https://doi.org/10.33778/kcsa.2020.20.4.113

4차 산업혁명시대 스마트 강군 건설을 위한 국방 데이터의 전략적 활용 방안연구

김 세 용*, 김 준 상**, 강 석 원***

요 약

4차 산업혁명은 고도화된 정보기술과 지능기술로 촉발되는 초연결 기반의 지능화 혁명이라 할 수 있으며, 이러한 기술을 구현하기 위해 가장 기본이 되는 것은 '데이터'이다. 본 연구에서는 국방 영역에서 이러한 지능화 혁명을 이끌어 내기 위하여 데이터를 전략적으로 활용할 수 있는 방안에 대해 제안한다. 우선 국내외 동향 및 선행 연구 분석을 통해 시사점과 국방 데이터 관리의 현 실태를 분석하였으며, 4가지 발전방향을 제시하였다. 향후 국방의 환경을 고려한 국방 데이터의 구축, 개방, 공유, 유통, 융합 등의 전 수명주기관리에 대한 환경을 조성하고 활용할 수 있는 여건을 조성해 준다면 4차 산업혁명 시대 스마트 국방혁신을 통한 디지털 강군으로 재탄생하는 밑거름과 지름길이 될 것으로 기대된다.

A Study on the Strategic Application of National Defense Data for the Construction of Smart Forces in the 4th IR

Seyong Kim*, Junsang Kim**, Seokwon Kang***

ABSTRACT

The fourth industrial revolution can be called the hyper-connected-based intelligent revolution triggered by advanced information technology and intelligent technology, and the basis for implementing these technologies is 'data'. This study proposes a way to strategically use data in order to lead this intelligent revolution in the defense area. First of all, implications through analysis of domestic and international trends and prior research and current status of defense data management were analyzed, and four directions for development were presented. If the government composes conditions for building, releasing, sharing, distribution, and convergence of defense data considering the environment of national defense in the future, it is expected that it will serve as a foundation and a shortcut to be a digitalized strong military through smart defense innovation in the era of the fourth industrial revolution.

Key words : 4thIR, Defense data, Bigdata, AI, Artificial Intelligence

접수일(2020년 09월 29일), 수정일(1차: 2020년 10월 18일), 게재확정일(2020년 10월 22일)

* 국방부 정보화기획관실 정보통신기술정책과(주저자)
** 국방부 정보화기획관실 정보통신기술정책과(공동저자)
*** 육군본부 시험평가단(교신저자)

1. 서 론

현재 우리는 4차 산업혁명이라는 새로운 패러다임의 대두로 인해 급변하는 세상에서 살고 있다. 이러한 4차 산업혁명은 고도화된 정보기술과 지능기술로 촉발되는 초연결 기반의 지능화 혁명으로 이러한 기술 구현은 근본적으로 디지털화 된 데이터에서 시작된다. 데이터 기반의 다양한 분석은 미래를 예측하고 검증할 수 있는 통찰력을 제공할 수 있기 때문에 불확실한 미래 작전환경에서 이상징후를 사전에 파악하고, 이에 대한 해결방안 및 의사결정을 신속하게 제공할 수 있다.

민간영역에서는 이러한 데이터 활용기술들을 적용하여 기존 서비스보다 성능 및 기능적으로 발전된 서비스들이 출시되고 있다. 특히 빅데이터, 인공지능 기술의 발전은 기존의 기술로는 구현 불가능했던 영역의 서비스를 가능하게 하는 혁명적 기술로, 지금까지 없었던 새로운 시장을 창출하고 있다. 현 정부도 데이터를 전략적 자산으로 인식하여 디지털 뉴딜 정책(2020)을 통한 데이터 댐 구축을 적극적으로 추진하고 있다. 각 정부부처 및 공공기관에는 데이터 기반의 행정 활성화 및 의사결정 지원체계 구축을 추진하고 있으며 이를 위해 데이터 가시화, 표준화, 품질관리 등을 강화해 나가고 있다[13].

우리 군도 이에 발맞추어 데이터 기반의 스마트 국방혁신을 추진하고 있다. 현재 국방 데이터를 기반으로 빅데이터, 인공지능 기술의 다양한 국방 분야 적용을 모색하고 있다. 전력 분야에서는 전투력 증강을 위해 자율무인체계, 무인로봇 해당 기술의 적용을 추진하고 있으며 국방 경영 효율화와 서비스 품질 향상을 위해 인사/군수/의료 분야에서도 해당 기술들을 접목해 나가고 있다[12]. 이러한 노력들이 최상의 결과로 나타나기 위해서는 기술 구현의 기초가 되는 양질의 국방 데이터를 대량으로 확보하고 이를 활용할 수 있는 생태계의 조성이 가장 중요하다.

하지만 국방 영역의 정보화 환경은 보안 규정 및 정책으로 인하여 데이터의 수집 및 활용에 한계가 있으며 폐쇄적인 조직의 문화적 특성으로 인해 데이터의 공유 및 융합이 매우 제한되고 있다. 따라서 우리는 국방 데이터를 수집하고 활용하는 방안과 더불어 보안 대책을 함께 고려해야 한다. 현재 수집, 활용, 보안 각 영역별 발전방안이나 문제 해결방안 등은 기존 연구들을 통해 제시되고 있지만 전사적 관점에서의 연구와 분석은 매우 부족한 상황이다. 이는 국방 분야가 타 분야와는 다르게 다양한 무기체계, 방대한 조직, 복잡한 네트워크 및 데이터 흐름 등의 특성을 가지고 있기 때문이다.

