https://doi.org/10.33778/kcsa.2021.21.4.049

미래전과 네트워크 환경 변화에 따른 보안대책

오 동 한*, 이 광 호**

요 약

4차 산업혁명의 기술 발전은 현재 국방 IoT 기기의 증가, 용사 개개인의 워리어플랫폼 활용, 유·무인 무기체계 운용, 지능화된 지휘소 등과 같이 발전할 것이다. 이는 첨단 과학을 중심으로 국방부에서 주도적으로 이끌어 나가고 있다. 수백, 수천대의 센서가 융합된 무기체계는 전장에서 감시정찰, 정밀타격, 사이버전자전, 기만작전 등에 활용될 것이다. 이러한 환경으로의 변화는 전장에서 작전 성능의 우수성을 가져오지만 무기체계가 외부로 노출될 경우 아군에게 치명적인 결과를 초래할 것이다. 본 논문에서는 현재 사용되는 네트워크를 중심으로 미래전 환경에서 변화하는 네트워크 환경을 분석한다. 그리고 발전된 네트워크 기술에 상응해야 할 정보 보안 문제에 대해 고찰하고 특히 군에서 도입해야 할 보안 기술을 제시하여 장차 우리 군이 나아가야 할 방향을 제시한다.

Security Measures in Response to Future Warfare and Changes in the Network Environment

Donghan Oh*, Kwangho Lee**

ABSTRACT

The 4th industrial revolution will develop the network environment of future warfare through the increase of IoT devices, individual warrior platforms, the operation of manned and unmanned weapon systems, intelligent command post. They are leading to the weapon system combined with hundreds or thousands of sensors will be used for surveillance and reconnaissance, electronic warfare, and deception operations on the battlefield. This change to the environment brings superiority in operational performance on the battlefield, but if the weapon system is exposed to the outside, it will lead to fatal results. In this paper, we analyze the network environment that is changing in the future warfare environment, focusing on the currently used network. In addition, it considers information security issues that must correspond to the evolving network technology and suggests various security measures to suggest the direction our military should take in the future.

Key words : Future Warfare, IoT, Unmanned System, AI, Blockchain

접수일(2021년 09월 28일), 수정일(1차: 2021년 10월 21일), (2차: 2021년 10월 28일), 게재확정일(2021년 10월 31일)

* 육군3사관학교 컴퓨터과학과(주저자)
** 육군3사관학교 컴퓨터과학과(교신저자)

1. 서 론

우리 군은 한반도 안보 상황의 변화, 인구 절벽 시대의 직면, 4차 산업혁명 기술의 발전 등과 같이 급변하는 안보 환경에 맞춰 군의 획기적인 발전을 위하여 국방개혁 2.0을 2018년 발표하였다. 국방부에서 발표한 국방개혁 2.0에 따라 우리 군은 국방예산에 천문학적인 금액을 투자하여 전력을 강화하기 위해 분주하게 노력하고 있다. 특히, 정보통신기술의 발전으로 세계의 흐름으로 변모하는 4차 산업혁명 기술에 많은 금액을 투자하고 있으며 개개인의 무기체계 개발에 집중함으로서 날로 위험성이 커지는 안보 위협에 대응하고 있다. 군은 국방개혁을 통하여 첨단 과학군으로 거듭나겠다는 포부를 밝혔으며 미래 군의 청사진은 무수한 유·무인 무기체계가 혼합하여 최소의 비용으로 최대의 효과를 가져가는 방향으로 진화하고 있다.

