Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 9 pp. 341-349, 2023

https://doi.org/10.5762/KAIS.2023.24.9.341
ISSN 1975-4701 / eISSN 2288-4688

인공지능(AI) 기술 도입을 위한 정책 및 적용사례와 한계점에 대한 연구

강지훈*, 정민경, 박주영, 이원영, 최은진
국방기술품질원

A Study on the Policies, Application cases and Limitations for the Introduction of Artificial Intelligence(AI) Technology

Ji Hoon Kang*, Min-Kyung Jeong, Joo-Young Park, Won-Young Lee, Eun-Jin Choi
Defense Agency for Technology and Quality

요 약 4차 산업혁명에 따른 디지털화, 자동화, 인공지능, 빅데이터 등의 기술혁신이 빠르게 진행되고 있으며, 이는 제품의 개발, 설계, 제조, 운용 등 다양한 분야에서 패러다임의 전환을 일으키고 있다. 특히, 인공지능 기술은 4차 산업혁명을 이끄는 중요한 요소로 기계학습과 딥러닝 알고리즘의 발전으로 인해 컴퓨터 비전, 음성인식, 자연어처리 등의 분야에서 높은 성능을 보이며, 이러한 기술은 이미 다양한 상용 제품 및 서비스에 적용되고 있다. 또한, 미국과 중국을 중심으로 전투원의 생존성을 향상시키고, 전투 효율성을 극대화하기 위한 수단으로 국방 분야에도 인공지능 적용이 활발하게 연구되고 있으며, 우리나라도 국방 분야에 인공지능 도입을 위하여 국방 인공지능 컨트롤타워인 국방AI센터 설립 등 많은 노력을 기울이고 있다. 이에, 본 논문에서는 민수/국방 분야 인공지능 기술 도입 필요성은 인식하고 현재 추진 중인 정책/전략 및 적용사례와 한계점에 관하여 연구하였으며, 결론적으로 향후 인공지능 기술을 활용한 목표의 다각적 설정 및 신뢰성 측면의 연구에 대한 중요성을 제시하였다. 본 논문의 결론을 바탕으로 향후 국방 분야에 신뢰를 기반으로 한 인공지능 기술 도입을 위한 효율적인 연구 수행 방향 설정에 도움이 되었으면 한다.

Abstract Technological innovations such as digitalization, automation, artificial intelligence, and big data are progressing rapidly as a result of the 4th Industrial Revolution, which is causing a paradigm shift in various fields, such as product development, design, manufacturing, and operation. In particular, artificial intelligence technology is playing a pivotal role in the 4th Industrial Revolution thanks to the advancements in machine learning and deep learning algorithms. It demonstrates high performance in fields such as computer vision, speech recognition, and natural language processing, and these technologies are already being applied to various commercial products and services. In addition, the application of artificial intelligence is being actively studied in the defense field as a means to improve the survivability of combatants and maximize combat efficiency, which is mainly being done in the United States and China. South Korea is also making significant efforts to introduce artificial intelligence in the defense field, including initiatives like the establishment of the Defense AI Center, which serves as a control tower for defense artificial intelligence. Accordingly, in this paper, we discuss the necessity of introducing artificial intelligence technology in civil and defense applications. We studied the current policies and strategies, application cases, and limitations. The importance of research on multifaceted settings and reliability aspects of goals using artificial intelligence technology is also discussed. The conclusions of this paper could help set a direction for efficient research for the introduction of trust-based artificial intelligence technology in the defense field.

Keywords : 4th Industrial Revolution, Artificial Intelligence, Application Cases, Limitations, Policies

*Corresponding Author : Ji-Hoon Kang(Defense Agency for Technology and Quality)
email: jh1989@dtaq.re.kr
Received July 7, 2023 Revised August 2, 2023
Accepted September 1, 2023 Published September 30, 2023

1. 서론

4차 산업혁명은 2016년 다보스에서 열린 세계경제포럼에서 처음 언급된 개념으로서 인공지능(AI), 빅데이터(Big Data), 사물인터넷(IoT) 기술을 근간으로 초연결 기반의 지능화 혁명으로 정의할 수 있다[1].

현재 4차 산업혁명으로 인한 패러다임 전환 속에서 변화에 발맞추기 위해 선진국을 중심으로 제도개선, 기술개발, 교육 등 다양한 측면에서 과업이 수행되고 있다. 우리나라도 4차 산업혁명에 대한 중요성을 인식하고, 2016년부터 정부 주도하에 4차 산업혁명 민군기술협력사업을 통해 기술개발 등 4차 산업혁명 대응을 위한 생태계 조성을 추진하고 있으며, 매년 예산 증액을 통해 투자를 확대하고 있다[2]. 특히, 4차 산업혁명의 핵심 기술 요소로 손꼽히는 인공지능에 대한 투자가 대폭 증가하고 있으며, 이를 기반으로 우리 사회 전반에 인공지능 기술이 적용된 다양한 제품들을 접할 수 있게 되었다. 대표적으로 컴퓨터 비전, 음성인식, 자연어처리 기술 분야의 높은 성능을 기반으로 개발된 지능형 CCTV, 음성인식 AI 비서, ChatGPT-4를 예로 들 수 있다.