본 논문에서는 기존 연구들을 바탕으로 전사적 관점에서 국방 데이터의 전략적 활용 및 발전방안에 대하여 제안하였다. 2장에서는 데이터 관련 기술의 국내외 동향과 기존의 국방 분야 데이터 관련 선행 연구들을 소개하였다. 3장에서는 국방 데이터 관리의 현 실태에 대한 부분을 설명한다. 4장에서는 국방 데이터의 전략적 활용을 위한 발전 및 추진 방안을 제시하고 5장에서 결론을 맺는다.

2. 국내·외 동향 및 선행연구

2.1 국내 동향

현재 범정부 차원에서 데이터의 전략적인 활용을 위해 플랫폼 구축, 데이터 전담조직 구성, 활용계획 수립 및 법령 제정 등을 활발히 추진하고 있다.

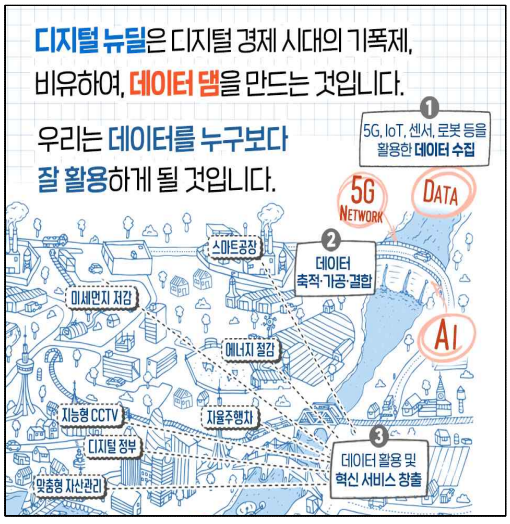
행정안전부는 데이터의 전략적 활용을 위한 인프라 구축 및 활용을 위하여 공공데이터활용 지원센터 및 공공데이터 포털을 2013년부터 운영 중에 있다. 또한 정부 빅데이터 공통기반 플랫폼인 ‘혜안’을 2016년도에 구축하여 각종 행정 분야에서 적극적으로 공공데이터를 활용할 수 있는 기반을 마련하였다. 또한 AI 학습데이터, 국가 데이터맵, 데이터 프리존, 안심존 등 고도화된 데이터 분석 환경을 구축하여 운영 중에 있다.

과기정통부는 혁신성장 전략투자의 일환으로 ‘데이터·AI 경제 활성화 계획’을 발표하여 본격적으로 추진하고 있다[3]. 또한 AI 구현을 위한 학습용 데이터와 분석 서비스 및 시스템을 한 번에 제공하는 AI 허브를 2018년에 구축하여 서비스

하고 있으며, 매년 데이터 구축 사업을 통해 빅데이터 및 학습용 데이터를 발굴하고 있다.

2020년 1월, 국회에서는 개인정보 데이터 활성화를 위하여 데이터 3법의 개정안을 통과시켰다. 이는 개인정보 보호법, 정보통신망법, 신용정보법을 새롭게 개정한 것으로 데이터 활용 확대와 안전한 이용을 위한 사회적 규범을 정립하고자 각 시민단체, 산업, 법조, 학계 등 다양한 분야의 의견을 수렴해 마련되었다[4][6][14]. 이번 법 개정을 통해 통계 작성, 연구, 공익적 기록 보존 등을 위해 가명 정보를 신용정보 주체의 동의 없이 이용 및 제공이 가능하게 되었다.

2020년 7월, 정부는 위기극복과 코로나 이후 글로벌 경제 선도를 위한 국가발전전략인 한국판 뉴딜 종합계획을 발표했다[13]. 한국판 뉴딜 종합계획은 첫째, 디지털 국가를 달성하고 비대면 유망 산업을 육성하는 '디지털 뉴딜', 둘째, 탄소 중립을 목표로 경제·사회 녹색전환을 추진하는 '그린 뉴딜', 그리고 고용·사회안전망과 사람 투자를 확대하는 '안전망 강화'의 3개 분야로 구성되어 있다.



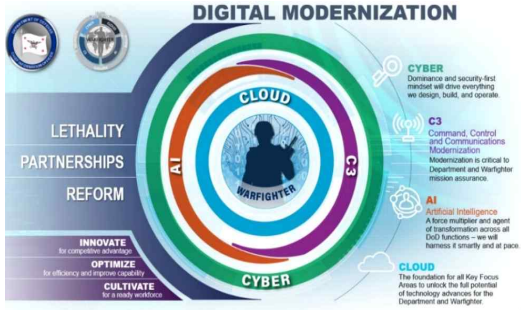
(그림 1) 디지털 뉴딜정책-데이터 댐

디지털 뉴딜은 (그림 1)과 같이 국가의 디지털 전환을 이끌기 위해 데이터를 모아 디지털 경제 기반이 되는 데이터 댐을 만드는 것으로, 디지털 역량을 전 산업 분야에 결합하는 것이 목표이다. 댐이 저장된 물을 이용하여 수력발전을 통해 전기를 생산하듯이, 데이터 댐은 저장된 데이터를 이용하여 새로운 산업과 비즈니스를 창출할 수 있다. 우선 데이터 댐 구축을 통해 데이터의 수집과 가공 과정에서 수많은 일자리가 창출된다. 또한 이를 활용하는 빅데이터 분석, 인공지능 등의 기술의 적용이 활발해져 기존 산업의 혁신을 이끌어내어 새로운 서비스와 일자리를 만들어낼 것으로 기대되고 있다.

2.2 국외 동향(미군 중심)

미 국방부는 2019년 7월 디지털 현대화 전략을 수립하였다[17]. 디지털 현대화 전략은 현대전에서 합동군에게 경쟁우위를 제공할 수 있는 디지털 환경을 발전시키기 위하여 수립되었다. 국방 전역에 걸쳐 기술적 능력을 향상시키고 디지털 영역에서의 경쟁력을 확대하기 위해 엔터프라이즈 시스템 채택을 강화하는 것이다.