종래의 전장은 모든 기기가 연결되어 유기적으로 활용되는 네트워크 중심전(Network Centric Warfare)으로 변화하였다. 하지만 미래전(Future Warfare)은 우주 및 사이버 공간을 포함한 다차원, 다영역 환경으로 변화하고 있으며 지휘통제체계, 감시정찰, 정밀타격과 같은 기술들이 결합하여 더욱 복합적인 환경을 조성할 것이다. 다영역에서의 전투는 체계들의 고기동성이 요구될 것이며 초연결 네트워크를 중심으로 효과중심작전과 동시 통합작전으로 전개될 것으로 판단된다. 기술의 발달로 인해 효과적인 작전의 성패는 합동성 구현이 필수적이다. 이는 적용성이 높은 사물인터넷(IoT) 기반의 네트워크 중심의 무기체계로 등장하였고 결과적으로 정보보호 대상 및 범위가 확대되고 있음을 의미한다. 아울러 모바일기술, 클라우딩, 빅데이터, 인공지능 등과 같은 신기술들이 활용되어 확대됨에 따라 새로운 사이버 위협이 생겨나고 미래전에서는 인간과 기계 인터페이스 분야가 개선되어 전장의 지휘소에서는 의사 결정이 단순하고 신속하고 정확해질 것이다. 무엇보다도 인공지능 분야의 발전은 인간의 의사 결정에 도움을 주면서도 인간이 제외된 상태에서 독자적인 의사 결정도 가능할 것으로 전망된다. 이는 시스템 자체로 스스로 판단하고 행동하여 인간이 직접 통제할 필요 없이 지능형 자율 체계가 도입되어 현재 군이 당면하고 있는 문제인 인구 절벽 시대를 극복해 나갈 것이다.

앞서 설명한 것과 같이, 정보통신기술로 인해 의사 결정의 신속성, 정확성을 높여주는 측면이 있지만, 무기체계 플랫폼들은 개개인의 용사가 소지해야 하는 센서들이 무수히 많아질 것이다. 이는 네트워크 환경 또한 더 복잡해지고 네트워크 트래픽 과부하를 초래할 뿐만 아니라 체계의 센서 정보가 유출된다고 한다면 아군에게 치명적인 결과를 초래할 수가 있다.

본 논문에서는 현재 도입될 무기체계에 대해 다루고 네트워크 환경의 변화가 어떻게 이루어질지에 대해 분석한다. 미군 등과 같은 선진국에서 제안하는 기술들을 조사하여 우리 군 또한 근미래에 도입될 네트워크 기술 체계와 현재 시스템과 그것들이 어떻게 국방 분야에 녹아들지에 대한 방향을 제시하고 네트워크 환경 변화에 따른 기술적인 취약점을 제시하여 현재 주목받고 있는 보안대책을 소개하며 미래군에서 적용해야 할 보안 기술에 대한 방향을 제시한다.

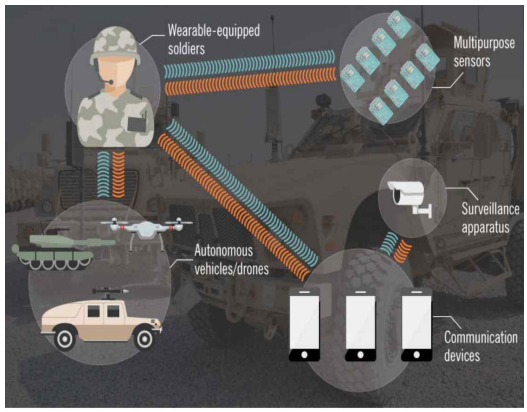
본 논문은 다음과 같이 구성된다. 2장에서는 현재 군에서 도입하고 있는 무기체계에 대해 살펴보고 3장에서는 선진국에서 개발되고 있는 네트워크 기술을 통해 군사적으로 적용되는 네트워크 극복기술에 대해 알아본다. 4장에서는 네트워크 환경 변화에 따른 보안 취약점을 분석하여 그에 상응하는 보안대책에 대해 다룬다. 끝으로 5장에서 결론을 맺는다.

2. 현재 군의 신개념 무기체계

2.1 국방 IoT(M-IoT)

사물과 사물을 연결하는 인터넷 기술인 IoT(Internet of Things)는 사물에 센서들을 부착하는 기술로서 실시간으로 데이터를 주고받는 인터넷 기반의 기술을 일컫는다. 국방 IoT(M-IoT)는 상황 인식, 의사결정, 임무 효과성을 위하여 감시 정찰, 지휘 통제 그리고 기타 지능형 사물을 연결하여 서비스를 제공하는 확장된 네트워크 기술이다. 비즈니스 데이터 플랫폼을 개발하는 Statista에 따르면 IoT 기기가 2025년에 전 세계적으로 7,544억 개로 예상한다 [1]. 이와 같은 IoT 기술의 개발은 사회 전 분야에서 이루어지고 있으며 이는 초연결, 초지능, 초고속 사회를 가능케 함을 의미한다. 군에서는 2017년부터 지능형 스마트 비행단 구축 사업을 시작으로 정보통신체계와 비행 장비를 연동하여 네트워크 구조를 최적화하고 비행 기지 내에 설치된 CCTV와 C4I를 연동하여 지휘통제실에서 모든 상황을 즉각적으로 통제하는 지휘 결심 가시화 체계를 구축하였다. [2]

