

석사학위논문

AI 윤리기준을 고려한
국방 AI 적용 가속화 방안 연구

2025년

한성대학교 국방과학대학원

국 방 전 력 학 과

국 방 A I 융 합 전 공

이 상 열

석사학위논문
지도교수 양병희

AI 윤리기준을 고려한 국방 AI 적용 가속화 방안 연구

A study on how to accelerate the application of
defense AI considering AI ethical standards

2024년 12월 일

한성대학교 국방과학대학원

국 방 전 력 학 과

국 방 A I 융 합 전 공

이 상 열

석사학위논문
지도교수 양병희

AI 윤리기준을 고려한 국방 AI 적용 가속화 방안 연구

A study on how to accelerate the application of
defense AI considering AI ethical standards

위 논문을 국방전력학 석사학위 논문으로 제출함

2024년 12월 일

한성대학교 국방과학대학원

국 방 전 력 학 과

국 방 A I 융 합 전 공

이 상 열

이상열의 국방전력학 석사학위 논문을 인준함

2024년 12월 일

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

AI 윤리기준을 고려한 국방 AI 적용 가속화 방안 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

이 상 열

4차산업혁명은 사회 쉰 영역에 급속도로 확산되어 다양한 변화를 가져다주고 있다. 첨단 과학기술의 핵심 분야인 AI는 4차산업혁명을 선도하는 분야로써 국방의 다양한 분야에 혁신을 일으키고 있으며, 일부 주요 국가를 비롯하여 세계 여러 나라에서 경쟁적으로 연구개발을 추진하고 있다. 우리 군도 국방 무기 및 전력지원체계와 국방행정 분야 등에서 AI 적용을 위해 많은 노력을 기울이고 있으나 아쉽게도 여러 가지 제한사항과 문제점 등으로 인해 쉽게 AI를 적용하지 못하고 있는 실정이다. 따라서 본 논문은 국방 분야에 AI를 적용하는 데 있어서 제한사항과 문제점으로 작용하고 있는 부분을 식별하여 AI 윤리적 관점과 국방 도메인 영역의 관점에서 발전방안을 제시하고 있다.

국방 분야에 AI를 적용하는 데 있어서 제한사항 및 문제점으로 작용하고 있는 분야는 크게 2가지로 예상할 수 있는데 첫째는 민간분야에서도 공통적으로 고민하고 있는 분야로서 AI 윤리적 관점에서의 ‘신뢰할 수 있

는 AI를 만들 수 있는가?’라는 부분이다. AI의 신뢰성에 영향을 미칠 수 있는 요소에는 여러 가지가 있을 수 있는데 국방 분야의 AI 적용에 있어서는 크게 안전성, 투명성, 견고성, 통제가능성, 책임성 등 5가지 정도를 윤리적 관점에서의 핵심 요소(윤리기준)로 판단하고 있는데 이 요소들에서 발생하고 있는 제한사항과 문제점을 들 수 있다. 둘째는 국방 도메인 영역의 관점에서 AI 기반체계, 전략 및 정책, 각종 훈령의 상호연계성, AI 적용을 위한 개념연구, 군사보안의 인식, AI 전문인력 및 조직의 운영, 의사결정시스템 등 軍이 가지고 있는 고유의 특수성과 업무추진 시스템에서 발생하는 여러 가지 제한사항과 문제점을 들 수 있다.

이러한 두 가지 제한사항과 문제점을 해소하기 위해서 다음과 같은 여덟가지 발전방안을 제시하였다. 첫째는 신뢰성 있는 국방 AI 적용을 위한 윤리기준의 정립, 둘째는 미래 지속발전이 가능한 AI 기반체계 구축, 셋째는 사용자 중심의 AI 법규, 제도 및 정책 발전, 넷째는 소요창출에서부터 획득체계까지 연계된 AI 발전 추진, 다섯째는 AI 기술 특성과 소요를 고려한 AI 개념연구, 여섯째는 개발자 및 운용자 중심의 보안 규제 해결방안 강구, 일곱째는 국방전력발전업무의 융합형 AI 전문인력 육성, 마지막 여덟째는 국방 AI 컨트롤타워 및 실질적인 의사결정기구 운용 방안에 대해서 제시하였다. 이상에서 제시한 여덟 가지의 발전방안은 향후 국방의 주 영역에 AI를 적용하는 데 있어서 제한사항 및 문제점을 효과적으로 해결할 수 있도록 해결 방향에 대한 개념을 제시하고 있다. 향후 본 연구가 다양한 후속 연구의 밑거름으로 작용하여 국방 AI의 여러 가지 난제를 조기에 해결하는데 크게 기여할 수 있기를 기대한다.

[주요어] AI 윤리적 관점, 신뢰할 수 있는 AI, 국방 도메인 영역의 관점

목 차

제 1 장 서론	1
제 1 절 연구의 배경 및 목적	1
제 2 절 연구의 범위 및 방법	3
제 2 장 AI의 군사적 활용을 위한 이론적 배경	4
제 1 절 AI의 개념	4
제 2 절 AI의 활용 사례	7
제 3 절 안전하고 신뢰성 있는 AI의 실현	20
제 4 절 주요국의 AI 군사적 활용 전략 및 정책	28
제 3 장 AI의 군사적 활용시 제한사항 및 문제점	51
제 1 절 AI 윤리기준의 인식 및 적용 측면	51
제 2 절 국방 데이터 및 플랫폼 등 AI 기반체계 측면	53
제 3 절 국방 AI 관련 법규, 전략 및 정책 수립 측면	55
제 4 절 국방기획관리기본훈령과 국방정보화업무훈령의 연계성 측면 ...	57
제 5 절 국방 AI 적용을 위한 개념연구 측면	61
제 6 절 국방 AI 적용시 군사보안의 인식 측면	63
제 7 절 AI 전문인력 및 조직 운영 측면	64
제 8 절 AI 관련 軍 내부 의사결정시스템 측면	66

제 4 장	국방 AI 적용 가속화를 위한 발전방안	68
제 1 절	신뢰성 있는 국방 AI 적용을 위한 윤리기준 정립	68
제 2 절	미래 지속발전이 가능한 AI 기반체계 구축	77
제 3 절	사용자 중심의 AI 법규, 제도 및 정책 발전	79
제 4 절	소요창출에서 획득체계까지 연계된 AI 발전 추진	82
제 5 절	AI 기술 특성과 소요를 고려한 AI 개념연구	84
제 6 절	개발자 및 운용자 중심의 보안 규제 해결방안 강구	87
제 7 절	국방전력발전업무의 융합형 AI 전문인력 육성	90
제 8 절	국방 AI 컨트롤타워 및 실질적인 의사결정기구 운용	93
제 5 장	결론	96
참고문헌		98
부록		100
ABSTRACT		103

표 목 차

[표 2-1] 기술 요소별 AI 기술수준 정의	5
[표 2-2] 기관별 AI 거버넌스 원칙	23
[표 2-3] 합동AI센터(JAIC) 분야별 주요임무	30
[표 2-4] 영국 국방부의 국방 AI 비전 달성을 위한 세부 전략	35
[표 2-5] 영국 국방부의 국방 AI 목표	36
[표 2-6] 국방AI센터(DAIC) 거버넌스	37
[표 2-7] 중국의 차세대 인공지능 발전계획	42
[표 2-8] 러시아 국방부의 AI 기술 개발 관련 10대 계획	44
[표 2-9] 4대 AI 플래그십 프로젝트 및 4대 분야 정책 추진방향	47
[표 2-10] 해군 AI 추진 분야 및 과제	50
[표 2-11] 공군 AI 추진 목표 및 과제	50

그림 목 차

[그림 1-1] 연구 목적	2
[그림 2-1] 자율제조 AI 적용 사례	7
[그림 2-2] 약지도 학습 기반 홍부 X영상 분류 및 병변탐지 사례	8
[그림 2-3] 지능형 재해·환경 모니터링 시스템 사례(한국전력)	9
[그림 2-4] AI 기반의 혁신적인 풀필먼트(Fulfilment) 사례	9
[그림 2-5] AI 기반의 과학적 농작물 생산과 유통 혁신 사례	10
[그림 2-6] 스타일 이미지 분석을 통한 새로운 작품 생산 기술 사례 ..	11
[그림 2-7] 육군 Army TIGER 여단 무인전투차량 시연 모습	12
[그림 2-8] 사이버 위협 자동 탐지 및 차단 체계(CHASE)	13
[그림 2-9] 자율무기시스템(Autonomous Weapon System) 개발 사례 ..	14
[그림 2-10] 지능형 지휘결심지원체계 통합상황실 예상 이미지	15
[그림 2-11] 지능형 지휘통제체계 사례	16
[그림 2-12] AI 기반 스마트 인재관리시스템	17
[그림 2-13] AI 기반 의료영상 판독시스템	18
[그림 2-14] 스마트 물류센터 사례	19
[그림 2-15] 육군 5사단 AI 경계작전센터 내부 모습	19
[그림 2-16] 美 국방성의 AI 윤리원칙(5가지) 기준(2020. 2)	21
[그림 2-17] 사람이 중심이 되는 인공지능(AI) 윤리기준	21
[그림 2-18] 2024 REAIM 고위급회의 개최식	25
[그림 2-19] 2024 REAIM 고위급회의 소그룹회의	26
[그림 2-20] 최고디지털AI책임관(CDAO) 설립(2022)	29
[그림 2-21] 합동AI센터(JAIC) 2.0 조직도	32
[그림 2-22] 美 국방부 CDAO 조직도	33
[그림 2-23] CDAO의 데이터, 분석 및 AI 적용 전략	34
[그림 2-24] 영국 국방AI센터(DAIC) 아키텍처 다이어그램	38
[그림 2-25] 독일군 인공지능(KI) 업무관련 조직도(구상안)	40

[그림 2-26] 국방혁신 4.0의 5대 중점 및 16개 과제	46
[그림 2-27] 국방 AI 비전과 목표	48
[그림 2-28] 육군 인공지능(AI) 추진전략	49
[그림 3-1] 무기체계를 대상으로 하는 국방기획관리 문서체계	58
[그림 3-2] 무기체계 획득 절차도	59
[그림 3-3] 국방정보체계 획득 절차도	60
[그림 4-1] AI의 군사적 활용시 신뢰성에 영향을 미칠수 있는 윤리기준 ..	70
[그림 4-2] AI(지능화) 소요판단 절차	86
[그림 4-3] AI 전문가에게 필요한 요구능력	91

제 1 장 서론

제 1 절 연구의 배경 및 목적

4차산업혁명 기술이 사회 전반에 빠르게 적용되며, 민간영역의 세계를 급격하게 변화시키고 있다. 국방영역에서도 주요 선진국을 중심으로 중요성을 인지하고 신속하게 첨단기술을 적용하기 위해 수많은 예산을 투자하여 집중적인 연구개발에 박차를 가하고 있다. 4차산업혁명 기술은 인공지능(이하 ‘AI’로 칭함), 사물인터넷(IoT), 빅데이터, 블록체인, 로봇공학 등 여러 가지 신기술들이 있으나 이중 AI는 4차산업혁명을 이끌고 있는 핵심 기술로 손꼽을 수 있다. 우리 軍도 이러한 4차산업혁명의 중요성을 인지하여 2010년대 후반부터 국방 분야에 AI 적용과 확산을 위해 다양한 노력을 기울이고 있다. 각 소요 군(육군, 해군, 공군, 해병대 등)에서는 국방 AI 적용을 위해 개념을 연구하고 소요를 창출할 수 있는 조직과 직책을 신설하여 업무추진을 시작하였으며, 국방부는 2021년에 국방 AI 추진전략 1.0을 발표하여 軍의 AI 전략을 이끌어가고 있다. 최근 2023년에 現 정부가 발표한 120대 국정과제 중 국방 분야에 AI 기반 첨단과학기술장군 과제가 반영되어 더욱더 많은 관심과 지원을 받으며, 국방 분야에 AI 적용 가속화를 위해 많은 노력을 기울이고 있다.

그러나 우리 軍은 AI 추진전략 수립, 국정 이행과제 제시 등 다양한 비전과 목표를 제시하고, 이를 달성하기 위해 많은 노력을 기울여 왔으나 아직도 수년째 국방 분야 AI 적용에 만족할 만한 가시적 성과를 내고 있지 못하는 실정이다. 이는 국방 분야에 근무하는 수많은 인원의 노력이 부족한 것이 아니라 AI가 가지고 있는 특성과 軍의 특수성으로 인한 여러 가지 제한사항과 문제점들이 장애물로 작용하여 AI의 발전 속도를 저하시키고 있기 때문이다. AI 발전에 장애물로 작용하고 있는 AI의 특성과 軍의 특수성을 구체적으로 살펴보면, 먼저 AI가 가지고 있는 주요 특성으로 AI는 일반적인 소프트웨어와 다르게 데이터, 알고리즘, 컴퓨팅 파워(플랫

폼) 등 여러 가지 요소들이 유기적인 상호작용을 통해 결과물을 만들어내는 특성을 가지고 있으며, 인간과 같은 지식의 성장이나 지능의 범위, 모달리티 등을 기술적으로 구현이 가능하나 구조가 복잡하고 난이도가 높아 개발에 어려운 특성이 있다. 또한 다른 첨단기술들과 비교하여 발전 속도가 매우 빨라 기술의 진부화에 많은 영향을 받고 있으며, 인간과 유사한 지능 수준을 구현할 수 있어 인간의 보조역할을 수행함으로써 신뢰성 확보가 최대의 핵심 요건으로 인식되고 있는 특성을 지니고 있다.

軍의 특수성 측면에서 AI는 민간분야와 달리 군사보안 분야에 매우 민감하게 반응하고 대응하기 때문에 각종 소프트웨어와 하드웨어의 반·출입과 사용이 자유롭지 못하며, 전략 및 정책 수립, 국방기획관리체계 반영, 개념연구, 기술개발 착수 등 다양한 절차와 의사결정시스템을 거쳐 연구개발 및 도입이 결정되기에 국방 분야에 신속한 AI 적용이 어려운 실정이다. 또한 외부 AI 전문인력 유입 및 軍 내부 전문인력 양성, AI 개발에 필요한 기반체계 구축 등 AI 적용에 필요한 인프라 구축이 정책 및 제도적인 측면에서 적극적으로 추진되지 못하는 문제점도 가지고 있다.

따라서 본 연구에서는 무기 및 전력지원체계 등 국방 분야에 AI 적용 가속화를 위해 AI가 가지고 있는 일반적인 특성과 軍 고유의 특수성으로 인해 발생하고 있는 다양한 제한사항과 문제점을 구체적으로 식별 및 분석하고, 이를 해소할 수 있는 여러 가지 발전방안을 제시하여 국방 분야 AI 발전 가속화에 기여하고자 한다.

[그림 1-1] 연구목적



제 2 절 연구의 범위 및 방법

본 연구 주제의 범위는 국방 분야 AI 적용 가속화를 위해 AI가 가지고 있는 일반적인 특성과 軍의 특수성으로 인해 발생하는 제한사항과 문제점을 식별 및 분석하고 이에 대한 발전방안을 제시하였다.

구체적인 범위를 살펴보면 첫 번째는 AI의 일반적 개념과 민간 및 군사 분야의 AI 활용 사례에 대해서 분석해 보고, AI의 군사적 활용시 영향을 미칠 수 있는 윤리원칙의 핵심적인 요소와 국내외 주요국의 군사적인 AI 활용 전략 및 정책에 대한 이론적 배경을 분석하여 제시하였다.

두 번째는 국방 분야에 AI 적용시 軍이 가지고 있는 고유의 특수성으로 인해 다양한 제한사항 및 문제점이 발생할 수 있는데 AI의 윤리적 관점과 국방 도메인 영역의 관점에서 제한사항과 문제점을 식별 및 분석하여 제시하였다.

세 번째는 식별된 제한사항과 문제점을 해소하기 위해 AI 윤리기준의 정립을 중심으로 국방의 다양한 도메인 영역에서 제한사항 및 문제점을 극복할 수 있는 발전방안에 대해서 제시하였다.

연구 방법으로는 먼저 국방 분야 AI 적용을 위해 軍 내부의 무기 및 전력지원체계와 국방 운영 등 다양한 분야(개념연구, 소요기획, 전력화사업, 분석평가, 조직관리, 인재육성, 제도 및 정책수립 등)에서 임무수행중인 전문가의 인터뷰와 토론회 등을 통해 국방 AI를 적용하는 데 있어서 걸림돌로 작용하고 있는 제한사항 및 문제점을 식별하였고, 이후 각 소요군(육군, 해군, 공군 등) 및 국방부, 연구기관 등 다양한 AI 부서에서 근무 중인 전문가 27명의 설문문을 통해 그들이 생각하고 있는 국방 AI 적용시 제한사항 및 문제점에 대해서 심층적으로 분석을 시행하였고, 우선적으로 발전시켜야 할 중요분야를 국방 도메인 영역과 연계하여 8개 분야로 나누어 각각의 발전방안에 대해서 제시하였다.

제 2 장 AI의 군사적 활용을 위한 이론적 배경

본 연구에서는 AI의 군사적 활용을 위해 AI의 일반적 개념과 활용 사례에 대해서 알아보고, AI를 군사적으로 활용시 신뢰성에 영향을 미칠 수 있는 윤리기준(원칙), 거버넌스 체계, 책임있는 AI(RAI) 추진사례와 해외 주요 국가 및 우리 軍의 AI 활용 전략과 정책에 대해서 분석해 본다.

제 1 절 AI의 개념

(1) 일반적 의미

인공지능(Artificial Intelligence, AI)이란 인간의 지각능력, 추론능력, 학습능력 등을 인공적으로 구현하려는 컴퓨터 과학의 세부분야 중 하나이며, 인간을 포함한 동물이 갖고 있는 지능 즉, 자연 지능(natural intelligence)과는 다른 개념이다.¹⁾

AI는 인간의 지능을 모방하여 최대한 인간과 유사한 지능을 구현할 수 있도록 기계·컴퓨터를 활용하여 구현한 학문 또는 기술로써 하드웨어와 소프트웨어를 활용하여 인공적인 지능을 만들어내는 4차산업혁명 기술 분야에 해당한다. AI는 인간의 지능과 유사하게 인식, 판단, 학습 등 3대 능력의 정도에 따라 일반적으로 강인공지능(Strong AI)과 약인공지능(Weak AI)으로 분류하고 있다.

포브스는 2019년 기준 현재의 AI 기술 수준은 좁은 인공지능(ANI: Artificial Narrow Intelligence)이며, 향후 인간처럼 다양한 분야에서 포괄적으로 학습하고 이해할 수 있는 일반 인공지능(AGI: Artificial General Intelligence)과 인간을 뛰어넘는 슈퍼 인공지능(ASI: Artificial Super Intelligence)으로 발전할 수 있을 것이라고 전망했다.²⁾

우리나라 국가산업의 측면에서 보면 AI는 1980년대에 단순 제어 프로그램으로 시작하였고, 1990년대에는 적절한 판단을 내리기 위한 추론 및

1) 위키백과: 인공지능의 개념

2) 포브스: “7 Type of Artificial Intelligence”, 2019.6.19.

탐색 등 DB 검색에 주로 활용되었으며, 2000년대에 들어서는 머신러닝으로 발전하였다. 2010년 이후에는 딥러닝 기술로 파급력이 증대되어 국가산업의 다양한 분야에서 매우 중요한 기술중의 하나로 자리잡고 있다. 이에 따라 국내는 물론 해외 주요 선진국들은 AI를 국가 차원에서 육성해야 할 핵심기술로 지정하여 전략적으로 중·장기 로드맵을 구상하여 체계적인 연구개발과 예산 투자를 추진하고 있으며, 국가산업의 전반은 물론, 국방 분야에도 적극적으로 AI 기술 적용을 추진하고 있다. 뿐만 아니라 AI 기술을 개발하는 데 있어서 프로젝트 관리, 개발 예산 및 일정, 응용이나 서비스 등 사업화 추진이 가능하고, 로드맵을 계획하여 수행할 때 기준이 될 수 있도록 기술 요소별 AI 기술수준을 정의³⁾하여 활용하고 있다.

[표 2-1] 기술 요소별 AI 기술수준 정의

LEVEL		i) 지 식 성 장	ii) 지 능 범 위	iii) 도 메 인	iv) 인 간 - AI 협 업	v)모달리티	vi) 통 합 인 지
ASI (Artificial Super Intelligence)	6	인간의 개입 없이 지식 성장	인간의 6대 지능 이상을 지원하고 빠르고 정확함	오픈 영역	AI 스스로 미션을 생성하고 수행	5개 이상	AI 자기인지와 인간보다 빠른 직관
AGI (Artificial General Intelligence)	5	인간의 부분개입 지식 성장	인간의 4대 지능 이상을 통합	이중 분야로 확장 가능	AI가 판단 근거 설득 인간-AI 상호합의	4개 이상	인간/상황/이력/지식 종합판단
	4	인간 개입으로 지식 성장	인간의 2대 지능 이상을 통합	유사 분야로 확장 가능	AI가 판단 근거를 설명하여 추천	2~3개	인간/상황/이력/지식 부분종합
ANI (Artificial Narrow Intelligence)	3	비지도 학습 (고정지식)	1개 분야 전문가 수준으로 지식처리 가능	동일 분야 내 확장	AI 추천으로 AI-인간 협업 미션 수행	ND	인간과 주변 상황 연결판단
	2	지도 학습 (고정지식)	단일 분량에서 단순한 업무처리	ND	AI-인간 협업으로 사전 정의된 미션 수행	ND	언어, 이미지, 감정, 현상 등 동종 인지
	1	규칙 기반 (고정지식)	정해진 조건 비교로 대응 처리	고정 분야 적용	사전에 정해진 순서에 따라 수행	1개	HW 인지 수치 의존 (온도 센서 등)
		독특한 AI (IQ)			인간과 소통하는 AI (EQ)		

* ND: Not Defined

출처: ATL 1.0: 인공지능 기술 수준 정의(한국전자통신연구원, 2020)

3) 한국전자통신연구원(ETRI) ATL 1.0 인공지능 기술 수준 정의 P.6, 2020

(2) 군사적 의미

군사적 의미의 AI는 일반적 의미의 개념을 바탕으로 지휘관이 국방영역의 군사업무 수행시 지휘결심(의사결정)을 지원하는 기술로 정의⁴⁾할 수 있으며, 국방의 다양한 영역에 AI 적용시 전장 환경을 인식하고(전장 인식), 상황을 분석하여 판단하고(자율판단), 이를 토대로 한 의사결정(지휘결심) 능력과 환경이 상호작용을 하는 물리적 지능(임무수행)을 의미하는 것⁵⁾으로 정의할 수 있다.

이와 더불어 우리 국방부에서는 국방의 쏘 영역에 AI 적용 확산을 위해 국방 AI 기능 구현 측면에서 국방 AI 영역을 국방운영 AI, 무기체계 AI, 전장지휘 AI 등 3개 분야로 구분⁶⁾하여 국방 운영의 효율화, 무기체계별 고도화, 지능형 전장 지휘통제체계 등 세부적인 추진전략을 수립하여 AI 적용을 추진하고 있으며, 세부 적용 분야는 아래 내용과 같다.

- 국방운영 AI: 경계, 군수, 의료, 인사 등 부대운영 및 전투임무 지원을 위한 서비스 분야
- 무기체계 AI: 전차, 자주포, 차량, 함정, 항공기 등 전투임무 수행에 필요한 전투장비 운용 분야
- 전장지휘 AI: 결심지원(의사결정) 지원을 위한 지휘통제체계 분야

또한 AI의 3대 구성요소인 데이터, 알고리즘, 플랫폼은 접근성, 전문성, 보안성 등 軍 특유의 운용환경과 특수성을 지니고 있다. 데이터 측면에서는 군사용 AI 개발에 필요한 軍 전용의 학습용 데이터가 반드시 필요하나 확보에 어려움이 있으며, 알고리즘 측면에서는 무기체계 및 전장지휘 AI 모델 개발을 위해서 전술적 운용개념 등 다양한 도메인 영역 군사전문가들의 전문지식과 참여가 반드시 필요하다. 또한 플랫폼 측면에서는 AI 운용환경의 특수성에 따라 악조건 및 극한의 환경 등에서도 운용될 수 있도록 Edge Computing, 모바일 기반, 소형화, 경량화 등 다양한 형태의 플랫폼 구축 요구가 필수적으로 수반되어야 하는 특징이 있다.

4) '23~'33 인공지능 종합발전계획 P.12(육군 교육사, 2022)

5) 미래국방 2030 AI 기술전략(국방기술진흥연구소, 2022)

6) 국방 인공지능(AI) 추진전략 2.0(국방부, 2022.3.)

제 2 절 AI의 활용 사례

(1) 민간분야 AI 활용

민간분야의 AI는 다양한 산업영역에서 혁신을 이끌며 적용되고 있다. 이러한 AI 적용 분야에는 제조업, 의료, 안전, 유통(물류), 농업, 엔터테인먼트, 자율주행 등이 있으며, 광범위하게 활용되고 있다. AI 기술은 다양한 산업 분야에서 업무의 효율성과 정확도를 높이고, 소비자의 만족도를 향상시켜 새로운 가치를 창출하는데 많은 기여를 하고 있으며, 대표적인 분야별로 AI 활용 사례를 분석해 본다.

(가) 제조업 분야의 AI 사례를 살펴보면, 다양한 산업현장에서 AI 기반의 로봇 또는 자동화 공정을 적용하여 생산성 및 제품의 품질향상, 작업시간의 단축, 작업자의 안전 보장 등 다양한 측면에서 긍정적인 효과를 얻고 있으며, 기업의 경쟁력을 향상시키는데 큰 기여를 하고 있다. 또한 산업현장에서 발생하는 여러 유형의 센서 데이터를 분석하여 각종 산업기계의 고장을 사전에 예방하고, 적절한 시기에 유지보수 활동을 통하여 수명을 연장함으로써 기계의 효율성을 극대화 시키고, 비용을 절감하는 등의 효과를 달성하고 있다. 이처럼 AI는 산업현장에서 제조업의 혁신을 이끌어 가고 있으며, 경쟁력을 강화하는 데 중요한 역할을 하고 있다.

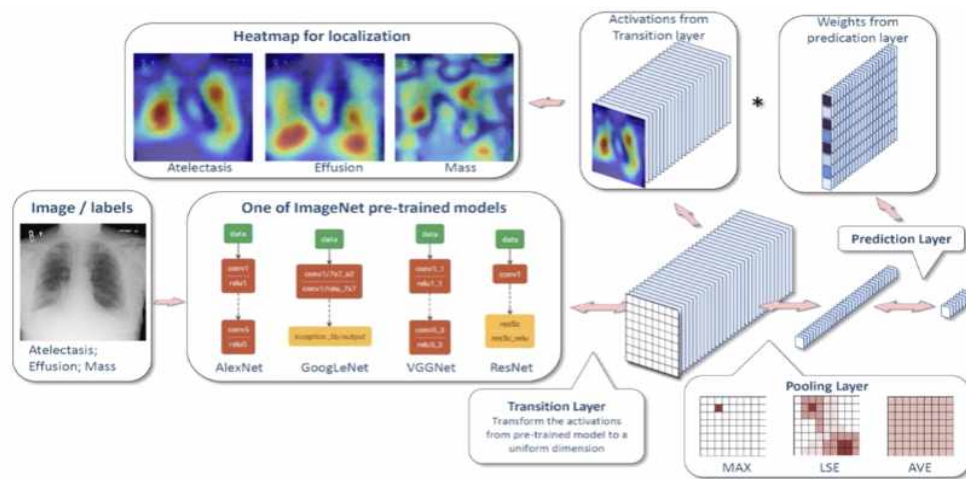
[그림 2-1] 자율제조 AI 적용 사례



출처: <https://www.hellot.net/news/article.html?no=92260>

(나) 의료 분야에서는 AI를 활용하여 각종 의료 데이터를 분석하여 질병을 조기에 진단하는 데 도움을 줄 수 있으며, X-ray, MRI, CT 등의 이미지 분석과 환자의 생체신호를 실시간 모니터링하여 이상징후를 조기에 감지할 수 있다. 또한 환자의 유전 정보와 병력 데이터를 활용하여 개인 맞춤형 치료가 가능하고, 신약 개발의 기간을 단축하는 데 도움을 줄 수 있으며, 각종 전자 의료 기록(EMR)을 분석하여 필요한 정보를 신속하게 검색할 수 있도록 지원이 가능하다.

[그림 2-2] 약지도 학습 기반 흉부 X영상 분류 및 병변탐지 사례



출처: <https://brunch.co.kr/@kakao-it/81>

(다) 안전 분야에서는 교통안전, 산업안전, 재난안전, 사이버안전 등 일상생활 전반에 걸쳐 다양한 곳에서 활용되고 있다. AI 기반의 교통안전 관리 시스템은 교통의 흐름을 분석하여 사고를 줄이거나, 교통체증을 완화시키는데 도움을 주고 있으며, 공장이나 건설현장 등에서는 작업자의 안전을 모니터링 하거나 위험요소를 감지하여 즉각적인 경고를 통해 사고를 예방할 수 있다. 또한 지진이나 홍수 등 각종 자연재해를 미리 예측하여 대응책을 강구하는데 활용되고 있으며, 인터넷 등 각종 전산망에 비정상적인 활동 등을 감지하여 사이버 공격 등을 예방하는 데 효과적으로 활용되는 등 인명과 재산을 보호하는 데 중요한 역할을 수행하고 있다.

[그림 2-3] 지능형 재해·환경 모니터링 시스템 사례(한국전력)



출처: <https://blog.naver.com/alcherads/223410727254>

(라) 유통 분야에서는 물류 경로 최적화, 재고 관리, 배송 일정 조정 등을 통해 공급망의 효율성을 높이는 데 AI를 활용하고 있으며, AI 기반의 챗봇 시스템을 활용하여 수많은 고객의 질의응답 및 문제해결에 도움을 주고 있다. 또한 각 매장 내 수요 예측, 효율적인 물품의 배치, 재고 관리 등을 위해 AI 알고리즘을 활용한 고객의 이동경로, 선호도 등을 분석하여 매장 운용의 효율성을 높이고, 매출의 증대 효과를 달성하고 있다.

[그림 2-4] AI 기반의 혁신적인 풀필먼트(Fulfilment)⁷⁾ 사례

발전 단계	1단계 : 물류창고	2단계 : 디지털화	3단계 : 지능화	4단계 : 자동화
대표 사례	• 중소유통 물류센터	• 중소유통 풀필먼트 센터 (포항, 창원)	• 마켓컬리	• 쿠팡(대구) • SSG(NEO)
사진				
주요장비	• POS • 상품보관 랙 • 지게차	• 창고운영시스템 • 자동화정비(DAS/DPS) • 디지털 프로세스	• AI, 데이터분석시스템 • IoT, 콜드체인 • 로봇 일부 활용	• AI, IoT • 자동화랙 • 입출고 로봇
주요 기능	• 입출고 • 상품보관 • 회계처리	• 실시간 재고관리 • 온라인 주문처리 • 점포 온라인 지원 • 배송연계	• 맞춤형 상품 소싱 • 최적 배송 경로 • AI 마케팅 • 자동 보고서 생성	• 무인화(피킹/패킹) • 자동 재고 관리 • AI 기반 입출고 검사 • AI 기반 위험 관리

출처: 한국전자통신산업진흥회 이슈 리포트 2023-13호

7) 풀필먼트(Fulfilment) 센터: 제품의 수령, 저장, 재고 관리, 분류 및 분배, 배송 준비 그리고 반품과 환급처리까지 물류의 모든 과정을 담당하면서 효율적인 제품의 흐름을 보장한다.

(마) 농업 분야에서는 AI를 활용하여 각종 농작물의 질병을 감지하고, 수확 시기를 예측하며, 자원을 효과적으로 관리하여 생산성을 획기적으로 향상시킬 수 있다. 물과 비료, 농약 등의 자원을 효율적으로 정확하게 사용하고, 질병 및 해충 감지, 기후변화 예측 등을 통해 농작물의 위험을 관리하고, 최적의 온도 및 일조량 등의 성장조건을 관리함으로써 농산물의 품질을 향상시킬 수 있다. 또한 부족한 인력문제의 해결을 위해 AI 기반의 자동화된 농기계를 활용하여 인건비를 절감하고, 작업의 정확도를 향상시킬 수 있는 등 농업의 미래를 변화시키고 있는 중요한 기술로써 자리를 잡고 있다.

[그림 2-5] AI 기반의 과학적 농작물 생산과 유통 혁신 사례



출처: <https://post.naver.com/viewer/postView.nhn?volumeNo=9425075&memberNo=36080930&vType=VERTICAL>

(바) 엔터테인먼트 분야는 우리의 일상에서 AI가 가장 활발하게 활용되고 있는 분야 중의 하나로 많은 부분에서 혁신과 효율성의 향상을 가져다주고 있다. TV방송, 영화, 음악 등 사용자의 시청 및 청취 기록을 분석하여 개인 맞춤형 콘텐츠 추천이 가능하고 뉴스 기사, 스포츠 리포트, 작곡 및 그림 그리기 등의 시스템이 개발되고 있다. 또한 인간의 고유 영역으로 여겨졌던 창작활동 부분에서도 딥러닝 알고리즘과 엄청난 데이터의 학습을 통해 새로운 아이디어와 콘텐츠를 생성함으로써 인간의 창의적

인 작업을 지원할 수 있는 능력을 갖추어 나가고 있어 앞으로 더욱 다양한 분야에서 활용될 것으로 예상된다.