디지털 현대화 전략은 (그림 2)와 같이 국가방위전략 구현을 위해 클라우드, 인공지능, 지휘·통제·통신, 사이버 보안으로 이루어진 로드맵을 계획하고 있다. 특히 인공지능을 가장 핵심적인 전략으로 가장 중요하다고 판단하고 있으며 이를 위한 데이터의 전략적 수집과 활용을 강조하고 있다.



(그림 2) 미 국방부 디지털 현대화 전략

디지털 현대화 전략의 목적은 '경쟁우위를 위한 혁신', '효율성과 개선된 능력을 위한 최적화', '민

첩하고 복원력 있는 방어태세를 위한 사이버보안 개선', 그리고 '준비된 디지털 인력을 위한 재능 배양'의 4가지로 설정되었다.

데이터 관리와 연관된 목적은 '경쟁우위를 위한 혁신'이며, 이 목적을 달성하기 위해 'AI-가능 능력의 채택과 통합을 가속화하기 위한 합동인공지능센터(JAIC : Joint Artificial Intelligence Center)의 신설', '민간 혁신을 이용하기 위해 엔터프라이즈 클라우드 환경 제공', '데이터를 전략적 자산으로 다룸' 등을 목표로 설정하여 추진하고 있다[18][19].

미 국방혁신위원회(DIB: Defense Innovation Board)는 데이터의 활용 및 관리를 위하여 4가지(접근, 분석, 사용, 표준) 분야에 대한 제안을 제시하였다[17].

첫째, 접근 분야는 현재 데이터가 NIPRNet(Non classified Internet Protocol Router Network) 또는 다른 접근 가능한 네트워크를 통해서도 탐색 가능하도록 구성하고, 모든 DB를 스캔(검색) 할 수 있는 코드를 구현해야 한다고 주장하였다. 또한 지식베이스를 종합하고 데이터 간의 연결 정보를 생성하여 그것을 사용자에게 제공할 수 있도록 구축해야 한다고 제안하였다.

둘째, 분석 분야는 데이터의 무결성을 보장할 수 있어야 하는데 데이터 분석과 의사결정 지원을 위한 별도의 오프라인 데이터 복사본의 생성 필요성을 주장하였다. 현재는 트랜잭션과 데이터 분석 시 동일한 데이터를 사용하여 분석하고 있어 원본 데이터의 훼손 가능성을 우려한 제안이었다.

셋째, 표준 분야는 기존의 합동표준위원회가 표준을 제정하는 구조에서 새로 발생하는 수요와 기회에 대응하기 위해 부서 전반에 걸쳐 유연한 협력과 참여를 촉진하는 형태로 개선해야 한다고 주장하였다.

넷째, 사용 분야는 단일 데이터베이스가 아닌 여러 데이터베이스로부터 데이터를 수집하여 활용할 수 있어야 하되 현재 파악되지 않은 다양한 목적을 위해 데이터가 활용될 수 있어야 한다고 제안하였다.

2.3 선행 연구

국방 데이터의 활용에 대하여 분석한 연구는 다수 수행되었지만 이러한 데이터를 활용하기 위해 무엇을 어떻게 준비해야하는 지에 대한 전사적 측면에서의 연구는 거의 이루어지지 않았다. 김세용 등 은 인공지능의 학습용 데이터의 신뢰성 보장을 위해 블록체인기술을 도입해야 함을 제시하였지만[5], 실증은 없었고 방법론적 방향성만 제시하였다. 신우택 등은 "국방 빅데이터/인공지능 활성화를 위한 다중메타데이터 저장소 관리시스템(MRMM) 기술연구"를 통해 국방부 뿐만 아니라 각 군에도 메타데이터 관리시스템을 도입하여 데이터 표준과 품질을 향상시켜야 함을 제시하였다[10]. 하지만 이 문제는 조직과 인력이 확충되어야 하며, 현재 국방 정보화 기본계획과 국방통합데이터센터의 클라우드 환경구축과 상충되는 개념으로 현실적으로 도입이 제한된다. 여성철 등은 "국방 정보체계의 비밀데이터 관리 방안을 제시하였다[11]. 이 연구를 통해 정보체계에 저장되어 있는 비밀 데이터의 경우, 기존 군사 보안업무 훈령으로 관리했을 경우의 제약 사항을 식별하였고, 이를 개선하기 위한 방안을 제시하였다. 황선웅은 국방 데이터의 전략과 구현 방안 연구를 통해 거버넌스의 정립, 데이터 자산의 가시화, 데이터 표준화 및 품질제고, 데이터 통합관리 기반환경 조성을 제시하였지만 데이터의 보안적 측면에서는 상세하게 다루지 않았다[15].

3. 국방 데이터의 현상 / 현 실태 분석

3.1 정책/제도 측면

국방 데이터 분야에서의 각종 정책과 제도 측면은 여러 가지 법령들이 상호 상충이 되면서 사용자의 유권해석에 따라 데이터의 저장과 유통 등의 수명주기가 각기 다르다. 국방 공공데이터 제공 훈령 상에는 데이터를 공개하고 공유해야 함을 강조하고 있다[2]. 하지만 군사 기밀사항에 대해서는 예외 조항을 두었는데 각 국방 기관 및 부서에서는 이를 근거로 데이터 공개 및 제공을 꺼려하

며, 심지어 국방 내부에서의 공유 및 활용도 거부하는 경향이 크다. 또한 각종 훈령과 제도, 지침 등은 데이터의 '활용' 보다는 '보호' 중심으로 작성되어 있다. 특히 국방 000체계의 경우 데이터 활용을 위해서 약 20여 개 기관의 승인을 받아야만 사용이 가능하도록 되어 있는 등 데이터를 사용하기 위한 절차가 매우 복잡한 경우가 많다.