위 사례와 같이, 국방 IoT는 각종 센서, 소프트웨어, 송수신 기능이 탑지된 감시정찰, 지휘통제체계, 미사일 발사체, 지능형 사물을 연결하는 것이 핵심이다. 국방 IoT 환경은 다양한 센서가 수집한 정보를 지휘소에 전달하고 지휘소에서는 센서를 제어할 수 있는 수준의 IoT와 인지기능을 추가하여 수집된 정보를 활용하여 전장 정보를 분석, 진단하고 적의 공격을 예측하여 효과적으로 지능 서비스를 사용해야 한다. 그러므로 군은 기존의 네트워크에서 IoT 프레임워크를 탑재하여 발전된 네트워크 인프라와 각종 국방 분야 서비스를 공유하고 센서 간 실시간성을 보장하여야 한다. 특히 IoT 기술은 디바이스 자체의 보안 결함이 매우 큰 기기이므로 군사 보안이 중요한 군에서는 보안을 특히 강화된 환경 안에서 지능화된 통신을 제공해야 한다. [8]



(그림 1) 전장 환경에서의 IoT 기반 구축 [3]

그림 1은 미국 버지니아 공대에서 전기 및 컴퓨터공학과에서 근무하는 Walid Saad 교수와 Naren Ramakrishnan 교수가 공동으로 제시한 개념도로서 전장 환경에서 IoT 기반을 구축하기 위한 그림이다. 위 두 사람이 제시한 연구는 미국의 육군연구소의 지원금을 가지고 2017년부터 진행하고 있다. 연구되는 분야는 웨어러블 디바이스, 다목적 센서, 자율주행차량과 드론 등과 같은 전장에 배치될 스마트기기의 전략적인 배치를 통하여 미래의 전장에서 IoT 기술이 적용된 환경으로 변화되는 환경을 연구하는 것이다. 하지만 IoT의 물리적으로 연동되는 점은 3자에 의한 무력화, 오용, 작동 정지, 기기 오류 등과 같은 다양한 증상을 수반한다. IoT 센서들은 영상, 신호 등과 같이 표현되는 정보를 이용한 보안 공격, 평문 인터페이스로 전송되는 치명적인 보안 취약점을 가진다. 그러므로 군에서는 IoT의 취약점을 통하여 기기와 직간접적으로 연동되는 타 IoT 기기가 전체 네트워크 작동에도 영향을 끼친다는 점을 고려해야 한다.

2.2 워리어플랫폼(Warrior Platform)

(그림 2) 개인 용사용 감시, 통신 운용 개념도 [6]

워리어플랫폼은 현재 군에서 개인 전투원의 인체를 하나의 기본 골격 형태로 설정하여 임무에 따라 물자와 장비 등을 최적화하는 기술로서 복합체계로 구성한 결과물을 의미한다. [4]. 군에서 개발하는 워리어플랫폼은 미국에서 개발하고 있는 미래보병체계 사업에 착안하였으며 대표 사업인 랜드 워리어와 퓨처 워리어라는 2개의 사업을 발전시킨 개념이다. 최근 개발되고 있는 센서 기술들을 활용하여 개인 용사가 개별적으로 전술단위의 C4I 체계정보를 수신받는 것을 목표로 전술 부대의 효과적인 상황공유를 가능케 하는 기술이다. 그러므로 전투복의 방호개념인 강화복을 넘어서서 첨단센서, IoT 등과 같은 핵심 기술을 접목하여 지휘소와의 통신기술 그리고 전장 상황인식 공유 등과 같이 활발하게 연구 및 개발되고 있다.

