Journal of the Korea Academia-Industrial cooperation Society
Vol. 23, No. 5 pp. 272-278, 2022

https://doi.org/10.5762/KAIS.2022.23.5.272
ISSN 1975-4701 / eISSN 2288-4688

사이버전무기체계 기술의 연구개발 동향 및 발전 방향

김민욱
국방기술진흥연구소

R&D Trend and Development Direction of Cyber Warfare Weapon System Technology

Minuk Kim
Korea Research Institute for Defense Technology Planning and Advancement

요 약 사이버전무기체계는 사이버 위협으로 부터 아군의 정보체계를 보호하고 사이버 공간에서 우위를 달성하기 위해 사용하는 무기체계이다. 최근 사이버전무기체계는 적국의 발전소, 금융기관 등의 기반시설에 막대한 피해를 초래할 수 있는 강력한 비대칭 전력으로 평가 받고 있으며, 이로 인해 사이버전장의 적 사이버공격을 효율적으로 대처·차단하고 아군의 자산을 보호하기 위한 사이버전무기체계 기술개발의 중요성이 점점 더 부각되고 있다. 본 논문에서는 국내 사이버전무기체계에 대한 분류 및 사이버전 기술의 분류를 살펴본 후 국내·외 사이버전무기체계 기술의 연구개발 동향을 조사·분석한다. 또한, 앞서 조사·분석한 사이버보안, 인공지능, 빅데이터, 운영기술 보안 등 여러 분야의 기술과 융합된 다양한 사이버전무기체계 기술의 국내·외 연구개발 동향 비교분석을 통하여, 사이버전무기체계 적용 인공지능 모델 보안과 무기체계 운영기술 보안이라는 국내 사이버전무기체계 기술의 연구개발 발전 방향을 제시한다.

Abstract The cyber warfare weapon system is used to protect the information of South Korean forces from cyber threats and achieve superiority of the forces in cyberspace. Recently, the cyber warfare weapon system of South Korea has been evaluated as a strong asymmetric power that can cause enormous damage to infrastructures, such as power plants and financial institutions, in enemy countries. In addition, the importance of developing cyber warfare weapon system technologies to efficiently cope with and block enemy cyber attacks has also been highlighted in the evaluation. This research examined the classification of the South Korean cyber warfare weapon system and related technologies and the research and development (R&D) trends of the South Korean and international cyber warfare weapon system technologies. In addition, this research compared and analyzed the South Korean and international R&D trends of various cyber warfare weapons system technologies fused with technologies of various other fields, such as cybersecurity, artificial intelligence, big data, and operational technology security. Subsequently, this research presented the R&D direction of South Korean cyber warfare weapon system technologies, such as the security technologies for the artificial intelligence model applied to cyber warfare weapon systems and weapon system operations, based on the comparison and analysis made.

Keywords : Cyber Warfare, Weapon System, Cyber Warfare Weapon System, Cybersecurity, Artificial Intelligence, Core Technology

*Corresponding Author : Minuk Kim(Korea Research Institute for Defense Technology Planning and Advancement)
email: kimminuk@krit.re.kr
Received April 6, 2022 Revised April 26, 2022
Accepted May 6, 2022 Published May 31, 2022

1. 서론

현대의 전장 환경은 기존의 육·해·공 중심의 전장에서 Fig. 1과 같이 사이버 공간으로 영역이 확장되고 있으며, 미래 사이버전장은 과학기술의 발전 및 4차 산업혁명의 중심 기술로 떠오른 인공지능, 빅데이터 등의 기술 발전에 힘입어 더욱 다각화된 방식의 사이버 공격이 증가할 것으로 예상된다. 이에 따라 미래 사이버전장의 적 사이버공격을 효율적으로 대처·차단하고 아군의 자산을 보호하기 위한 사이버전무기체계 기술개발의 중요성이 점점 더 부각되고 있다.

