Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 9 pp. 539-546, 2023

https://doi.org/10.5762/KAIS.2023.24.9.539
ISSN 1975-4701 / eISSN 2288-4688

인공지능 기반 무기체계 데이터 품질평가 지표에 대한 고찰

서석호*, 박주영, 정민경, 이원영, 최은진
국방기술품질원

A Study on AI-based Weapon System Data Quality Evaluation Indicators

Suk-Ho Seo*, Joo-Young Park, Min-Kyung Jeong, Won-Young Lee, Eun-Jin Choi
Defense Agency for Technology and Quality

요 약 첨단 과학화 강군건설을 위하여 인공지능 기술이 접목된 무기체계의 도입이 최근 확대되고 있다. 이에 따라 무기체계의 무결한 성능 구현을 위하여 핵심인 데이터의 체계적인 품질관리가 요구되고 있다. 현재 국내 국방 분야에서는 인공지능 기술에 대한 전략, 인프라 구축 등 기반을 마련하고 있으나, 체계적인 데이터 품질관리를 위한 전략은 다소 미흡한 실정이다. 따라서 본 논문에서는 현재 미 정립된 국방 데이터 품질관리 방안 마련을 위한 선행 연구로서 국내·외 인공지능 기반 무기체계 도입 현황 및 주요국의 데이터 관련 추진전략을 조사하고, 최근 군이 도입하여 시범운용 중인 지능형 경계시스템 등 표적탐지 및 추적 분야 무기체계의 데이터 품질관리 시 고려되어야 할 평가지표에 대하여 제시해 보았다. 다양성, 충분성, 신뢰성 및 보안성 지표를 도출하였으며, 본 연구결과는 향후 무기체계 데이터 품질관리 방안 등 가이드라인 마련 시 활용 가능할 것으로 판단된다.

Abstract The introduction of weapon systems incorporating artificial intelligence technology is expanding the construction of a strong and advanced science-based military. Accordingly, quality control of data, which is the core of artificial intelligence, is required to realize the perfect performance of the weapon system. The foundation is laid in the domestic defense field by establishing strategies and building infrastructure for artificial intelligence technology. On the other hand, the strategy for data quality management is insufficient. Therefore, as a preceding study to prepare measures for defense data quality management that have not been established, this study examined the status of domestic and foreign AI-based weapon systems and data-related strategies. The evaluation indicators considered in the data quality management of target detection and tracking weapons systems currently piloted by the military are presented. The diversity, sufficiency, reliability, and security indicators were derived. These results are expected to be utilized for establishing guidelines, such as weapon system data quality management plans.

Keywords : Artificial Intelligence, AI-based Weapon System, Quality Management, Data, Military

1. 서론

인공지능은 첨단 과학화 강군건설을 위한 핵심기술이며, 미래전장의 주도권을 확보하기 위한 핵심 전력이다. 이에 세계 주요국은 인공지능 주도권 확보를 위하여 국방 인공지능 거버넌스 구축 및 기술개발을 위한 투자를 확대하고 있으며, 미래전장에서 우위를 선점하고자 자국 차원의 인공지능 정책 구축 등 국가역량을 결집하고 있다.

*Corresponding Author : Suk-Ho Seo(Defense Agency for Technology and Quality)
email: seosukho90@dtaq.re.kr
Received July 18, 2023 Revised August 9, 2023
Accepted September 1, 2023 Published September 30, 2023

이에 국내에서는 범정부적으로 국정과제 수립 및 국방혁신 4.0 추진 등 '인공지능 국가전략' 및 '국방 인공지능 추진전략'을 마련하고 있으며, 인공지능 과학기술 중심의 발전 모색으로 중장기 무기체계 대상전력으로 인공지능 관련 전력을 다수 포함하는 등 국가 안보력 강화를 위하여 국방 다양한 분야에 인공지능 기술을 적용하고자 국방부를 중심으로 국방 인공지능 추진 체계 정립 등 인공지능을 통한 국방 全 영역의 혁신을 추진하고 있다[1,2].

최근 인공지능 기반 무기체계의 도입은 확대되고 있으며, 특히 표적탐지 및 추적 분야에 특화된 무기체계들의 시범 운용이 활발한 추세이다. 대표적으로 '다출처 영상융합체계', '중요시설 경계시스템' 및 'GOP 과학화 경계시스템' 등의 사업과 신개념 획득 패러다임인 신속획득사업의 추진을 통하여 획득 운용 중인 '음원활용 AI 경계시스템' 및 'TOD AI 객체인식 경고시스템' 등이 있다.

