J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

미래 사이버위협에 대응 가능한 『Army TIGER 사이버방호체계』 구축을 위한 제언

Proposal for the『Army TIGER Cyber Defense System』Installation capable of responding to future enemy cyber attack

박 병 준[1] 김 철 중[2*]
Byeong-jun Park Cheol-jung Kim

요 약

미래형 전투체계를 구현하기 위해 전력화가 진행중인 육군 Army TIGER체계는 기동화, 네트워크화, 지능화 등 육군의 전투방식과 전투수행능력에 혁신적인 변화가 예상된다. 이를 위해 육군은 드론, 로봇, 무인차량, 인공지능 등이 적용된 다양한 무기체계를 도입하여 전투에 활용할 것이며, 다양한 무인체와 인공지능의 활용은 신기술이 적용된 장비의 육군 내 도입과 다양한 종류의 전송정보, 즉 데이터 증가가 예상된다. 하지만 현재 육군에서는 기능별 Army TIGER 전력화체계를 활용한 전투수행방안 중심의 연구 및 전투실험에 집중하고 있는 반면, Army TIGER 부대별로 증가되는 무인체와 무인체에서 생산, 전송되는 데이터에 따른 사이버위협 및 신규체계 전력화에 따라 구축되는 클라우드 센터, AI지휘통제실 등에 대한 정보체계를 대상으로한 사이버보안 대응방안 연구는 추진하지 못하는 실정이다. 이에 본 논문에서는 육군 Army TIGER 전력화체계의 구조 및 특성을 분석하여 장차 사이버위협에 대응 가능한 『Army TIGER 사이버 방호체계』 구축 필요성 및 적용 가능한 사이버보안 기술에 대한 제언을 하고자 한다.

☞ 주제어 : 아미 타이거(Army TIGER), 드론, 로봇, 무인차량, 인공지능, 클라우드 센터, 사이버보안

ABSTRACT

The Army TIGER System, which is being deployed to implement a future combat system, is expected to bring innovative changes to the army's combat methods and comabt execution capability such as mobility, networking and intelligence. To this end, the Army will introduce various systems using drones, robots, unmanned vehicles, AI(Artificial Intelligence), etc. and utilize them in combat. The use of various unmanned vehicles and AI is expected to result in the introduction of equipment with new technologies into the army and an increase in various types of transmitted information, i.e. data. However, currently in the military, there is an acceleration in research and combat experimentations on warfigthing options using Army TIGER forces system for specific functions. On the other hand, the current reality is that research on cyber threats measures targeting information systems related to the increasing number of unmanned systems, data production, and transmission from unmanned systems, as well as the establishment of cloud centers and AI command and control center driven by the new force systems, is not being pursued. Accordingly this paper analyzes the structure and characteristics of the Army TIGER force integration system and makes suggestions for necessity of building, available cyber defense solutions and Army TIGER integrated cyber protections system that can respond to cyber threats in the future.

☞ keyword : Army TIGER, Drone, Robot, unmanned Vehicle, AI, Cloud Center, Cyber defense

1. 서 론

최근 민·관·군을 막론하고 다양한 사이버공격이 급증하고 있으며, AI(Artificial Intelligence) 등 신기술을 기반으로 고도화되는 상황에서 사이버방호체계 구축의 중요성은 계속 증가하고 있다.[1] 육군은 사이버작전센터 창설, 사이버 특기자 선발 및 사이버 직책 개편 등 조직, 인력, 제도 등 모든 분야에서 사이버 능력향상을 위한 단계별 발전을 추진하고 있으며, 군에서 운용중인 네트워크(국방망, 전장망, 인터넷, 단독망)별 특성에 맞는 사이버방호체계를 구축 및 운용하고 있다.[2]

현재 육군에서 전력화중인 Army TIGER 체계는 미래형 전투체계를 구현하기 위해 드론, 로봇, 무인차량, 인공지능 등 신기술을 적용해 전투원의 생존확률과 전투 효율성을 극대화한 것이 특징이며, 다양한 체계의 전력화가 현재도 계속 진행중이다.[3] 이에 따라 전력화 체계를 활

1 Department of Cyber/C4I, ROKA Signal school, Daejeon, 34056, Republic of Korea
2 Department of Cyber protection, ROKA Signal school, Daejeon, 34056, Republic of Korea
* Corresponding author(army_ict_cyber@army.mil.kr)
[Received 06 October 2023, Reviewed 24 October 2023(R2 04 December 2023), Accepted 06 December 2023]

용한 전투수행방법에 대한 연구 및 세미나가 진행중이며, 전투원과 드론봇 전투체계, 워리어플랫폼 등 모든 전투체계가 연결되는 네트워크화와 인공지능 기반의 초지능 의사결정체계가 상황판단과 결심을 지원하는 지능화도 병행하여 추진되고 있다.[4]

(그림 1) Army TIGER 4.0 체계 개념도[5]
(Figure 1) System concept diagram of Army TIGER 4.0 [5]