[그림 2-6] 스타일 이미지 분석을 통한 새로운 작품 생산 기술 사례



출처: 고희의 ‘별이 빛나는 밤’(Google Arts & culture)

(2) 군사 분야 AI 활용

미래에는 전장의 범위가 지상, 해상, 공중 등 전통적인 범위에서 우주, 사이버 및 인지·심리 영역으로 확대되어 전면전과 국지도발, 하이브리드전 등 다양한 전쟁 양상으로 복잡성이 증가할 것이며, AI·드론봇 등 첨단과학기술 기반의 무기체계 등장으로 미래전의 전투수행개념에 많은 변화가 생길 것으로 예상된다. 특히 국내 저출산 문제로 2037년 이후 인구절벽의 시대가 도래하여 병력자원의 부족이 예상되며, 이에 따라 전쟁에서도 인명중시 풍조가 강화되어 AI 기반의 자율형 무기체계(Autonomous Weapon System), 유무인복합전투체계 등을 적극 활용하여 인명피해의 최소화 및 병력감축 상황에 대비한 대응책을 추진할 것으로 예상된다. 이를 토대로 국방 분야 AI 활용이 추진되고 있는 몇 가지 사례에 대해서 분석해 본다.

(가) 무기체계 분야의 AI 활용

1) 무인전투시스템: 지상 무인차량, 자율 비행드론, 4족보행 로

봇 등 다양한 무기체계에 AI가 탑재되어 24시간 적군에 대한 감시정찰 및 공격임무 수행, 장애물 제거, 보급 및 수송, 대량의 데이터 수집 및 분석 등 현대전에서 전투의 효율성과 군사작전의 안전성을 획기적으로 향상시키고 있다.

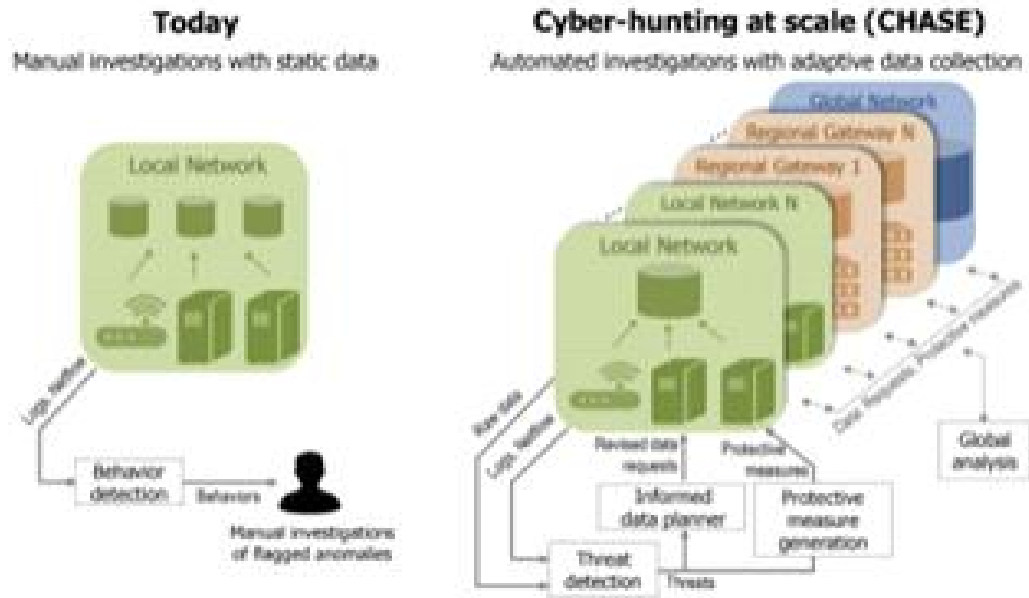
[그림 2-7] 육군 Army TIGER 여단 무인전투차량 시연 모습



출처: 육군 Army TIGER 여단 시범 보도자료(2022.6. NEWSIS)

2) 사이버 공격 및 방어시스템: 컴퓨터 네트워크를 통해 가상의 공간에서 다양한 수단을 활용하여 적의 정보체계를 교란, 거부, 통제, 파괴하는 등의 공격과 이를 방어하는 시스템으로 구분되는 무기체계 분야의 한 부분이다. 사이버 공격분야는 대량의 데이터 분석 및 패턴 인식을 통해 자동으로 공격을 실시하는 자동화 공격, 소셜미디어와 같은 다양한 플랫폼에서 특정대상을 공격하는 사회공학적 공격, 특정 웹사이트나 서버를 마비시키는 DDOS 공격 등이 있으며, 이러한 위협들의 비정상적인 패턴을 실시간대로 탐지하는 시스템과 사이버 공격이 발생되었을 때 특정 IP 주소를 차단하거나, 시스템을 격리하는 등의 조치를 취하는 자동화 대응 등의 방어시스템이 있다. 이러한 사이버 공격과 방어는 상호작용을 통해 매우 정교하고 치밀하게 이루어져 복잡성을 더욱 증가시키고 있으며, 사이버전은 군사적으로 미래의 중요한 작전영역으로 인식되고 있다.

[그림 2-8] 사이버 위협 자동 탐지 및 차단 체계(CHASE)



출처: 미래국방 2030 AI 기술전략(국방기술진흥연구소, 2022)

3) 자율무기시스템(Autonomous Weapon System): AI와 로봇 기술의 군사적 결합은 자율무기시스템(autonomous Weapon System)의 형태로 나타날 것이다. AI는 자율 무기체계의 두뇌로서 역할을 수행하며, 로봇은 몸통을 구성하는 요소이다. ‘자율성(Autonomous)’이라는 것은 자신의 행동을 스스로 통제하고 책임을 지는 것을 말하며, 인간의 통제없이 무기 자신이 스스로를 통제함을 뜻한다. 지금까지 무기는 대부분 인간의 직접적인 통제로 운용되는 수동적인 전투수단이었으나 자율무기시스템(Autonomous Weapon System)은 이러한 기존의 무기시스템과는 완전히 다른 개념으로 무기체계가 인간 전투원과 같이 하나의 독립된 전투 주체가 된다.⁸⁾ AI 기반의 자율무기시스템(Autonomous Weapon System)은 군사적으로 많은 부분에서 전술적 이점을 제공하고 있기 때문에 미래의 전투 양상을 변화시켜 나아갈 것으로 예상되지만, 완전 자율성, 정확도 및 속도 등의 기술적 문제와 군사적 활용성을 둘러싼 윤리적 문제해결이 앞으로의 발전방향에 지대한 영향을 미칠 것으로 예상된다.

8) 인공지능과 로봇의 군사적 활용과 선행 과제: 한국국방기술학회 논문지 송윤선, 2021.3.

[그림 2-9] 자율무기시스템(Autonomous Weapon System) 개발 사례



TUGV 전투 로봇



환자후송 로봇



Cruiser 전투로봇



ARV(무장) 전투로봇

출처: 인공지능 자율무기시스템에 대한 심층분석(박상우, 2024.4.)

(<https://blog.naver.com/kenjisama/223403958979>)

(나) 전장지휘 분야의 AI 활용

1) 지휘결심지원시스템: 미래의 전장환경은 지금보다 더 복잡하고 판단해야 할 요소가 많아져서 지휘관 및 참모가 의사결정을 내리는데 있어서 많은 어려움이 예상됨에 따라 세계 주요 군사강국들은 이러한 문제를 해결하기 위해 전투에서 의사결정을 신속하고 정확하게 수행하기 위해 지휘결심지원 AI를 적극적으로 개발하고 있다. 인간은 생물학적 특징으로 장시간 無 수면상태 하 지속적인 작전을 수행할 수 없으며, 전시에 高스트레스 환경에서 여러 가지 인지적 오류를 범할 수 있으나 AI는 인간과 달리 24시간 365일 정확한 임무수행이 가능하여 인간이 범할 수 있는 인지적 오류발생 확률을 획기적으로 줄여 불확실한 전장상황을 가시화하고 지휘관이 최선의 방책을 선정하는데 기여할 수 있다. 지휘결심지원 AI 시스템은 작전계획수립 및 작전실시간 의사결정 과정에서 인간 지휘관을 보좌하여 대량의 데이터를 신속하게 분석하고, 지휘결심에 필요한 중요 정보를 추출하여 지휘관에게 제공하는 기능을 수행할 수 있으며, 전장상황(적군의 이동 및 배치, 적의 의도 등)을 예측하여 다양한 시나리오를

활용하여 모델링 및 시뮬레이션함으로써 결과를 예측하고 지휘관이 효과적이고 빠른 지휘결심을 할 수 있도록 논리적 근거를 제공할 수 있다. 따라서 지휘관 및 참모는 AI를 통해 지휘결심에 필요한 다양한 정보수집, 조사, 분석 등의 불필요한 작업활동에 소요되는 시간과 노력을 줄임으로써 보다 나은 상황인식을 가능하게 하고 개인적인 직관이나 경험에 대한 의존도를 낮추어 전투에만 집중할 수 있는 여건을 조성해 줄 수 있다.

[그림 2-10] 지능형 지휘결심지원체계 통합상황실 예상 이미지



출처: 국방 AI참모 시스템 개발 보도자료(한화시스템, 2022.11.)

2) 지능형 지휘통제체계: 현대의 군사작전에 매우 중요한 역할을 수행하고 있으며, 정보의 수집 및 분석, 대용량 데이터의 실시간 전송 보장, 전투 클라우드 환경 구축, 전 영역의 정보공유체계 통합 연결 등 다양한 기술(초지능)과 시스템의 연결(초연결)을 통해 군사작전의 효율성을 높이고 전투수행 전 기능의 효율적인 통합운용에 기여하고 있다. 주요 사례를 살펴보면, 현재 미군에서는 합동전영역지휘통제(JADC2)의 일환으로 효율적인 전장지휘 및 결심지원 체계 구축을 위해 ‘고담 플랫폼(Gotham Platform)⁹⁾’, ‘TITAN (Tactical Intelligence Targeting Access Node)’¹⁰⁾

9) Gotham Platform: 센서, 드론, 위성, 인간정보 등 다양하게 수집된 정보를 융합 제공하는 시스템

10) TITAN(Tactical Intelligence Targeting Access Node): 이동식 지상 정보기지국으로 지상, 공중, 우주에 배치된 감지체계(센터)를 연동, 각종 유형의 정보를 자동 처리하는 기능 수행

등의 시스템을 구축하여 운용 중에 있으며, 한국군에서는 다양한 정찰자산에서 생성된 영상정보를 체계에서 융합하여 신뢰도가 향상된 영상정보를 주요 전장관리정보체계로 전파하여 전략표적타격작전을 지원할 수 있는 다출처영상융합체계¹¹⁾를 전력화하여 운용 중에 있다.

[그림 2-11] 지능형 지휘통제체계 사례



<전장관리정보체계 전파 및 표적타격 작전 지원>

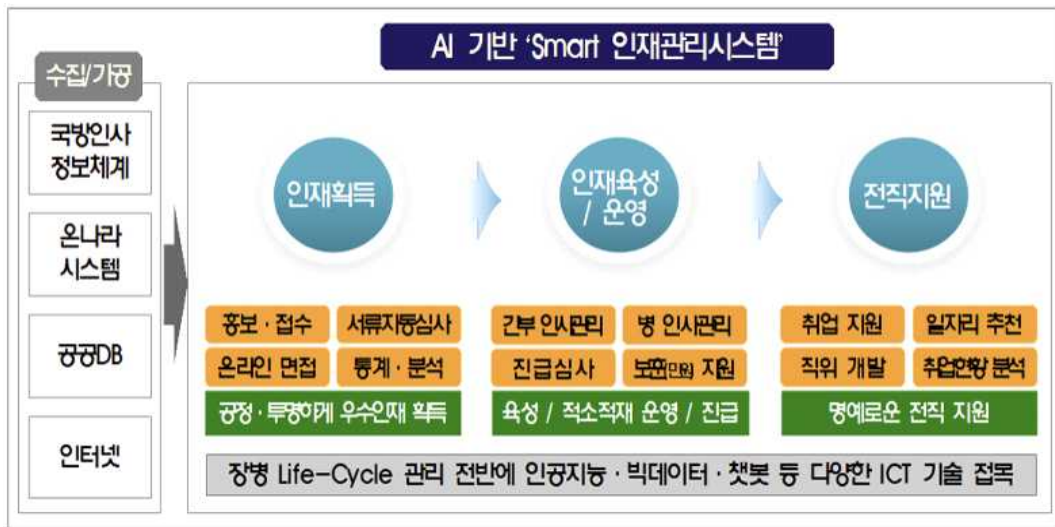
출처: 방사청, 다출처영상융합체계 전력화 완료 보도자료(2022.12.)

11) 다출처영상융합체계(기본형): 탐지, 교란, 파괴, 방어 수행을 위해 신속하고 정확한 감시정찰 영상정보 처리 및 분석 능력이 가능한 체계

(다) 국방운영 분야의 AI 활용

1) 인사/행정분야: 국방 분야의 인사업무와 행정시스템은 AI 적용에 필요한 데이터 확보와 플랫폼 구축이 무기체계에 비해 상대적으로 용이하여 다양한 부분에서 AI 기술이 쉽게 적용되어 국방 운영의 효율성을 증대시키고 있다. 주요 사례로는 우수인재 획득 및 최적임자 추천, 취업지원 등 다양한 서비스 제공이 가능한 스마트 인재관리 시스템이 있으며, 방대한 진급 심사자료를 단시간에 효율적으로 분석 및 제공이 가능한 디지털 진급심사제도 등이 있다. 또한 장병들의 정신전력 향상을 위한 정신전력 교육지원시스템과 온라인 정보를 실시간 검색 및 수집할 수 있는 온라인 정보분석 시스템 등의 행정 서비스 분야에도 AI 기술을 활용하고 있다.

[그림 2-12] AI기반 스마트 인재관리시스템

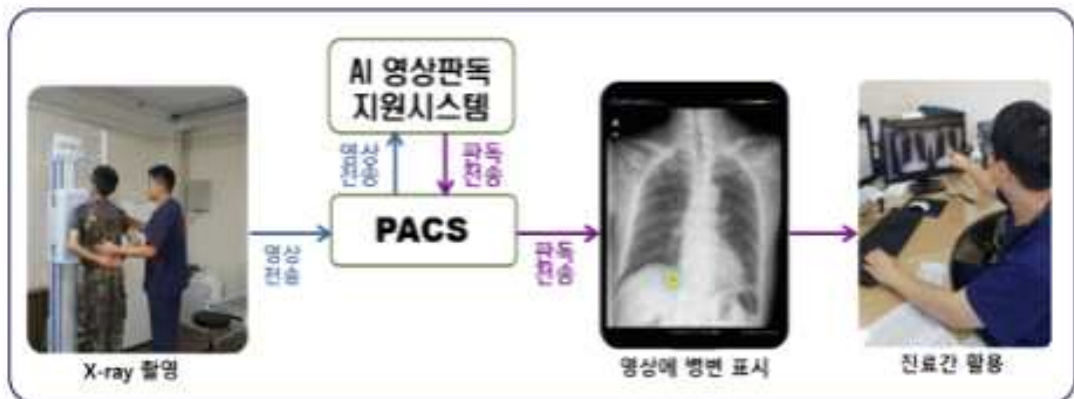


출처: 미래국방 2030 AI 기술전략(국방기술진흥연구소, 2022)

2) 의무분야: 의무분야의 AI 기술은 각종 질병의 진단을 신속하고 정확성 높게 진단하며, 환자의 상태를 보다 정밀하게 평가하여 효율적인 건강관리를 지원하는데 주로 활용되고 있다. 주요 사례로는 X-Ray, CT, MRI 등의 영상에서 질환여부 및 종류의 판독을 수행하는 '영상판독 시스템'이 있으며, 장병들의 정신적/심리적 상태를 추정하고 필요시 상담 및 치료로 연계시키는 '스마트 케어 시스템' 등이 있다. 전시에는 생체 데

이터(음성, 영상 등)를 기반으로 신체 이상증상 신호 분석을 통해 환자 상태를 파악하고 진료등급을 계산하여 응급처치를 지원하는 ‘AI 기반의 환자분류 시스템’이 있으며, 대량 전상자 발생 및 재난사태 발생시 환자 관리와 신속한 응급처치 지원이 가능한 ‘AI 기반 응급의료시스템’ 등의 구축을 위해 연구가 진행되고 있다.

[그림 2-13] AI 기반 의료영상 판독시스템



출처: 미래국방 2030 AI 기술전략(국방기술진흥연구소, 2022)

3) 군수분야: 다양한 국방자원(장비, 물자, 탄약, 급식 등)은 다른 분야와 달리 특성상 매일 또는 수시로 많은 양의 데이터가 생성되고 있기 때문에 AI를 활용시 운용의 효율성과 생산성을 극대화 시킬수 있는 분야중에 하나이며, 현재 우리 軍은 국방자원의 군수운영 효율화를 위해 무인화 및 자율화 기반의 ‘스마트 군수혁신’을 추진중에 있다. 몇가지 사례를 살펴보면 먼저, 시설운영과 물류 측면에서는 전체 정비공정의 실시간 모니터링을 통해 생산성 및 품질향상이 가능한 ‘스마트 팩토리’가 있으며, 입고, 출고, 보관 등 전체 프로세스의 자동화 및 지능화 시스템 구축을 위한 ‘스마트 물류센터’와 최적의 경로 추천 및 실시간 관제업무 수행이 가능한 ‘스마트 수송운영 관리체계’등이 있다. 예측시스템 측면에서는 수요 및 정비소요를 예측하여 선제적으로 대응할 수 있는 ‘수리부속 수요 예측 시스템’과 ‘軍 시설 안전에 대한 예측 시스템’, ‘전·평시 의무물자 소요산정 모델’, ‘상태기반 정비체계’ 등이 개발되어 활용될 것으로 예상된다.

[그림 2-14] 스마트 물류센터 사례



출처: 미래국방 2030 AI 기술전략(국방기술진흥연구소, 2022)

4) 기타(스마트부대 및 경계작전 등) 분야: AI, 빅데이터, 5G 등 4차 산업혁명 기술을 부대운영 분야에 적용하여 경계작전, 병력관리, 시설관제 등 부대운영 전반의 효율성 향상에 활용하고 있다. AI 기반의 과학화경계작전체계는 전방의 GOP 지역의 각종 센서(중·근거리 카메라, 투과레이다, 레일로봇, 열영상 감시장비 등)를 거점단위의 작전센터에서 통합운영하여 작전의 완벽성을 향상시킬 계획이며, 부대 경계작전 체계는 다양한 센서의 데이터를 통합 분석하여 감시 오탐율을 최소화하고 부대 경계작전의 자동화 및 무인화를 추진할 예정이다.

[그림 2-15] 육군 5사단 AI 경계작전센터 내부 모습



출처: 'GOP의 눈' AI 경계작전센터에 가다. 보도자료(2024.5.)

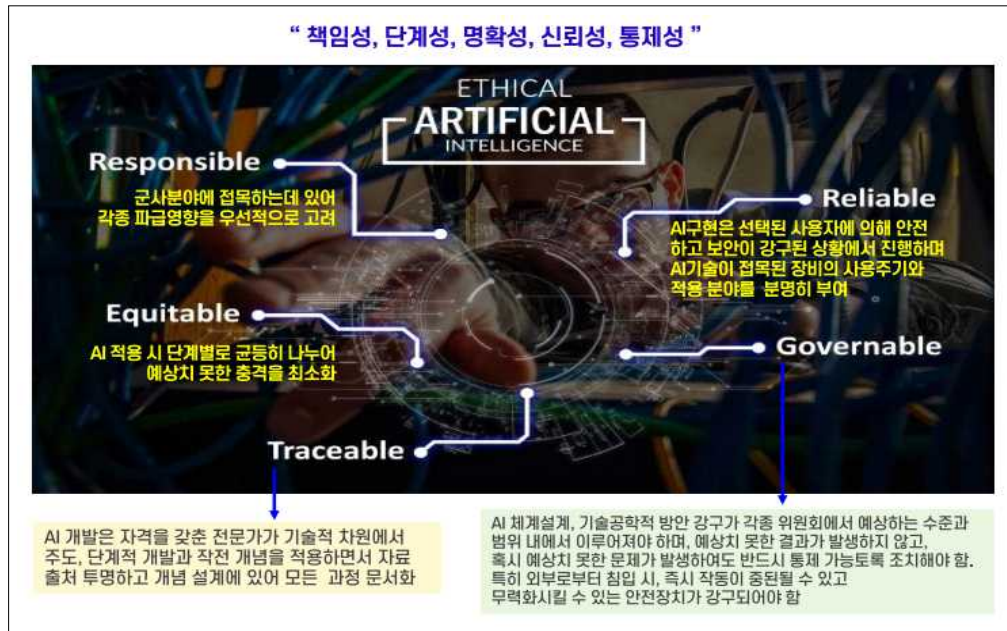
제 3 절 안전하고 신뢰성 있는 AI의 실현

(1) AI 윤리기준(원칙)의 필요성

AI는 인간과 유사한 형태로 인식, 판단, 학습 등의 지능을 인공적으로 생산해 내는 기술이다 보니 인간에게는 매우 유익한 기술이면서도 동시에 인간에게 심대한 피해를 입힐수도 있는 특징을 지니고 있다. 인간에게는 윤리¹²⁾라는 규범이 있어서 사회의 각 생활 영역에서 나타나는 문제점들에 대해서 분석하고 해결방안을 모색하여 교육과 실천을 통해 지켜 나아갈 수 있도록 하고 있으나 반면에 AI는 인간과 같은 윤리 또는 도덕적 규범이 존재하지 않기 때문에 신뢰성에 있어서 여러 가지 문제점들이 대두되고 있다. 이에 따라 이러한 AI를 개발하고 적용하는 데 있어서 다양하게 발생하고 있는 문제점들을 식별하고 인간의 윤리나 도덕적 규범과 같은 관점에서 AI도 윤리 개념이 필요하다는 인식이 생겨 AI 윤리에 관한 연구가 국내외적으로 활발하게 진행되고 있다. 해외 주요 기관에서 제시하고 있는 AI 신뢰성 또는 윤리와 관련된 개념을 살펴보면 먼저 국제표준화 기구(International Organization for Standardization, ISO)에서는 AI 신뢰성을 크게 가용성, 회복탄력성, 보안성, 안전성, 프라이버시, 책임성, 통합성 등으로 구분하여 제시하고 있으며, 경제협력개발기구(Organization for Economic Cooperation and Development, OECD)에서는 AI 신뢰성을 지속 가능한 사회와 인간 중심의 가치에 부합할 수 있도록 투명성, 설명가능성, 견고성, 안전성 등으로 구분하여 제시하고 있다. 또한 美 국립표준연구소(NIST)에서는 AI 신뢰성의 특성을 정확성, 탄력성, 객관성, 보안성, 설명가능성, 안전성 등으로 구분하고 있으며, 유럽위원회(European Commission, EC)에서는 AI의 신뢰성을 합법성, 기술적·사회적 견고성 등으로 구분하여 제시하고 있다. 이 밖에도 많은 기업과 대학에서 AI 신뢰성(윤리)에 관한 연구를 진행하고 있는 가운데 국방 분야 AI 개발에 선도적 위치에 있는 미국은 국방성(DARPA) 주도하에 AI 윤리적 발전을 위한 5가지 원칙을 공식적으로 채택하였으며, 세부 내용은 아래의 [그림 2-16]에서 보는 바와 같다.

12) 윤리: 사람으로서 마땅히 지키거나 행해야 할 도리, 표준국어대사전

[그림 2-16] 美 국방성의 AI 윤리원칙(5가지) 기준(2020.2.)



출처: 2024 세계신안보포럼 라운드테이블 제시내용(외교부, 2024.10.)

이와 더불어 우리나라에서는 2020년에 아래 [그림 2-17]과 같이 사람이 중심이 되는 인공지능(AI) 윤리기준¹³⁾을 발표하여 각 분야에 AI 적용시 활용하기 시작하였으며, 결국 AI 윤리는 신뢰할 수 있는 AI를 개발하고 적용하기 위해 AI가 반드시 갖추어야 할 핵심 요소이고, 이를 실천할 수 있는 이론적이고 합리적인 실천 지표가 제시되어야 한다.

[그림 2-17] 사람이 중심이 되는 인공지능(AI) 윤리기준



출처: 과학기술정보통신부, 인공지능 윤리기준(2020)

13) 과학기술정보통신부와 정보통신정책연구원에서 제정, 2022

(2) 안전하고 신뢰성 있는 AI 활용을 위한 거버넌스 체계 정립

안전하고 신뢰할 수 있는 AI 활용을 위해 세계 주요국들은 AI 거버넌스 체계의 중요성을 인식하여 하루라도 빨리 체계를 구축하고 관련 제도를 정립해 나아가기 위해 많은 노력을 기울이고 있다. 최근에는 잠재적 위험성과 안보 문제 등의 우려로 군사 분야 AI의 거버넌스에 대한 논의가 국내외적으로 활발하게 이루어지고 있어 국방 분야에 적용을 위한 AI 거버넌스에 대한 개념과 중요성, 원칙 등에 관한 연구사례를 분석해 본다.

(가) AI 거버넌스의 개념: AI 툴과 시스템이 안전하고 윤리적으로 유지되도록 보장하는 가드레일 역할을 하며, 안전, 공정 및 인권 존중을 보장하기 위해 AI 연구, 개발 및 활용을 안내하는 프레임워크, 규칙 및 표준을 수립한다. 혁신과 신뢰를 촉진하면서 편향성, 개인정보 침해 및 오용과 같은 위험을 해결하는 감독 매커니즘을 포함하고, AI 거버넌스에 대한 윤리적 AI 중심 접근법은 AI 개발자, 사용자, 정책 입안자 및 윤리학자를 포함한 광범위한 이해관계자들이 참여해야 하며, AI 관련 시스템이 사회의 가치에 맞게 개발되고 사용되도록 보장하여야 한다. 또한 AI 거버넌스는 인간 개입으로 인해 AI 생성 및 유지 관리에 발생하는 내재적 결함을 해결하며, AI는 인간이 개발한 고도로 설계된 코드와 머신러닝의 산물이기 때문에 인간의 편견과 오류에 취약하다. 거버넌스는 이러한 위험을 완화하기 위한 구조화된 접근방식을 제공하여 결함이 있거나 유해한 결정을 방지하기 위해 머신러닝 알고리즘을 모니터링, 평가 및 업데이트 한다.¹⁴⁾

(나) AI 거버넌스의 중요성: AI 기술이 대중화되고 다양한 분야에 적용되기 시작함에 따라 관련규정을 준수하며, 신뢰성을 확보한 가운데 부작용이 없이 활용되려면 AI 거버넌스가 반드시 필요하다. 최근 Chat GPT가 대중화된 이후 몇 년 사이에 국내외적으로 다양한 챗봇이 소셜 미디어를 통해 전파되면서 잘못된 학습결과에 따라 여러 가지 형태의 부작용이 발생하여 AI 및 이와 유사한 소프트웨어의 편향성이 세간의 이목을

14) AI 거버넌스란 무엇인가?(팀 무치 외 1인, 2023.11.)에서 내용 참조
<https://www.ibm.com/kr-ko/topics/ai-governance>

끝게 되었으며, 이로 인해 발생하는 피해를 방지하고 대중의 신뢰를 유지하기 위한 건전한 AI 거버넌스의 필요성이 강조되고 있다. 이러한 사례는 AI나 이에 준하는 소프트웨어가 적절한 통제 없이 활용될 경우 사회적으로 큰 파장을 일으킬 수 있으므로 통제가능한 AI의 활용 측면에서 AI 거버넌스의 중요성이 높아지고 있음을 알수 있다. 결국 AI 거버넌스는 AI가 인간의 존엄성이나 가치, 생명 등을 침해하지 않도록 보장하는 것을 목표로 하고 있으며, 윤리기준(원칙)을 토대로 안전하고, 책임있는 AI 기술의 성장을 촉진하는 방향으로 나아가고 있다.

(다) AI 거버넌스 원칙: 조직은 AI 기술을 개발하고 광범위하게 활용하는데 있어서 자기 자신과 소비자를 보호하기 위해 원칙을 만들고 필수적으로 도입을 추진하고 있는데 해외 글로벌 IT기업과 美 정부기관에서 규정하여 활용하고 있는 대표적인 AI 거버넌스 원칙 사례는 아래의 [표 2-2]에서 보는바와 같다.

[표 2-2] 기관별 AI 거버넌스 원칙

구 분	AI 거버넌스 원칙
IBM (美 IT기업)	• 공감: AI가 모든 이해관계자에게 미치는 영향을 예측하고 대처 • 편향성 제어: 학습데이터를 엄격하게 검토하여 공정하고 편견 없는 결정을 보장 • 투명성: 조직은 AI 기반 결과의 논리와 추론을 설명 • 책임성: 높은 기준을 수립하고 준수하며, AI의 영향에 대한 책임을 짐.
美 백악관 행정명령	• AI 안전 및 보안: AI 시스템의 안전성과 신뢰성 보장을 위한 툴 및 테스트 개발 • 개인정보 보호: 개인정보를 보호하는 기술의 개발 및 활용을 우선 • 형평성과 인권: AI가 다양한 분야에서 차별과 편견을 악화시키는 것을 방지 • 소비자, 환자 및 학생 보호: 생명을 구하는 의약품 개발 • 근로자 지원: AI가 일자리와 직장의 해로운 영향을 완화하기 위한 원칙 개발 • 혁신과 경쟁 촉진: 숙련된 AI 전문가의 미국 진출을 촉진 • AI 분야의 글로벌 리더십: 국제 파트너와 중요한 AI 표준의 개발 및 구현을 촉진 • 정부의 AI 사용: AI 전문가 채용 가속화를 통해 정부의 책임감 있는 AI 배포 보장

출처: AI 거버넌스란 무엇인가?(Tim Mucci 외 1인, 2023.11.)

(3) AI의 책임있는 군사적 이용의 노력

우리나라 외교부와 국방부의 공동 주관으로 2024년 9.9.~10. 간 「2024 인공지능의 책임있는 군사적 이용에 관한 고위급회의(이하 ‘2024 REAIM 고위급회의¹⁵⁾」가 성황리에 진행되었다. REAIM 고위급회의는 2022년 11월 한·네덜란드 정상 간 합의에 따라 AI의 군사적 이용이 국제 평화와 안보에 미치는 영향에 대한 이해를 제고하고 관련 국제규범 형성 과정에 기여하고자 출범한 국제 다자회의체이다. 제1차 REAIM 고위급회의는 2023년 2월 네덜란드 헤이그에서 한국과 네덜란드가 공동으로 주최하여 미국과 중국 등 61개국의 정부 관계자들과 국제기구 등 약 2,000여 명이 참가하였다. 1차 회의를 통해 AI의 군사적 의사결정을 인간이 완전히 신뢰하기에는 아직 기술적 발전에 제한이 있다는 것을 확인하였으며, 인간의 개입, 통제와 감독이 반드시 동반되어야 하고 AI가 사용하거나 처리, 생산하는 데이터 관련 정보활동에 있어서 국제규범은 적용되어야 하며, AI의 군사적 문제에 대응하는 일은 국가뿐 아니라 모든 이해당사자가 대응해야 할 당면한 도전으로 인식될 수 있어야 하는 ‘공동 행동 촉구서’에 서명하고 “국제법에 따른 의무와 국제 안보와 안정, 책임성을 훼손하지 않는 방향으로 군사용 AI를 개발하고 사용하는 데 전념하겠다”라고 선언을 하여 국제규칙 제정 논의의 시작을 알리는 계기가 되었다. 제2차 REAIM 고위급회의는 2024년 9월에 서울에서 개최되었으며, 우리나라를 포함하여 네덜란드, 싱가포르, 케냐, 영국 등 5개국이 공동 주최국으로 참여하였다. 이번 회의에는 90여개국의 정부 대표단과 국내외 국제기구, 학계, 산업계, 시민사회, 청년 등을 포함하여 약 2,000명이 참석하여 국제사회에서 높은 관심과 기대를 모았다. 이번 2차 서울 REAIM 회의는 군사용 AI의 개발과 사용 그리고 인간의 통제와 규범을 구축하는데 있어서 이해당사자들의 공조를 역설한 1차 헤이그 REAIM 회의의 답변에 대한 성격으로 국제사회의 실천을 촉구하는 가이드라인인 ‘행동을 위한 청사진(Blueprint for Action)’을 발표¹⁶⁾하여 AI 규범과 거버넌스 형성을 위한 구체적인 행동과

15) 2024 REAIM 고위급회의: Responsible AI in the Military domain (REAIM) Summit 2024

16) 2024 AI의 책임있는 군사적 이용에 관한 고위급회의(REAIM) 결과 보도자료(2024.9.10.)

실천을 위한 논의의 장을 만들었다.

개회식에서 우리 정부의 김용현 국방부 장관은 AI가 군사 분야에 적용되면서 軍의 작전 능력을 비약적으로 향상시켰으나 오남용에 의한 심각한 피해도 초래할 수 있는 양날의 검과 같은 특성을 가지고 있다고 평가하면서 군사 분야 AI의 책임있는 이용에 대한 균형 잡힌 이해와 국제사회의 협력이 필요하다고 강조하였다. 특히 3개의 세션(소그룹회의)에서는 구체적인 행동과 실질적인 이행을 위해 각계각층의 전문가들이 다양한 주제에 대해 활발한 논의를 시행하였다.