국방 보안업무훈령 및 전장관리정보체계 관리지침 등에는 운영 및 훈련 데이터의 보관 기관이 매우 짧게 규정되어 있어 추후 활용이 거의 불가능하다. 관리 측면에서도 단위정보 시스템 중심의 데이터 표준화, 상호운용성 및 연동 위주의 절차만 제시하고 있고 데이터의 전략적 분석 차원의 정책은 정립되어 있지 않아 전사적인 측면에서 데이터가 관리가 불가능한 상황이다.

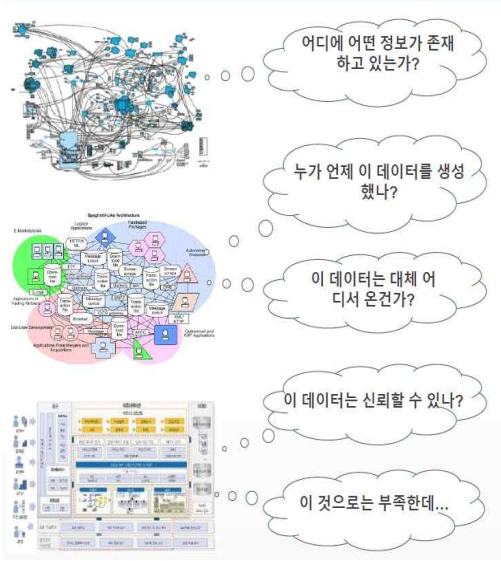
관련 법령인 국방정보화 기반조성 및 국방정보자원관리에 관한 법률(법률 제12553호) 또한 개략적인 데이터 관리에 대한 조항만 나열하고 있어 제대로 된 관리책임을 부여할 수 없는 실정이다.

보안의 3요소는 기밀성, 무결성, 가용성으로 이 3개의 요소 모두 최적의 균형을 유지하는 것이 가장 중요 하다. 하지만 현재 군의 보안은 기밀성에만 초점이 맞춰져 있어 사용자의 데이터 활용 범위를 크게 제한시키고 있다. 공급자는 보안규정 미준수라는 미명아래 데이터 저장, 공개가 제한되고 사용자 역시 보안규정으로 인해 열람이 제한되는 경우가 상당하다.

결국 현재 국방 영역에서는 데이터의 관리와 활용 측면을 고려하지 않은 법령 및 국방 보안규정의 한계로 인하여 양질의 데이터 축적이 제한되며, 데이터 확보 절차도 복잡하고 어려워 국방 데이터의 사용 활성화에 제한요소로 작용하고 있는 상황이라고 판단할 수 있다.

3.2 데이터 활용환경 측면

대부분의 국방 관계자들은 국방 데이터를 잘 활용하지 못하고 있다고 판단하고 있다. 국방 정보체계가 보유하고 있는 수 많은 데이터들을 활용하여 새로운 가치를 창출할 수 있다고 생각하지만 정작 현실은 이러한 데이터가 어디에 있고, 어떤 데이터가 있는지 식별조차 어려운 실정이다. 국방 데이터는 (그림 3)과 같이 "어디에", "어떤 데이터가", "어떻게" 존재하고 활용되는지 종합적인 관리가 이루어지고 있지 않아 데이터 활용에 대한 인식이 매우 저조한 실정이다. 국방 데이터의 사용자들은 어디에 어떤 정보가 존재하고 있는지 찾을 수 있는 수단과 방법이 부족하며, 필요한 데이터를 찾더라도 그 데이터에 대해 "누가", "언제" 이 데이터가 생산되었는지에 대한 확인이 제한되어 데이터에 대한 신뢰성의 검증이 어려운 상황이다.



(그림 3) 국방 데이터 활용 현실태[8]

현재 각 국방 기관에서는 보유하고 있는 데이터에 대한 공개 및 공유를 거부하는 경향이 매우 강하여 데이터의 유통이 거의 이루어지고 있지 않다. 특히 국방 기관에서 데이터 보안 문제는 국가안보에 치명적인 위협을 가할 수 있는 위중한 사안으로 보안사고 발생 시 무거운 처벌을 피할 수 없기 때문에 해당 업무 담당자들은 데이터의 공유 및 활용에 매우 소극적인 상황이다.

결국 분산되어 있는 국방 데이터들이 융합되어 활용되면 더욱 큰 가치를 창출할 수 있으나 이러한 이유로 인해 데이터 활용 환경이 매우 제약되

어 있는 상황이다.

3.3 국방 데이터 표준 및 품질관리 측면

데이터는 국방의 '중요한 전략적 핵심 자산'임에도 불구하고 데이터의 품질 점검 및 활용 노력 미흡으로 데이터의 신뢰성이 저하되고 있다. 국방정보체계 기능에 대한 유지보수 및 성능개선은 지속 추진되고 있으나, 오류데이터 정비 및 데이터 표준화 등에 대한 데이터 관리는 매우 소홀한 수준이며, 범정부 차원의 데이터 품질진단 및 표준준수율도 타 부처보다 낮은 수준을 보이고 있다[1]. 매년 정부에서 제공해주는 품질진단 도구인 SDQ로 진단을 하고 있지만 진단 이후 개선작업이 충분히 이루어지지 않고 있다. 이를 국방부 차원에서 개선해 나갈 필요성이 존재하지만 현재는 이를 수행할 컨트롤 타워와 정책, 시스템 등이 준비되지 않은 상황이다. 특히 인공지능에 활용할 데이터는 편향성 등의 문제가 발생하지 않도록 신뢰성을 확보해야 하는데 이런 역할을 수행할 역량이 부족한 실정이다.

국방 데이터는 그 양이 방대하여 기존 인력으로 관리하기에는 한계가 있기 때문에 자동화된 시스템이 필요하다. 그러나 데이터 생성에서부터 활용까지 전 단계에 원활한 데이터 유통관리를 위한 시스템이 없어 데이터의 품질저하를 가속화 시키고 있다.

