

국방 블록체인 기술 동향 및 국방 ICT 융합 전략 연구

Study on Trends and Strategies for Defense Blockchain and ICT Technologies

이경휴 (K.Hyu Lee, khyulee@etri.re.kr)

국방ICT 융합연구실 책임연구원

박혜숙 (H.Sook Park, parkhs@etri.re.kr)

국방ICT 융합연구실 책임연구원

ABSTRACT

To keep pace with other powerful nations in this era of the era of digitalization and to emerge stronger in the world, the defense forces of South Korea aim to innovate and prepare themselves for digital battlefields of possible wars in the future. The resources in the defense sector, which is the core of defense intelligence, is based on an intelligent mission collaboration tactical network system via cyber, command, control, communication, and computer (C4), and military and non-human weapons. Defense intelligence depends on the degree of the convergence of advanced Information and communication technologies (ICTs). Considering this aspect of defense intelligence, We plan to determine the application status of defense blockchain technology and examine the feasibility of applying blockchain technology and the core of applied technology. Generally, a key feature of blockchain technology is its data integrity in untrusted environments. There are various types of core technologies for the blockchain depending on the target areas of application in the defense sector, and it is also essential to derive new application strategies for core technologies that are applied in combination with other ICT technologies. We plan to demonstrate new defense ICT converged technologies (DNAB2: Data, Network, AI, BigData, Blockchain) and DNAB2-As-Services in the defense strategy.

KEYWORDS 국방 블록체인, 국방 전술 망, 전장사물인터넷, 국방 로지스틱, 국방 ICT 융합

1. 서론

국방 영역에서 미래전은 디지털 전장으로 전환을 누가 얼마만큼 신속한 혁신에 입각하여 실행함

에 따라 국력의 향방을 가늠하는 시대에 본격 접어들었다. 국방 영역에서 강력한 국방 정보체계에 의한 최첨단의 사이버 전장 구축, C4(Command, Control, Communication, Computer), 군인을 포함

* DOI: <https://doi.org/10.22648/ETRI.2020.J.350102>

* 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단 정보통신기획평가원의 지원을 받아 수행된 연구임[방송통신산업기술개발사업-다매체 다중경로 적응적 네트워크 기술 개발].



한 각종 유무인체 무기화에 의한 지능적인 임무 협업 전술 망 체계 등이 국방 지능화에 핵심 대상이다.

국방 지능화는 결국 첨단 ICT 기술이 융합되는 정도에 따라 좌우되는 현실이다. 이런 국방의 주류에 편승하여 국방 블록체인 기술의 적용 현황을 파악하고, 블록체인 기술의 적용 타당성과 적용 기술 핵심을 파악하고자 한다.

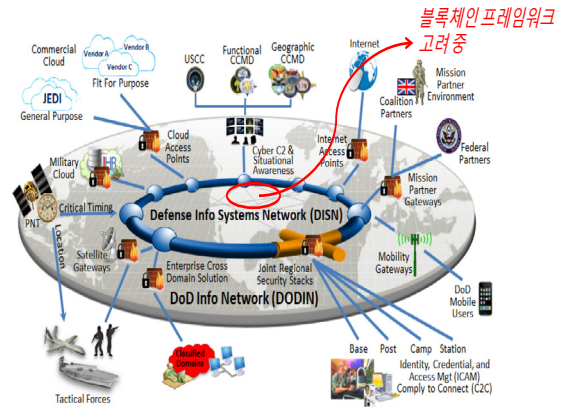
일반 영역과 마찬가지로 블록체인 기술의 핵심 기능은 신뢰할 수 없는 환경에서의 신뢰 수준을 고도화하는 데이터 무결성이다. 국방 영역에서 적용되는 분야에 따라 블록체인 핵심 기술의 종류도 다양하고, 타 ICT 기술과 융합되어 적용되는 새로운 핵심 기술 적용 전략 도출도 매우 중요하므로 한국 국방이 경쟁력을 가지는 분야에 국방 로지스틱에 의한 국방 ICT*DNAB2 접근 전략을 제시하고자 한다.

II. 국방 블록체인 기술 동향

1. 국방 블록체인 정책 국외 동향

2019년 발표된 미국 ‘국방 디지털 현대화 전략’ 프레임워크 전략은 그림 1과 같다. 블록체인을 통한 통신부문의 개선 전략 계획을 포함하고, 미 DARPA(미국 국방 고급 연구 프로젝트 기관)를 통해 블록체인 기반의 해킹 불가능한 안전한 메시징 플랫폼 개발에 관한 실험연구를 진행하도록 적극 지원 중이다[1].

이와 관련된 중요 정책은 (1) 국방 디지털 현대화는 사이버보안, C3(명령/제어/통신), 인공지능, 클라우드 기술 정책을 국방CIO로 선정, (2) 전략 목표는 국방 경쟁력 강화, 국방 효율화 능력 강화, 사이버보안 증진, 디지털 전장 강화이며, 모든 DoD의 정보 자원 관리에 적용, (3) 국방 블록체인



출처 미국국방부의 “DoD DIGITAL MODERNIZATION STRATEGY,” DoD Office of Prepublication and Security Review, 2019.7.12.

그림 1 미국 DoD의 CIO 국방연합정보 환경 프레임워크 추진도

의 역할은 사이버보안과 국방암호화 정책에서 블록체인 네트워킹 특징인 고 신뢰, 보안투명성, 고장 허용성 세 가지 특성을 국방에 최대한 활용, (4) 국방 블록체인 네트워크는 사이버 공격으로부터 손상 가능성 해소와 더불어 막대한 비용 절감을 위해 이 분야에 최우선으로 하는 정책을 실행, (5) 모든 국방 전술상에 연계된 유무인체들의 ‘연합정보화 환경 프레임워크’ 정책으로 이들 요소들의 생산 단계부터 반영, 자율적 연합동작 능력 인프라 포트폴리오를 그림 1과 같이 추진 중이다.

국외 국방 블록체인 기술 적용 정책 및 연구 분야 등은 표 1과 같이 분야별로 구분하여 제시한다.

