한다.

2) AI 무기체계의 신속한 획득 제한

LLM 기술발전 속도는 빠르게 증가하고 있다. ‘AIP’가 LLM을 적용한 무기체계라는 점에서 의의가 있지만 앞으로 LLM 발전에 따라 더욱 정교

31) 국방부 국방개혁실. (2022.3), 7. 재인용, statista. (2023.1.26.). The Companies Holding the Most AI Patents. <<https://www.statista.com/chart/19211/companies-with-the-most-ai-patents>> (검색일: 2024.2.12.) 재인용

32) 국방부 국방개혁실. (2022.3), 7.

33) 서울경제. (2023.10.24.). 중국폰 들고 “삼성 타도” 외친 그 남자…알고보니 전직 ‘삼성맨’. <<https://m.sedaily.com/NewsView/29W32079W7>> (검색일: 2024.2.13.)

해질 것이다. 이런 기술 특징을 고려했을 때 정보통신기술(ICT)과 밀접하게 연계되어있는 AI 기술이 접목된 무기체계를 일반적인 무기체계 ‘획득 프로세스(acquisition process)’를 적용하여 개발할 경우 많은 문제점이 발생한다. 특히, 일반적인 획득절차를 적용하면 소요결정, 각종 분석 및 검증 등 사업 준비에 7년 이상, 시험평가에 2년, 양상준비에 2년 이상 소요되는 등 절차가 복잡하다.³⁴⁾ 약 10~15년 장기간 소요되고 전력화 시점에는 이미 낙후된 기술이 적용되는 문제가 있다.³⁵⁾

또한 소요기획 단계 핵심은 전장에서 무기체계 운영개념설정과 실질적인 구현을 위한 무기 ‘주요작전운용성능’(이하‘ROC’)³⁶⁾을 결정하는 것이다.³⁷⁾ ROC는 [그림 3-4]와 같이 장기소요 결정 시 최초 제시되고 중기소요전환 간 최종 결정되며, 이후 사업이 진행되면서 수정된다.



· 사추 : 사업추진기본전략 / **사타 : 사업타당성 조사

[그림 3-4] 연구개발절차와 ROC 결정·수정³⁸⁾

소요군과 합참의 소요제기와 소요 결정단계에서 ROC는 무기체계 획득 가능성, 운영개념과 상호연관성을 갖고 다른 요소 결정에 영향을 주고받는 등 핵심적인 역할을 한다. 소요 결정 이후 선행연구, 탐색개발과 체계

34) 오원진. (2024.1). 무기체계 신속획득제도(Fast-Track) 정착을 위한 제언. 『국방과 기술』, 539, 81.

35) 최성빈. (2012.11). 미국의 국방획득절차 개선 방향 소개 및 시사점. 『주간국방논단』, 1438, 1~2.

36) 작전운용성능은 주요 작전운용성능, 합동성 및 상호운용성, 보안대책, 기술적·부수적 성능으로 구성된다. ROC는 영어로 Required Operational Capability로 표현하지만, 군사력 건설 업무 추진 시에 주요 작전운용성능으로 통용되고 있기에 본 연구에서는 주요 작전운용성능을 ROC로 표현하였다.

37) 김홍빈. (2021). 한국군 군사력 건설에서 진화적 ROC 적용방안 연구. 『한국방위산업학회지』, 28(3), 94.

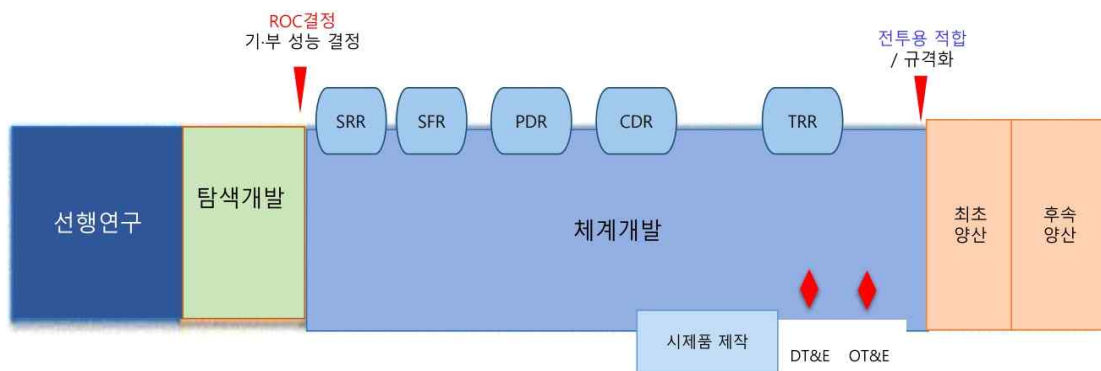
38) 오원진, 심상렬. (2018.6.23.). 무기체계 작전운용성능(ROC)의 수정 원인 및 최소화 방안 연구. 『한국방위산업학회지』, 4. 참고 재구성

개발 근거를 제공하고, 연구개발이나 구매 등 획득방안을 결정하는 기준이 된다. 이러한 ROC는 데이터를 통해 성능이 계속 향상되는 LLM 기술 특징을 고려, 결정 후 변화가 없다면 전력화 시점에는 무기체계의 기술 진부화가 발생한다.

3) AI 무기체계 시험평가 방법 부재

LLM의 무기체계 적용을 위한 핵심기술 연구개발 이후 체계개발에 적용하는 문제도 중요하다. 체계개발은 작전운용성능을 만족하는 무기체계를 설계, 그에 따른 시제품을 제작하여 시험평가를 거쳐서 양산에 필요한 국방규격을 완성하는 단계로 그 수행절차는 [그림 3-5]와 같다.

주요 수행내용으로 체계요구조건 검토(SRR), 체계기능검토(SFR), 기본설계검토(PDR), 상세설계검토(CDR), 시험 준비상태검토(TRR), 시험평가(DT & OT) 및 결과판정, 체계기능 형상 확인(FCA), 물리적 형상 확인(PCA) 등을 수행한다. 또한 제조성숙도 평가를 진행하며, 그 결과를 양산단계 진입 여부 결정 시 반영한다. 체계개발단계 종료 시점은 국방 규격화가 완료되는 시점이다.



[그림 3-5] 체계개발절차

여기서 중요한 사항은 시험평가(OT & DT)다. LLM 기술 특징을 고려했을 때 품질이 검증된, 전투용 적합 판정받은 무기체계를 사용하기 위해서는 시험평가가 중요하기 때문이다.

시험평가는 개발 및 운용 측면에서 무기체계 객관적인 성능을 검증하고 평가하는 기초자료를 획득하는 과정이다. LLM은 AI 모델 성능이 데이

터에 의해 결정되고 평가에 별도의 데이터가 필요하다는 특징이 있다. 따라서 LLM은 첨단기술로 관리되고 운용자 관점에서 평가가 이뤄져야 한다. AI 기반 무기체계도 시험평가 3대 원칙 즉, 적법성, 객관성, 타당성이 준수되어야 하는데 첫째, 효율적인 시험평가를 수행하기 위해 AI 적용 관련 법령 및 규정이 정비되어야 하고 둘째, 시험평가결과 판정 시 합리적인 판단기준이 정립되어야 하며 셋째, 시험평가 객관성과 신뢰성 확보를 위한 전문지원조직을 강화할 필요가 있다. 하지만 LLM 즉, AI가 적용된 무기체계에 대한 시험평가 방법 및 법령이 부재하다는 제한이 있다.

4) AI 모델 품질관리를 위한 기반환경조성 미흡

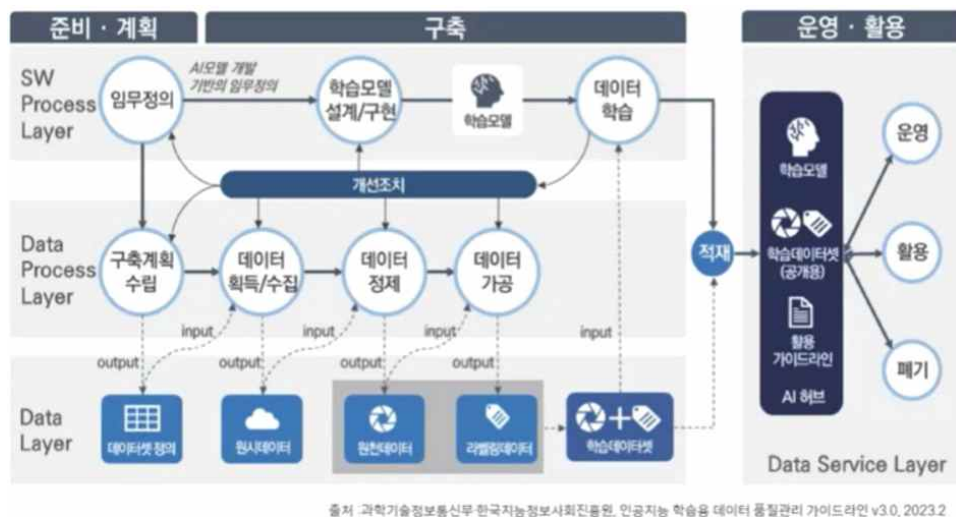
LLM을 구현하기 위해 품질 좋은 많은 데이터가 중요하다고 강조하였으며 [표 3-2]와 같은 사례를 보았을 때 그 중요성을 더욱 체감할 수 있다.

[표 3-2] 데이터 중요성(사례)

구분	내용	비고
① ³⁹⁾	미 공군의 인공지능(AI) 무인기(드론)가 ‘임무에 방해된다’며 드론을 통제하던 조종사가 있는 관제탑을 파괴하는 일이 벌어졌다.	편향된 데이터 학습 사례
② ⁴⁰⁾	챗GPT가 인터넷 상에 떠있는 정보를 무차별 수집했다는 사실…특히 훈련 데이터에는…이용자의 이름, 이메일 주소, 전화번호 같은 민감한 개인정보도 포함돼 있었다.	데이터 비식별화 미흡 (개인정보 보호 미흡)
③ ⁴¹⁾	“데이터 수집 단계에서부터 편향성을 제거하고 꾸준히 모니터링해야 한다.” - 이혜숙 한국과학기술센터혁신센터 소장 -	데이터 품질, 다양성 강조
④	“쓰레기를 놓으면 쓰레기가 나온다”는 말처럼, “디지털 시대에 데이터의 중요성은 그만큼 더 커질 수밖에 없다.” - 신혜은 충북대 법학전문대학원 교수 -	데이터 중요성
⑤ ⁴²⁾	국내 기업 등의 인공지능 학습용 데이터 구축은 많은 시간과 비용이 소요되며, 인공지능 도입·개발에 진입장벽으로 작용 * 인공지능 서비스 개발에서 데이터 구축에 자원의 80%가 투입	데이터구축이 AI 도입의 장애 요인으로 작용
⑥ ⁴³⁾	우리 군에게…가장 중요하면서도 어려운 부분은 양질의 데이터 확보이다. 데이터가 없다면 인공지능 구현은 불가능하며 얼마나 양질의 데이터를 획득할 수 있느냐가 인공지능 발전의 초석이 될 것이다.	국방 데이터 확보 중요성, 어려움

39) 김용훈. (2023.8). 미래 한반도 해역 대잠전 시나리오 기반 해양 유·무인 복합체계 발전방향. 『국방과 기술』, 534, 86.

①, ② 사례는 데이터 품질검증 없이 무분별한 학습결과로 초래된 것이며, ③, ④는 데이터 중요성, ⑤는 학계 데이터 부족에 따른 AI 도입 어려움을 보여준다. ⑥은 국방 데이터 확보의 중요성과 어려움을 시사한다. 민간업체 대상으로 시행된 군 데이터 수요조사 설문(22년 7월)에서도 많은 전문가가 연구간 필요한 신뢰할 수 있는 품질 좋은 데이터와 정확히 라벨이 정의된 데이터를 요구했다. 또한 다량의 데이터가 제공된다면 기꺼이 많은 플랫폼 개발에 도전해 볼 의향을 내비쳤다.⁴⁴⁾ 이렇게 중요한 데이터가 구축되는 과정은 [그림 3-6]과 같다.



[그림 3-6] 데이터 구축 프로세스 및 데이터 생애주기

데이터 구축계획을 수립하고 원시데이터를 확보 후 데이터 정제를 통해 원천데이터를 확보한다. 이후 원천데이터를 가공함으로써 라벨링 데이

40) 네이버 뉴스. (2023.12.5.). 챗GPT에 ‘같은 단어 반복하라’ 했더니.... <https://n.news.naver.com/article/092/0002313854?type=editn&cds=news_edit> (검색일: 2024.2.2.)

41) 네이버 뉴스. (2023.12.6.). ‘괴물 AI’ 막으려면 편향성 극복 규제 법제화해야 <https://n.news.naver.com/article/310/0000112564?type=editn&cds=news_edit> (검색일: 2023.12.8.) ④항도 동일자료 인용

42) 한국지능정보사회진흥원. (2023). 『2023년 인공지능 학습용 데이터 라벨링 전문교육(프로젝트 관리) 강의자료』 참고

43) 최근하, 오재진, 김영길. (2020), 48-51.

44) 한국전략문제연구소. (2022.9.15.). 『민군 겸용 데이터 플랫폼 구축』, 16-19.에서 ‘민간 데이터 소요 분석결과’ 내용을 정리

터를 확보하고 모델이 활용하게 될 학습 데이터셋⁴⁵⁾이 구축된다.

인공지능 서비스개발에서 데이터구축에 자원의 80%가 투입되는 등 많은 예산과 전문가가 필요하며 데이터를 전문적으로 다루는 ‘데이터 라벨러’ 소요도 증가할 것이다.⁴⁶⁾ LLM을 적용한 무기체계 획득을 위해서 모델이 학습할 데이터구축과 품질관리가 중요하나 기반환경이 미흡하다.

지금까지 LLM 기술 특징과 적용사례를 기초로 무기체계 적용 시 제한사항을 도출했는데 요약하면 다음과 같다.

[표 3-3] LLM의 무기체계 적용 시 제한사항

특징	제한사항
전문적인 기술영역	핵심기술 개발을 위한 전문가 및 공감 부재
기술발전 속도가 빠름	AI 무기체계의 신속한 획득 제한
데이터 학습을 통해 성능향상 다양한 품질 좋은 데이터 필요	AI 무기체계 시험평가 방법 부재
	AI 모델 품질관리를 위한 기반환경조성 미흡

45) 데이터 구축 과정에서 데이터에 대한 개념은 다음과 같다. (출처: 한국지능정보사회진흥원. (2023))

원시 데이터	기계학습을 목적으로 획득 단계에서 수집 또는 생성한 음성, 이미지, 영상, 텍스트 등의 데이터
원천 데이터	원시데이터를 라벨링 공정에 투입하기 위해 필요한 전처리 등 정제 작업을 수행한 데이터로 라벨링 데이터가 부여되지 않은 상태의 데이터
라벨링 데이터	원천데이터에 부여한 ‘참값’, 과령형식이나 해상도 등의 속성, 설명이나 주석 등이 포함된 ‘어노테이션’의 집합
학습 데이터	인공지능의 기계학습에 사용하는 원천 및 라벨링 데이터의 묶음을 말하며, 사용하는 목적에 따라 ‘훈련, 검증, 시험 데이터셋’으로 구분

46) 최근 데이터 라벨링 시장 규모가 25년에 29조 원대 규모로 커질 것이며, 테크 업계 관계자는 “AI가 인터넷 같은 범용 기술로 자리 잡는 만큼, 데이터 라벨링 수요는 더욱 늘 수밖에 없다”고 했다. (출처: 조선일보. (2024.2.15.). ‘데이터 라벨링’의 진군 <https://www.chosun.com/economy/tech_it/2024/02/15/QO4GYZSTSFDPAW2JZRDJ6VWI4> (검색일: 2024.2.15.))

제 4 장 대규모 언어모델(LLM)의 무기체계 적용 방안

앞서 도출한 제한사항을 극복하기 위해 아래와 같이 네 가지 사항을 고려해야 한다.