3.4 국방 빅데이터 / AI 적용 추진 측면

국방부는 국방의 다양한 데이터를 활용하여 빅데이터 및 AI 기술개발과 국방에 적용을 추진해 나가고 있다. 하지만 데이터 수집에서 활용까지 제약사항이 과다하여 수집을 위해 상당한 노력과 시간이 낭비되고 있다. 그렇다 보니 관련 최신 기술 확보 및 데이터 축적을 위한 단위 기능별로 사업을 추진하여 일회성 사업으로 종료되는 경우가 많다. 사업 종료 이후의 확대 사업 추진, 정책 반영 등의 환류 활동 또한 미흡하여 최신 기술의 국방 분야 도입 및 확산이 느리게 진행되고 있다. 이로 인해 유사 기능의 사업들이 개별적으로 추진되고 있어 사업의 중복성과 예산의 낭비 등이 우려된다.

특히 인공지능 관련 사업은 신뢰성 있는 학습용 데이터셋 구축 사업이 병행되어야 하는데 이에 대한 종합적인 계획이 부재하여 향후 관련 사업의 추진에 한계가 있는 상황이다. 또한 공통기술이나 데이터 등을 활용하고 상호간의 노하우 등을 공유할 수 있는 문화와 시스템이 정착되어 있지 않아 여러 문제가 발생하고 있다. 실제 국방 R&D 또는 과기정통부 R&D 사업 등으로 대규모의 예산을 투입하여 개발하고 있는 영상(이미지)분석체계 같은 경우 군에서 데이터를 제공하지 않거나 제한된 공간에서만 데이터 활용이 가능하다. 결국 데이터의 신뢰성이 저하되어 구현된 학습 모델의 예측률이 떨어지고, 개발된 결과물들을 외부로 반출하지 못함으로 인해 확산이 제한되는 어려움을 겪고 있다. 또한 이러한 사업이 추진되고 있음을 국방부 또는 각 기관(군) 실무자들이 인식을 못함에 따라 노력의 낭비와 예산의 중복 투자 등이 지속적으로 발생하고 있다.

3.5 국방 데이터의 보안적 측면

현재 PC, 서버, 네트워크 장비, 스마트기기 등 장비의 종류에 관계 없이 해커들의 무차별적인 공격대상이 되어 피해사례가 급증하고 있다[15]. 특히 2018년 시만텍의 "인터넷 보안 위협 보고서"에 따르면 악성코드의 변종은 작년 대비 92.0%, 랜섬웨어 악성코드의 변종은 46.0%로 각각 증가했다고 한다[3]. 이처럼 사이버 위협이 증가하고 있고 주변의 위협 국가가 상당수 상존하는 한국의 상황에서는 국방 데이터의 전략적 활용은 국가 안보위협의 핵심적인 요소가 될 수 있다. 따라서 국방 데이터의 활용에 있어서 사이버 보안 측면에서의 능력 강화가 필요하다.

국방 데이터의 보안 아키텍처가 수립되어 있지 않아 보안대책이 조각나 있는 상황으로 매우 비효율적일 뿐만 아니라 그 자체가 상당한 보안 위협으로 작용하고 있다. 예를 들면 보안을 위하여 여러 가지 관문으로 방화벽과 악성코드 탐지 에이전트를 구축하였으나 통합된 보안 전략이 구축되어

있지 않아 실효성이 저하되고 있다. 특히 국방 데이터의 전략적인 활용을 위해서는 대용량 데이터셋 구축이 필수적인데 그러한 데이터셋 구축을 위해서는 분산되어 있는 데이터의 수집이 필요하다. 다수의 데이터가 수집되다보면 다양한 종류의 사이버 위협 수단들이 포함될 수 있기에 이에 대비한 대책이 필요한 실정이다.

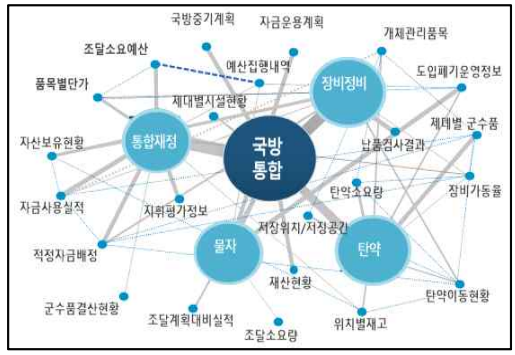
또한 수집된 데이터들은 개인정보가 포함되어 있을 수 있다. 이는 곧 개인정보활용에 대한 법적 문제로 귀결된다. 따라서 국방 데이터의 전략적 활용을 위해서는 개인정보보호에 대한 대책 강구가 필요하다. 현재는 각 업무 담당자에 의한 기밀성 유지 대책이 유일한 개인정보보호 방법으로 총체적인 개인정보 보호대책이 시급하다.

마지막으로 앞서 언급한 보안대책의 기획, 계획, 수행, 평가를 위한 전문 조직 및 인력이 필요하다. 현재는 국방 기관 내에도 주요 사이버 보안을 담당하고 있는 기관과 인력이 다수 존재하고 있으나 현재 보유하고 있는 데이터의 규모를 고려했을 때 상당히 부족한 실정이다. 따라서 향후 발생할 수 있는 데이터 증가량과 사이버 방호 장비의 발전과 더불어 필요한 조직 및 인력의 확대가 필요하다. 특히 수많은 ICT 장비들이 보급되고 있는 현 실정을 고려할 때 보안 인증이 되지 않은 장비들에 대한 검토를 수행하는 조직의 구성이 시급한 실정이다.