그러나 현재 육군에 전력화중인 다양한 Army TIGER 전력화 체계들에 의해 변화가 발생하게 될 네트워크, 의사결정체계, 각종 데이터 종류에 대해 적 사이버위협에 대응 가능한 사이버방호체계 구축을 위한 연구가 절실한 시점에 있다. 현재까지 Army TIGER 전력화 체계에 대한 사이버방호체계 구축 연구가 미 실시된 이유는 드론, 로봇, 무인차량, 인공지능 등 기존 육군에서 미 사용중이던 신규 전력체계들의 활용을 극대화하여 육군이 추구하는 미래형 전투체계를 구현하는 것에 집중되어 있기 때문이다. 또한 Army TIGER 부대는 기존 보병여단 및 대대에 신규 전력화체계를 도입하여 변화하는 형태로 전력화 이후에도 보병여단 및 대대의 형태를 유지하며, 이러한 부대 구조는 육군 사이버작전수행지침 內 사이버방호체계 부대별 운용지침 범주안에 포함됨에 따라 추가적인 사이버방호체계의 도입은 현재 고려하고 있지 않은 상태이다.

이에 본 논문에서는 육군에 전력화중인 Army TIGER 전력화체계를 대상으로 구조 및 특성 분석을 통하여 다양한 사이버위협에 대응 가능한 『Army TIGER 사이버방호체계』에 대한 운용개념과 체계도입 필요성 및 사이버보안 기술에 대한 제언을 하고자 한다.

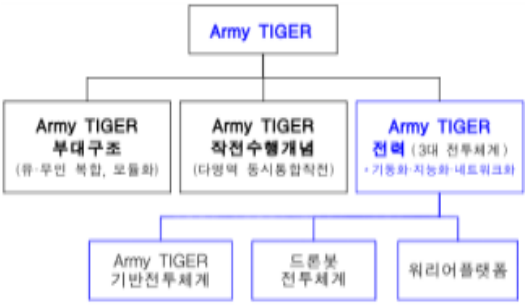
(표 1) 사이버 공격 유형[6]
(Table 1) Types of Cyber Attacks[6]

분 류	설 명
정보유출 (계정정보)	이용자의 PC 혹은 모바일 기기내 저장된 ID/PW등을 탈취하는 악성코드
다운로더	추가 악성코드를 인터넷이나 네트워크를 통하여 다운로드 후 설치 및 실행하는 악성코드
랜섬웨어	PC의 중요파일(문서, 사진 등)을 암호화 하고 금전을 요구하는 악성코드
원격제어	해커가 원격지에서 악성코드에 감염된 좀비 PC들을 제어하는 목적으로 이용하는 악성코드
정보유출 (기기정보)	감염된 PC 혹은 모바일 단말기의 정보를 탈취하는 악성코드
드롭퍼	정상 애플리케이션인 것처럼 배포된 뒤 실행되면 바이러스 코드를 실행하는 악성코드
해킹툴	불법침입, 정보유출, 제3자 공격 등 해킹목적을 위한 도구 프로그램
웜바이러스	자신을 복제하고 네트워크를 통해 전파할 수 있는 악성 프로그램
백도어	몰래 컴퓨터에 접속하여 악의적인 행위를 할 수 있도록 출입통로 역할을 해주는 악성코드

2장에서는 Army TIGER에 대한 이해를 위해 구성요소 및 기반전투체계, 드론봇 전투체계, 워리어 플랫폼의 3대 전투체계에 대해 서술하고 3장과 4장에서는 3대 전투체계 중 기반전투체계와 드론봇 전투체계에 대한 분석을 진행, 구축 가능한 사이버방호체계에 대한 운용개념과 구축소요에 대해 설명하며, 이후 다양한 데이터가 종합, 분석되는 아군의 정보체계에 대해 사이버위협으로부터 보호가 가능한 방안을 도출하였다.

2. Army TIGER 체계

Army TIGER는 첨단과학기술 육군으로의 군사혁신을 상징하고, 기동화·지능화·네트워크화된 4세대 이상의 지상전투체계로 무장된 육군의 모습을 의미하며, 부대구조, 작전수행개념, 전력을 포괄한 상위개념을 가진다.[3]



(그림 2) Army TIGER 구성요소 [3]
(Figure 2) Components of Army TIGER [3]

Army TIGER 전력(3대 전투체계)은 기동화·지능화·네트워크화 특성을 가진 전력체계의 하위로 표2와 같이 기반전투체계, 드론봇 전투체계, 워리어플랫폼의 3대 전투체계로 구분된다.[3]

(표 2) Army TIGER 3대 전투체계 용어 정립
(Table 2) Establishment of terminology for Army TIGER's three major combat system

구 분	내 용
기반전투체계	첨단과학기술을 접목한 미래 지상전투체계
드론봇전투체계	현용전력과 통합된 드론과 로봇의 유·무인 복합전투체계
워리어플랫폼	전투원의 치명성과 생존성을 향상시킨 육군의 개인전투체계

2.1 Army TIGER 데이터 유통량 변화

Army TIGER 체계의 전력화로 육군의 모습은 대대급까지 많은 변화가 예상된다. 군사보안의 문제로 공개되어 있지 않은 체계를 비롯하여 표3에서와 같이 지휘결심 지원 AI, 정찰/공격드론 등 다양한 체계들이 기동화, 지능화, 네트워크화되어 변화된 모습외에도 데이터의 흐름 및 유통량 변화가 예상된다.