워리어플랫폼 기술은 목적에 따라 5가지로 구분할 수 있는데 가장 첫 번째는 용사 간 정보공유다. 단위 부대 내의 모든 병사가 음성, 데이터, 고용량의 영상정보를 실시간 전송할 수 있어야 하며 이를 가능하기 위해서는 무선환경에서 적응형 고속무선 통신이 가능해야 하며 Ad-hoc 중계 기술, 주파수 도약 및 암호화 기술이 필수적이다. 두 번째는 전장 영상 획득이다. 이는 영상정보와 센서 기술이 필수적이며 다중 영상 센서 및 전시기에 기반한 주야간 전장 감시가 가능해야 한다. 이를 위해 주간 및 야간 영상을 획득해야 하며 전장의 전 방향 촬영을 위해 360도 영상 및 전술 정보 전시가 가능해야 한다. 영상 관점에서는 다중센서 파노라믹, 이종센서 영상합성 기술과 무선구간 영상전송을 위해 적응형 영상 압축 및 복원 기술이 필요하다. 세 번째로는 표적탐지이다. 두 번째에 언급된 영상 기술과 연계하여 영상 신호정보를 처리하여 주야간 인원과 표적에 대한 자동탐지와 분류를 가능해야 한다. 네 번째는 피아 위치 확인이다. 그림 2와 같이 개인 용사는 통합헬멧 기반의 피아 위치를 획득하고 음성통화가 가능해야 한다. 통합헬멧에 내장된 GPS 수신기를 통하여 개인 용사의 위치

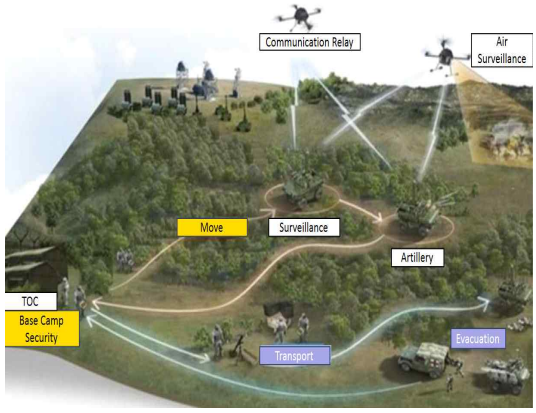
(그림 3) 통합형 헬멧 구성도 [6]

정보가 최신화되며 이는 지휘소와 공유돼야 한다. 그리고 양안투과식 전시기를 통하여 피아 위치를 확인하고 전장 정보를 실시간 공유해야 한다. 그리고 헬멧 내의 안테나와 음성 송수화기를 통하여 기반 정보가 전송돼야 한다. 마지막으로 운용자 편의 기능이다. 이는 사용자에게 편의를 제공하기 위해 시선 방향에 따른 영상이 전환돼야 하며 이를 위해 비선형 영상 압축 기술이 필요하다.

2.3 무인 전투체계

최근 미래전장 환경은 로봇을 군사작전에 활용하는 양상으로 변모하고 있다. 미군은 이라크 전쟁과 아프가니스탄 전쟁에서 무인정찰기에 감시장비와 미사일 장비를 탑재하여 지상에 있는 표적들을 공격하는 데 사용하였다. 그리고 소형 로봇들을 전술적으로 활용하여 폭발물 제거, 정찰감시 등 무인 전투체계를 효과적으로 사용하였다. 이처럼 미래전장 환경에서는 무인 전투체계가 주도적인 임무를 수행할 것이다. 육군에서는 현재 군단급에서 전자전 무인정찰기를 활용하여 지상뿐만 아니라 공중에서도 우위를 점하고 있다. 그뿐만 아니라 육군은 차후에 보병 대대급에도 무인기를 전력화하기 위해 노력하고 있으며 반도의 70%가 산악으로 둘러싸인 우리 군의 지형적인 요소를 고려하였을 때 정보전과 전자전에서도 우세한 환경을 조성할 것이다. 현재 개발되고 있는 무인 감시장비에는 근거리 소형 UAV, 초소형 저고도 UAV, 수직이착륙형 스마트 UAV, 다목적 초소형 회전익 비행체, 무인감시 로봇 등이 개발되고 있다.