[표 4-1] LLM의 무기체계 적용 시 고려사항

특징	제한사항	고려사항
전문적인 기술영역	핵심기술 개발을 위한 전문가 및 공감 부재	LLM 핵심기술 개발 및 인재양성
기술발전 속도가 빠름	AI 무기체계의 신속한 획득 제한	AI 무기체계의 신속한 획득 프로세스
데이터 학습을 통해 성능향상 다양한 품질 좋은 데이터 필요	AI 무기체계 시험평가 방법 부재	AI 무기체계 시험평가
	AI 모델 품질관리를 위한 기반환경조성 미흡	무기체계 품질관리를 위한 기반환경조성

첫째, LLM 핵심기술 개발 및 인재양성 방안이 필요하다. LLM을 무기 체계에 적용하기 위한 핵심기술 개발이 필요하며 그 기초가 인재양성이다. AI 기술은 컴퓨터 프로그램 및 데이터에 대한 전문지식을 갖추어야 구현할 수 있는 전문적인 기술영역이다. 따라서 군내 인공지능에 대한 정책 및 기술적인 전문능력을 갖춘 인재를 양성해야 한다. 또한 전문적인 기술이 각 무기체계에 적용되었을 때 거부감 없이 사용할 수 있도록 전 장 병 공감(친숙화)이 필수적이다.

둘째, AI가 적용된 무기체계의 신속한 획득절차가 필요하다. LLM은 데이터 학습을 통해 성능이 향상되기 때문에 무기체계를 획득하는 과정에서 ROC 수정과 진화적 획득이 필수적이며, 기술 진부화를 방지하기 위한 신속한 획득 프로세스 적용이 필요하다.

셋째, AI 무기체계 시험평가 방안이 필요하다. LLM은 데이터품질에 따라 환각을 일으키기도 한다. 따라서 모델을 개발할 때 데이터 및 성능확인이 매우 중요한 요소다. 무기체계에 대한 객관적인 시험평가로 소요군이 성능 검증된 무기체계를 사용할 수 있도록 하는 것이 중요하다.

넷째, 무기체계 품질관리를 위한 방안이 필요하다. LLM은 다양한 품질 좋은 데이터가 많으면 많을수록 신뢰할 수 있는 모델이 만들어진다. 하지만 국방 데이터⁴⁷⁾는 일부 데이터를 제외한 나머지가 민간에서 획득하는데 제한적이기 때문에 군내 각종 데이터를 구축할 수 있는 기반환경조성이 필수적이며 구축된 데이터를 기반으로 무기체계가 획득되는 과정에서 품질관리를 수행할 수 있는 제도적 보완이 필요하다.

본 장에서는 네 가지 고려사항을 중심으로 구체적인 방안을 제시하였다.

제 1 절 LLM 핵심기술 개발 및 인재양성 방안

국방전략기술은 국가안보 유지, 미래 전장 선도, 국가과학기술 융합 관점에서 국방목표 달성을 위해 전략적 투자 및 육성이 필요한 기술이다. 정책·기술·경제적 관점의 선정지표를 설계·평가하여 국방전략기술 10대 분야를 선정하는데, 첫 번째 기술이 인공지능이다. 인공지능은 선진국을 기준(미국 100) 88수준으로 평가된다.



[그림 4-1] 인공지능 기술 수준⁴⁸⁾

「국방과학기술혁신 기본계획」의 국방과학기술 발전 방향에 근거하여

47) 국방 데이터는 활용 가능한 양이 매우 적으면서 확보 또한 어려운 경우가 많아 범용적으로 AI 기술을 사용하는데 한계가 있음. (출처: 한국국방기술학회. (2020.12). 『국방 인공지능 발전계획 수립 연구』, 12.)

48) 이재국, 이일로. (2022.7.4.). 국방 AI 플랫폼 개발을 위한 제언. 『KRIT Issue Paper』, 03, 7.

인공지능의 구체적인 기술개발 방향 및 확보방안을 「국방기술기획서」에 제시하고 있다. 이를 통해 우선, LLM 핵심기술 개발방안을 제시하고 핵심 기술 개발을 뒷받침할 인재양성 방안을 제시하였다.

1) LLM 핵심기술 개발방안

「국방기술기획서」에 AI를 활용한 전장 상황분석과 의사결정 지원으로 미래 전장 우위를 달성하고, 지능형 국방운영체제로 혁신하여 인구절벽에 대응하며 고효율 국방운영 구현을 목표로 네 가지 중점기술을 제시하고 있다.

첫째, 지능형 전장 인식/판단으로 다중/다종 수집자산으로 수집되는 자료/정보를 기반으로 모델링/분석/융합/학습/정보생성/추론하는 인공지능 기반 지능형 전장 상황 인식/판단 기술이다.

둘째, 지능형 통합지휘 결심으로 미래전의 복잡한 전장 환경에서 지휘관의 효과적인 지휘 결심을 위해 인공지능으로 전장 상황분석·판단 결과에 따른 최적의 방책을 제시하여 한국형 ‘결심중심전’을 구현하는 기술이다.

셋째, 스마트 전력지원으로 첨단무기체계 운용, 물자/탄약/수송지원, 인사/행정/의료 등 다양한 전력지원 활동으로부터 생성되는 방대한 데이터를 인공지능을 통해 지능화하여 과학적, 효율적인 전투지속을 지원하는 것이다.

넷째, 국방 AI 플랫폼으로 국방 AI 분야 기능별 원천기술을 확보/활용 가능토록 하고, 데이터 수집·관리·활용 기반을 구축하여 목적에 맞춰 활용 가능한 AI 플랫폼을 개발하는 기술이다.

이러한 기술을 활용해 향후 5년에는 ‘지능형 탐지체계’, 15년에는 ‘AI 기반 다중분석체계’, 15년 이후는 ‘AI 기반 지휘 결심지원체계’ 구축을 목표로 하고 있다.

개발 목표를 달성하기 위한 중점기술별 단/중기 및 장기 목표기술을 정리하면 [표 4-2]와 같다.

[표 4-2] 중점기술별 목표기술 (요약)⁴⁹⁾

중점기술	시기별 목표기술		
	단/중기(~F+5)	장기(~F+10)	장기 이후(~F+15)
1. 지능형 전장 인식/판단	다중센서 기반 영상 개선 기술	자율적 지능화 전장 상황/위협 판단 기술	-
	전출처 정보융합 및 실시간 전송기술 등 18건	3차원 전장 정보 관리 및 가시화 기술 등 13건	
2. 지능형 통합지휘결심	-	요구정보 및 전장환경을 정책 추천 기술	-
		대기뢰전 유·무인 복합 운용 기술 등 5건	
3. 스마트 전력지원	AI 기반 군수데이터 분석기술	증강현실 기반 시뮬레이터 구축 기술	-
4. 국방 AI 플랫폼	무기체계 SW 신뢰성 확보를 위한 AI 기반 테스트 기술 등 3건	지능형 에이전트 개발 기술 등 3건	-

지능형 전장 인식/판단에서는 텍스트, 이미지, 영상 등 다양한 출처로 수집된 정보를 인식하고 분석하여 판단하거나 3차원(텍스트, 이미지, 영상 등) 가시화가 중점이다. 지능형 통합지휘 결심에서는 전장을 인식하고 판단한 것을 기초로 정책을 자동으로 생성하거나 추천하여 지휘 결심을 지원하고 유·무인 복합과 효과적인 의사소통으로 효율적인 운용이 중점이다. 스마트 전력지원은 여러 비정형 데이터를 분석하고 시뮬레이션하는 기술이 중점이며, 국방 AI 플랫폼은 다양한 데이터를 일원화하여 여러 분야에서 효율적으로 활용하기 위한 에이전트를 개발하는 것이 중점이다. 이러한 네 가지 중점기술을 구현하기 위해서는 멀티모달에 의한 LLM이 핵심이 될 것이다.

국방 AI 중점기술 분야를 기초로 국방 무기체계에 LLM을 적용할 수 있는 기술은 [표 4-3]과 같다.

49) 방위사업청, 국방기술진흥연구소. (2023). 『‘23~’37 국방기술기획서(일반본)』, 25~34.

[표 4-3] 무기체계에 적용 가능한 LLM 기술

중점기술	적용 사례	내용
1. 지능형 전장 인식/판단	AI 참모(비서) *합동전영역지휘통제체계 (JADC2)	전장 인식, 정보수집분석, 전략적 의사결정(최선의 방책 조언)
	통신(의사소통)	무전 내용(음성)을 텍스트로 변환
	언어 번역기	연합훈련 간 활용(다국어 통신과 번역)
2. 지능형 통합지휘 결심	유·무인복합체계 (MUM-T)	생체인식을 통한 원격통제
	디지털 휴먼	상담 및 협상, 포로 심문, 심리전 등
3. 스마트 전력지원	군수 공장 (무기체계 제작)	소프트웨어 작성, 로봇 학습 → 디자인, 제작, 품질검사 자동화
	AI 교관 (군사교육 및 시뮬레이션)	질의응답, 강의록 제작, 콘텐츠제작, 강의, 문제출제 및 채점, 설문 및 성과분석
	콘텐츠제작	국방신문, 뉴스, 정신전력 자료 및 홍보영상 제작
4. 국방 AI 플랫폼	무기체계(SW) 품질관리	무기체계 획득 전 과정에서 품질관리 수행
	챗봇(국방 GPT)	미세조정된 모델을 특정 전문 병과에 활용

첫째, 지능형 전장 인식/판단 분야는 대표적으로 AI 참모(비서), 무전기 등 통신, 언어 번역기에 적용할 수 있다. AI 참모는 현재 개발을 위해 노력하고 있는데 아이언맨 ‘자비스’처럼 멀티모달 기능으로 다 출처 영상 융합으로 전장을 인식하고 분석하여 최선의 방책을 조언하기 위한 핵심이 LLM이다. LLM이 이미지, 비디오, 오디오, 텍스트 간의 인식 및 출력을 가능하게 할 것이다. 또한 무전기 등 통신에 LLM을 적용하면 실시간 음성이 텍스트로 변환되어 기록되며 음질이 저하된 잘 들리지 않는 내용을 예측, 텍스트로 제시하면서 작전 간 의사소통에 기여할 것이다. 세계 각국 언어로 학습된 LLM은 연합작전 간 다양한 상황에서 전장을 올바르게 인식할 수 있다.

둘째, 지능형 통합지휘 결심 분야는 유·무인 복합체계 운용과 디지털 휴먼에 적용할 수 있다. 유·무인 복합체계의 효율적인 운용을 위한 핵심은 사람과 로봇 간 의사소통이다. 텍스트, 음성, 이미지 심지어 생체신호를 통해 로봇을 제어할 수 있어야 하는데 모달리티 데이터에 의해 학습된

LLM이 이를 가능하게 할 것이다. 각 로봇 엣지 컴퓨터의 LLM은 다양한 상황에서 로봇 스스로 가장 적합한 결심을 할 수 있게 하는 원동력이 될 것이다. 디지털 휴먼은 평소 장병들에 대한 상담서비스를 통해 상담관 역할을 대체하고, 대화를 통한 감정인식 및 방언, 북한 주민 언어이해는 전시에 유용하게 활용할 수 있다. 적 무전 및 포획문서에 대한 정확한 해석과 학습된 아바타를 통한 포로 심문은 전시에 정확한 정보를 제공해 줄 것이다. 또한 최근 전쟁사레처럼 가상 디지털 휴먼을 활용한 고도 심리전을 가능케 하는 등 비살상 효과를 만들어 내는 무기체계 한 축으로 역할을 기대할 수 있다.

셋째, 스마트 전력지원 분야는 무기체계를 제작하는 군수공장, AI 교관, 콘텐츠제작에 적용할 수 있다. 군수공장에서는 각 부품에 대한 설계와 생산을 최적화하고, 로봇을 학습시켜 디자인, 제작, 품질검사 등 제작 전 과정에서 작은 결함까지 식별하는 등 자동화를 통해 생산성 향상에 도움을 줄 수 있다. 먼저, 설계 및 모의실험에 있어서 설계된 무기체계에 대한 시뮬레이션 결과를 자연어로 질의하고, 시스템이 해당 결과를 분석하여 설계 결정에 대한 의사결정을 지원할 수 있다. 또한 개발자는 반복적인 코드 패턴이나 단순 함수를 코딩하는 것을 AI 서비스에 일임하여 전체 프로그래밍 작업의 효율을 높일 수 있다. 깃허브에 따르면 개발자는 코파일럿이 생성한 코드 26퍼센트 정도를 수락했으며, 개발자 코드 파일 중 평균 27퍼센트 정도가 코파일럿을 통해 생성되었다. 파이썬의 경우에는 코파일럿을 통한 코드 생성 비율이 40퍼센트까지 차지하는 수준이라고 알려져 있다.⁵⁰⁾

AI 교관은 모달리티 기능을 학습한 LLM으로 교육생 질의응답, 주제에 맞는 강의록 제작, 콘텐츠제작, 강의, 문제출제 및 채점, 설문 및 성과분석 등이 가능하여 교관이라는 고급인력을 대체할 수 있다. 또한 장병들은 AI 교관과 학습을 통해 LLM이 적용된 무기체계를 효과적으로 활용할 수 있을 것이다. 콘텐츠제작에서는 국방신문, 뉴스, 교육 콘텐츠제작 등 그림과 영상을 포함한 기사를 작성하고, 디지털 휴먼은 뉴스를 전달하며, 정신전

50) 김대환, 고은진. (2023.7.31.), 261. 24.

력 자료 및 홍보영상을 제작할 수 있어서 인력 및 시간을 절약할 수 있을 것이다.

넷째, 국방 AI 플랫폼 분야는 무기체계 품질관리 및 챗봇에 적용할 수 있다. 국방 AI 플랫폼은 다양한 데이터의 총체적 집합이다. 활용 중인 무기체계, 교리, 언어, 특정 전문기술 등 다양한 데이터를 활용하여 무기체계 획득 전 과정에서 품질관리를 할 수 있으며 품질이 보장된 무기체계를 획득할 수 있게 할 것이다. 또한 특정 분야에 미세조정된 챗봇은 사용자에게 원하는 정보를 적시에 다양한 형태로 제공해줄 것이다. 최근(24년 7월) 국방부에서 인트라넷 서비스를 개시한 ‘국방생성 AI(Generative Defense AI)’가 대표적인 사례이다. 국방 내부망에서 군사용어 특화번역, 군 내부규정 질의응답, 문서 요약 등 맞춤형 서비스를 시범적으로 제공하고 있다.⁵¹⁾

무기체계 적용 가능한 LLM 기술을 「국방기술기획서」 국방 AI 중점기술 분야를 기준으로 제시하여 설명하였다. 이러한 기술들은 단기, 중기, 중·장기, 장기로 구분하여 체계적으로 추진해야 한다. 가장 먼저 개발해야 할 핵심은 ‘국방에 특화된 한국어 LLM’이다. 생성형 AI 기초에 LLM이 있는 것처럼 다양한 무기체계에 LLM을 적용하기 위해서는 국방에 특화된 한국어 LLM 구축이 선행되고 국방이 소유권을 갖도록 하는 것이 중요하다.

2) 인재양성 방안

육군⁵²⁾은 부족한 인재를 양성하기 위해 5년간(22~26년) AI 관련 직위(373개)를 고려, 400명 인재양성을 목표로 ‘육군 인공지능(AI) 역량 강화 추진계획’을 작성하여 추진하고 있다. 이를 기초로 체계적인 인재양성 방안을 제시하면 [표 4-4]와 같다.

신분별 목적에 맞게 교육과정이 수립되어 있다. 인재양성과 공감 형성 두 가지의 목적으로 총 5개 교육으로 구성되어 있다. 한 건을 제외, 모든

51) 지티티코리아. (2024.7.7.). AI와 LLM로 강력해지는 국방력. <<http://www.gttkorea.com/news/articleView.html?idxno=11917>> (검색일: 2024.9.21.)

52) 신뢰할 수 있는 내용을 위해 소속된 조직, 경험한 것을 토대로 분석하였으며, 그 속에서 제시한 방안은 국방 전체에 방향성을 제공해줄 것이다.

교육을 국방부 예산으로 수행함으로써 대내외적으로 군의 AI 인재육성을 위한 의지를 표명함과 동시에 기타 AI 기술 분야도 국방 예산확대를 도모할 수 있다. 군내 전문가 부재로 민간위탁 교육이 불가피할지 모르지만, 장기적으로 ②, ④는 군주도 시행, 민간과 차별되는 군 특성에 맞는 교육이 가능하다. 과정별 교육을 주관하는 기관은 충분한 검토가 필요하다.