이처럼 무기체계에 인공지능 적용은 확대되고 있으나 인공지능 기반 무기체계에 적합한 품질관리 기준과 절차는 미 정립 상태이며, 특히 총 수명주기(life cycle)에 걸쳐 학습과 성능향상이 지속적으로 수반되는 특성에 따라 고품질 데이터 확보는 필수적이지만 이러한 데이터 확보를 위한 검증 기준과 같은 품질관리 방안이 마련되지 않은 상황이다.

인공지능 기술 분야의 우위를 선점하기 위해서는 무결점의 인공지능 기술 구현은 필수적이며, 이를 위해서는 무결점의 양질의 데이터를 확보하는 것이 필수라고 할 수 있다. 인공지능 기술에서 데이터는 가장 중요한 요소이며, 그중에서도 질적으로 우수한 데이터의 확보는 필수적이다. 저품질의 데이터는 신뢰성이 떨어지는 결과물을 만들어내며 그로 인한 성능, 서비스 등의 저하와 출력의 오류라는 심각한 문제를 발생시킬 가능성이 있으므로 고품질 데이터 확보의 중요성은 지속 강조되고 있다[3]. 특히 Fig. 1과 같이 美 의회(GAO : Government Accountability Office)에서는 인공지능 사용에 있어 관리, 감독을 위한 '책임성 프레임워크'를 제정하고 데이터의 중요성을 강조하고 있음에 따라[4], 인공지능의 일관된 성능 발휘를 위하여 데이터에 대한 품질관리는 필수적이라고 할 수 있다.

이에 민간에서는 과기정통부를 주축으로 '인공지능 학습용 데이터셋 구축 안내서' 및 '인공지능 학습용 데이터 품질관리 가이드라인'을 마련하였으며, 데이터 품질관리 지표 및 단계별 수행사항 등의 기준을 제시하며 이를 기반으로 데이터 계획-구축-운영-활용 측면에 적용하여 활용 중이다[5,6]. 이에 따라 국방 분야도 폐쇄적 환경, 한

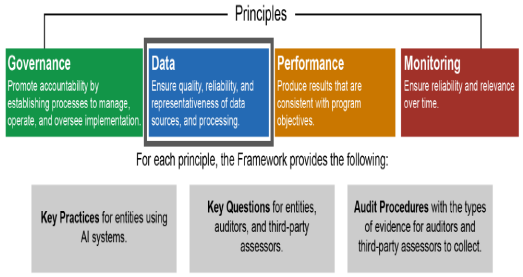

Fig. 1. Guide for reading the framework(Artificial Intelligence An Accountability Framework for Federal Agencies and Other Entities Department of defense, GAO) [4]

정된 자원 및 정제되지 않은 운용환경 등 국방특성을 고려한 데이터 품질관리 가이드라인이 수립될 필요성이 있으며, 특히 국방이라는 특수한 환경에 의한 데이터 수집·생성·공유·활용 등의 제한사항 및 체계별 운용목적, 환경 등의 특성을 고려한 데이터 품질관리 방안의 마련은 필수적이라고 할 수 있다.

이에 따라 본 논문에서는 주요선진국의 인공지능 무기체계 도입 현황 및 데이터 관련 전략을 알아보고 최근 확대 적용 중인 표적탐지 및 추적 분야 체계에서 데이터 품질관리 방안에 대한 가이드라인 수립 시 고려되어야 할 데이터 평가지표를 제시하고자 한다.

2. 본론

2.1 인공지능 기반 무기체계 도입 현황

주요선진국은 미래전을 대비하여 '국가 AI전략'을 수립하고 있으며, 국방 AI 거버넌스 구축, 인공지능 기술개발 확대 및 독자적 무기체계 도입을 위한 투자를 적극적으로 추진하고 있다.