민수 분야에서 이러한 인공지능 관련 기술확산이 최근 미국, 중국 등을 중심으로 전투원의 생존성을 향상시키고, 전투 효율성을 극대화하기 위한 수단으로 국방 분야에도 빠르게 도입되고 있다. 이에 따라 국방 분야에 인공지능 적용을 위한 정책/제도개선 및 연구가 활발히 진행되고 있다. 특히, 미 국방부는 인공지능 기술을 활용하여 모든 군사분야에 혁신적인 발전을 이루고 국제사회에서 주도권을 지속하기 위해 2018년 6월에 “국방 인공지능 전략”을 발간하였으며, 2022년 인공지능의 국방 분야 도입을 위한 신뢰 확보방안으로 “책임 있는 AI 전략 및 구현경로”를 제정하였다[3]. 우리나라도 이에 맞춰 “제2창군 수준의「국방혁신 4.0」추진으로 AI 과학기술 강군 육성”이라는 국정과제를 선정하여 국방부를 중심으로 국방 인공지능 컨트롤타워인 국방AI센터 설립을 추진하고 있으며, 점진적으로 국방 연구개발 투자 비중을 늘려가고 있다.

한편, 이러한 사회 전반의 인공지능 기술 적용에 대하여 우려스러운 부분도 존재한다. 아직 인공지능 기술에 대한 신뢰성, 설명 가능성, 적대적 공격 등의 문제에 대한 해결책이 명확하지 않은 점은 잠재적 위험요소를 내재한다고 볼 수 있다. 특히, 이러한 위험요소들은 국방 분야의 경우에는 국가적 재산뿐만 아니라 전투원의 생존성이라는 중요한 요소와 직결된 사안이기에 지속적으로 중요하게 다루어져야 할 부분이다.

본 논문은 앞서 언급한 인공지능 기술과 관련된 사회적 환경을 참고하여 2절에서 민수/국방 분야 인공지능 기술 도입을 위한 정책에 관하여 조사하였으며, 3절에서 인공지능 기술을 적용한 연구개발 사례와 기술 한계점을 분석하였다. 최종적으로 결론에서 이를 바탕으로 국방 분야에 신뢰를 기반으로 한 인공지능 기술 도입을 위한 연구 방향성에 대해 제언하였다.

2. 인공지능 기술 관련 정책/전략

우리나라를 포함한 미국, 영국, 중국 등 많은 국가가 인공지능 기술과 관련된 정책과 전략을 제시하고 있으며, 기술의 발전, 한계점 분석, 세부 추진전략 반영을 위하여 계속해서 노력하고 있다. 본 장에서는 민수/국방 분야를 구분하여 국내외 인공지능 기술 관련 정책/전략에 대하여 분석하고자 한다.

2.1 민수 분야 인공지능 기술 관련 정책 분석

2.1.1 미국

미국은 2016년「AI 국가 R&D 전략 계획(과학기술정책실)」,「AI의 미래를 위한 준비(국가과학기술위원회)」를 발표하며 미국이 나아갈 인공지능 정책의 포괄적인 로드맵을 제시하였으며, 2020년「국가 AI 이니셔티브법」 제정을 통해 인공지능 정책의 법적 기반을 마련하여 정책연구, 연구개발, 교육·훈련, 인프라, 부처 간 협업 사항 등 분야에서 세부 추진전략을 도출하고 있다. 이에, 인공지능과 관련한 많은 과제를 관리하고 예산 집행의 투명성 확보를 위해 2021년「연방기관 및 기타기관에 대한 인공지능 책임 프레임워크(미 회계감사원)」를 배포하였으며, 해당 프레임워크의 주요 내용은 거버넌스, 데이터, 퍼포먼스, 모니터링 4개 핵심 영역에 대한 감사절차, 감사자 및 평가자가 고려할 사항이다[4]. 또한, 2023년 인공지능 설계, 개발, 배포 및 사용하는 조직에 위험관리틀 제공과 신뢰할 수 있고 책임 있는 인공지능 시스템 개발 및 사용 촉진을 위하여「AI 위험관리 프레임워크(미국표준기술연구소)」를 발표하였으며, 단계 전반에서 수행되어야 할 행위에 대하여 Fig. 1에 나타내었다[5]. 해당 프레임워크의 주요 내용은 거버넌스, 위험식별, 분석/평가, 자원할당 및 대응 등의 요소에 대하여 인공지능 생애주기별 각 단계의 중점영역에서 시험평가와 연관하여 검토되어야 함을 포함한다.

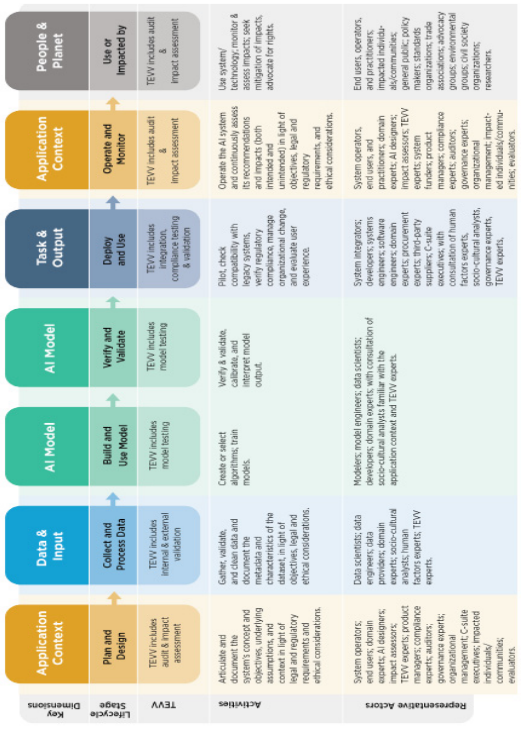

Fig. 1. AI actors across AI lifecycle stages[5]

2.1.2 영국

영국은 2017년 「영국 AI 산업 검토 보고서(디지털문화미디어스포츠부)」를 통해 데이터 접근성, 전문인력 양성, 인공지능 연구, 인공지능 활용 등 4개 분야에 대하여 정책적 권고를 제시하였으며, 이후 2021년 「국가 AI 전략(디지털문화미디어스포츠부)」을 발표하였다. 해당 전략은 인공지능의 글로벌 파급효과의 중요성 및 국가 간 기술경쟁 심화에 대한 전망에 따라 향후 10년간 영국의 인공지능 및 과학 분야 초강대국으로서 위상 유지를 위한 국가 차원의 장기적 요구에 대한 투자, 인공지능 활용 이점 보장, 거버넌스 운영 등을 주요 목표로 설정하고 있다[6]. 또한, 신뢰 가능한 인공지능 도입을 위하여 데이터윤리혁신센터를 통해 인공지능에 대한 표준 및 가이드 개발을 선도적으로 추진하고 있다.

