THE JOURNAL OF KOREAN INSTITUTE OF ELECTROMAGNETIC ENGINEERING AND SCIENCE. 2021 February.; 32(2), 119～126.

http://dx.doi.org/10.5515/KJKIEES.2021.32.2.119
ISSN 1226-3133 (Print) · ISSN 2288-226X (Online)

사이버전자전 기술 및 발전방향

Cyber Electronic Warfare Technologies and Development Directions

김소연 · 김성표 · 박범준 · 정운섭 · 추헌우* · 윤정* · 김진용*

Soyeon Kim · Seongpyo Kim · Beom Joon Park · Un Seob Jeong · Hunwoo Choo* · Jeong Yun* · Jinyong Kim*

요 약

미래 전장은 초연결 네트워크 전쟁이 될 것이다. 육 · 해 · 공 · 우주 공간이 주파수 스펙트럼으로 연결된 미래 전장에서 전자전(EW: electronic warfare)과 사이버전(CW: cyber warfare) 영역은 점차 더 중첩될 것이고, 이에 효과적으로 군사작전을 수행하기 위해서는 두 기술을 융합한 사이버전자전(CEW: cyber electronic warfare) 기술이 필요하다. 사이버전자전은 전자전의 원거리 고출력 전자파 송출능력과 사이버전의 정보(메시지) 조작/교란능력을 통합하여 시너지 효과를 발휘할 수 있는 기술이다. 본 논문은 전자전 입장에서 바라본 주파수 스펙트럼 확장과 사이버공간으로 전장영역 확대 추세에 따른 사이버전자전 기술에 대해 소개하고, 사이버전자전 발전방향에 대해 기술하였다.

Abstract

Future warfare will be on a hyper-connected battlefield. In the future battlefield where the domains of land, see, air, and space are connected by a frequency spectrum, electronic warfare and cyber warfare domains will gradually overlap, and to effectively perform military operations, a cyber electronic warfare technology that combines the two technologies is required. Cyber electronic warfare is a technology that can exert a synergistic effect by integrating the ability to transmit high-power electromagnetic waves from electronic warfare systems to long distances and the information manipulation/disruption ability of cyber warfare. This paper introduces cyber electronic warfare technologies according to the trend of expanding the frequency spectrum from the perspective of electronic warfare and expanding the battlefield to cyberspace, and describes the directions of the cyber warfare development.

Key words: Cyber Warfare, Electronic Warfare, Cyber Electronic Warfare, Network Centric Warfare

Ⅰ. 초연결 사회와 사이버

1-1 사이버 위협의 공격양상 발전전망

초연결 사회라는 말은 2008년 미국 IT 컨설팅회사 Gartner Inc.에서 처음으로 사용되었으며, 모든 객체와 공간이 네트워크화 되어 시 · 공간에 제약받지 않는 상호소통으로 새로운 가치화 혁신을 창출할 수 있는 사회를 의미한다. 그러나 초연결 사회는 불특정 다수의 고도 · 지능화된 사이버 위협이 폭발적으로 증가된 사회이기도 하다. 이는 사이버 위협 또한 초연결되기때문이다. 그림 1은 초연결 사회 핵심기술들과 더불어 여기에 기생하는 각종 사이버 위협 기술들을 보여준다[1].

특히, 최근에는 주파수/메시지 조작 등을 통해 사이버공간을 오염하던 사이버 위협에 의한 공격이 사이버 공

국방과학연구소(Agency for Defense Development)
*육군정보학교(Republic of Korea Army Intelligence School)
· Manuscript received November 16, 2020 ; Revised December 3, 2020 ; Accepted December 15, 2020. (ID No. 20201116-013S)
· Corresponding Author: Soyeon Kim (e-mail: comet613net@add.re.kr)

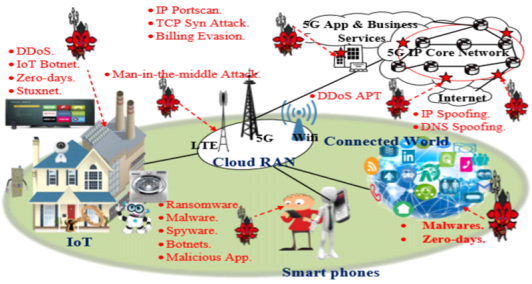


그림 1. 초연결 사회와 사이버 위협
Fig. 1. Hyper connected society and cyber threats.