미국의 경우 '국방 AI전략('18)' 수립 및 JAIC(Joint AI Center)를 중심으로 인공지능 기술 기반 무기체계 도입을 추진하고 있으며, 중국의 경우 패권국인 미국에 대한 상대적 열세를 극복하기 위하여 군집(swarming) 기술의 전술 효과성에 주목하여 군집 드론, 군집 수상정 및 잠수정 전투체계 구축에 집중하고 있다[7]. 이외 러시아 등 주요선진국에서는 무기체계 인공지능 도입 촉진을 위하여 국방부 예하 총괄조직을 신설하여 인공지능 기반 군사력 강화를 추진하고 있다. 이에 국내에서도 국방 인공지능 컨트롤 타워를 조직하고자 국방부 내 '국방AI센

Table 1. AI-applied Weapon System

Nation	Weapon System	Details
U.S.	Autonomous Unmanned Submarine (Sea Hunter)	· The first autonomous unmanned submarine developed by DARPA · Autonomous unmanned vessel to navigate and continuously identify subsea submarines
U.S.	Quadruped Walking Robot	· Positioned at borders and bases for conducting patrol · Identify abnormalities in the base by acquiring large amounts of data and performing calculations using sensor platform
China	Unmanned Ground Vehicle	· Perform reconnaissance, attack, search, and destroy missions with orbital mobile device · Automatic avoidance function possible through application of artificial intelligence
Russia	Unmanned Ground Vehicle (Uran)	· A multi-functional combat robot that supports targeting and performs surveillance and reconnaissance missions

터 추진팀'을 운용 중이며, 각 군・국방기관 등으로 분산된 인공지능 업무를 통합, 연계하는 총괄기관으로의 역할 수행을 위하여 법령·제도·예산·인프라 구축 등의 업무를 담당하고 있다. 이처럼 대외 주요선진국은 인공지능 기반 전력도입을 위하여 기반을 구축하고 있으며 동시에 Table 1과 같이 인공지능 기반 무기체계 도입을 통한 군사력 강화를 추진하고 있다.

이와 같은 미래전장 패러다임의 변화에 따라 우리 군도 다양한 획득 방법으로 인공지능 기반 무기체계 도입을 추진하고 있다. 현재는 인공지능 분야에 대한 생태계 조성을 위한 소요기획 단계에 치중되어 있으나, 무기체계 인공지능 적용을 위하여 방위사업청은 미래도전개발사업 및 핵심기술개발사업 등의 사업을 추진 중이다. 대부분 기초 및 선행 핵심연구의 초기 단계이지만 국방부, 방위사업청 및 각 군 등은 연구개발, 구매 및 시범사업 등을 통하여 인공지능 기반 무기체계 도입을 위한 분위기를 조성하고 있다. 특히 인공지능 기술 분야 중 대표적으로 표적탐지 및 추적 기술과 연관된 체계가 대표적으로 개발 및 시범 운용 중이며, 대표적인 사업 현황은 Table 2를 통하여 확인할 수 있다.

현재 국내 국방 분야의 인공지능 기술적용 무기체계 도입은 초기 단계로 향후 중장기적으로 도입 운용될 체계의 성공적 전력화를 위하여 해결해야 할 현안들이 다수 존재한다. 그 중 앞서 언급한 바와 같이 무기체계의 무결한 성능 구현을 위한 고품질의 데이터 확보방안 마련이 가장 시급하다고 할 수 있다. 인공지능 기술적용 무기체계는 전력화 시 군 요구사항 충족을 위하여 개발 또는 양산시 실제 운용환경 데이터 혹은 그 환경을 모사한 유사 데이터 및 합성데이터 등을 통한 요구성능에 대한 완전한 학습이 선행되어야 한다. 하지만 보안, 외부공개 제한 등 군사보안과 같은 무기체계 개발환경의 특성으로 충분한 학습데이터 확보, 보유 등의 제한사항이 존재하며, 수집데이터도 학습데이터로써 활용 가능한 수준인지에 대한 검증 기준 미수립으로 실질적인 학습데이터로써 효용성 여부에 대한 판단 기준이 불명확한 상황이다. 이러한 한계점은 체계의 불완전 학습으로 이어지며, 불완전 학습은 성능 미흡으로 귀결될 수밖에 없다. 이에 따라 향후 인공지능 기반 무기체계의 중장기적 도입을 위해서는 군 환경에 적합한 데이터 품질관리 방안의 마련이 선행되어야 한다.