2.1.3 중국

중국은 인공지능 분야 발전이 급속도로 진행되는 국가로 2015년 「중국제조 2025(국무원)」를 발표하며, 2025년까지 제조업에 인공지능 도입하는 '스마트 제조육성' 개념을 언급하였다. 이후, 2016년 「"13.5"국가과기혁신규획(국무원)」에서 인공지능 사업 확장을 공표하며 지능형 제조 및 로봇을 "과기혁신 2030프로그램"의 대형프로젝트로 지정하여 대규모 지원에 나섰으며, 2017년 「차세대 AI 발전규획(국무원)」을 통해 중요 국책과제로 확정되었다. 차세대 AI 발전규획은 인공지능 발전을 총 3단계 구분하였으며, 2030년까지 인공지능 기술 및 응용을 포함하여 전반적으로 세계 선두수준에 도달시키고 세계적인 인공지능 혁신 중심지로 도약을 목표로 삼고 있다. 이를 위한 6대 핵심 임무로서 인공지능 과기혁신시스템 구축, 지능형 경제 육성, 지능형 사회 건설, 인공지능 군민융합 강화, 지능형 인프라시스템 구축, 차세대 인공지능 중대 과기프로젝트 선행배치를 선정하였다[7]. 또한, 인공지능 시스템의 신뢰성 개선의 중요성을 인식하여 2021년 「신뢰할 수 있는 AI에 대한 백서(산업정보기술부)」를 배포하였으며, 주요 내용은 개인 정보 보호, 명확한 책임, 다양성 및 관용을 통해 제어할 수 있고 신뢰할 수 있으며 투명하고 설명 가능한 AI를 달성을 위한 경로 분석 등을 통해 향후 인공지능 개발을 위한 방향을 제시하고 있다[8].

2.1.4 한국

우리 정부는 2017년 4차 산업혁명위원회를 설립하고 DNA(Data·Network·AI)를 3대 혁신 신산업으로 삼아 분야별 대책을 발표하고 지원을 대폭 늘려왔다[9]. 특히, 인공지능 관련하여 2018년 「인공지능 R&D 전략」을 발표하였으며, 2019년 과기정통부를 비롯한 전 부처가 참여하여 마련한 「인공지능(AI) 국가전략」을 발표하였다. 해당 전략은 세계를 선도하는 인공지능 생태계 구축, 인공지능을 가장 잘 활용하는 나라, 사람 중심의 인공지능 구현 등 3대 분야에 대하여 인프라, 기술 경쟁력, 규제혁신, 스타트업, 인재양성 및 전 국민 교육, 산업 활용, 디지털 정부, 일자리, 윤리 등 9대 추진전략으로 구성되어 있다[10]. 또한, 앞서 언급한 국가들과 마찬가지로 신뢰할 수 있는 인공지능 도입 관련하여서도 많은 정책연구를 추진 중이며, 이에 대한 중간 결과로서 2021년 「신뢰할 수 있는 인공지능 실현전략(안)」, 2022년 「신뢰할 수 있는 인공지능 개발안내서(안)」 등을 배포하였다.

2.2 국방 분야 인공지능 기술 관련 정책 분석

2.2.1 미국

미 국방부는 2017년 Project Maven을 통해 인공지능 개발에 착수하였으며, 2018년 DARPA 주관으로 20억 달러의 예산을 투입하여 'AI Next Campaign'을 추

진하고 있다[11]. 이에 따라 국방 분야 AI 도입을 위한 정책이 빠르게 연구되고 있다. 2018년 6월 「국방 인공지능 전략(국방부)」을 발간하였으며, 이에 따라 인공지능 적용 무기체계 획득을 위한 전략적 접근 및 중점분야 수행과업이 추진되고 있다. 또한, 2022년 6월 인공지능의 국방 분야 도입을 위한 신뢰 확보방안으로 「책임 있는 AI 전략 및 구현경로(국방부)」를 제정하였으며, 6대 원칙인 거버넌스 확보, 전투원 신뢰 보장, 수명주기 관리, 요구사항 검증, AI 생태계 구축과 전문인력 양성에 대하여 방향을 제시하고 있다[12]. 이 밖에도 미 국방부는 합동인공지능센터(Joint Artificial Intelligence Center, JAIC)를 설립함으로써 인공지능 관련 과업들을 효율적으로 조정·통제할 수 있도록 하였으며, 이는 현재 우리나라 국방부에서 추진하고 있는 국방AI센터의 조직·임무 설계 시 참고 모델로 제시되었다.