전력화가 예상되는 체계 중 드론, 로봇, 무인차량, 지휘결심체계에서는 데이터의 생산, 수집, 전송이 예상되며, 이를 시나리오 기반으로 정보유통능력을 분석한 결과는 다음과 같다.

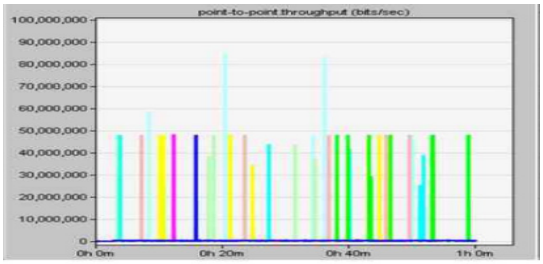
(표 3) Army TIGER 무기체계[7]
(Table 3) Army TIGER weapon system[7]

구 분	무기체계
지휘통제체계	• B2CS • ATCIS-II • 이동통신중계용 드론 • 차륜형 지휘소 차량 • 지휘결심지원 AI • 워리어플랫폼 개인전장단말기 • 소부대무전기-II 등
감시정찰체계	• 정찰드론 • 근거리 감시 레이더 • 다기능 관측경 • 대대급 UAV 등
타격체계	• 공격드론 • 현궁 • K242 박격포 • 대대급 자폭드론 • K-5 중기관총 • K-4 고속유탄기관총 등
지원체계	• 폭발물 탐지 및 제거 로봇 • 다목적 무인 차량 등

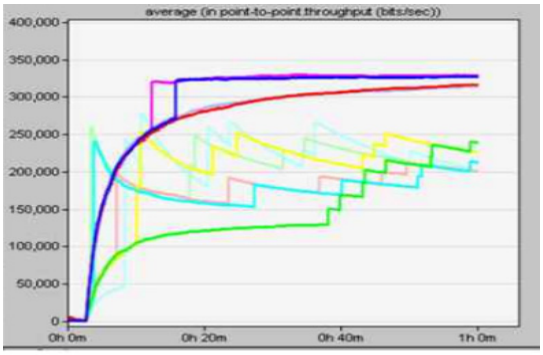
(표 4) 정보유통 분석을 위한 시나리오#1, 2
(Table 4) Scenarios for analyzing information distribution #1, 2

구 분	시나리오
1단계 (시나리오 #1)	최초 전면전이 발생하여 GOP 방어작전을 수행
2단계 (시나리오 #2)	최초 GOP 지역에서 방어작전을 수행하던 중 수 Km 철수하여 종심지역을 방어

표4의 시나리오 1, 2를 분석한 결과 평균 정보유통량은 200 ~ 400Kbps 수준을 나타냈다. 그러나 최대 정보유통량은 50Mbps 이하로 나타나지만 순간적으로 50Mbps를 초과하는 경우가 발생하였다. 평균 정보유통량과 최대 정보유통량에서 많은 차이가 발생하는 이유는 정찰/공격드론 같은 미래 무인 무기체계 다수에서 중대 및 대대본부에 동시에 영상정보를 전송하는 경우가 발생하며, 이로 인해 순간적으로 급증하는 것으로 나타났다.[7] 데이터의 유통량 증가가 사이버위협의 증가를 나타내는 것은 아니다. 그러나 드론, 로봇 등 Army TIGER에 전력화되는 다양한 체계에서 수집되는 정보는 전투와 관련된 내용을 포함하고 있어 지휘관의 지휘결심, 전투현장 분석 등에 필수적 요소로 활용될 것이다. 3장에서는 Army TGIER 기반전투체계의 5가지 기능을 분석하여 사이버위협에 대응하기 위해 보완이 필요한 부분을 판단하였다.



시간별 최대 정보유통량(순시값)



시간별 평균 정보유통량

(그림 3) 시나리오 기반 정보유통량 분석 결과[7]
(Figure 3) Scenario-based information flow analysis results[7]

3. 기반전투체계 분석

Army TIGER 기반전투체계는 무기체계, 전력지원체계, 정보화체계, 교육훈련, 부대관리 5가지 기능으로 구성되어 있으며, 첨단과학기술을 적용한 미래 보병부대의 인원, 장비, 시설 등 하드웨어와 스마트체계(소프트웨어)를 패키지화 한 모델을 적용하고 있다.[3]

3.1 Army TIGER 기반전투체계

무기체계는 지휘통제, 정보, 기동, 화력, 방호 각각의 전투수행기능별 기동화·지능화·네트워크화를 전력화하여 전투효율성을 증대하기 위해 로봇, 드론 등 다양한 무인체를 도입하고 있으며, 이러한 무인체는 병력(전투원)을 대신하여 전투를 수행하고 다양한 전장상황에서 병력을 지원하게 된다. 무인체를 활용한 전투수행을 위해 원격조종의 기능은 필수적이며, 이에 따라 영상전송 및 저장, 위치확인, 무인체 조작을 위한 통신 등 각각의 무인체는 다양한 기능을 보유하고 있다.