[그림 2-18] 2024 REAIM 고위급회의 개회식



먼저 1세션에서는 ‘AI가 국제평화와 안보에 미치는 영향’을 주제로 AI가 국제 전략 환경, 특히 분쟁 역학과 대량살상무기(WMD) 확산에 미칠 수 있는 잠재적인 영향을 평가하고, AI의 군사적인 이용이 가져올 혜택과 위험에 대해 고찰하였으며, 2세션에서는 ‘군사 분야 AI의 책임 있는 이용 이행방안’에 대해 논의하였고, 참석자들은 AI의 책임 있는 군사적 이용을 위해 필요한 주요 원칙과 조치를 식별하고, 책임성, 신뢰성, 투명성 등 일반적인 원칙을 구체적인 행동으로 전환할 수 있는 방안을 모색하였다. 3세션에서는 ‘AI 미래 거버넌스 구상’에 대한 토론이 이루어졌으며 참석자들은 AI의 책임 있는 군사적 이용을 위한 국제 거버넌스 발전 방향과 국제협력 증진 방안 등에 대해 논의하였다.

[그림 2-19] 2024 REAIM 고위급회의 소그룹회의



그림 I. ‘군사적 의사결정에서 AI의 책임있는 사용보장’에 대한 소그룹회의



그림 II. ‘AI 무기체계의 시스템 수준 평가방안’에 대한 소그룹회의

또한 특별 세션은 두 차례에 걸쳐 개최되었으며, 첫 번째 특별 세션은 마이크로소프트(Microsoft), 네이버(Naver), 스탠퍼드대학교 등 산업 및 학계의 주요 인사들이 ‘정책 입안자가 알아야 할 AI의 요체’라는 주제하에 발전 방향에 대한 식견을 나누었고, 두 번째 특별 세션에서는 한국의 KAIST, 영국 방산기업 BAE Systems, 교황청 그레고리오 대학교 등 기술 공학 관련 인사들이 모여 책임 있는 AI를 위한 정책을 공학적·기술적으로 구현하는 방안을 모색하였다.

정부대표 라운드테이블에서도 네덜란드, 싱가포르, 케냐 등의 국방장관 및 90여 개국 정부 대표들이 모여 군사 분야 AI 관련 ‘기본 원칙과 우선 순위’, ‘우려 사항 및 과제’, ‘국제협력 전망’ 등에 대한 의견과 해안을 공유하였다.

우리 정부의 조태열 외교부 장관은 폐회사에서 이번 2차 REAIM 고위급 회의를 통해 국제사회의 노력과 해안이 담긴 결과물으로써 ‘행동을 위한 청사진(Blueprint for Action)’을 발표하였으며, 이 청사진에는 공동 주최국들과 총 20개 조항으로 이루어진 국제사회의 실천을 촉구하는 가이드라인이 반영되어 있다. AI의 군사적 사용에 대한 규범을 다루는 이번 청사진은 먼저 △軍의 상황인식과 정보 분별력 증진 및 평화구축에의 기여 등 아직 완성되지 않은 AI 기술이 세계평화와 안보에 끼치는 긍정적 영향을 인정하는 동시에, △군사용 AI 기술의 위험에 대한 현대 국제사회의 이해와 예측이 불완전하며 △AI가 대량살상무기(WMD)의 확산을 촉발해서는 안 될 것과 군축·비핵화와 같은 국제사회의 노력에 기여해야 함을 강조하였다. 또한 전 세계 각국이 처한 서로 다른 안보 환경으로 인해 각국 AI의 군사적 사용에 대한 시각이 서로 상이하므로, 향후 AI 군사 규범 논의는 누구도 배제하지 않는 개방된 형태여야 함을 강조하였다. 다양한 각국 입장을 반영한 열린 거버넌스를 가동하기 위해서는 개발도상국의 AI 역량 구축이 전제되어야 한다. 국가 간 AI에 대한 지식의 격차가 좁혀져야 규범 구축 논의에 참여할 수 있기 때문이다. 아울러 제시된 청사진은 향후 AI의 군사적 이용에 대한 거버넌스는 AI 알고리즘을 결정 짓는 데이터에 대한 거버넌스 논의를 동반해야 하고, AI 기술의 빠른 발전에 상응하는 융통성 있고 균형 잡힌 현실적인 거버넌스가 필요함을 강조했다.

제 4 절 주요국의 AI 군사적 활용 전략 및 정책

(1) 미국의 국방 AI 전략 및 정책

(가) 국방 분야 AI 전략 추진배경: 2010년대 초중반 미국은 과거에 자신들이 누렸던 압도적인 국방과학기술의 우세성이 더 이상 보장받을 수 없다고 판단하고, 경쟁국(중국, 러시아 등)과 국방과학기술의 간격을 다시 벌리기 위해 2014년 척 헤이글 국방장관에 의해 레이건 국방포럼(RNDF: Reagan National Defense Forum)에서 제3차 상쇄전략(Third Offset Strategy)을 발표한다. 4차산업혁명의 핵심 분야인 IT 분야에서 빅데이터, 알고리즘, 컴퓨팅 파워 등의 발전이 혁신적으로 이루어짐에 따라 국방과 안보 분야에서 AI 활용에 대한 전략적 가치의 중요성을 조기에 깨달았으며 민간분야에서 IT 신기술의 급속한 발전 추세를 간파하고 신속히 국방 전략(NDS: National Defense Strategy)에 AI와 무인, 자율무기 등의 첨단기술을 반영하여 국가적인 차원에서의 노력을 기울이게 되었다.

(나) 국방 AI 관련 조직의 설립과 정책의 흐름: ①美 국방부의 가장 우선순위가 높은 디지털 과제를 해결하기 위해 2015년에 국방디지털서비스(DDS: Defense Digital Service)팀을 설립하였다. 어떠한 분야에 긴급한 문제가 발생하거나 AI를 적용하여 문제해결이 필요한 조직이나 영역을 지원하기 위해 AI 및 데이터 분야의 기술자들로 구성된 집단을 설립하였으며, 주로 인공위성 발사 지원, 드론 개발 및 대응, 민감한 데이터 확보, 군인 및 민간인이 사용하는 디지털 서비스 관리 등의 임무를 수행하고 있다. ②2016년에는 국방부(DoD)의 전사적인 다중 도메인 데이터, 분석, 의사결정 지원이 가능한 AI 플랫폼인 ADVANA를 설립하였다. ADVANA는 국방부(DoD) 사용자에게 공통 비즈니스 데이터, 의사결정 지원분석 및 데이터 도구를 제공하는 데이터 및 분석 플랫폼으로써 수백 개의 비즈니스 시스템에서 데이터를 가져와 데이터를 검색, 이해 및 사용할 수 있도록 지원하고 데이터 저장소의 역할도 수행하며, 국방 AI 전략에 맞는 다양한 분

석 기능을 제공한다. ③국방 데이터의 관리와 조직의 프로세스 개발을 주도하기 위해 2018년에 최고데이터책임관(CDO: Chief Data Officer)를 설립하였다. 국방 분야의 데이터 수집, 사용 권한 등 데이터 관리를 총괄하는 조직으로써 향후 최고디지털AI책임관(CDAO: Chief Digital AI Officer)으로 통합되어 AI 영역의 조직과 연계하여 AI 발전을 효과적으로 지원하는 임무를 수행하고 있다. ④국방부와 각 군에서 분산적으로 수행해 오고 있는 AI 업무를 통합하여 효과적인 거버넌스를 구축하고 국방의 AI 구심점 마련을 위해 2018년에 국방부 內 예하의 조직으로 합동AI센터(JAIC: Joint Artificial Intelligence Center)를 설립하였다. 주요임무는 AI 지원기능 제공을 가속화하고 국방 분야 전반에 걸쳐 AI 영향력을 확장함과 동시에 합동군의 군사적 우위를 달성하기 위한 AI 활동을 보장하고 있다. 마지막 ⑤全 국방조직에 대한 AI 지배력을 강화하고 AI 조직의 위상을 제고시키며, 데이터의 장벽 해결과 혁신적인 AI의 신속한 적용을 위해 조직을 통합하고 AI 거버넌스를 강화하는 차원에서 2022년에 최고디지털AI책임관(CDAO: Chief Digital AI Officer)을 창설하였다. 국방 행정으로부터 전장에 이르기까지 全 국방영역의 데이터, 분석, AI 채택과 적용의 가속화를 총괄하는 국방의 데이터 및 AI의 최고 거버넌스 조직으로서 임무와 역할을 수행하고 있다. 위에서 언급한 5가지의 AI 관련 조직 중에 우리 軍의 국방 AI 발전에 벤치마킹이 될 수 있는 합동AI센터(JAIC)와 최고디지털AI책임관(CDAO) 운용 사례에 대해서 좀 더 구체적으로 분석하여 본다.

[그림 2-20] 최고디지털AI책임관(CDAO) 설립(2022)



출처: CDAO 홈페이지(www.ai.mil)

(다) 합동AI센터(JAIC: Joint Artificial Intelligence Center)¹⁷⁾

1) JAIC 1.0의 비전은 “AI 적용을 통해 美 국방부를 변화시킨다(Transform the Department of Defense through AI)”이다. 이는 美 국방부가 적대국들의 위협에 맞서 안보와 번영을 보장하고, 첨단과학기술 분야에 우위를 지속적으로 유지하기 위해 군사 영역과 국방 운영 전반에 걸쳐 국방의 개혁과 혁신의 수단으로서 AI를 인식하고 있다는 메시지를 잘 보여주고 있다.

2) JAIC의 목표는 ①AI 핵심기술 식별을 위한 국방정책 수립 ② 지도부 인식수준 변환 ③각 소요군에 적용방법 수립 ④기존 장비 및 무기체계와의 보완적 관계수립 등 4가지를 설정하여 추진 중에 있다.

3) JAIC의 수행업무는 AI 핵심기술을 신속하게 적용, 국방부에 적용할 범위 선정, 악성 사이버 공격에 대비한 방책 강구, AI 도입의 공동 기반체계 구축, 방산업체와 대학, 연구기관, 동맹국 및 파트너십 국가 간 협력체계 구축, 전문인력 양성, AI 채택에 따른 윤리와 안전장치 강구 등이 있으며, 분야별 세부 내용은 아래의 [표 2-3]에서 보는 바와 같다.

[표 2-3] 합동AI센터(JAIC) 분야별 주요임무

구 분	주 요 내 용
플랫폼 관리	• JCF(Joint Common Foundation) 운용 및 관리 ↳ 국방 AI 개발 및 시험평가를 위한 보안 클라우드 기반 플랫폼
사업수행	• 중요한 군사 임무(정보, 군수, 방호, 의무 등)에 AI 적용을 위한 사업 추진 * Maven Project: 영상인식 AI를 드론에 적용하여 이용한 표적 식별 및 공격
시험평가	• 개발된 AI에 대한 군사 임무에 활용 가능여부 판단
대외협력	• 산학연 및 동맹국 AI 관련 부서와 기술교류, 정책 수립 등을 위한 협력 * AI Partnership for Defense 개최(한국, 미국, 일본 등 14개국 참가)

출처: CDAO 홈페이지(www.ai.mil)

17) 국방 인공지능센터 창설 및 운영방안 연구 자료(2023.4.)에서 내용 참조

4) JAIC가 설립된지 2년이 경과하며 美 국방부(DoD)의 가치를 극대화하고 합동군 전쟁에 대한 AI 지원을 위해 2020년에 ‘JAIC 2.0’으로 조직을 재편성하고 임무와 역할을 재정립하였다. 구체적으로는 ① 보안, 예산 책정, 재무, 계약 및 물류 분야의 애플리케이션을 위한 AI 개발 및 배포, ② AI 제품 및 서비스에 있어서 더 스마트하고 효과적인 조달자가 될 수 있도록 교육, ③ 동맹국 및 파트너 국가에 있는 AI 인재 허브에 대한 이해와 모니터링, 그리고 연결을 주도, ④ AI 접근방식, 알고리즘 및 교훈에 대한 서비스, 기관 간 국제적 공유를 위한 구심점 역할, ⑤ 소수의 AI 프로젝트에 대한 자체적 해결, ⑥ AI 알고리즘을 해킹하거나 중단하기 위한 적대적 머신러닝 기법의 실험과 테스트 주도 등 6가지 방법을 통해 軍의 AI 사용 가속화를 추구하고자 하였다.¹⁸⁾

5) 2020년 JAIC 2.0 전환 이후 각 소요군과 전투사령부가 필요로하는 AI의 요구사항을 식별하여 적용하는 초점을 두었으며, 임무와 역할도 초기에 비해 보다 구체화 되고, 다양한 분야로 업무영역이 확대되었다. JAIC 2.0 전환시 조직은 총 5개 부서로 편성되었으며, 부서별 수행 업무와 역할을 구체적으로 살펴보면 ① 참모(운영)부에서는 인사, 행정지원, 시설, 법률고문, 보호 및 대응 등의 업무수행, ② 사업, 예산 및 획득부에서는 사업계획, 사업분석, 작전연구, 예산, 획득계획, 계약 등의 업무수행, ③ 전략 및 정책부에서는 전략 및 소통, 기술정책, 국제문제, 전략적 인적자본 등의 업무수행, ④ 제품 부에서는 데이터 및 AI, 시험평가 및 산정(감정), JCF¹⁹⁾ 운영 등의 업무수행, ⑤ 임무 부에서는 미션 인게이지먼트(전략적 참여), 작전 및 교육, 합동 전투작전, 비즈니스 프로세스 혁신, 위협 감소 및 보호, 전투원 건강, 합동군수, 합동정보전 등의 업무를 수행하고 있다.

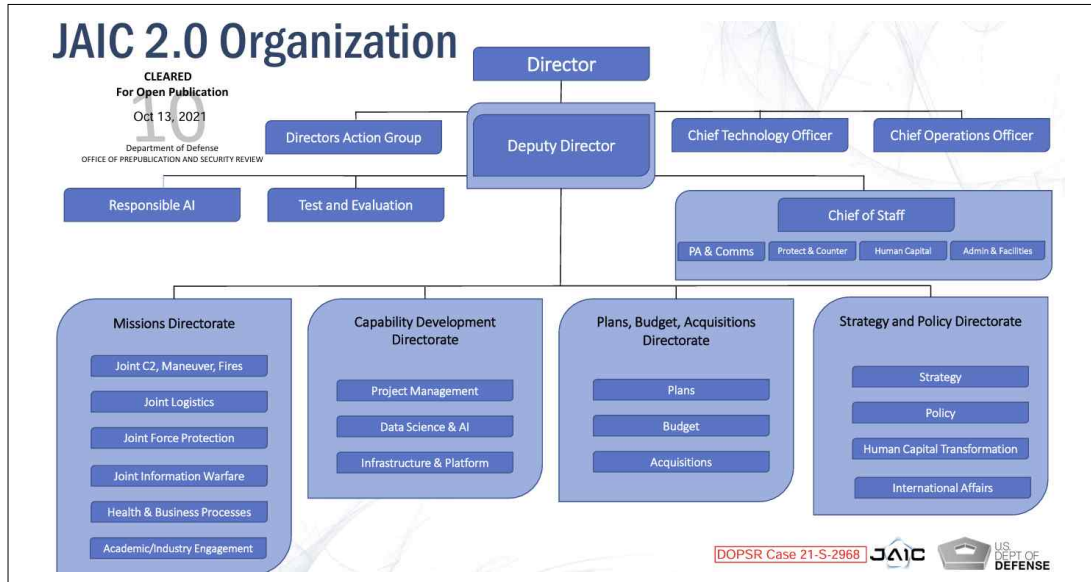
6) 2021년에는 JAIC 2.0 전환시 편성되었던 5개 부서중에 AI 제품부를 요구능력(전투)발전(Capability Development Directorate) 부서

18) 합동AI센터(JAIC)가 軍의 AI 사용을 가속화할 수 있는 6가지 방법에서 참조
(<https://www.defenseone.com/ideas/2021/01/pentagons-ai-hub/171721/>)

19) JCF(Joint Common Foundation): 軍 전체의 사용자가 안전한 환경에서 국방부 데이터에 접근하고 AI 솔루션을 개발할 수 있도록 클라우드 기반 플랫폼으로 AI 도구의 테스트 및 채택을 가속화하기 위한 국방부(DoD) 차원의 개발

로 변경하여 사용자의 요구를 식별하고 구체화하는 등 임무의 중요성을 강화하였으며, 그 외의 부서별 조직도는 아래의 [그림 2-21] 에서 보는 바와 같다.

[그림 2-21] 합동AI센터(JAIC) 2.0 조직도



출처: https://www.ai.mil/docs/JAIC_2.0_org_chart_09_2021.pdf

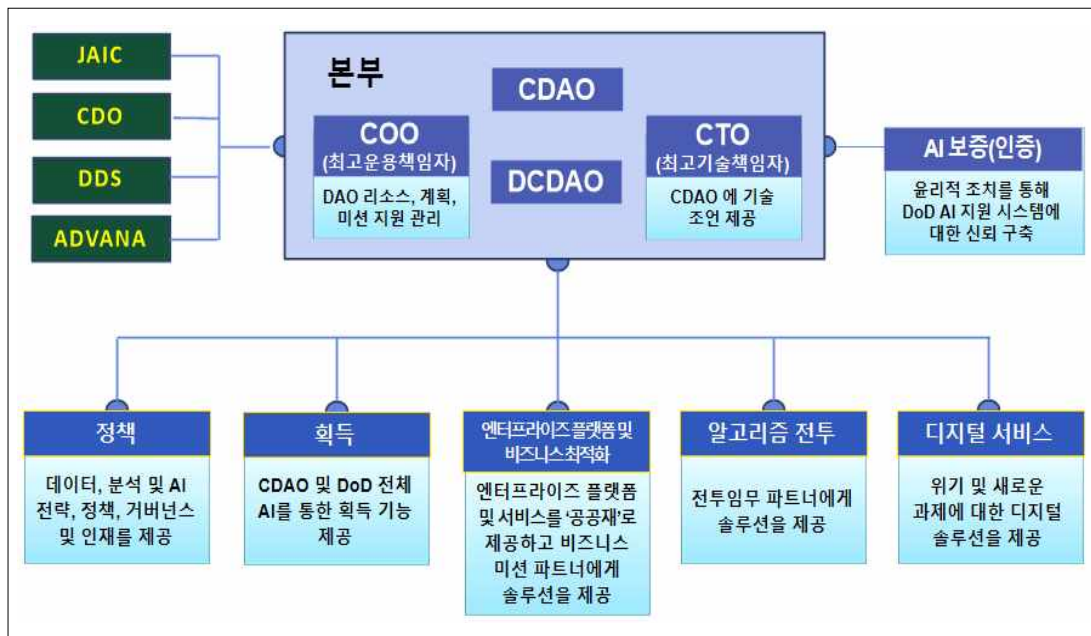
(라) 최고디지털AI책임관(CDAO: Chief Digital AI Officer)²⁰⁾

1) 2018년 美 국방부(DoD)는 AI를 국방 쏠 분야에 적용 확산 하고 AI 기술 중심의 합동전력체계를 구축하고자 ‘국방 인공지능 전략서 (Department of Defense Artificial Intelligence Strategy)’를 발표했으며, 그해 ‘합동AI센터(JAIC: Joint Artificial Intelligence Center)’를 창설하여 AI를 국방 업무에 적극적으로 도입하기 시작했다. 그리고 2022년에는 합 동AI센터(JAIC)를 포함하여 최고데이터책임관(CDO: Chief Data Officer), 국방디지털서비스(DDS: Defense Digital Service), AI 데이터 플랫폼을 관할하는 ADVANA 등 4개 조직을 통합하여 최고디지털AI책임관(CDAO: Chief Digital AI Officer, 이하 ‘CDAO’)을 신설하는 대규모 조직개편을 단행하였다. CDAO는 의사결정의 우위를 확보할 수 있도록 美 국방부

20) 국방 인공지능센터 창설 및 운영방안 연구 자료(2023.4.)에서 내용 참조

(DoD)의 국방 행정으로부터 전장에 이르기까지 전 국방영역에서 AI와 데이터 분석, 디지털 서비스 등을 총괄하는 국방 AI의 최고 거버넌스의 조직이다. CDAO의 주요 기능으로 AI에 대한 국방부(DoD)의 정책과 획득에 관여, AI 및 디지털 지원 솔루션의 개발 및 배포를 위한 플랫폼 운영, 전투 임무 솔루션 제공, 긴급 과제의 신속대응을 위한 디지털 서비스 제공 등이 있으며, 세부 조직도는 아래의 [그림 2-22]에서 보는 바와 같다.

[그림 2-22] 美 국방부 CDAO 조직도



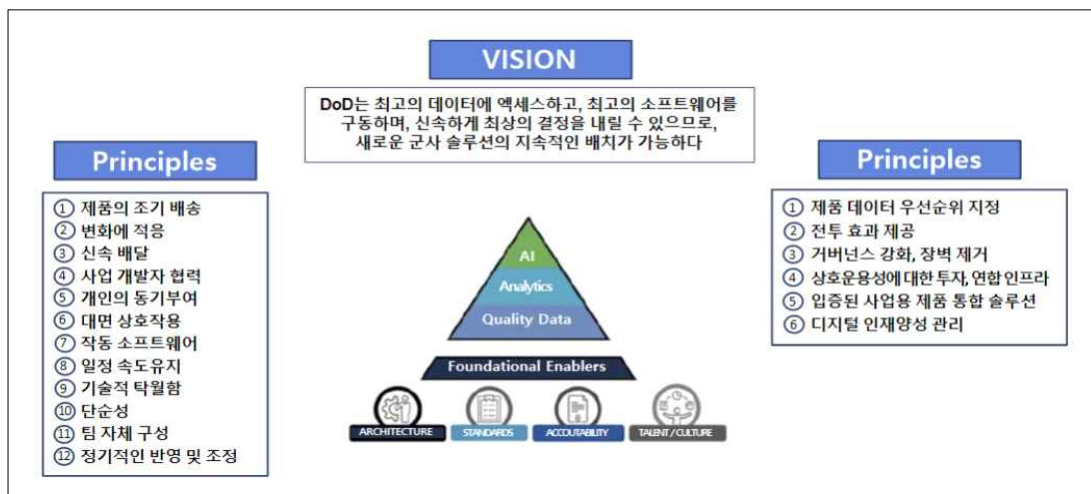
출처: 해외 주요국의 국방 AI 현황 연구(이지은 외 2인, 2023.3.)

2) CDAO는 美 국방부(DoD)의 AI 데이터 분석, 디지털 서비스 등의 총괄 조직으로서 책임있는 AI 및 데이터 전략 수립과 생태계 구현, 그리고 책임있는 AI 전략 및 구현경로((Responsible Artificial Intelligence Strategy & Implementation Path, 이하 RAI S&IP)를 발표하였다. RAI S&IP는 윤리, 투명성, 책임성, 인권을 우선시하는 AI 시스템 개발 및 구축을 위한 계획이며, 이 전략과 경로에는 AI 시스템의 개발, 테스트 및 배포를 위한 지침과 이러한 지침의 준수를 모니터링하고 보장하기 위한 메커니즘이 포함되어 있다. 이 전략과 지침은 민관군, 산학연 등의 이해관계

자들이 협력하여 개발하였으며, 모두가 공유할 수 있도록 거버넌스 구조를 포함하고 있다.

3) 또한, 美 국방부(DoD)는 AI 윤리원칙을 공식화하고 AI 프로젝트 자금을 늘렸으며 AI 및 데이터 생태계를 구성하였다. AI 윤리원칙은 책임성, 형평성, 추적성, 신뢰성, 통제성 등에 대해 구체적으로 정의하고 있다. 이처럼 미국은 CDAO를 신설하여 거버넌스 체계를 갖추고 RAI S&IP를 통해 AI의 책임있는 활용성을 추구하고 있으며, 민간군 산학연 등과 광범위한 협업체계를 구축하여 다양한 AI 및 데이터 플랫폼을 운영하며, 각 소요군 및 전투사령부를 지원하고 있다. CDAO의 데이터, 분석 및 AI 적용 전략은 아래의 [그림 2-23]에서 보는 바와 같다.

[그림 2-23] CDAO의 데이터, 분석 및 AI 적용 전략



출처: 해외 주요국의 국방 AI 현황 연구(이지은 외 2인, 2023.3.)

(2) 영국의 국방 AI 전략 및 정책

(가) 영국 정부는 2021년 9월 10년 동안 AI 분야 연구 및 혁신 초강대국 달성을 위해 AI 국가전략인 ‘NAIS(National Artificial Intelligence Strategy)’를 발표하였다. 영국의 경제환경과 국민의 삶을 개선하고 새로운 국가전략을 통해 AI를 기반으로 회복력, 생산성을 향상하고 민간과 공공 부문을 혁신하기 위해 AI 국가전략의 3대 목표를 다음과 같이 제시하

였다. 첫째 AI 생태계의 수요 변화에 따라 장기적으로 투자하고, 관련 계획을 수립하여 과학과 AI 분야 강국으로서의 리더십을 유지하며, 둘째 AI 기반 경제로의 전환을 지원하고, 모든 경제 부문과 지역에 혜택이 돌아가도록 보장하며, 셋째 혁신과 투자를 장려하고, 공공의 근본적 가치를 보호하기 위한 국내외 AI 기술 권리 거버넌스를 확보하는 것이다. 전략적인 관점에서 보면 AI 발전에 필요한 인력, R&D, 자본 등 핵심적인 요소에 대해 수요 중심의 맞춤형 전략을 영국의 現 상황에 맞게 잘 수립하였으며, 거버넌스 관점에서는 혁신전략 및 데이터 전략 등 각종 전략을 AI를 중심으로 데이터, 컴퓨팅, 클라우드 거버넌스와 연계하여 통합적인 거버넌스를 마련하여 AI 기술 표준화 정립을 추진하고 있다.²¹⁾

(나) 정부의 AI 국가전략을 토대로 영국 국방부(MOD)는 2022년에 ‘국방 인공지능 전략’을 발간하였다. 국방부(MOD)는 “AI 측면에서 우리 규모에 비해 세계에서 가장 효과적이고 효율적이며 신뢰할 수 있고 영향력 있는 국방 조직이 되는 것이다”라고 비전을 선언하였으며, 이를 위한 세부 전략을 아래의 [표 2-4]와 같이 제시하였다.

[표 2-4] 영국 국방부의 국방 AI 비전 달성을 위한 세부 전략

구 분	세부 전략
효과성	• 전투에서 승리할 수 있는 능력과 지원기능을 제공하고, 영국의 동맹국 및 AI 생태계와 협력하고 파트너십을 맺을 수 있는 능력
효율성	• 기술을 혁신적으로 사용하여 기능을 제공하고, 운영을 수행하고, 조직 전체에서 생산성 이점을 실현
신뢰성	• 대중, 파트너 및 직원들의 신뢰를 받아 AI 시스템의 아전과 신뢰성, 그리고 우리의 핵심 가치에 따라 합법적이고 윤리적인 AI 사용에 대한 명확한 약속을 제공
영향력	• AI 기술의 글로벌 개발을 형성하고 AI 관련 문제를 긍정적인 방향으로 관리하고, 협력하고, 모범을 보임

출처: 영국 국방부 국방 인공지능 전략(2022.6.)

21) THE AI REPORT 2021(NIA AI 미래전략센터, 2021)에서 내용 참조

(다) 또한 국방 AI 전략을 위해 아래의 [표 2-5]에서 보는 바와 같이 4가지 목표와 이를 추진하기 위한 조치 및 행동사항을 제시하였다.

[표 2-5] 영국 국방부의 국방 AI 목표

구 분	세부 전략
목표 1	- 국방부를 ‘AI 지원’ 조직으로 전환한다 * 조치: 리더와 인력의 기술을 향상하고 핵심 인재를 모집하며, 정책적 과제를 해결하고 디지털, 데이터 및 기술 인에이블러를 현대화한다
목표 2	- 국방 우위를 위해 속도와 규모에 맞게 AI를 채택하고 활용한다 * 행동: 성공을 위해 조직하며, 단기적이고 장기적인 기회를 활용하며, 체계적인 실험 및 국제적으로 협력한다.
목표 3	- 영국의 국방 및 보안 AI 생태계를 강화한다 * 조치: 자신감을 구축하고 요구사항을 명확히 하며, 사업적 장벽 해결, 참여와 공동 창작 장려, 비즈니스 성장을 지원한다
목표 4	- 안보, 안정성 및 미주적 가치를 증진하기 위해 글로벌 AI 개발을 구체화한다 * 조치: 책임감 있는 글로벌 AI 개발을 옹호하고, 보안과 안정성을 촉진하며 향후 보안 정책을 개발한다

출처: 영국 국방부 국방 인공지능 전략(2022.6.)

(라) 영국 국방AI센터(DAIC) 설립 및 운영

1) 판도를 바꿀 수 있는 AI의 힘을 활용하고 부서 전반에 걸쳐 AI 기능에 대한 일관된 이해와 개발을 가속화하기 위해 2022년 4월에 국방AI센터(DAIC, Defense AI Center, 이하 ‘DAIC’로 칭함)를 설립하여 운영하기 시작하였다. DAIC는 영국 국방부의 AI 핵심 조직으로서 다음과 같은 임무를 수행한다. 첫째 비전을 제시하는 허브 역할을 수행하여 국방 전반에 걸쳐 AI 개발 및 사용을 옹호하며, 둘째 전략적 이점에서 돌파구를 창출하는 AI 프로젝트의 신속한 개발, 제공 및 확장을 가능하게 하고 조정하며, 셋째 광범위한 국방에 대한 공통 서비스로서 소 방위 디지털·데이터 서비스 및 전문 지식 소스에 대한 액세스를 제공한다.

2) DAIC는 AI 핵심 조직으로서 3가지 주요기능(임무)을 수행하기 위해서 다음과 같은 주요업무를 수행한다. 첫째 사용자가 AI를 신속하고 규모에 맞도록 프로토타입을 개발하고, 테스트, 보증, 배포를 용이하게 해주는 조언과 지원, 도구 및 서비스를 제공하며, 둘째 AI 전문직 책임자를 지정하고 AI 지식, 기술 및 경력 개발을 지원함으로써 국방 전반에 걸쳐 AI에 대한 이해를 개선하며, 셋째 AI 지원 시스템의 테스트, 보증, 인증 및 규제를 위한 프레임워크 구축하며, 넷째 軍용 AI 애플리케이션부터 행정관리 시스템에 이르기까지 사내 제품 파이프라인 및 제품 팀과 함께 다양한 AI 기술을 연구하고 AI 개발을 가속화하며, 다섯째 정부, 국제 파트너 및 동맹국, 산업 및 학계의 파트너를 포함하여 군대를 지원하기 위해 최고의 태도와 협력적인 조직으로 임무수행을 준비한다.

3) DAIC의 거버넌스는 국방부 본부와 DAIC, 전략사령부 등 3개 기관으로 분리되어 있으며 세부 담당분야는 아래 [표 2-6]에서 보는 바와 같다. 거버넌스의 구성과 함께 DAIC는 국방부의 기존 조직인 국방디지털실(Defense Digital), 국방과학기술연구소(DSTL), 군수장비·지원실(Defense Equipment & Support) 소속의 미래능력그룹(Future Capability Group)간의 협력을 주도하며 국방 AI 가속화의 구심점 역할을 수행하고 있다.

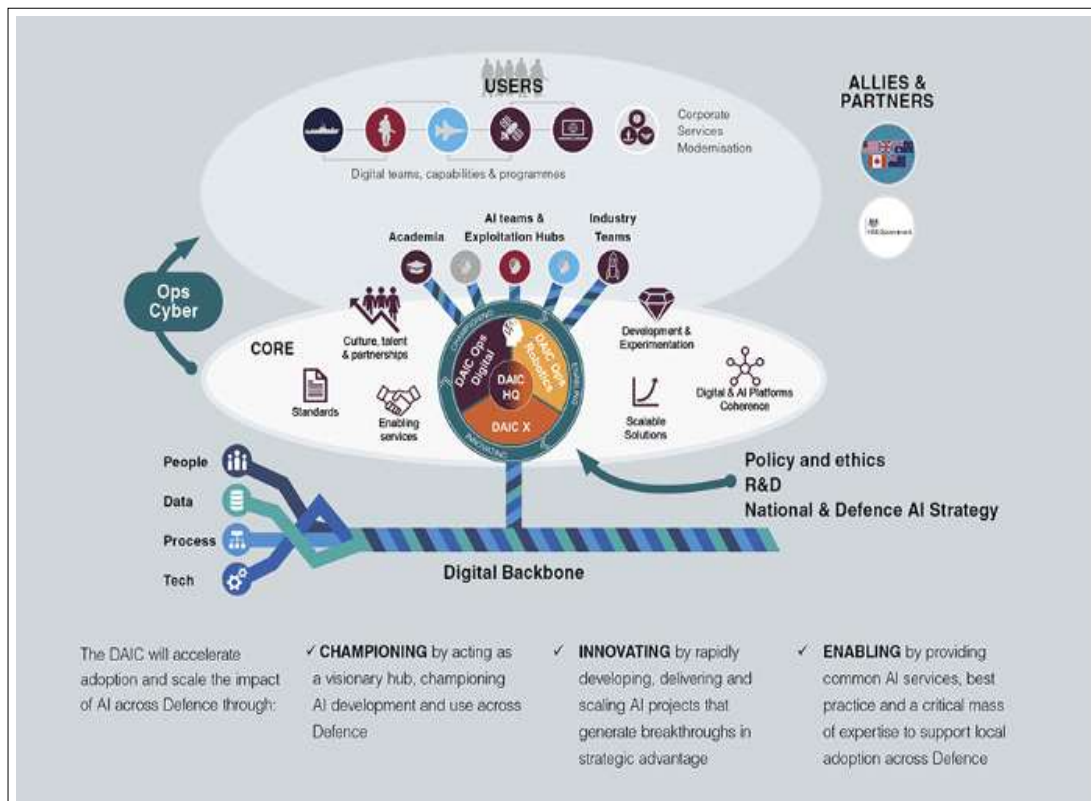
[표 2-6] 국방AI센터(DAIC) 거버넌스

구 분	거버넌스 담당분야
국방부(MoD) 본부	AI 정책 및 전략 설정, 기능 목표 정의, 전략 프로그램 지시 및 전반적인 일관성 보장
DAIC 사업부/기능 책임자	AI 전략 및 본부 지침에 따라 가장 관련성이 높은 AI 형태 추구
전략사령부 (국방디지털)	전투 영역 전반에 걸쳐 전략 및 작전 통합을 보장

출처: 영국 국방부 국방 인공지능 전략(2022.6.)