Table 2. AI-applied Weapon System

Acquisition Method	Weapon System	Details
Research and Development (R&D)	Multi-source Video Convergence System	· A system for integrated analysis and sharing of data collected from major reconnaissance assets such as satellites and reconnaissance aircraft
Purchase	GOP Scientific Guard System	· A system that analyzes surveillance images through artificial intelligence and provides warning notifications and analysis results to operators
Rapid Demonstration Acquisition Project(RDAP)	TOD AI Object Recognition Guard System	· A system that detects abnormal situations and recognizes objects in real time by applying artificial intelligence technology to TOD installed in border areas
Rapid Demonstration Acquisition Project(RDAP)	AI Alert System using Sound Source	· A system that analyzes video and sound data in real time with artificial intelligence technology and provides notification to the operator

Table 3. National Strategy for Artificial Intelligence[7,10,11]

Nation	Strategy Details
U.S.	· Expand investment in artificial intelligence to secure cutting-edge technology for future warfare · DARPA, DIU, and JAIC are collaborating on an artificial intelligence project *Strategy: DoD Artificial Intelligence Strategy, DoD Digital Modernization and DoD Data Strategy
U.K.	· DASA under Ministry of Defense promotes the introduction of artificial intelligence · Introduce the project of 'DASA' that maximizes data utilization · Define data as a strategic asset and announce *Strategy: Data Management Strategy and Data Strategy for Defense
China	· Introduction of artificial intelligence technology to overcome the military inferiority against the US · Promote AI-based military innovation led by the Central Military Commission · Announce the strategy below to improve national defense and security *Strategy: Next-Generation Artificial Intelligence Development Plan

2.2 데이터 관련 주요국 국가전략

주요선진국은 4차 산업혁명의 촉발 및 인공지능 기술의 발전에 따라 안보환경 패러다임의 전환을 위하여 Table 3과 같이 인공지능 기술적용 무기체계 도입 확대를 목표로 국가전략을 수립하고 있다. 특히 미국과 영국은 체계적 데이터 확보 및 데이터 중심 조직 구축을 위한 전략을 마련하고 있음을 확인할 수 있다. 미 국방부는 국방 인공지능 전략(DoD Artificial Intelligence Strategy, 2018), 디지털 현대화 전략(DoD Digital Modernization Strategy, 2019) 및 국방 데이터 전략(DoD Data Strategy, 2020)을 발표하였으며, JAIC(Joint AI Center) 및 CDAO(Chief Digital AI Officer)를 중심으로 국방 인공지능 거버넌스 구축 체계를 마련하고 있다. 국방 데이터 전략(DoD Data Strategy)은 다음 Fig. 2를 통하여 확인할 수 있으며, 8대 가이드원칙, 4대 필수역량 및 7대 목표로 구성되어 있음을 확인할 수 있다[8]. 특히 데이터를 전략적 자산으로 정의하고 데이터 접근 가용성, 목적에 적합한 데이터, 신뢰할 수 있는 데이터 및 안전한 데이터 등의 프레임워크를 구성함으로써 목적에 부합하는 데이터, 신뢰성, 보안성 및 안전성 등의 요소를 포함한 데이터 전략을 수립하고 있음을 확인할 수 있다.

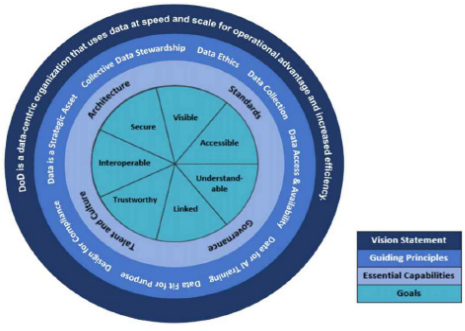

Fig. 2. Data Strategy Framework(DOD data strategy, Department of defense) [8]

영국 국방부(Ministry of Defence)는 데이터를 국방 전반 의사결정 및 효율성 개선의 핵심전략으로 정의하며 데이터 관리 전략서(Data Management Strategy) 및 국방 데이터 전략(Data Strategy for Defence)를 발표하였으며, 국방 데이터 프레임워크를 구성하여 데이터를 전략적 자산으로 활용하고자 하는 환경을 도모하고 있다[9]. 특히 Fig. 3을 통하여 확인할 수 있듯이 국방 데이터 규칙을 정의함으로써 국토, 해양, 항공, 우주 및 사이버 영역에서 국방부의 데이터 활용 역량을 향상하고자 한다. 국방 데이터 전략(Data Strategy for Defence) 및 데이터 관리 전략서(Data Management Strategy)를 통하여 영국 국방부의 데이터 관리 전략에 대한 방향성을 제시하고 있으며, 데이터 표준화에 기반한 활용성 제고, 목적에 부합하는 데이터, 접근 권한의 제어를 위한 보안, 안전 설계 및 선별된 데이터를 통한 신뢰성 확보 등을 포함한 프레임워크를 구성하고 있다. 이외, 영국 정부는 국방안보추진국(DASA: Defense and Security Accelerator)을 중심으로 인공지능 기술의 군사 분야로 적용을 추진하고 있으며, 통합작전개념(IOC) 및 미래작전개념(FOC) 등의 국방 전략을 정립하고 있다[10,11].