(그림 4) 기반전투체계 - 무기체계
(Figure 4) Basic combat system -Weapon system

전력지원체계는 AI기반 모든 플랫폼이 초연결되어 각각의 장비별 센서에서 발생하는 데이터를 전송, 수집, 가공의 절차가 필요하다. 이를 구현하기 위해서는 무선, 유선으로 구성된 네트워크와 AI 지휘통제를 위한 서버장비의 도입이 필수적이다. 이를 보호하기 위해 네트워크 보호 및 서버보안 SW 적용에 대한 대책이 필요하다.

(그림 5) 기반전투체계 - 전력지원체계
(Figure 5) Basic combat system - Power support system

정보화체계는 모든 전투플랫폼을 네트워크로 연결하여 클라우드 기반 빅데이터를 활용 할 수 있는 지능형체계를 구축한다. 전력지원체계에서 발생하는 데이터를 종합한 전 제대의 통제 개념으로 네트워크보호 및 서버보

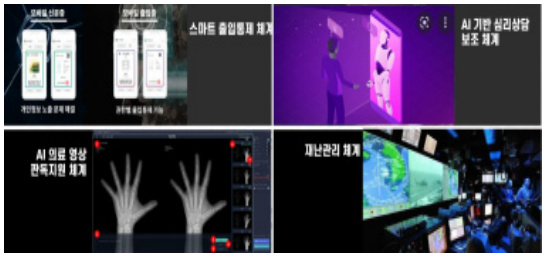
(그림 6) 기반전투체계 - 정보화체계
(Figure 6) Basic combat system - Information system

안 SW 적용이 필요 할 것으로 판단되며, 전 제대의 데이터를 관리하는 통합클라우드 센터는 적 사이버위협의 주요 목표가 될 것으로 예상된다.

합성훈련환경 기반의 과학화훈련체계를 활용 실기동, 가상모의, 워게임, 게임 훈련을 단계적으로 실시하여 제대별 작전수행능력을 배양하기 위한 교육훈련 분야는 네트워크의 연동이 필요하다. 이를 보호하기 위해서는 사이버방호체계를 구축 전 군 보안지침에 맞는 연동서버의 구축이 필요하며, 연동서버 구축간 서보보안 SW의 설치, 네트워크 보호를 위한 대책이 필요하다.

(그림 7) 기반전투체계 - 교육훈련
(Figure 7) Basic combat system - Education and training

AI기반의 출입통제, 병력관리, 재난 및 안전관리 등의 스마트한 부대관리체계를 구축하여 최상의 전투력 발휘 여건을 보장하는 부대관리체계 또한 네트워크 연동이 필요하다. 이에 네트워크 연동을 위한 연동서버 및 서버보안 SW, 네트워크 보호를 위한 대책이 필요하며, 전투원 의료영상 및 심리상담을 위한 지원체계 구축간 외부병원에 구축되어 의약품, 혈액 등 환자의 의료정보 공유시스템인 PTS(Pneumatic Tube System)와의 연동도 고려하여야 한다. 이때 고려하여야 하는 사항은 위에 작성된 연동서버 및 서버보안 SW, 네트워크 보호 대책과 동일하다.



(그림 8) 기반전투체계 - 부대관리
(Figure 8) Basic combat system - Unit management

3.2 기반체계 분석으로 식별된 문제점

기반체계 5가지 기능을 분석한 결과 가장 큰 특이점은 다양한 무인체가 군에 도입되며, 이를 조작간 외부 네트워크와 연결, 데이터의 송·수신이 발생한다는 것이다.

무인체의 원거리 조작을 위해 군 전송체계를 사용한다고 가정시 무인체 통제장치(GCS)와 무인체 플랫폼에 대한 취약점 검증이 필요하며, 운용간 수집된 영상정보의 전송 및 저장시에도 영상정보에 대한 무결성 검증이 미실시된 상태에서 군 전용네트워크를 사용해야 하므로 무인체 체계별 네트워크 보호 및 데이터 무결성 검증을 위한 대책이 필요하다.

또한 다양한 무인체에서 발생하는 데이터 통신을 위해 네트워크의 보호를 위한 노력도 필요하며, 다양한 사이버위협에 대응하기 위해서 MTD(Moving Target Defense)*와 같은 기술을 적용하여 서버장비가 집중된 네트워크의 보호를 고려해야만 할 것이다.

MTD 기술은 미국 백악관이 지난 2011년 발표한 '연방정부의 사이버보안 연구개발을 위한 전략전 계획' 중 가장 주목받은 혁신적 개념으로서 '아무것도 신뢰하지 않는다'는 것을 전제로한 '제로 트러스트(zero trust)' 개념 기반의 사전 예방적 혁신기술이다. 최근 공군에서도 1년간 가능성 시험을 거쳐 성공적인 결과를 얻은 사례가 있다.[8]

서버와 클라이언트 사이에 주소변경 기술과 기만시스템을 사용하는 MTD 기술을 정보화체계외 Army TIGER 전력화체계에 적용시 사이버 공격에 상대적으로 유리한 입장이 될 것으로 판단된다.[8]

(그림 9) 공군 MTD - 영상감시체계[8]
(Figure 9) Air Force MTD - Video Surveillance System[8]