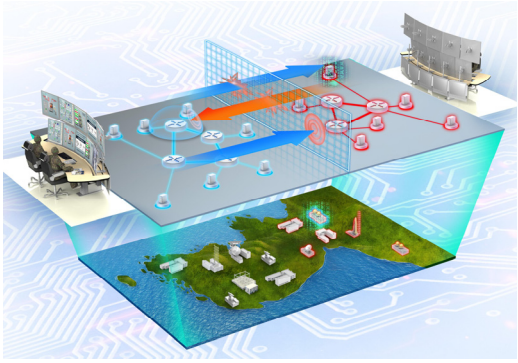

Fig. 1. Operational Concept for Cyber Warfare Weapon Systems[1]

국방과학기술조사서에 의하면 사이버전무기체계란 적의 사이버위협으로부터 아군의 정보체계를 보호하고 사이버 공간에서 우위를 달성하기 위해 사용하는 무기체계로 사이버 공격이나 방어에 사용되는 하드웨어 및 소프트웨어로 예방·감시·탐지·차단·복구·공격·대응 등 활동단계별로 다양한 기능이 포함된 무기체계를 의미한다.

임무별로 분류하면 아래 Table 1과 같이 사이버 공간의 위협을 감시·정찰하고 정보화 하는 작전을 수행하는 사이버감시정찰체계, 사이버작전 임무를 수행하기 위하여 작전을 계획·지시·통제하는 사이버지휘통제체계, 능동적인 방어 작전을 수행하는 사이버능동방어체계의 3가지 임무를 통합하는 체계인 사이버전장관리체계와 사이버 수단으로 적 사이버 표적을 교란·마비·파괴시키는 작전을 지원하는 사이버공세적대응체계, 사이버작전 훈련을 위한 사이버 훈련체계로 구성된다[1].

Table 1. Classification of Cyber Warfare Weapon Systems

Classification and Mission	
Cyber Battlefield management system	Cyber ISR
	Cyber C2
	Cyber APS
Cyber Offensive Response System	
Cyber Training System	

국방과학기술 표준분류체계에 의하면 사이버전 기술은 8개 대분류 중 하나인 정보통신 기술 분야의 하위에 위치하고 있으며, 사이버전 기술의 세부 하위 기술들은 아래 Table 2와 같이 사이버무기, 정보체계마비, 통신망마비, 인증/접근통제, 암복호화, 침입예방, 침입탐지/대응, 피해복구/침해감내 기술로 구성되어 있다[2].

Table 2. Classification of Cyber Warfare Weapon System Technologies

Technology	Sub-Technologies
Cyber Warfare	Cyber Weapons
	Information System Paralysis
	Network Paralysis
	Authentication / Access Control
	Encryption and Decryption
	Intrusion Prevention
	Intrusion Detection / Response
	Damage Recovery / Tolerance

본 논문에서는 아래 Fig. 2와 같이 국외와 국내의 대표적인 사이버전무기체계 기술의 연구개발 동향을 조사하고, 개발동향의 비교·분석을 통해 미래의 전장 환경에 부합하는 국내 사이버전무기체계 기술의 발전 방향을 제시한다.

Fig. 2. Research Process Conceptual Diagram

2. 사이버전무기체계 기술 국외·국내 연구개발 동향

2.1 국외 연구개발 동향

하버드 케네디 공공정책대학원 벨퍼센터에서 발표한 국가사이버전력지수(NCPI: National Cyber Power Index)에 의하면 미국의 사이버전 능력은 세계 1위로 평가 되고 있으며, 사이버 인텔리전스, 감시정찰, 방어, 공격 등 모든 분야에서 높은 역량을 보유하고 있는 것으로 확인된다[3]. 미국은 사이버무기체계 기술의 연구개발에서도 선도적인 역할을 수행하고 있으며, 미 국방부고등연구계획국(DARPA: Defense Advanced Research Projects Agency, 이하 DARPA)을 중심으로 사이버무기체계에 적용 가능한 다양한 프로그램들의 연구개발을 수행 하고 있다.

연구개발이 완료된 DARPA의 프로그램과 연구개발이 진행 중인 프로그램 중 사이버전무기체계에 적용이 가능할 것으로 판단되는 프로그램의 목록은 각각 아래 Table 3, Table 4와 같다.