4) AI 기반체계로서 디지털 백본(Digital Backbone, 중추망)과 디지털 파운드리(Digital Foundry)를 구축함으로써 AI와 국방 데이터를 융합하여 힘을 발휘하고, 규모와 속도에 맞게 AI를 개발 및 활용할 수 있도록 지원하는 지원 및 제공부서로 국방 전반에 걸쳐 AI의 영향을 확장하기 위해 아키텍처를 구상하였으며, 세부 사항은 아래의 [그림 2-24]에서 보는 바와 같다.

[그림 2-24] 영국 국방AI센터(DAIC) 아키텍처 다이어그램²²⁾



출처: 영국 국방부 국방 인공지능 전략(2022.6.)

22) DAIC 아키텍처 다이어그램: DAIC는 디지털 백본(Digital Backbone, 중추망)에서 출발하며 사람, 데이터, 프로세스, 기술 등 4가지로 구성되어 있다. DAIC의 중심에는 본부를 중심으로 DAIC Ops Digital, Robotics, DAIC X 등으로 둘러싸여 있으며 외부의 핵심 책임분야로는 서비스 활성화, 문화와 인재 및 파트너십, 개발 및 실험, 확장 가능한 솔루션, 디지털 및 AI 플랫폼의 일관성 등이 있다. 외부로 나아가서는 학계, 산업 팀, AI 팀 및 사용자 커뮤니티의 익스플로잇 허브와 협력하고 있다. 정리하자면 DAIC는 국방 전반에서 AI 개발 및 사용을 총괄하는 허브기관으로서의 최고리더(챔피언)로서 군사적이고 전략적인 측면에서 우위 확보를 위해 돌파구를 만드는 AI 개발 및 사용을 옹호하고 AI 프로젝트를 신속하게 개발, 제공 및 확장하여 국방혁신을 추진하며, 공통의 AI 서비스, 모범 사례, 그리고 전문지식을 제공하여 국방 전반에 걸쳐 현지 채택을 지원함으로써 영향력을 확대해 나아가고 있다.

(3) 독일 연방청의 국방 AI 전략 및 정책

(가) 독일 정부는 2018년 최초로 「국가 AI 전략(KI²³⁾ Strategie²⁴⁾」을 수립하여 범정부 차원에서 해당 업무를 추진 중이며, 이를 토대로 각 부처별로 AI 전략 구현을 위한 업무추진과 30억 유로(한화 약 4조 원) 규모의 대규모 예산 투자를 계획 중에 있다. 국방부는 「국방업무 영역에서의 AI 활용」 개념서를 발간하여 적용 중이며, 연방 경제/에너지부 주관 AI 로드맵 연구를 추진해 나아가고 있다. 다만, 미국, 영국 등 인공지능 분야의 군사적 활용에 선도적인 국가들과는 달리, 독일은 AI의 군사적 활용에 대한 정치적인 논란과 인간이 개입되지 않는 수준의 첨단무기 사용에 대한 부정적 여론으로 인해 AI 관련분야의 대외적인 활동과 업무 추진에 있어서 다소 소극적인 자세를 취하고 있다.

(나) AI 관련 軍 연구기관(조직) 현황

1) 독일 육군은 2019년 육군발전 청이 중심이 되어 다음의 [그림 2-25] 독일군 인공지능(KI) 업무 관련 조직도와 같이 AI 관련 업무추진을 위한 조직을 구상하였다. 부서별 주요임무로 육군발전처의 AI 실무조직은 육군 내 AI와 관련한 제반 업무를 조율하는 주요 조직으로 연구조직과 산업체 간의 업무 조율 및 협업 촉진 역할을 수행하며, 육군 AI 개발센터와 육군 AI 데이터센터는 AI 분야의 업무지원을 담당하고 있다. 추가적으로 사이버 정보군 예하에 연방군디지털센터²⁵⁾가 설치되어 연방군 전체의 디지털 관련 업무 전반을 담당하고 있으며, 이와 별도로 Cyber Hub를 설치하여 연방군 전체에 대한 디지털화, 인공지능(KI) 등 최첨단기술을 연방군에 적용하기 위한 다양한 軍 개혁 과제의 개발 및 적용 노력을 진행하고 있다. 전반적으로 민간에서의 기술발전 추세가 군내 기술 개발

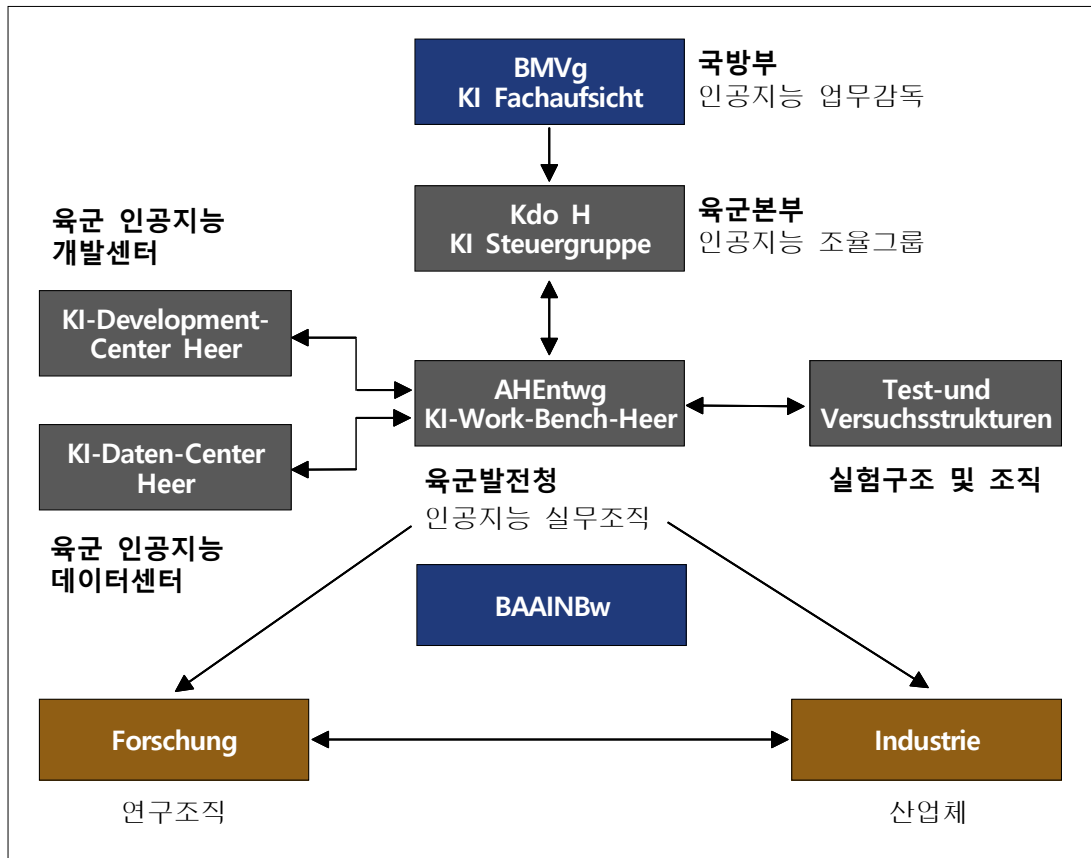
23) KI(Künstliche Intelligenz): 인공지능(AI)에 대한 독일어 원어 명칭

24) 독일 연방정부의 국가적 인공지능 전략 개정판(Fortschreibung_KI_Strategie BReg DeZember 2020)

25) Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber-und Informationsraum(ZDigBw) 센터장은 준장급으로 예하에 참모부 및 5개의 부로 구성

여건보다 매우 앞선 상황이므로 독일군은 자체적으로 관련 기술의 개발보다는 현재의 민간 기술발전 추세에 맞춰 해당 기술의 軍 내부에서의 활용 방안 등을 우선적으로 검토하고 있는 상황이다.

[그림 2-25] 독일군 인공지능(KI) 업무 관련 조직도(구상안)



출처: 독일군 「국방업무 영역에서의 인공지능 활용」 개념서(2021)

(다) AI의 군사적 활용 전략 및 발전방향

1) 연방정부의 AI 전략에 따르면 독일 정부는 5개 분야(인력, 연구개발, 전환(교육) 및 활용, 관련규범, 사회)로 구분하여 추진 중점과 향후 적용계획을 밝히고 있으며, 국방부 차원에서는 軍의 대비태세를 향상시키고, 미래의 능력을 효과적으로 유지하기 위해서 AI를 활용할 것임을 명시하고 있다. AI를 활용함으로써 현존 전투력을 강화하고, 새로운 능력을 창출할 수 있으며, 현존 AI 기술과 인간 능력간의 결합을 통해 많은

장점을 도출할 수 있을 것으로 평가하고 있다. 이외에도 AI를 통해 軍의 다양한 행정업무를 효율적으로 처리할 수 있을 것으로 평가하고 있다.

2) 현재의 기술발전 상태를 고려시 군사적 영역에서 AI는 작전 수행간 상황과악 및 의사결정과정을 지원하기 위한 데이터의 분석 및 처리를 지원할 수 있을 것으로 보고 있다. 최근 몇 년전에 독일 지휘참모대학에서는 AI를 적용한 부대지휘절차(한국군의 전술적계획수립절차)를 주제로 세미나를 실시한 적이 있으며, 이 세미나에서는 ‘現 AI 기술수준을 기반으로 계획수립절차의 일부과정에 적용시 성과가 있다’라는 내용이 발표되기도 하였다.

3) 향후 가까운 미래에는 정찰, 지휘 및 지원영역 전반, 플랫폼(무기·장비) 사용간 효율성 제고가 가능할 것으로 평가되고 있으며, AI를 적용할 수 있는 예상 분야로서 선제적 위협 평가 및 조기경보체계, 정찰시스템(센서 데이터) 자동화 처리, 영상정보 평가 및 처리, 무인 또는 자동화 정찰 및 효과(무기)체계의 운용, 자동화된 상황평가, 작전간 적(방책) 시뮬레이션, 의사결정 지원, 사이버 위협 분석 및 방어, 무기체계(센서 체계와의 연결) 운용, 자동화된 통역체계, 자동화된 방호체계(방공, 적 공중 공격에 대한 대응조치, 차량 능동방호 對 IED, 드론방어) 등이 있을 것으로 판단하고 있다.

4) 육군발전청의 AI 입장문서(Positionsapier KI in den LaSK)에 따르면 독일 육군은 우선 영상 분석분야, 전술 USA(무인비행체) 운용, 차세대 BMS(Next Generation Battle Management System), 물자 및 인프라 분야, 평가(분석)절차 개선 등 5개 중점분야를 설정하여 추진을 준비하고 있으며, 연방군계획청에서는 AI의 군사적 활용 가이드북 등 AI 관련 다양한 연구 및 검토를 진행 중에 있다.

(4) 중국의 국방 AI 전략 및 정책

(가) 중국은 비대칭 전력의 지속적 강화를 통해서 미국 3차 상쇄전략에(Third Offset) 대응할 수 없음을 인식하고, 향후 미래전장에서의

핵심은 AI·우주·사이버 등 첨단과학기술 분야가 될 것임을 확신하여 2030년까지 중국이 AI 컴퓨터 기술에서 세계를 선도할 목적으로 국무원 주도하에 아래의 [표 2-7]에서 보는 바와 같이 2017년에 ‘당의 차세대 AI 개발계획’을 수립하여 추진할 것을 발표하였다. 이를 달성하기 위해 중국군이 채택할 수 있도록 軍과 民이 겸용으로 활용할 수 있는 기술개발을 꾸준히 강조하였으며, 특히 데이터를 중국의 전략적인 자산으로 인식하여 2030년까지 세계 데이터의 30%를 보유할 수 있도록 목표를 수립²⁶⁾하였으며, 어떠한 국가도 데이터에 접근할 수 없도록 통제하고 있다.

[표 2-7] 중국의 차세대 인공지능 발전계획

구 분	세부내용
1단계 (2017~2020)	중국의 AI 산업을 글로벌 경쟁업체와 비슷한 수준으로 발전시키는 것이며, 이를 위해 AI 산업을 새로운 경제성장 축으로 육성하는 전략
2단계 (2021~2025)	일부 AI 분야에서 세계 최고에 도달하는 것을 목표로 하고, 이를 위해 중국의 산업고도화와 경제발전을 선도하는 주요 원동력으로 지능사회 건설을 추진하는 데 기준점 설정
3단계 (2026~2030)	글로벌 AI 혁신의 중심센터로 도약하는 것으로, 인공지능의 글로벌 거버넌스에 적극적으로 참여·추도하려는 의지를 포함

출처: 국방분야 인공지능 기술 도입의 주요쟁점과 활용 제고방안(윤정현, 2021.8.)

(나) 중국 공산당과 중국군은 현대의 IT 힘의 활용을 통해 미군이 보여주었던 다양한 능력들에서 심대한 영향을 받았으며, 정보화 전쟁, 지능형 전쟁에 대한 중요성에 대해 점진적으로 중요성을 인식하게 되었다. 이에 따라 시진핑은 2017년 19차 당대회에서 2020년까지 인민해방군이 기계화와 정보화로 군사력을 제고하고, 2035년까지 현대화를 추진하여 2050년에는 세계 일류의 강한 군대를 만든다는 강군몽(强軍夢) 달성 계획을 발표²⁷⁾하기도 하였으며, AI를 4차산업혁명 시대 글로벌 강국을 만드

26) Algorithmic Warfare Applying Artificial Intelligence to Warfighting(Peter Layton, 2018)

27) 4차 산업혁명시대 중국의 군사혁신: 군사지능화와 군민융합(CMI) 강화를 중심으로(차정미, 2020)

는 핵심기술로 인식하고 군사력 현대화의 방향을 ‘지능화(知能化) 군’ 건설에 맞춰 활발하게 추진하고 있다. 중국은 미국을 능가하는 초강대국이 되기 위해 AI에 많은 노력을 기울이고 있으며, 민간 및 군사용 모두에 지대한 관심을 가지고 있다. 이를 위해 AI 기술에 반드시 필요한 클라우드 컴퓨팅, 빅데이터, 양자 기술 및 무인시스템 등의 군사적 운용을 통해 ‘지능화(知能化)전쟁’을 수행할 수 있는 강한 군대를 육성하겠다는 목표를 가지고 있다.²⁸⁾

(다) 2024년 현재 중국의 AI 기술은 각종 통계에서 미국에 이어 세계 2위의 수준에 있는 것으로 알려져 있다. AI 기술에는 인식, 판단, 결심, 무인, 자율주행 등 여러 가지 분야가 있는데 그중에 특히 안면인식, 자연어처리, 자율주행 등과 같은 일부 분야에서는 이미 미국을 앞서가고 있는 것으로 알려지고 있다. 국방 분야의 AI 조직이나 편성 등에 대해서는 공개된 정보는 없으나 AI 개발을 위한 다수의 연구센터가 있으며, 그 연구센터들의 상당수는 국가의 AI 산업, 특히 군사적 목적을 위해 설립된 것으로 보고 있다. 오래전부터 인민해방군, 특수전사령부 등 일부의 주요 군부대에 AI 연구센터를 설립하여 운용 중인 것으로 알려져 있으며, 대다수의 방산업체와 대기업은 국가 시책으로 AI 연구소를 운영하고 있고, 정부의 지침에 따라 드론, 로봇, 무인, 자율무기 등 AI 기술 전환 관련 연구 과제를 다수 수행하고 있는 것으로 알려지고 있다. 주요 사례로는 국립 국방기술대학교(NUDT)에 위치한 국방기술핵심연구소는 자율시스템, 빅데이터, 클라우드 컴퓨팅을 포함한 군사 애플리케이션을 위한 AI 기술 개발을 수행하고 있으며, 중국에서 가장 큰 국영 방산회사 중 하나인 중국 전자기술회사(CETC)가 설립한 국방과학기술 산업연구센터(DSTI) 역시 매우 대규모로 지휘통제 시스템, 물류시스템, 정보·감시·정찰(ISR) 시스템 등 군사용 AI 기술 개발에 주력하고 있다.²⁹⁾

28) 중국이 AI를 활용한 군사력 증강을 목표로 하는 방법, Javin Aryan, This is the 119th article in the series – The China Chronicles

29) 국방 인공지능센터 창설 및 운영방안 연구: 중국의 국방 인공지능 정책 목표와 전략 (국방기술학회, 2023.4.)

(5) 러시아의 국방 AI 전략 및 정책

(가) 러시아는 2008년부터 국방의 현대화 계획에서 AI에 대한 투자 계획을 구상하고, 2025년까지 군사장비의 30%를 자동화하기 위한 계획을 수립하였다. 2017년 푸틴 대통령은 “AI 기술을 독점하여 수많은 정보를 효과적으로 식별하여 실시간으로 의사결정을 할 수 있는 국가가 세계를 지배하게 될 것이다”라고 선언³⁰⁾하면서 러시아의 AI 발전을 위해 훈련 프로그램, 입법적 지원, 민관 협력, 스템(STEM: 과학(Science), 기술(Technology), 공학(Engineering), 수학(Mathematics)분야) 발전의 중요성을 강조하였다. 이에 따라 러시아 정부는 2017년 12월 모스크바 물리기술대(MIPT)에 AI센터를 설립하여 정부의 AI 기술 개발과 전문인력의 서방 국가로의 유출 차단을 위한 활동을 지원하고, 러시아의 일류 국영기업이나 민간 기업 그리고 여러 대학들과 함께 AI 분야 협력을 강화하고 있다.³¹⁾ 또한 2019년에는 2025년까지 AI 분야에서 세계를 선도하는 국가로서의 지위 달성을 위해 ‘대담한 구상(daring initiatives)’을 발표하였다.

[표 2-8] 러시아 국방부의 AI 기술 개발 관련 10대 계획

구 분	세부내용
1	러시아 과학 아카데미를 비롯한 관련 기관이 AI 기술 개발 컨소시엄 구축
2	프로그램 구축 자금을 조성하여 자동화 기술 도입
3	전문가 양성 과정 마련
4	에라 테크노폴리스(Era technopolis) 캠퍼스에 고급 AI 연구 시스템 구축
5	국립 AI 센터 설립
6	타국의 연구 및 개발 상황 모니터링
7	AI 위게임 진행
8	AI 기술에 대한 법칙 준수
9	군사전문가들과 군사 포럼 교류
10	AI 콘퍼런스 개최

출처: 미·중·러의 국방 인공지능 정책 방향과 시사점(안보전략연구센터, 2020)

30) Keith Dear (2019), “Will Russia Rule the World Through AI?” The RUSI Journal

31) EMERiCs 신흥지역정보종합포털, “러시아 AI에 주력”, 러시아 Tass 등(2019.10.)

(나) 2020년 이후 러시아의 AI 군사적 활용 추세를 보면 국방 분야에 AI 개발을 지속적으로 추진하고 있는 가운데 여러 가지 전략 및 정책 문서를 작성하고, AI 조직 생태계를 확장하며, 법적 체계 구축과 교육 프로그램을 조정하고 개발을 가속화하기 위해 광범위한 민군 기술협력을 촉구하고 있다.³²⁾ 2021년 푸틴은 극초음속, 레이저 및 로봇공학과 같은 핵심 무기시스템의 전투 기능을 향상시키는 과정에서 AI가 결정적 돌파구를 마련해줄 수 있다고 강조한 바 있으며 러시아가 AI의 군사적 활용과 군사능력 전환에 국가적인 총력을 기울이고 있는 것으로 추측된다.³³⁾

(다) 서방의 주요 국가와 마찬가지로 연방정부 차원에서 AI 기술 개발과 중장기 전략계획을 주요 국가전략으로 공표하고 이를 추진하고 있으며, 최근 러시아-우크라이나 전쟁으로 전쟁 발발 이전에 수립된 각종 계획 추진에 어느 정도의 차질이 예상되나 오히려 이번 전쟁의 경험을 바탕으로 AI의 군사적 적용과 활용 확대의 기조는 이전에 비해 보다 강화될 것으로도 예상되고 있다. 러시아-우크라이나 전쟁은 국방영역에서 AI의 보다 적극적인 적용과 활용의 유인책으로 작용하고 있다고 볼 수 있다. 즉 전장에서 입증된 유용성 외에도 AI 기반 무기시스템과 이와 관련된 첨단 와해기술(EDT: Emerging and disruptive technologies)의 발전이 러시아의 열세를 보완하는 최고의 방법으로 간주하고 있는 것으로 추정되며, 이는 결국 전장에서 AI를 적용하려는 강력한 시도와 노력으로 이어질 것으로 보인다.³⁴⁾ 러시아-우크라이나 전쟁을 통해서 러시아는 AI 기반의 무기체계를 시험하거나 전장에 직접 투입하는 사례가 언론을 통해 지속적으로 보도되고 있어 AI가 탑재된 치명적 자율무기체계(Lethal Autonomous Weapon System)의 개발이 내부에서 지속적으로 연구개발되고 있는 것으로 추정할 수 있다.³⁵⁾

32) 국방 인공지능센터 창설 및 운영방안 연구, “러시아 국방부의 인공지능 정책 목표와 전략” (한국국방기술학회, 2023.4.)

33) DIAO Report, High Hopes Amid Hard Realities, Defence AI in Russia, Katarzyna Zysk

34) 위 각주와 같음

35) “러시아軍, 우크라이나에 세계 최초 인간 살상용 로봇 ‘마커’ 투입”(2023.2.)

(6) 한국의 국방 AI 전략 및 정책

(가) 정부의 국가 AI 추진전략

1) 정부는 2019년 12월 최초로 국가 AI 전략을 수립하여 발표하였다. 주요 내용으로 2030년까지 디지털 경쟁력 세계 3위, AI를 통한 경제효과 455조원 창출, 삶의 질에 있어서 세계 10위권으로 목표를 설정하고 이를 위해 3대 분야에 9개 전략과 100가지 실행과제를 제시하였다. 2022년 5월 윤석열 대통령은 취임 후 110개의 국정 이행과제를 발표하였으며, 이중 103번째 과제는 국방분야 과제로써 ‘제2 창군 수준의 국방혁신 4.0 추진으로 AI 과학기술강군 육성’을 위한 과제이다. 국방부는 정부에서 발표한 국정 이행과제를 추진하기 위해 2023년 3월에 ‘국방혁신 4.0 기본계획’을 발표하였다. 국방혁신 4.0은 AI·무인·로봇 등 4차산업혁명 과학기술 기반으로 ①북핵 및 미사일 대응능력 획기적 강화, ②군사전략 및 작전개념 선도적 발전, ③AI 기반 핵심 첨단전력 확보, ④군구조 및 교육훈련 혁신, ⑤국방 R&D 및 전력증강체계 재설계 등을 혁신하여 경쟁우위의 AI 과학기술 강군을 육성하기 위한 계획이며, 세부 내용은 아래의 [그림 2-26]에서 보는 바와 같다.

[그림 2-26] 국방혁신 4.0의 5대 중점 및 16개 과제



출처: 국방혁신 4.0 기본계획(국방부, 2023.3.)

2) 2024년 9월 26일 윤석열 대통령은 국가인공지능위원회 출범식 및 제1차 회의에서 인공지능 3대 강국(AI G3) 도약을 위한 대한민국 AI 혁신의 청사진이 담긴 「국가 AI 전략 정책방향」을 발표³⁶⁾하였다. 전례없이 빠르고 광범위하게 발전하고 있는 AI 기술이 향후 국가안보와 경제를 좌우하며, 국가 생존과 직결될 수 있어 AI 혁신 가속화와 글로벌 AI 리더십 구축을 위해 「국가 AI 전략 정책방향」을 수립하였다. 이번에 발표한 「국가 AI 전략 정책방향」은 AI G3 국가 도약을 통해 글로벌 AI 중추 국가 실현의 비전을 제시하였고, 범국가적으로 추진해 나아갈 핵심 과제인 ‘4대 AI 플래그십 프로젝트’와 AI 생태계의 핵심인 ‘4대 분야 정책 추진방향’을 포함하고 있으며 세부 내용은 아래의 [표 2-9]에서 보는 바와 같다.

[표 2-9] 4대 AI 플래그십 프로젝트 및 4대 분야 정책 추진방향

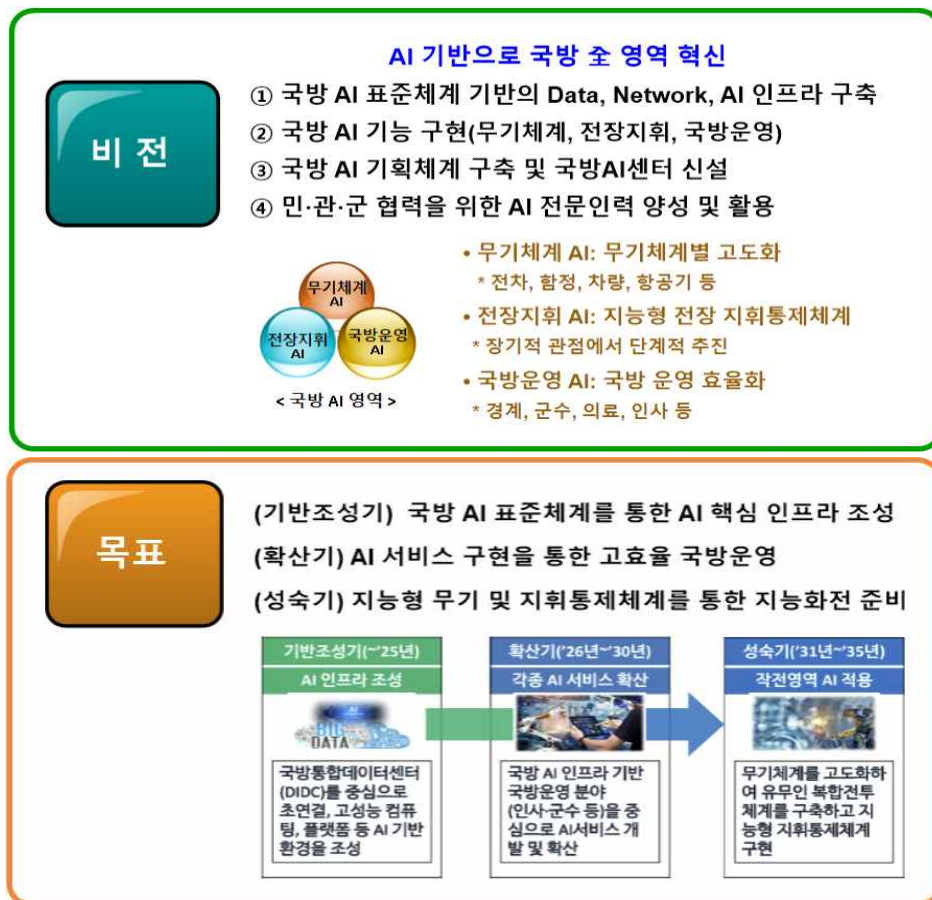
구 분	세부내용
4대 AI플래그십 프로젝트	· 국가 AI 컴퓨팅 인프라 대폭 확충 * 최신 GPU 보유규모 현재 대비 15배 향상 · 민간부문 AI 투자 대폭 확대 * 민간: 총 65조원, 정부: 투자 활성화 지원 · 국가 AX(AI+X) 전면화 * AI 도입률 산업 70%, 공공 95% · AI 안전·안보·글로벌 리더십 확보
4대 분야 정책 추진방향	· 스타트업·인재 확충 * AI 유니콘 기업 10개 육성, 20만 AI 인재 확보 · 기술·인프라 혁신 * 저작물 활용 촉진 제도개선, 트래픽·전력 수요 증가 대응 · 포용·공정기반 조성 * 디지털 포용법 제정, 질서·권리보호 기반 확립 · 글로벌 리더십 확보 * 선도국·국제기구 협력 확대

출처: 「국가 AI 전략 정책방향」 발표(과학기술정보통신부, 2024.9.)

36) 「국가 AI 전략 정책방향」 발표(과학기술정보통신부, 2024.9.26.)

(나) 국방부는 2021년부터 「국방 AI 추진전략 1.0」을 수립하여 국방 분야 AI 발전을 위한 업무를 본격적으로 추진하기 시작하였으며, 2022년에는 정부의 국정 이행과제인 국방혁신 4.0 추진과 연계하여 국방 분야 AI 적용을 위해 비전과 목표가 제시된 「국방 인공지능(AI) 추진전략 2.0」을 발표³⁷⁾하였다. 또한 2023년 4월에는 국가안보 유지, 미래전장 선도, 국가과학기술 융합 관점에서 국방목표 달성을 위해 전략적 투자 및 육성이 필요한 ‘10대 전략기술 분야’와 지능형 전장인식 및 판단, 지능형 통합 지휘결심, 국방 AI 플랫폼 등 ‘30개 국방전략기술’이 반영된 「’23~’37 국방과학기술혁신 기본계획」을 제시하였다.

[그림 2-27] 국방 AI 비전과 목표



출처: 국방 인공지능(AI) 추진전략 2.0(2022.3.)

37) 「국방 인공지능(AI) 추진전략 2.0」(국방부, 2022.3.)

(다) 육군은 AI 과학기술강군 선도를 위해 지상작전 수행개념을 바탕으로 아미타이거 전력의 3대 핵심요소인 기동화, 지능화, 네트워크화를 추진하고 있으며, 첨단과학기술 강군의 핵심인 AI를 군사적으로 운용하기 위해 다양한 부서와 기관에서 활발한 연구와 노력을 기울이고 있다. 2020년 5월에 軍 최초로 AI 발전 추진전략을 수립하여 육군 전 분야에 AI를 적용하고 육군 전반에 AI를 활용하기 위해 인프라 구축, 제도 및 정책 마련, 협력체계 구축, 기반환경 등을 구축해 나아가고 있다. 2024년 5월에는 ‘AI를 선도하는 First Mover로서 역할을 수행하며, AI를 통해 첨단과학기술로 무장된 강한 육군 육성’을 비전으로 제시하였고, AI 발전 기반을 위한 핵심 인프라 조성과 미래전장을 주도하는 육군 핵심전력 지능화를 목표로 설정하여 제시하였다. 육군의 AI 비전과 목표 구현을 위한 구체적인 추진전략은 아래의 [그림 2-28]에서 보는 바와 같다.

[그림 2-28] 육군 인공지능(AI) 추진전략



출처: 육군 인공지능(AI) 추진전략(육본 정책실, 2024.5.)

(라) 해군은 「해군 군사혁신 2045」 추진방향을 기반으로 ‘국방혁신 4.0’과 연계하여 AI 추진전략을 정립하였다. 해군전략과 미래 해군작전 개념을 구현하고, AI 과학기술 기반의 정예 해군력 건설을 위해 AI 기반의 해군 전 임무영역 혁신을 목표로 선정하였으며 목표 달성을 위해 첫째 전 임무영역 AI 적용 소요창출, 둘째 AI 발전 기반을 위한 데이터 관리 인프라 구축, 셋째 AI 전문인재 양성 및 제도개선 등 3가지 중점을 설정하였다. 세부 추진분야 및 과제는 아래의 [표 2-10]에서 보는 바와 같다.

[표 2-10] 해군 AI 추진 분야 및 과제

추진 분야	세부 과제
전 임무영역 AI 적용 소요창출	① AI 소요기획 업무 프로세스 정립 ② AI 적용 체계 자체 개발 ③ AI 적용 확산을 위한 소요발굴 생태계 조성
AI 발전 기반을 위한 데이터 관리 인프라 구축	④ 빅데이터 구축을 위한 데이터 수집 시스템 확보 ⑤ 해양·전장정보 데이터 관리 및 활용 시스템 구축 ⑥ 데이터 공유를 위한 초고속 네트워크 구축
AI 전문인재 양성 및 제도개선	⑦ 軍 특화 AI 역량 강화 교육 ⑧ AI 전용 교육장 구축 및 운영 ⑨ AI·데이터 업무 기준 정립을 위한 제도 마련

출처: 국방혁신 4.0 해군추진계획(해군 정보화부, 2022)

(마) 공군은 공군비전 2050, 공군 미래전 수행개념, 공군 기본정책서에 AI 활용 개념과 필요성을 명시하여 AI를 공군의 핵심기술로써 인식하고 공군 쏘 임무 분야 혁신에 활용을 위해 노력하고 있다. 이에 따라 2021년 5월에 ‘공군 인공지능(AI) 발전계획’을 수립하였고, ‘AI를 통한 공군 쏘 임무 분야 혁신’이라는 비전의 구현을 위해 3대 추진 목표와 9개 추진과제를 제시하였으며, 세부 내용은 아래의 [표 2-11]에서 보는 바와 같다.

[표 2-11] 공군 AI 추진 목표 및 과제

추진 목표	세부 과제
전 임무 분야에 AI 활용을 위한 소요발굴·사업화	① 공군 핵심기능 혁신을 위한 AI 소요발굴 및 사업추진 ② AI 기술 적용 임무체계 자체 개발·활용 ③ 쏘 임무 분야 AI 확산을 위한 소요기획 강화
임무 데이터의 체계적인 관리를 통한 AI 기반 마련	④ 공군 데이터 관리정책 수립 ⑤ 데이터 수집·저장·효율적 활용을 위한 인프라 개선 ⑥ AI 대응 사이버보안 정책 발전 및 역기능 해소
AI의 효율적 활용을 위한 인재양성 및 제도개선	⑦ AI 활성화·공감대 형성을 위한 교육 강화 ⑧ AI 기술 전문인력 확보를 위한 제도개선 ⑨ AI 적용 확산을 위한 공군 추진체계 확립

출처: 공군 인공지능(AI) 발전계획(공군 정보화부, 2021.5.)