* MTD(Moving Target Defense) : 보호대상 서버의 IP, Port 주소를 지속적이고 랜덤하게 변화시켜 사이버 위협 공격을 사전 예방 할 수 있는 서버보호 솔루션

3.3 기반전투체계 분석 결과에 따른 사이버방호체계 구축 소요

Army TIGER 기반전투체계 각각의 분야에 대해 네트워크, 저장매체, AI서버, 연동접점 등에 보완이 필요한 사항을 예측 할 수 있으며, 이를 현재 육군에서 운용중인 사이버방호체계를 확대 적용 및 보완하는 방법으로 판단한 결과는 표 5와 같다. 또한 추가로 클라우드센터, AI지휘통제실과 같이 제대별 다양한 정보가 수집, 가공, 분석, 처리되는 서버군이 집중되는 네트워크의 영역을 보호하기 위해서는 앞에 언급된 MTD와 같은 기술의 적용 가능성을 판단하는 것도 필요하리라 생각된다.

(표 5) 기반전투체계 사이버방호체계 구축소요
(Table 5) Requirements for establishing a basic combat system cyber protection system

구 분	보호 영역			
	네트워크	저장매체	서버(AI)	연동접점
무기체계	O	O	O	-
전력지원체계	O	△	O	△
정보화체계	O	△	△	-
교육훈련	O	△	-	O
부대관리	O	△	O	O

4. 유·무인 복합전투수행을 위한 무인체 보유 취약점 대응

육군에서는 드론봇전투체계에서 전력화되는 드론, 로봇, 무인차량 등 다양한 무인체를 전투에 적용, 유·무인복합전투수행 방안을 발전시키고 있다. 유인 전투력에 무인체를 편성하여 전투수행간 위협 및 취약점을 극복하는 것에 중점을 두고 전력화 중이며, 본 논문에서는 다양한 무인체중 기존 드론에 대한 취약점 연구 결과를 통해 군에 도입되는 드론에 발생 가능한 문제점을 네트워크와 애플리케이션 중심으로 설명하고자 한다.

4.1 유·무인복합 전투수행방안

유·무인복합 전투수행방안은 국방개혁에 의한 부대개편 완료 이후 2차 인구 절벽 도래에 따른 병력 자원 감소를 해소하고 전투간 병력의 피해를 최소화하고 전투효율을 극대화 할 수 있는 최선의 방법이라고 판단된다.

(그림 10) 유형별 유·무인복합전투체계 로드맵[9]
(Figure 10) Manned and unmanned complex combat system - Type[9]

그림 10의 붉은색으로 표기된 장비들은 기 배치 및 운용중인 체계[9]로 이런 다양한 체계를 활용한 유·무인복합 전투수행방안을 실현하기 위해서는 도입되는 무인체에 대한 취약점을 해소하여 외부의 사이버 위협으로부터 안전한 상태에서 운용이 가능하여야 하며, 지속적인 연구를 통해 식별된 무인체의 사이버 취약점에 대응방안을 강구하여야 한다.

4.2 무인체의 사이버 취약점

Army TIGER 체계에 도입되는 무인체는 군사보안상 이유로 모델과 기능에 대해 실제 명칭을 제시할 수는 없어서 기존 연구자료를 참고로 설명하고자 한다. 표6은 지금까지 연구된 무인체 중 드론의 주요 구성요소와 분야별 사이버 취약점이며, 구성요소별 다양한 취약점이 존재하는 것을 확인 할 수 있다.[10]

(표 6) 드론의 주요 구성요소와 분야별 사이버 취약점 현황
(Table 6) Status of major components of drones and Cyber vulnerabilities by field

구성요소	취약점	내용
GPS	GPS 스푸핑	GPS 좌표 임의 변경을 통한 드론 납치[11,12]
자이로 스코프	오프셋 값 추적	자이로스크포의 오프셋 값을 사용하여 드론 추적[13]
	센서 값 불안정	공진 주파수를 사용한 데이터 임의 변동[14]
인증	접근제어	접근인증과정 부재로 인한 공격[12,15,16]
	인증 해제	암호화 되어 있지 않은 부분을 사용한 인증 해제 [12,15,17]

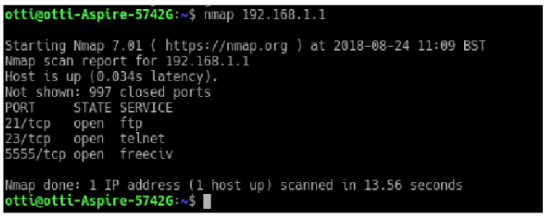
(계속)

구성요소	취약점	내용
애플리케이션	하드코딩	주요 데이터 애플리케이션 내부 자체 배치[16,17]
	암호화되지 않은 데이터 전송 취약점	평문 데이터 노출을 통한 개인정보 탈취[12,15,17]
네트워크	개방향 Wi-Fi 취약점	개방향 Wi-Fi를 사용한 드론 납치[12,15,17,19]
	개방된 포트 취약점	개방된 포트를 통한 루트 접근 권한 획득[15]
	퍼징 공격	데이터 무작위 주입을 통한 드론의 오작동 유도[20,21]
	DoS 공격	과도한 패킷 주입을 통한 시스템 과부하 발생 [15,18,19,20]
	중간자 공격	위장을 통한 사용자 개인정보 데이터 탈취 [15,22]

본 논문에서 네트워크와 애플리케이션 중심으로 서술하는 이유는 GPS, 자이로스코프 등 전자신호에 의해 영향을 받을 수 있는 기존의 취약점에 대해서는 군의 타 기능에서 연구가 진행중에 있기 때문이다.