4. 전략적 활용을 위한 발전방안

4.1 국방 데이터 활성화 여건 조성

국방부 정보화기획관실 주도로 국방 데이터 분야에 대한 컨트롤 타워 역할을 수행하면서 국방 데이터 전 수명주기에 대한 효율적 관리를 위한 단계별 중장기 발전계획과 세부이행과제를 수립하여 추진해 나가야 한다. 더불어 20년 연말에 발표 예정인 국방 인공지능 발전계획과 연계하여 국방 영역 전반에 걸쳐서 데이터를 가장 잘 활용할 수 있는 여건을 조성해야 한다. 현재 추진 중인 국방 데이터훈령에는 '데이터제공의 의무화'와 '민감·비밀정보 제공기준을 정립'하고 최소 실장급을 위원장으로 국방 데이터관리 위원회를 구성하도록 제정해야 한다. 또한 데이터분석 및 융합을 위한 정보 요구 시 특별한 사유가 없는 한 데이터 제공을 의무화하고, 민감한 개인정보·군사정보, 비밀데이터 등은 안전한 활용을 위한 데이터 제공 및 활용 절차(기준)을 마련해야 한다. 이러한 정책적 기준에도 불구하고 데이터 관련 분쟁이 발생 시 해결이 가능하도록 국방 데이터관리위원회에서 분쟁을 조정할 수 있는 권한을 부여할 필요가 있다.



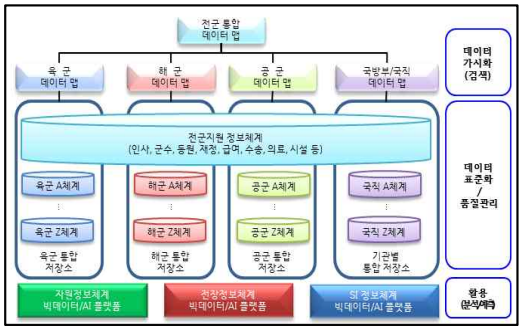
(그림 4) 국방 데이터 맵(예시)

전군에서 생산되고 관리하고 있는 데이터를 손쉽게 찾고 확인할 수 있도록 전군에 서비스가 가능한 데이터 맵을 구축하여 (그림 4)와 같이 국방 데이터의 가시화를 추진해야 한다. 해당 기능은 별도로 구축하는 것이 아닌 국방 빅데이터 분석포털 또는 구축 예정인 국방 지능형 플랫폼과 연계하여 서비스가 될 수 있도록 개발해야 한다.

4.2 국방 데이터 관리 생태계 구축

국방 데이터 관리체계는 (그림 5)와 같이 평문 데이터는 물론 비밀 데이터, 특수정보 데이터까지 통합적으로 관리할 수 있도록 구축을 하되 국방망(자원망, 전장망, SI망 등)의 환경을 고려하여 종합적으로 검토 후 구축해야 한다. 국방부 차원의 전군지원 시스템에 대한 통합 DB와 각 군의 특성에 맞는 데이터 수집 및 관리를 위한 각 군별 데이터 저장소를 구축하고, 이러한 데이터를 식별할 수 있는 데이터 맵과 데이터 표준화 및 품질관리

를 동시에 수행할 수 있는 통합관리환경으로 구축하여 활용성과 효율성을 제고시켜야 한다.



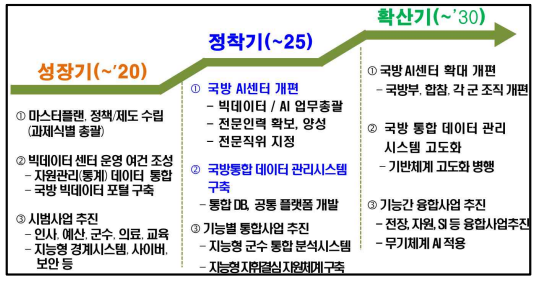
(그림 5) 국방 데이터 관리체계(안)

국방 데이터 구조, 표준, 품질, 흐름 등을 고려하여 데이터 거버넌스 프레임워크를 설계 및 운영 방안을 수립하여 데이터의 신뢰성, 정합성을 보장받을 수 있는 플랫폼 구축을 구축하고 이에 따르는 데이터 관리정책, 관리시스템, 관리프로세스 및 관리조직 등을 종합적으로 고려하여, 이를 하위 체계간의 통합 및 연계 운영절차 및 기준을 수립하여야 한다. 데이터 거버넌스 기반 데이터 포털의 고려요소로는 분석을 수행하는 데이터분석가와 분석결과 정보를 조회 활용하는 일반 사용자가 어디에 어떤 데이터가 있고 어떻게 활용해야 할지를 알 수 있도록 데이터 현황을 제공받을 수 있어야 한다. 또한 데이터 품질관리 운영정책·제도와 연계하여 각 기관별 데이터 표준화·품질담당을 지정하고 운영하며, 정기적 진단을 통해 품질향상 및 표준데이터로의 전환을 추진해야 한다.

더불어 이러한 정책추진과 활동을 위한 데이터 관리 조직 및 인력이 확충 또는 보강되어야 한다. 전체적으로 군 인력이 감축되는 측면을 고려하여 인원보충이 제한된다면 각 기관별로 전향적으로 검토를 통해 임무 재조정을 하여 데이터 관련 조직 또는 인력을 보강해야 한다. 국방 분야에서도 데이터 직렬 또는 부특기를 부여하여 전문인력을 지속적으로 관리할 수 있는 체계를 발전시켜야 한다. 마지막으로 국방 분야 데이터 및 관련 기술을 개방·공유하고 관련분야 전문가 등의 교류협력 등을 통한 집단지성 활용을 위해 민-관-군-산-학-연 협력체를 구성하여 연구개발 생태계를 조성하여 활용하여야 한다.