Fig. 3. The Defence Data Rules(Data Strategy for Defence, Ministry of Defence) [9]

이처럼 주요선진국은 데이터를 전략적 자산으로써 국방업무 혁신의 핵심 요소로 판단하고, 데이터 활용, 적용 등을 위한 데이터 관리 추진전략을 수립하고 있으며, 특히 데이터의 목적 부합성, 신뢰성, 보안성 및 안전성 등의 요소를 공통으로 포함한 전략을 정립하였음을 확인할 수 있다.

이에 정부에서도 국방부, 방위사업청, 과기정통부 등 민간 및 국방 분야에서 데이터 관련 추진전략 등의 수립을 통하여 양질의 데이터 구축 필요성 및 데이터를 체계적으로 구축하고 활용하는 방안을 마련하고 있다. 우선, 민간에서는 국가 데이터 전략의 일환으로 'AI 국가전략' 및 디지털 뉴딜정책 등을 발표하고, DNA(Data·Network·AI) 분야에 대대적 투자에 집중하고자 하며, 이를 위하여 데이터 수집 등 활용을 위한 데이터 댐 구축 및 디지털 집현전 시범 운영 등을 통하여 질 좋은 데이터의 대규모 확대를 촉진하고자 한다. 국방 분야에서는 국방부 주관 '국방 인공지능 추진전략안('21)을 마련하여 'AI 개발에 필요한 데이터 확보' 등 5대 분야 추진계획을 수립하였으며, 양질의 데이터 확보를 위한 제도 및 기반환경 구축 등의 전략을 정립하고자 한다. 또한, 방위사업청은 무기체계 획득 전문기관으로서 AI 무기체계 개발을 목표로 데이터 수집, 축적·가공, 활용 기반 구축 전략을 포함한 3대 추진전략을 발표하였다[12].

2.3 데이터 평가지표

2.1절 및 2.2절을 통하여 국내 및 해외 주요국에서 인공지능 기반 무기체계 도입을 위한 환경 조성을 위하여 국가적인 인공지능 추진전략을 수립하고 있음을 확인하였으며, 특히 데이터를 인공지능 기술의 핵심으로 인식하고 데이터 관리를 위한 전략을 수립함을 확인하였다. 이에 따라 현재 국내에 도입, 시범 운용 중인 표적탐지 및 추적분야 무기체계에 대한 데이터 관리가 필요할 실정이며, 우선 본 절에서는 데이터 품질관리를 위한 품질평가 지표를 제안하고자 한다.

주요 표적탐지 및 추적분야 체계는 2.1절에 언급하였듯 감시/정찰 무기체계 및 경계시스템 등을 포함하는 무기체계를 의미한다. EO/IR, 초분광 영상, SAR 영상, LiDAR, 편광 영상, 음원 등의 물리적 센서를 활용하는 체계이며, 인공지능 기술이 접목된 인공지능 기반 지능형 감시/정찰/경계 체계이다. 이러한 체계는 국방 분야의 특성상 민간 유사 시스템과는 다르게 불특정 다수의 사용자, 정제되지 않은 운용환경, 한정된 자원 등의 난해한 조건에서 운용되는 상황이 전반적이며, 생명과 직결되는 작전 수행 등에 따라 매우 높은 수준의 신뢰성을 요구하는 특징이 있다. 이에 따라 민간분야와의 차별점을 고려한 데이터 평가방안 수립이 필요하며, 이를 위하여 데이터가 체계 개발 및 운용유지 등 무기체계 전순기에 활용되어도 적합한지에 대한 적합성 여부 판별을 위한 다음의 네 가지 평가지표를 제시하였다.