4.2.1 개방된 포트 취약점

개방된 포트 취약점은 특정 포트를 통해서 사용자의 명령을 수신하고 수집된 영상정보를 드론으로부터 사용자에게 전송하는 드론의 통신방식을 악용한 취약점으로 포트가 개방되어 있거나 해당 포트에 비밀번호가 활성화 되어 있지 않을 경우 외부로부터 접근권한을 획득 할 수 있다.[15]



(그림 11) 오픈 포트 취약점[15]
(Figure 11) Open Port vulnerabilities[15]

4.2.2 하드코딩 취약점

하드코딩 취약점은 개발과정에서 프로그램 소스 코드에 직접 포함하는 것을 말하며 네트워크 IP, 데이터 암호화 키를 그대로 하드코딩하여 영상정보를 캡처하거나 암호변경, 복호화가 가능하다.[16, 17]

```
private static final int PORT_NUMBER = 2121;
private static final String PWD = "yuneec";
private static File ROOTDIR = new File(Environment
private static final boolean SHOULD_TAKE_FULL_WAKE
private static final String USERNAME = "root";
```

(그림 12) 하드코딩 취약점[16]
(Figure 12) Hard coding vulnerabilities[16]

따라서 전력화 되는 무인체들에 대해 도입 단계에서부터 개방된 포트 취약점, 하드코딩 취약점 등 식별된 무인체의 취약점에 대한 검증이 필요하다

5. 방 안

현재까지 3장과 4장에서 분석한 Army TIGER 기반 전투체계와 드론봇전투체계를 활용한 유·무인 복합전투수행방안 분석을 통하여 장차 다양한 사이버위협에 대응 가능한 Army TIGER 체계구축을 위한 사이버방호체계 구축, 사이버작전 조직 보강, 사이버작전 지원, 제대별 『사이버 방호체계』 운용개념의 4개 분야에 대한 기술적 제언을 하고자 한다.

5.1 사이버방호체계 구축

Army TIGER 체계의 전력화는 전투수행방법과 육군의 무기체계 변화가 가장 큰 특징으로 분석 될 수 있다. 다양한 체계의 전력화 장비들은 육군의 미래형 전투체계 구현을 위해 현재 운용중인 네트워크에 연결되어 다양한 정보를 생산, 전송, 공유하게 될 것이다. 따라서 드론, 로봇, 무인차량, 개인전투체계 등 모든 장비와 체계에 대해 도입단계에서부터 통신방식, 생산 데이터 등에 대해 분석이 필요하고 또한 네트워크보호, 서버보호 영역의 사이버방호체계에 대해 사이버작전수행지침에 명시된 구축 기준을 대대급까지 확대 적용이 필요 할 것으로 판단된다. 지금까지는 육군에서 운용중인 사이버방호체계를 확대 적용하여 사이버위협에 대응하기 위한 방안이며, Army TIGER 전력화 체계의 모든 장비에 대한 네트워크화로 집중되는 데이터의 보호를 위한 방안검토도 필요하다. 현재 육군에서 운용중인 전장관리체계 외에 Army TIGER 전력화에 따라 추가되는 서버군이 운용되는 네트워크의 전체 영역에 대한 사이버방호체계 도입이 필수적인 것으로 판단된다.

5.2 사이버작전 조직 보강

현재 육군의 Army TIGER 체계는 대대급에서 여단급까지의 변화에 집중하고 있으며, 사단급 이상 제대의 편제 및 구조는 현재 추가 연구가 진행중이다. 따라서 본 논문에서는 여단급 이하 제대의 편제 및 구조 중심으로 연구 및 기술하였다. 현재 Army TIGER 체계가 전력화되는 여단급 이하 제대에는 사이버직책이 미편성되어 있어서 사이버 전문특기 인력 추가 운용이 필요하다. 사단급까지는 사이버방호실 기능이 편성되어 운용되고 있으나 여단급 이하 제대에는 아직까지 사이버 기능을 통신부서에서 담당하고 있는 현실이다. 사이버방호체계의 직접적인 운용이 없다 하더라도 영상전송, 저장, 네트워크 연결이 예상되는 Army TGIER 전력화 체계들에 대한 End-Point 취약점 관리를 위한 전술제대급 사이버인력의 편성이 필요할 것으로 판단된다. 또한 전력화 체계를 도입하는 단계에서 사이버위협 및 취약점을 해소 할 수 있도록 취약점 진단팀을 사업관리부서에 편성하는 방법도 고려가 가능하다.