2.2.2 영국

영국 국방부 산하 국방 보안 촉진 기구(Defense and Security Accelretor, DASA)는 2020년 1월 인공지능 관련 프로젝트를 공개하였으며, 해당 프로젝트를 통해 2040년까지 영국의 해군, 육군, 공군 장비 플랫폼 설계 및 운용방식 개선을 위한 인공지능 기술개발을 목표로 추진되고 있다. 이와 관련하여 2022년 6월 국방부 및 국방과학연구소(Defence Science and Technology Laboratory, Dstl) 주도하에 「국방 인공지능 전략(국방부)」를 발표하였으며, 국방 인공지능 기술 도입 비전과 접근법, 계획 등 전반적인 내용이 언급되어 있다[13]. 본 전략의 4가지 목표는 결정에서의 이점, 효율성, 새로운 기능에 대한 접근, 전체 군 병력 지원이며, 이를 달성하기 위한 주요 계획은 기술 도입, 인재채용 및 활용, 교류 활성화, 조직 구성원 전문성 향상, 정책/절차/법률 마련 등 5가지 과업으로 추진되고 있다. 해당 과업에 대한 추진은 국방AI자율유닛(Defence AI and Autonomy Unit, DAU)과 국방AI센터(Defence AI Centre, DAIC)를 중심으로 이루어지고 있다[14].

2.2.3 중국

중국은 2017년 19차 당대표자대회에서 시진핑 주석이 “인공지능이 군사 분야에 미칠 중대한 파장을 과학적으로 예견하고 군사 지능화의 발전을 가속화해야 함”을 강조하였다. 이에 중앙군사위원회 차원에서의 인공지능 기술 기반의 군사혁신을 추진하고 있으며, 2018년 3월 「군민융합전략요강(군민융합발전위원회)」를 통해 광범위한 데이터 분석과 학습능력을 갖춘 군의 혁신 방향을 제시하였다. 해당 전략요강을 통해 중국 정부가 추구하고자 하는 목표는 군민융합을 통해 미국에 상대적으로 열세에 있는 군사작전 분야를 극복하는 것이다[15]. 이를 위해 대규모 전장 환경에 대한 정보를 활용하여 의사결정 지원 등 인공지능 기술을 토대로 군사 지능화를 추진하고 있으며, 이는 세계 일류 강군을 꿈꾸는 강군몽의 핵심요소이기도 하다.

2.2.4 한국

우리 정부는 2017년 1월 국방부 업무보고를 통해 미래지향적 국방 역량 강화의 일환으로 인공지능 등 첨단기술의 국방 분야 융합 및 선진국의 국방혁신 사례 적용 등을 명시하였으며, 대통령 직속 4차 산업혁명위원회에서 의결된 ’4차 산업혁명 스마트 국방혁신 추진 계획‘을 통해 부분적으로 국방 분야 인공지능 도입이 추진되었다. 2020년 12월 「국방 인공지능 추진전략(국방부)」를 통해 국방 분야 인공지능 도입과 관련하여 3대 핵심 가치와 5대 추진전략, 13개 주요과제에 대하여 제시하였다. 이후, 2022년 “제2창군 수준의「국방혁신 4.0」추진으로 AI 과학기술 강군 육성”이 국정과제로 선정됨으로써 국방 분야 인공지능 기술 도입이 본격적으로 추진되고 있으며, 국방부와 방위사업청을 중심으로 정책연구가 활발히 수행되고 있다. 이에 관한 결과로서 2023년 3월 「국방혁신4.0 기본계획(국방부)」에 따라 인공지능 기반 핵심 첨단전력 확보를 위한 유·무인 복합전투체계 구축, 우주·사이버·전자기스펙트럼 영역 작전수행능력 강화, 합동 전 영역 지휘통제체계 구축 추진을 목표로 하고 있다. 인공지능 기반 첨단전력은 1단계 원격통제형 중심, 2단계 반자율형 체계 시범, 3단계 반자율형 체계확산 및 자율형 체계 전환으로 구분하여 확보하는 것으로 계획되었으며, 2027년까지 국방 R&D 예산을 국방비의 10% 이상으로 확대 투자할 예정이다.

3. 인공지능 기술 적용사례 및 한계점

본 절에서는 앞서 언급한 인공지능 기술과 관련된 사회적 환경을 참고하여 민수/국방 분야에 인공지능 기술의 적용사례와 사례별 한계점을 분석하였다.

3.1 민수 분야 사례 및 한계점

3.1.1 화재 판별 및 조기 진화 시스템

해당 기술은 재난 예방 조기경보 영역 영상 분야 적용사례로써 정확하고 빠르게 화재를 감지하여 조기 진화를 수행하는 것을 목표로 하고 있다. 기존의 열 감지 기반 소화 시스템은 온도 감지 센서에 의존하기 때문에 천장의 높이, 실내 면적 등 환경적 요인으로 인해 감지 시간이 지연되어 조기 진화에 어려움이 있을 수 있다. 이에 인공지능 기술을 적용하여 화재 감지 역량을 높이고자 하였다. 해당 기술의 구현은 YOLO 모델을 활용하였으며, 입력 CCTV 영상으로부터 객체의 위치 및 분류작업을 동시에 진행한다. 학습된 모델은 영상이 주어지면 화재 발생 지점을 박스 형태로 표시한다. 이때, 화재가 연속으로 3회 이상 검출되면 모델은 최종 화재로 인지해 소화 작업을 진행하게 된다. 해당 기술의 한계점으로써 불을 사용해야 하는 장소에서 단지 불이 탐지된 것만으로 이를 화재 발생으로 잘못된 판단을 내릴 수 있다는 “잘못된 화재 판단”, CCTV 영상만을 활용하여 화재를 탐지해야 하므로 “사각지대에 대한 화재 탐지 불가" 등이 있을 수 있다.