그림4는 미래전장에서 운용될 지상무인무기체계를 설명하는 개념도로써 드론과 같은 무인항공기를 이용하여 지상과 공중을 연결해주는 통신 중계, 음영지역에 감시정찰을 위해 무인항공기를 투입하여 지휘본부의 의사 결정 과정에 지



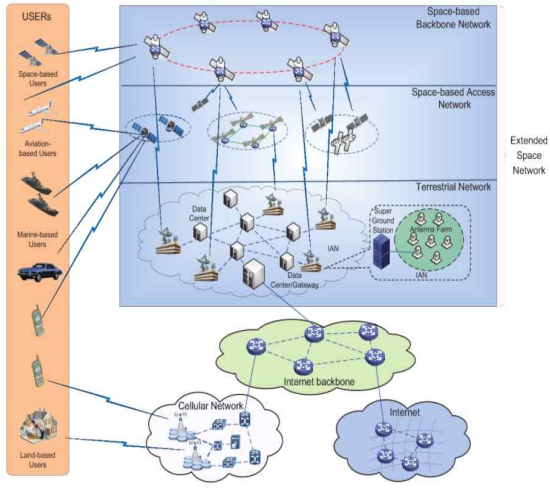
(그림 4) 지상무인무기체계 개념도 [10]

대한 영향을 끼칠 수 있으며 물리적으로 전투물자를 운반하거나 환자 수송과 같이 전투 지원 분야에서도 사용될 수 있다.

3. 미래 국방에 적용될 네트워크 기술

3.1 다차원, 다영역 네트워크 (초고속)

다차원, 다영역 환경은 종래의 지상, 해상, 공중의 3계층을 넘어서서 우주, 사이버 공간을 포함하는 5차원의 다차원 영역의 확대를 의미하며



(그림 5) 통합 네트워크 개념도 [11]

소규모 네트워크로 대변되는 대대급 제대에서도 영역 간의 동시 전장화를 통하여 지휘 통제체계, 감시정찰, 정밀타격자산이 복합적으로 결합하고 자율시스템이 도입되어 효과 중심작전으로 변화될 것이다. 이는 전장 환경에서 발생하는 수많은 데이터가 생성되고 소비될 것이며 데이터 생성과 함께 지휘소에서는 독자적인 의사 결정을 통하여 신속하게 처리해야만 전장 환경에서 실시간으로 대응할 수 있을 것이다. 특히 공중에서 백본의 역할이 중요하여 고속의 무선링크를 사용하여 음성, 비디오, 인터넷 및 기타 다양한 데이터를 처리하고 전송할 것이다.

3.2 Swarm (초연결)

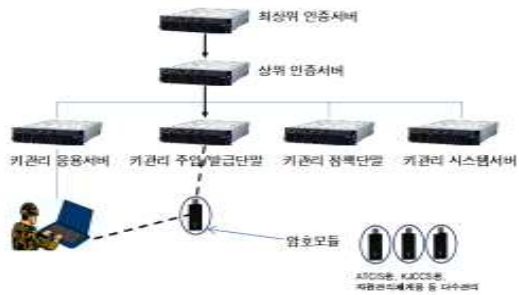
미국 고등연구계획국(DARPA)에서는 미래전장에 대응하기 위한 제3차 상쇄전략으로 군집로봇을 집중적으로 연구하고 있다. 미래전장이 다영역으로 변화됨은 공중뿐 아니라 지상, 해상을 포함한 군집 제어 기술이 필수적이다. 특히 통신이 제한된 환경에서 한 명의 통제권자가 여러 대의 무인 체계를 통제하여 협력하는 기술은 2015년부터 개발되고 있다. 그리고 지상군이 시가전에서 고층 빌딩이나 도심 지역의 좁은 공간에서 무인항공체계와 무인지상체계를 혼합하여 적을 탐지하고 공격하는 공격형 군집 비행 전술 프로그램도 진행하고 있다. 현재 군은 인력 감축과 4차 산업혁명 기술 발전에 맞추어 드론봇 군사연구센터, 드론 교육센터, 드론봇 전투단을 창설하였으며 운용적인 측면에서 초연결된 네트워킹 환경에 따라 지휘부에서 군집행동제어, 군집상황인식, 군집네트워킹, 군집관리제어 등 다수의 UAV들을 효과적으로 제어하는 기술이 개발될 것이다.