Table 3. Completed Darpa Programs Applicable to Cyber Warfare Weapon Systems[4]

Programs	Related Technology Keywords
ACD	Cybersecurity
AIMEE	Cybersecurity, AI
APAC	Cybersecurity
CRASH	Cybersecurity
CFAR	Cybersecurity
EdgeCT	Cybersecurity, Edge Networking
XD3	Cybersecurity, Networking
HACMS	Cybersecurity, OT Security
ICAS	Cybersecurity
MRC	Cybersecurity
PROCEED	Cybersecurity
QED for RML	Cybersecurity, Machine Learning, AI
STAC	Cybersecurity
Transparent Computing	Cybersecurity
VET	Cybersecurity

Table 4. Ongoing Darpa Programs Applicable to Cyber Warfare Weapon Systems[5]

Programs	Related Technology Keywords
ASED	Cybersecurity, Social Engineering
AISS	Cybersecurity, Secure Chip
CHESS	Cybersecurity, Human-Computer Collaboration
CASE	Cybersecurity, OT Security, Embedded System Security
CHASE	Cybersecurity, Big Data
Enhanced Atrribution	Cybersecurity, Big Data
HARDEN	Cybersecurity, AI
HACCS	Cybersecurity, AI
MICE	Cybersecurity, AI
RADICS	Cybersecurity
SHEATH	Cybersecurity
SMOKE	Cybersecurity

DARPA는 실시간, 광대역 동적 네트워크 환경에서 군이 사이버 전장과 사이버작전을 직관적으로 이해·계획하고 효과적으로 관리할 수 있도록 하는 시스템 프레임워크인 『Plan X』, 사이버보안에 취약한 호스트를 개선하여 보안에 강력한 차세대 호스트 설계방식을 연구하는 『CRASH』, 군 클라우드 네트워크 환경의 보안위험에 효과적으로 대응하기 위해 클라우드 네트워크 공격을 탐지하고 대응하는 기술인 『MRC』, DDoS 공격에 대한 복원력 향상 기술을 개발하는 『XD3』 등 다수의 사이버보안 기술 분야 프로그램들의 연구개발을 수행하였으며[6], 운영기술(OT : Operational Technology, 이하 OT) 보안, 인공지능, 사회공학, 빅데이터 등의 다양한 기술 분야와 융합된 사이버보안 기술의 연구개발 프로그램들이 증가하고 있는 추세이다.

사이버영역과 물리영역의 연결성이 점차 증가함에 따라 무기체계 OT 보안의 중요성이 증대되고 있으나, 기존의 사이버전무기체계에 적용되는 전형적인 사이버보안 기술만으로는 무기체계 OT 영역에 대한 악의적 행위자의 공격에 대응하기에는 부족하다. DARPA는 이러한 무기체계 OT 보안 영역의 기술공백을 해소하기 네트워크로 연결된 임베디드 시스템의 취약성을 보완하기 위한 사이버-물리 융합 시스템을 개발하는 『HACMS』프로그램의 연구개발을 수행하였으며, Fig. 3과 같이 임베디드 컴퓨팅 시스템의 사이버 복원력을 개선하기 위한 설계,

분석 및 검증 도구를 개발하는 『CASE』프로그램의 연구개발을 진행 중이다.

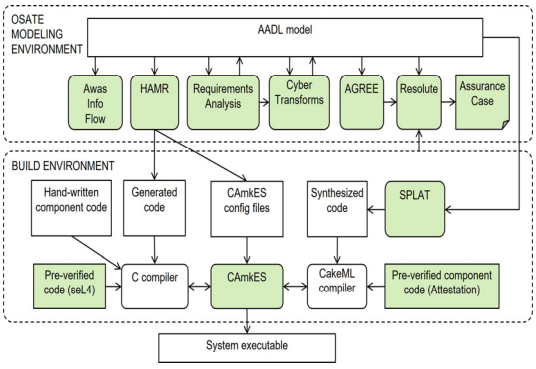

Fig. 3. Architecture of the BriefCASE tool as part of the CASE Program[7]

또한, 공격자 활동에 대한 가시성을 제공하여 악의적인 공격자들의 운영 및 전술 관련 정보를 생성하기 위한 기술, 도구 및 정보를 공유하기 위한 『Enhanced Attribution』, Fig. 4와 같이 컴퓨터와 인간이 소스 코드 및 컴파일 된 바이너리와 같은 소프트웨어 아티팩트에 대한 공동 추론을 통해 모든 유형의 취약성을 발견하고 해결하는 기능을 개발목표로 하는 『CHESS』, 새로운 공격 벡터를 탐지 및 특정화하고, 올바른 상황 별 데이터를 수집하고, 보호 구역 전체에 보호 조치를 전파하는 자동화 도구를 개발하는 『CHASE』, 악성 봇넷 이식 및 대규모 악성 코드에 효과적으로 대응할 수 있는 자율 소프트웨어 에이전트를 개발하기 위한 『HACCS』 등 인공지능, 빅데이터, 사이버보안 등의 다양한 기술 분야가 융합된 연구개발 프로그램을 진행 중이다.