[표 4-4] 인공지능(AI) 인재양성 방안(핵심내용)

구분		내용	비고																				
①	AI 인프라 구축 및 문화조성	- AI 교육장 구축(총 42개 부대 신청, 6개 부대 추진, 3개 부대 선정) * 각 (병과)학교기관 우선 구축, 교육 간 활용 - 인공지능 경진대회(군 장병, 4인 1팀)	국방부 예산 (공감 형성)																				
②	군 특화 AI 전문 교육과정 [소집]	교육과정 요약 <table border="1"> <thead> <tr> <th>과정</th><th>기간(과정) *연 기수 유지</th><th>자격요건</th><th>주관</th></tr> </thead> <tbody> <tr> <td>정책·제도 수립</td><td>8주(2)</td><td>KT AICE BASIC 이상 소지</td><td>국방부 (육군본부)</td></tr> <tr> <td>소요기획·사업관리</td><td>10주(기본·심화)</td><td>KT AICE ASSOCIATE 이상 소지</td><td>국방부 (육군본부)</td></tr> <tr> <td>체계개발·운용</td><td>12주(기본·심화)</td><td>KT AICE ASSOCIATE 이상 소지</td><td>ADD</td></tr> <tr> <td>AI 핵심인재 양성</td><td>12주(입문·기본·심화)</td><td>KT AICE PROFESSIONAL 이상 소지 또는 관련 이상 학위소지자</td><td>ADD</td></tr> </tbody> </table>	과정	기간(과정) *연 기수 유지	자격요건	주관	정책·제도 수립	8주(2)	KT AICE BASIC 이상 소지	국방부 (육군본부)	소요기획·사업관리	10주(기본·심화)	KT AICE ASSOCIATE 이상 소지	국방부 (육군본부)	체계개발·운용	12주(기본·심화)	KT AICE ASSOCIATE 이상 소지	ADD	AI 핵심인재 양성	12주(입문·기본·심화)	KT AICE PROFESSIONAL 이상 소지 또는 관련 이상 학위소지자	ADD	국방부 예산 (인재육성)
과정	기간(과정) *연 기수 유지	자격요건	주관																				
정책·제도 수립	8주(2)	KT AICE BASIC 이상 소지	국방부 (육군본부)																				
소요기획·사업관리	10주(기본·심화)	KT AICE ASSOCIATE 이상 소지	국방부 (육군본부)																				
체계개발·운용	12주(기본·심화)	KT AICE ASSOCIATE 이상 소지	ADD																				
AI 핵심인재 양성	12주(입문·기본·심화)	KT AICE PROFESSIONAL 이상 소지 또는 관련 이상 학위소지자	ADD																				
③	장병 맞춤형 온라인 교육 [온라인]	- AI 분야 온라인 교육과정 * 입문 → 초급 → 중급 → 고급, 장병 취업 교육 연계 * 수행기관 : 구름(카카오 엔터프라이즈), 엘리스	국방부 예산 (공감 형성, 인재육성)																				
④	전 장병 생애주기 및 소양교육 [소집]	- 승진자 교육(지휘참모 및 리더과정 / 교육사) * 육군대학 및 중·대령 지휘관리과정 의무화 교육 검토 - 부대 순회교육(전 부대 / ITSA, KOSSA) * 성과분석을 통한 미참여 부대의 의무화 시행 검토 - AI 실무교육(초·중·고급 / AI 실무자 / ADD) * 과정별 연계된 교육내용 시행, 교육 현장확인 강화	국방부 예산 (공감 형성, 인재육성)																				
⑤	AI 관련 신기술 교육 기회 확대 [소집, 온라인]	- KT AICE(KT에서 시행하는 온라인 플랫폼 기반 AI 교육) * 소집 교육 전 AI 소양함양을 위한 필수교육으로 활용 - NIA(한국지능정보사회진흥원) 데이터-라벨링 교육 * 수료 후 개인 기록변경 가능토록 제도 마련(인재관리)	정보화부 추진 (공감 형성, 인재육성)																				

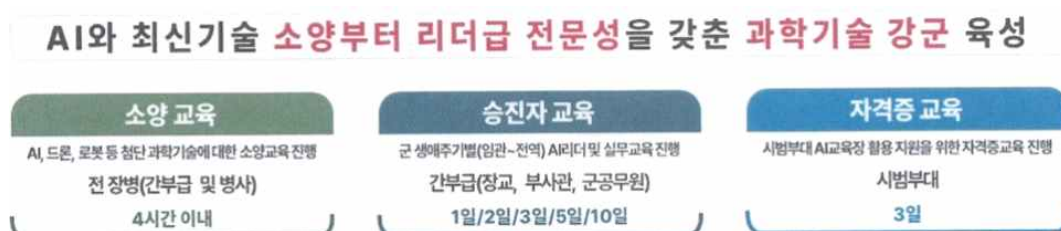
①에서 AI 교육장(AI Lab) 구축은 23년까지 3개 부대만 구축되었다. 실제 구축된 곳을 방문했을 때 인터넷 기반 실습용 노트북과 AI 학습 서적, 환경 등 잘 조성되어 있었으며 장병들이 동아리 활동으로 교육장을 활용하고 있었다. AI 교육장은 공감대 형성 차원에서 중요한 요소지만, 교육장이 구축된 부대에 국한된다는 제한이 있다.

따라서, AI 교육장은 각 (병과)학교기관에 우선 구축하여 교육 간 활용해야 한다. 군에 비교적 오래 근무하는 간부들은 각 (병과)학교를 통해 교육받을 수밖에 없다. 모든 인원이 AI 교육장을 활용함으로써 장병들까지 공감 확산이 빠르게 진행될 수 있다.

②는 목적이 뚜렷한 군 특화 AI 전문교육과정이다. 지원자에 관한 기본자격요건 없이 교육을 장기간 편성하면 목적에 맞는 지원자 발굴 제한과 교육에 대한 부담이 발생한다.

따라서, 교육 취지에 맞게 기본자격요건을 갖춘 대상을 교육해야 한다. 교육 기간은 입문·기본·심화로 구분 및 단축하여 지원자들이 부담 갖지 않도록 함으로써 우수한 인원들이 교육받을 수 있도록 여건을 조성해야 한다. 지원자가 일정 이상 수준을 갖추었기에 교육내용을 검토하면 기간을 단축할 수 있다.

③은 장병 맞춤형 교육으로 단계별 수준에 맞는 교육을 취업과 연계하여 사회 인재육성과 군내 공감 형성 차원에서 시행이 필요하다.



[그림 4-2] 전 장병 AI·SW 생애주기 및 소양교육

④는 생애주기 및 소양 교육으로 공감대 형성이 주목적이지만 AI 실무 교육은 인재육성 효과까지 달성할 수 있다. 생애주기 및 소양 교육은 [그림 4-2]와 같이 소양 교육(12개 과제), 승진자 교육(소령 이상, 6개 과정), 자격증 교육으로 구분되며 온라인을 통한 교육 신청으로 이뤄진다.

[표 4-5] 23년 교육 추진현황⁵³⁾

구분	소양교육(회)	승진자 교육(일)
교육기관	4개 기관(47회)	7개 기관(33.75일)
부대	24개 부대(42회)	10개 부대(67일)
합계	88회(22년 871회)	100.75회(22년 138회)

23년 부대 순회교육(소양 교육 및 승진자 교육) 결과를 확인해보면 [표 4-5]와 같이 교육 횟수대비 참여 기관(부대)이 적은 것, 22년 대비 교육 실적이 적은 것을 고려했을 때 교육홍보와 부대별 관심에 따라 교육 기회가 달라진다고 판단된다. 따라서 각 부대로 공문을 발송함과 동시에 승진자 교육을 야전 지휘관 임무를 수행할 육군대학 및 중·대령 지휘 관리과정 대상으로 의무 교육한다면 홍보 효과가 있을 것이다. 위와 같이 시행했음에도 미 참여한 기관(부대)은 의무교육을 고려해야 한다.

AI 실무교육은 초·중·고급으로 나누어져 있으며 신설된 AI 교육장에서 민간강사에 의해 교육이 진행되며 과정별 교육내용은 [표 4-6]과 같다.

[표 4-6] AI 실무교육 과정별 교육내용⁵⁴⁾

구분	교육시간	주요 내용 (평가 없음)
초급	1주 44H (연 4개 기수)	•1-2일 : 함수 이해, 퍼셉트론 구현, 다층 신경망 구현 •3-4일 : 학습 알고리즘 구현(역전파, 합성곱, CNN 등) •5일 : 설문 조사, 수료식 및 간담회, 부대 이동
중급	2주 80H (연 2개 기수)	•1일 : 이미지, 인공지능 기술 이해(딥러닝 모델 구현, 레이어 설계) •2일 : 이미지 식별 위한 이해 및 구성(국방 데이터 이해, 라벨링) •3-6일 : 표적 식별 위한 AI 기술 적용(이미지 전처리, 신경망 구현) •7-9일 : 이미지 활용, 표적식별 프로젝트(모델구축 실습) •10일 : 프로젝트 발표 및 소감문 작성

본 교육의 주 내용은 AI 기술 지식습득으로 초급은 알고리즘이해 및 구현에 중점을 두고, 중급은 이미지에 국한된 알고리즘이해, 데이터 라벨링 및 모델구축에 중점을 두고 있다. 초급에서 기초기술을 습득 후 중급에서 신경망을 활용한 모델구축 심화 실습을 하는 등 연계성을 고려하여 교

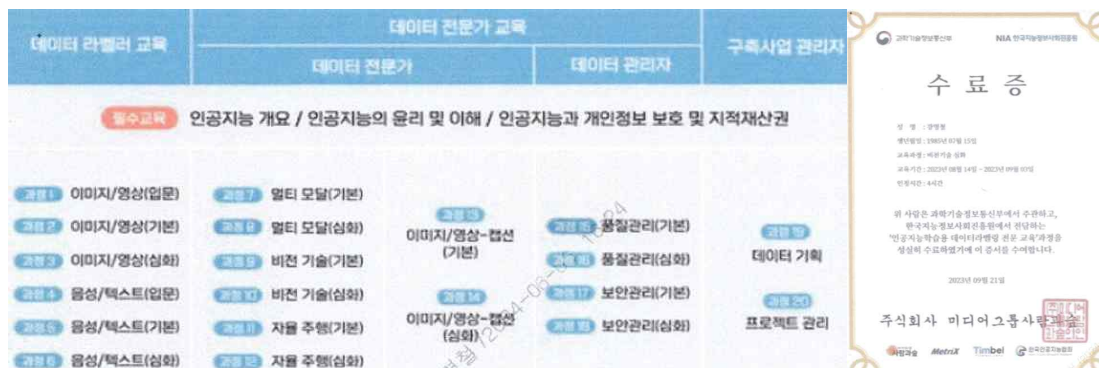
53) KOSSA. (2023.9.8.). 『「전 장병 AI·SW 생애주기 및 소양교육」 신청안내』 ④ 관련 내용은 본 참고자료를 활용, 자격증 교육과정은 AI 교육장을 활용한 교육으로 대상이 제한된다는 점에서 제외하였고 교육결과 분석에서 세부 부대명은 본 자료를 참고

54) 각 과정 일자별 교육계획 내용을 정리, 고급(연 1개 기수)은 24년 첫 교육으로 제외

육내용이 구축되어 있다. 따라서 AI 실무교육은 연계성을 위해 취지에 맞는 교육을 시행하고 강사 임의로 내용을 변경하지 않도록 현장을 확인하는 시스템구축이 필요하다.

⑤는 민간 AI 교육플랫폼(KT AICE)으로 총 5개 Level 중 2개 과정(Basic, Associate)을 교육하는데 Basic은 비전공자 대상 NO 코딩으로 교육되며, Associate는 준/전공자 대상으로 기획 및 분석 내용으로 구성된다. 또한 자격증시험 기회를 제공하여 수료 후 민간자격증을 획득, 기록변경 함으로써 개인 능력향상과 인재관리 측면에서 유용한 교육이다.

데이터-라벨링 교육은 과학기술정보통신부가 주관, 25년까지 시행하는 범정부 차원의 ‘인공지능 학습용 데이터 구축사업’ 일환이다. AI 도입 장애물인 데이터를 AI-Hub⁵⁵⁾에 구축하기 위해 데이터 라벨러 육성에 중점을 둔 전문교육이다. 세부 교육과정은 [그림 4-3]과 같다.



[그림 4-3] 데이터 라벨링 전문교육 과정, 수료증

AI 개요부터 이미지/영상, 음성/텍스트, 멀티모달, 비전기술, 자율주행 등 다양한 분야의 AI 학습용 데이터를 다룬다. 데이터에 관한 품질 및 보안, 기획 및 프로젝트관리까지 전 분야를 학습할 수 있는 효과적인 교육이다. ⑤는 사회구성원을 대상, 정부 차원의 교육으로서 타 과정 AI 교육 전 필수 소양함양을 위한 교육으로 효과적이다. 이는 국방부 예산 절감뿐만 아니라 타 과정에서 소양을 갖춘 인원을 대상으로 교육하기 때문에 해당 내용을 배제함으로써 교육 기간을 단축할 수 있다.

55) AI 허브는 AI 기술 및 제품·서비스 개발에 필요한 AI 인프라를 지원함으로써 누구나 활용하고 참여하는 AI 통합 플랫폼으로 인공지능 학습용 데이터셋이 구축된 곳이다. (네이버 지식, 검색일: 2024.2.21.)

지금까지 설명한 다섯 가지 교육제도도 중요하지만, 무엇보다 우수한 인원들이 관심 가지고 지원하도록 제도 보완이 필요하다. 예를 들어 AI 관련 보직의 진급율을 높이거나 해외연수 기회부여, 업무 수당 지급 등이 있을 것이다. 또한 교육을 이수한 인원은 인재관리 측면에서 개인기록변경이 가능토록 제도를 정비해야 한다. AI 관련 전문화된 인원을 위한 인사관리 주기 등을 고려하여 진급 예정자를 AI 관련 직위에 활용하는 등 인사제도개선 또한 병행되어야 할 것이다.

위에서 제시한 인재양성 방안은 충분한 검토가 필요하다. 전문인력이 전문성을 유지한 채 군에 좀 더 오랜 기간 근무할 수 있도록 하여 노력의 통합이 이뤄질 수 있는 기반을 만들어야 할 것이다.⁵⁶⁾

제 2 절 LLM 기반의 무기체계 획득방안

최근 ‘신속소요’를 비롯한 새로운 무기체계 획득절차를 신설하는 「방위사업법」 개정 법률안이 23년 5월 9일 국무회의를 통과, 23년 8월부터 시행되었다. 이번 방위사업법 개정은 지난 2006년 방위사업법이 제정된 이후 처음으로 기존 ‘일반획득절차’와 다른 별도의 ‘획득절차’를 신설한 것으로 [그림 4-4]와 같이 ‘신속획득’제도를 마련한 것이다.⁵⁷⁾



· 사추 : 사업추진기본전략 / **사타 : 사업타당성 조사

[그림 4-4] 일반소요 절차와 신속소요 / 시범사업 절차 비교

56) 최근하, 오재진, 김영길. (2020), 46.

57) 보도자료.(2023.6). ‘신속획득(Fast Track)’제도, 금년 8월부터 시행. 『국방과 기술』, 532, 15.

먼저 ‘신속소요’는 민간의 성숙된 기술이나 정비 핵심기술개발 등을 통해 이미 입증된 기술을 무기체계에 적용하는 사업일 경우 5년 이내에 군 전력으로 도입할 수 있도록 절차를 개선한 것이다. 소요 결정 이후 실시하던 선행연구 등 분석·검증단계를 생략하고 바로 ‘사업추진 기본전략’을 수립해 단기간에 착수한다. 이는 기존에 사업 착수까지 장기간이 걸려 착수 시점에는 이미 기술이 진부화되는 문제를 개선하겠다는 취지다. 그리고 기존 장기간 소요되던 개발시험평가와 운용시험평가를 통합하였고 별도 양산절차 없이 연구개발 직후 전력화될 수 있도록 하였다.