3.3 Edge AI (초신뢰)

엣지 컴퓨팅은 AI 기능을 가진 컴퓨터를 활용하여 데이터 처리 및 저장 등을 하는 기술로서 종단 네트워크의 반응 속도를 향상시키는 기술이다. 엣지 컴퓨팅은 클라우드와 같이 중앙 서버를 활용하는 것이 아니라 기기 자체의 컴퓨팅 파워를 이용한다. 따라서 서비스 지연 문제가 발생하지 않으며 IoT 기기 증가로 인한 네트워크 부하 처리 문제, 정보 침해 문제도 해소한다. 전장환경에서 지휘소는 정보를 수집하고 융합하여 종합적으로 판단하고 무기체계와 상호 소통하면서 전투를 수행하는 지능형 C4I로 운용된다.

4. 미래전의 네트워크 환경을 대응하기 위한 보안기술

현재 국방관련 암호장비와 인증체계는 전장관리정보체계를 기준으로 키관리체계(KMI), 국방인증체계(MPKI)를 사용하고 있다. 암호 방식은 공개키 암호 방식을 이용하며 사용자 신원과 전자문서의 변경 여부를 확인할 수가 있다. 전장관리체계는 그림 6과 같이 사용자가 전장체계와 같은 네트워크에 접속하기 위해서는 암호 모듈을 이용하여 접속한다. 암호키 같은 경우에는 인편으로 배달되고 있다. 군에서 개발하고 있는 무기체계와 미래에 적용될 네트워크 기술은 군에서 활용하게 될 다양한 자산이 노출될 가능성이 크며 노출 시 적에게 치명적인 위협이 될 수가 있다. 이러한 위협에 효과적으로 대처하기 위해서는 아래와 같은 기술의 도입이 필요하다.



(그림 6) 전장관리체계 PKI 구조 [13]

4.1 양자암호 (초고속)

앞서 설명한 다차원, 다영역 네트워크에서는 여러 영역을 연결해주고 신속하게 임무수행하는 것을 목표로 하며 적군의 무기체계 및 암호해독 능력도 그에 비례하여 상승할 것으로 판단된다. 이는 군이 사용하고 있는 현재의 암호체계가 취약함은 물론 미래에 적용되게 될 양자컴퓨터와 같이 성능이 우수한 컴퓨터를 이용할 경우에 군의 암호체계가 무력화를 초래할 것이다. 이는 효과적인 지휘가 불가능함을 의미한다. 그러므로 우리 군은 미래의 기술 발전에 따라 암호체계의 무력화를 대응할 양자암호를 도입해야 한다. 양자암호는 빛 입자인 광자를 이용하는 방식으로서 암호화와 복호화 과정에서 암호키로 양자를 활용하며 양자의 특성을 가진다. 따라서 암호키를 전송할 때에 외부로부터 탈취를 시도할 때 양자의 상태가 변하는 특징을 가지고 있어 인편으로 배달되는 취약점을 극복할 수 있는 기술이다. 특히 양자의 중첩 특성을 통하여 3자가 통신을 도청하게 될 때 중첩현상이 붕괴하여 정확한 정보 탈취가 어렵다. 양자의 얽힘의 특성은 3자가 통신을 도청할 때 송, 수신자에게 경고할 수가 있다. 양자의 불확실성의 특징은 3자가 신호를 탈취할 경우 복제하여 보낼 때 오류 값을 증폭시켜 도청되는 사실을 인지하게 된다. 현재 미군은 양자암호통신을 이용하여 무선통신체계 기술을 접목한 연구를 진행 중이다. 우리 군 또한 미래의 네트워크를 고려해봤을 때 현재의 보안대책이 미래의 작전보안에 취약한 점을 들어 양자암호를 적극적으로 개발해 나가야 한다.