2. 국방 “블록체인” 분야별 적용 분석

대부분 선진국가의 국방은 인구 감소로 인하여 군사 인적 자원이 감소하고 국방예산 또한 감소 추세이다. 이를 고려하여 미래 국방은 최첨단화 도입으로 인적 자원에 의존하기보다 최첨단 무기체와 인공지능에 의존하여 사이버 전쟁에 대비하기 위해 군사 통제권을 준비 중이다. 국방 방위 부문이

표 1 국방 블록체인 국외 동향표

국가/기관/분야	내용
[미국방부-전체] 연합정보화환경프레임워크(사이버보안)[1]	-“미국 국방 디지털 현대화 전략” 국방 정보 자원의 관리 전략 계획인 “PLAN FY19-23” 2019년 7월 정책 수립 공포(블록체인활용 정책 포함) -모든 국방 전술상에 연계된 유무인체들의 “연합정보화 환경 프레임워크” 정책으로 이들 요소들의 생산단계부터 반영, 자율적 연합동작 능력 인프라 포트폴리오 추구 중
[미국방부-총괄] [3]	-미국 트럼프 대통령은 “블록체인을 사이버보안 등 군대 적용 연구비 승인 문서(Military Spending Bill)”에 사인(약 1.1 billion/년) -블록체인의 7대 활용분야 선정 (1) 사이버공격, (2) 무기체계 제조 개발, (3) 전장 신뢰 보장, (4) 정부 보호, (5) 국방물류/계약, (6) 무기체 보호, (7) NATO 응용
[미국방부] 사이버 공격[1,15,16]	-사이버 공격 분야를 확대, 초연결되는 상황을 고려하여 파워 공급 네트워크, 컴퓨터, 유무선 이동 무기체를 연결하는 모든 상황에 예상되는 사이버 공격에 대비한 강력한 보안 및 신뢰 수단인 블록체인 적용
[미국-NATO-DARPA] 무기체계 보호[4,6]	-모든 유무선 이동 무기체계를 보호하고 강화하는 분야 NATO의 경우는 ‘Navy’s Aegis Combat System’에 블록체인을 이용하여 네트워크 분산화 정책을 조속히 적용 예정 -블록체인 기반의 무기체계 모니터링시스템 개발을 위한 방위 산업체와 파트너십 발기
[미국방부-해군] 블록체인 전함[4]	-‘블록체인 전함’이라는 명명하에 분산 네트워크를 사용 -‘이지스함’을 제어하고, 분산 노드들이 동일한 Data Set에서 작동하도록 하는 미래의 전함 제어를 준비
[NATO-국방] 연합 미션 네트워크[5,14]	-국방분야 신뢰 관리에 정책과 표준으로 블록체인 적합성에 대한 정책 검증을 실시 중 -NATO는 FMN(Federated Mission Networking) 환경에서 데이터 및 네트워크에 블록체인 도입 전략화 중 -연합 군사작전에 블록체인 기반으로 분산 원장을 활용하는 신뢰 보안용 작전 명령 적용 표준화 협정(STANAG 4778) 비준 절차 중
[EU-EDA] 군 통신 데이터 무결성[6]	-EDA(European Defence Agency)하에 블록체인 기술을 도입하여 Peer-to-Peer 통신과 데이터의 확산성 및 무결성을 위한 연구 정책 진행 중 -2019년에는 국방용 IoT 네트워크, 사이버 국방, 보안 메시징 등 블록체인 기반의 새로운 국방 응용 서비스 정책을 도입할 예정
[미국-DARPA] 메시지시스템[7]	-2016년에 미국 DARPA에서 “블록체인 메시지 시스템”을 연구하여 2017년에 ITAMCO사가 전송 및 수신 방식에서 메시지 생성을 분리하는 해킹 방지 메시징 및 트랜잭션 플랫폼 앱을 개발함
[미국방부] 전장 IoT[8]	-전장사물인터넷(IoBT: Internet-of-Battlefield Things)을 센서, 무기, 이동형 무기체, 로봇 그리고 각종 웨어러블 디바이스(센싱, 통신, 액터 등)들이 군대와 협업하기 위한 블록체인 협동 강화 시스템 연구 개발 중 -전체적으로, 위성 통신을 활용 지상 무기 이동체와 아주 밀접하게 협업하는 블록체인 기반 전장 플랫폼
[미국방부] 적층가공(AM: Additive Manufacturing)[9]	-적층가공(AM)은 3D 인쇄 군사 용어. 미군은 AM 방식을 사용하여 무기와 차량을 위한 프로토타입과 부품을 제작. 1년 전 미 해군은 단 4주 만에 전체 잠수정을 3D로 인쇄 -미 해군은 블록체인이 AM 프로세스에 가져올 수 있는 잠재력 존재 인식. 2017년 이래 AM 사업의 각 단계 내에서 블록체인을 통합하기 위해 노력. 이러한 방식으로 분산 네트워크를 사용하면 디지털 스레드의 요구 사항을 충족. 이론적으로 무제한의 안전한 데이터 저장소를 제공. 또한 네트워크의 노드를 사용하여 전체 AM 프로세스에서 데이터를 공유 -블록체인은 또한 앞으로 다가올 AM을 일반적인 제조 공급 체인에 광범위하게 채택할 수 있는 원동력

(계속)

표 1 국방 블록체인 국외 동향표

국가/기관/분야	내용
[캐나다-국방과학연구소] 국방 전술 망[2]	-국방 전술 망에서 블록체인 활용 전략 연구를 수행 중 -블록체인의 활용 차원에서 무결성, 자원 관리(네트워크 관리, 정책 관리, 전파 분배)를 기반으로 블록체인 기술 종합 적용 마스터 플랜을 연구 중 -"Tactical Clusters" 분야는 군인이 미래 착용하는 웨어러블 장치들을 군인 개별 군집 단위로 고려하여, 군집 정보 전송을 블록체인 레이어별(TRANSACTION, BLOCK, CONSENSUS, CHAIN)로 정립해가는 연구 전략 존재
[인도-국방연구소]군사 운영[10]	-국방 운영시스템에 블록체인 적용으로 네트워크 생존성을 향상하기 위한 연구 중 -인도 국방 전장 NEMO(Network Enabled Military Operations) 모델에 블록체인 적용, 전장의 3가지(자원, 통신채널, 데이터) 측면 고신뢰화 추구
SupplyBlockchain (미국회사)[11]	-NATO MapN에 의해 협약된 군 의무훈련인 "Vigorous Warrior 19"에 블록체인 SW를 공급 -Vigorous Warrior 19는 NATO의 가장 큰 의무관련 훈련이며 39개국 2,500명 이상이 참여하고, 1,000여 개의 시나리오, 300개의 의무조치, 1,500개의 재난상황이 시뮬레이션됨 -의약품의 추적, 글로벌적 위조 약품에 의한 피해 감소, 음식의 출처, 인도주의적 원조의 투명성 확보를 위해 사용됨
PENTOZ[12]	-Blockchain Military Applications의 한 영역으로 AI-enabled Drones의 데이터를 블록체인으로 관리하여 비행내용과 수행행동을 기록 -해군의 타격시스템(미사일, 레이더, 군함 등)은 하나의 복합적인 시스템 구성체이므로 위협에 대응하기 위한 분산화된 블록체인 필요성 제기 -Additive Manufacturing(AM)은 3D 프린팅 용어이며 이와 관련한 데이터에 대한 안전한 보관에 블록체인 활용 필요

더 이상 뒤지지 않도록 보장하기 위해 모든 형태의 필드 레벨링 기술도 채택하는 경향이다. 이는 필수적인 ICT 첨단 기술을 융합에 기반을 두고 추진 중이다.