3.1.2 심층 신경망을 이용한 검색 알고리즘

해당 기술은 스마트시티 영역 언어 분야 적용사례로써 심층 신경망을 사용하여 언어를 이해하는 효과적인 검색 알고리즘이다. 기존의 검색엔진은 키워드 검색을 바탕으로 알고리즘이 구성되어 사용자가 입력하는 문자가 길어질수록 검색의 정확도가 하락한다. 반면, 제안 기술은 버트(Bidirectional Encoder Representations from Transformers, BERT)라는 트랜스포머 심층 신경망 구조를 사용하여 문장을 이해하고 문장의 길이와 상관없이 효과적으로 검색을 수행한다. 트랜스포머 구조를 확용한 언어 이해 심층신경망 학습 관련 개요를 Fig. 2에 나타내었다. 해당 기술의 구현은 트랜스포머가 문장을 입력으로 받으면 문장의 각 단어를 하나의 벡터로 변환한다. 이후에 각 벡터 간의 연관성을 어텐션 연산을 통해 계산한다. 어텐션 연산은 입력 쿼리(Query)와 모든 키(Key) 간의 유사도를 계산하는 연산이다. 트랜스포머는 어텐션 연산을 반복하여 입력 문장을 벡터 형태로 표현한다. 트랜스포머 훈련을 위해서는 무작위로 입력 문장의 단어를 가리고 이를 예측하는 마스킹 훈련 방법을 사용하며, 이를 통해 트랜스포머는 문장의 문맥을 파악하고 앞뒤 단어를 통해 해당 단어를 유추하는 능력을 배운다. 트랜스포머의 결과 벡터들은 데이터베이스에 있는 벡터들과 유사도가 비교되어 가장 높은 유사도를 가진 데이터를 검색 결과로 반환한다. 해당 기술의 한계점으로써 훈련에 사용되는 데이터가 인터넷에서 확보된 문서를 기반으로 구성되기 때문에 성별, 인종, 정치 성향 등 다양한 분야에 대해서 특정한 편향을 가질 수 있으며, 제안된 기술에 사용되는 트랜스포머 모델은 많은 연산량을 요구하기 때문에 도입장벽이 높다.

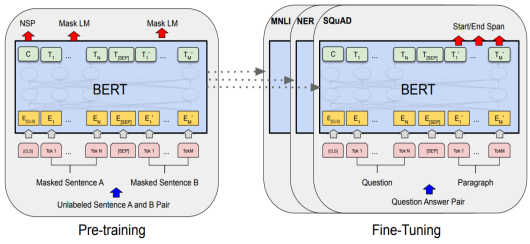

Fig. 2. Overview of Pre-training of Deep Bidirectional Transformers for Language Understanding[16]

3.1.3 코로나 19 환자 산소 요구량 예측 인공지능

해당 기술은 의료진단 영역 예측 분야 적용사례로써 코로나 19 증상으로 응급실에 들어오는 환자에 대해 초기 검사만으로 산소 보충 필요 여부를 판단하는 인공지능 기반 예측서비스다. 해당 기술은 연합 학습(Federated learning)을 사용하여 커뮤니케이션의 효율성을 높이고, 환자의 개인 정보를 보호하고, 많은 병원의 정보를 활용하는 것을 가능하게 하였다. 연합 학습은 여러 곳에 분산된 기기나 로컬 데이터를 보유한 서버에서 데이터의 공유 없이 개별적으로 모델 학습을 수행한 후, 갱신된 모델의 파라미터들을 중앙 서버로 보내 취합해서 하나의 모델로 통합하는 기법으로 분산학습 솔루션 개요를 Fig. 3에 나타내었다. 따라서 한 장소에 많은 데이터를 모아놓고 학습하지 않아도 전체 데이터를 활용한 성능을 낼 수 있으며 개인 정보 또한 보호할 수 있다. 이렇게 통합한 모델을 다시 분산된 클라이언트에게 배포하고 클라이언

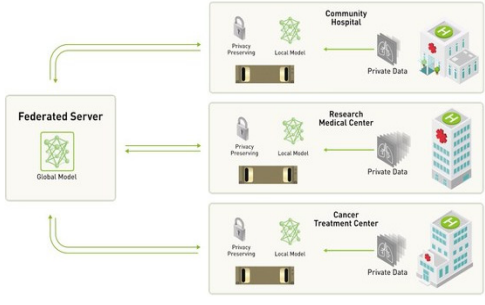

Fig. 3. Overview of Federated learning framework[17]

트가 새롭게 얻어지는 데이터로 모델을 지속적으로 학습한다. 해당 기술의 한계점으로써 클라이언트가 서버에 악의적인 업데이트를 할 경우 이를 식별할 효과적인 보호 기능이 없으면 글로벌 모델이 손상될 수 있다. 이렇게 악의적인 적대적 공격이 반복되면 모델의 정확도는 낮아질 수밖에 없다.

3.1.4 3D 라이다(LiDAR) 인식 알고리즘

해당 기술은 자율주행 영역 센서 분야 적용사례로써 효율적인 실시간 3D 라이다 인식을 목표로 한다. 3D 라이다 인식은 이미지 처리에 비교해서 시간이 많이 소요되는데 이는 자율주행 차량의 사고와 직결되는 문제이다. 자율주행 차량은 제한적인 하드웨어를 사용하기 때문에 효율적인 라이다인식 알고리즘이 필요하다. 이에 제안기술은 Sparse Point-Voxel Convolution Neural Network(SPVCNN)을 기반으로 짧은 시간에 효율적인 연산을 통해 3D 라이다 인식을 수행하였다. 또한, 제안기술은 최초 신경망의 구조를 문자열 형태로 나타낸 후 해당 문자열을 생성하는 순환 신경망(Recurrent Neural Network, RNN)을 생성하고, 순환 신경망이 생성한 문자열을 바탕으로 신경망을 다시 구축하고 데이터셋으로 신경망을 학습하여 성능이 좋아지는 방향으로 강화학습을 수행함으로써 최적의 신경망 구조를 만드는 방식인 Neural Architecture Search(NAS)라는 방식을 적용하였으며, 알고리즘의 개요를 Fig. 4에 나타내었다.해당 기술의 한계점으로써 최적의 신경망 구조를 찾기 위해 반복적으로 구조를 바꾸며 훈련해야 하며, 기존 데이터셋보다 많은 양의 데이터를 이용하기 때문에 학습에 많은 시간이 소요된다.