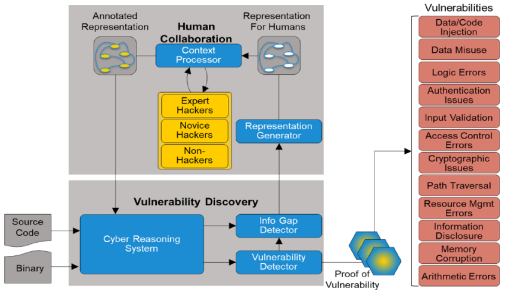

Fig. 4. CHESS System Overview[8]

호주의 DST는 사이버 취약점 발견을 위한 딥러닝 연구를 수행하였으며, 독일의 ZITis 는 사이버공격 조기 탐지를 위한 인공지능 연구 프로젝트인 KISTRA를 수행하고 있다. 또한, 네덜란드의 TNO는 사이버전 훈련의 레드팀, 블루팀의 활동을 개선하기 위한 기계학습 피드백 루프를 개발하고 구현하는 Purple AI 개발 프로젝트를 수행하는 등 미국 이외의 국가들 또한 인공지능, 빅데이터 등 4차 산업혁명 중심기술을 적용한 다양한 사이버무기체계 기술의 연구개발을 수행하고 있다[9].

2.2 국내 연구개발 동향

국내에서는 사이버전무기체계 적용에 필요한 기술을 사전에 확보하기 위하여 국방연구개발의 사업 형태 중 하나인 핵심기술 연구개발 사업을 통해 다양한 사이버전무기체계 기술의 연구개발을 수행 하고 있다.

과거 국내의 사이버전무기체계 핵심기술 연구개발은 대부분 국방과학연구소 주관으로 진행되었으며, 인터넷에 공개된 핵심기술 과제 제안서 공모문, 위탁연구 수행기관 선정을 위한 공모문 등의 정보를 바탕으로 사이버 공간의 객체이동 및 침입감내 기술, 사이버전 효과분석 및 검증기술, 머신러닝 기반의 모의 데이터 생성 기술, 사이버 공방 시험기법, 멀티레이어드 사이버작전 상황도 구축 기술 등의 다양한 사이버전무기체계 기술의 연구개발이 수행되었음을 추측할 수 있다. 현재는 민간시장의 기술이 성숙됨에 따라 국방과학연구소뿐만 아니라 산·학·연 주관의 사이버전무기체계 기술의 핵심기술 연구개발 또한 점차 증가되고 있는 추세이다.

국내 사이버전무기체계 기술의 연구개발 또한 해외 선진국들과 마찬가지로, 4차 산업혁명의 중심기술인 인공지능, 딥러닝, 빅데이터 등의 기술을 적용한 연구개발이 진행되고 있다.

방위사업청이 2021년 발간한 '21-'35 핵심기술기획서 일반본에 의하면 현재 연구개발이 진행 중이거나 미래에 연구개발이 진행될 예정인 사이버전무기체계 핵심기술과제의 목록을 아래 Table 5와 같이 확인 할 수 있다.

최근에는 산·학·연 주관의 연구개발 과제인 『초지능형 사이버 지휘통제 및 능동대응 기술』과, 『사이버전 레드팀/블루팀 자동화 기술』이 착수되어 연구개발 진행 중에 있다.