제 3 장 AI의 군사적 활용시 제한사항 및 문제점

본 연구에서는 AI의 군사적 활용시 일반적 관점에서 신뢰할 수 있는 AI 개발을 위해 AI 윤리기준 인식 및 적용 측면에 대한 제한사항 및 문제점을 분석해 보고, 軍의 특수성을 고려하여 국방 도메인 영역의 관점에서 국방 AI 기반체계 구축, AI 법규, 전략 및 정책 수립, 국방기획관리기본훈령 및 정보화업무훈령의 연계성, AI 개념연구, 국방 AI 적용시 군사보안의 인식, AI 전문인력 및 조직 운영, AI 관련 軍 내부 의사결정시스템 등 軍 내·외부의 여러 가지 영향요인에 의한 제한사항 및 문제점을 식별하고 분석해 본다.

제 1 절 AI 윤리기준의 인식 및 적용 측면

(1) AI 윤리기준 및 원칙에 대한 인식

AI는 다른 소프트웨어들과는 달리 인간과 같은 지능을 지니고 있어 윤리기준 또는 원칙의 필요성에 대해서 지속적인 논의의 대상으로 여겨지고 있으며, 쏘 세계적으로 다양한 연구기관 및 국가에서 AI 윤리기준 및 원칙을 연구하고 적용하기 위해 많은 노력을 기울이고 있다. 2020년 이후 최근에는 AI의 군사적 이용에 있어서 윤리기준의 적용방안 모색을 위한 국제적 논의가 활발하게 진행되고 있으며, 앞서 2장에서 언급한 것처럼 ‘REAIM(인공지능의 책임있는 군사적 이용에 관한 고위급회의)’이라는 행사를 2023년부터 매년 개최하며 AI의 책임있는 군사적 이용을 위해 필요한 원칙과 조치사항을 식별하고, 구체적인 행동으로 전환할 수 있도록 쏘 세계의 여러 국가가 모여서 방안을 모색하고자 국제협력회의체를 신설하였다. 국내·외적으로 AI 윤리기준 및 원칙에 관한 연구가 활발하게 이루어지고 있으나 아직까지는 강제적으로 적용하기 위한 법률적 근거나 사회적 합의 등이 이루어질 수 있을 정도로 충분한 연구와 대책이 마련되어 있지 않은 실정이다. 특히 AI는 첨단과학 기술을 대표하는 분야이며, 사회의 모든 영역과 국방영역에 있어서 초일류 국가로 도약하는데 결정적 역할을

수행할 수 있는 핵심기술로써 국가 차원에서 국익이나 사회 발전을 제한할 수 있는 우려가 있어서 AI를 통제하는 법률이나 제도, 윤리기준 및 원칙 등의 제정을 적극적으로 시행하지 못하고 있다. 다행히도 2018년 OpenAI사에서 ‘GPT(Generative Pre-trained Transformer, 자연어 처리 AI모델)’가 출시되는 시점을 기준으로 AI 윤리에 관한 연구가 활발하게 진행되고 있으며, 사회 전반에 AI가 다양하게 활용되고 긍정적 요소와 부정적 요소가 나타나게 되면서부터 AI 윤리기준 또는 원칙 제정의 필요성이 적극적으로 대두되고 있다. 그러나 아직까지는 AI 윤리기준 및 원칙을 제정하고 적용해야 할 정도로 AI 기술이 다양화되고 보편화되지는 않았으며, 사회 전반에 적용하기 위해 인간의 존엄성과 공익을 증진하는 방향으로 AI 기술이 발전할 수 있도록 최소한의 기본 원칙과 핵심 요소만을 제시³⁸⁾하고 있는 가이드라인이 발표되었고, 기술의 발전 속도와 더불어 윤리기준에 대한 적용방안도 동시에 발전시켜 나아가는 전략을 추진하고 있다. 아쉽게도 우리 국방 분야에는 아직까지 AI 기술이 골고루 확산하지 않았으며, AI 적용을 위해 다양한 소요창출 및 기획, 기반체계 구축 등 역량 강화에 집중하고 있어 AI 윤리에 대한 필요성과 인식의 정도가 아직까지는 낮은 수준에 머물고 있는 실정이다.

(2) 국방 분야 AI 윤리기준 적용을 위한 개념 정립 추진

국방 분야에서도 2020년도 이후 국방부 및 각 소요 군을 중심으로 AI의 군사적 적용을 위한 AI 윤리기준(원칙) 개념연구를 활발하게 진행하고 있다. 그러나 이러한 연구는 군사용 AI 윤리기준 또는 윤리원칙(준칙) 제정을 위한 기초연구 형태로써 AI 윤리기준 관련 국내·외 동향과 주요 쟁점에 대한 분석, 향후 발전 방향에 대한 개념을 제시하는 정도의 수준으로 연구를 진행해 오고 있다. 국방 분야에 AI를 적용하는 목적은 민간분야에 AI를 적용하는 목적과 활용 방향성 측면에 있어서 차이점이 있으며, 민간에서 다양하게 연구되는 AI 윤리기준의 기본 원칙과 핵심 요소 등은 군사적 활용목적에 부합되지 않는 부분이 있고, 일부분을 제외하고 대부분은

38) 「사람이 중심이 되는 인공지능(AI) 윤리기준」(과학기술정보통신부, 2020)

적용하는데 제한사항이 많이 있어 국방부 및 각 소요군 차원에서는 적극적으로 수용하여 적용하기에 어려운 실정이다. 국방 분야의 AI는 국방 운영의 효율성을 향상시키고, 무기체계 및 전력지원체계(무기체계 지원 요소)를 지원하여 군사적 목적을 달성하는데 목표를 두고 있다. 따라서 아직까지는 AI 윤리기준을 크게 고려하지 않고 기반체계 구축에 중점을 두고 있으나, 향후 무기체계 및 국방운영 분야에 AI가 본격적으로 확산하여 적용되는 시기가 다가올 것으로 예상됨에 따라 현재의 기초(선행)연구를 확대하여 구체적인 적용방안이 도출될 수 있도록 응용 및 심화 연구의 활성화가 필요한 실정이다.

제 2 절 국방 데이터 및 플랫폼 등 AI 기반체계 측면

(1) 국방 데이터의 수집·활용·공유 등 관리체계

(가) AI는 데이터를 기반으로 컴퓨터 프로그램 스스로가 인지한 상황을 추론하고 판단한 결과를 통해 최적의 결정을 내린다. 또한, AI는 데이터를 인식하고 분류하며 다양한 의사결정의 영향 요소를 예측하고 이를 상황에 맞게 활용한다. 따라서 데이터로 학습한 결과를 분석 또는 예측하기에 AI의 성능이나 품질을 결정짓는 요소가 데이터인 것이다. 즉, 우수한 AI를 만들기 위한 재료가 양질의 데이터인 것으로, AI 연구개발을 위해서는 양질의 데이터를 대량으로 확보하는 것이 중요하다.

(나) 국방 분야에서 활용되는 국방 데이터는 크게 4가지로 분류할 수 있다. 첫째는 국방통합데이터센터(DIDC)에서 관리하는 전장관리데이터와 자원관리데이터가 있으며, 둘째는 각종 훈련센터(과학화전투훈련단, 전투지휘훈련단 등)에서 훈련 간 생산되는 훈련데이터가 있다. 셋째는 각 소요 군에서 운용 중인 무기체계 및 전력지원체계 등에서 발생하는 단일체계 데이터가 있으며, 넷째는 각급 부대에서 직무수행 간 발생하는 국방업무의 지식이 담겨 있는 기타 데이터로 분류할 수 있다. 이러한 4가지

국방 데이터들은 각 소요군 및 기관별로 별도의 체계와 방법을 통해 수집 및 관리되고 있으며, 일부 정형데이터³⁹⁾를 제외하고 대부분은 원시데이터⁴⁰⁾ 및 비정형데이터⁴¹⁾ 형태로 보관되거나 관리되고 있어 AI 개발을 위해서는 별도의 AI 학습용데이터⁴²⁾를 생산하는 과정을 거쳐야 한다. 군사용 AI 개발에 필요한 학습용데이터는 원시데이터나 비정형데이터를 정제 및 가공, 라벨링 등의 과정을 거쳐야 하는 어려움이 있는데 최초 원시데이터나 비정형데이터를 확보하는 단계에서부터 군사보안을 이유로 접근성이 떨어지고, 활용성에 있어서 많은 제약이 있어 국방에 AI를 적용하는데 근본적인 한계점(또는 문제점)으로 작용하고 있다. 최근에는 국방부 內 각 조직별로 AI 개발에 필요한 다양한 AI 학습용데이터 구축사업을 진행하여 다종의 학습용데이터를 보유하기 시작하였으나 데이터 관리의 주체가 불명확하고 보유 데이터를 타인(타 기관)과 공유할 수 있는 기준이나 관련 근거 등이 마련되지 않은 이유로 활발하게 활용되지 못하고 있다. 또한, 군사 전력의 핵심인 각종 무기체계는 비밀에 준하는 강도높은 군사보안으로 원시(비정형)데이터의 수집 및 제공이 매우 까다로워 무기체계 AI 적용에 큰 걸림돌로 작용하고 있고, 일부 감시·정찰 무기체계 및 모의훈련 체계 등은 운용 간 생산되는 데이터가 휘발성 데이터로서 저장되지 않고 운용 실시간 소멸하거나 일정 기간이 지나면 삭제되는 시스템이 적용되고 있어 데이터의 수집과 활용이 매우 어려운 실정이다. 무엇보다도 국방 AI 데이터의 수집·관리·공유(제공) 등에 대한 표준체계(표준화)가 국방부 및 각 소요 군별로 정립되지 않아 국방 분야 AI 적용 속도를 저하시키는 주요 원인 중의 하나로 보여지고 있다.

(2) 국방 AI 적용을 위한 플랫폼 등 인프라 구축

39) 정형데이터: 미리 정해 놓은 형식과 구조에 따라 저장되도록 구성된 데이터(네이버 지식백과)

40) 원시데이터: 데이터가 발생하거나 생성하는 것이 개인이나 조직에 의해 만들어지는 데이터
(네이버 지식백과)

41) 비정형데이터: 정의된 구조가 없이 정형화되지 않은 데이터(네이버 지식백과)

42) AI 학습용데이터: 머신러닝, 딥러닝 등 AI 모델 학습을 위해 활용되는 데이터를 총칭하는 것
(네이버 지식백과)

현재 국방부는 軍 내부 자체적인 AI 개발환경 구축을 위해 2024년부터 1 단계 사업으로 국방망에 국방 지능형 플랫폼을 구축하여 운영하고 있으며, 각 소요 군은 자체적인 AI 사업을 통해 AI 학습용 데이터, AI 모델, 플랫폼 구축 등을 추진하고 있다. 그러나 국방 AI 적용 활성화를 위한 소프트웨어, AI 알고리즘, 데이터, 컴퓨팅 파워 등을 통합하여 효과적으로 관리하는 AI 공통 플랫폼은 부재하며, 향후 구축 전망도 다소 불투명한 상황으로 판단된다. 관련 제도와 정책, 법규 및 규정 등의 제정과 추진의 어려움으로 AI의 3대 구성요소인 데이터, 알고리즘, 컴퓨팅 자원(플랫폼)의 효과적인 통합체계 구축이 미진한 것으로 보인다. 국방 분야의 AI 적용 활성화를 위해서는 소요창출 및 개념연구, 소요기획, 연구개발(사업수행), 운용/관리, 유지보수(고도화), 폐기 등 AI 생애주기(AI Life Cycle) 전반의 과정을 관리할 수 있는 도구 또는 시스템 구축이 필요하다.

제 3 절 국방 AI 관련 법규, 전략 및 정책 수립 측면

(1) 국방 AI 적용을 위한 각종 법령, 제도, 규정 등의 개선

정부는 AI 시대의 국가적인 AI 전략 추진을 지원하고 지능정보기술 개발과 산업 진흥을 위해 2020년에 ‘지능정보화 기본법’ 마련과 ‘데이터 3법(개인정보보호법, 정보통신망법, 신용정보법)’ 개정 등 AI 법제 개선을 추진하였으며, AI 등 신기술 및 산업에 걸림돌이 없도록 규제 샌드박스 운영, 포괄적 네거티브 전환, AI·데이터 분야 규제혁신 작업반 구성 등 규제 개선을 위한 노력을 추진하고 있다. 정부의 이러한 노력에도 불구하고, 우리 軍은 국방전력발전업무 체계상 방위사업법, 국방과학기술혁신촉진법, 국방정보화법 등 다수의 법률은 예하의 행정규칙(훈령, 규정 등)이 원활한 업무를 추진하기 위해 제·개정 할 수 있도록 개선되지 못하고 여전히 복잡한 법체계를 가지고 있는 상황이다. 정부나 국방부에서는 AI 기반의 첨단 무기체계를 조기에 적용하도록 독려하고 있으나 소요 및 획득절차, 예산 등의 업무가 나누어져 있고 관련된 지침이나 규정 등은 상위 법령에 따라 별도의 방식으로 추진되고 있으며, 제·개정이 추진되더라도 각 기관의

관점에서 제·개정 작업이 추진됨에 따라 혼란을 초래하고 있다.

(2) 국방 AI 적용을 위한 상·하급 부대의 전략 및 정책 수립

앞에 2장에서 언급하였듯이 현재 국방부 및 각 소요군은 각자 자체적으로 AI 추진전략과 정책을 수립하여 국방 분야에 AI 적용을 위해 많은 노력을 기울이고 있다. 그러나 국방부 및 각 소요군의 AI 추진전략과 정책은 상하 연계성이 부족하고, 각자가 생각하고 있는 주요 관심분야 중심의 추진전략과 정책을 수립하여 추진함으로써 노력이 집중되지 못하고 분산되어 있는 상황이다. 국방부는 기획조정실 이하의 지능정보화정책관실에서 국방 AI와 관련된 정책과 전략의 총괄적인 역할을 수행하고 있으나 무기체계, 전력지원체계, 국방행정 분야 등 국방 소 분야에 AI 적용을 위한 컨트롤타워로서 역할을 수행하지 못하고 있다. 이는 무기체계 및 전력지원체계 분야의 업무 권한과 책임, 전문성 등을 보유하지 못하여 국방 소 분야에 대한 비전과 목표 등 구체적인 업무추진 방향과 과업을 제시하지 못하는 한계점을 가지고 있기 때문이다. 아울러서 각 소요군(육군, 해군, 공군, 해병대 등)은 합참 중심의 소요를 통제하는 무기체계와 각 소요군 및 국방부에서 통제하는 전력지원체계 중심의 전력발전 업무를 수행함으로써 정보화체계 중심의 AI 추진전략과 정책을 제시하고 있는 국방부의 추진전략과 방향성을 일치하지 못하는 구조적인 문제점을 가지고 있다.

(3) AI 관련 예산을 고려한 사업 및 소요기획 추진

국방 AI 적용을 위한 연구개발 및 사업 예산은 크게 방위력개선사업과 전력운영사업으로 구분되어 추진된다. 방위력개선사업은 방위사업청 주관의 본사업(체계개발, 구매 등), 연구개발(R&D) 사업(핵심기술, 미래도전 등) 등으로 구분되어 추진되며, 전력운영사업은 대부분 국방부 지능정보화정책관실 주관의 본사업(국방정보화사업 등), 연구개발(부처협력 ICT R&D) 등으로 구분되어 추진된다. 무기체계 AI 적용을 위한 예산은 대부분 합참 통제하 방사청 주관으로 본사업 및 R&D 형태로 수행되어 국방부 지능정보화정책관실의 AI 추진전략과 연계성을 유지하기가 어려운 실정이

며, 국방부 지능정보화정책관실 주관하 집행하는 전력운영비의 국방정보화사업 예산은 AI 적용을 위한 무기체계나 전력지원체계 등 대상 체계가 없이 AI 기술만을 개발하기 위한 실험적 또는 시범사업 형태로 각 소요군 및 기관별 산발적으로 추진되고 있다. 방위사업청 주관의 AI 사업 예산은 대부분 대상 또는 목표체계 적용을 위한 본사업과 핵심기술 사업이 있어 목적성이 있는 AI 사업이 추진되는 반면 국방부 주관의 AI 사업 예산은 대부분 대상 및 목표체계가 없는 상태에서 사업이 진행되다 보니 예산 사용 대비 성과 측면에서 효율성이 많이 떨어지고 있는 상황이다. 또한 AI 관련 국방정보화사업 수행시 近 미래에 대상 무기체계 및 전력지원체계 적용을 고려하지 않은 상태에서 소요기획 업무가 추진되고 있는 실정이다.

제 4 절 국방기획관리기본훈령과 국방정보화업무훈령의 연계성 측면

(1) 국방기획관리체계와 국방정보화기획체계의 국방 AI 업무 분산

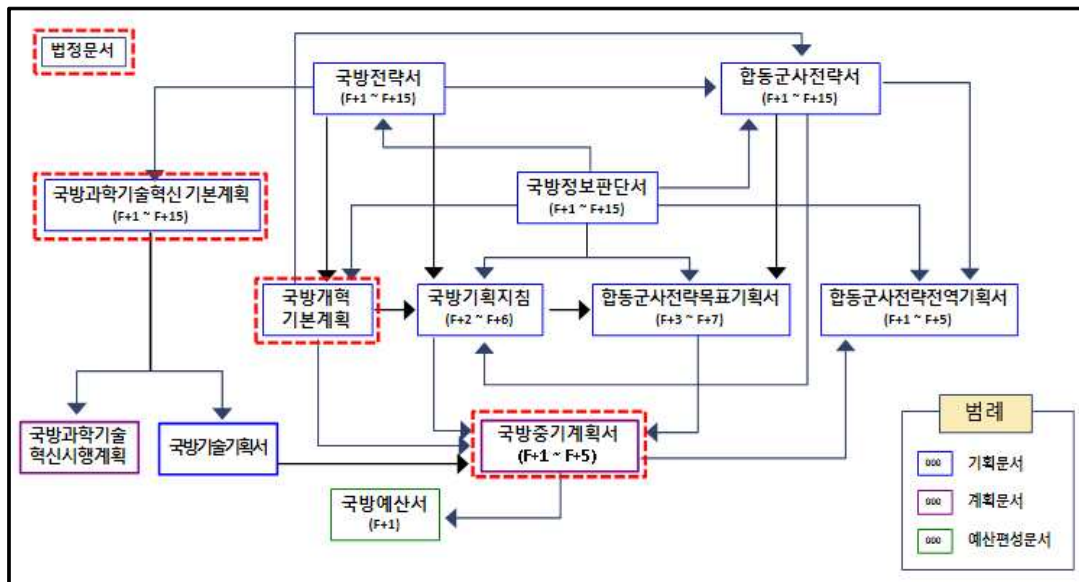
(가) 국방부 훈령 상에 국방기획관리기본훈령과 국방정보화업무훈령의 상호연계성 부족은 국방 AI 적용 추진의 걸림돌로 작용하고 있다. 국방기획관리기본훈령은 국방목표를 설계하고 군사력의 건설과 유지 및 운영 방향을 종합적·체계적으로 모색하여 국방자원을 효율적으로 관리하기 위하여 국방기획관리(PPBEE)⁴³⁾에 대한 기본방침 및 제반 절차를 규정⁴⁴⁾하고 있으며, 국방기획관리(PPBEE)에 관련된 각종 규정 및 지침에 기준이 되는 시스템으로 활용되고 있다. 국방기획관리(PPBEE)는 군사력 건설(방위력개선)을 위한 국방의 무기체계 획득 관리 절차의 기반이 되는 핵심 체계로서 기획(Planning), 계획(Programming), 예산(Budgeting) 등 업무추진에 대한 관련 근거가 되는 문서체계를 아래의 [그림 3-1]과 같이 유지하고 있으며, 국방부 및 합참, 각 소요군 등 모든 부대 및 부서는 이

43) 국방기획관리(PPBEE): 기획(Planning), 계획(Programming), 예산(Budgeting), 집행(Execution), 평가(Evaluation)

44) 국방기획관리기본훈령(국방부훈령 제2627호, 2022.2.3. 시행)

를 근거로 무기체계에 대한 전력발전업무를 추진해야 하고, 국방 AI 분야도 무기체계에 AI 적용시 이 문서체계에 근거하여 AI 적용 업무를 추진하여야 한다. 현재 무기체계 분야 AI는 방사청을 중심으로 방위력개선비를 활용하여 핵심기술, 미래도전국방기술, 민군기술협력, 신속연구개발 등 다양한 형태로 적용을 위한 연구와 사업이 활발하게 진행되고 있다.

[그림 3-1] 무기체계를 대상으로 하는 국방기획관리 문서체계



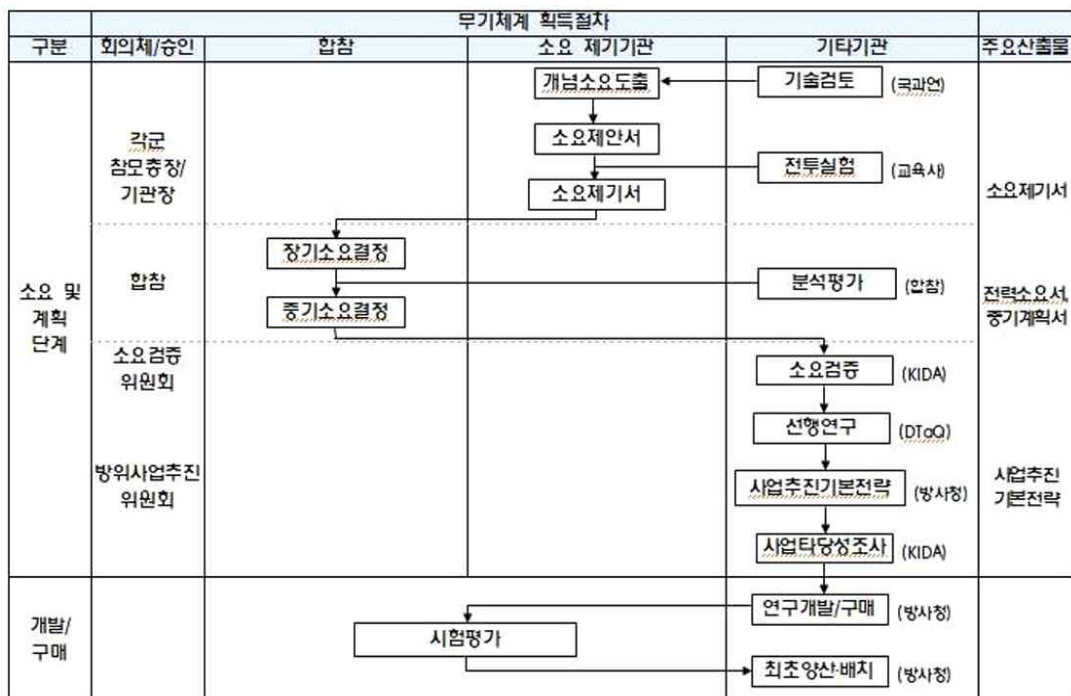
출처: 국방기획관리기본훈령(국방부훈령 제2627호, 2022.2.3.)

(나) 반면 국방정보화업무훈령은 ‘국방정보화법(국방정보화 기반조성 및 국방정보자원관리에 관한 법률)’에 근거하여 국방정보화기본계획을 수립하고 전력운영비 상에 반영된 국방정보화사업(기획, 계획, 예산, 집행, 운영 및 유지보수 등)을 추진하고 있으나 국방 AI 등 지능정보화 업무와 관련된 기획 및 계획 분야가 국방기획관리체계와 연계되어 추진되지 못하고, 국방운영 분야와 자원관리체계 등 기반체계와 인프라 관련 사업영역으로만 한정되어 수행됨으로써 무기체계 분야의 AI 적용 지원을 위한 업무수행이 효과적으로 수행되지 못하고 있는 것으로 평가되고 있다.

(2) 국방획득관리체계 AI 적용을 위한 노력

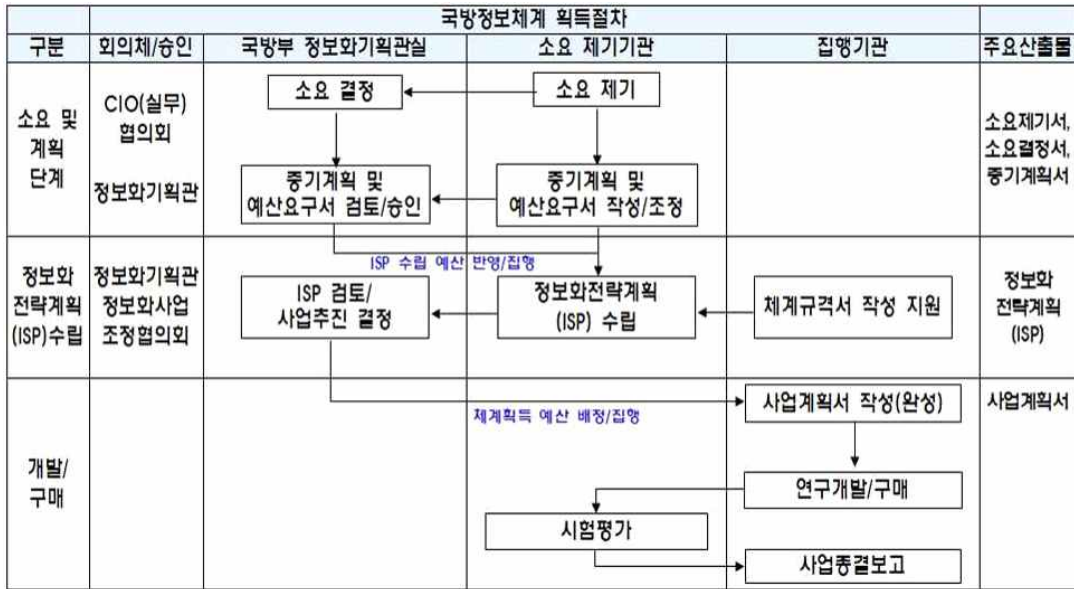
국방 소요의 획득 절차는 크게 방사청 주관의 무기체계와 국방부 및 각 소요군 주관의 전력지원체계(국방정보체계 포함)로 구분된다. 무기체계의 획득 절차는 각 소요군의 소요제기를 합참에서 검토 후 합동참모회의를 거쳐 소요를 결정하고 합동군사전략목표기획서(JSOP)에 반영하며, 방사청에서는 국방 중기계획 요구서를 국방부에 제출하여 검토 후 국방 중기계획이 완성된다. 국방 중기계획에 향후 5년간 필요한 예산운영을 포함하여 구체적인 계획을 반영하고, 이 계획에 따라 연구개발 및 구매, 임차사업 등이 진행된다. 반면에 전력지원체계(국방정보체계)의 획득 절차는 각 소요군 및 기관의 소요요청을 국방부에서 검토하여 소요제기서를 만들며, 해당 소요의 성격에 따라 국방부 또는 각 소요군 주관하 소요를 획득한다. 소요 및 주관부서가 결정되면 소요 검증을 국방연구원(KIDA) 주관 하 실시하고, 사업 추진 기본계획을 수립하여 전력지원체계 사업계획서를 만든다. 이후 무기체계와 동일하게 국방 중기계획에 반영되어 예산을 편성하고 연구개발 및 구매, 임차사업 등이 진행된다.

[그림 3-2] 무기체계 획득 절차도



출처: 국방정보체계 획득절차 개선(고광춘, 2022.10.13.)

[그림 3-3] 국방정보체계 획득 절차도



출처: 국방정보체계 획득절차 개선(고광춘, 2022.10.13.)

이처럼 무기체계와 전력지원체계(국방정보체계)는 각 체계별로 획득업무를 담당하는 조직이 분리되어 있고, 업무수행 절차와 관련 법규, 예산구조가 서로 달라 각 체계에 AI 적용을 기획하고 획득하는데 어려움이 발생하고 있다. 전력체계 중에서도 국방정보체계는 SW의 특성상 무기체계와 전력지원체계 모두에게 공통적으로 사용되는 체계인데 때로는 무기체계에 포함되어 방위력개선비로 획득이 추진되고, 때로는 전력지원체계에 포함되어 전력운영비로 획득이 추진됨에 따라 통합적이고 체계적이지 못한 구조로 되어 있다. 방위력개선비로 획득되는 무기체계의 경우는 핵심기술 연구개발시 AI 기술이 포함되어 별도의 예산과 업무절차가 필요 없으나 전력운영비에 반영된 AI 획득예산은 대부분 독립적인 실험 및 시범사업의 형태로 데이터 구축, 플랫폼 개발 등 AI 기반체계를 구축하는 데 활용되고 있어 무기체계 분야에 AI 적용은 사실상 어려운 상황이다. 국방의 전력발전업무체계는 무기체계를 중심으로 추진되고 있으며, 무기체계에는 전력지원체계와 국방정보체계가 전부 포함되어 있는데 예산은 분리되어 각각의 조직에서 별도로 집행되는 현재의 시스템은 향후에도 지속적으로 유지될 것으로 보여 무기체계 AI 적용에 걸림돌로 작용할 것으로 판단된다.

제 5 절 국방 AI 적용을 위한 개념연구 측면

(1) 개념선도형 및 기술선도형 전력체계 발전

(가) 군사력 건설 또는 전력체계 발전은 유형에 따라 수요가 주도(Demand pull)하는 ‘개념선도형’ 발전과 기술이 선도(Technology Push)하는 ‘기술선도형’ 발전으로 구분할 수 있다. ‘개념선도형’ 방식의 전력체계 발전 방식은 전통적인 형태로 수요를 중심으로 소요 기획을 통해 확보하고자 하는 전력체계의 작전운용 개념, 조직편성, 전략 및 교리 등을 구상하고 전력화를 추진하여 확보하는 방식으로 軍이 필요로 하는 전력체계를 계획한 시기에 확보할 수 있다는 장점이 있다. 그러나 이 방식은 체계적이고 단계적인 추진을 통해 안정적인 전력체계를 발전시킬 수 있으나 전력체계 확보 시간이 과다하게 소요되는 단점과 막대한 예산 소요, 기술의 진부화, 기존 전력체계에 최신기술 적용 제한 등 여러 가지 문제점을 안고 있다. 이에 따라 4차산업혁명 시대를 맞이하여 軍은 첨단기술을 전력체계 발전에 활용하고자 ‘기술선도형’ 전력체계 발전을 연구하여 도입하게 되었다. 이 방식은 민간의 기술발전 속도를 파악하고 여러 가지 첨단기술을 조기에 식별하여 군사적 목적에 부합한 전력체계의 개발을 軍에 요구(소요제기)함으로써 단기간에 전투의 효율성을 극대화할 수 있는 전력체계를 전력화하여 전쟁의 판도를 바꿀 수 있는 게임체인저(Game changer)로서 활용될 수 있는 장점이 있다. 그러나 이 방식은 적은 예산으로 짧은 기간에 전투력 향상에 도움을 줄 수 있는 장점이 있으나 장기적인 관점에서 현존 및 잠재적인 적의 위협에 대비한 전략, 작전운용 개념, 교리 등의 충분한 연구와 준비가 제한되어 중구난방식의 전력체계 도입이 이루어질 수 있다는 단점을 가지고 있다.

(나) 위의 대표적인 2가지 사례를 고려해 볼 때 AI는 4차산업혁명을 주도하는 대표기술로써 ‘기술선도형’ 전력체계 방식에 부합하는 것을 알 수 있다. 현재 우리 軍의 AI 기술 전력체계 적용은 초기 단계

로써 전략이나 개념(운용개념, 작전운용성능, 기술·전력구조, 요구능력 등)에 대한 충분한 연구가 반영되지 않은 채 다양한 부서에서 다소 중구난방식의 소요기획과 실험 또는 시범사업 형태의 여러 가지 AI 기술 적용이 진행되고 있어 장기적인 관점에서 보면 예산의 낭비, 불필요 장비 및 자원의 생성, 관리소요 증가, 군사보안 통제소요 증가, 유지보수, 성능개량(고도화) 문제 등 다양한 해결과제가 나타나고 있는 상황이다.

(2) 국방 AI 적용을 위한 개념연구

우리 軍은 2019년부터 국방부를 비롯하여 각 소요 군별로 軍내에 AI 관련 조직과 직책을 적극적으로 신설하고, 본격적으로 국방 분야에 AI 적용 업무를 추진하기 시작하였다. 약 5년이 지난 現 시점에서 국방부와 각 소요 군은 AI 관련 연구와 각종 사업을 다양하게 추진하고 있으나 AI 기술을 활용하여 국방 분야에서 ‘무엇을? 어떻게 할 것인가?’에 대한 구체적인 개념(필요성, 운용개념, 작전운용성능, 적용범위, 요구능력 등)을 명확하게 제시해 주지 못하고 있다. 무기 및 전력지원체계(국방정보체계)의 획득을 위한 국방기획관리 문서체계에는 국방기획지침, 전략서, 합동군사전략목표기획서(JSOP), 장기무기체계발전방향 등 획득을 지원하기 위한 다양한 문서들이 있는데 AI 기술을 적용하여 활용하기 위한 구체적인 전략이나 개념, 방향성 등을 명확하게 제시해 주지 못하고 있다. 이는 국방기획관리 문서체계를 생산하는 조직에 AI 기술에 대한 전문적 지식을 갖춘 인재가 많지 않은 원인도 있으나 근본적으로는 How to Fight(어떻게 싸울 것인가?)에 대한 개념을 조직적으로 연구하는 기관이나 부서가 부족하여 다양한 무기 및 전력지원체계에 AI 적용을 위한 전략과 개념(필요성, 운용개념, 작전운용성능, 적용범위, 요구능력 등)을 제시해 주지 못하고 있는 것으로 판단된다. AI는 다른 첨단 과학기술과 달리 소수의 기능만 요망 수준을 달성하면 되는 기술이 아니다. 인간과 유사한 지적 능력을 보유하고 있어 무기 및 전력지원체계에 적용하려면 여러 가지 고려해야 할 요소들이 많아 개념을 명확하게 정립하지 않고 국방 분야 적용을 추진하지 않으면 여러 가지 예상하지 못한 문제점들이 발생할 수도 있다.