‘시범사업’은 각 군에서도 수행할 수 있도록 하여 군이 원하는 무기체계를 신속히 확보하도록 하였다. 또한 사업 이후 ‘신속소요’처럼 선행연구와 같은 분석·검증 단계를 생략하고 시범 운용단계에서 6개월간 성능입증 시험⁵⁸⁾을 수행하면, 그 결과로 시험평가를 대체할 수 있다.

‘시범사업’은 21년 도입되었고 방위사업청 예규로 ‘신속시범사업 업무관리 지침’을 관리 중이다. [표 4-7]과 같이 최근 개정(23.12.14)된 지침을 보면 빠른 무기체계도입을 위한 국방의 끊임없는 노력을 알 수 있다.

[표 4-7] 신속시범사업 업무관리 지침 주요변경사항 (요약)⁵⁹⁾

구분	~에서	~으로	비고
사업 분류	신속연구개발사업 신속시범획득사업	신속시범사업	신속시범사업으로 통합
사업 규모	연구개발(500억 원 미만) 획득사업(50억 원 이하)	500억 원 미만	사업의 융통성 확보
용어변경	군사적 활용성 확인	성능입증 시험	-
사업조사분석	-	소요중복성 및 소요제기 가능성 검증 항목추가	예산 중복투자 방지
연구개발 수행	-	PM의 요청가능한 항목 구체화	사업간 PM ⁶⁰⁾ 의 권한 강화
제28조 신설	-	시제품 검사·검수	시제품 품질 보증
후속 조치	긴급소요·중기소요·추가 시범사업 건의	긴급소요	전력화 지연방지

58) 각군 참모총장 및 해병대사령관이 시범사업의 성과를 객관적·합리적으로 평가하기 위하여 기관 소속 공무원 및 직원과 민간전문가로 구성된 성능입증시험팀을 구성하여 시행하는 평가 (출처: 국방부. (2023.9.25.). 『전력발전업무훈령 제2845호』, 38.)

59) 방위사업청. (2023.12.14.). 『신속시범사업 업무관리 지침 제884호』. 기초로 정리

60) PM(Project Manager): 프로젝트의 계획과 실행에 있어서 전체적인 책임과 관리, 운영의

이러한 ‘신속획득(Fast-Track)’제도 마련과 지속적인 진화는 고무적이라 생각한다. 하지만 SW와 특성이 비슷한 LLM을 비롯한 AI 기술에 효과적일지는 세밀한 검토가 필요하다. AI 분야에서 선진화된 기술을 보유한 주변국이 IT 전력 및 소프트웨어 획득을 위한 별도의 프로세스를 구축하고 있다는 것을 고려했을 때 우리 국방은 AI 기술 즉, SW 중심의 무기체계 획득을 위한 별도의 프로세스가 없다는 한계를 가지고 있다.

또한 ROC 수정과 진화적 획득 관련 내용은 [표 4-8]과 같이 ‘전력발전업무 훈령(2023.9.25.)’에 명시되어 근거를 제공하고 있다.

[표 4-8] ROC 수정과 진화적 획득의 법적 근거

구분	내용
ROC 수정 (p.17)	합참은 전력소요서(안) 작성 시 특별한 사유가 없는 한 기술발전추세를 고려하여 진화적 획득전략(나선형, 점증형)을 우선적으로 고려한다.
진화적 획득 (p.29)	합참은 국방과학기술 발전추세를 고려하여, 소요제기기관에서 수정 요구한 작전운용성능 항목 이외에도 필요한 작전운용성능 항목을 합동전략회의를 통해 추가, 수정 또는 삭제할 수 있다.

이를 바탕으로 [그림 4-5]와 같이 무기체계 획득 시 ROC 수정과 진화적 획득(점증적 개발이)이 이루어지고 있다.

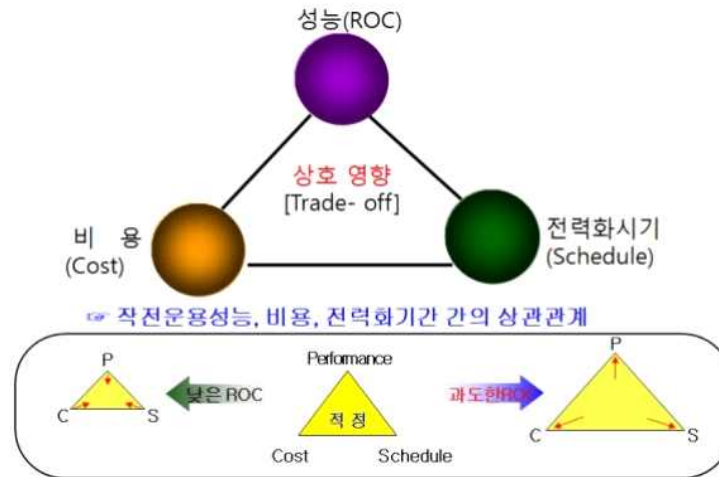


[그림 4-5] ROC 수정 현황 및 원인⁶¹⁾

권한을 가진 사람 도는 직책 (네이버 지식, 검색일: 2024.2.12.)

61) 오원진, 심상렬. (2018.6.23.), 7~9. ROC 수정과 관련된 국내 연구는 매우 빈약하며, 관련 자료는 대부분 비문으로, 자료획득이 매우 어려운 실정이기 때문에 최신 현황을 제시하지 못한 제한사항이 있지만, ROC 수정이 지속 이루어지고 있음을 인식하는 차원에서 참고 가능한 자료이기에 제시

하지만 실질적인 문제점이 있는데 우선, ROC 수정이 실제로는 소극적으로 시행되고 있다는 것이다. ROC는 [그림 4-6]과 같이 성능을 높이면 비용과 기간이 늘어나며, 성능을 줄이면 비용도 적고 개발하는 기간도 짧지만, 적과 싸워 이길 수 없는 무기체계를 만들 수 있기 때문이다.⁶²⁾



[그림 4-6] ROC 고려요소 간 상충관계⁶³⁾

또한 사업 진행에서 기술 수준을 고려 ROC를 수정하는 것도 진화적 획득의 일환이며, 위에서 제시한 바와 같이 법적으로 이를 보장하고 있다. 하지만 ROC 수정통계를 보면, ROC 완화가 많은 부분을 차지하다 보니 봐주기 논란 등 감사 대상이 된다는 인식과 더불어 빈번한 ROC 수정은 방산 기업체의 도덕적 해이로 연결될 소지가 있다. 따라서 ROC 수정은 비용과 기간에 영향을 미치고 합참과 소요군 인식에 따라 소극적인 실정이다.

둘째, 진화적 획득 중 나선형 개발적용에 대한 문제다. 진화적 획득은 기술적 진부화를 방지하고 일부 성능을 조기 전력화함으로써 전력 공백을 최소화할 수 있는 장점이 있다. 점증적 개발적용은 일반무기체계에 한정하여 접근하는 것으로 AI 기술이 적용된 정보체계나 SW에 대한 적용은 점증적 방식보다는 나선형 방식을 적용해야 한다. 하지만 진화적 획득전략에서 나선형은 개발범위와 일정, 예산을 예측할 수 없고, 현재까지 추진

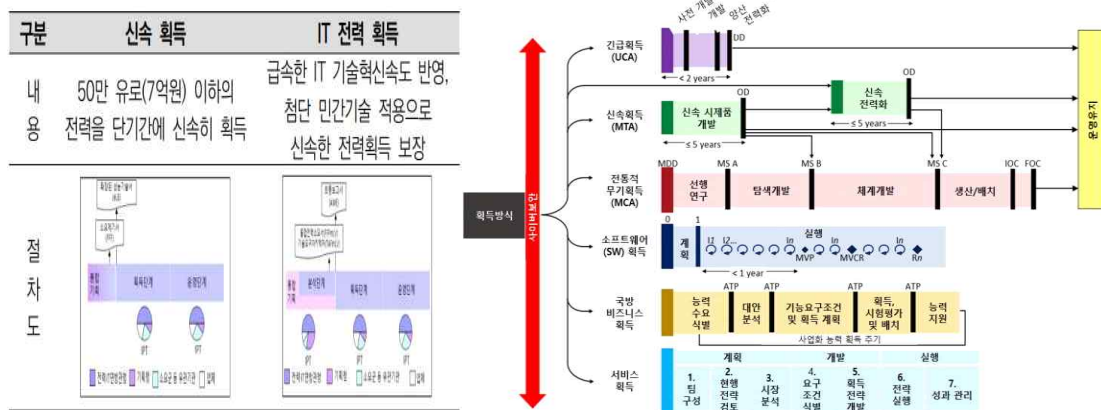
62) 김홍빈. (2021), 97.

63) 김홍빈. (2021), 97. 재인용

사례도 없어 현실적으로 의사결정이 제한된다는 문제점이 있다.⁶⁴⁾

따라서, LLM이 적용된 무기체계 신속한 획득을 위해 아래와 같이 총 세 가지 방안을 제안한다.

우선, AI 기술이 접목된 무기체계의 신속한 획득을 위해서는 주변국처럼 소프트웨어 획득을 위한 별도의 프로세스구축이 필요하다. 선진화된 AI 기술을 보유한 미국과 독일은 [그림 4-7]과 같이 각 소프트웨어 트랙 (Software Acquisition), IT 전력획득절차가 별도로 신설되어 있다.



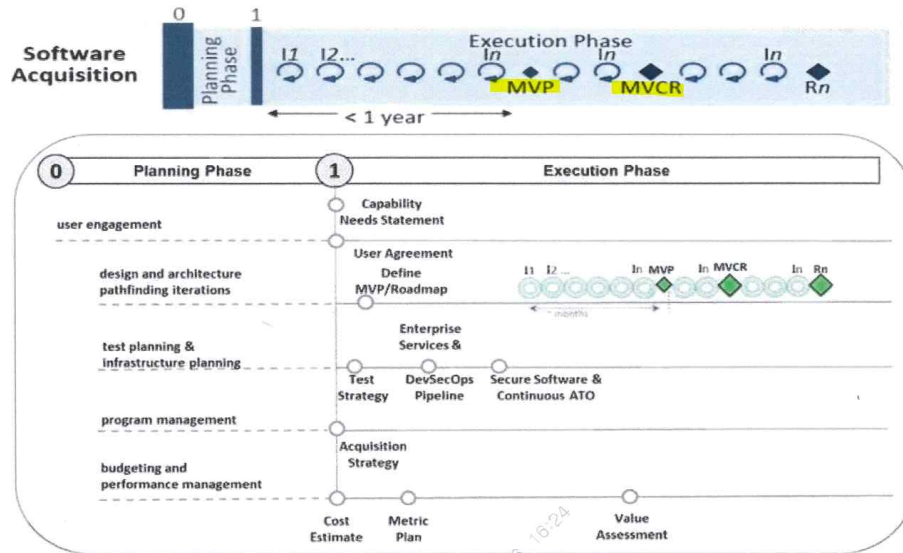
[그림 4-7] IT 전력획득절차(독일), 적응형획득 Framework(미국)

미국은 기본이 되는 주요획득사업(MDAP)외에, 우회 통로절차로서 2년 내 새로운 능력을 획득하게 하는 긴급소요 및 신속획득절차(Urgent / Emerging Operational Needs)와 함께 최신기술과 경험을 보유한 중소기업에 신속한 시제제작과 전력화를 보장해주는 중간단계획득(Middle Tier Acquisition)이 마련되어있다.

특히, 무기체계와 정보화 시스템에 AI 기술과 서비스의 적용을 위해 [그림 4-8]과 같이 소프트웨어 집약형 사업에 적합한 소프트웨어 트랙이 신설되어 있다. 이 트랙의 사업은 1년 내 반복적인 개선과 시험이 가능한 다중의 초고속 단기개발을 보장하는 애자일⁶⁵⁾ 방식 개발절차다.

64) 김홍빈. (2021), 97~108.

65) 소프트웨어 개발 방법론의 하나로, 처음부터 끝까지 계획을 수립하고 개발하는 폭포수 (Waterfall) 방법론과는 달리 개발과 함께 즉시 피드백을 받아서 유동적으로 개발하는 방법이다. (네이버 지식, 검색일: 2024.2.17.)



[그림 4-8] 소프트웨어 획득절차(미국)

사업팀은 1년 이내 획득전략을 마련하면서 기본적인 최소기능을 갖춘 소프트웨어 초기 버전인 ‘최소실행가능결과물(MVP, Minimum Viable Product)’을 정의하고 개발해야 한다. 또한 사용군의 요구를 충족할 소프트웨어 제품을 제공하는 ‘최소실행가능능력양도품(MVCR, Minimum Viable Capability Release)’과 나머지 기능의 로드맵을 개발해야 한다. MVP 목표는 평가, 피드백 및 개선을 위해 사용자에게 기본역량을 신속하게 전달하는 것이며, MVCR은 납품 일정에 따라 사용자에게 운영환경에 제공하기에 적합한 기능 집합으로서 산물이다.

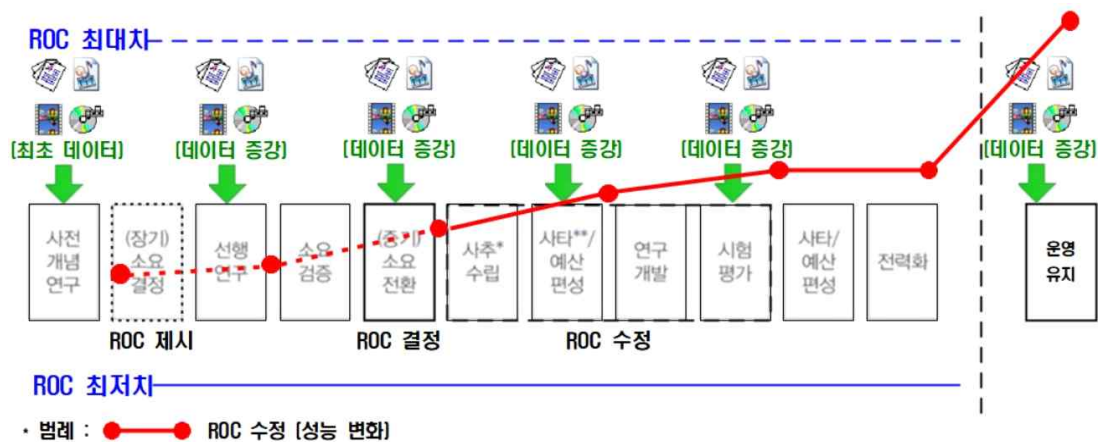


(방위사업청 제공)

[그림 4-9] 소프트웨어 중심 무기체계 획득업무 프로세스 개선안

이는 진화적 획득방법 중 ‘나선행 개발’ 전략과 유사한데 우리도 무기체계 내 내장형 소프트웨어와 SW 중심 무기체계 등을 중심으로 비교적 단기간(6개월~1년)에 획득할 수 있는 ‘SW 획득 프로세스(가칭)’ 신설이 필요할 것이다. 그 개념은 [그림 4-9]와 같다. 이때 본 절에서 두 번째로 제안한 ROC 최저치와 최대치 설정 등 ROC 수정 활성화 방안을 함께 고려한다면 시행 가능한 제도가 될 것으로 판단된다.

둘째, ROC 핵심능력이 포함된 최저치와 최대치⁶⁶⁾를 초기 단계에 설정하는 것, 이와 더불어 ROC 최대치를 기준으로 사업 기간과 비용에 충분한 여유 범위를 지정하는 제도도입을 제안한다. 이를 적용한 개념도는 [그림 4-10]과 같다.



[그림 4-10] ROC 수정 개념 (ROC 최저·최대치 설정)

최초 설정된 ROC와 최초데이터를 활용하여 최저·최대치의 ROC를 제시한다. 이후 사업 기간 중 추가되는 데이터 및 LLM 기술발전에 따른 ROC 핵심능력을 최대치 범위 내에서 자유롭게 수정하는 것이다.

ROC 최저·최대의 테두리 범위 내에서 융통성 있게 수정하는 것으로 ROC 수정을 눈치 보거나 감사 대상이 될 걱정이 없다. 사업 기간과 비용도 여유 있기에 자연스럽게 무기체계 성능이 향상될 것이다. ROC 핵심능력 최소치는 수준 이하로 성능이 저하되는 것을 방지하고, 최대치는 소요

66) 미국의 획득체계 및 무기체계 성능 결정의 특징은 또한, 최저치와 목표치를 제시하여 개발에 융통성을 두고 있으며, 개발과정에서 전 단계보다 성능이 저하되는 것을 방지하는 장치를 두고 있다는 특징이 있다. (출처: 오원진. (2018.6.23.), 5.)