이 대안 중 하나가 '블록체인'이다. 블록체인이 아직은 완전한 대안 기술로 제시될 상황은 아니지만, 군대 공급 망, 사이버보안 및 현장 내 통신뿐만 아니라 지사 간 통신은 블록체인 기술의 장점을 얻을 수 있다고 보고 있다. 세계가 최첨단에 있고 군사 인력이 쇠퇴하고 있는 현실에서 사이버 전쟁 측면에서는 블록체인을 방어 목적으로 적용할 수 있는 것에 지대한 가치를 부여하고 있다[3].

가. 국방 물류/계약 추적 분야: 국방 물류 신뢰 구축

일반 산업에서 물류 공급 망은 손실, 낭비 및 사기를 줄임으로써 수익성을 유지하는 데 중요하

다. 방위 산업에서는 스테이크홀더의 몫이 항상 높기 때문에 공급 망 보안을 유지하는 것이 더 중요하다.

모든 국가의 국민은 군대를 지원해야 한다는 데 동의할 수 있지만, 방위 산업은 재정 손실과 낭비 보다는 현실에서 비 신뢰 공급 망으로 인한 누수 현상이 가장 큰 문제이다. 미국 국방부는 아프가니스탄 관련 지출에서 낭비되고 잘못 안내된 지출 비용이 총 170억 달러라고 추정하였다[3]. 민간인과 정치인이 군사 업무와 지출에 대해 얼마나 많은 감독을 할 수 있는지에 대한 제한이 있지만, 이러한 기금이 어디로 가고 있으며 어떻게 사용되는지에 투명해야 한다. 재정 책임을 제외하고, 군대는 단순히 가장 진보된 안전한 공급 망 관리 도구를 갖추어야 하며, 이 도구 중 하나가 블록체인 기술이다.

국내외 국방 활성화에 필수적인 무기, 장비 및 기타 아이템을 효과적으로 추적할 수 있어야 한다. 국방 공급 기업은 블록체인으로 최첨단 공급망 감독 플랫폼에 소속되어야 하며, 이는 가장 중요한 국방 공급망 신뢰 구축에 혁신이 될 것이다.

나. 정부 및 전장 메시지 보안

미국 상원 의원은 국방 E-메일 사용에서 견고한 암호화를 도입하지 않고 있다는 지적하고 있다[3]. 결과적으로 미국 국방에서 E-메일의 85%만을 암호화 대상으로 적용하고, 나머지 15%는 보안 위협에 노출되어, 이를 지능형 사이버보안 기술로 위협 노출 15%를 해결해야 한다고 보고 있다[3]. 블록체인 암호화 기술을 통해 자동화 수단을 추가하여 전자 메일뿐만 아니라 다른 형태의 기관 간 및 현장 통신에 대한 감독 비용을 블록체인 기술로 줄일 수 있다고 본다.

다. 사이버 전쟁 시대 준비

단순히 영리 목적의 사이버 공격과 전쟁 행위의 사이버 공격 사이의 경계선은 매우 근접하다. 둘 중 하나에 대한 예방 조치를 취하는 것이 중요하지만 사이버 전쟁 행위가 기업에 대한 랜섬웨어 침입보다 더 어려운 문제이다. 미국 연방 정부는 2018년에 61,000건의 사이버 공격을 받았으며, 각각의 위협 수준은 다양하다[3].

상호 연결된 그리드 컴퓨팅에 의존하는 미국 에너지 부문이 치명적인 사이버 공격에 가장 취약한 지점이라는 견해이다. 에너지 산업은 2014년 해커가 가장 많이 목표로 삼았으며, 79건의 사건이 기록되었다. 이러한 공격의 약 55%는 APT(Advanced Persistent Threats)에 의해 수행되었으며, 이는 아주 정교한 해커이다[3].

블록체인이 모든 것을 막을 수 있는 솔루션은 아

니지만 중앙 집중식 장에 지점보다 보안 인프라에서 분산 방식으로 중앙 집중식 폐해를 해결하는 실마리로 적용할 수 있다. 각종 전력망, 컴퓨터 시스템 또는 잠재적으로 취약한 다른 네트워크를 사이버 침입으로부터 보호하는 것을 막론하고 사이버 위협에 대한 포괄적인 방어 수단을 만드는 것이 방위 산업의 최우선 과제 중 하나이다.

라. 군대용 제조 개선

2018년 9월 미군이 3D 인쇄 기술을 사용하여 현장 콘크리트 막사를 건설하기 시작하였다. USMCSC(US Marine Corps Shipments Command)는 현재 '세계에서 가장 큰 3D 프린터'를 활용하여 40평방피트의 프로토타입을 40시간 만에 완성하였다. 적층 제조의 한계와 이점을 테스트한 것이다. 2017년 7월 해병대는 자사의 Big Area Additive Manufacturing 기계를 사용하여 최초의 3D 인쇄 잠수함 선체를 인쇄하였다. 같은 해 6월, 그들은 적층 제조를 사용하여 니블러 드론을 성공적으로 만들 수 있었다. 지난 4월 육군은 수류탄 발사기, 방탄복, 군용 식사 주문 제작 등 3D 프린팅 기술에 대한 더 많은 응용 프로그램을 선보였다. 미국 방위 산업은 3D 프린팅 기술을 채택한 것이 분명하다. 문제는 블록체인 기술로 프로세스를 어떻게 더 향상시킬 수 있을까 하는 측면에서 고려 중이다.