4.2 블록체인 (초연결)

무수히 많은 체계가 연결되어 임무수행하는 군은 지휘소에서 지휘관을 중심으로 작전 운용이 되기 때문에 중앙에서 무기체계를 통제하는 시스템이다. 이는 전시에 매우 취약한 네트워크 구조이다. 왜냐하면 지휘소가 파괴될 경우 네트워크 환경 자체가 성립되기 어렵기 때문이다. 그러므로 우리 군은 블록체인을 도입하여 이를 대비해야한다. 블록체인은 P2P(Peer-To-Peer) 시스템으로서 구성원 모두가 데이터 송수신에 관여하고 인증하는 시스템으로 추가적인 노드가 발생하면 전체 참여자에게 공유가 되기 때문에 근원적으로 사이버 공격이 어렵다. 그러므로 중앙 집중식 시스템의 인프라에서 분산 방식으로 비문을 전송함으로써 지휘소 파괴와 같은 중앙 집중식 시스템에서 일어날 수 있는 문제점을 해결하고 극단적으로 늘어나고 있는 전자기기 및 센서들의 탈취와 데이터 장비 유출로부터 안전하기에 군에서 적극적으로 개발하여 도입하여야 한다. 특히, 미군은 2019년 “국방 디지털 현대화 전략”을 통하여 통신부문에 블록체인을 적용한 계획을 구상하였으며 DARPA를 통하여 블록체인 기반의 메시징 플랫폼 개발에 연구를 진행해 나가고 있다. [15] 블록체인 기술은 중앙기관의 개입 없이 거래 참여자가 개인 간 거래를 직접 관리하고 인증하는 기술이다. 이를 통해 군에서 발생하는 무수한 데이터를 해시함수 처리하여 데이터 변조를 방지할 수 있다. 그리고 국방 분야에서는 미리 약속된 키 값을 이용하여 다수의 무기체계가 3자가 개입할 때 약속된 키 값을 이용하여 검증, 공유하고 유효성을 인증하여 3자에 대한 암호, 비문 탈취에 효과적인 기술이다.

4.3 AI기반 SOAR (초신뢰)

SOAR(Security Orchestration, Automation and Response)는 수많은 사이버 위협을 자동적으로 분류하고 표준화된 업무 프로세스에 따라 사용자와 체계가 유기적으로 협력할 수 있도록 지원하는 플랫폼이다. 미래 군의 지휘소에서는 무엇보다도 신뢰성 있는 네트워크 보장이 필요하며 이는 필연적으로 분산컴퓨팅 구조를 사용함을 의미한다. 지휘소에는 인공지능 기술을 바탕으로 실시간으로 정보를 분석하고 불필요한 정보는 선별적으로 처리한다. 인공지능 기술은

발달된 보안관제시스템을 바탕으로 보안에 위협을 가하는 데이터도 실시간으로 파악하고 처리하게 된다. 이상 및 위협을 탐지하여 이벤트 발생에 따른 장애를 예측하고 수집된 보안 정보를 취합하여 신속하게 의사결정을 돕고 대처하는데 지휘소에 도움을 준다.

5. 결 론

국방개혁 2.0에 따른 국방 분야의 혁신과 미래전의 다영역으로의 변화는 우리 군이 점차 능동적이고 유기적으로 대처해야 함을 의미한다. 현재 군에서 개발하여 전력화하고 있는 국방 IoT, 워리어플랫폼, 무인전투체계는 현재 인력이 감축되어 용사의 수는 감소하고 있지만, 개인 용사 한 명이 지니는 센서가 최소 30개에서 100개에 이른다. 이는 네트워크가 굉장히 복잡해지고 보안에 취약한 특징을 지니고 있음을 의미한다.

센서의 발달로 변화되고 있는 점과 더불어 미래의 네트워크는 AI, 군집 드론과 같이 현재보다 기하급수적인 네트워크 기기의 증가를 의미하며 전장 영역에서 네트워크 과부하뿐만 아니라 데이터가 탈취될 경우 신뢰할 수 없는 환경으로 변화되어 우리를 위협하는 기술로 바뀔 수 있음을 시사한다.