군의 무리한 요구로 인한 개발업체의 부담을 줄일 수 있는 장치가 될 것이다. 전력화 후에도 기술발전과 추가되는 데이터를 활용한 성능향상을 도모해야 한다. 이를 위해 제공된 데이터 및 모델 소유권을 연구기관에 부여, 지속적인 성능개량과 무기체계 개발확대 기회를 주는 등 제도적 장치가 필요하다.⁶⁷⁾ 물론 데이터를 타목적으로 사용하는 것에 대한 강력한 제재도 필요할 것이다. 이러한 소유권 문제 특히, 군 관련 사항은 민감하므로 장·단점 분석 등 충분한 연구가 선행되어야 한다.

셋째, ROC 수정 제도를 적용한 ‘나선형 개발’의 과감한 시도가 병행된다면 AI 기술이 접목된 무기체계 진화적 획득에 대한 교훈을 얻을 수 있다. 이를 토대로 추진사례가 없었던 ‘나선형 개발’전략 발전을 도모할 수 있을 것이다.

제 3 절 LLM 기반의 무기체계 시험평가 방안

1) 시험평가 방안

LLM이 적용된 AI 무기체계는 학습을 통한 성능향상이 시험평가 전·중·후 지속적으로 이루어지고, 기존 SW와 동작 특성이 차이 나기 때문에 기존 시험평가 방법에 의한 이분법적(합/불) 판정 적용이 제한된다. 또한 일반 무기체계는 통제 주체가 사람이라면, AI 무기체계는 1차 통제 주체가 AI이므로 전통적 무기체계와는 다른 AI 시험평가를 위한 별도의 절차가 필요하다.

따라서, AI 무기체계 신뢰성 향상을 위한 단계별 시험평가 추진을 제안한다. 총 2단계로 1단계는 데이터 기반한 AI 모델 성능평가, 2단계는 실 운용환경 시험평가로 진행한다. AI 모델 성능평가(1단계)는 주 체계와 분리된 AI 모델에 대한 요구 성능 충족 여부를 사전에 구축된 데이터를

67) 개발된 AI 모델은 모두 방위사업법과 방위사업관리규정에 따라 정부 소유로 귀속되며 개발에 참여한 기업이나 주관기관도 동일 모델을 활용한 향후 사업수행이 원칙적으로 불가능함. 미국은 연구기관이 특허권을 소유하도록 허용하면서 정부가 실시 권만을 확보할 수 있도록 하고, 개발 결과물의 소유권은 연구기관에 귀속하며, 연구 기관은 이를 활용하여 사업화를 시도할 수 있는 정책을 시행하고 있음. (출처: 한국국방기술학회, (2020.12), 174~175.)

이용하여 평가한다. 실 운용환경 시험평가(2단계)는 현장 데이터 성능평가와 체계성능 시험평가를 진행한다. AI 무기체계 단계별 시험평가를 위한 사전 조치사항은 [표 4-9]와 같다.

[표 4-9] AI 무기체계 시험평가를 위한 조치사항

주관	내용
국방부	데이터 기반 AI 모델 성능평가 및 시험평가, 운영유지기간 데이터 수집/관리를 위한 추가 인프라(HW·SW·인원·시설) 구축 필요
국방부	전담기관에 의한 데이터 기반 AI 모델 성능평가 실시 후 협의체에 의한 성능인증이 가능한 제도로 개선 필요 * 육군은 'AI 인증위원회'를 구성, AI 모델에 대한 성능인증 실시
방사청	AI 무기체계 운용·구매시험평가 전 AI 모델 성능인증 실시
시평단 (육군 시험평가단)	데이터 기반 AI 모델 성능평가를 위해 AI 무기체계 연구개발용 데이터셋과 분리된 시험평가용 데이터셋 별도 확보 추진 * 멀티모달 데이터 즉, 텍스트, 이미지, 오디오, 비디오 등 다양한 형식의 데이터 구축 필요

AI 모델은 학습 과정을 통해 구현되며 정확한 AI 모델 성능평가를 위해 학습에 사용되지 않은 별도 평가 데이터셋을 활용한 성능측정이 필요하다. 위 내용이 조치되었다는 것을 가정, 구매사업 AI 무기체계 시험평가 세부방안은 [그림 4-11]과 같다.

획득	제안서 평가, 대상장비 AI 모델 학습 및 성능인증		구매시험평가	운영유지
담당 기관	방사청(업체)	방사청 (시평단)	시평단 AI 인증 TF 시험과	분평단
수행 업무	군 작전환경 데이터 적용 학습	AI 모델 성능평가/인증	실 운용환경 시험평가	추가 성능향상 확인
데이터	Training(include Validation)	Test	현장 데이터 성능평가	체계성능 시험평가
	군 사전 구축 데이터(10)	실 환경 데이터		
	학습용(8)	평가용(2)	추가 학습용	평가용
				운영유지기간 추가 수집된 데이터

(1단계) AI 모델 성능평가

① (방사청) AI 모델 학습 및 성능평가

② (소요군 위임시 시평단) AI 모델 성능평가

(AI 무기체계 성능인증위원회) 성능인증

(2단계) 실 운용환경 시험평가

① 현장 데이터 성능평가

* 배치 - 학습 기간 부여 - 성능평가

② 체계성능 시험평가

* 시험평가 - 성능인증위원회 최종 평가

[그림 4-11] 구매사업 AI 무기체계 시험평가

1단계 AI 모델 성능평가는 제안서 평가를 통과한 업체 대상으로 구매 시험평가 전 방사청 주관으로 업체 AI 모델 학습 및 성능평가를 시행한다. 필요시, 시평단 AI 성능인증 TF⁶⁸⁾에 위임가능 하다. 소요군 위임 시 시평단 AI 성능인증 TF는 사전 구축된 시험평가용 데이터셋을 활용, 데이터에 기반한 AI 모델 성능평가를 시행한다. 성능평가 결과를 바탕으로 AI 무기체계 성능인증위원회에서 AI 모델에 대한 성능인증을 시행한다.

2단계 실 운용환경 시험평가는 현장 데이터 성능평가와 체계성능 시험평가로 구분된다. 현장 데이터 성능평가 절차는 다음과 같다. AI 모델 성능인증 완료 후 AI 무기체계를 실 운용 현장에 배치한다. AI 무기체계가 실제 운용환경에서 데이터 수집, 데이터셋 제작 및 AI 모델 고도화를 위한 학습 기간을 부여한다. AI 모델 고도화 이후 현장 데이터 활용하여 성능평가를 3회 이상 실시한다. 이때 평가의 신뢰성을 위해 실 운용환경에서 수집된 데이터는 학습과 평가용으로 각각 분할(8:2 비율) 한다.

현장 데이터 성능평가가 종료되면 체계성능 시험평가를 진행한다. 우선, AI 무기체계의 AI 모델 성능평가를 제외한 작전운용성능, 합동성 및 상호운용성, 군 운용 적합성 항목에 대한 체계성능 시험평가를 진행한다. 이후 AI 모델 성능인증, 현장 데이터 활용 성능평가, 체계성능 시험평가 결과를 종합하여 AI 무기체계 성능인증위원회에서 최종 평가를 진행한다.

연구개발 사업 AI 무기체계 시험평가 세부방안은 [그림 4-12]와 같다.

1단계 AI 모델 성능평가는 개발시험평가 단계에서 시행된다. AI 모델 성능평가 전문기관인 기품원에서 AI 모델에 대해 학습 및 성능평가, 성능인증을 시행한다. 성능평가 전문기관에 의한 성능인증 시 소요군(시평단) 사업 담당이 입회한다. 이후 2단계 실 운용환경 시험평가는 구매사업과 같은 절차로 이루어진다.

68) AI 무기체계 신뢰성 보장을 위해 데이터 기반 AI 모델 성능평가를 담당하는 조직으로 육군 시험평가단 예하 편성된 조직

획득	연구개발	개발시험평가	운용시험평가	운영유지
담당 기관	방사청(연구개발 주관기관)	기품원	시험단 AI 인증 TF 시험과	분평단
수행 업무	군 작전환경 데이터 적용 학습 Training(include Validation)	AI 모델 성능평가/인증 Test	실 운용환경 시험평가 현장 데이터 성능평가 체계성능 시험평가	추가 성능향상 확인 IOC (분평단)
데이터	연구개발용 데이터(국방 AI 센터, KIDA 등) 학습용(8)	평가용(2)	실 환경 데이터 추가 학습용 평가용	운영유지간 추가 수집된 데이터

(1단계) AI 모델 성능평가

- ① (기품원) 개발시험평가 단계에서 AI 모델 학습 및 성능평가
* 성능 인증 시 소요군(시험단) 입회

(2단계) 실 운용환경 시험평가

- ① 현장 데이터 성능평가
* 배치 - 학습 기간 부여 - 성능평가
② 체계성능 시험평가
* 시험평가 - 성능인증위원회 최종 평가

[그림 4-12] 연구개발 사업 AI 무기체계 시험평가

AI 무기체계 특성상 운용유지단계에서 고도화는 필수적이다. 운용하면서 계속 데이터를 수집하여 추가학습을 통한 고도화 후 수시 전력화평가 등 성능을 평가할 수 있는 방안이 추가로 필요하다. 또한 시험평가 및 운영유지 간 구축된 데이터셋을 지속 축적하여 기존 AI 무기체계 고도화 및 차후 AI 무기체계 관련 사업에 환류토록 방안을 추가로 마련해야 한다.

지금까지 설명한 시험평가 방안에서 핵심은 결국 1단계 AI 모델의 성능을 평가하는 것이다. 산업계에서 새로운 모델이 나올 때마다 벤치마크 데이터를 가지고 평가를 진행하며 그 결과를 기초로 홍보하고 있다. 즉, AI 모델 성능평가를 위해서는 ‘벤치마크’라는 별도의 도구가 필요하다는 것이다. 산업계에서 활용 중인 벤치마크는 [표 4-10]과 같다.

각 벤치마크는 추론 능력, 진실성, 함수생성능력, 언어이해 등 ‘무엇을 평가할 것인가’에 초점을 두고 다양한 데이터셋이 구성되어있다. 그리고 이러한 벤치마크들은 영어에 특화되었으며 단순 언어뿐만 아니라 멀티모달을 지원하는 벤치마크도 상용화되어있다.

[표 4-10] 벤치마크 데이터셋 종류⁶⁹⁾

종류	내용
Eureka	- Microsoft 제작, 최신 AI 모델 12개를 심층 분석해 기존 단순 점수 비교방식을 넘어, 각 모델의 강점과 약점을 다 각도로 파악 - 표준화된 평가 : 대규모 기초 모델에 대한 평가를 표준화 - 멀티모달 지원 : 언어 및 멀티모달 데이터를 모두 지원
MMLU	- UC Berkley 제작, 종합적인 언어 이해도 평가 - 인문학, 사회과학 및 법과 같은 전문적인 분야 포함 57개 주제로 대략 16,000개 문제로 구성 - 난이도는 초등학생에서 전문가 수준까지 넓은 범위
CPQA	- Google 제작, 대학원 수준의 문제로 구성된 벤치마크 - 물리학, 화학, 생물학 분야의 전문가들이 작성한 488개의 문제 - 매우 어려운 벤치마크 데이터셋으로 평가 (박사학위 소지자 65%, GPT-4가 39% 정확도)
HumanEval	- Open AI 제작, python 함수를 잘 생성하는지 평가 - 프로그래밍 언어, 알고리즘, 간단한 수학 등의 이해도 평가를 위해 총 164개 프로그래밍 과제로 구성
ARC Challenge	초등학교 수준(미국 기준 3학년~9학년) 과학 시험을 통해 모델의 추론 능력을 평가하는 벤치마크
TrustfulQA	답변을 생성할 때 모델의 진실성을 평가하기 위한 벤치마크

다양한 벤치마크에 대해 학계에서는 오히려 부정적인 의견이 있다. LLM을 평가 시 표준화 기준이 부족하다는 것이다. [그림 4-13]과 같이 Open AI, 구글, 엔트로픽 등 주요 개발사들이 서로 다른 벤치마크를 적용하고 있어서 AI 모델의 위험과 한계를 체계적으로 비교하기 어렵기 때문이다.⁷⁰⁾

Reported responsible AI benchmarks for popular foundation models

Source: AI Index, 2024 | Table: 2024 AI Index report

Responsible AI benchmarks	GPT-4	Llama 2	Claude 2	Gemini	Mistral 7B
TruthfulQA	✓	✓	✓		
RealToxicityPrompts	✓			✓	
ToxiGen		✓			
BOLD		✓			
BBQ			✓	✓	

[그림 4-13] 주요 AI 모델의 벤치마크 적용현황

69) (주)셀렉트스타. (2024). LLM 평가란? 셀렉트스타의 AI 성능 평가 방법. <<https://selectstar.ai/ko/blog/tech/what-is-llm-evaluation>> (검색일: 2024.12.17.) 참고 정리.

70) HAI. (2024), Chapter 5.

위 분석을 기초로 무기체계에 적용된 AI 모델 성능평가 시 다음을 고려해야 한다. 첫째, AI 모델별로 평가하고자 하는 중점을 ROC와 연계하여 선정해야 한다. ‘무엇을 평가할 것인가’를 선정해야 어떠한 벤치마크 데이터셋을 활용할지 판단할 수 있을 것이다. 둘째, 어떤 중점이든 평가할 수 있도록 사전 다양한 멀티모달 데이터를 체계적으로 수집해야 한다. 셋째, 한국어에 특화된 벤치마크 데이터셋을 보유해야 한다. 궁극적으로는 국방에서 자체 연구개발을 통해 소유하고 활용해야 하지만, 기간 및 비용을 고려했을 때 ‘Open Ko-LLM Leaderboard2’⁷¹⁾ 등과 같은 한글화 벤치마크를 구매하는 것도 고려해야 한다. 이러한 평가 도구인 벤치마크도 세계적인 기준에 부합해야 성능이 우수한 무기체계를 획득할 수 있을 것이다.

2) 시험평가 관련 법령 보완방안

위에서 제시한 시험평가 방안은 법령 및 규정 정비와 병행되어야 한다. 따라서 AI 무기체계 시험평가와 관련된 법령 및 규정을 분석하고 보완해야 할 방향을 제시하였다. AI 무기체계 시험평가 내용은 훈령 이상의 법령에서는 관련 내용이 없으므로 최근 개정(2023.9.25.)된 「국방 전력발전 업무 훈령(제2845호)」의 내용을 기준으로 분석하였다.

[표 4-11] 운용요구서 관련 조항/운용요구서 서식(보완)

조항	내용
제16조 (사전개념연구 수행)	⑨ 국과연은 제57조에 따른 운용요구서 작성을 위해 사전개념연구와 연계하여 별지 제3호서식 에 따른 운용요구서 초안(운용능력, 위협, 임무시나리오, 운용형태요약 및 임무유형(OMS/MP) 등을 포함한다.)을 작성하여 소요제기기관으로 제출한다.
제57조 (운용요구서 작성)	② 방사청은 소요제기기관에서 제출한 운용요구서 작성내용을 포함하여 운용요구서를 작성(별지 제3호서식 ‘운용요구서 완성 항목’)하고, 합참·소요제기기관 등 관련기관·부서의 의견을 수렴하여 완성한다.
별지 제3호서식 운용요구서(ORD)	☐ 소요제기기관 제출 운용요구서 항목 4.3 전투시나리오 (필요시 인공지능 분야 적용) ☐ 운용요구서 완성 항목 6.3.3 상호운용성 (필요시 인공지능 분야 적용)

71) 셀렉트스타와 upstage가 공동으로 만들고 관리하며, 기존 영어 데이터를 번역한 데이터셋과 셀렉트스타에서 만든 한국인의 사회적 가치관 및 기본 지식 등이 얼마나 일치하는지 평가하는 KorNAT 데이터셋으로 구성.