5.3 사이버작전 지원

사이버작전 지원은 다양한 전력화체계의 도입으로 변화되는 모습에 포함되어야 하는 분야를 제언하고자 한다. 다양한 전력화 체계 도입으로 정보통신 기능에서는 사이버, 통신운용, 통신중계드론 운용 등 추가적인 임무가 발생하게 된다. 하지만 현재 타 전투기능의 비약적 발전에 비해 전력화중인 Army TIGER 체계를 지원하기 위한 기능의 변화는 미비하다. 조직의 확대는 미반영된 상태로 사이버작전, 통신중계드론의 운용 및 관리 임무가 추가될 것으로 예상되며, 위 업무를 원활히 수행하기 위해서는 사이버작전과 드론운용을 동시에 임무수행 가능한 전술용 지원차량의 도입도 고려되어야 할 것이다.

부대별 드론 관제차량을 활용시 드론의 정비 및 이동, 정비가 가능하고 드론관제 시스템을 활용, 사이버작전과 관련된 관제도 동시에 임무수행 가능 할 것으로 판단된다.

(그림 13) 드론 관제용 차량 및 내부시스템[23]
(Figure 13) Cyber & Drone Control Vehicle and Internal System[23]

5.4 『사이버방호체계』 제대별 운용개념 정립

사이버방호체계 운용개념은 현재 전력화중인 Army TIGER 부대의 최종 모습에 따라 변화 될 수 있다.

그러나 전력화 이후 운용개념 정립시 사이버방호체계가 정상기능을 수행하지 못하는 상태로 적의 사이버위협에 노출될 수 있다. 이에 현재 구상 가능한 제대별 운용방안을 제시하고자 한다. 첫 번째 군단급 통합운용 방안으로 군단급 통합 운용방식은 Army TIGER 전력화체계가 도입되는 모든 제대를 군단 단위로 통합하여 관제, 위협대응을 수행하는 방안으로 현 육군의 모습과 유사하나 Army TIGER 전력화 체계에 대한 전문 대응인원의 추가 편성이 필요할 것이다. 두 번째 여단급 독립 운용 방안은 사이버 인력의 추가 편성을 통해 여단단위 자체 관제 및 위협대응 능력을 보강하는 방안이다. Army TIGER 전력화로 각 부대는 기동화되며, 독립작전이 가능한 형태로 변화하고 있어 상급부대와의 통신을 위한 네트워크 변화가 잦을 것으로 판단된다. 이는 실시간 로그전송 및 분석의 제한을 뜻하며, 이를 보완하기 위해 여단급 부대 사이버 인력 보강이 필수적이다. 이를 통해 여단급 부대에 실시간 관제 및 위협대응 능력을 보강시 현재 Army TIGER 전력화가 진행중인 부대에 사이버위협 대응능력이 더욱 강화될 것으로 판단된다.

6. 결 론

결론적으로, 육군의 전력화가 진행중인 Army TIGER 전력화 체계들에 대한 네트워크, 의사결정체계, 각종 데이터에 대하여 다양한 사이버위협에 대응 가능한 사이버방호체계 구축과 조직보강은 필수적인 과제이며, 이를 위한 지속적인 기술연구 및 소요검토가 절실한 시점에 와있다. 군이 이를 체계적으로 추진하기 위해서는 Army

TIGER 전력화를 담당하는 책임부서에서 전투수행방법 연구 및 무기체계별 전투실험과 병행한 제대별 사이버방호체계 구축 및 각 무기체계별 사이버침해 유형별 작전적 영향성 분석을 위한 추가적인 사이버분야 전투실험과제 선정 및 전투실험 데이터 분석이 필요한 상황이다.

본 논문은 현재까지 육군이 전력화중인 Army TIGER 전력화체계를 대상으로 구조 및 특성 분석을 실시하였고, Army TIGER 전력(3대 전투체계) 중 Army TIGER 기반전투체계와 드론봇 전투체계에 대한 분석을 통하여 미래 사이버위협에 제대별로 대응이 가능한 『Army TIGER 사이버 방호체계』에 대한 도입의 필요성과 사이버보안 기술을 제시하였다. 이 논문을 바탕으로 더욱 고도화 되는 적 사이버위협에 보다 신뢰성 있고 생존성 있는 Army TIGER 전력화체계가 구축되기를 기대한다.

참고문헌(Reference)

[1] 보안뉴스, “범세계적 사이버 보안 위협 극복방안은? ‘민관협력’과 파트너국가간 소통”, 23.7.17, https://m.boannews.com/html/detail.html?idx=120145

[2] 육군본부 사이버작전센터, 사이버작전수행지침

[3] 육군본부, Army TIGER 종합발전 실행계획

[4] 국방일보, “육군 아미타이거 부대 통합 네트워크 구축 속도 낸다,” 23.7.13. https://www.mnd.go.kr/cop/kookbang/kookbangIlboView.do?categoryCode=dema0004&boardSeq=35434&id=mnd_020102000000

[5] 김귀근, “백두산 호랑이 상징 AI 지상전투체계 시동,”연합뉴스, 2018. https://www.yna.co.kr/view/AKR20180930041500001

[6] 한국과학기술정보연구원, “최신 사이버위협 동향 및 대응 방안 분석,” https://doi.org/10.22810/2018KRR016

[7] Junseob Kim, Sangjun Park, Jinho Cha, Yongchul Ki, ″Future tactical communication system development plan through Army TIGER information distribution capability analysi″, Journal of Convergence for Information Technology, Vol. 21, No. 4, PP. 23-30, 2021. https://doi.org/10.22156/CS4SMB.2021.11.06.014