블록체인이 데이터를 보다 안전한 전송 도구의 역할을 할 수 있는 것처럼 독점적인 적층 제조 청사진 및 디자인은 중앙에 저장되는 것이 아니라 분산된 개인 블록체인에서 공유될 수 있는 환경으로 혁신하는 것이다. 블록체인 기술이 발전하고 가능성이 실현됨에 따라 군대는 블록체인 기술과 새로운 제조 도구에 대한 의존성을 결합하는 대체 방법을 찾고 있다.

마. NATO Applications: Military, Logistics, Finance

2016 NCI 챌린지의 일환으로 혁신가들은 NATO 회원들 협력을 가능하게 하는 ‘블록체인의 군사적 적용’ 범주의 아이디어를 공유하도록 장려하고 있다. NATO는 DARPA와 함께 블록체인 솔루션을 구현하여 북대서양 조약기구 회원을 지원하겠다는 의사를 발표하였다. 유럽과 북미에 걸쳐 29개의 회원국이 있으므로 회원국 간의 커뮤니케이션은 미국과 대서양의 국경을 넘어 진행 중이다.

1949년에 설립된 NATO 협정은 2024년까지 동

맹국이 GDP의 2%를 국방 지출에 투자할 것임을 2014년 합의에 의하여 입증되는 것처럼 지속 발전하고 있다[3]. 특히 테러와의 싸움에 더 잘 맞고, 게다가 방어 측면에서 공정한 분담을 구현하는 방법에 중점을 두고 있다. NATO 블록체인 애플리케이션을 위한 제안에는 회원과 원조 수령인 사이의 지불 및 상품 전송 능률화 및 면밀한 추적, 안전한 방식으로 군 물류 분산, 쉽게 접근 가능하고 조작 방지 및 안전한 방식으로 회원 간의 정보 공유 등 표 2와 같은 서비스이다.

NATO 국방은 미국 DARPA와 협력하여 2016년 10월 처음으로 군대에 블록체인을 사용하겠다고 발표하였다[18]. NATO의 블록체인 기술 개발을 별도로 분석할 필요가 있는데, 이 기구가 국가 협력 기구이므로 신뢰 있는 협업 환경 구축이 필수라는 점을 들어 체계적으로 기술개발 구축과 블록체인 기술의 신속한 현장 적응력이 높은 점에서 주목할 만하다. 표 2에서 FMN(협의임무) 블록체인 기술은 국방의 C4SIR 체계에 따른 블록체인 기술의 적응도와 타당성, 그리고 협력 연구개발 체계까지도 정형적으로 접근하고 있어 주목할 만하다.

표 2 국방 블록체인 NATO 동향

국가/기관/분야	내용
NATO FMN Initiative [13]	-FMN은 NATO 국가 간 연합작전체계 능력 확보를 목적으로 C4SIR 체계, 의사결정, 지능화, 생존성, 호환성 문제의 해결을 위해 구성된 NATO의 이니셔티브 조직으로서 현재 NATO 혁신의 가장 중요한 역할을 담당 -FMN의 구축과 관련하여 블록체인 활용에 대한 연구들이 NATO Agency를 주축으로 활발히 수행 중
NATO NCI Agency [5]	-NATO 동맹국간의 정보체계 호환성을 설계하기 위한 노력의 일환으로 NATO 국가간에 개발된 표준인 STANAG(Standard Agreement) 4774, 4778을 블록체인으로 구현하기 위한 연구 및 계획 중 -STANAG 4774: 정보의 기밀성을 표현하기 위한 레이블 기호 -STANAG 4778: 정보의 메타데이터 바인딩 메커니즘
NATO NCI Agency [14,15]	-NATO 에이전시들 및 산학연 합동으로 NATO FMN의 혁신을 위한 29개의 팀을 구성하고 해커톤 실시, 보고서 발행 -NCI 에이전시를 중심으로 NATO 코어 서비스와 기술적 채팅(Jchat), GIS를 지원하기 위한 분산파일저장 방법으로 InterPlanetary File System(IPFS) 프로토콜과 연계하여 블록체인을 이용 -주소 기반 콘텐츠, 버전관리, P2P 파일시스템과 Merkle DAG, 자체인증 이름공간(Self-certifying namespace)을 사용하여 분산파일시스템과 블록체인을 연계하고 있음

바. 데이터 도난방지, 국제 공급망 보호

세계 최대의 힘은 모두 블록체인 기술을 구현하기 위해 경쟁하고 있으며, “외부 위협에 대한 방어보다 군사 응용 프로그램에 더 명확한 유스 케이스는 없다”라고 보고 있다. 가장 정교한 디지털 무기를 보유한 국가인 미국/중국/러시아 등은 ‘디지털 봉쇄’ 수단으로 블록체인을 사용하는 방법을 찾기 위해 무기 경쟁의 한가운데에 있다.

미국 국방부는 사이버 공격으로부터 320만 명의 글로벌 네트워크를 보호할 책임이 있다고 한다. 특히, 민감한 정보가 담긴 방대한 저장소와 정보의 대량 캐시 도난 가능성에 할당된 ‘테라바이트의 사

망'을 보호해야 한다고 한다. 전 세계의 국방은 방어 게임을 할 때 이용할 수 있는 모든 도움을 이용할 수 있다. 군대는 정기적으로 국제 공급 망을 활용한다. 글로벌 정보 공유는 국방의 최상의 정보 전략을 확보하면서 각국의 국방비용을 절감하는데 필요하다[3].

미래 디지털 시대는 중요한 인프라, 특정 거래 또는 국제 군사 작전을 지배하는 원장의 공격을 통해 필수 국제 군사 공급망의 중단을 시도하는 새로운 종류의 위협에 직면하고 있다. 군대는 블록체인 기술이 군사 거래 및 공급 망과 관련된 기록을 교란, 획득 또는 근절하기 위한 침투 시도를 효과적으로 탐지하고 차단할 수 있는 방법을 실험 중이며, 이를 추진 중이다.

사. 무기 시스템 보호 및 완성

군사 위협과 공격적인 캠페인이 점점 디지털화되고 있으며, 많은 사람들이 전 세계에서 제공하는 가장 진보된 컴퓨터 뒤에 배치된 기술을 구상하고 외부 공격을 탐지하고 공격자에 대한 공격을 시작한다.