4.3 전략적 국방 빅데이터 / AI 발전 추진

국방 데이터의 전략적 활용을 통해 국방 각 영역에 빅데이터와 AI를 접목하여 국방효율화와 전력증강에 앞서가야 한다. 20년 연말 공표예정인 '국방 인공지능 발전계획'과 연계하여 20년까지는 성장기를 거치고 25년까지는 국방전반에 이를 활용하고 정착할 수 있는 문화를 조성한 후에 25년 이후 국방 전 분야에 확산을 할 수 있도록 (그림 6)과 같이 단계별로 추진해 나가야 한다.



(그림 6) 전략적 국방 빅데이터/·AI 추진방향(안)

중장기 마스터 플랜을 수립하여 국방 전 분야에 확산을 추진하되, 각 기능별(정보, 작전, 인사, 군수 등) 발전 방향과 국방 클라우드 환경 구축 등을 고려하여 나간다. 또한 국방 통합데이터관리 시스템(지능형 플랫폼) 구축을 통해 앞서 제시한 국방 데이터 수명주기 관리는 물론 데이터 개방, 유통, 활용, 융합과 공통기술 활용 등을 효율적으로 관리해 나갈 수 있도록 추진해 나가야 한다.

4.4 국방 데이터 특성을 고려한 보안 강화방안

4.4.1 사이버 위협 대비 가용성 강화

민간의 다수 기업 및 기관들은 대부분 인터넷 기반의 업무환경을 구축하고 있지만 국방 기관에서는 기밀성 유지를 위하여 국방망을 사용하고 인터넷 연결을 최소화하였을 뿐만 아니라 인터넷을

활용한 장치가 있을지라도 방화벽을 통하여 불법 또는 비정상적인 데이터는 원천적으로 차단하고 있다. 이는 기밀성 유지에는 충분히 기여하고 있으나 가용성 측면에서는 매우 비효율적인 부분이라 할 수 있다. 이러한 문제의 해결을 위해 외부 데이터의 안전한 수집을 위한 데이터의 이력관리와 위변조 방지를 위한 블록체인기술, 지능형 위협차단을 위한 딥러닝 기술 적용 보안 장비도입 등 최신 ICT기술의 선구적인 활용을 위한 노력이 필요하다.

4.4.2 국방 데이터 보안 아키텍처 / 평가모델 적용

빅데이터와 인공지능 기술을 국방 영역에 적용하기 위해서는 여러 영역의 데이터 융합이 반드시 필요하다. 이를 위해 개인정보, 데이터 보안, 데이터 소유권 등에 대한 제도개선이 필요하다. 데이터 보관 및 축적을 지속적으로 추진 가능하도록 국방 보안업무 훈령 및 전장관리체계별 운영 지침을 안보지원사령부와 사이버사령부 등 관련 부서와 협력하여 개정을 추진해야 한다. 특히 비밀 또는 SI데이터를 활용하기 위해서 동일 이상의 보안 시스템, 즉 인력이나 인증된 장비, 또는 보안대책이 강구된 장소에 대한 유권해석의 문제가 발생하지 않도록 일관된 지침을 하달할 필요가 있다.

또한 국방 보안 생태계 구축을 위해 클라우드 기반의 시험환경 구축, 시험검증 도구의 개발, 상용 제품 서비스를 위한 신뢰성 검증 평가 기준 및 가이드라인의 개발이 필요하다. 보안 기술의 신뢰성 검증 평가 기준과 시험검증 도구 개발은 보안 서비스 및 보안 활용기술에 대한 버그 검증 기술 및 체계를 고착할 수 있고 보안 개발도구를 구축은 보안 핵심엔진 및 핵심 서비스의 품질검증을 가능하게 한다.

4.4.3 개인정보보호법 개정

데이터 3법 개정으로 데이터 활용 확대의 법적 기반이 만들어졌으나 국방 영역에서는 아직 해당 법률을 적용할 지침이나 행정규칙이 수립되지 않은 상황이다. 따라서 개인정보의 이용에 관한 지침이나 행정규칙을 국방 데이터 활용 전략과 맞추어 개방적으로 정비해야 한다. 정보체계에서 개인정보를 활용할 때 개인의 사전 동의를 전제로 폭넓게 법적 권한을 부여하고 합리적인 개인정보의 보호와 이용여건을 보장해야 한다. 본인의 의사에 따라 이루어지는 개인정보에 관한 사전 동의를 하는 시점에서 제공되는 개인정보의 종류 이용범위와 기간, 상업적 이용, 목적 외 이용, 타 기관으로의 제공 등을 다양한 항목별로 당사자가 직접 선택하도록 법률로서 정의하되 개인의 기본권을 포기하는 것이 아닌 법률로 보호해야 한다. 개인정보 비식별 조치 가이드라인 내용 중 데이터 3법과 상충되는 내용을 정비하고 법제화해서 실효성을 갖추어야 한다.

5. 결 론

4차 산업혁명은 지능화 혁명을 기반으로 '경제·사회 구조적 과제'의 해결이 가능한 혁신성장의 새로운 모멘텀으로 주목받고 있다. 이러한 4차 산업혁명 기술의 업무적용을 위해 각 기능별 실제 데이터 축적·활용이 매우 중요한 시점이다. 이를 위해 핵심 데이터 관리 생태계 환경을 구축하고 역동적인 국방적용 활성화 기반조성을 위해 본 연구를 진행하였다. 본 연구를 통해 국방 분야 데이터 관리에 대한 현 실태를 분석해 보았으며, 국내외 동향분석을 통한 시사점을 도출하고 이를 종합적으로 검토하여 국방 분야 데이터의 전략적 활용을 위한 발전방안을 연구하였다.