간에만 국한되지 않고, 물리적 공격으로까지 진화되고 있는데 이는 그림 2와 같이 정리될 수 있다.

그림 2에서 알 수 있듯이, 사이버 위협의 교란대상과 공격수단은 “사이버 공간에 대한 정보탈취/오염을 위한 악성코드”에서 “물리적 공간에 대한 주요 시설 파괴, 핵심인물 암살을 위한 물리적 공격” 으로 발전되고 있다. 이는 물리적 공격으로 인한 파급효과가 훨씬 더 크기 때문이다. 물리적 사이버 위협의 대표적인 예로는 고정형 RC-IED(radio control improvised explosive device, 무선조정 급조폭발물), RC-IED 탑재 소형 드론, 미사일/공격무기 장착 중형급 이상 드론 등이 있다. 현재, 사이버 공간에 대한 공격 기술로는 사이버전 기술을 이용한 악성코드 전파 기술, 고정형 RC-IED 대응 기술로는 전자전 기술을 이용한 RC-IED 교란 기술, 폭발물 등을 장착한 소형급

Attack Method	Malware	Fixed RC-IED	Commercial drone	Military drone
Target	Cyber space (Infection)	Physical Facility/ Person (Destruction/ Assassination	Physical Facility/ Person (Destruction/ Assassination	Physical Facility/ Person (Destruction/ Assassination
Case	Stuxnet Infection(Iran)	Terror/Guerilla	Maduro Assassination Failure	Soleimani Assassination
Response Technology	Cyber warfare	Electronic warfare	Cyber electronic warfare	Intelligent cyber electronic warfare
	Current Trend		Future Trend	

그림 2. 사이버 위협 공격양상 진화
Fig. 2. Progressive attack trend of cyber threats.

드론 대응 기술로는 전자전 기술에 메시지조작 기술을 중첩하여 드론의 궤도이탈/추락유도를 야기시킬 수 있는 기초단계의 사이버전자전 기술 등이 있다. 향후, 위성 및 고고도 원거리에서 정밀타격 등의 임무를 수행하는 군용 중형대급 드론 대응을 위해서는 지능화된 사이버전자전 기술이 필요할 것으로 전망된다.

1-2 사이버위협에 의한 비정규/국지戰의 증가

RC-IED는 Shooter(사수)가 원격(무전기, 휴대폰 등)제어장치로 특정주파수에 반응하는 급조폭발물 기폭장치를 조정하여 폭발을 유도하는 무선조정 급조폭발물로써, 전문지식이나 첨단기술 없이도 제작/설치가 용이하고, Shooter(사수)의 피해를 최소화하면서 주요 시설 파괴하거나 핵심인물을 수십-수백m 거리 밖에서 암살할 수 있어 2000년대 이후 이를 이용한 세계 곳곳의 테러/게릴라가 급증하고 있다(그림 3)[2].

최근에는 RC-IED를 소형 드론에 장착하여 수백m-수km 원거리에서 목표물을 공격하는 방식이 등장했다. 대표적인 예는 2018년 6월 니콜라스 마두로(베네수엘라 대통령) 드론 암살미수 사건으로, 국가방위군 창설 81주년 행사에서 마두로 연설 도중 공중에서 드론 2대가 폭발하였으며, 군인 7명이 부상 당했다. 물리적 사이버 위협 대응에 대한 가장 큰 관심을 불러일으킨 사건은 2020년 1월 거셈 솔레이마니(이란軍 사령관) 암살이다. 사령관 일행이 시리아에서 바그다드 국제공항에 도착하여 출발한 직후 무장한 드론의 조준폭격에 의해 솔레이마니를 포함한 5명이 사망하였다. 미국은 중형급 무장드론(MQ-9/리퍼)

그림 3. 테러/게릴라용 무선조정 급조폭발물(예)
Fig. 3. RC-IED for terror/guerilla(example).