미 해군의 이지스(Aegis) 전투 시스템은 군대의 디지털화와 전통적인 무기를 결합 중이다. Aegis의 기본 컴퓨팅 및 레이더 기능의 무결성을 유지하는 것은 Aegis의 청사진이 적군의 손에 닿지 않도록 해야 할 뿐만 아니라 본연의 기능 발휘에도 중요하다. '블록체인 전환[17]'은 이지스 전투 시스템을 운영하는 데 필요한 데이터를 분산시키고, 모든 컴퓨터 종속 시스템과 마찬가지로 이지스 시스템의 중앙 집중식 특성으로 인한 해킹 위협에서 탈피시키는 방식을 적용하는 것이 핵심이다[3,4].

국방 블록체인 기술은 본연의 블록체인 장점만을 고려하여 국방에 적용하는 동향이 다각도로 존재하지만, 국방이라는 보안특성으로 핵심기술 실

현 및 실증이라는 측면에서 개방되지 않고 있고 대부분 프로젝트는 계획이거나 설계 단계인 것으로 파악된다. 국방 영역에서 산재해 있는 미래 지향적 해결점은 블록체인 기술 개념과 우선은 일치하고 있다. 그 사례와 논술적 타당성은 지금까지 사례 분석에서 추론이 가능하다.

국방 영역은 방대한 자원들이 존재하며, 앞으로 미래에 나올 군사 웨어러블 자원들까지 예상하면 연결통신의 한계성, 모든 군사자원의 관리의 한계성, 특히 전장에 동적 자원의 한계성으로 인하여 신뢰 인프라 구축(블록체인/초저지연 연결), 자원들이 최대한 합의능력을 발산하기 위한 지능화 추구(인공지능/빅데이터), 전술적인 상황에 모든 정보의 실감인식(데이터/미디어/로봇인식) 등이 반드시 필요하다. 본고는 블록체인 기술 동향에 중점이므로 다음 장에서는 국방 전술 망 측면에서 블록체인 기술 특징과 고려 사항을 제시하고자 한다.

III. 국방 전술 망과 블록체인 기술

1. 국방 블록체인 기술 특징

블록체인 기술은 경제 산업의 여러 부문에 적용될 수 있는 특징이 주류이다. 그러므로 블록체인 기술의 적용은 산업 물류 분야에서 적용된다. '식품 공급 신뢰 분야'에서 블록체인의 분산 원장을 사용한다. 식품이 이동하지 않고 공급 망을 통해 이동함에 따라 식품 공급원 물류에 대한 신뢰 정보를 저장하고, 사용자가 스마트 계약 거래의 일부로 소스코드를 제출한다. 그리고 네트워크를 통해 모든 피어(Peer)에게 전파된다. 블록체인을 가상머신과 페어링함으로써 사용자 소스코드는 네트워크의 모든 노드에서 액세스하고 실행하여 분산된 '세계 컴퓨터'를 만든다[19].

산업 부문에서의 지속적인 연구 개발은 국방 방

위 산업으로 확산되고 있다. 국방 과제를 해결하기 위해 블록체인 기술을 적용하려는 개발 노력은 그만큼 안전하고 기밀이 보장되는 고 가용성 데이터 조정 및 협업 메커니즘 블록체인으로서 군사 작전의 적용 가능성에 최근 연구가 급속 진전되고 있다.

군사 네트워크에서의 안전하고 신뢰할 수 있는 진정한 전술 커뮤니케이션을 위한 블록체인의 실행 가능성이 이기종 컴퓨팅 및 감지 플랫폼에서 신뢰, 개인 정보 보호 및 보안을 가능하게 하는 블록체인 기술이 전장의 현대화를 촉진하고 있다.

이 새로운 기술에 대한 연구와 군대에 대한 잠재적인 응용에 대한 연구가 확실히 필요하지만 분산 명령/제어 및 자율적인 기동을 가능하게 하는 기술이 사용될 방어 네트워크 및 컴퓨팅 환경의 한계를 극복해야 하는 과제이다.

2. 전술 망 블록체인 기술 특징

전술 네트워크에서는 일반적인 인터넷 연결이 군사 작전 중에 사용되는 네트워크는 특성화되어야 한다. 네트워크상에 간섭 및 방해, 간헐 현상 및 저 대역폭(DIL: Disconnected, Intermittent, Limited bandwidth) 조건 및 환경을 극복해야 한다. 전술 작전의 본질은 역동적이고 모바일 환경이 지리적으로 분산되어 있으며, 극한의 환경 조건으로 인하여 결과적으로 전술 네트워크 상용성, 특히 성능 면에서 전술 망 블록체인은 전술 공간에서 실행 가능한 시스템을 고려해야 한다[19,20].

전술 망은 모바일 배치 전술로 다양한 네트워킹 장비를 활용한다. 현재 전술 망은 신뢰할 수 있는 인프라 기준이 없으며, 장비는 대부분 고정식인 것이 현실이다. 전술 망은 현재 두 가지 기본 유형을 지니고 있다. (1) 저지연 시간을 제공하지만 이동 환경에서 지상파, 모바일 애드혹으로 형성된 네트

워크(MANET) 시스템, (2) 레디오 단거리 및 매우 간헐적으로 비시선 범위를 제공하는 위성 통신 시스템 등으로 구성된다.

전술 망 기술은 네트워크 안전성보다 더 고려해야 하고, 매우 높은 대기 시간을 갖는 이기종 네트워킹 환경으로 저 대역폭 DIL은 일반적인 상업용 인터넷은 광섬유 연결로 연결된 엔터프라이즈 네트워크와 비슷하다. 사용자에게 고속, 저 지연, 안정적인 통신을 제공해야 한다.

전술 네트워크와 셀룰러를 포함한 상용 인터넷 사이에는 몇 가지 주요 차이점이 있다. (1) 전술 네트워크는 멀티 홉, MANET이며 인터넷은 광통신을 통해 연결된 엔터프라이즈 네트워크, (2) 인터넷은 거의 항상 연결되어 있지만 이동성 또는 방해로 인해 전술 네트워크는 분할 가능해야 하며, (3) 전술 네트워크는 경쟁이 심하고 혼잡한 무선 주파수 환경에서 작동하는 반면 셀룰러 및 Wi-Fi 사용자는 공동 작업하여 스펙트럼을 공유, (4) 전술 네트워크는 일반적으로 초당 몇 메가비트(Mbps) 이하의 낮은 데이터 속도를 제공 등이 차이점들이다. 일반 셀룰러 및 Wi-Fi는 최대 수백 Mbps의 데이터 속도와 훨씬 낮은 대기 시간을 제공 등과 같은 차이점을 두고 있다.