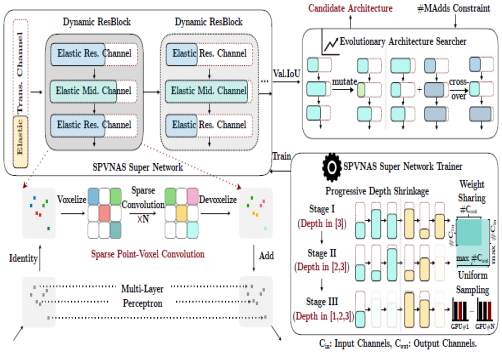

Fig. 4. Overview of Sparse Point-Voxel Convolution Neural Network(SPVCNN)[18]

3.2 국방 분야 사례 및 한계점

3.2.1 원격사격통제체계 표적 식별 시스템

해당 기술은 최근 육군 제5보병사단과 협약을 체결하고 군에서의 시범 운용에 돌입한 ”지능형 다목적 무인 차량“에 적용된 원격 사격 통제체계(Remote Controlled Weapon Station, RCWS)의

정밀타격을 위하여 개발되었다. 제안기술의 정밀타격을 위한 시스템에는 총성을 감지해 스스로 화기를 돌려 공격할 수 있는 딥러닝 기술을 적용하였다.

또한, 가시광 및 열 영상을 통해 표적을 식별하고, 안정화 및 자동추적기술을 바탕으로 주간 및 야간 기동 중에도 움직이는 표적을 정밀하게 추적, 타격할 수 있다. 해당 기술은 YOLO v5와 SiamRPN 기반의 네트워크를 함께 학습하여 실시간으로 표적을 탐지 추적할 수 있도록 설계되었으며, 도출된 정보를 바탕으로 전장 상황을 정확히 인식하고 신속하게 대응하는데 주안점을 두고 개발되었다. 해당 기술의 한계점으로써 악의적인 목적을 가진 공격자가 굳이 해당 시스템 내부에 접근하지 않더라도 무인 차량이 센서를 통해 바라보는 물리적 환경에 특정 패턴을 보이는 적대적 패치를 부착하게 되면 무인 차량의 예측 및 결정에 악영향을 줄 수 있다.

3.2.2 통합 시각 증강 시스템

해당 기술은 미 육군이 병사들의 인지증강을 위해 개발한 기술로써 병사들의 머리 부분에 탑재형 디스플레이(Head Mounted Display, HMD) 모듈의 형태로 착용 가능하며, 병사들이 훈련 및 임무 수행 중에 필요한 각종 정보(환경정보, 작전 개요, 주변 지형도 및 건물 구조 등)를 증강현실(Augmented Reality, AR)로 제공하는 것을 목표로 한다. 제안기술은 HoloLens2라고 불리는 민간용 AR 웨어러블 기기에서 출발하였으며, 적외선 카메라를 이용한 열 영상과 야시경 센서를 통합하였고, 개인화기의 열상 조준경을 통합해 조준사격을 더 용이하게 하도록 개발되었다. 또한, AR 기술과 GPS 기술을 접목하여 TAK(Team Awareness Kit)기반의 지도를 띄워 작전지에 대한 정보를 쉽게 얻고 아군의 위치를 보고하는 기능이 있으며, 외국어를 자국어로 실시간 번역해주는 기능과 카메라를 통해 생체정보를 얻고 신원을 파악하여 적인지 아군인지 식별하는 기능도 포함되어 있다. 이 기술은 딥러닝 기술을 자유롭게 접목할 수 있는 플랫폼 기술로 통합 시각 증강 시스템(Integrated Visual Augmentation System, IVAS)을 착용하여 객체 인식을 하고 싶다면 객

체 인식 알고리즘인 YOLO v5 모델을, 그리고 객체분할 태스크를 수행하고 싶다면 Mask R-CNN 모델을 각각 학습시킨 모델을 접목하여 AR 형태로 출력시키는 방식으로 사용할 수 있다. 해당 기술의 한계점으로써 대부분 시각정보를 IVAS에 의존하게 되는 만큼 나쁜 의도를 가진 공격자들이 적대적인 기계학습 또는 데이터 오염과 같은 기술로 IVAS 시스템을 해킹할 위험이 커진다. 이 경우 사용자 개인의 정보가 노출될 위험이 있다.

3.2.3 전투기 조종 AI 알고리즘

해당 기술은 AI 알고리즘이 일반적으로 조종사가 담당하는 비행 중 특정 업무를 수행할 수 있게 개발되었다. 대표적인 수행 가능 업무로 AI 조종 알고리즘과 조종사 간의 정찰기 레이더 정보 공유, 조종사가 모의 적기를 경계하는 사이 적의 미사일 발사장치 등을 탐지하는 업무를 들 수 있다. 제안기술은 구글 딥마인드에서 개발하여 체스, 바둑, 비디오 게임 등에 사용되어 온 뮤제로(μZero) 알고리즘을 전투기 비행 환경에 맞게 변형한 버전으로 게임에 관한 아무런 정보 없이 백지상태에서 경기를 치르면서 스스로 게임의 규칙과 보상을 터득하는 강화학습 알고리즘이 적용되었다. 해당 기술의 한계점으로써 악의적인 의도를 가진 전파방해나 재밍(Jamming)에 통제력을 상실할 수 있는 위험이 크다.