[8] 뉴스투데이, “공군, 차세대 사이버방어 기술 MTD 적용한 운영시험 성공”, 22.9.29., https://www.news2day.co.kr/article/20220929500028

[9] 방위산업청, “첨단과학기술을 활용한 미래무기 무인·로봇 체계-미래무기 Part1”, 2017.6.20., https://m.blog.naver.com/dapapr/221033207078

[10] 무인이동체 드론의 취약점분석 및 대응기술 연구 동향, 정보보호학회지, Vol. 30, No. 2, PP.49-57, 2020. https://scienceon.kisti.re.kr/commons/util/originalView.do?cn=JAKO202013965595426&oCn=JAKO202013965595426&dbt=JAKO&journal=NJOU00291864

[11] Arteaga, S. P., Hernández, L. A. M., Pérez, G.S., Orozco, A. L. S., and Villalba, L. J. G., “Analysis of the GPS Spoofing Vulnerability inthe Drone 3DR Solo,” IEEE Access, Vol. 7, pp. 51782-51789, 2019. https://doi.org/10.1109/ACCESS.2019.2911526

[12] Dey, V., Pudi, V., Chattopadhyay, A., and Elovici, Y., “Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study,” 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), IEEE, pp. 398-403, 2018. https://doi.org/10.1109/VLSID.2018.97

[13] Son, Y., Noh, J., Choi, J., and Kim, Y., “Gyrosfinger: Fingerprinting drones for location tracking based on the outputs of mems gyroscopes.” ACM Transactions on Privacy and Security (TOPS), 21.2, 1-25, 2018. https://doi.org/10.1145/3177751

[14] Son, Y., Shin, H., Kim, D., Park, Y., Noh, J Choi, K., and Kim, Y., “Rocking drones with intentional sound noise on gyroscopic sensors, In 24th {USENIX} Security Symposium ({USENIX} Security 15), pp. 881-896., 2015. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son-updated.pdf

[15] Westerlund, O., and Asif, R., “Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things,” 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS). IEEE, pp. 1-10., February 2019. https://doi.org/10.1109/UVS.2019.8658279

[16] Kim, D., and Kim, H. K., “Security Requirements of Commercial Drones for Public Authorities by Vulnerability Analysis of Applications,” 2019. https://doi.org/10.48550/arXiv.1909.02786

[17] Nunez, J., Tran, V., and Katangur, A., “Protecting the Unmanned Aerial Vehicle from Cyberattacks,” In Proceedings of the International Conference on Security and Management (SAM), The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). pp. 154-157, 2019.
https://www.proquest.com/openview/444cac98c1c13da04b8d796e175ed3b6/1.pdf?pq-origsite=gscholar&cbl=1976342

[18] Kwon, Y. M., Yu, J., Cho, B. M., Eun, Y., and Park, K. J., “Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles,” IEEE Access, 6, 43203-43212, 2018.
https://doi.org/10.1109/ACCESS.2018.2863237

[19] Vasconcelos, G., Carrijo, G., Miani, R., Souza, J., and Guizilini, V., “The impact of DoS attacks on the AR. Drone 2.0,” In 2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR) IEEE., pp. 127-132., October 2016.
https://doi.org/10.1109/LARS-SBR.2016.28

[20] Bonilla, C. A. T., Parra, O. J. S., and Forero, J. H. D., “Common security attacks on drones,” International Journal of Applied Engineering Research, 13(7), 4982-4988, 2018.
https://www.ripublication.com/ijaer18/ijaerv13n7_51.pdf

[21] Domin, K., Symeonidis, I., and Marin, E. “Security analysis of the drone communication protocol: Fuzzing the MAVLink protocol,” 2016.
https://www.esat.kuleuven.be/cosic/publications/thesis-284.pdf

[22] Rodday, N. M., Schmidt, R. D. O., and Pras, A. “Exploring security vulnerabilities of unmanned aerial vehicles,” NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium,, IEEE, pp. 993-994, April 2016,
https://doi.org/10.1109/NOMS.2016.7502939

[23] 동아일보, “규제와 규제개혁사이 나는 드론과 쫓는 규제”, 2017.8.4. https://www.donga.com/news/It/article/all/20170804/85682209/1

◐ 저 자 소 개 ◑

박 병 준(Byeong-jun PARK)
1990년 육군사관학교 컴퓨터공학과(공학사)
1996년 미군 해군대학원 시스템공학(공학석사)
2015년~2016년 국군 사이버작전사령부 500센터장
2019년~현재 교육사령부 육군정보통신학교 사이버/C4I학처 학처장
관심분야 : AI/빅데이터 분석, 사이버보안 기술, 침해조사·분석
E-mail : goodman6446@yahoo.com

김 철 중(Cheol-jung KIM)
2004년 관동대학교 컴퓨터공학과(공학사)
2008년~2009년 국군 간호사관학교 교양학과 전산학교수
2015년 아주대학교 정보통신대학원 정보보호/C4I학과(공학석사)
2022년~현재 교육사령부 육군정보통신학교 사이버/C4I학처 운영체제보안교관
관심분야 : 시스템보안, Drone
E-mail : lfordeath9484@gmail.com