전술 망 블록체인 기술에서는 핵심 해결 사항은 (1) 확장성 문제: 전술 네트워크가 블록체인에 의해 생성된 트래픽 요구를 지원할 수 있는 경우에도 트랜잭션/메시지를 다른 모든 노드에 분배할 것인지 또는 해당 독립 전술 그룹 노드에만 분배할 것인지 여부, (2) 파티션 문제: 전술적 네트워크에서 도메인 블록체인을 지원할 수 있는가? 블록체인 기술이 노드 이동 중 파티션으로 인해 포크를 원활하게 병합할 수 있는가? 전술 망 블록체인 기술의 핵심은 확장성 및 파티션을 해결하여 전술 망의 블록체인 적용 성능을 달성하는 것이다.

이는 새로운 전술 망 블록체인 기술을 위한 새로운 네트워크를 개발하면서 블록체인에 의해 생성된 대규모 트래픽 수요를 지원하는 기술, 그리고 다른 하나는 새로운 블록체인을 개발하는 것이다.

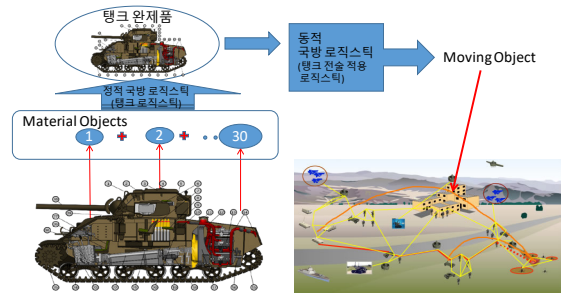
IV. 국방 ICT(DNAB2) 융합화 전략

1. 국방 ICT 융합화 전략

ICT/IoT 신기술의 국방 적용에 저해되는 정책 및 규정상 제한사항을 해소함으로써 향후 ICT/IoT 기술이 국방 전투력 향상에 보다 기여할 수 있는 여건이 확보될 수 있도록 예산을 반영하여야 한다. 신 ICT/IoT 기술을 국방시스템에 적극 적용함으로써 무기/비무기 체계의 효과성/효율성, 보안성, 민첩성, 융통성 증대와 비용절감이 가능하다. 국방사물인터넷(IOBT)은 IoT를 통해 센서와의 연결 부분을 강화함으로써 Sensor-to-Shooter라는 궁극적인 NCW 개념 구현이 보다 쉬워지고 발전된 ICT/IoT 기술의 국방 적용 사례를 통해 수출 및 민수 확대에 기여하고, 궁극적으로 자주국방에 기여할 수 있을 것이다[21].

ETRI는 국방 ICT 융합화 추진을 위한 추진과제를 진행 중이다. 광역 국방 영역 중 일부 영역에서 ICT 적용 실험적 성격이 강한 부분으로 현재 진행 중이며, 체계적인 국방 융합화를 위한 기반 마련으로 국방 지능화의 목표를 준비 중이다[22].

미래 전장의 디지털화를 위한 국방 ICT 융합화 기반은 특정 영역 단위로 접근하는, 즉 융합화 특정 영역을 기반으로 발전하는 체계로 하여 점점 확대하는 방식과 디지털 시대에 신 군통합지휘체계와 신 디지털 무기화로 인한 국방 로지스틱을 정립하면서 ICT 융합화로 진행을 병행해야 하는 환경이 되고 있다. 그러므로 국방 ICT 융합화를 위한 기반 연구가 필요하다. 이런 의미에서 국방 로지스



출처 탱크이미지 Malyszczk [CC BY-SA 3.0(<https://creativecommons.org/licenses/by-sa/3.0/>)] 네트워크중심전 MDMPwizard [CC BY-SA 3.0 (<https://creativecommons.org/licenses/by-sa/3.0/>)]

그림 2 군사용 무기체 탱크의 로지스틱 객체화 모델링

틱스를 위한 접근 전략과 모델링을 새롭게 제시하고자 한다. 물론 국방 블록체인 기술도 이를 기반으로 적용함을 포함한다고 볼 수 있다.

‘국방 로지스틱스’는 하나의 군사용 무기체와 같은 개발을 위하여 여기에 소요되는 재료 공급, 즉 생산부터 군사가 직접 사용하는 성능을 내기까지의 전 과정을 품질관리하는 과정이라 볼 수 있다. 이런 군사용 자원 하나하나가 통합되어 수용하는 군사용 집합체(탱크, 전투기, 함정 등)의 견고성과 성능을 반영하게 된다.

이런 국방 로지스틱은 ICT의 첨단 기술 융합 없이는 국방 현대화/지능화를 달성할 수 없다. 국방 로지스틱스는 그림 2와 같이 특정 무기체 탱크를 적용하여, 두 가지 측면에서 분류하여 접근 전략을 제시한다. 하나는 정적인 측면과 동적인 측면에서 역할이다.

‘정적 국방 로지스틱’은 군사용 재원이 공급되어 특정 배치 및 구축되는 과정이며, 그림 2에서 장갑차가 전장에 공급되기 전 단계, ‘동적 국방 로지스틱’은 군사력을 발휘하는 상황, 즉 전술 및 작전상에서 군사용 재원이 사용되는 상황으로 그림 2에서 탱크가 전술 망에 연결 공급되고 NCW 기반으로 다른 무기체와 연합 동작되는 것을 말한다.

두 분류 모두 ICT 융합화는 필수적이고 영향이 지대하다.

ICT 융합화 측면에서 두 가지 국방 로지스틱상 정보화 기술(DNAB2)은 필수이다. 실례로 앞서 언급한 ‘블록체인 전함[17]’의 경우 본 전함의 생성과 군사 현장에서 작전 수행까지 최첨단 현대화를 위해 ICT 융합화 접근 전략을 갖추도록 해야 한다.

2. 국방 ICT*DNAB2 융합화 모델링

국방 ICT 융합화를 위한 일반 모델링, 즉 프레임워크 기반 모델링을 제시한다. 국방의 전체 로지스틱 대상을 보는 시각을 다음과 같이 객체화하는 개념이다.

- 모든 군사 자원(군인까지 포함)이 객체 정보화 인식이 가능하게(IoT, 센서 등) 해야 한다.
- 객체 정보화가 집합을 위한 네트워킹, 정보 교환을 위한 네트워킹이 되어야 한다.
- 운용상에서 모든 국방 로지스틱스는 하나의 유기체로 동작할 준비가 되어야 한다.