그림 4. 솔레이마니 암살 사례
Fig. 4. Soleimani assassination case.

을 본토에서 인공위성을 이용하여 원격으로 운용하고 정밀타격을 지시한 것으로 추정되고 있다(그림 4)[3].

이와 같은 세계 각국의 비정규/국지戰 추세로 미루어 볼 때, 미래에는 더욱더 초연결 네트워크를 이용한 사이버 위협 공격이 증가되고 가속화될 것이다. 따라서 이에 대한 대응 방안이 무엇보다도 시급하며, 이를 위해서는 위협의 특징을 면밀히 파악하여 그 진화속도를 뛰어 넘는 대응 기술을 개발하여야 할 것이다.

Ⅱ. 사이버전자전 개념 및 사례

2-1 사이버전자전 개념 및 필요성

사이버전자전이란 전자기 스펙트럼을 이용하여 적의 무선 네트워크 공간을 비롯한 사이버 공간을 교란, 파괴, 통제하는 군사적 행위를 의미한다.

그림 5에서 알 수 있듯이 전자전과 사이버전의 스펙트럼이 중첩하는 곳, 즉 대상 위협 주파수가 중첩하는 곳에서 사이버전자전은 수행되어질 수 있다[4]. 즉, 사이버전자전은 전자전의 주요 대상 위협 주파수 대역이 레이다에서

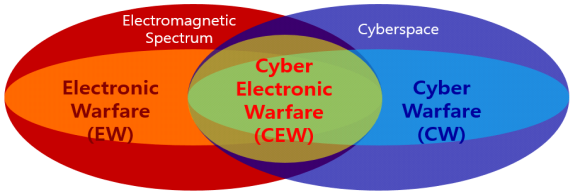


그림 5. 사이버전자전(CEW) 개념
Fig. 5. Cyber electronic warfare concept.

표 1. 사이버전, 전자전, 사이버전자전 특징
Table 1. Cyber warfare, electronic warfare, cyber electronic warfare characteristics.

	Cyber warfare	Electronic warfare	Cyber electronic warfare
Target	Cyber space	Physical space (spectrum space)	Physical+ cyber space
Attack	Malware	High power electromagnetic spectrum	High power electromagnetic spectrum+ malware
Effect	Cyber space infection (long term)	System obstruction (short term)	Cyber space and system obstruction (long term)

통신 영역으로 확장되고, 사이버전의 유선 네트워크 교란 기술이 무선 네트워크 교란기술로 점차 발전되면서 나타내게 된 개념으로 이해될 수 있다. 따라서, 전자전과 사이버전 기술이 융합될 수 있는 사이버전자전 영역은 두 기술이 진보하면 할수록 더욱 확장될 것으로 추정된다.

사이버전, 전자전, 사이버전자전의 특징을 비교·분석하면 다음과 같다[5],[6].

표 1에서 알 수 있듯이 사이버전 기술은 정보교란 능력에서 전자전보다 우위에 있다. 즉, 악성코드(예> 허위메시지, 바이러스) 등으로 사이버 공간의 정보를 지속적 또는 장기적으로 조작하고 교란할 수 있다. 반면에 전자전 기반 기술은 고출력 무선전파 송출능력에서 사이버전보다 우위에 있다. 따라서 물리적 전자기 스펙트럼 공간에서 수십-수백km 밖의 위협(敵 종심에 위치한 지휘통제 체계 등)을 공격할 수 있다. 사이버전자전은 사이버전과 전자전 기술의 장점을 취합하여 물리적 무선 네트워크(스펙트럼) 공간과 사이버 공간에서 공격 시너지 효과 창출을 할 수 있으므로 진화하는 사이버 위협대응을 위한 핵심적인 기술이 될 수 있을 것이다[6].