제 6 절 국방 AI 적용시 군사보안의 인식 측면

국방 분야에 AI 적용을 저해하는 요소가 무엇인가?라는 질문에 많은 사람들은 전문인력 부족, 군사보안 문제, 데이터 확보 어려움, 각종 규제 등 다양한 요소들을 이야기하는데 항상 등장하는 저해 요소를 손꼽으라면 바로 군사보안 문제일 것이다. AI 개발자, 운용자, 관리자 등 AI 업무 관련 관계자들은 군사보안 문제를 국방 AI 적용에 있어서 가장 큰 제약을 주는 저해 요소 중에 하나로 인식하고 있다. 이는 AI 적용시 기본적으로 해결해야 할 보안 규제가 많고 해결이 어려우며, 해결방안이 제시되지 않으면 개발을 진행할 수 없으므로 AI 적용에 걸림돌로 인식하고 있다. AI는 단일의 소프트웨어로 이루어진 기술이 아니라 데이터, 알고리즘, 플랫폼 등 3대 구성요소가 유기적으로 결합하여 기능을 발휘하는 기술로써 각각의 구성요소를 개발하거나 구축할 때 해결해야 할 군사보안 문제가 남아있어 AI를 적용하는 데 있어서 큰 어려움으로 작용하고 있다. 국방 AI를 개발하는 개발자의 입장에서 인식조사를 살펴보면 대부분의 軍 관계자들은 軍 내부 시설에서 AI 개발을 시행하길 원하고 있으나 軍 내부에는 외부의 인터넷망 접속, 오픈소스 사용, AI 학습 및 시험 운용을 위한 플랫폼 구축, 데이터 수집 및 사용 등 다양한 분야에서 제한사항이 있어 AI를 쉽게 개발할 수 없는 상황이다. 또한 AI는 다른 첨단과학 기술과는 다르게 인간과 유사한 지능이 만들어지고 성장하며, 특정 부분이 아닌 국방 전 분야에 적용될 수 있고, 개발, 운영유지, 성능개량, 폐기 등 여러 부분에서 관리 요소가 복잡하여 안정적으로 구축하고 운용하는데 매우 어려운 특징을 가지고 있다. 아울러서 AI가 국방 분야에 적용되기 시작한 지 얼마 되지 않은 상황에서 다른 기술들과는 달리 보안 문제에 대해 해결해야 할 과제들이 많고, 문제해결에 난이도가 높아 쉽게 해결되지 못하고 있는 부분도 AI 적용의 어려움을 가중하고 있다. 따라서 국방 AI 적용에 있어서 군사보안 문제는 위에서 언급한 여러 가지 제약사항과 특징을 고려하여 개발자나 관리자 등 다양한 시각에서 제한사항과 문제점이 무엇인지 구체적으로 식별 및 분석해 보고 이에 따른 해결방안의 모색이 필요하다.

제 7 절 AI 전문인력 및 조직 운영 측면

(1) 국방 AI 관련 전문인력 확보 및 관리

(가) 국방 분야에 AI 적용이 활발하게 추진되려면 ‘기술적(알고리즘, 데이터, 컴퓨팅 자원 등) 관리 능력’과 ‘도메인(정책수립, 소요기획, 개념연구, 사업추진, 전력화 등) 관리 능력’에 있어서 전문성을 보유한 인력의 확보가 중요하다. 국방 분야의 AI 인력은 채용, 보직, 운용 등에 있어서 軍 고유의 인사관리 제도와 시스템으로 인해 민간의 방식과는 큰 차이를 보이고 있으며, AI 지식 습득의 난이도와 복잡성으로 인해 단기간에 전문지식을 갖춘 인력을 확보하고 적재적소에 보직하여 임무를 수행하게 하는 것이 매우 어려운 실정이다. 국방부 및 각 軍 본부는 AI 전문인력 확보를 위해 인재 양성 및 관리 시스템, 조직 신설 등 중·장기적으로 다양한 정책과 제도를 수립하여 추진하고 있으나 이러한 정책과 제도는 최상급 기관의 관심과 예산지원에도 불구하고 예하 조직 및 관련 기관에서는 AI 전문인력을 제대로 확보하지 못해 괄목할만한 업무성과를 나타내지 못하고 있다. 이는 軍 내부적으로 AI 인재를 양성하고 활용하는 방법에 있어서 상·하급제대 및 각 기관별 유기적인 협조체계가 구축되지 않고 개별적인 정책과 업무를 추진함으로써 시너지 발휘가 제한되었으며, 특정 병과와 주특기 인원에 편중된 각종 특화교육은 ‘기술적(알고리즘, 데이터, 플랫폼 등) 관리 전문가’ 양성에만 치우치게 되었고, 상대적으로 ‘도메인(정책수립, 소요기획, 개념연구, 사업추진, 전력/획득 등) 전문가’ 양성에는 소홀하여 국방 전 분야에 균형된 AI 발전을 추진하지 못하고 있다.

(나) 2019년 이후 국방부 및 각 軍에 AI 조직과 직책들이 본격적으로 신설되기 시작하여 조직의 전문성을 향상시키고, 조기에 획기적인 업무성과를 달성하기 위해 국내외 위탁교육, 軍 특화교육, 정책연수 과정 등 수많은 전문인력 양성 프로그램을 신설하여 추진해 왔다. 그러나 국방부 및 각 軍의 전문인력 양성 과정을 담당하는 기관은 교육생 선발과 양

성 과정에만 관심을 기울이고 수료자원들의 인사관리에는 관심이 부족하였으며, 인사관리의 권한과 책임이 없어 전문인력들이 교육 수료 후 다양한 AI 관련 부서에 적시적으로 활용되지 못하는 등 체계적인 인사관리 시스템이 운영되지 못하였다. 또한 현재도 다양한 AI 전문인력 양성 프로그램이 활발하게 시행되고 있으나 여전히 기술적 관점에서의 전문인력 양성 프로그램 위주로 진행되고 있으며, 도메인 관점에서 정책과 제도 수립, 개념연구, 사업추진, 전력/획득업무 등의 전문가를 양성하기 위한 프로그램이나 교육과정이 부재하여 관련 업무를 수행하는 부서에서는 여전히 AI 전문인력이 부족하여 AI 업무수행에 어려움을 겪고 있다.

(2) AI 조직 운영

국방부 및 각 軍 본부는 국방 AI 추진의 가속화를 위해 2019년 이후 본격적으로 AI 관련 조직과 기관의 신설을 추진하였다. 육군을 시작으로 해군, 공군, 국방부 본부 등에 2019년부터 2021년까지 순차적으로 AI 관련 조직들이 생겨나기 시작하여 AI 기반체계 구축과 각종 소요창출을 통한 사업을 추진하였으며, 민간의 최신 AI 기술의 軍 적용을 위해 산·학·연 협력체계를 구축하는 등 활발한 활동을 이어나갔다. 특히, 국방부 및 각 軍 본부는 AI 관련 상설 및 TF 성격의 여러 조직을 신설하여 AI 정책 구현을 위한 업무분장, 제도 수립, 예산편성 및 사업 집행 조정·통제, 전문인력 확보, 산·학·연 협력생태계 구축 등 다양한 업무를 수행하였다. 그러나 2019년 이후 5년이 지난 현재 시점에서 나타나고 있는 현상을 분석해 보면, 첫째는 AI 업무수행 조직이 분산 및 중복 편성되어 있는 것을 볼 수 있고, 법적으로 권한과 책임을 가지고 있는 컨트롤타워가 부재하여 국방 AI 적용을 추진하는데 필요한 각종 중요업무에 대해 조정·통제가 제대로 이루어지지 않고 있다. 둘째는 각 조직들의 임무와 기능 측면에서 정책 수립, 데이터 구축, AI 모델 개발, 기술관리, 대외협력 업무 등에 있어서 유사하거나 중복되는 경향이 있어 조직의 최적화를 위해 임무와 기능 또는 편제를 변경해야 할 필요성이 있다. 셋째는 업무수행체계 측면에서 전력 지원체계(국방정보체계) 업무수행 중심의 조직편성으로 무기체계 AI 적용

을 위한 개념연구, 소요기획, 시험평가, 획득 등의 업무수행체계가 반영된 조직의 신편과 확대 편성이 미흡한 실정이다.

제 8 절 AI 관련 軍 내부 의사결정시스템 측면

국방부와 합참, 각 소요군은 무기 및 전력지원체계(국방정보체계 포함)의 소요제안(제기)으로부터 예산편성·사업관리 단계에 이르기까지 기획관리체계 및 획득체계 그리고 각 소요군 전투발전체계상에 다양한 의사결정기구(협의회)를 운용하고 있다. 무기체계 분야는 각 소요군 및 관련 기관의 전력 소요제기를 통해 합참의 ‘합동참모회의’에 심의·의결을 거쳐 최종적으로 소요를 결정하고, 각종 기획관리체계 문서에 반영하여 전력화를 추진하고 있다. 또한 전력지원체계 분야는 각 소요군 및 관련 기관에서 소요요청을 통해 국방부 및 각 소요군 본부에서 소요를 종합 후 기관별 전력지원체계 위원회를 통해 소요를 결정하고 예산을 반영하여 획득을 추진하고 있다. 전력지원체계 일부에 해당하는 국방정보체계는 ‘국방 고위정보화책임관(CIO)협의회’ 운영 훈령에 의거 국방 정보화를 체계적으로 추진하기 위해 별도로 ‘국방 고위정보화책임관(CIO)협의회’를 운용하여 정보화 사업과 정보체계자원의 기획·조정·관리 등의 의사결정을 수행하고 있으며, 각 소요 군도 국방부에 국방정보체계의 소요 제출을 위해 자체적으로 국방부와 유사한 기능을 수행하는 CIO 위원회를 각 소요군 규정에 반영하여 별도로 의사결정시스템을 운영하고 있다. 이 밖에도 국방부 및 각 소요 군은 다양한 전력체계들의 소요결정과 예산반영, 사업추진 등의 의사결정을 위해 여러 유형의 의사결정기구(협의회)를 행정규칙 등에 반영하여 체계적으로 업무를 수행하고 있다. AI와 관련된 의사결정기구로는 2022년 12월에 국방부 최초로 ‘국방 데이터관리위원회’를 개최하여 국방 AI의 소요 발굴 및 기획, 전략적인 데이터 구축 및 활용, AI 관련 정부 부처협력사업 추진 등의 업무에 대하여 논의를 하였다. 이후 2024년 6월에는 ‘국방 데이터·인공지능업무 훈령’을 제정한 뒤 ‘제1차 국방 데이터·인공지능위원회’를 개최하여 국방 데이터 및 인공지능 분야의 정책 및 제도

개선에 관한 사항을 심의하고 조정하는 역할을 수행하고 있으며, 이와 보조를 맞춰 각 소요 군도 국방부의 추진전략에 따라 자체적으로 ‘각 소요군 별 데이터·인공지능 위원회’를 설치하고, 관련 규정 제정을 추진하고 있다. 국방부 및 각 소요 군은 ‘국방 데이터관리위원회’와 ‘국방 데이터·인공지능 위원회’ 등이 설치되기 이전에는 대부분이 ‘국방 고위정보화책임관(CIO) 협의회’와 각 소요 군의 ‘CIO 협의회’를 통해 AI 및 데이터 구축업무에 대한 소요를 결정하고, 예산편성 및 사업관리 업무를 추진하여 왔다. AI는 무기체계, 전력지원체계, 국방정보체계 등 다양한 체계에 공통적으로 적용되는 기술로 국방의 다양한 분야에 적용하기 위해 기획관리체계 및 획득체계, 전투발전체계 등에 추진계획을 반영하여 관리되고 있으나 실제 AI를 적용하기 위한 전력운영비의 소요결정과 예산편성 등은 주로 국방정보체계를 중심으로 추진되어 왔다. ‘국방 고위정보화책임관(CIO)협의회’ 운영 훈령에 근거한 독자적인 AI의 소요결정, 예산운영 및 사업관리 추진은 타 훈령에 근거하여 추진 중인 무기체계 및 전력지원체계의 전력화(획득) 추진계획과 연계성이 낮고, 타 협의회와의 협력이 제한되어 기획관리 및 획득체계, 전투발전체계 등의 문서에 반영된 AI 기술 적용계획과 연관성 및 통합성이 떨어지는 한계점을 가지고 있다. 이는 각 소요군이 상급 부대(국방부)의 훈령과 각 소요 군의 자체 규정에 따른 업무수행 시스템으로 인해 각 군 본부 및 예하부대로 내려갈수록 타 부서 및 협의회와의 원활한 업무협조체계 구축이 구조적으로 어려운 문제점을 가지고 있다. 아울러서 다양한 무기체계 및 전력지원체계에 AI 적용을 위한 업무를 균형되게 추진할 수 있는 권한과 책임 및 예산을 가진 상급부대 컨트롤타워의 부재도 예하부대의 AI 적용 추진을 위한 의사결정에 혼선을 주고 있는 실정이다.

제 4 장 국방 AI 적용 가속화를 위한 발전방안

본 연구에서는 앞에 3장에서 제시한 AI의 군사적 활용시 걸림돌로 작용하고 있는 여러 가지 제한사항과 문제점들의 분석 결과를 바탕으로 다양한 관점에서 국방 AI 적용 가속화를 위한 발전방안을 제시해 본다.

제 1 절 신뢰성 있는 국방 AI 적용을 위한 윤리기준 정립

(1) 군사적 관점의 AI 윤리기준 정립

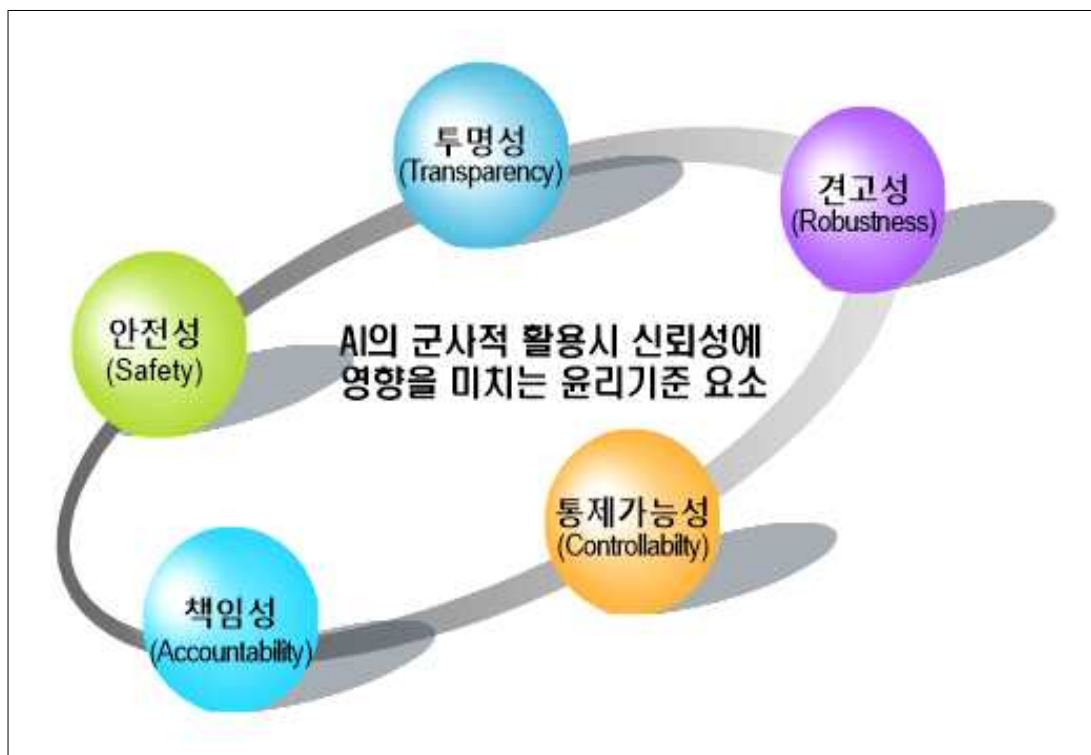
(가) AI 기술발전의 가속화와 더불어 국내·외적으로 AI 윤리기준에 대한 연구성과가 가시화되고 있어 민간영역뿐만 아니라 국방영역에서도 AI 윤리기준 적용에 대한 논의가 점차 증대되어 가고 있다. 지난 2023년 이후 2차례에 걸친 ‘REAIM(인공지능의 책임있는 군사적 이용에 관한 고위급회의)’을 통해 안전하고 신뢰성 있는 AI의 군사적 활용에 대한 공감대가 크게 형성되었으며, 앞으로 AI를 군사적으로 이용함에 있어 투명하고, 안전하며, 책임감 있게 활용될 수 있도록 다양한 국제회의체와 기관 등에서 논의가 증대될 것으로 예상된다. 이러한 국제회의와 향후 예상되는 논의의 배경에는 AI 선도국가들을 중심으로 AI를 군사적으로 활용하기 위한 정당성을 이미 인정하고 있다는 것을 알 수 있으며, 인간의 존엄성과 윤리를 중요시하는 국가들은 상대적으로 AI 기술발전이 저조하여 AI 기술의 군사적 이용에 대한 정당성에 다소 부정적인 견해를 보여 다양한 논쟁이 지속되어 왔다. 이러한 국제적 논쟁과 추세를 고려해 볼 때 AI가 군사적으로 이미 활용되고 있는 現 시점에서 AI의 군사적 활용에 대한 옳고 그름에 대한 문제(정당성 문제)는 더이상 논쟁의 대상이 될 수 없을 것으로 판단되며, 이제는 AI의 군사적 활용(정당성) 문제에 대해서 수용하는 자세를 견지하고, AI를 군사적으로 활용하는 데 있어서 인간의 존엄성을 보장하는 가운데 ‘어떻게 하면 안전하고 책임감 있게 사용할 수 있을것인

가?’에 대한 국제적 논의와 합의를 이끌어 가는게 더 바람직한 방향이라고 판단된다. 현재 AI의 군사적 활용에 대한 가장 큰 우려의 시각은 아마도 치명적 자율무기체계(Lethal Autonomous Weapon System)에 AI를 적용하는 문제일 것이다. 치명적 자율무기체계(Lethal Autonomous Weapon System)에 AI를 적용시 인간의 존엄성 훼손과 전쟁법(전시국제법) 미준수 우려 등 다양한 윤리적 문제를 일으킬 수 있는 소지가 있어 이를 해결하기 위해 군사적 AI 활용에 대한 윤리기준(원칙)의 제정 및 준수가 필요한 것이다. 군사적 AI 활용에 대한 윤리기준(원칙)을 정립하기 위한 연구와 논의가 각 국가별로 이미 진행되고 있으며, 우리도 ‘AI를 군사적으로 활용시 수반되는 윤리기준 또는 원칙이 무엇이 있는지?’ ‘이를 제정하기 위해서는 어떠한 난제들을 해결해야 하는지?’ 구체적인 범위를 지정하고 기준을 정립하기 위한 연구를 추진해야 할 필요성이 있다. 시작 단계에서부터 여러 가지 분야를 모두 적용할 수 있는 윤리기준을 정립할 수 없으므로 우선은 AI 소요기획 단계에서부터 폐기시까지 생애주기(Life Cycle) 전반에 대해서 군사적 관점과 요건을 충족시키며, 신뢰할 수 있는 AI를 개발하고 운용하는 데 필요한 윤리기준 정립을 추진해야 한다.

(나) 신뢰할 수 있는 AI를 개발하고 운용하기 위해서는 AI가 갖추어야 할 윤리기준들이 많이 있을 수 있는데 기술 개발자와 사용자 입장에서 모두를 충족시킬 수 있는 윤리기준들이 필요하다. AI의 윤리 관점 또는 신뢰할 수 있는 AI 개발관점에서 필요한 기준으로는 안전성(Safety), 공정성(Fairness) 및 편향(Bias) 방지, 투명성(Transparency) 및 설명가능성(Explainability), 견고성(Robustness), 정보보호(Security), 통제가능성(Controllability), 공공성(Publicity), 책무성(Accountability) 등 다양한 요소가 있을 수 있다. 이러한 AI의 신뢰성에 영향을 주는 여러 가지 기준 중에 군사적으로 활용시 영향을 미칠 수 있는 핵심적인 윤리기준을 5가지로 판단하였다. 첫째는 안전성(Safety)으로 군사용 AI는 무결성, 정확성, 치명성 등 운용환경의 특수성에 따라 기술적으로 복잡하고 가혹한 환경하에 운용되며, 내외부적으로 다양한 위협에서 지속적인 능력 발휘가 가능

해야 함에 따라 안전성이 반드시 확보되어야 한다. 둘째는 투명성(Transparency)으로 기술개발, 서비스 설계, 제품 기획 등의 의사결정 과정에서 개발자와 사용자, 운용관리자 등의 의견이 필히 반영되어야 하며, 사용시 예상되는 위험과 제한사항, 필요정보 공개 및 공유 등의 과정이 적절하게 이루어져야 한다. 셋째는 견고성(Robustness)으로 군사용 AI는 가혹하고 복잡한 전장 환경에서도 원활히 그 기능을 발휘할 수 있는 강건함(내구성)을 가져야 한다. 넷째는 통제가능성(Controllability)으로 AI의 오작동 또는 의도하지 않거나 예상하지 못한 위험으로부터 피해 상황을 제거할 수 있도록 정책 및 제도적 측면과 기술적 측면에서 통제성을 확보할 수 있도록 가용한 수단과 방법의 강구가 필요하다. 마지막 다섯째는 책무성(Accountability)으로 군사용 AI의 공급 및 확산, 운용결과 발생할 수 있는 다양한 문제점에 대한 책임을 개발자-공급자-사용자가 공유해야 하며, 오작동 및 사고 발생에 대비하여 공정하고 합리적인 책임 보상 원칙을 마련해야 한다.

[그림 4-1] AI의 군사적 활용시 신뢰성에 영향을 미칠수 있는 윤리기준



이처럼 인공지능의 군사적 활용시 신뢰성에 영향을 미칠 수 있는 윤리 원칙의 핵심 요소에 대해서 개략적으로 판단해 보았으며, 각 요소별로 개념과 여러 가지 특징 등에 대해서 다음과 같이 구체적으로 제시해 본다.

1) 안전성(Safety)

일반적으로 각종 사물이나 기계 등의 경우 인간의 통제하에 움직이는 경우가 대부분이다. 그런데 AI는 인간이 부여한 능력 범위 내에서 또는 자체 학습을 통해 그 이상의 범위(영역)에서 스스로 자율적인 선택과 결정을 할 수 있는 자율성(Autonomous)을 가질 것으로 예측이 된다. 이러한 자율성(Autonomous) 부분은 AI를 군사적으로 활용하는 군대에서 긍정적인 측면과 부정적인 측면에서 이슈가 되며 매우 민감하게 반응하고 있다. 긍정적인 측면에서는 미래 병력자원 감소에 따라 부족한 병력을 AI가 탑재된 무기체계가 대신할 수 있으며, 인명피해를 최소화하는 가운데 자율성을 겸비한 치명적 자율무기체계(Lethal Autonomous Weapon System)를 적극적으로 활용하여 적보다 먼저 군사력의 우위를 달성하여 전쟁의 주도권을 확보하는데 큰 기여를 할 수 있다. 반대로 부정적인 측면은 전쟁수행시 적과 아군의 인명(人命)을 인간(군인)이 아닌 AI가 결정하는 데에 있어서 이를 허용하고, 여기에서 발생하는 도덕적 위험성을 감수할 것인가에 대해서 화두로 떠오르고 있다. 따라서 이러한 문제에 대응하기 위해 AI에게 도덕적 규범을 부여하여 안전하게 활용할 수 있는 방안에 관해서 활발한 연구가 진행되고 있다. 또한 AI가 가지고 있는 잠재적인 위험을 최소화하고, AI의 오작동에 의한 인명(人命) 사고의 방지를 위해 인간의 제어 대책이 강구될 수 있도록 통제 가능성 요소의 측면에서 대책이 강구되어야 하며, AI를 활용시 인명(人命)과 관련해서 발생하는 모든 행위의 결과에 대한 책임 소재를 명확히 해야 하고, 안전과 관련된 정보가 적시 적절하게 공유될 수 있도록 책임성 요소 측면에 대한 대책도 연계하여 강구되어야 한다.

2) 투명성(Transparency)

투명성은 AI를 사용하는 데 있어서 안전하고 신뢰할 수 있는 시스템을 구축하는데 하나의 중요한 구성요소이다. 딥러닝 기술이 급속도로 발전함에 따라 수많은 AI는 그들이 제시한 결과값에 대해 명확한 이유를 설명할 수 없는 블랙박스 형태의 시스템으로 구축되어 있다. 아직까지도 인간은 AI가 왜 그러한 결론(결정)을 내렸는지 의사결정의 세부적인 과정을 명확하게 밝혀내지 못하고 있다. 그러면 AI의 투명성이 중요한 이유는 무엇일까? 안전, 의료, 교통 등 인간의 생명과 재산상에 막대한 피해를 줄 수 있는 분야에서는 AI가 어떠한 기준과 논리 과정을 거쳐 결론을 내렸는지 이해하기 전까지는 어느 누구도 안전하게 AI를 사용하지 못할 것이다. 특히 군대에서 적과의 전투를 수행하며, 사람의 생명을 해치고 시설물을 파괴하기 위해 개발되고 있는 각종 치명적 자율무기체계(Lethal Autonomous Weapon System) 등에 AI가 장착될 시 명확한 의사결정 과정을 논리적으로 제시하지 못하면 어느 누구도 AI를 효율적으로 사용할 수 없을 것이다. 전 세계적으로 현재까지 개발된 다양한 형태의 AI(객체식별, 자연어 처리, 생성형 언어모델, 대화형 챗봇 등)는 결론(결과값)을 제시하는 과정에서 다양한 오류와 잘못된 결정, 신뢰할만한 답변 제시 부족 등 크고 작은 사용자 불만으로 투명성(설명 가능성) 측면에서 큰 도전에 직면하고 있으며, 이러한 불신과 불안에 대해서 단시간에 해소하기는 어려울 것으로 보인다. 따라서 우리는 이러한 AI의 투명성에 대한 중요성을 조기에 인식하여 AI 윤리의 한 분야로써 정책 및 제도적 측면에서 기준과 원칙을 정립하고, AI 적용의 확산을 위해 기술개발시 알고리즘, 데이터, 소프트웨어 등의 공개가 필요하며, 개발자-공급자-사용자간 신뢰성 향상을 위해 정보를 공유하는 등 투명성을 강화하기 위해 노력해야 한다.

3) 견고성(Robustness)

AI의 견고성은 다양한 환경에서 AI 모델이 안정적으로 동작하며, 예상치 못한 입력이나 가혹한 환경에서도 오작동하지 않고, 견고한 성능을 유지하는 능력을 의미한다. 최근 객체식별, 자연어 처리 등 다양한 분야에서 AI 모델이 적극적으로 활용되고 있으나 AI 적대적공격

(Adversarial attack)⁴⁵⁾의 등장으로 AI의 취약성에 대한 문제가 지속적으로 제기되고 있다. 자연 상태에서 얻을 수 있는 정상적인 데이터로 학습된 AI가 자연 상태의 데이터에 대해 100%의 인식 성공률을 보이더라도, AI의 취약점을 파고드는 적대적공격(입력 데이터의 임의 변형 또는 물리적 조작 등)을 통해 AI가 오작동하도록 유도할 수 있는 것으로 확인되고 있다. 실제 예로 개체식별 AI 모델이 카메라나 센서 등을 통해 적대적 샘플이 포함된 데이터를 입력함으로써 객체식별 AI 모델을 기만하는 적대적공격이 실용적이고 높은 성공률을 보이는 것으로 확인되고 있다. 적대적공격 및 방어 기술조사 보고서⁴⁶⁾에 의하면 이미 미국 등 AI 기술 상위 5개국은 2019년부터 적대적공격의 취약성에 대해서 인식하고 적대적 정보에 강한 딥러닝 모델의 개발을 추진하고 있다. 적대적공격에 대응하기 위해 국내외적으로 딥러닝에 문제를 일으키는 적대적 유사공격 기술, 학습 및 검증단계에 대한 적대적공격 및 방어 기술, 모델 설계에 대한 적대적공격 및 방어 기술 등에 관한 연구가 활발히 진행되고 있다. 현재의 AI 기술 수준과 발전 속도를 고려해 볼 때 가까운 미래에 국방의 다양한 분야에 AI 모델이 적극적으로 활용될 것으로 예상되며, 우리 군도 AI 모델의 견고성(Robustness)을 향상시키기 위한 대비책 마련이 조속히 추진될 필요가 있다. 현재 각 군에는 객체식별 AI가 다양한 영역에서 활발하게 개발되어 적용되고 있는 시점에서 외부의 적대적 세력에 의한 AI 적대적공격이 가해질 경우 객체식별 AI가 탑재된 우리 군의 감시정찰체계를 무력화시킬 수 있는 취약요소로 작용하여 군의 입장에서는 매우 심각한 잠재적 위협으로 인식될 수 있어서 신속한 대응능력 구비가 필요하다.

4) 통제가능성(Controllability)

일반적으로 사물이나 기계의 경우 운용자인 인간의 손길을 거쳐야 움직이게 된다. 그런데 AI는 일정한 학습과 알고리즘을 통해서 특정범위

45) AI 적대적공격: AI 모델을 대상으로 하는 적대적공격은 기계학습 및 인공지능 시스템의 보안 취약점을 이용하여 의도적으로 잘못된 결과를 유도하거나 모델의 정보를 탈취하는 다양한 기술을 포함한다. triangular.tistory.com, 2024.5.

46) 적대적공격 및 방어 기술조사 보고서 23호, KAIST 유영준

내에서 스스로 자율적인 선택과 의사결정을 내리는 자율성(Autonomous) 지위를 가질 것으로 예측이 된다. 최근 벌어지고 있는 우크라이나-러시아 전쟁에서는 인간의 통제없이 적군을 향하여 공격하는 AI 기반의 공격드론이 등장하였으며, 이스라엘-하마스 전쟁에서는 무기체계에 탑재된 AI가 타격 목표의 우선순위를 고려하여 작전을 수행하는 사례도 공개되었다. 이처럼 AI가 다양한 무기체계에 탑재되어 치명적 살상무기체계의 효과를 극대화하는 초유의 사태가 벌어지고 있다. 향후 AI의 성능이 고도화되어 인간의 통제를 벗어나면 핵무기 및 대량살상무기를 넘어서는 위험을 초래할지도 모른다는 군사전문가들의 경고가 잇따르고 있다. 물론 AI가 자율성(Autonomous)을 갖는다고 해서 무조건 큰 문제가 되고 위험한 결과만을 초래하는 것은 아니다. AI를 통제할 수 있는 충분한 대비책과 안전장치를 마련하면 얼마든지 효과적으로 활용할 수 있고, 다양한 분야에 AI 활용 성과를 극대화할 수 있다. 위에서 언급한 것처럼 AI가 급속도로 발전함에 따라 AI의 위험성에 대한 여러 가지 경고의 메시지들이 전파되어 세계 각국은 AI를 안전하고 효과적으로 통제하며, 활용할 수 있도록 윤리 기준을 제정하고, 보호장치 마련을 위해 적극적인 연구를 진행 중에 있다. 우리나라도 지난 2017년 과학기술정보통신부와 한국정보통신산업진흥원(NIA)이 함께 AI의 4대 윤리원칙을 발표하였으며, 그중에 통제가능성(Controllability)의 원칙을 군사적으로 활용시 핵심 원칙 중의 하나로 선정하여 제시하였다. 통제가능성(Controllability) 원칙은 지능정보기술 및 서비스에 대한 인간의 제어 가능성 및 오작동에 대한 대비책을 미리 마련하고, 이용자 권익보호 등 사회적 의무를 충실히 수행해야 한다고 정의하고 있다. 이는 AI를 활용하면서 의도하지 않은 피해를 방지하는 능력과 피해 상황 발생시 위험을 제거하는 능력을 갖추도록 보장하는 의미를 내포하고 있다. 군사적으로 AI를 활용시 운용적 측면에서 통제가능성(Controllability)에 대한 정책 및 제도 마련이 필요하며, AI 시스템의 오류나 취약점에 대처할 수 있는 기술적(시스템적) 측면에서 통제(제어) 가능성을 확보할 수 있는 수단과 방법에 관한 추가적인 연구도 필요하다.