연구개발추진 간 소요제기기관에서 작성하고 방사청에서 완성하는 ‘운용요구서(ORD, Operational Requirements Document)’는 소요제기기관 의견이 반영된 요구서이다. 연구개발 방향과 시험평가 관련 기초를 제공하기 때문에 AI 무기체계 시험평가 시 중요하다. 본 훈령에서 운용요구서와 관련된 내용은 [표 4-11]과 같다. 하지만 별지 서식 ‘운용요구서’에 AI를 고려할 수 있는 항목이 없어 보완하였다.

AI 기반 전투 수행방법변화에 맞춘 전투시나리오 구현을 통해 요구능력 확인이 가능할 것이며, AI 기술에 대한 상호운용성 표준화 필요성에 기초하여 보완한 내용이다.

AI 기반 시험평가는 시험평가계획을 종합적으로 명시한 ‘시험평가기본계획서(TEMP, Test and Evaluation Master Plan)’ 작성이 가장 중요하다. 탐색 개발 이후 연구개발주관기관이 AI 기술 적용현황이 포함된(시험항목, 방법, 장소, 소요예산 등) ‘예비시험평가기본계획서’를 작성하고 체계개발종료 이후 ‘시험평가기본계획서’를 구체화한 뒤 개발시험평가(DT)와 운용시험평가(OT)를 시행해야 한다.

[표 4-12] 시험평가 관련 조항

구분	내용	비고
제63조 (시험평가기본계획서 작성)	④ <u>합참은 시험평가기본계획서 및 시험평가계획 작성지침 작성 시 별지 제4호서식에 따라 작성한다.</u>	별지 제4호서식 개선필요
제64조 (개발시험평가계획수립)	① 연구개발주관기관은 체계개발실행계획서 및 시험평가기본계획서를 근거로 필요시 계획검토회의(소요제기기관 포함)를 거쳐 <u>별지 제5호서식에 따라 개발시험평가계획(안)을 작성하여 방사청에 제출하고, 방사청은 이를 검토하여 개발시험평가 착수일 2개월 전까지 합참에 제출한다</u> ③ 개발시험평가 항목은 다음 각 호를 포함한다. ... 1. 무기체계 기능·성능시험 ... 라. 소프트웨어시험	별지 제5호서식 개선 필요 / 개발시험평가항목 AI 분야 개선 필요
제65조 (개발시험평가 결과조치)	④항의 3. 전 항목에 대한 재시험평가를 수행하는 경우에는 <u>별지 제5호서식의 개발시험평가계획서에 따라 수행한다.</u>	
제67조 (운용시험평가계획수립)	② <u>소요제기기관은 체계개발실행계획서, 시험평가기본계획서 및 개발시험평가계획서(또는 계획(안))를 근거로 별지 제7호서식에 따라 운용시험평가계획(안)(제1항의 상호운용성시험평가 개략계획(안)을 포함한다)을 작성하여 운용시험평가 착수일 2개월 전까지 합참에 제출한다.</u>	별지 제7호서식 개선필요

훈령에서 시험평가 관련조항은 [표 4-12]와 같으나, 관련 서식에 AI를 고려할 수 있도록 상하 연계한 보완이 필요하다. 보완 내용은 [표 4-13]와 같다.

[표 4-13] 시험평가 관련 내용 및 서식(보완)

구분	내용
별지 제4호서식 시험평가기본계획서	3. 시험평가계획 개요 아. 기타 (필요시 인공지능 분야 적용) 4. 개발시험평가 계획 바. 기타 (필요시 인공지능 분야 적용) 5. 운용시험평가 계획 바. 기타 (필요시 인공지능 분야 적용) 6. 통합시험 계획 라. 기타 (필요시 인공지능 분야 적용)
제64조 (개발시험평가계획 수립)	③ 개발시험평가 항목은 다음 각 호를 포함한다. 다만, 무기체계의 특성, 시험장 및 시험장비, 환경적 위험에 따른 안전 등을 고려하여 이를 조정할 수 있다. 1. 무기체계 기능·성능시험 가. 주요 작전운용성능 시험 나. 기술적·부수적성능 시험 다. 설계검토를 통하여 확정된 기능 및 성능시험 라. 소프트웨어시험 (필요시 인공지능 분야 포함) 마. 환경시험 바. 전자파 적합시험 등
별지 제5호서식 개발시험평가계획서	1. 개요 사. 기타 (필요시 인공지능 분야 적용) 3. 시험평가 기간, 장소 및 방법 라. 기타 (필요시 인공지능 분야 적용)
별지 제7호서식 운용시험평가계획서	4. 시험평가 항목 및 기준 라. 기타 (필요시 인공지능 분야 적용)

시험평가 관련 서식에 AI 분야 적용에 대해 명시함으로써 계획수립 시 반드시 고려될 수 있다. 상하 연계성을 유지하기 위하여 ‘시험평가기본계획서’부터 ‘운용시험평가계획서’까지 동일내용으로 보완한 사항이다. AI 무기체계 기능 및 성능은 결국 소프트웨어에 포함되어 있기에 개발시험평가 항목 중 소프트웨어시험에서 고려될 수 있도록 내용을 보완하였다.

마지막으로 ‘성능 유지관리’ 측면이다. 학습을 주로 하는 AI 기반 무기체계 시험평가는 학습이 자동화되고 폐기될 때까지 해야 하는 연속적인

작업이다. 지속적인 유지관리의 제도화가 필요하다. 현재 무기체계개발 이후 시행하는 성능개량사업(국방정보시스템은 약 7년, 일반 무기체계는 약 10년) 방식은 AI 무기체계에 문제점이 발생할 수 있다. 정보시스템 진부화에 나타나는 문제보다 더욱 심각할 수 있다. 장비(하드웨어) 위주의 유지관리 제도를 보완할 수 있도록 AI SW에 대한 유지관리 대상(국내개발, 상용, 국외도입)과 관리범주를 지정했으며 [표 4-14]와 같다.

[표 4-14] AI 유지관리 대상과 관리범주

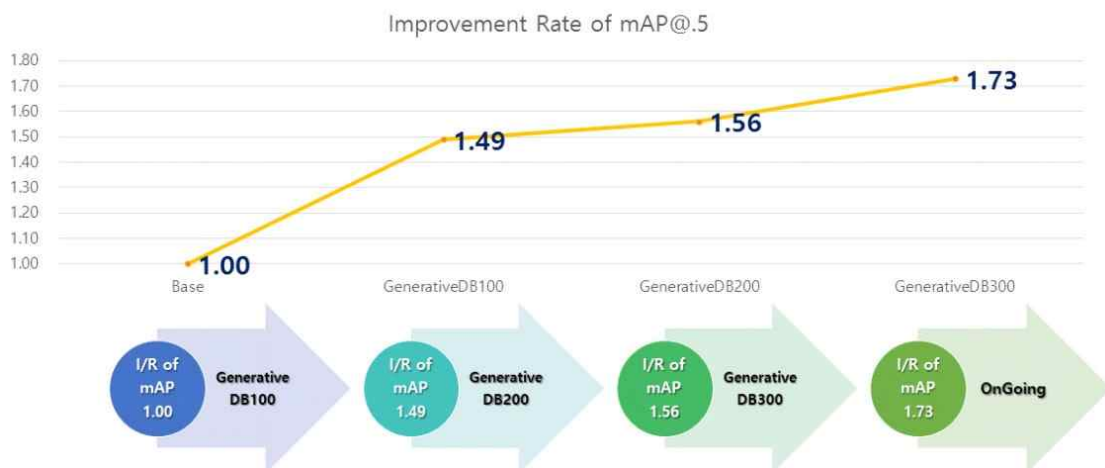
대상	관리범주
국내개발 인공지능 SW	① 하드웨어나 OS, 네트워크 등에 대한 성능, 기능개선 및 기술적 발전에 대응하기 위한 변경 (완전유지관리) ② 군의 작전개념 변경에 따른 기능변경, 추가, 보완, 폐기, 사용방법의 개선, 학습데이터 변경 등 (적응유지관리) ③ 프로그램의 비정상적 기능 수정 및 보완 (수리유지관리) ④ 소프트웨어에 대한 오류탐지 및 품질관리 (예방유지관리)
상용 인공지능 SW	① 제품지원, ② 기술지원, ③ 사용자 지원
국외도입 인공지능 SW	국외도입 소프트웨어는 버전과 빌드 정보 관리

무기체계는 성능을 개선하려면 개발 이후 성능개량사업까지 대체로 10년 이상 기간이 필요하다. 또한 빠르게 진화하는 AI 무기체계 개발 특성상 완벽하게 학습하여 성능과 보안성이 보장되기 어려운 특성이 있다. 따라서 제시한 유지관리 대상과 관리범주를 기초로 AI 모델을 학습시키고 업데이트 가능한 AI 무기체계 유지관리체도가 장기적으로 필요할 것이다.

LLM 등 첨단기술을 적용한 무기체계 연구개발을 성공시키기 위해서는 미래 전에 필요한 AI 무기체계 특성 및 전장 영역확장, 전투 수행방법발전 등에 대비해야 한다. 관련 제도 및 법령이 우선 반영되어야 AI 무기체계에 대한 시험평가역량을 확보할 수 있을 것이다.

제 4 절 LLM 기반의 무기체계 품질관리 방안

군 보안 문제로 충분하지 않은 데이터의 양, 원하는 상황의 이미지 부족 등 문제점이 발생하게 되는데 이를 ‘데이터 임밸러싱’이라고 한다.⁷²⁾ 민간방산 업체와 연구기관에서 문제점 해결 방안으로 ‘이미지 생성 모델을 이용한 데이터 증강’⁷³⁾을 [그림 4-14] 실험결과를 근거로 대안으로 제시하고 있다.



[그림 4-14] 생성형 영상 DB 추가, 기존 DB 대비 개선 효과⁷⁴⁾

하지만 해당 논문에서 단점을 제시했듯 근본적인 대책이 될 수 없다. 첫째, 생성된 영상들 가운데 의도한 바와 다르게 생성되거나, 육안으로 보기에 부자연스러운 영상이 역시 존재했다. 실제 환경에서는 존재하지 않을 법한 객체 간 배치 정보가 그것이다. 둘째, 적용한 최신 객체 탐지 기술이 지도학습 방식이었기 때문에 생성된 영상으로부터 객체 정보를 라벨

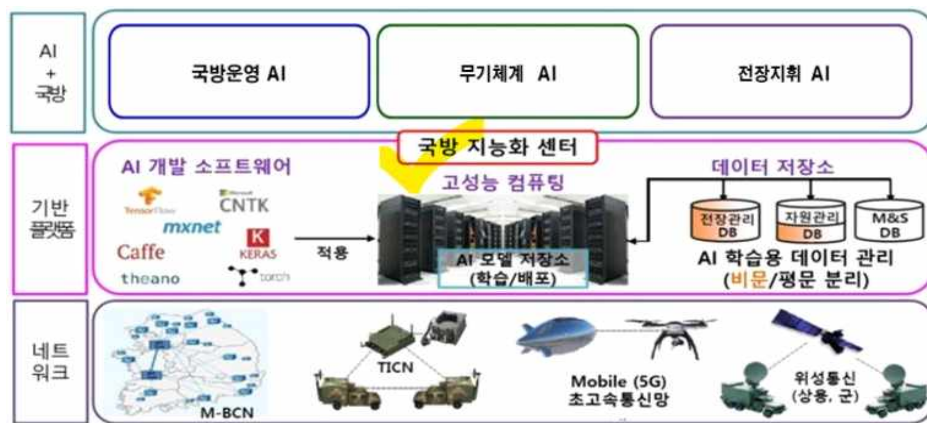
72) Wei Li and others. (2022). EID-GAN : Generative Adversarial Nets for Extremely Imbalanced Data Augmentation. 『IEEE Transactions on Industrial Information』, 19(3)

73) 국방과학기술발전세미나(2023.11.21.) 발표 의제 중 “국방 지휘통제 의사결정 AI 연구소 개” 자료 참고

74) 성능에 대한 개선 정도는 AI 기반 생성한 영상을 추가하지 않은 기존 DB로 학습한 경우를 1.00로 환산했을 때 생성 영상을 추가한 DB로 학습한 경우를 마찬가지로 환산하여 나타낸 개선율을 활용함. 그림과 같이 100장의 생성 영상을 학습데이터에 추가하면 개선율 1.49, 200장을 추가할 경우 1.56, 그리고 300개 추가할 경우 1.73의 성능 향상을 확인할 수 있다.

링하는 작업을 직접 수행해야 했다.⁷⁵⁾ 즉, 이미지 및 영상 데이터에 국한되며, 군 데이터를 직접 수집하는 것에 비해 품질 보증이 어렵고 별도 데이터 생성과정과 라벨링 등 불필요한 노력과 추가예산이 소요된다.

이런 근본적인 문제를 해결하기 위해 데이터 수집·활용을 포함, AI 개발 및 운영에 필요한 소프트웨어, 필수 알고리즘과 데이터, 컴퓨팅 자원 등으로 구성하는 국방 ‘AI 플랫폼’⁷⁶⁾ 구축을 추진하고 있다. ‘국방 인공지능(AI) 추진 전략 2.0’에 ‘국방 지능형 플랫폼 사업’을 담고 있는데 [그림 4-15]와 같다.



* 「국방 AI 표준체계」를 적용한 국방 지능형 플랫폼 구현은 국방부 전체의 데이터 통합 관리 및 AI 적용을 위해, **클라우드 기반 인프라**, 데이터 거버넌스 포털, 인공지능 분석 서비스를 제공하는 국방 지능형 플랫폼 구축 추진

[그림 4-15] 국방 지능형 플랫폼 사업 개요

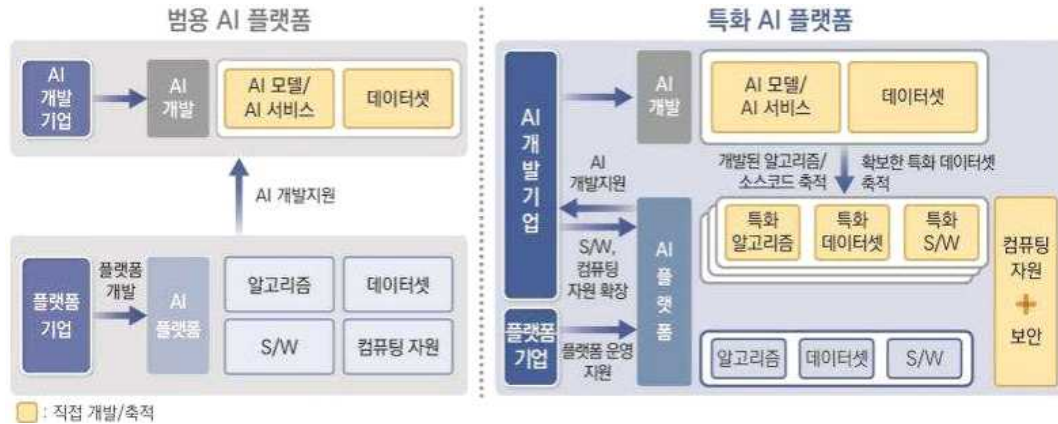
기존 C/S(Client & Server) 환경에서 클라우드 컴퓨팅 서비스(Cloud Computing Service) 환경으로 대전환될 것을 예상⁷⁷⁾, 클라우드 방식의 플랫폼 구축을 적용하고 있다.⁷⁸⁾ ‘AI 플랫폼’은 [그림 4-16]과 같이 ‘범용 AI 플랫폼’과 ‘특화 AI 플랫폼’으로 구분할 수 있다.

75) 김대환, 고은진. (2023.7.31.), 261. 33.

76) 이재국, 이일로. (2022.7.4.), 2. AI 플랫폼 관련 설명은 본 자료 참고

77) , 한영식, 윤종택. (2023.11). 저궤도 위성(LEO Satellite) 기반 차세대 군 통신망 기술동향 및 연구방향. 『국방과 기술』, 537, 112.

78) 이재국, 이일로. (2022.7.4.), 8.에서도 미국방부(DoD)의 보안 클라우드 기반 AI 플랫폼 JCF(Joint Common Foundation) 구축사례 등을 고려 우리 국방 분야도 자체적인 보안 AI 플랫폼을 구축해야 한다고 주장하고 있음.