2-2 해외동향 및 사례

2014년 이후, 군사 선진국(미국, 호주, 일본, 영국, 캐나다 등)들에서는 사이버작전과 전자전을 교리, 조직, 기술 등의 측면에서 융합하고 통합하려는 동향들이 있으며, 다

양한 CEW 통합도구/프로그램들을 운용 중인 것으로 추정된다. 그림 6은 해외 주요 사이버전자전 사례들을 요약 정리한 것이다.

사이버전자전이 수행된 사례로는 일명 '과수원 작전(operation orchard)'으로 불리는 이스라엘 공군의 시리아 지역내 핵시설에 대한 공격이 있다(2007년 9월 6일). 이란 핵시설에 대한 공격은 이스라엘 공군에 의해 수행되었으며, 10여대의 항공기(F-15I 전투기, F-16I 전투기, 1대의 전자정보수집기, 1대의 헬기 등)가 시리아를 향해 공격작전을 수행하였으며, 시리아 레이다 사이트가 재밍 등 전자공격과 재래식 정밀폭탄으로 파괴되었다. 이스라엘 공군의 F-15I는 이스라엘의 엘리스라사의 SPS-2110 전자전 체계를 탑재한 것으로 알려졌으며, 이 전자전체계는 일명 '서터(Suter)'라고 불리는 사이버전자전 소프트웨어가 내장된 것으로 알려졌다. 2007년 9월에 수행된 이같은 이스라엘의 시리아 군사시설물에 대한 진기한 공중공격으로 인해 서터라고 알려진 재밍기술에 대해 세계적인 관심을 갖기 시작했다[7],[8].

이란의 미국 무인기 해킹 또한 유명한 사이버전자전사례로써, 2011년 12월 4일 미국의 록히드마틴사 RQ-170 무인기가 이란 북동쪽의 카슈마르시 근처에서 이란군에 의해 나포되었다. 이란 정부는 핵시설 정찰 중이던 미국 무인기를 사이버전자전 장치에 의해 유도시켜 착륙시켰다고 발표했다. 미국 정부는 처음에는 이란 정부의 주장을

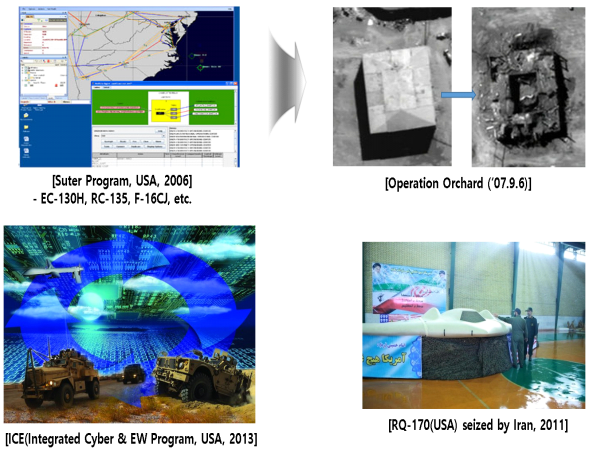


그림 6. 해외 사이버전자전 사례
Fig. 6. Foreign cyber electronic warfare cases.

그림 7. Krasukha와 Krasukha에 의해 파괴된 드론들
Fig. 7. Krasukha and drones destroyed by Krasukha.

부인하였으나, 오바마 대통령이 나중에 보고를 받아 미국 무인기가 떨어진 사실을 인지하였고, 무인기를 돌려달라고 요청하였다. 2012년 4월 이란은 무인기가 수집한 데이터를 추출하는데 성공했다고 주장했다. 2013년 2월 7일 이란정부는 RQ-170으로부터 추출한 비디오 영상을 공개했다. 무인기는 칸다하르 기지에 착륙하기 위해 들어오는 모습을 보여주고 있으며, 무인기가 수집한 모든 데이터를 완전히 디코딩하였다고 주장하였다[9],[10].