5) 책무성(Accountability)

책무성(Accountability)의 사전적 의미⁴⁷⁾는 자신의 행동에 대한 책임을 지는 태도나 의식을 말한다. 즉 자신이 하는 일에 대한 책임을 물을 사람에게 설명할 수 있는 능력을 의미한다. 반면 책임성(Responsibility)은 책무성(責務性)과 달리 ‘어떠한 직무를 잘 수행 했는가?’라는 의미를 말한다. 쉽게 이야기하면 책무성(責務性)은 ‘설명할 수 있는 능력’이며, 책임성(責任性)은 ‘책임을 지는 능력’을 의미한다. 국내외적으로 다양한 AI 윤리 원칙의 연구자료를 분석해 보면 AI의 책무성(Accountability) 또는 책임성(Responsibility)과 관련된 윤리원칙은 대부분의 논문이나 연구자료에서 등장하고 있다. 특히 2023년에 발표된 AI 윤리원칙 기반의 윤리 측정지표 논문에 AI 윤리 책무성 원칙에 대한 측정지표가 제시⁴⁸⁾되어 있는데 우리는 이 부분에서 주목할 필요가 있다. AI의 윤리 책무성 원칙의 측정지표를 크게 준법성 측면과 책임 식별성 측면으로 분류하였으며, 준법성 측면에는 총 9가지로 법·제도 준수, 개인정보 제공 동의 획득, 데이터 사용 사전 허가 획득, 법적 근거 확보와 제시, 사용 설명서와 기능 일치성, 사용 범위 법적기준 문서화, 이용자 안전 우선 보호, 신고자에 대한 법적 보호, 이용자 요구사항 대응 등이 있으며, 책임식별성 측면에는 총 5가지로 설계자 책임식별, 제작자 책임식별, 운영자 책임식별, 이용자 책임식별, 개발자 책임식별 등이 있다. 이러한 내용들은 AI 기술 및 서비스에 대한 정보 공유, 사고 등에 대한 책임성(Responsibility)에 대한 분배를 명확하게 규정하고, 배상의 정도를 정확하게 측정하여 문제 발생시 누구에게 그 결과를 물어야 하는가에 대한 행위 주체별 책임에 대한 원칙을 정의하고 있다. AI의 개발부터 운용까지의 전 단계에 대한 책임(Responsibility)의 요소를 구체적으로 제시하여 국방분야 에서도 많은 부분에 있어서 적용의 필요성이 있는 것으로 판단되고 있다. 민간이나 국방의 다양한 분야에서 AI를 활용시 AI의 결정 및 행동에 대해 개발자와 운영자는 관련 부분에 대해서 책임을 져야 한다. 또한 AI 설계, 개발 및 활용 과정에서 주체를 설정함으

47) 책임성과 책무성의 정의: 국어대백과사전

48) 인공지능 윤리원칙 분류 모형 및 윤리 측정지표 개발과 신뢰성에 관한 연구: 성균관대학교, 소순주, 2020

로써 발생할 수 있는 피해나 오류를 최소화하도록 노력해야 하며 문제 발생시 책임소재를 명확히 하고, 이를 수정하거나 개선할 수 있도록 관련 절차의 마련도 필요하다. 결론적으로 국방 분야 AI는 민간분야와 달리 국가 안보, 군인의 안전과 생명, 전쟁의 승패를 좌우할 수 있는 영향력이 있는 만큼 책무성(Accountability)에 대한 중요성 인식이 높아야 하며, 신뢰할 수 있는 AI의 핵심적 윤리기준 요소로 관리될 수 있도록 해야 한다.

(2) AI 생애주기(AI Life Cycle) 연구

AI를 군사적으로 활용하는 데 있어서 정당성을 보장받기 위해 윤리기준(원칙)을 정립하고 가이드라인을 제시하여 활용하는 것도 중요하나 실질적으로 하나의 AI를 활용하기 위해 기획 단계에서 임무(Task:활용목적)를 정의하고, 개발과정을 거쳐 운용 및 관리를 하며, 일정 기간 활용 후 더는 사용되지 않거나 성능이 떨어져 활용성이 떨어지게 되면 폐기하는 단계까지 각 단계별 AI의 이력 관리(통제)와 추적이 가능하도록 ‘AI 생애주기(AI Life Cycle)’ 적용에 관한 연구가 필요하다. ‘AI 생애주기(AI Life Cycle)’를 적용하는 목적은 AI를 군사적으로 활용시 좀 더 투명하고 안전하며, 신뢰할 수 있게 AI를 개발하며 활용하고 있음을 증명할 수 있는 수단(체계)으로써 RAI(Responsible AI, 책임있는 AI)의 활용을 추구하고자 하는 국제사회의 추진 방향과도 일치하기 때문에 ‘AI 생애주기(AI Life Cycle)’ 적용을 위한 구체적인 추진 방법에 관해 연구가 필요한 실정이다. ‘AI 생애주기(AI Life Cycle)’ 관련 국내외 연구기관에서는 기획 및 요구분석, 데이터 수집 및 전처리, 모델 개발, 검증 및 평가, 배포, 운영 및 모니터링, 유지보수, 폐기 및 대체 등 다양한 단계로 분류하고 있으나 국방에서는 무기 및 전력지원체계 획득 절차와 효율성을 고려하여 소요 기획 단계, 개발단계, 운용/유지보수단계, 폐기단계 등 4단계로 분류하여 각 단계별 세부 기준과 행동화 지침을 마련해야 한다. 이러한 ‘AI 생애주기(AI Life Cycle)’ 기준과 단계별 세부 행동화 지침이 원활하게 적용되기 위해서는 이를 지원할 수 있는 법령(훈령), 규정 등 제도개선과 정책이 함께 추진되어야 한다.

제 2 절 미래 지속발전이 가능한 AI 기반체계 구축

(1) AI 기반체계 구축을 위한 효과적인 전략 및 정책 수립

AI를 개발하고 다양한 분야에 적용하기 위해서는 AI 3대 구성요소(알고리즘, 데이터, 플랫폼)가 필요하며, 지속적인 운용유지와 발전을 위해서는 이러한 3대 구성요소(알고리즘, 데이터, 플랫폼)의 체계적인 관리 시스템 구축이 선행되어야 한다. 현재 국방부 및 각 소요 군은 국방 분야에 AI 적용을 위해 자체적으로 추진전략과 정책 등을 수립하여 추진하고 있는데 이러한 전략과 정책의 추진에 있어서 가장 먼저 언급되는 분야가 바로 AI 기반체계 구축 분야이다. AI 기반체계 구축은 AI를 개발하여 활용하는 데 있어서 반드시 선행되어 갖추어져야 하는 필수분야로써 크게는 데이터 수집 및 관리, 모델 관리, 인프라, 보안 등 4가지 요소로 구분할 수 있으며 앞으로는 윤리기준까지 포함이 필요하다. 2021년에 국방부에서 발표한 국방 AI 추진전략 2.0에서는 2025년까지 기반조성기로써 AI 기반체계를 구축하고, 2026년부터 본격적으로 AI 서비스를 구현하여 고효율의 국방운영과 무기 및 전력지원체계에 AI 적용을 추진하려고 목표를 정하고 있으며, 각 소요 군에서는 2025년까지 AI 기반체계 구축을 위해 상급 부대와 연계하여 여러 가지 기반체계 구축사업과 제반 노력을 기울이고 있다. 그러나 아쉽게도 AI 기반체계 구축을 위한 상·하급 부대가 연계된 구체적인 추진전략이나 정책이 수립되어 있지 않아 AI 기반체계 구축이 체계적으로 추진되지 못하여 국방 분야 AI 적용을 가속화 시키는 데 많은 도움을 주지 못하고 있다. 따라서 상급부대 차원에서 AI 기반체계 구축을 위한 구체적인 추진전략과 정책을 수립하여 각 소요군이 다양한 국방 분야에 AI 적용을 가속화할 수 있도록 지원해야 한다. AI 기반체계 구축을 위한 추진전략과 정책 수립은 미래 국방 AI 기술이 지속적으로 발전될 수 있도록 위에서 언급한 AI 3대 구성요소(알고리즘, 데이터, 플랫폼)가 반영된 4가지 요소(데이터 수집 및 관리, 모델 관리, 인프라, 보안)에 대해서 구체적인 발전계획이 수립되어야 하며, 국방의 다양한 분야에 AI 적용 시 지속적으로 고도화(진화적) 발전이 될 수 있도록 각 요소별로 표준체

계(표준화)를 구성할 수 있도록 시스템적·제도적 기반을 마련해야 한다. 또한 AI 기반체계 구축의 예산은 대부분 국방 정보화 예산으로 지휘통신 체계 분야를 중심으로 발전계획을 수립하고 편성되는 경향이 있는데 이를 탈피하여 AI 기반의 미래 작전수행개념과 국방 AI 적용 개념을 지원할 수 있는 체계 구축에 중점을 두고 예산이 편성되고 집행이 될 수 있도록 전략과 정책을 수립하는 것이 필요하다.

(2) 수요자 전체를 위한 AI 인프라 구축 추진

국방부는 국방 AI 추진전략 2.0에서 ‘국방 AI 표준체계’ 기반의 D.N. A⁴⁹⁾ 인프라 구축을 제시하고 있다. ‘국방 AI 표준체계’는 국방의 모든 영역에서 수집된 데이터를 AI 체계에 적용하여 AI 학습을 이행하고, 학습된 AI 알고리즘(모델)을 적재적소에 재배포 및 활용하기 위해 일련의 시스템적·제도적 기반을 구성하는 체계로써 체계기반구조(시스템적 기반: 데이터 센터, AI학습체계, 유무선 통신망, 제도적 기반: 데이터 관리제도, 보안제도), AI 플랫폼, AI 서비스로 구분하여 인프라를 구축하고자 한다. 그런데 이러한 구축계획은 개발자와 관리자 중심의 인프라를 구축하는 계획이 많이 포함되어 있으며, 실제 AI를 사용하는 운용자(사용자) 입장에서의 인프라는 많이 반영되고 있지 못하다. 관리의 효율성과 개발의 용이성에 중점을 두고 인프라를 구축할 경우 실제 사용하는 운용자가 서비스 제공에 어려움을 겪을 경우 이러한 체계는 지속적으로 유지하기 어려우며, 체계를 변경하거나 개선할 경우 많은 시간과 예산을 투자해야 하는 어려움이 뒤따를 수 있다. 따라서 AI 인프라는 개발자, 운용자(사용자), 관리자 등 수요자 모두의 요구를 충족시킬 수 있도록 구축되어야 한다. 예를 들어 데이터의 수집·활용·저장·공유 등 관리체계를 구축할 경우 개발자 및 관리자 입장에서는 클라우드 기반의 인프라 구축이 서비스를 제공하거나 관리하는 데 장점이 많을 수 있으나 운용자(사용자) 입장에서는 중앙집중방식의 클라우드보다는 분산처리방식의 엣지컴퓨팅(온디바이스) 형태의 인프라 구축이 편리하기 때문에 훨씬 더 선호할 수 있다. 또한 국방 분야에 여러

49) D.N.A(Data, Network, AI): 국방 AI 추진전략 2.0(국방부, 2021)

가지 AI 모델 개발과 학습용데이터 구축 사업이 활발히 진행됨에 따라 다양한 플랫폼과 서버 등이 무수히 증가하고 있으나 이를 통합하거나 분산하여 관리할 수 있는 시스템이나 방법을 적용하기 위한 계획을 수립하는데 어려움을 겪고 있으며, 고성능의 GPU 자원이 다수 도입됨에 따라 점차 전력 사용에 대한 문제점이 대두되어 가고 있다. 따라서 AI 인프라 구축은 위에서 언급한 수요자 전체를 충족할 수 있으며, 미래에 예상되는 문제점들을 식별하여 해소할 수 있도록 단계별 로드맵을 수립하여 구축해 나아가야 한다.

제 3 절 사용자 중심의 AI 법규, 제도 및 정책 발전

(1) 국방전력체계 발전 지원을 위한 법률 및 행정규칙 개선

국방전력체계 발전을 지원하고 업무추진의 근거를 제공하고 있는 법제 업무는 크게 2가지로 구분할 수 있는데 첫째는 방위사업법, 국방과학기술혁신촉진법, 국방정보화법 등 다수의 법체계를 구성하고 있는 ‘법률’이 있으며, 둘째는 국방전력발전업무훈령, 국방기획관리기본훈령, 국방정보화업무훈령 등 법률의 하위 수준에서 활용되고 있는 ‘행정규칙’이 있다. ‘법률’과 ‘행정규칙’은 동일하게 법적인 효력을 가지고 있으나 성격과 제정 과정에서 차이점이 있다. ‘법률’은 국회의 의결을 통해 만들어지며, 헌법에 근거하여 국회의원들이 제정하다 보니 국방 분야의 충분한 전문지식과 발전방향성, 활용성 측면 등에 있어서 운용자(사용자) 중심에서 충분히 고려되지 않고 기본적인 법적 틀에서 제정되다 보니 구체적인 실행을 위한 방향성을 제공하기 어려운 실정이다. 이에 따라 각종 법률은 구체적인 실행을 돕기 위해 하위의 규범인 ‘행정규칙’을 제정하게 되는데 하나의 법률과 연계된 다수의 ‘행정규칙’들이 제정되고 있으며, 이러한 ‘행정규칙’을 제정하고 관장하는 부서가 다르다 보니 국방전력체계를 발전시켜 나가는 데 있어서 예산 운용이나 의사결정 등 다양한 분야에서 문제점들이 발생하고 있다. 또한 국방전력발전업무의 주요 시스템은 ‘법령(법률)’이 아닌 ‘행정규칙’ 중의 하나인 ‘국방전력발전업무훈령’에서 관련된 업무와 절

차를 총괄하여 추진함에 따라 다른 ‘법령(법률)’이나 ‘행정규칙’ 등을 통제할 수 있는 상위 법령으로서 위상을 갖지 못하여 국방전력체계 발전을 주도하지 못하고 있다. 특히 AI와 같은 첨단과학 기술은 무기체계 및 전력지원체계(정보체계 포함) 등 국방전력체계의 모든 분야에 적용될 수 있는 첨단과학 기술이다 보니 다양한 ‘법률’과 ‘행정규칙’에 적용되는 부분이 있어 국방 분야에 적용시 여러 가지 제한사항과 문제점에 부딪힐 가능성이 상존한다. 따라서 AI를 포함한 첨단과학 기술이 반영된 국방전력체계 발전을 체계적으로 추진하기 위해서는 현행 국방전력발전업무체계 프로세스의 근거가 되는 대표적인 ‘행정규칙’이나 ‘법률’이 국방전력발전업무 전체를 총괄하는 자격을 갖추어 추진해 나아갈 수 있도록 법제 업무상 상위 규범으로서 위상을 갖도록 개선 작업이 필요하다. 국방전력발전업무체계는 국방전력발전업무 훈령이라는 ‘행정규칙’에 근거하여 업무 프로세스를 적용하고 있으며, 이 훈령에는 국방전력체계의 핵심 분야인 무기체계 발전업무, 전력지원체계 발전업무, 국방군수관리 업무, 방위산업 지원 등의 요소가 모두 포함되어 있어 타 행정규칙이나 법률에 있어서 상위 규범으로서 위상을 갖게 될 경우 소요, 획득, 예산, 의사결정 등 다양한 분야에서 체계적인 업무수행과 효율성을 향상시킬 수 있어 국방전력체계 발전에 디딤돌 역할을 수행할 수 있을 것으로 판단된다. 아울러서 ‘행정규칙’이나 ‘법률’ 체계 개선시 관리자나 통제기관 중심에서 사용자 중심으로 개선시 국방전력체계 발전에 큰 시너지 효과를 볼 수 있을 것으로 예상된다.

(2) 상·하급 제대 연계성 유지와 구현 가능한 AI 전략 및 정책 수립

국방부는 2022년 국정 이행과제인 국방혁신 4.0 추진을 위해 5대 분야 12개 추진과제를 작성하여 발표하였으며, 국방부 예하 소 부대(서)는 국방혁신 4.0 구현을 위해 제대(부서)별 다양한 형태의 추진계획을 수립하고 이를 구현하기 위해 많은 노력을 기울이고 있다. 이러한 국방혁신 4.0 추진과제의 시행과 구현을 위해서는 국방부 및 합참 등 국방정책과 군사전략을 수립하는 최상위부대(서)에서 각 분야 및 과제별 추진을 위한 명확한 책임(주도)부서를 선정하고, 추진과제별 구체적인 로드맵을 작성

하며, 現 국방 군사력 건설의 추진 방향에 대한 연계성(전환)을 검토하는 등 실질적이고 시행 가능한 추진계획의 작성이 필요하다. 現 국방혁신 4.0 추진계획이 2022년 발표된 이후 이를 구현하기 위해 각종 세부 계획이 수립되고, 추진을 위한 전략 및 정책회의 등이 다양하게 개최되고 있으나 군사력 건설의 기준이 되는 국방기획관리체계상의 각종 기획 및 계획문서에 국방혁신 4.0 추진을 위한 구체적인 내용들이 체계적으로 반영되지 못하고 있어 국방부 및 합참, 각 소요군, 연구기관 등의 관련 부서에서는 이를 위한 대책 마련이 필요한 실정이다. 특히 국방부 및 합참 예하의 각 소요 군과 軍 관련 기관은 상급 부대의 전략과 추진 방향에 맞춰 정책 및 제도를 수립(연구)하고, 관련 사업의 소요를 제기하여 예산을 반영하고 절차에 의해 업무를 추진하기 때문에 국방기획관리체계 문서 내에 추진과제에 관한 내용이 반드시 포함되어야 한다. 또한 각 소요군 등 예하 부대(서)는 기획 및 계획문서에 반영된 전력체계와 첨단기술에 대해 전력화 및 연구개발을 추진하기 때문에 상급 부대에서는 이를 지원하기 위해 명확한 추진전략과 정책을 수립하여 하달해 주어야 한다. AI는 첨단과학 기술로써 활용성과 호환성(운용의 다양성), 성장성 측면에 많은 장점이 있으며, 미래 무기 및 전력지원체계 전 분야에 적용하여 활용이 가능한데 현재는 국방부 정보화정책관실을 중심으로 국방정보체계 및 국방운영(행정) 분야 중심의 전략과 정책 수립에 업무가 집중됨에 따라 무기체계 분야의 AI 적용을 위한 전략 및 정책 수립의 노력이 상대적으로 부족한 실정이다. 따라서 향후 무기체계 AI 적용 및 국방 전 영역의 AI 적용 가속화를 위해서는 국방부 및 합참의 무기체계 전력증강을 담당하는 부서를 중심으로 AI 적용을 위한 추진전략과 기획문서를 작성하여 각 소요군 및 관련 기관이 정책과 제도발전 계획을 수립할 수 있도록 상·하급 제대가 연계된 업무시스템을 구축해야 한다.

제 4 절 소요창출에서 획득체계까지 연계된 AI 발전 추진

AI는 일반적으로 독립적인 체계가 아니 각종 전력체계(무기체계, 전력지원체계, 정보체계 등)에 포함되어 해당 체계의 운용이나 성능의 향상을 지원하는 소프트웨어 기술로써 활용되는 특징이 있다. 이러한 AI를 국방의 다양한 영역에 적용하기 위해서는 각종 전력체계(무기체계, 전력지원체계, 정보체계 등)의 소요기획 단계에서부터 소요결정(신규 또는 성능개량 사업, 신속시범사업, 기타 실증사업 등) 과정에 이르기까지 업무 프로세스의 일부분에 반드시 포함되어야 한다. 그러나 현재의 각종 전력체계(무기체계, 전력지원체계, 정보체계 등) 업무 프로세스상에 AI를 포함하여 적용하는 일은 절대 쉽지 않다. 이러한 이유에는 여러 가지가 있을 수 있는데 대표적인 사례를 살펴보면, AI 기술은 다른 소프트웨어와는 달리 개발의 난이도와 고도의 전문성, 유지보수(고도화) 대책강구, 기술의 진부화 방지대책 마련, 소요 업무 담당자의 전문성 부족 등 여러 가지 제한사항과 문제점 때문에 소요 기획 및 소요결정 부서, 획득체계 담당 부서 등에서 각종 기획관리체계와 전투발전체계 문서 등에 AI를 제대로 반영하지 못하는 상황이 발생하고 있다. 이에 따라 각종 전력체계(무기체계, 전력지원체계, 정보체계 등)의 소요결정(신규 또는 성능개량, 신속시범사업 등) 과정에서 AI 분야는 자연스럽게 제외 또는 축소되거나 반영 시기가 지연되는 사례가 빈번하게 발생하고 있다. 따라서 이러한 문제를 조기에 해결하고, 각종 전력체계(무기체계, 전력지원체계, 정보체계 등)에 AI 적용 가속화를 위해서는 첫째, 각각의 단위 전력체계별로 소요창출 단계에서부터 소요기획, 소요결정, 획득(전력화)까지 유기적으로 연계된 업무시스템을 구축하여 업무를 추진하는 것이 중요하다. 현재 국방 분야의 AI 적용을 위해 다양한 부대(서)와 기관, 그리고 민간에서는 소요창출을 위한 아이디어 제시와 시범사업 및 실증연구를 활발하게 진행하고 있으므로 각 소요군 및 국방부 예하 부대에서는 이러한 소요들을 적극적으로 발굴하고 면밀한 검토를 통해 각종 전력체계(무기체계, 전력지원체계, 정보체계 등)에 소요(신규 또는 성능개량, 신속시범사업 등)를 반영하기 위한 소요제기서를

작성해야 하며, 합참 및 각 소요 군은 전력화(획득) 예산 확보를 위해 소요를 결정하고, 기획관리체계 및 전투발전체계 등의 관련 문서에 소요결정 내용을 반영하여 획득을 추진해야 한다. 두 번째는 전력운영비에 국방정보화사업 예산 중 AI 적용 확산을 위한 별도의 사업 예산(국방실험사업, 빅데이터선도사업, 정부부처 협력사업 등)이 있는데 이러한 예산들은 각종 전력체계(무기체계, 전력지원체계, 정보체계 등)의 AI 적용 지원을 위한 실증 또는 실험사업의 형태로 활용되지 못하고 있으며, 주로 AI 기반체계 구축, AI 학습용데이터 구축, 국방행정 효율화를 위한 AI 개발사업 위주로 진행됨에 따라 AI 관련 예산을 효율적으로 활용하지 못하고 있는 실정이다. 국방정보화사업은 국방정보화법, 국방정보화업무훈령, 국방정보화종합발전계획 등 자체 상위 법률 및 행정규칙과 발전계획에 의거 국방정보화체계 발전에 중점을 두고 자체적인 회의체나 의사결정기구(국방 CIO 등)를 통해 해당 분야에 필요한 사업 소요를 결정하여 추진함으로써 무기체계나 전력지원체계의 AI 적용 지원에 필요한 사업을 추진하지 못하고 있다. 따라서 이러한 문제점을 보완하기 위해 국방부 정보화정책관실에서는 국방정보화사업의 예산중 AI 적용 확산에 사용되는 예산(국방실험사업, 빅데이터 선도사업, 정부부처 협력사업 등)은 각종 전력체계(무기체계, 전력지원체계, 정보체계 등)의 전력화(획득) 소요제기 및 소요결정 지원을 위한 실증 및 시범사업에 적극적으로 반영시킬 수 있도록 추진해야 한다. 또한 국방부 및 합참의 전력담당부서와 각 소요 군의 전력(전력지원체계)담당 부서의 의견을 수렴하고, 소요결정을 위한 회의체 및 의사결정기구(CIO) 등에 무기 및 전력지원체계 업무 관련 부서들의 참여를 포함하여 각종 전력체계에 AI 적용이 적극적으로 반영될 수 있도록 실질적인 지원시스템을 구축하여야 한다.

제 5 절 AI 기술 특성과 소요를 고려한 AI 개념연구

(1) 수요견인 및 기술선도형 맞춤형 AI 개념연구 추진

국방 초 영역에 AI를 적용하기 위해서는 소요창출의 시작점이라고 할 수 있는 ‘운용개념(Operation Concept)’ 및 ‘구조화개념(Framework Concept)’ 등에 대한 개념연구가 반드시 필요하다. ‘운용개념(Operation Concept)’이 소요창출을 담당하는 기획자와 운용자 간의 인식 차이(Gap)를 해소하기 위한 틀(Framework) 이라면 ‘구조화개념(Framework Concept)’은 운용자와 개발자 간의 인식 차이(Gap)를 해소하기 위한 틀(Framework) 이라고 할 수 있다. 국방 전력체계(무기 및 전력지원체계)들의 전력화(획득) 방법은 대부분 ‘수요견인(Demand Pull)’ 방식으로써 개념연구 단계에서 ‘싸우는 방법(How to Fight)’의 연구를 통해 필요한 전력체계(무기 및 전력지원체계)의 운용개념을 정립하고, 기획관리 및 획득체계 절차를 거쳐 전력화(획득)를 추진한다. 최근에는 4차산업혁명의 발전으로 AI와 같은 첨단과학 기술을 각종 전력체계(무기 및 전력지원체계)에 신속하게 적용하기 위해 ‘기술선도형(Technology Push)’ 전력체계(무기 및 전력지원체계) 획득방식을 확대 적용해 나아가고 있다. 위에서 언급한 두 가지 방식 모두 전력체계(무기 및 전력지원체계)에 AI 적용시 개념연구 결과를 토대로 각각의 획득체계 방식을 통해 AI가 적용된 전력체계(무기 및 전력지원체계) 전력화(획득)를 추진하고 있으나 개념연구의 방법이나 내용의 깊이, 넓이 등에 있어서는 차이를 보이고 있다. 수요견인(Demand Pull) 획득체계 방식은 전통적인 전력체계 전력화(획득) 추진 방법으로써 선행연구(사전개념연구) 등을 통해 전력체계에 대한 개념연구를 깊이 있게 할 수 있어 획득체계 전반에 걸쳐 개발자와 운용자에게 운용개념을 제공할 수 있고, 개발의 방향성과 작전요구성능(ROC), 시험평가 등의 기준을 비교적 명확하게 식별 및 제공할 수 있어 운용자 중심으로 전력체계 개발을 추진해 나아갈 수 있는 장점이 있으나 전력체계 획득까지의 기간이 매우 오래 걸리기 때문에 기술 진부화(陳腐化)에 영향을 많이 받고, 조기에 성능개량 및 고도화에 대한 대책을 강구해야 하기 때문에 AI 기술을 적용하는데 어려

움이 많이 있다. 한편 기술선도형(Technology Push) 획득체계 방식은 상대적으로 짧은 기간에 전력체계의 전력화(획득)를 추진하는 장점이 있는데 반해 선행연구 및 사전개념연구와 같은 개념연구가 상대적으로 부족하여 전력체계 개발간 소요 기획자, 운용자, 개발자 간의 인식 차이(Gap)가 크게 발생할 수 있는 우려가 있으며, 운용자보다는 개발자 중심의 개발 추진으로 전력화(획득)하여 활용하는 데 어려움이 있고, 운용개념이 미흡하여 지속적인 운영유지가 어려울 수 있는 단점이 있다. 각 획득체계 방식의 특성과 장단점 등을 고려해 볼 때 무기체계에 패키지로 적용되는 AI 기술의 경우는 수요견인(Demand Pull) 획득체계 방식을 채택하여 무기체계의 성능발휘 여건이 보장될 수 있도록 AI 기술 진부화(陳腐化)를 방지할 수 있는 개념이 포함되어야 하며, 전력지원체계(국방정보체계) 등에 적용되는 AI 기술의 경우는 기술선도형(Technology Push) 획득체계 방식을 채택하여 전력체계에 AI를 쉽고 빠르게 적용할 수 있고, 지속적으로 운영유지가 가능할 수 있는 개념이 포함될 수 있도록 추진하는 것이 효과적이라고 할 수 있다. 결과적으로 이러한 수요견인(Demand Pull) 획득체계 방식과 기술선도형(Technology Push) 획득체계 방식은 각각의 장단점과 특징을 가지고 있어서 전력체계(무기 및 전력지원체계)의 특성을 고려하여 각각의 획득체계 방식에 맞게 AI 기술의 개념이 기획관리 및 획득체계에 반영될 수 있도록 관련 기관의 적극적인 제도개선 노력과 연구가 필요하다.

(2) 전력체계의 AI(지능화) 소요판단 절차 적용

전력체계(무기 및 전력지원체계)에 AI를 적용하기 위해서는 국방전력 발전업무 內에 각종 체계(기획관리체계, 획득체계, 전투발전체계 등)에 반영되어 절차를 거쳐 추진하는 것이 일반적인 방법이다. 일부 국방정보화 사업을 통해 추진되는 AI 사업은 실험 또는 시범 성격의 사업으로써 대상 체계의 전력화를 고려하지 않고, 기술 자체를 목표로 개발을 진행하거나 국방정보체계 內에 적용을 목표로 하여 국방 운영(행정) 분야 중심의 개발 및 사업이 진행되고 있다. 기술 자체를 목표로 하거나 대상 전력체계에 AI 기술을 적용하기 위해서는 다양한 방법과 절차들이 있을 수 있는데 기

존의 기획관리 및 획득체계 절차를 준수한 가운데 AI로 무엇을 할 것인가? 에 초점을 맞춰 시작 단계에서부터 논리적이고 체계적인 AI(지능화) 소요를 도출하는 것이 무엇보다도 중요하다. 따라서 전력체계에 AI 적용을 위한 시작 단계인 소요 기획 단계에서부터 아래의 [그림 4-2]처럼 ‘AI(지능화) 소요판단 절차’를 논리적이고 체계적으로 만들어 적용함으로써 전력화(획득) 절차가 원활하게 진행될 수 있도록 신뢰성을 보장해야 한다.

[그림 4-2] AI(지능화) 소요판단 절차(안)



제 6 절 개발자 및 운용자 중심의 보안 규제 해결방안 강구

국방 AI 적용에 있어서 보안 규제 문제는 개발자, 운용자, 관리자 등에 있어서 큰 제한사항으로 작용하고 있으며, 국방 AI 적용시 개발과 운용을 보호하고 감독하는 보호기관(보호자) 입장에서도 마찬가지로 국방 AI 개발 및 운용의 원활한 업무수행 여건을 보장하지 못하고 있어 어려움을 겪고 있다. 국방 AI는 각 전력체계에 포함되어 있는 소프트웨어들과 유사하게 해당 체계를 지원하는 기술로써 운용되는데 인간과 같은 지능을 보유하고 있는 특성 때문에 다른 소프트웨어와 차별되게 개발단계에서부터 운영유지, 성능개량(고도화), 폐기에 이르기까지 군사보안 측면에서 보호조치가 필요한 부분이 많이 있다. 이러한 이유는 AI 기술은 인간과 같이 인식, 추론, 판단, 학습 등의 지능을 갖추고 軍의 다양한 영역에서 의사결정을 지원하는 시스템으로 운용되기 때문에 개발 및 운용시 여러 가지 군사적 윤리기준(신뢰성, 견고성, 편향 방지, 설명 가능성, 책무성 등)을 고려해야 하고, 일반 소프트웨어들과는 달리 개발단계에서부터 3대 구성요소인 알고리즘(AI 모델), 데이터, 플랫폼 등에 대한 보안대책이 철저하게 강구돼야 할 필요성이 있다. 앞으로 近 미래에는 AI 기술이 대중화되어 대부분의 국가가 국방 분야에 AI를 활용하게 되는데 자국의 AI는 보호하고, 적국 또는 非 우방국의 AI를 공격할 가능성이 언제든지 남아 있다. 이때 AI는 데이터, 알고리즘, 플랫폼 등 어느 한 분야에서라도 적대적공격을 받을 경우 AI 성능에 치명적인 오류가 발생하여 軍의 의사결정 지원 임무수행 시 잘못된 결과를 제공할 가능성이 크다. 따라서 이러한 이유로 국방 AI 개발 및 운용 관련 시스템 보호기관(보호자) 입장에서는 국방 AI를 보호하기 위해 개발단계에서부터 폐기단계까지 AI 생애주기(AI Life Cycle) 전반에 대해 보안 가이드라인 또는 보호 대책을 강구하여 보안의 취약요소와 문제점을 제거하려는 노력을 기울이고 있다.

현재 우리 국방 분야의 AI 적용은 기반체계 구축단계로써 대부분 국방 행정의 정보체계 분야를 중심으로 AI 기술을 개발하고 있다. 국방전력발전업무 프로세스와 예산 문제를 이유로 아직은 무기 및 전력지원체계에

AI를 적용하지 못하고 국방 행정 중심의 정보체계에 적용 가능한 수준의 AI 기술개발이 대부분을 차지하고 있다. 이러한 정보체계 분야의 AI 개발 사례를 분석해 보면, 개발단계에서부터 운용 및 관리단계까지 여러 가지 보안대책 강구를 거쳐 현재 활용되고 있는 AI 체계들이 일부 있으며, 대부분 사업 단계에서 여러 가지 어려움을 겪었으나 특정한 보안 규제로 사업이 중단되거나 개발이 완료되지 못한 AI 체계는 없다. 이는 AI 사업 유형별로(모델 개발사업, 데이터 구축사업, 플랫폼 구축사업 등) 처음 시도하는 사업들이 많다 보니 데이터를 수집하여 학습용데이터를 구축하고, 오픈소스를 활용하여 AI 모델을 개발하며, AI를 운용할 수 있는 플랫폼 등을 軍 부대 내에 구축하는 과정에서 크고 작은 시행착오와 어려움을 겪다 보니 관련 기관의 협조와 업무수행 여건의 불편함(시간소요, 추가비용 발생 등)에서 오는 제한사항들이 대부분이다. 최근 3~5년 사이 다양한 AI 사업들이 각 기관별로 시행됨에 따라 유사한 보안대책 강구 과정을 거치면서 軍 관련 기관과 시스템 보호기관에서는 많은 노하우가 습득되었고, 민간 기업체 입장에서도 여러유형의 軍 사업을 시행하면서 보안대책 강구와 관련해서 자체적으로 대책강구와 기술을 많이 확보한 상태이다.