3.2.4 위성 영상 분석 솔루션

해당 기술은 항공, 위성 영상을 기반으로 지구 관측 분석 서비스 제공을 목표로 하는 영상 데이터 분석 플랫폼이다. 항공기, 선박 등의 개체를 식별 및 분석하는 작업과 관심 지역의 변화 여부를 탐지하는 작업을 수행할 수 있으며, 사용자가 영상을 분석하기 쉽도록 영상 해상도를 개선하는 기술도 적용되어있다. 제안기술은 위성 영상 안에 보이는 다양한 종류의 객체들을 검출하고 분류해 냄으로써 다양한 인사이트를 획득하는 것을 주안점으로 개발되었다. 객체 검출과 관련하여 위성 영상에서 많은 객체가 좌우 비율이 다르고 회전된 경우가 많으므로 각도를 고려한 탐지기술, 획득할 수 있는 데이터양이 한정되어 있어 적은 양의 데이터만을 활용한 탐지기술 등이 고려되었다. 또한, 적외선, 레이더 영상 등 다양한 센서를 활용할 수 있도록 도메인별 특화 모델을 구성하여 개발되었다. 기술 구현의 베이스라인 알고리즘은 특징점 피라미드 네트워크(Feature Pyramid Network, FPN)를 사용하였으며, 일부 알고리즘 변형을 수행하였다. 해당 기술의 한계점으로써 위성 영상의 경우 데이터 특성상 데이터 구축이 매우 어려우므로 초기 데이터셋을 구축할 때 라벨링이 잘못되게 되면 잘못된 데이터셋이 만들어질 수 있다. 이로 인해 객체 검출 모델이 잘못 만들어진 데이터셋으로 학습될 시 오작동을 일으킬 위험이 있다.

4. 결론

본 논문에서는 민수/국방 분야 인공지능 기술 도입을 위한 정책 및 인공지능 기술을 적용한 연구개발 사례와 기술 한계점에 대한 분석을 수행하였다. 그 결과 두 가지 결론을 도출하였다. 첫 번째 결론은 명확한 목표설정과 투자 분야의 다각화이다. 현재 선진국을 중심으로 민수/국방 분야를 막론하고 인공지능 기술을 도입하기 위하여 많은 정책이 배포되고 있으며, 이에 따라 R&D 예산도 증가하고 있는 것을 확인할 수 있었다. 우리나라도 최근 인공지능 기술 도입을 위한 정책적 제시가 이루어지고 있으며, 많은 연구와 투자를 통해 거버넌스 구축을 위해 노력하고 있다. 하지만, 특정 R&D 위주의 투자가 중심이 되는 것이 한계점이라 생각된다. 인공지능 기술 도입으로 실효성을 얻기 위해서는 인공지능 기술을 특정 분야에서 특정 역할을 무엇을 위해 수행하여야 하는지에 대한 명확한 목표설정이 주어져야 그에 적합한 R&D를 수행할 수 있을 것으로 생각된다. 이는 별도의 연구 주제로 다루어져야 할 부분이며, 무엇보다 선행적으로 수행되어져야 할 과업이다. 또한, 선진국에서도 중요하게 다루고 있는 인공지능 기술의 신뢰 확보와 관련하여 많은 연구와 투자가 필요하다. 두 번째 결론은 첫 번째 결론 마지막 부분에도 잠시 언급하였지만, 개발된 대상물에 대해 지속적인 유지·관리 및 평가를 통한 사용자의 신뢰 확보이다. 모든 분야에 인공지능을 도입하기 위해서는 도메인 격차를 극복하는 과업과 강건성, 보안성, 윤리성 등 인공지능 기술에 대한 신뢰를 확보하기 위한 과업이 필수적이다. 특히, 인간의 생명과 보안 등에 직결되는 분야에 사용되는 인공지능 기술은 더욱 신뢰를 바탕으로 다루어져야 할 것이다. 이를 위해서 미국을 비롯한 여러 나라에서 신뢰할 수 있는 인공지능 도입을 위한 연구가 진행되고 있지만, 아직 연구성과를 제시하기에는 부족한 부분이 많은 것 같다. 우리나라도 최근 「신뢰할 수 있는 인공지능 개발안내서(안)」을 배포하는 등 노력을 하고 있으나, 아직은 방법론적인 내용이 대다수이다. 이러한 상황에서 신뢰할 수 있는 인공지능 기술의 빠른 도입을 위

해서는 실효성 있는 연구성과를 낼 수 있는 환경구성과 예산의 투자가 바탕이 되어야 할 것으로 생각된다. 본 연구를 통해 2가지 결론을 바탕으로 명확한 목표설정을 위한 R&D 연구 분야 카테고리화 및 신뢰할 수 있는 인공지능에 대한 연구 방향성을 제시하였다. 향후, 본 논문의 결론을 바탕으로 국방 분야에 신뢰를 기반으로 한 인공지능 기술 도입을 위한 효율적인 연구 수행 방향 설정에 도움이 되었으면 한다.