『초지능형 사이버 지휘통제 및 능동대응 기술』은 산·학·연 주관으로 연구개발이 수행되고 있으며, 사이버전장 환경을 제공하기 위해 사이버 악성봇 공격 및 사이버 위협의 빠른 확산 방지를 위하여 인공지능 기반 분석을 통해 사이버 위협 상황을 인지하고 능동적으로 대응하는 기술을 확보하는「사이버전장 공격 확산 방어용 사이버 위협 상황인지기반 능동대응 기술」, 사이버 자산정보 및

Table 5. Core Technology Programs Applicable to Cyber Warfare Weapon Systems[10]

No.	Programs
1	Secure SW Design Verification Technology
2	High-Reliability Self-Healing System Technology
3	Public Information-Based Enemy Cyber Information Detection and Target management Technology
4	Normal and Treat Traffic Analysis Technology Based on Deep Learning
5	Weapon System HW Hidden Malicious Function Detection Technology
6	Cyber Asset Search Technology
7	Cyber Warfare TTP Automatic Development Technology
8	Research on Technology to Respond Hidden Intrusion Attacks
9	Anonymous Network Use Attacker Tracking Technology
10	Defense Cyber Attack Tracking Technology
11	Intrusion Tolerance Technology to Respond to Network Attacks
12	Cyber Warfare Simulation Combat Technology
13	System Secret Penetration and Mission Performance Technology
14	Intelligent Intrusion Inference and Cyber Threat Analysis Technology
15	Cyber Warfare Training Red Team/Blue Team Automation Technology
16	Mission Impact Analysis Technology by Cyber Warfare
17	Integrated Cyber Situational Awareness and Analysis Technology in Preparation for Targeted Attacks
18	Honeypot-Based Attack Pattern DNA Extraction Cybergenomic Technology
19	Hyper Intelligent Cyber C2 and Active Response Technology

사이버 위협정보를 자동으로 수집/분석하고 군 사이버 작전 간 식별 및 경보 되는 공격 시도 및 침투 활동에 대한 대응 프로세스 자동화를 지원하는 기술을 확보하는 「빅데이터/인공지능기반 군 사이버 위협 탐지 및 대응방책 지원 기술」, Fig. 5(a)와 같이 사이버 공격의 대상이 되는 시스템(보호대상)의 주요 속성을 능동적으로 보호함으로써 공격자의 분석 복잡도와 공격목표 선정의 불확실성을 증폭시켜 공격의 준비 및 시도를 사전에 무력화하는 능동적인 사전 보안기술을 확보하는 「네트워크 추적 및 데이터 유·노출/훼손 공격 능동 방어 기술」, 사이버 전장 환경을 OT 영역으로 확대한 훈련환경 구성 기술, 사이버 전장 환경의 가시화 기술, 빅데이터/인공지능을 기반으로 훈련결과를 분석·평가하는 기술을 확보하는 「지능형 사이버 훈련 기술」, Fig. 5(b)와 같이 사이버 지휘통제 및 능동대응 핵심 인공지능 모델에 대한 정보유출/데이터오염/모델기만 위협에 대응하기 위하여 인공지능 모델에 대한 취약성을 분석하고, 인공지능 입력 데이터/패킷에 심층 검사를 통해 공격을 탐지하고 차단하는 기술 확보하는 「사이버전장관리 인공지능 모델 보안 기술」의 확보를 목표로 한다[11].

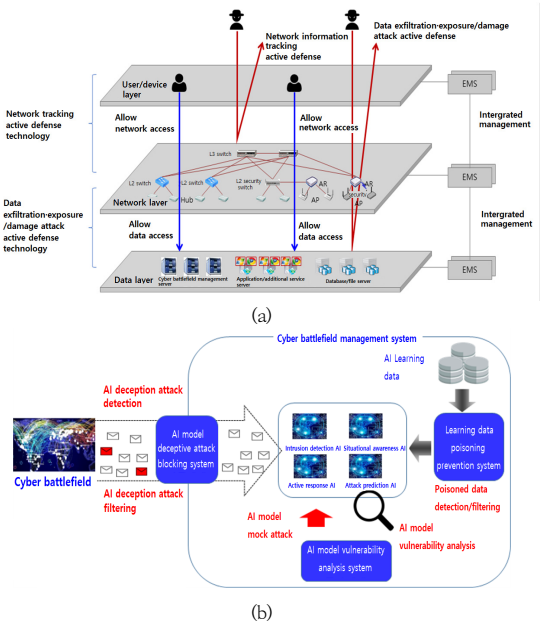

Fig. 5. Hyper Intelligent Cyber C2 and Active Response Technology Conceptual Diagram[11]
(a) Network tracking and data leakage·exposure/damage attack active defense technology (b) Cyber battlefield management artificial intelligence model security technology

『사이버전 레드팀/블루팀 자동화 기술』은 산·학·연 주관으로 연구개발이 수행되고 있으며, 사이버전 훈련에서 공격과 방어를 자동화함으로써 사이버전 훈련의 수준향상과 훈련의 일관성을 보장하고 사이버전 전술 개발을 지원하기 위한 기술의 개발을 목표로 한다[12].