[그림 4-16] 범용 AI 플랫폼과 특화 AI 플랫폼 특징 비교

‘범용 AI 플랫폼’은 다양한 사업영역에 범용적으로 활용하도록 플랫폼 기업에서 서비스하는 플랫폼이다. AI 플랫폼으로부터 개발에 필요한 요소들을 지원받아 AI 모델/서비스를 개발·운영하는 것에 중점 둔 것이다. 개발자가 별도 물리적 환경구축이 필요 없도록 ‘퍼블릭 클라우드’⁷⁹⁾ 형태의 컴퓨팅 자원을 활용한다. 반면 ‘특화 AI 플랫폼’은 특정 사업영역에 최적화되도록 자체 구축하는 플랫폼이다. AI 개발·운영을 통해 획득한 알고리즘·데이터 등을 축적하여 AI 플랫폼 성능을 지속 개선한다. 해당 사업영역 특성이나 보안 요구사항 등을 고려하여 ‘프라이빗 클라우드’⁸⁰⁾ 컴퓨팅 자원을 활용한다. 국방은 특수한 환경으로 ‘프라이빗 클라우드’ 컴퓨팅을 활용한 ‘특화 AI 플랫폼’을 적용해야 할 것으로 판단된다.

국방 지능형 플랫폼 사업과 병행한 국방 데이터 품질관리 분야를 통해 새로운 가치를 창출하기 위한 전략 마련과 데이터 공유 기반환경조성이 필요한 시점이다. 단편적으로 기술적인 측면보다 품질관리 업무 중심의 거버넌스 정립방안이 필요하기에 국방 및 국방기술품질원 데이터구축 시 다음과 같은 방안을 제안한다.

첫째, 기품원 3대 업무 분야와 연계한 품질관리 데이터구축 중점을 설

79) 클라우드 리소스(H/W, S/W, 기타 지원 인프라 등)를 클라우드 서비스 업체를 통해 인터넷 환경으로 제공받는 형태로, 리소스를 클라우드 업체가 소유하고 관리함. (출처: 이재국, 이일로. (2022.7.4.), 3.)

80) 클라우드 리소스를 단일 조직에서 독점적으로 사용하는 형태로, H/W와 S/W를 조직 전용으로 사용하며 네트워크 또한 조직 구성원만 접근 가능함. (출처: 이재국, 이일로. (2022.7.4.), 3.)

정해야 한다. 연구개발 단계 품질관리는 무기체계별 기술 분야 데이터를 구축, 양산단계 품질관리는 신뢰성 평가 표준화, 규격화 관련 데이터를 구축하고, 운영유지단계 품질관리는 무기체계 운용자별 장비가동률, 운용성 관련 데이터를 구축해야 한다.

둘째, 소요군별, 무기체계별 품질관리 데이터 자산 가시화로 통합 및 연계성을 강화해야 한다. 데이터 활용성 증진을 위해 품질관리 데이터 목록을 작성하여 공유하고 품질관리 메타데이터 관리시스템(MDR)을 구축하여 데이터관리자, 시스템개발자, 업무담당자들 활용 편리성을 위해 검색기능을 강화하고 데이터 통제 및 조정 활동을 수행해야 한다. 또한 비밀 및 민감 데이터 활용 등급제를 고려 데이터 활용 시 보안 요구사항을 관리해야 한다.

셋째, 품질관리 시스템에서 운용되는 원천데이터 표준화와 데이터 수준을 고도화해야 한다. 국방환경 및 기품원 환경에 적합한 데이터 품질관리 프로세스를 정립하고 제도화해야 하며, 품질관리 시스템 표준준수실태 및 보안상태를 점검하여 원천데이터 수준 향상이 필요하다.

넷째, 품질관리 관련 기관의 기반환경조성에 따른 실질적인 활용능력을 제고시켜야 한다. 무기체계 관련 개발 및 데이터 분석, 사용자, 관리자 간 유기적인 협력을 유도할 필요가 있다.

다섯째, 체계적인 품질관리 데이터 구축(수집/분석/평가 등)을 위한 ‘빅데이터 관리조직’을 편성해야 한다. 중장기계획에 의거 소규모 데이터관리 시범조직을 운영 후 성과분석을 통해 단계별로 확대하여 최종 ‘품질관리 빅데이터 센터’를 편성해야 한다. 무기체계 품질관리 업무수행을 위한 영역 및 역할을 정립해야 하는데 정책 및 거버넌스는 국방부, 데이터 분석 및 연동/제공은 관련 기관 협업부서가, 품질관리 시스템관리는 기품원이 수행할 수 있을 것이다. 또한 데이터 정책 및 실무는 가능하면 장기보직이 가능한 군무원 위주로 보직하여 효율성을 극대화해야 한다.

여섯째, AI가 적용된 무기체계에 대한 품질관리에 대한 가이드를 아래와 같이 정립해야 한다.

[표 4-15] 무기체계 품질관리 가이드(평가항목 및 지표)

모델평가		
1. 알고리즘 적정성	2. 성능의 유효성	3. 모델의 신뢰성
1-1. 표적탐지 주요 AI 모델 1-2. 표적분할 주요 AI 모델 1-3. 표적추적 주요 AI 모델 1-4. 대표적인 모델평가용 데이터셋/측정 지표별 최근 모델 비교	2-1. 성능지표	3-1. 적대적 공격에 대한 강인성 3-2. 새로운 환경에 대한 적응성 3-3. 결과도출 근거에 대한 설명 가능성
데이터평가		
1. 기준 적합성	2. 기술 적합성	3. 통계적 다양성
1-1. 다양성: 포괄성, 변동성 1-2. 신뢰성: 데이터 준비, 수집 1-3. 충분성: 데이터 규모평가 1-4. 균일성: 클래스 간 비율 1-5. 사실성: 인위적 생성데이터 1-6. 공정성: 편향성 평가	2-1. 파일 포맷 2-2. 해상도 2-3. 프레임 레이트 2-4. 픽셀당 비트 수	3-1. 클래스 분포도 * 적/아군 장비 데이터 및 라벨링 분포 3-2. 인스턴스 분포도 * 클래스별 보유 데이터 수의 분포

모델평가는 총 알고리즘 적정성 등 3개 항목 8개 지표, 데이터평가는 기준 적합성 등 3개 항목 12개 지표를 제시하였으며 이를 기초로 무기체계 품질관리를 위한 별도의 가이드를 명문화해야 한다.



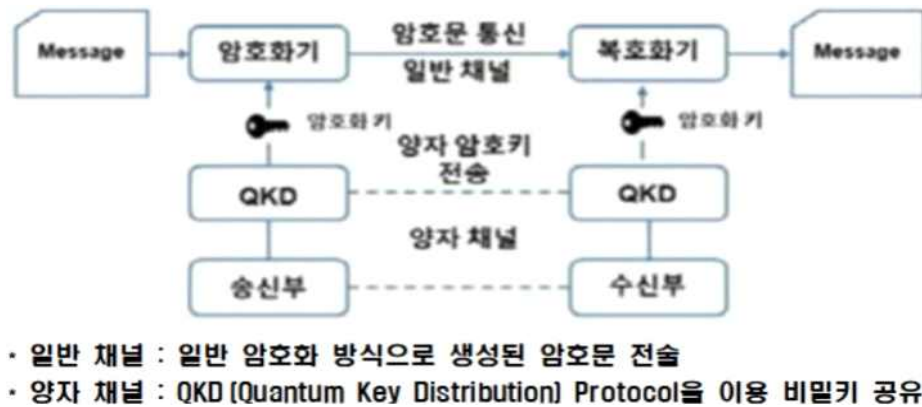
[그림 4-17] 양자기술 분류⁸¹⁾

마지막으로 클라우드 보안 문제는 ‘양자기술’과 결합하여 해결하는 방안을 검토해야 한다. 양자기술은 [그림 4-17]과 같이 양자통신, 양자컴퓨

81) 김종영. (2023.5). 미래 전장의 게임체인저, 양자기술의 국방적용 방안 고찰. 『국방과 기술』, 531, 48. 재인용

터, 양자 센서 등의 응용 분야로 구분할 수 있다. 이중 ‘양자통신’은 양자 역학적 특성을 이용하여 두 개소 또는 여러 개소 간에 정보를 주고받는 것을 말하는데 암호통신을 위한 암호키 분배에 양자기술을 적용하여 ‘초 신뢰통신’을 제공한다.

KT 융합기술원에서는 2018년부터 양자 암호키를 레이저빔 형태로 전송하는 무선 양자키 분배 기술을 개발 중이며, 최근 지상 2Km 구간에서 양자 신호전송에 성공하였다. 이를 계기로 2024년에는 지상 10Km까지 양자암호 키 전송범위를 늘리는 등 양자 신호전송기술을 개발할 예정이다.⁸²⁾



[그림 4-18] 양자 암호화 개념도

‘양자기술’은 AI와 함께 ‘10대 국방전략기술’에 포함된 분야로 빠른 기술성숙도를 달성할 것으로 판단된다. 이를 클라우드 기반 ‘AI 플랫폼’에 적용한다면 높은 수준의 보안을 유지할 수 있을 것이며, 이러한 기술 융합은 AI 분야에 추가적인 시너지효과를 발휘할 것이다.

82) 연재성, 한영식, 윤종택. (2023.11), 118. 양자 암호화 관련 설명은 본 자료 참고

제 5 장 결 론

제 1 절 연구내용 요약

[표 5-1] 연구내용 요약 (기대효과)

기술 특징	LLM의 무기체계 적용 시 고려사항	적용 방안
전문적인 기술영역	LLM 핵심기술 개발	• 「국방기술기획서」 AI 중점기술 분야와 연계한 LLM 기술개발, 국방에 특화된 한국어 LLM 우선 개발 ⇒ 체계적인 핵심기술 개발, 무기체계에 LLM 적용 확대
	인재양성 방안 필요	• 국방부 예산 활용, AI 예산확대 도모 • (병과)학교기관에 AI 교육장 우선 구축 • 전문교육 자격요건 설정, 교육 기간 단축 • 승진자 교육, 미참여 부대 의무화 시행 • AI 실무교육 현장확인 시스템구축 • 개인 기록변경, 인사관리 주기 개선 ⇒ ① 군 주도로 국방 특성 고려한 교육이 가능하고 ② LLM 기술에 대한 홍보 효과 극대화 및 공감을 촉진 하며, ③ 전문교육에 대한 부담을 해소, 과정별 연계 있는 교육으로 우수 인원 확보가 가능하고, ④ 효율적인 인재관리로 유출 방지 가능
기술발전 속도 빠름	AI 무기체계의 신속한 획득 프로세스 필요	• SW 획득 프로세스 신설 ⇒ AI 무기체계 신속획득보장 • ROC 최저·최대치 설정 ⇒ ROC 수정의 융통성 확보 • ROC 수정 제도가 적용된 나선형 개발 전략의 과감한 시도 ⇒ 나선형 개발의 발전 도모
데이터 학습 통해 성능향상	AI 무기체계 시험평가 방안 필요	• AI 무기체계 ‘단계별 시험평가 방안’ 적용 ⇒ AI 모델 성능평가로 신뢰성 확보, 다양한 운용환경 시험평가 및 운용유지단계 고도화 가능 • 시험평가 관련 서식 개선 ⇒ 계획부터 AI 고려 가능 • AI 기반 무기체계의 유지관리 대상 및 관리범주 마련, 제도화 ⇒ 기술 진부화 방지
다양한 품질 좋은 데이터 필요	AI 무기체계 품질관리를 위한 기반환경조성 필요	• 기품원 3대 업무 연계한 품질관리 데이터구축 중점설정 • 품질관리 데이터 가시화 • 품질관리 프로세스 정립, 원천데이터 표준화 • 유관 기관의 상호 유기적인 협력 유도 • 빅데이터 관리조직 편성 • AI 무기체계 품질관리 가이드 마련 • 클라우드에 양자 기술(암호화) 적용 ⇒ ① 체계적인 품질관리 데이터구축이 가능하고 업무 효율을 극대화한다. ② 조직의 통합 및 연계 강화, ③ 원천데이터 수준 고도화 및 데이터의 실질적 활용 제고, ③ 품질관리 신뢰성 확보, ④ 데이터 활용 간 초 신뢰 보안제공

기술발전은 인간이 보다, 나은 삶을 영위하기 위한 노력의 산물이다. 그 노력의 산물 중 하나가 인공지능인데 우리 일상생활에 깊숙이 침투해 있다. 세계적으로 AI 기술을 적용하기 위해 노력하고, 선도하기 위한 움직임이 활발하다. 특히, 세계가 경악할 만큼 심각한 인구감소문제를 가지고 있는 우리에게 AI 전환은 필수이다. 따라서 AI 중 활용 가능성이 무한한 LLM을 이론적으로 고찰하여 LLM 기술 특징을 도출하고 활용현황을 알아보았다. 이후 3장에서 무기체계 적용사례와 기술 특징에 기초한 제한사항을 분석했다. 분석된 내용을 토대로 4장에선 대규모 언어모델(LLM)의 무기체계 적용 시 고려사항을 중심으로 적용방안을 제시했다. 그 내용을 요약하면 [표 5-1]과 같다.

LLM이 적용된 무기체계를 전력화하기 위해 제시한 네 가지 방안은 다음과 같은 효과가 있다. 첫째, 전문적인 기술영역인 만큼 효과적인 AI 인재양성을 가능하게 할 것이며, 이를 토대로 LLM 핵심기술 개발과 무기체계 적용이 가속화될 것이다. 둘째, LLM 기술발전 속도가 빠르기에 무기체계를 신속히 획득할 수 있는 발판을 마련할 것이다. 셋째, AI 무기체계 시험평가 방안으로 LLM이 적용된 무기체계에 대한 성능평가가 가능하게 될 것이다. 따라서 소요군은 성능이 검증된 무기체계를 활용할 수 있다. 넷째, LLM 무기체계 품질은 곧, 데이터품질과 같다. 품질관리를 위한 데이터 수집, 활용, 품질관리 등의 기반환경조성으로 LLM이 적용된 무기체계 품질관리를 가능하게 할 것이다.

제 2 절 추가 연구사항

연구한 분야는 LLM 핵심기술 및 인재양성, 무기체계 획득, 무기체계 시험평가, 무기체계 품질관리 네 가지다.

LLM 핵심기술 및 인재양성 분야는 국방에 특화된 한국어 LLM 개발을 위한 체계적인 접근의 연구가 필요하다. 예를 들어 LLM이 학습할 데이터는 텍스트, 오디오, 비디오 등 다양하다. 텍스트에서도 교범 내용, 기능별 보고서, 사후검토 내용으로 세분화시킬 수 있을 것이다. 또한 양성한

인재 유출 방지를 위한 인사 관리제도 개선은 필수적이다. 따라서 세부적인 추가 연구가 필요하다.

무기체계 획득, 시험평가, 품질관리 분야는 AI 무기체계를 좀 더 신속하고 정확하게 획득하기 위한 여러 방안이 논의되고 있다. 현재 세계적으로 분쟁이 지속되는 것을 고려했을 때 전시 LLM 등 최신기술이 적용된 무기체계 획득, 시험평가, 품질관리 방안에 관한 추가연구가 필요하다.

이와 더불어 ‘블랙박스’와도 같은 인공지능 모델에 신뢰성을 더할 수 있는 ‘설명 가능한 인공지능’⁸³⁾, 주요 위협국들이 손쉽게 AI를 이용하여 비대칭전을 수행할 경우를 대비한 Anti-AI 기술 역시도 군사적 적용에 중요한 부분으로 향후 지속적인 연구가 필요하다.⁸⁴⁾

제 3 절 결 언

첨단기술은 인간이 진화하기 위한 수단으로 사용해 왔다. 1~3차 산업혁명을 지나 4차 산업혁명과 지능정보 사회가 도래했는데 그 중심에 AI가 있다.