미래 국방의 패러다임은 정보화 및 지능화가 필수 조건이 되고 방어 및 공격도 대등하게 정보화 및 지능화 추세로 가면서 전장의 조건은 네트워크 중심전(NCW)에 기반을 두고 추진하게 된다.

그러나 이는 사후적인 전장의 상황만을 인식하여 접근하는 방식이다. 더 근본적인 접근은 국방의 모든 자원은 제조 물류 공급 망부터 정보화 및 지능화 체계를 고려하여 접근해야 한다.

국방에 대한 ICT 융합화 접근은 국방의 모든 필요한 자원을 제조하고 공급하는 과정부터 시작된다. 국방 ICT 적용에 따른 국방 지능화를 목표 ICT 융합화 과정을 전략적이고 일반 모형화하여 그림 3과 같이 제시하고자 한다. ICT*DNAB2가

모두 적용되는 기본적인 접근 개념을 새롭게 정의해야 한다. ICT*DNAB2 적용은 모든 것 하나하나가 물리적 객체와 논리적 객체가 컴퓨터 내에서 결합되는 기본 구조로 인식되어야 한다. 이와 같은 구조는 사물 하나를 객체화시켜야 하고 이들 객체는 모두 Attribute/Method/Event/Data를 반드시 소유/인식되어야 한다.

이는 ICT 융합화의 다른 영역에서도 반드시 필수적이다. 이것이 융합화를 달성하는 데 연관/연합 프로그래머블 한 소프트웨어를 증가시키면서 더욱 견고하면서 지능을 갖추도록 하는 기본 철학이 된다.

국방 영역에서는 특히 ICT 융합화 단계인 제조 물류공급 단계 ICT*DNAB2을 적용하는 것은 바로 다음 단계인 국방 전술 작전 단계에 ICT*DNAB2 융합화에 직결되는 것이고, 그림 3에서 국방무기체 OBJECT 간에 군집합의 통신이 가능하여 전체적인 국방 지능화를 높이는 것과 직결되는 개념이다.

그림 3의 일반화 모델을 국방 영역에서 실례로 들면 앞장에서 언급한 ‘블록체인 전함’과 같은 함장 내에 여러 무기체(OBJECT)가 제조과정에서 군집합의 전술을 적용하게끔 정보화 특징들을 모두 내포되어야 한다.

국방 로지스틱 측면에서 ‘정적 로지스틱’을 ICT*DNAB2 적용하는 것은 바로 ‘동적 로지스틱’을 ICT*DNAB2를 적용하는 것과 직결되어 전체적인 국방 ICT 적용으로 인한 국방 지능화를 점차적으로 증진시키는 것이다.

지금까지는 주로 국방의 물리적인 측면(무기체 측면)에서 ICT*DNAB2을 적용하는 사례로 제시하였으나, 국방의 사이버전쟁 같은 경우 인공지능, 즉 소프트웨어로 인한 국방 ICT 융합화 및 지능화 측면에서 접근 역시 유사하다. 사이버 환경에서는

그림 3에서 OBJECT는 사이버 측면에서 정보매체 (영상, 위치지리정보단위, 기상정보 등)가 하나의 객체 단위로 특징 정보를 내포하여, 국방 작전 수행에 필요한 모든 정보화 체계 로지스틱스 구축 기술적용에 기본이 되어야 한다.

국방 사이버 및 정보화 체계 역시 ‘정적 로지스틱’과 ‘동적 로지스틱’으로 구분되어 구축되어야 한다. 국방 정보 소스로부터 정보가 생성되고 결합되는 구조가 DB에 정착될 때까지가 군사 정보 제조 과정이라 보면 이를 기반으로 빅데이터 분석 및 인공지능 처리로 인한 실시간 군사 작전 결정 과정은 ‘동적 로지스틱’을 처리하는 과정이다.

국방에 ICT*DNAB2가 정성적으로 융합하기 위한 기반은 국방 영역 중 하나의 로지스틱 경로를 추진하면서, 다른 로지스틱 경로와 통합되면서, 점차 융합 견고성이 증대되고, 국방 지능화 지수는 점차 상승하는 척도로 볼 수 있다.

이러한 국방 영역에서 모델은 다른 재난/사회문 제해결 영역에서도 적용되고 확장될 수 있는 근간 이 될 것이다.

국방 블록체인을 적용하는 것도 결국 가장 중요한 신뢰망 구축과 확고한 보안망을 구축 인프라로 작용될 것으로 보지만, 그 기반은 ICT*DNAB2 차 원에서 융합하기 위한 근본적인 기반 확보가 필요 하다.

또한, 이것이 국방에서 우선 먼저 정착해야 할 필요성은 국가 기밀 영역이면서 치밀한 결정에 대 하여 ICT*DNAB2 융합화가 그 책임을 다해야 하 는 이유이다.

V. 결론 및 시사점

국가 디지털화 시대에 따라 세계가 더욱 강력해 지면서, 국방 분야의 혁신과 미래 전쟁을 위한 디

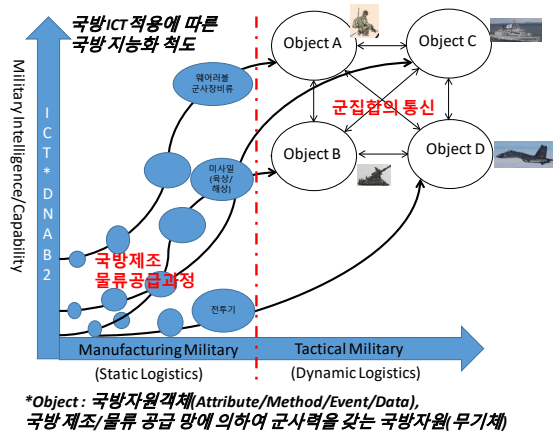


그림 3 국방 ICT*DNAB2 융합을 위한 로지스틱 객체화 모델링 단계

지털 전장에 대비할 수 있는 대한민국 국방의 시대 이다. 국방 인텔리전스의 핵심인 국방 부문의 모든 리소스는 사이버, C4(명령, 제어, 통신, 컴퓨터) 및 군용 및 비인간 무기에 의한 지능형 미션 협업 전 술 네트워크 시스템을 기반으로 한다.