그러므로 우리 군은 현재의 발전과 더불어서 현재 전장관리체계의 취약점과 변화하는 환경에 발맞추어 양자암호통신과 블록체인을 도입하여 적군으로부터 데이터 유출로 인한 사고를 줄이고 전시에 운용하기에 불리한 중앙 집중식 시스템에서 분리하여 블록체인을 개발함으로써 데이터 송수신 간 검증되고 인가된 인원만 취급할 수 있도록 변화해야 한다. 또한 실시간 보안관제시스템에 인공지능을 도입하여 보안 위협에 신속하게 대응해야 한다.

참고문헌

[1] L. Yushi, J. Fei and Y. Hui, Study on application modes of military Internet of Things (MIOT)," 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), pp. 630-634, Zhangjiajie, 2012.

[2] Hyun-Jin Han, Dea-Woo Park, "Cybersecurity of The Defense Information System network connected IoT Sensors", Journal of the Korea Institute of Information and Communication Engineering, Vol. 24, Nol. 6, 2020.

[3] Laying groundwork for the Internet of Battlefield Things, ECE(Electrical and Computer Engineering) NEWS by Virginia Tech, 2017.

[4] Seongdo Kim, Kyunghwan Kim, Dongmin Im, Jihye Kwon, "Building a human-centered defense Warrior Platform in preparation for the 4th industrial revolution.", Conference Papers of Ergonomics Society of Korea, pp.176-185, 2017.

[5] Se-ho Lee, Ho-jun Lee, Hee-won Yang, Young-cho Jang, "The Combat Effectiveness Analysis of Warrior Platform Improvement Using AWAM", Journal of Knowledge Information Technology and Systems, Vol. 15, No. 3, pp. 331-346, June 2020.

[6] Junsung Choi, "Communication and situation recognition technology research status for the Warrior Platform.", Defense & Technology(483), pp.82-93, 2019.

[7] Defence science and technology glossary, "Unmanned combat system." https://dtims.dtaq.re.kr (Searching: 2020. 12.7.)

[8] Kyungsoo Kim, Yongwoon Lee, "The unmanned weapon system, the human role division and manned-unmanned complex system", Defense & Technology(483), pp.130-139, 2019.

[9] N. Gonzalez-Prelcic, R. Mendez-Rial, and R.

W. Heath Jr, “Radar aided beam alignment in mmwave V2I communications supporting antenna diversity”, In Proc. the 2016 Information Theory and Applications Workshop, Feb. 2016.

[10] Sunwoo Cho, et al. “Survey on Machine Learning Algorithms for SDN/NFV Automation”, The Journal of Korean Institute of Communications and Information Sciences, Vol. 44, No.1, pp. 92-105, 2019.

[11] Liu, Jiajia, et al. "Space-air-ground integrated network: A survey." IEEE Communications Surveys & Tutorials Vol. 20, No. 4, pp. 2714-2741, 2018.

[12] Sunwoo Cho, et al. “Survey on Machine Learning Algorithms for SDN/NFV Automation”, The Journal of Korean Institute of Communications and Information Sciences, Vol. 44, No.1, pp. 92-105, 2019.

[13] 이원만, 구우권, 박태형, 이동훈 “전장관리체계(C4I)에서의 암호 및 인증방법 개선 방안에 관한 연구”, 융합보안논문지 vol. 12, No. 6, pp. 39-50, 2012.

[14] 이진욱, 최윤호, 김용준, 박찬재, “미래전의 이지스(Aegis), 양자암호통신의 국방분야 적용 방안.”, 국방과 기술(510), pp. 94-99, 2021.

[15] USA-DoD (Department of Defense), “DoD DIGITAL MODERNIZATION STRATEGY,” DoD Office of Prepublication and Security Review, 2019.

〔저자소개〕

오 동 한 (Donghan Oh)
2015년 3월 육군3사관학교 정보공학과 학사
2020년 2월 아주대학교 석사 NCW학과 석사
2020년 3월~현재 육군3사관학교 컴퓨터과학과 강사
email : donghan@mnd.go.kr

이 광 호 (Kwang-ho Lee)
2007년 2월 육군3사관학교 경제학과 학사
2016년 8월 연세대학교 정보보호학과 학사
2017년 2월~현재 아주대학교 NCW학과 박사과정
email : loveney@naver.com