또한 AI는 軍의 의사결정을 지원하고 군사 업무의 효율성을 향상시키기 위한 목적으로 활용하기 위해 다양한 부서에서 개발을 추진하고 있는데 AI 개발시 군사보안 측면에서 가장 어려움을 겪고 있는 분야가 바로 데이터 분야라고 할 수 있다. 데이터를 제외한 나머지 알고리즘과 플랫폼 분야는 기존 정보체계의 소프트웨어 개발과 유사한 형태의 보안대책을 준용하면 큰 문제 없이 개발 후 적용이 가능하다. 그런데 데이터는 AI의 성능을 좌우하는 핵심 분야로서 AI를 개발하기 위해서는 데이터를 수집하여 가공 및 정제 과정을 거쳐 학습용데이터를 생성하여 AI 모델에 학습을 시켜야 하는 과정을 거쳐야 한다. 이외에도 성능개량(고도화)을 위해 지속적인 데이터 수집과 학습용데이터 생성작업 등 관리 및 제공(배포) 등의 과정을 수행해야 함에 따라 보안대책 강구가 필요한데 AI 모델별 데이터의 유형(이미지, 영상, 텍스트, 신호, 주파수, 자연어 등)이 다양하고 수량이 과다한 특징이 있어 보안대책 강구가 쉽지 않은 경향이 있다. 따라서

이러한 데이터는 개발자나 운용자의 요구 및 임무 정의(Task)에 따라 확보 기준의 한계를 정립하여 수집 및 관리, 제공 등의 업무를 추진해야 한다. 무분별한 데이터 확보와 관리체계의 부실은 AI 모델 적용에 위험 요소로 작용할 수 있으므로 개발하고자 하는 AI 모델에 맞춰 데이터 로드맵 구축을 통해 필요한 데이터만을 확보할 수 있도록 계획해야 한다. 이러한 데이터 구축체계가 정립되면 그에 따른 보안대책 강구 요소와 범위를 정하는데 용이하여 보호기관의 입장에서 개발자나 운용자의 업무수행 여건 보장을 위한 기준을 수립하는데 용이할 수 있다.

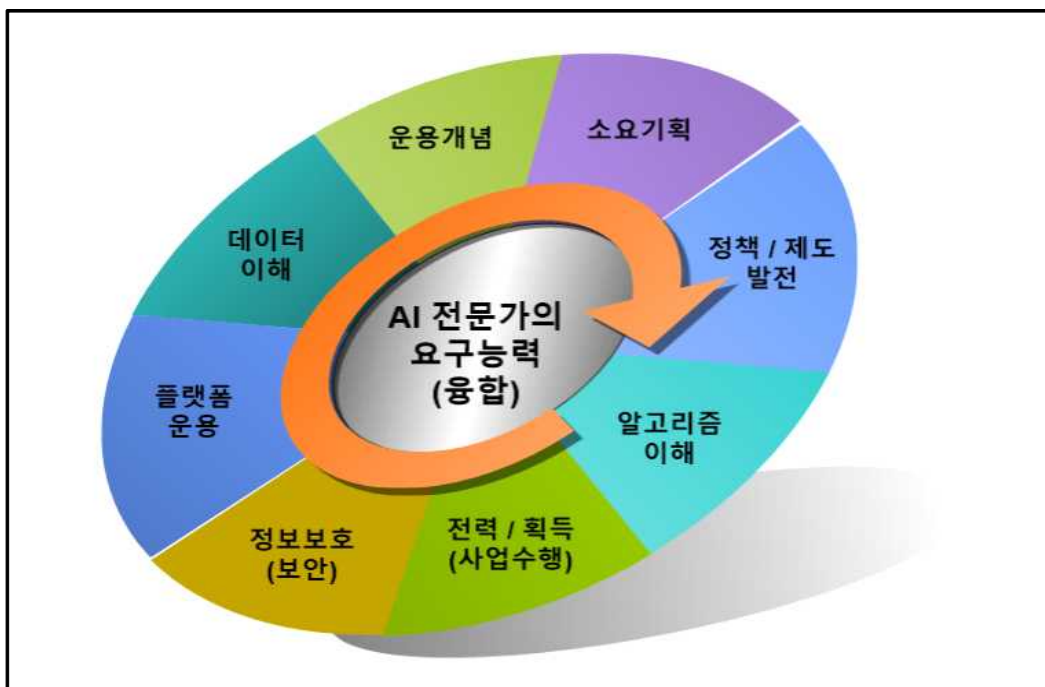
제 7 절 국방전력발전업무의 융합형 AI 전문인력 육성

국방 분야에 AI 적용 가속화를 위해서는 소요창출, 예산확보, 기반환경(인프라) 구축, 인재 육성 등 여러 가지 요소를 체계적이고 계획적으로 추진하기 위한 노력과 지원이 중요하다. 그중에서 가장 중요하다고 볼 수 있으며, 확보하기까지 많은 시간이 걸리는 분야는 인재 육성 분야일 것이다. 우리 軍의 AI 관련 전문인력은 2010년대 후반에 들어서부터 본격적으로 양성되기 시작되었으며, 2020년대에 들어서는 국방부가 국내 주요 대학과의 업무협약을 통해 대학원 학위과정에 軍 인력 TO(규정에 따른 적정 인원수)를 확보하여 적극적으로 전문인력 양성을 추진하고 있다. 그에 따라 2024년 현재는 초급간부로부터 대령급 고급 간부에 이르기까지 다양한 계층에서 석·박사 학위를 취득한 인원이 배출되기 시작하고 있다. 이와 더불어 국방부 및 각 소요 군은 軍 자체적으로 AI 관련 전문인력 양성을 위해 전문학위 교육 이외에 AI 특화교육, 소양 교육, 보수교육 등 자체적인 교육 프로그램을 신설하여 활발하게 운영하고 있다. 그런데 대부분의 교육 프로그램과 전문학위 교육은 기술적 관점(AI 알고리즘, 데이터, 플랫폼 등)에서 전문지식을 습득하기 위한 커리큘럼 중심으로 시행되고 있으며, 이렇게 습득한 전문지식을 바탕으로 국방전력발전 분야에 적용(응용)하기 위한 교육 진행은 소수에 불과하며, 교육내용 측면에서도 전문성과 업무 활용성이 낮은 수준에 머물고 있다. 현재 AI 전문인력 양성 정책과 제도는 AI 기술에 대한 전문지식을 습득한 軍 인력을 양성하는 데 초점이 맞춰 있다 보니 아직은 이를 활용하여 국방전력발전업무에 적용(응용)할 수 있는 능력을 갖추기 위한 교육은 시행되지 못하고 있다. 또한 AI 기술이 아직은 국방에 다양한 분야에 적용되어 활용되는 사례가 적다 보니 AI 기술을 다양한 국방 분야에 적용(응용)할 수 있는 방법을 습득하고 있는 전문가도 부족하며, 교육과정을 신설하여 운용할 수 있는 여

건이나 제도 수립도 제한되고 있는 실정이다.

따라서 이러한 제한사항을 극복하기 위해서는 AI 전문인력 육성에 대한 軍 내·외부 교육과정의 교육내용 변화와 AI 전문인력이 갖추어야 할 필요능력에 관한 연구와 그 능력을 구비시키는 방안에 대한 대책이 필요하다. 먼저, 첫 번째는 AI 교육제도의 변화로써 현재의 전문학위(석·박사 위탁교육, 능력개발 위탁교육 등) 교육은 現 시스템을 유지하여 AI 기술의 학문적 지식을 습득한 전문인력을 양성하며, 국방부 및 각 소요 군에서 자체적으로 운용 중인 AI 관련 軍 특화교육, 소양 교육, 보수교육 등은 AI 관련 전문지식 습득을 위한 교육내용 이외에 국방전력발전업무에 적용할 수 있는 응용 분야를 필히 교육해 AI 소요창출과 소요기획 등으로 이어질 수 있도록 추진해야 한다. 두 번째는 국방의 다양한 분야에 AI 전문인력을 육성하기 위해서는 아래의 [그림 4-3]에서 제시한 바와 같이 AI 전문가에게 필요한(요구되는) 능력이 무엇인지를 분석하고, 그 능력을 구

[그림 4-3] AI 전문가에게 필요한 요구능력



비하기 위한 효과적인 방법이 무엇인지를 찾아서 정책 및 제도적 관점에서 적극적으로 검토하여 추진할 필요성이 있다. AI는 다른 소프트웨어 기술과는 달리 국방의 모든 분야에서 활용이 가능한 고도의 첨단기술로써 다양한 분야(운용개념 연구, 소요기획, 전력/획득, 유지보수/관리, 성능개량 등)에 전문지식과 업무수행 경험(개념)이 없으면 적용하기 어려운 분야이다. 특히 AI는 일반 소프트웨어와는 다른 특징이 있어서 개발자 및 소요 기획자가 운용개념, 전력/획득(사업화), 유지보수/관리, 고도화(성능개량), 정보보호, 데이터, 알고리즘 등의 업무 분야를 제대로 알지 못할 경우 무기 및 전력지원체계에 적용시 어려움이 발생할 수 있으므로 여러 가지 업무 분야가 융합된 업무 지식의 습득이 반드시 필요하며, 이러한 융합된 업무 지식을 보유한 전문인력을 많이 양성시킬 수 있도록 해야 한다. 따라서 국방의 다양한 분야에 AI 적용 가속화를 위해서는 AI와 관련된 학문적 전문지식 습득을 바탕으로 군사 분야 AI의 운용개념 연구, 소요기획, 전력/획득(사업수행), 정책 및 제도발전, 정보보호, 기타 기술적 관리 분야(알고리즘, 데이터, 플랫폼 등) 등 AI 업무수행에 필요한 요구 능력을 갖춘 전문가를 많이 양성할 수 있도록 보직제도 개선과 軍 내부의 다양한 특화교육 및 소양 교육 프로그램 추진 등의 제도적 마련이 필요하다. 또한 국방의 쏠 분야에 균형된 AI 발전을 추진하기 위해서는 전투병과 및 비전투병과, 무기체계 및 전력지원체계 등 다양한 병과(특기)와 업무수행 분야에서 임무 수행 중인 인원들의 전문학위 교육과 軍 특화교육도 균형되게 추진하여 쏠 분야가 연계성을 유지하며 동시에 발전될 수 있도록 제도적 개선과 관심을 기울여야 한다.

제 8 절 국방 AI 컨트롤타워 및 실질적인 의사결정기구 운용

국방부 예하부서 및 각 소요 군은 국방 분야 AI 적용을 위해 다양한 조직과 기구들을 편성하여 운용하고 있다. 국방부와 각 소요군이 다양한 조직들을 동시다발적으로 편성하여 운용할 수밖에 없는 이유는 AI가 가지고 있는 고유의 특성에서 찾아볼 수 있다. AI는 일반적인 소프트웨어와 달리 3대 구성요소인 데이터, 알고리즘(AI 모델), 플랫폼(컴퓨팅 자원) 등으로 구성되어 있으며, 각 구성요소는 유기적으로 연계되어 기능 발휘를 통해 결과물을 제시하는 특징을 가지고 있다. 각 구성요소는 모두가 필히 확보되어야 하며, 확보되는 데 걸리는 시간과 소요 예산, 기술적 난이도는 상당히 높은 수준이며 무엇보다도 동시에 발전시켜 나아가야 하는 어려움이 있다. 따라서 국방부와 각 소요 군은 이러한 어려움과 중요성을 인지하여 각 기관별로 중요도(우선순위) 및 정책 방향에 따라 각 구성요소(데이터, 알고리즘, 플랫폼)의 발전을 위해 각 기관에서 필요한 조직을 편성하고 예산을 확보하여 업무를 추진하고 있다. 2010년대 중반 이후부터 국방부 및 각 소요 군은 데이터의 중요성을 인식하여 국방부 데이터담당관실을 중심으로 빅데이터 및 DB(데이터베이스) 관련 부서들을 각 소요 군에 많이 신설하여 데이터 구축 및 관리업무를 중점적으로 추진하였으며, 2010년 후반부터는 AI 관련 연구 및 개발센터, 소요 및 정책 발전부서(과) 등의 조직을 편성하여 본격적으로 국방 분야에 AI 적용을 위한 업무를 추진하고 있다. 2024년 현재는 국방부 및 예하 부설기관과 각 소요 군 등에 다양한 AI 조직들이 편성되어 있으며, 제각기 국방 분야에 AI 적용을 위해 많은 노력을 기울이고 있다. 그러나 여러 조직들이 신설되어 운용되고 있으나 다양한 국방 분야에 AI 적용은 미흡한 실정이다. 대부분은 국방 행정(정보체계)의 효율화 및 최적화 추진을 위한 AI 적용 사업(개발)과 미래 AI 개발 및 연구에 필요한 데이터 구축사업을 중심으로 추진하고 있으며, 무기 및 전력지원체계 AI 적용을 위한 업무는 제대로 추진되지 못하고 있다. 이러한 이유에는 여러 가지가 있을 수 있는데 대표적으로 두 가지 정도 이유를 들 수 있다. 첫째는 AI와 관련된 예산업무를

담당하는 부서, 국방 AI 소요의 기획 및 결정 업무를 담당하는 부서, AI 정책 및 제도 발전업무를 담당하는 부서 등 국방 AI 적용에 있어서 핵심적인 분야에 업무를 추진하는 부서들의 업무를 융합하고, 조정·통제 과정을 거쳐 올바른 방향으로 이끌어갈 수 있는 컨트롤타워 조직의 부재를 들 수 있고, 둘째는 조직법상에 상급부서는 아니지만 각 부서에서 수행하는 AI 업무의 정책과 업무추진 방향성 등을 일치시키고, 사업추진을 위한 소요결정 및 예산 할당 등의 의사결정 업무를 수행할 수 있는 회의체로써 의사결정기구의 부재를 들 수 있다. 따라서 이 두 가지 문제점을 개선하고 국방 AI 적용의 가속화를 보장하기 위해서는 다음과 같은 발전방안 적용이 필요하다.

첫째, 국방 AI 적용 가속화를 위해 국방부 및 각 소요 군에서는 AI 개념연구, 소요 기획, 정책 및 제도 수립, 사업수행, 개발, 시험평가, 데이터 구축 등 여러 가지 업무를 수행하기 위해 다양한 AI 부서를 운영하고 있는데 이러한 부서들이 추진 중인 업무의 방향성을 일치시키고, 중복성을 배제하며, 유기적인 협조체계를 구축하여 시너지를 발휘할 수 있도록 각 소요 군별 AI 업무의 실질적인 조정·통제 역할 수행이 가능한 컨트롤타워 조직을 편성하여 운용한다. 이러한 컨트롤타워 조직은 여러 부서들의 업무를 체계적이고 효과적으로 조정·통제할 수 있도록 3대 핵심 업무(정책 및 제도 수립, 소요 기획, 예산 등) 분야에 대한 통제력을 필히 확보하고 업무를 추진해야 한다. 둘째는 실질적인 권한과 책임을 가지고 있으며 AI 발전을 지원할 수 있는 의사결정기구의 운용이다. AI는 앞서 여러 분야에서 언급하였듯이 모든 무기 및 전력지원체계에 적용하여 활용할 수 있는 첨단과학 기술 이다 보니 특정한 부서나 컨트롤타워 조직만을 가지고 국방의 모든 분야에 AI 적용을 통제하며 추진할 수는 없다. 특히 국방전력 발전업무는 전투발전의 7대요소(교리, 구조·편성, 교육훈련, 무기·장비·물자, 리더십, 인적자원, 시설 등)를 중심으로 각 기관 및 부서에서 법령과 규정에 따라 다양한 업무절차(프로세스)를 거쳐 여러 유형의 예산을 활용하여 업무를 추진해 나아가고 있으며, 각 업무 분야에서 효율성을 향상시키고, 발전을 도모하고자 AI 적용을 추진하고 있다. 그러나 정보화부서 등

일부 부서를 제외하고 대부분의 부서가 AI 적용을 위한 예산을 확보하고 있지 못하기 때문에 균형된 전투발전 추진과 AI 예산 활용의 투명성 보장을 위해 각 부서의 결정권자들이 모여 국방 AI 적용을 위한 정책 결정이 이루어질 수 있도록 의사결정기구(회의체)를 운용하는 것이 중요하다. 이러한 의사결정기구(회의체)는 AI 컨트롤타워에서 조정·통제할 수 있는 분야가 아닌 국방부 또는 각 소요 군별로 해당 제대에서 AI 적용을 위해 필요한 중요분야에 대해 우선순위 및 예산편성 등의 정책안건 결정을 추진함으로써 통합적이고 신뢰성 있는 업무수행체계의 구축이 가능하여 체계적인 AI 발전을 추진하는 데 큰 도움이 될 수 있을 것으로 판단된다.

제 5 장 결론

AI는 국가산업 전반에 혁신을 선도하는 4차 산업의 핵심기술로 자리를 잡고 있으며, 산업의 쏠 영역에 적용되어 생산성 증대 및 효율성 향상 등 혁신을 창출하면서 기존의 경쟁 구도에 근본적인 변화를 촉발하고 있다. 또한 미국, 중국 등 주요국은 AI 주도권 확보를 위해 국가적인 노력을 기울이고 역량을 결집하여 국가 차원의 AI 정책을 공표하며, 대대적인 투자와 개발에 집중하고 있다. 아울러서 국방 분야에도 많은 영향을 끼치게 되어 주요국을 중심으로 국방 분야에 AI 적용을 위한 막대한 예산과 인력을 투자하여 AI 기술 주도권을 확보하기 위해 사활을 걸고 있다. 미래에는 현재보다 더 확장되고 복잡한 전장 환경에서 전투를 수행해야 함에 따라 AI가 Game Changer이자 병력감축 시대의 핵심적 대안으로써 역할을 수행할 것으로 예상된다. 이에 따라 주요국들은 안전하고 신뢰성 있는 AI를 확보하기 위해 윤리원칙을 제정하고, 거버넌스 체계를 정립하여 체계적으로 국방 AI를 적용할 수 있도록 다양한 전략과 정책을 추진해 나가고 있다. 그러나 이러한 AI는 기술적 특성과 軍 특수성으로 인해 군사적으로 활용시 여러 가지 제한사항 및 문제점을 가지고 있다. 이러한 제한사항과 문제점들을 분석해 보면 먼저, 윤리적 관점에서 인간에게 위협이 될 수 있는 위험성이 있고, AI 기반체계를 구축하는 데 오랜 시간이 소요되며, AI 적용을 위한 법과 규제의 개선 소요 그리고 소요 기획 및 획득을 위한 운용개념의 정립 등이 필요하다. 또한 국방 AI 적용을 위해 우수한 AI 전문인력이 필요하고, 산재되어 있는 AI 조직을 조정·통제할 수 있는 컨트롤 타워의 신설이 필요하며, 중요 정책이나 사업 소요를 결정할 수 있는 의사결정기구(회의체)의 운용이 필요하다. 따라서 이러한 제한사항 및 문제점들을 해결하고 국방 AI 적용 가속화를 지원하기 위해 8가지의 발전방안을 정립하였으며, 주요 내용은 다음과 같다. 첫째는 AI는 인간과 유사한 지능을 보유하게 됨에 따라 윤리적 관점에서 문제점 및 위험성이 발생할 가능성이 있어 이를 해결하기 위해 군사적 활용에 적합한 윤리기준을 정립해야 하고, 둘째는 일반 소프트웨어와는 달리 데이터, 알고리즘, 플랫폼 등으로 구성되어 유기적인 연계성을 통해 성능을 발휘하는 특성을 고려하여 지속적으로 발전이 가능

한 AI 기반체계를 구축하여야 한다. 셋째는 국방 AI도 민간분야의 AI와 유사하게 법과 제도, 전략과 정책 등의 수립을 통해 단계적이고 체계적인 발전을 유도해야 하며, 넷째는 소요창출로부터 획득체계까지 국방전력발전업무 절차와 연계된 발전시스템을 구축해야 한다. 다섯째는 국방 분야에 AI를 어떻게 적용하여 활용할 것인가에 대한 명확한 운용개념을 정립하여 소요창출 및 소요 기획을 지원해야 하고, 여섯째는 국방 분야에 AI 적용시 여러 가지 보안규제를 해결하기 위해 개발자나 운용자 중심에서 제한사항 및 문제점을 식별하여 맞춤형 해결방안을 모색해야 한다. 일곱 번째는 AI를 국방의 쏠 분야에 적용하기 위해서는 특정 분야의 전문지식만을 가지고 업무를 추진하는 것이 아니라 운용개념 연구, 소요기획, 전력 및 획득, 정책 및 제도수립 등 다양한 분야에 대한 전문지식 습득이 필요하므로 국방전력발전업무 절차 전반의 전문지식을 갖춘 융합형 인재의 육성이 필요하다. 마지막 여덟 번째로는 국방부 및 각 소요 군에 흩어져 있는 각종 AI 조직을 실질적으로 조정·통제할 수 있는 컨트롤타워의 신설이 필요하며, AI 사업소요, 정책 및 제도 결정 등 중요 사안에 대한 의사결정을 수행할 수 있는 별도의 의사결정기구(회의체) 신설도 필요하다.

이상과 같이 국방 AI 적용시 최근 수년간 걸림돌로 작용되어왔던 제한사항과 문제점 등을 분석해 보았고, 이에 따른 발전방안을 제시해 보았다. 이 연구는 국방전력발전을 위해 노력하는 모든 구성원들이 국방 AI 적용을 위한 업무추진시 AI의 기술적 특징과 軍이 가지고 있는 특수성을 이해하고, 발생가능한 제한사항과 문제점을 조기에 식별하여 해결방안을 모색함으로써 국방 AI 적용 업무를 수월하게 추진하는 데 도움이 될 수 있을 것으로 판단된다. 그러나 본 연구에서 제시한 국방 AI 적용시 제한사항 및 문제점과 발전방안에 관한 연구는 주관적이고 개념적인 내용이 반영되어 있을 수 있다. 이는 국방 AI를 적용하기 위한 연구와 개발의 역사가 짧아 과학적 분석을 위한 데이터가 제한되어 특정 기관 및 인원들의 경험적 요소와 주관적 견해가 들어있을 수밖에 없다. 따라서 앞으로 이러한 개념연구 수준의 연구 결과를 구체적으로 분석하고 실행으로 옮길 수 있는 후속 연구가 진행될 경우 국방 분야의 AI 적용은 현재보다도 한 단계 더 발전된 수준에 도달할 수 있을 것으로 기대해 본다.

참 고 문 헌

1. 국내문헌

- 1) 육군 AI 통합 로드맵 2022-2033(육군 교육사, 2021)
- 2) '23~'33 인공지능 종합발전계획(육군 교육사, 2022)
- 3) 국방 인공지능(AI) 추진전략 2.0(국방부, 2022.3.)
- 4) 미래국방 2030 AI 기술전략(국방기술진흥연구소, 2022)
- 5) 전자통신동향분석 ATL 1.0: 인공지능 기술 수준 정의
(한국전자통신연구원, 2020)
- 6) 한국전자통신산업진흥회 이슈 리포트 2023-13호(KEA, 2023)
- 7) 인공지능과 로봇의 군사적 활용과 선행 과제: 한국국방기술학회 논문지
(송윤선, 2021.3.)
- 8) 인공지능 자율무기시스템에 대한 심층분석(박상우, 2024.4.)
- 9) 국방 AI 참모 시스템 개발 보도자료(한화시스템, 2022.11.)
- 10) 다출처영상융합체계 전력화 완료 보도자료(방사청, 2022.12.)
- 11) 'GOP의 눈' AI 경계작전센터에 가다(보도자료, 2024.5.)
- 12) KIMA 뉴스레터 제703호(한국군사문제연구원, 2020.3.)
- 13) 인공지능 윤리기준(과학기술정보통신부, 2020)
- 14) '2024 AI의 책임있는 군사적 이용에 관한 고위급회의(REAIM)'
결과 보도자료(2024.9.10.)
- 15) 2024 세계신안보포럼 라운드테이블 발표자료(양병희, 2024.10.)
- 16) 국방 인공지능센터 창설 및 운영방안 연구
(한국국방기술학회, 2023.4.)
- 17) 해외 주요국의 국방 AI 현황 연구(이지은 외 2인, 2023.3.)
- 18) THE AI REPORT 2021(NIA AI미래전략센터, 2021)
- 19) 국방분야 인공지능 기술 도입의 주요 쟁점과 활용 제고방안
(윤정현, 2021.8.)
- 20) 4차 산업혁명시대 중국의 군사혁신: 군사지능화와 군민융합(CMI)
강화를 중심으로(차정미, 2020)

- 21) 미·중·러의 국방 인공지능 정책 방향과 시사점(안보전략연구센터, 2020)
- 22) 국방혁신 4.0 기본계획(국방부, 2023.3.)
- 23) ‘국가 AI 전략 정책방향’ 발표(과학기술정보통신부, 2024.9.)
- 24) 육군 인공지능(AI) 추진전략(육본 정책실, 2024.5.)
- 25) 국방혁신 4.0 해군추진계획(해군 정보화부, 2022)
- 26) 공군 인공지능(AI) 발전계획(공군 정보화부, 2021.5.)
- 27) 사람이 중심이 되는 인공지능(AI) 윤리기준(과학기술정보통신부, 2020)
- 28) 국방기획관리기본훈령(국방부훈령 제2627호, 2022.2.3. 시행)
- 29) 국방정보체계 획득절차 개선(고광춘, 2022.10.13.)
- 30) 인공지능 윤리원칙 분류 모형 및 윤리 측정지표 개발과 신뢰성에 관한 연구 (성균관대학교 소순주, 2020)

2. 국외문헌

- 1) 포브스: “7 Type of Artificial Intelligence”(2019.6.19.)
- 2) AI 거버넌스란 무엇인가?(팀 무치 외 1인, 2023.11.)
- 3) CDAO 홈페이지(www.ai.mil)
- 4) 영국 국방부 국방 인공지능 전략(2022.6.)
- 5) 독일 연방정부의 국가적 인공지능 전략 개정판
(Fortschreibung KI Strategie BReg DeZember 2020)
- 6) 독일군 「국방업무 영역에서의 인공지능 활용」 개념서
(육군 교육사 국외교환교관 연구자료, 2021)
- 7) Algorithmic Warfare Applying Artificial Intelligence to Warfighting
(Peter Layton, 2018)
- 8) 중국이 AI를 활용한 군사력 증강을 목표로 하는 방법,
Javin Aryan, This is the 119th article in the series-The China Chronicles
- 9) “Will Russia Rule the World Through AI?” The RUSI Journal
(Keith Dear, 2019)
- 10) EMERiCs 신흥지역정보종합포털, “러시아 AI에 주력”,
러시아 Tass 등(2019.10.)
- 11) ‘러시아軍, 우크라이나에 세계 최초 인간 살상용 로봇 ‘마커’ 투입’
(인터넷 보도자료, 2023.2.)

부 록

국방 분야의 AI 적용시 제한사항 및 문제점으로 작용하고 있는 요소의 식별과 우선적으로 발전시켜야 할 핵심 분야에 대한 설문조사

본 설문조사는 국방 분야에 AI 적용시 걸림돌로 작용하는 여러 가지 제한사항 및 문제점을 식별하고, 이러한 제한사항 및 문제점이 국방 AI를 적용하는데 얼마나 큰 걸림돌로 작용하고 있는지 각계각층 전문가들의 설문을 통해 내용을 구체적으로 분석하고 발전방안을 도출하고자 합니다.

국방 분야 AI 적용시 제한사항 및 문제점은 군·산·학·연의 다양한 기관에서 공통적으로 느끼고 있는 분야에 대해 인터뷰, 토론, 의견수렴 등을 통해 도출하였으며, 식별된 여러 가지 제한사항 및 문제점을 중심으로 국방 AI 발전 가속화를 위해 우선적으로 해결해야 할 핵심 분야 4가지를 도출하여 국방 AI 발전 가속화 업무를 추진하는 데 활용하고자 합니다.

설문은 총 6개의 항목으로 구성되어 있으며, 이 중 4개의 항목은 설문자의 전문성과 인식을 조사하는 분야로 단답형으로 응답하시면 되고, 2개 항목은 핵심 분야로 가중치를 고려하여 해당하는 란에 ○(혹은 √) 표시를 해주시기를 바랍니다.

아무쪼록, 이 연구가 국방 분야에 AI 적용 가속화에 많은 기여를 할 수 있도록 여러분의 적극적인 협조를 부탁드립니다.

< 본 설문에 기재된 모든 정보는 익명으로 처리하며, 오직 연구 목적으로만 사용됨을 알려드립니다.>

2024.11.25.

연구원 : 이 상 열

<설문서 내용>

1. 귀하의 직업은 어디에 해당합니까? ()
 - ① 현역(예비역) 군인 : 계급 ()
 - ② 교수/연구원 : 직급 ()
 - ③ 공(군)무원 : 직급 ()
 - ④ 기타 기업체/공공기관 : 직급 ()
2. 귀하께서 종사하고 있는 국방 AI 관련 업무 분야는 무엇인가요? ()
 - ① AI 개념연구 업무 ② AI 관련 사업
 - ③ AI 소요기획 업무 ④ AI 전문인력 관련 업무
 - ⑤ AI 조직 관련 업무 ⑥ AI 교육 및 정책발전 업무
 - ⑦ AI 법규 및 제도 관련 업무 ⑧ AI 관련 협력업무
 - ⑨ AI 전력화 추진업무 ⑩ 기타()
3. 귀하께서는 국방 AI 관련 업무를 수행한지는 얼마나 되었습니까? ()
 - ① 1년 이내 ② 1년 ~ 2년
 - ③ 2년 ~ 3년 ④ 3년 ~ 4년
 - ⑤ 4년 이상
4. 귀하께서는 우리 국방 분야에 AI 적용이 정상적으로 잘 추진되고 있다고 생각하십니까? ()
 - ① 매우 그렇다
 - ② 그렇다
 - ③ 보통이다
 - ④ 그렇지 못하다
 - ⑤ 매우 그렇지 못하다

5. 국방 AI 적용시 제한사항 및 문제점으로 작용하는 여러 가지 요소에 대해 각 요소별 귀하가 생각하는 점수를 부여해 주시기 바랍니다.

국방 AI 적용시 제한사항 및 문제점으로 작용하는 요소	매우중요한 문제이다 (4점)	중요한 문제이다 (3점)	문제로 보인다 (2점)	잘 모르겠다 (1점)	문제로 보이지않음 (0점)
군사보안 규제					
AI 윤리기준 미 정립					
AI 기반체계 구축 미흡					
AI 개념연구 부족					
AI 전문인력 부족					
컨트럴타워 등 전문조직 운영 미흡					
AI 법규 및 제도개선 미흡					
軍내 의사결정기구 운용 문제					
AI 전략수립 및 제도발전 미흡					
획득체계 및 기획관리체계 등 전력발전업무체계의 구조적 문제					
기타()					

6. 귀하가 생각하기에 국방 AI 적용 가속화를 위해 가장 우선적으로 발전시켜야 할 중요분야는 3가지는 무엇이라고 생각하는가?

(가중치: 1순위 4점, 2순위 3점, 3순위 2점, 4순위 1점)

(1순위: 2순위: 3순위: 4순위:)

- ① 군사보안
- ② AI 윤리기준 미정립
- ③ AI 기반체계 구축
- ④ AI 개념연구
- ⑤ AI 전문인력 확보
- ⑥ AI 컨트롤타워 신설
- ⑦ AI 법규 및 제도개선
- ⑧ 軍내 강력한 의사결정기구 운용
- ⑨ 구체적인 AI 전략 및 정책 수립
- ⑩ 국방전력발전업무체계 상 AI 적용을 위한 업무절차 개선

ABSTRACT

A study on how to accelerate the application of defense AI considering AI ethical standards

Lee, Sang-Yeol

Major in Defence AI Convergence

Dept. of Defence Force Power

Graduate School of National Defense Science
Hansung University

The Fourth Industrial Revolution is rapidly spreading throughout all areas of society, bringing about various changes. AI, a core field of advanced science and technology, is a leading field of the Fourth Industrial Revolution and is innovating in various fields of defense, and is competitively promoting R&D in several countries around the world, including some major countries. Our military is also making great efforts to apply AI in the fields of defense weapons and power support systems, and defense administration, but unfortunately, it is not easily applied due to various limitations and problems. Therefore, this paper identifies the limitations and problems that are acting on the application of AI to the defense field, and presents development plans from the perspective of AI ethics and defense domain.

There are two major restrictions and problems in the application of AI to the defense sector. The first is a common concern in the private sector, which is 'Can you create a reliable AI?' from an AI ethical perspective. There can be many factors that can affect the reliability of AI. In the application of AI in the defense sector, five major factors such as safety, transparency, robustness, controllability,

and accountability are judged as key factors from an ethical point of view (ethical standards), including limitations and problems arising from these factors. Second, from the perspective of the defense domain, there are various limitations and problems arising from the military's unique specificity and work promotion system, such as AI-based systems, strategies and policies, interconnection of various instructions, conceptual research for AI application, recognition of military security, operation of AI professionals and organizations, and decision-making systems.

To address these two limitations and problems, the following eight development measures were proposed. The first is the establishment of an ethical standard for the application of reliable defense AI, the second is the establishment of an AI-based system that can sustainably develop in the future, the third is the development of user-centered AI laws, systems, and policies, the fourth is the promotion of AI development linked from demand creation to acquisition systems, the fifth is an AI conceptual study that considers the characteristics and needs of AI technology, the sixth is the development of a security regulation solution centered on developers and operators, and the seventh is the development of a convergent AI expert in defense power generation work, and the eighth is the operation plan of a defense AI control tower and a practical decision-making mechanism. The eight development measures presented above suggest the concept of solutions to effectively solve limitations and problems in applying AI to the entire area of defense in the future. It is hoped that this study will serve as the foundation for various follow-up studies in the future and contribute significantly to early resolution of various difficulties in defense AI.

[Keywords] AI Ethical Perspectives, reliable AI, defense domain perspective