이외에도, 사이버전의 공격 대상이 되는 무기체계(내장형) SW 개발에 설계보안 기술을 접목함으로써, 설계단계에서 보안성 및 SW 안정성을 위해 적용되어야 하는 기술/기법과 더불어 무기체계 SW의 설계보안에 대한 검증기술 연구개발 하는 『Secure SW 설계검증 기술』, 적 사이버 상황 정보 획득을 위하여 인터넷 등의 공개정보를 기반으로 정보를 수집하고 적의 사이버 정보를 분석 및 관리하는 기술을 개발하는 핵심기술 과제인 『공개정보기반 적 사이버정보 탐지 및 표적관리 기술』, 무기체계로부터 발생하는 정상 트래픽과 악성코드로부터 발생하

는 위협 트래픽을 학습하여 통합 딥러닝 모델을 구축하고, 구축된 모델을 이용하여 입력 트래픽에서 잠재적 위협 트래픽을 식별하고 종류를 분석하는 과제인 『딥러닝 기반의 정상 및 위협 트래픽 분석 기술, 인터넷 공간에서 통신 프로토콜을 통해 외부 사이버 자산(서버, 라우터, 스위치 등) 관련 정보를 자동으로 수집하고 사이버 자산에 대한 모델링 및 추론을 통해 외부 사이버 자산에 대한 정보를 분석 및 관리하는 과제인 『사이버 자산 검색 기술』 등 다양한 사이버전무기체계에 적용이 가능한 핵심 기술들의 연구개발이 국방과학연구소 및 산·학·연 주관으로 예정되어 있다.

3. 사이버전무기체계 기술 발전방향

앞서 살펴본 국외·국내 연구개발 동향에 의하면 사이버전무기체계에 적용하기 위한 다양한 기술들의 개발이 진행되고 있으며, 특히 인공지능 기술, OT 보안 기술과 융합된 형태의 사이버전무기체계 기술의 연구개발이 증가하고 있는 추세이다.

3.1 사이버전무기체계 인공지능 모델 보안

현대에는 인공지능 기술이 다양한 분야와 융합되면서 인공지능 자체에 대한 위협이 증가하고 있으며, 이에 대응하기 위해 MITRE는 Microsoft, IBM등과 협업하여 인공지능 시스템에 대한 적대적 위협 환경(ATLAS : Adversarial Threat Landscape for Artificial-Intelligence Systems)을 발표하는 등 인공지능 보안에 대한 중요성이 부각되고 있다.

국외뿐만 아니라, 국내에서도 다양한 사이버전무기체계 기술에 인공지능을 적용한 연구가 진행되고 있지만, 사이버전무기체계 기술에 적용되는 인공지능에 대한 보안기술의 연구개발은 『초지능형 사이버 지휘통제 및 능동대응 기술』의 세부 과제인 「사이버전장관리 인공지능 모델 보안 기술」 1건으로 부족한 것으로 확인되어 사이버전무기체계 적용 인공지능 모델에 대한 보안을 향상시키기 위한 기술의 추가적인 연구가 필요하다.

3.2 무기체계 OT 보안

미래 전장에서는 기존의 독립망에서 운용되는 무기체계의 연결성이 점차 증가하면서 OT 보안의 중요성이 증대될 것으로 예측된다. 이에 국외뿐만 아니라 국내에서도 무기체계 OT 보안의 중요성이 인식되어 무기체계 소프트웨어의 설계보안에 대한 검증기술을 연구개발 하는 『Secure SW 설계검증 기술』, 하드웨어 구성코드로부터 무기체계 시스템에 대한 사이버 위협의 원인이 되는 악성기능을 탐지하기 위한 기술을 개발하는 『무기체계 HW 은닉 악성기능 탐지기술』 등의 무기체계 OT 보안을 강화하기 위한 연구개발들이 예정되어있다.