평가지표는 다음의 사항을 고려하여 선정하였으며, 다양성, 충분성, 신뢰성 및 보안성으로 구성된다. 첫째, 폐쇄적 환경에 따른 한정된 데이터 자원으로 발생하는 인공지능 무기체계의 편향된 학습(과적합, 과소적합 등)을 방지하고자 다양한 변수, 환경 등 목적에 부합하는 데이터 확보 필요성에 입각하여 데이터 다양성 및 충분성 지표를 제시하였다. 둘째, 적대적/악의적 접근의 주요 대상이 되는 국방 분야의 특성상 데이터의 보안 및 신뢰성 확보는 필수요소이며, 특히 주요국의 국방업무의 핵심 요소로서 데이터를 전략적 자산으로 판단하고 신뢰성 및 보안성을 포함한 전략을 정립함에 따라, 데이터 품질관리를 위한 평가지표로서 신뢰성 및 보안성 지표를 제시하였다.

2.3.1 다양성

다양성은 학습 목적에 부합하도록 실제 전장의 데이터와 유사한 특징을 가진 데이터를 확보해야 하는 특성을 의미한다. 이러한 다양성은 다시 포괄성과 변동성의 두 가지 요소로 나뉠 수 있으며, 데이터 평가 시 고려되어야 한다.

첫 번째로 포괄성은 데이터가 다양한 전장 환경, 체계의 운용조건 등을 반영하여 얻어질 수 있도록 포괄적인 측면이 고려되었는지를 의미한다. 표적탐지 및 추적 시 활용된 센서 종류(EO/IR, SAR 등), 탐지 및 추적시간, 탐지 및 추적장소(시가지, 개활지, 해양, 항공 및 우주 등), 센서의 이동 속도, 위치정보(GPS), 개체 분류(지휘통제, 감시정찰, 기동, 함정, 방호 등) 및 개체정보 등을 바탕으로 다양한 종류의 클래스와 인스턴스를 포괄적으로 포함하였는지를 고려하여야 한다.

두 번째로 국방 분야는 다양한 변수와 조건 등에 따라서 상황이 지속적으로 변화하는 특성이 있다. 변동성은 사물, 사람, 장소, 시간, 환경 등 데이터 정보가 실제 전시 또는 경계상황 등에서 나타나고 나타날 수 있는 변동 가능성이 있는 다양한 범위를 충족하고 있는지와 이를 체계 학습에 반영될 수 있도록 구성하였는지를 의미한다. 표적탐지 및 추적 시 환경조건(지형, 기후조건, 날씨 정보, 시간, 해양상황 등), 장소(시가지, 개활지, 해양, 항

공 및 우주 등) 및 군사 작전상황(표적의 배치, 움직임, 작전계획 등) 등의 변수의 상황별 변화를 고려하여 데이터를 구성하였는지 고려하여야 한다.

2.3.2 충분성

충분성은 데이터 카테고리, 인스턴스가 모델 학습의 신뢰를 제공할 만큼 유의미한 수로 구성이 되어 있는지를 의미한다. 일반적인 딥러닝 알고리즘과 마찬가지로 표적탐지 및 추적모델의 경우 데이터의 양에 비례하여 성능이 향상되며, 이에 따라 체계 성능의 높은 신뢰성 확보를 위해서는 충분한 양의 데이터를 확보해야 한다. 하지만 국방 분야의 특성상 한정된 데이터 수량으로 학습과 검증 그리고 평가를 위한 데이터를 분류하여 보유하는 것에 대한 어려움이 있으며, 적성국 잠수정의 해안 침투, DMZ 철책 침투 등 난해하고 확보하기 어려운 코너케이스(Corner Case)에 대한 실제 데이터 보유의 어려움 등이 존재한다. 이에 따라 체계 학습을 위한 데이터 확보의 한계점이 파악되며, 이러한 사항을 해소하기 위한 다음의 두 가지 방안이 정립되었는지 고려되어야 한다.

첫 번째로 표적 탐지 및 추적 모델은 학습용 데이터, 검증용 데이터, 테스트용 데이터와 같이 학습, 성능검증, 최종 성능확인 등 단계별 목적에 따라 양적으로 충분한 데이터셋을 구성하도록 하여야 한다. 하지만 비밀, 비공개 데이터 등으로 인한 데이터 수의 부족으로 데이터셋을 구분할 수 없다면 과소적합(Underfitting)이 발생하지 않도록 방안을 강구해야 하며, K-Fold 교차검증 등 다양한 교차검증 방안과 데이터 확장 등, 상황별 과소적합 방지 방안에 대하여 정립하여야 한다.