국방 지능은 결국 첨단 ICT 기술의 수렴 정도 에 의존하는 현실이 되었다. 국외 국방 블록체인 기술의 적용 상태를 파악하고, 블록체인 기술 적용의 타당성과 응용 기술의 핵심을 조사 분석하였 다. 일반적인 영역에서와 같이 블록체인 기술의 주요 기능은 신뢰할 수 없는 환경에서의 데이터 무결성이다.

국방 적용되는 영역에 따라 다양한 유형의 블록 체인 핵심 기술이 있으며, 다른 ICT 기술과 함께 적용되는 새로운 핵심 기술 적용 전략을 도출하는 것도 매우 중요하다.

국방 로지스틱스는 국방 전략과 전술의 수단이 며, 실제 전쟁에서 가능한 결정을 가능하게 하는 것이며[23], 이는 국방 ICT 융합이 기반이 된다. 국 방 ICT 융합은 새로운 방위 ICT 융합 기술(DNAB2) 과 DNAB2-As-Services로 국방 지능화 및 국방력 신뢰구축에 혁신을 도모할 중요한 시기이다.

용어해설

적층가공(AM: Additive Manufacturing) 3D 프린팅 기법 중에 하나로 재료를 분사해서 한 겹 한 겹 쌓아 나가면서 실제 모양과 같이 입체적으로 만들어 나가는 기법

로지스틱스(Logistics) 재화의 생산-소비-보관-수송-포장-하역 등 물류 단계에서 재화의 관리체계, 즉 행위를 제공하는 유/무형의 서비스. 물류관리+자재관리라는 등식으로 이전에는 표현되나 최근 신기술 측면에서는 하나의 사물이 탄생부터 소멸까지 거쳐 가는 행위를 정보화 기술로 표현

국방 로지스틱스(Military Logistics) 일반 로지스틱스를 국방에 적용하는 행위로 국방력 증가를 위하여 모든 군사용 무기체 등 재원의 견고성, 효율성을 위한 운용 능력을 위해 생산에서 공급까지 지원행위를 디자인 및 통합하는 행위. 사이버 측면에서는 군사정보화 구축의 적용에 확대

디지털 스레드(Digital Thread) 세 가지 핵심 구성 요소인 고정 데이터 저장 및 참조 기능, 설계가 올바르게 작동하지 않거나 개선이 필요한지 식별하는 수단, 생산 프로세스에서 앞으로 나아갈 수 있는 확장성, 각 이전 단계에서 수집한 데이터를 사용하여 프로세스 개선을 적용하는 방법

약어 정리

A2/AD	Anti-Access/Area Denial
AM	Additive Manufacturing
C4SIR	Command Control Communications Computer Intelligence Surveillance Reconnaissance
CIO	Chief Information Officer
DIL	Disconnected, Intermittent, Limited bandwidth
DISA	US Defense Information System Agency
DNAB2	Data, Network, AI, BigData, Blockchain
DoD	Department of Defense
FDM	Federated Mission Networking
IOBT	Internet Of Battle Thing
MANET	Mobile Ad hoc Network
NATO	North Atlantic Treaty Organization
NCI	NATO Communications and Information Agency
NCW	Network Centric War

TIDE Think-Tank For Information
Decision and Execution

참고문헌

- [1] USA-DoD(Department of Defense), "DoD DIGITAL MODERNIZATION STRATEGY," DoD Office of Prepublication and Security Review, 2019.7.12.
- [2] T. J. Willink, "On blockchain technology and its potential application in tactical networks," DRDC(Defence Research and Development Canada) Scientific Report, April 2018.
- [3] "Blockchain For Military Defense: 7 Possible Use Cases," Sam Mire, DISRUPTOR Daily, 9 November 2018.
- [4] "Smart Blockchain Battleships Are Right Around the Corner," Salvatore Babones, The National Interest, May 18 2018.
- [5] "Does NATO need a blockchain?," Military Univ. of Technology, Poland NATO-CIS(Communication and information System, 2018. 9.
- [6] EDA, "BLOCKCHAIN TECH IN DEFENCE," SALVADORLLOPIS SANCHEZ, EDA Project Officer, European Defence Matters, May 2018.
- [7] <https://www.prnewswire.com/news-releases/itamco-to-develop-blockchain-based-secure-messaging-app-for-us-military-300464063.html>
- [8] "Blockchain enabled Internet-of-Battlefied Things Platform," IEEE MILCOM 2018.
- [9] <https://coincentral.com/blockchain-military-applications-the-future-tech-of-the-armed-forces/>
- [10] 인도국방대학, "Employability of Blockchain Tech in Defense application," IEEE-ICIS, 2019.6.20.
- [11] "MAPN: Military Medicine and the Romanian," Ministry of National Defense.
- [12] <https://www.pentoz.com/blockchain-technology/>
- [13] NATO, "FMN: Federated Mission networking," 2018.
- [14] TIDE(Think-Tank For Information Decision and Execution), "2018 TIDE Hackathon Final Report," NCI(NATO Communications and Information) Agency, 2018.
- [15] "The latest customers for the technology behind bitcoin are NATO and the US military," Ian Kar, GENERAL BLOCKCHAIN, May 11, 2016.
- [16] "US Defense Department to Develop Blockchain Cyber Security Shield," Coindesk, <https://www.coindesk.com/us-department-of-defense-is-developing-a-blockchain-cybersecurity-shield>, 2019.07.29.
- [17] <https://www.yahoo.com/news/smart-apos-battleships-apos-around-001000511.html>
- [18] Medha Basu, "Why US and NATO Military are looking at Blockchain," Govinsider. Asia, 7 OCT 2016.

- [19] Noah Weston, Jared Willard, Peng Wang, "Performance of blockchain technology on DoD tactical networks," Proc. SPIE 11013, Disruptive Technologies in Information Sciences II, 10 May 2019.
- [20] Misty Blowers(Datalytica), Maj Shaun Scrafford(US Air Force), Jon Williams(John's Hopkins), "Blockchain Technologies and Distributed Ledger Systems as Enablers for Real Time Decision Support," Proc. SPIE 11013, Disruptive Technologies in Information Sciences II, 10 May 2019.
- [21] 이종섭(군사문제연구원), "미래전 수행을 위한 국방시스템 구축 및 발전 방안," 구글, 2018, pp. 51-64.
- [22] ETRI, "미래 전장에 대비하기 위한 국방과 ICT 기술의 융합," 2019.8.27, p. 23.
- [23] <https://logisticsinwar.com>, 2019.