하지만, 기동·함정·항공·유도무기 등 다양한 분야의 무기체계는 각각의 운용 환경에 따라 필요한 OT 보안 기술이 상이할 것으로 예상되어 분야별로 적용할 수 있는 OT 보안 기술의 추가적인 연구개발이 필요하다.

4. 결론

우리는 초연결·초지능의 시대인 4차 산업혁명 시대에 살아가고 있으며, 이는 확장된 연결성으로 인해 사이버 보안 기술이 더욱더 중요해지고 있음을 의미한다. 이는 국방 영역에서도 마찬가지이며, 2022년 러시아·우크라이나 사태의 사이버전 확대에서도 알 수 있듯이 현대의 전장 환경은 육·해·공 중심의 전장 환경에서 새로운 전장인 사이버공간으로 이미 확장되었음을 알 수 있다.

본 논문에서는 미래 사이버전 환경에 부합하는 사이버전무기체계 기술의 연구개발 방향을 제시하기 위해 국외의 사이버전무기체계 기술의 연구개발 동향과 국내의 사이버전무기체계 기술의 연구개발 동향을 조사·분석 하였으며 이를 토대로 사이버전무기체계 인공지능 모델 보안, 무기체계 OT 보안이라는 두 개의 사이버전무기체계 기술 연구개발 방향을 제시하였다. 국내 사이버전무기체계 기술의 연구개발 추진 간 방향성 정립에 활용될 수 있기를 기대한다.

References

[1] Defense Agency for Technology and Quality, Defense Science and Technology Survey(Defense Science and Technology Development Trends) : Vol.2 C3 Weapon System, pp.98-100, Dec. 2019.

[2] Korea Research Institute for Defense Technology Planning and Advancement, Defense Technology Standard Classification, https://dtims.krit.re.kr/vps/OINF_searchStndList.do#none, Mar. 2022.

[3] Belfer Center, National Cyber Power Index 2020,

pp.11-12, Sep. 2020.

[4] Defense Advanced Research Projects Agency, Cyber, https://www.darpa.mil/tag-list?tag=Cyber, Mar. 2022.

[5] Defense Advanced Research Projects Agency, our research, https://www.darpa.mil/our-research, Mar. 2022.

[6] Defense Agency for Technology and Quality, Defense Science and Technology Survey(Defense Science and Technology Development Trends) : Vol.2 C3 Weapon System, pp.128-138, Dec. 2019.

[7] D. Cofer, I. Amundson,J. Babar, D. Hardin, K. Slind, "Cyber Assured Systems Engineering at Scale", IEEE Security and Privacy, p.5, Mar. 2022
DOI: https://dx.doi.org/10.1109/MSEC.2022.3151733

[8] System for Award Management, Computers and Humans Exploring Software Security (CHESS), https://sam.gov/opp/cb10b80125a2e1377f3920586d36b5c9/view, Mar. 2022.

[9] Korea Research Institute for Defense Technology Planning and Advancement, Defense Science & Technology Level Assessment, pp.166-193, Dec. 2021.

[10] Defense Acquisition Program Administration, '21-'35 General Copy of Core Technical Planning, pp.228-241, Mar. 2021.

[11] Korea Research Institute for Defense Technology Planning and Advancement, Request for Proposal of Hyper Intelligent Cyber C2 and Active Response Technology, https://dtims.krit.re.kr/vps/OINF_CtPrjNotiList.do, Mar. 2022.

[12] Korea Research Institute for Defense Technology Planning and Advancement, Request for Proposal of Cyber Warfare Training Red Team/Blue Team Automation Technology, https://dtims.krit.re.kr/vps/OINF_CtPrjNotiList.do, Mar. 2022.

김 민 욱(Minuk Kim) [정회원]

• 2016년 2월 : 경상국립대학교 항공우주 및 소프트웨어공학부 (학사)
• 2016년 1월 ~ 2020년 7월 : 퍼스텍(주) 선임연구원
• 2020년 9월 ~ 2020년 12월 : 국방기술품질원 연구원
• 2021년 1월 ~ 현재 : 국방기술진흥연구소 연구원

〈관심분야〉
국방기술기획, 정보통신