두 번째로 표적탐지 및 추적 시 실제 데이터로 확보하기 어려우나 발생 가능한 상황에 대하여 충분한 데이터를 확보하여야 한다. 앞서 언급한 바와 같이 적성국 전투원 혹은 민간인의 DMZ 월책 행위 등과 같은 코너케이스(Corner Case)는 실제 데이터를 확보하는 것이 제한됨에 따라 체계 오작동 및 성능 저하를 유발할 수 있다. 이에 따라 합성데이터 생성, 데이터 부각화 등 다양한 상황에 대한 데이터 확보방안을 정립하여야 한다.

2.3.3 신뢰성

신뢰성은 데이터 준비, 수집 단계에서 체계의 오작동 및 성능 구현을 방해하는 적대적 공격에 대한 제거, 방어 등 모델의 강인함을 구현할 방안이 수립되었는지를 의미한다. 두 가지 요소로 구분되며, 데이터 평가 시 고려되어야 한다.

첫 번째로 적대적 공격에 강인한 표적탐지 및 추적모델을 위하여 적대적 공격 데이터를 제거할 수 있는 수단의 보유 여부에 대하여 고려되어야 한다. 국방 분야의 특성상 전·평시 적성국의 지속적인 위협에 노출되는 특성으로, 데이터 수집 및 모델 학습 시, 중독공격(Poisoning Attack) 등을 통하여 데이터 편향, 데이터 변조 등과 같은 데이터 오염을 유발하고 인공지능 모델의 기능 저하 및 인공지능 모델의 결정을 빗나가게 하는 공격이 가능함에 따라 의도적으로 삽입된 악의적 데이터를 제거할 수 있는 수단의 보유 여부가 고려되어야 한다.

두 번째로 적대적 공격에 강인한 표적탐지 및 추적모델을 위하여 적대적 공격 데이터의 생성 및 추가 가능한지 고려되어야 한다. 적대적 공격방법 중 하나인 회피공격(Evasion Attack)으로 특정 패턴 추가 또는 최소한의 변조 등 식별하기 어려운 방법으로 데이터를 변조하여 인공지능 모델의 의사결정을 빗나가게 할 수 있음에 따라 노이즈 데이터 생성 및 추가 가능 여부의 고려가 필요하다. 이러한 방법은 적의 경계시스템 등 표적탐지 및 추적으로부터 아군을 보호할 수 있으며, 반대로 적으로부터 대응을 가능하게 함에 따라 필수적으로 고려되어야 할 사항으로 판단된다.

2.3.4 보안성

보안성은 비밀 민감데이터가 다수인 국방 환경에서 데이터에 대한 접근제어와 공유, 활용 등을 위한 공급망의 보안이 확보되었는지를 파악하는 것을 의미하며, 데이터 평가 시 고려되어야 한다.

국방 분야의 특성상 전·평시 사이버 위협이 증가하고 있으며, 고도화된 사이버전 수행으로 다양한 공격이 이루어짐에 따라 방어적 예방체계 등의 보안성 확보가 필수적이다. 이처럼 사이버 위협과 같은 접근 권한이 없는 비인가 조직, 인원의 접근은 데이터의 위·변조와 같은 훼손을 가능케 하며, 악의적 데이터 조작을 통해 데이터의 다양성 및 신뢰성을 저하시킬 수 있다. 이에 따라 데이터 접근제어 방안이 수립되어야 하며, 데이터 변경 이력 확인 등을 통해 변조 또는 훼손 여부를 확인하는 사항이 고려되어야 한다. 또한, 데이터의 획득, 가공 및 유통 시 비밀 민감데이터는 보안성이 확보된 폐쇄된 공급망을 활용하여 데이터의 공유 및 관리가 필수적이다. 이러한 특성에 따라 데이터 유통 시 데이터 경로 히스토리 및 망 외 유출 여부를 파악할 수 있는 방안이 마련되어야 하며, 주기적인 모니터링 등을 통한 공급망 보호 방안을 정립하여야 한다.

3. 결론

본 논문은 현재 미 정립된 국방 데이터 품질관리 방안 마련을 위한 선행 연구의 일환으로서 국내·외 인공지능 기반 무기체계 도입 현황 및 주요국의 데이터 관련 추진 전략을 조사하고, 데이터 품질관리 시 고려되어야 할 평가지표에 대하여 제시하였다.