국방 분야는 현실적으로 국가보안이라는 치명적 위협에 의해 데이터에 대한 개방 및 공유가 제한되는 독특한 문화를 가지고 있으며, 이에 따라 데이터의 가시성 부족과 데이터 활용측면에서 활성화가 부족하며, 데이터의 품질과 표준화도 타 부처에 비해 미흡하여 활용에 제약사항이 많다. 또한 이러한 데이터를 활용하여 4차 산업혁명의 핵심인 빅데이터/AI를 접목하는데 많은 어려움을 겪고 있는 현실이다.

'데이터 중심'의 선진 국방경영 및 업무혁신과 군 전력증강을 위 국방 데이터 관리를 위한 4가지

추진방향을 다음과 같이 제시하였다. 첫째로 국방부 정보화기획관실이 국방 데이터 업무에 관한 컨트롤 타워 역할을 수행하면서 활용 활성화 여건을 조성할 수 있도록, 정책과 제도를 개선해 나가야 한다. 둘째로 국방의 특수한 상황을 고려한 국방 데이터 관리 생태계(기반환경 및 협력체계)를 구축하여 데이터의 생성, 공유, 유통, 융합 등이 활발히 이루어지고 관련 기술을 발전시켜 나갈 수 있도록 환경을 조성해야 한다. 셋째로, 이러한 데이터를 활용하여 새로운 가치 창출을 위하여 국방분야 빅데이터 및 AI의 전략적 추진을 위한 단계별 발전방향을 제시하였고 마지막으로 국방 데이터의 보안 강화 방안을 통해 보다 안정되고 신뢰성이 확보된 환경에서 데이터를 활용할 수 있는 여건조성방안을 제시하였다.

국방 데이터를 활용한 지능화된 국방정보화 환경구축과 및 무기체계 발전을 위해 국방 내외부의 다양한 데이터를 수집, 통합, 유통, 융합/분석하여 국방경영 효율화와 경쟁력 강화, 전력증강을 통한 작전 수행능력 제고 등을 위해 지속적으로 발전시켜나가야 함은 물론 이를 위한 투자와 노력을 전사적으로 투자하여 국방 데이터의 활용성이 증대되기를 기대한다.

참고문헌

[1] 국방 공공데이터 품질평가결과(19년), 국방부 내부 행정자료, 2019.

[2] 국방부 훈령 제 2223호, 국방 공공데이터제공 훈령, 국방부, 2018.

[3] 김민주, “지능형 지속 위협 사례 분석을 통한 보안 요구사항 추천 프레임워크”, 아주대학교 대학원 2019.

[4] 김서안. “데이터 3법 개정의 의미와 추후 과제”, 융합보안논문지, 20(2), pp. 59-68. 2020.3.

[5] 김세용, 권혁진, 최민우, “국방분야블록체인 및 인공지능 융합방안연구”, 인터넷정보학회논문지. Vol. 21 No. 2 pg. 81-91, 2020.

[6] 김태욱, “데이터3법 통과…의료·AI 등 산업 탄력 전망”, KISO저널 (38), pp. 25-29, 2020.3.

[7] “데이터·AI경제 활성화 계획(‘19~’23년)”, 관계부처 합동, 2019. 1.16.

[8] 데이터스트림즈, “ICT 신기술활용 국방 데이터 거버넌스 체계 구축방안” 국방부 소개자료, 2018.12.3.

[9] 박영철 외 7명, “사이버보안체계 강화를 위한 정보보호법제 비교법 연구”, 한국인터넷진흥원 연구보고서, pp263, 2015.

[10] 신우택, 이진희, 김정우, 신동선, “국방 빅데이터/인공지능 활성화를 위한 다중메타데이터 저장소 관리시스템(MRMM) 기술 연구”, 인터넷정보학회논문지. Vol. 21 No. 1, pp.169-179, 2020.

[11] 여성철, 문종섭, “국방정보체계의 비밀데이터 관리 방안 연구”, 정보보호학회 논문지, 24(6), pp 1285-1292, 2014.

[12] 육군본부, 육군기본정책서 ´19 ~ ´33, 2018.

[13] 한국판 뉴딜 종합계획, 관계부처합동, 2020.07.14.

[14] 한눈에 보는 데이터 3법-대한민국 정책브리핑, 대한민국정부, 2020.

[15] 황선웅, ″4차 산업혁명 시대의 국방 데이터 전략과 구현방안″, 국방정책연구, vol. 124, pp.61-93, 2019.

[16] A. Cavoukian, J. Polonetsky, and C. Wolf, ″SmartPrivacy for the Smart Grid: Embedding Privacy in the Design of Electricity Conservation″, The Future of Privacy Forum, 2009(11).

[17] Defense Innovation Board, “DIB Recommendation”, 2017.

[18] DoD Digital Modernization Strategy, DoD, 2019.

[19] DoD Net-Centric Data Strategy, DoD, 2013.

〔저자소개〕

김 세 용 (Seyong Kim)
2001년 3월 육군사관학교 핵화학학사
2009년 1월 국방대학교 운영분석 석사
2020년 8월 충남대학교 경영학박사수료
2014년 12월 국방부 국방통계담당
2019년 2월 ~ 현재 국방부 국방 빅데이터/인공지능정책담당
Email : seyong58@naver.com

김 준 상 (Junsang Kim)
2003년 1월 한양대 컴퓨터공학 학사
2005년 1월 한양대 컴퓨터공학과 석사
2017년 1월 한양대 컴퓨터공학과 박사
2008년 ~ 2012년 : 해군사관학교 컴퓨터학과 전임강사
현 재: 국방부 정보화기획관실 전산사무관
Email : kjspbe@korea.kr

강 석 원 (Seokwon Kang)
2002년 2월 육군사관학교 전자공학과학사
2010년 2월 아주대학교 NCW공학과 석사
2015년 ~ 2016년 육군 3사관학교 컴퓨터공학과 조교수
2018년 ~ 현재 육군 시험평가단 위성/통신체계 시험평가장교
email : note3857@hanmail.net