References

[1] C. I. Chung, "The Korean Revolution in Millitary Affairs in the Era of the Fourth Industrial Revolution", Korean Journal of Millitary Affairs, Vol.6, pp.1-38, 2019.
DOI: http://dx.doi.org/10.33528/kjma.2019.12.6.1

[2] U. K. Jung, D. Y. Kim, "Artificial Intelligence-Based Defense Project Research on security vulnerabilities and countermeasures", korean Journal of Public Safety and Criminal Justice, Vol.21,.No.3, pp.425-454, 2019.
DOI: http://dx.doi.org/10.21181/KJPC.2022.31.3.425

[3] K. H. Choi, J. J. Oh, Y. G. Kim, "The Implications to ROK Armed Forces from the Artificial Intelligence Strategy of U.S. Department of Defense and Army", Journal of The Korea Association of Defense Industry Studies, Vol.27, No.1, pp.41-52, 2020.
DOI: http://doi.org/10.52798/KADIS.2020.27.1.4

[4] GAO, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities, Policy Report, the U.S. Government Accountability Office(GAO), United States of America.

[5] NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), Policy Report, National Institute of Standards and Technology(NIST), United States of America.
DOI: https://doi.org/10.6028/NIST.AI.100-1

[6] Department for Digital, Culture, Media&Sports, National AI Strategy, Policy Report, HM Government, United Kingdom.

[7] KOSTEC, China's Artificial Intelligence Policy Trend, Issue Report, Korea-China Science&Technology Cooperation Center(KOSTEC), Korea.

[8] Matt Sheehan, China's New AI Governance Initiatives Shouldn't Be Ignored, Carnegie Endowment for International Peace, c2022 [cited 2022 Jan.], Available From: https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127 (accessed Jul., 2023)

[9] Ministry of Culture, Sports and Tourism, Artificial Intelligence(AI), Policy Briefing of Korea, c2021 [cited 2021 Nov.], Available From: https://www.korea.kr/special/policyCurationView.do?newsId=148868542 (accessed Jul., 2023)

[10] Ministry of Science and ICT, National Strategy for Artificial Intelligence, The Government of the Republic of Korea, Korea.

[11] J. H. Yoon, Major Issues in the Introduction of AI Technology in the Defense Field and Plans to Improve Utilization, Technical Report, Science&Technology Poicy Institute, Korea, 2021.

[12] DoD, U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway, Policy Report, the U.S. Department of Defense(DoD), United States of America.

[13] J. E. Lee, J. S. Lee, C. S. Ryu, "A study on the current status of defense AI in major foreign countries", Journal of the Korean Institute of Defense Technology, Vol.5, No.1, pp.19-24, 2023.
DOI: http://dx.doi.org/10.52682/jkidt.2023.5.1.19

[14] Ministry of Defense, Defense Artificial Intelligence Strategy, Policy Report, HM Government, United Kingdom.

[15] C. H. Lee, China's Strategy to build an 'Intelligence Army' through Civil-Military Convergence, Korea Institute for Maritime Strategy(KIMS), c2019 [cited 2019 Aug.], Available From: https://kims.or.kr/issubrief/kims-periscope/peri166/ (accessed Jul., 2023)

[16] J. Devlin, M. W. Chang, K. Lee, K Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding", Proceedings of NAACL-HLT 2019, the North American Chapter of the Association for Computational Linguistics(NAACL), Minneapolis, Minnesota, pp.4171-4186, Jun 2019.
DOI: https://doi.org/10.48550/arXiv.1810.04805

[17] Nicola Rieke, What Is Federated Learning, NVIDIA Blog, c2019 [cited 2019 Oct.], Available From: https://blogs.nvidia.com/blog/2019/10/13/what-is-federated-learning/ (accessed Jul., 2023)

[18] H. Tang, Z. Liu, S. Zhao, Y. Lin, J. Lin, H. Wang, S. Han, "Searching Efficient 3D Architectures with Sparse Point-Voxel Convolution", ECCV 2020, European Conference on Computer Vision(ECCV), Vol.12373, Aug. 2020.
DOI: https://doi.org/10.1007/978-3-030-58604-1_41

강 지 훈(Ji Hoon Kang) [정회원]

- 2013년 2월 : 경상대학교 전자공학과 (학사)
- 2015년 8월 : 경상대학교 전자공학과 (석사)
- 2016년 8월 ~ 2019년 7월 : 한국산업기술시험원(KTL) 연구원
- 2019년 8월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방, 전자공학, 인공지능, 시험평가

정 민 경(Min-Kyung Jeong) [정회원]

- 2020년 2월 : 부산대학교 나노메카트로닉스공학과 (공학사)
- 2019년 12월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방, 인공지능, 전자회로, 반도체 공정기술

박 주 영(Joo-Young Park) [정회원]

- 2015년 2월 : 숭실대학교 전기공학과 (공학사)
- 2019년 1월~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방, 전기, 전자, 인공지능, 사이버보안

이 원 영(Won-Young Lee) [정회원]

- 2019년 2월 : 홍익대학교 컴퓨터정보통신공학과 (공학사)
- 2021년 2월 : 홍익대학교 전자전산공학과 (공학석사)
- 2020년 11월 ~ 21년 12월 : 국방기술진흥연구소(KRIT) 연구원
- 2022년 1월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방, 인공지능, 소프트웨어 설계검증, RMF(Risk Management Framework)

최 은 진(Eun-Jin Choi) [정회원]

- 2019년 2월 : 한국기술교육대학교 컴퓨터공학부 (공학사)
- 2021년 2월 : 성균관대학교 전자전기컴퓨터공학과 (공학석사)
- 2022년 7월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방, 전자공학, 인공지능, 사이버보안, RMF(Risk Management Framework)