해외 주요국은 국가적 인공지능 추진전략을 수립함으로써 인공지능 기반 무기체계 도입을 위한 환경을 조성하고 있으며, 전략적 자산으로써 데이터 관리 전략을 수립하고 있다. 특히 데이터 전략 프레임워크로 목적 부합성, 신뢰성, 보안성 및 안전성 등의 요소를 포함하여 국방업무 혁신의 핵심 요소로서 데이터 활용성을 제고하고 있다. 국내 국방도 무기체계로 인공지능 기술의 적용이 확대되어가는 단계로서 경계시스템 등 표적탐지 및 추적 무기체계가 도입 및 시범운용 중에 있으며, 국방부 및 방위사업청을 중심으로 국방 인공지능 전략 및 데이터추진 전략을 수립하고 있다.

이러한 점에 입각하여 표적탐지 및 추적분야에 대한 데이터 품질관리 시 고려되어야 할 네 가지 평가지표(다양성, 충분성, 신뢰성 및 보안성)를 도출하였고 이렇게 도출된 네 가지 평가지표는 현재까지 미 정립된 표적탐지 및 추적 분야 무기체계의 데이터 품질관리 방안과 같은 가이드라인 마련 시 평가지표로서 적용 가능할 것으로 사료되며, 이외 데이터 준비 단계의 데이터 수집 기준 및 군에서 기 보유중인 데이터에 대한 활용 가능 여부 판별 기준 등으로도 적용이 가능할 것으로 판단된다.

이렇게 제안한 데이터 평가지표를 바탕으로 연차별 평가지표 고도화 및 연계 평가지표를 추가 개발하여 '표적탐지 및 추적 분야 데이터 품질관리 가이드라인' 수립 등 향후 국방 분야에 적합한 데이터 품질관리 가이드라인을 순차적으로 수립할 계획이다.

References

[1] J. W. Ahn, S. W. Noh, T. H. Kim, I. W. Yun, "An Empirical Study on Defense Future Technology in Artificial Intelligence", *Journal of the Korea Academia-Industrial cooperation Society*, Vol.21, No.5, pp.409-416, 2020.
DOI: http://doi.org/10.5762/KAIS.2020.21.5.409

[2] J. W. Ahn, S. W. Noh, T. H. Kim, "An Empirical Study on the Prediction of Future New Defense Technologies in Artificial Intelligence", *Journal of the Korea Academia-Industrial cooperation Society*, Vol.21, No.9, pp.458-465, 2020.
DOI: http://doi.org/10.5762/KAIS.2020.21.9.458

[3] J. K. Cho, Policy Recommendations for Defense Artificial Intelligence, Research Report, Korea Institute for Military Affair, Korea, pp.13-22.

[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] NIA, Data Quality Management Guidelines for AI Learning, Technical Report, National Information Society Agency, Korea.

[6] NIA, Guideline for Building Data sets for AI Learning, Technical Report, National Information Society Agency, Korea.

[7] J. J. Lee, "U.S.-China Military Technology Competition and Power Transition: Focusing on Artificial Intelligence, Autonomous Weapon Systems" *Korea and World Politics*, Vol.38, No.3, pp.1-35, 2022.
DOI: http://doi.org/10.17331/kwp.2022.38.3.001

[8] DOD, DOD data strategy, Department of Defense(DoD), United States of America.

[9] MOD, Data Strategy for Defence : Delivering the Defence Data Framework and exploiting the power of data, Ministry of Defence, United Kingdom.

[10] KIDET, A Study on the Establishment of Defense Artificial Intelligence Development Plans, Research Report, The Korean Institute of Defense Technology(KIDET), Korea, pp.60-62.

[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 Policy Institute, Korea.

[12] KRIT, Future Defense 2030 Technology Strategy, Research Report, Korea Research Institute for defense Technology planning and advancement (KRIT), Korea, pp.13-15.

서 석 호(Suk-Ho Seo) [정회원]

- 2015년 2월 : 충남대학교 재료공학과 (공학사)
- 2017년 2월 : 충남대학교 신소재공학과 (공학석사)
- 2017년 12월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방품질경영, 신소재공학, 금속재료공학

박 주 영(Joo-Young Park) [정회원]

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

〈관심분야〉
국방품질경영, 전기, 전자, 사이버보안

정 민 경(Min-Kyung Jeong) [정회원]

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

〈관심분야〉
국방품질경영, 전자회로, 반도체 공정기술

이 원 영(Won-Young Lee) [정회원]

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

〈관심분야〉
국방품질경영, 소프트웨어 설계검증, K-RMF

최 은 진(Eun-Jin Choi) [정회원]

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

〈관심분야〉
국방품질경영, 사이버보안, K-RMF