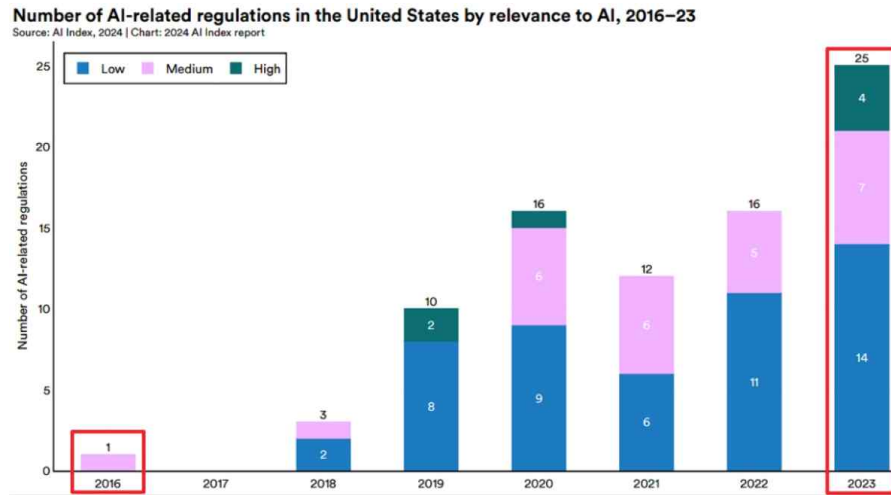
최근 영국에서 열린 ‘인공지능(AI) 안전 정상회의’에서 “AI의 파국적 위험을 막도록 협력하자”며 세계 첫 공동선언을 발표했다. 미국과 치열한 기술 경쟁을 벌이는 중국까지 참여해 눈길을 끌었다. 하지만 협력 선언 이면에 AI 산업규제를 주도하려는 국가 간 기 싸움이 치열했다. 미국과 영국을 중심으로 규제기관설립 주도권 다툼이 시작됐고, AI의 규제 범위와 강도를 두고 주요국별로 이견이 가시화됐다.⁸⁵⁾ 이는 결국 주요국들이 자국 AI 기업에 유리한 방향으로 규제를 주도하고 타국 AI 산업에 진입장벽

83) 설명 가능한 AI(eXplainable AI, XAI): 인공지능이 판단한 결과에 대한 이유를 사람이 이해할 수 있는 방식으로 제시하는 것을 말함. 특정한 판단에 대해 알고리즘의 설계자조차도 그 이유를 설명할 수 없는 ‘블랙박스’ 인공지능과 대비되는 개념이며, 불확실성을 해소하여 인공지능에 대한 신뢰성을 높이는 방법임. DARPA는 약 800억 원의 예산을 투입하여 ‘유리박스’를 목표로 한 프로젝트를 진행하고 있음. (WIKIPEDIA, 검색일: 2024.2.17.)

84) 최근하, 오재진, 김영길. (2020), 51.

85) 네이버 뉴스. (2023.11.3.). ‘AI 파국적 위험 막게 협력’...美·中·英 등 28개국 첫 공동선언. <https://n.news.naver.com/article/020/0003529030?type=editn&cds=news_edit> (검색일: 2023.11.4.)

을 쌓아 AI 패권을 공고히 하려는 의도로 분석할 수 있다.



[그림 5-1] 미국 AI 관련 규제 수의 변화⁸⁶⁾

실제로 [그림 5-1]과 같이 지난 5년간 미국의 AI 관련 규제 수가 16년 1건에서 23년 25건으로 증가하였다. 국방 무기체계 분야 인공지능 기술 또한 마찬가지다. 선진국이 기술우위를 선점하고 국제적 인공지능 윤리기구·가이드 라인 등을 통해 경쟁국과 위협국들의 인공지능 기술을 통제할 가능성이 있다. 따라서 AI 중 최신 트렌드 기술인 LLM을 국방 무기체계 분야에 신속히 적용해야 한다.

지금까지 인류가 기술발전을 스스로 가로막은 사례는 없었다. 하지만 인공지능 기술로 인한 일자리 소실, 개인 인권침해, 소유권 등 재산권 다툼, 인류 지배력 상실 등 많은 걱정과 우려로 AI를 두려워하는 현상이 나타나고 있다. 하지만 역사적으로 세계적인 움직임을 따라가거나 선도하지 못하면 도태되기 때문에 국방의 AI 전환은 우리 군의 사명임이 분명하다.

AI 중 LLM을 이해하고 무기체계에 적용하기 위한 방안을 제시한 본 연구는 매우 의미 있다고 평가하고 싶다. 특히, LLM이 도입될 각종 무기체계의 원활한 사용을 뒷받침해줄 ‘시험평가와 품질관리’ 관련 분석은 기존연구에서 다루지 않은 사항이기에 더욱 의미 있다. 앞으로 본 연구를 통해 LLM 이해를 도와 국방 도입이 활발해지길 바라고, 본 고를 바탕으로 활발한 후속연구가 이어지길 기대하면서 마침표를 찍는다.

86) HAI. (2024), Chapter 9.

참 고 문 헌

1. 국내문헌

- 강명철. (2023.7). 우크라이나-러시아 전쟁 간 포병 운용 분석. 『전투발전』
- 교육사령부. (2022.7.12.). 러시아-우크라이나 전쟁 전훈분석 및 전투발전 방향 토의
- 교육사령부. (2023.11.21.). 『국방과학기술 발전 세미나』
- 국방부. (2023.2.28.). 『2023_national_defense_brochure01』
- 국방부. (2023.9.25.). 『전력발전업무훈령 제2845호』
- 국방일보. (2022.5.30.). 도네츠 강 건너던 러 대대급 병력 전멸 ‘일등공신’
- 국방전산정보원 빅데이터팀. (2019.5.1.). 『인공지능(AI), 머신러닝, 딥러닝』
- 국방기술진흥연구소. (2022.1.16.). 『미래국방 2030 기술전략(요약본)』
- 김용훈. (2023.8). 미래 한반도 해역 대잠전 시나리오 기반 해양 유·무인 복합 체계 발전방향. 『국방과 기술』
- 김대환, 고은진. (2023.7.31.). 생성형 AI 기술을 활용한 국방 무기체계 개발. 『국방과학기술플러스』
- 김종영. (2023.5). 미래 전장의 게임체인저, 양자기술의 국방적용 방안 고찰. 『국방과 기술』
- 김홍빈. (2021). 한국군 군사력 건설에서 진화적 ROC 적용방안 연구. 『한국 방위산업학회지』
- 네이버 뉴스. (2024.1.1.). 인공지능·인류 공존이 시작됐다. <https://n.new.naver.com/article/030/0003169877?type=editn&cds=new_edit> (검색일: 2024.1.1.)
- 네이버 뉴스. (2023.11.9.). AI 입은 갤럭시S24, 통화하면서 실시간 통역해준다. <https://n.news.naver.com/article/092/0002310782?type=editn&cds=news_edit> (검색일: 2023.11.9.)
- 네이버 뉴스. (2023.12.10.). 한국이 사라진다...전 세계 걱정거리 된 韓 저출산. <<https://n.news.naver.com/article/448/0000439617>>

?type=editn&cds=news_edit>(검색일: 2023.12.10.)

네이버 뉴스. (2023.12.31.). CNN 한국군, 새로운 적은 ‘저출산’...병력 유지 어려워. <https://n.news.naver.com/article/018/0005646681?type=editn&cds=news_edit>(검색일: 2023.12.31.)

네이버 뉴스. (2023.12.5.). 챗GPT에 ‘같은 단어 반복하라’ 했더니.... <https://n.news.naver.com/article/092/0002313854?type=editn&cds=news_edit> (검색일: 2024.2.2.)

네이버 뉴스. (2023.12.6.). ‘괴물 AI’ 막으려면 편향성 극복 규제 법제화해야 <https://n.news.naver.com/article/310/0000112564?type=editn&cds=news_edit> (검색일: 2023.12.8.)

네이버 뉴스. (2023.11.3.). ‘AI 파국적 위험 막게 협력’...美·中·英 등 28개국 첫 공동선언. <https://n.news.naver.com/article/020/0003529030?type=editn&cds=news_edit>(검색일: 2023.11.4.)

대한민국육군발전협회. (2023.11). 『미래 육군 상비병력 절감방안 연구』 방위사업청, 국방기술진흥연구소. (2023). 『‘23~’37 국방기술기획서(일반본)』 보도자료. (2023.6). ‘신속획득(Fast Track)’제도, 금년 8월부터 시행. 『국방과 기술』 보안뉴스. (2024.2.13.). 마이크로소프트 365 등 기업 클라우드 앱 노리는 캠페인 주의보 <https://m.voannews.com/html/detail.html?idx=126631&tab_type=1> (검색일: 2024.2.15.)

방위사업청. (2023.12.14.). 『신속시범사업 업무관리 지침 제884호』

서울경제. (2023.10.24.). 중국폰 들고 “삼성 타도” 외친 그 남자...알고보니 전직 ‘삼성맨’. <<https://m.sedaily.com/NewsView/29W32079W7>> (검색일: 2024.2.13.)

연재성, 한영식, 윤종택. (2023.11). 저궤도 위성(LEO Satellite) 기반 차세대 군통신망 기술동향 및 연구방향. 『국방과 기술』

오원진. (2024.1). 무기체계 신속획득제도(Fast-Track) 정착을 위한 제언. 『국방과 기술』

오원진, 심상렬. (2018.6.23.). 무기체계 작전운용성능(ROC)의 수정 원인 및 최소화 방안 연구. 『한국방위산업학회지』

육군본부. (2022.12.31.). 『기준 0-3 군사용어』

육군본부. (2023.3.8.). 『23년도 육군 인공지능(AI) 역량 강화 추진계획』

이정우, 김영인. (2023.11). 미래 AI 기반 디지털 전쟁에 대비하는 합동 AI Master Plan 발전방향. 『국방과 기술』

이재국, 이일로. (2022.7.4.). 국방 AI 플랫폼 개발을 위한 제언. 『KRIT Issue Paper』

장사정 정밀화력체계 과학기술그룹. (2024.7.5). 팔란티어 기업 및 군사용 인공지능 플랫폼 발표. 『화력전투발전 군사과학기술개발 동향』

조선일보. (2024.2.15.). ‘데이터 라벨링’의 진군 <https://www.chosun.com/economy/tech_it/2024/02/15/QO4GYZSTSFDPAW2JZRDJ6VWI4> (검색일: 2024.2.15.)

지티티코리아. (2024.7.7.). AI와 LLM로 강력해지는 국방력. <<http://www.gttkorea.com/news/articleView.html?idxno=11917>> (검색일: 2024.9.21.)

최성빈. (2012.11). 미국의 국방획득절차 개선 방향 소개 및 시사점. 『주간국방논단』

최근하, 오재진, 김영길. (2020). 미 국방부 및 육군의 인공지능(AI) 전략이 한국군에 주는 시사점. 『한국방위산업학회지』

한국구방기술학회. (2020.12). 『국방 인공지능 발전계획 수립 연구』

한국국방기술학회. (2023.11.27.). 『전 장병 SW·AI 생애주기 및 소양교육』

한국지능정보사회진흥원. (2023). 『2023년 인공지능 학습용 데이터 라벨링 전문교육(프로젝트 관리) 강의자료』

한국전략문제연구소. (2022.9.15.). 『민군 겸용 데이터 플랫폼 구축』

IT WORLD뉴스. (2024.8.26.). 생성형 AI의 한계…점점 명칭해지는 인공지능의 미래. <<https://www.itworld.co.kr/news/348359>> (검색일: 2024.10.27.)

KIDA. (2022.6). 『(인공)지능 시대 한국의 국방력 건설 방향』

KOSSA. (2023.9.8.). 『「전 장병 AI·SW 생애주기 및 소양교육」 신청안내』

SW정책연구소(SPRI). (2019). 『국방 무기체계 SW관리 조직 및 법제도 현황』

분석 연구』

(주)셀렉트스타. (2024). LLM 평가란? 셀렉트스타의 AI 성능 평가 방법.
<<https://selectstar.ai/ko/blog/tech/what-is-llm-evaluation>>

2. 국외문헌

HAI(Stanford Institute for Human-Centered Artificial Intelligence). (2024).
AI Index Report 2024. <<http://aiindex.stanford.edu/report>>

<http://paperswithcode.com/sota>

MIT Technology Review (2023.1.9.). AI that makes images: 10 Breakthrough
Technologies 2023. <<https://www.technologyreview.com/2023/01/09/1064864/image-making-ai-10-breakthrough-technologies-2023/>>

statista. (2023.1.26.). The Companies Holding the Most AI Patents.
<<https://www.statista.com/chart/19211/companies-with-the-most-ai-patents>> (검색일: 2024.2.12.)

Wei Li and others. (2022). EID-GAN : Generative Adversarial Nets for
Extremely Imbalanced Data Augmentation. 『IEEE Transactions on
Industrial Information』

YOUTUBE. (2023.4.26.). Palantir AIP | Defense and Military.
<https://www.youtube.com/watch?v=XEM5qz__HOU>

ABSTRACT

A Study on the Application of Large Language Model(LLM) to Militarize Weapons Systems

Kang, Myung-Chul

Major in Defense AI Convergence

Dept. of Defense Force Power

Graduate School of National Defense Sciences

Hansung University

With the advent of the Fourth Industrial Revolution, the age of super-giant AI has begun. Neighboring countries are strongly promoting AI's defense application by selecting it as an important national task. The importance of our military is also increasing due to the population cliff problem.

With the advent of the Generative Pre-trained Transformer (GPT), which uses big data analysis technology for AI, the value and importance of ultra-large AI services have increased. Generative AI is a representative service of ultra-large AI. Generative AI is an AI model that generates various contents. The 'Large Language Model (LLM)' generates textual content as a type of Generative AI, and many Generative AI develop based on LLM.

The LLM-based, generative AI market average annual growth is about 38%, and it is used in various fields across society, including financial services, medical and life sciences, automobiles and manufacturing, media and entertainment, telecommunications, and energy. LLM is developing into a 'large Multimodal Model(LMM)' trained based on various modality data such as image or audio along with text. Considering the LLM development trend, the availability will be infinite and even more important.

Considering future war patterns, it is important to acquire intelligent weapons systems as the battlefield environment must be gradually modified in the direction of unmanned, automated, and autonomous. Palantir Technologies, a leading big data analysis company, has launched an 'Artificial Intelligence Platform(AIP)' for corporate and military applications. By integrating LLM with existing AI and machine learning technologies, AIP provides comprehensive solutions for different fields, such as defense and businesses. As such, efforts to apply LLM to weapons systems have begun.

LLM will recognize the battlefield and enable information collection and analysis, strategic decision-making, military education and simulation, multilingual communication and translation. It will also be an important key to acquiring intelligent weapons systems. Therefore, the application of LLM in weapons systems is an important issue and will be a key to achieving an edge in the competition for defense artificial intelligence hegemony in the future. This paper studied LLM, that is, to derive a plan to militarize weapons systems to which the latest technology is applied (the activity of developing or purchasing weapons systems and deploying them to the required group).

First of all, starting with the LLM theoretical consideration, the importance of LLM was recognized through the status of use and

future reprint patterns, and an example of applying LLM to the weapon system was presented. When militarize the weapon system through examples, restrictions were derived and application plans were presented in four aspects.

First, in terms of developing LLM core technologies and nurturing human resources, the 'LLM technology applicable to weapons systems' based on the four key technologies in the Defense Technology Plan was analyzed. Since then, a 'systematic talent development plan' has been proposed in terms of human resource development and empathy so that these core technologies can be developed and applied to national defense.

Second, in terms of weapons system acquisition, it was proposed to establish an Agile-type 'SW acquisition process' that can be acquired in a relatively short period (6 months to 1 year), focusing on embedded software and SW-oriented weapons systems in the weapons system. In addition, in order to modify ROC freely in the process of acquiring weapons systems, a plan to set the minimum and maximum including ROC core capabilities in the initial stage was proposed.

Third, in terms of weapon system test evaluation, a step-by-step test evaluation plan (1st stage: AI model performance evaluation, 2nd stage: actual operation environment test evaluation) suitable for AI weapon system was proposed, and related laws and regulations to support this were analyzed and supplemented. In addition, in order to prevent technological obsolescence between operation and maintenance, it also proposed a 'measures to institutionalize the maintenance and management categories of AI-based weapon systems'.

Fourth, in terms of weapon system quality management, a 'plan to

establish governance centered on quality management tasks' was proposed, including the organization of a big data management organization, a weapon system quality management guide, and the application of quantum technology to the cloud.

This proposal will make us aware of the applicability of LLM's weapon system. It will also quickly acquire LLM-applied weapon systems and provide the foundation for the required group to utilize quality-verified weapon systems after performance evaluation.

【Key words】 Generative AI, Large Language Model (LLM), Multimodal, Data, Weapon system