최근(2015년 이후) 사례로는 러시아 내전에 투입 중인 Krasukha-2, 4에 의한 적 드론 유인/추락 사례가 있다(그림 7). Krasukha 는 지상기반 차량형 전자전 장비로써, 항공기 및 UAV, 드론 등 공중 표적 대응용 고출력 재머이다. Krasukha는 아르메니아 러시아 군사기지 주변에서 기지 방호용으로 대드론 작전을 수행 중인 것으로 알려져 있으며, 기존의 전자전 전파송신 기술에 사이버전 메시지 조작기술을 융합하여 무장/자살드론을 원하는 곳으로 유도하여 추락시킬 수 있는 것으로 추정되고 있다[11].

2-3 국내 동향

2014년 이후, 해외 사이버전자전 사례와 동향이 알려지며, 국내에서도 사이버전자전에 대한 개념과 기술연구 필요성이 계속 제기되어 왔으나, 아직은 개념연구 단계로 파악된다.

관련 국내 주요 동향으로는 2017년 사이버전자전 개념을 항공우주작전에 적용하려는 최초 시도가 있었고, 2018년 합동성대토론회에서 사이버전자전의 군사작전 적용 방안에 대한 토의가 있었다[12],[13]. 2018년 이후에는 육군 주도로 사이버전자전 교리/교범을 정립하려는 움직임이

있다. 2019년에는 '사이버전자전'이 육군 10대 게임체인저로 선정되었으며, 이와 관련된 연구가 지속적으로 진행중이다.

Ⅲ. 사이버전자전 소요기술 및 발전전망

사이버전자전에 소요되는 기술들 중 위협 진화추세에 맞추어 중점 개발되어야 할 주요 핵심기술에 대해 다루고자 한다.

3-1 전자파를 이용한 메시지 교란기술

현재, 전자전과 사이버전의 대상 위협이 중첩되는 주파수 스펙트럼은 통신대역으로 식별되고 있으며, 해당 대역에서 '원거리 고출력 전자파 탐지/송출'로 대표되는 전자전 능력과 '정보(메시지) 조작/교란'으로 대표되는 사이버전 능력을 융합하여 두 기술이 시너지 효과를 발휘할 수 있는 사이버전자전 기술로 발전시켜야 한다.

기존 전자전 통신대역 교란기술은 무선통신 방해를 유도하는 잡음 송출 기술이 주를 이루었으나, 최근에는 허위 메시지를 전파할 수 있는 기만 기술을 이용하여 메시지를 조작할 수 있는 사이버전자전 기술로 점차 진화 중이다. 기만 기술은 '신호세기, 신호위상, 신호 지속구간' 등을 변조하여 원래의 메시지를 조작하는 기술로써 조작의 정도와 내용은 대상위협과 공격목적에 따라 달라질 수 있다. 사이버전자전 기술 융합 분야는 대상위협의 특성에 기반하여 사이버전 기술로 원하는 위협에 악영향(임무수행 방해, 오동작 등)을 미칠 수 있는 악성코드를 생성하고, 생성된 코드를 전자전의 기만기술로 전자기파로 변환한 뒤 이를 고출력으로 송신하는 분야가 될 것이다.

3-2 무선 네트워크 취약접점 자동탐지 기술

사이버전자전 기술의 핵심은 보안에 취약한 무선 네트워크 접점을 자동으로 파악하고 공격하는 것이 될 수 있다(그림 8). 암호장비나 비공개 프로토콜로 무장한 위협을 공격하기 보다는 비교적 보안이 취약한 침투접점을 자동으로 파악하고, 이를 통해 악성코드를 장입하는 기술로 스마트한 공략 개념이 필요하다. 취약접점을 통해 장입된 악성코드들은 적 네트워크를 통해 자연스럽게 전파

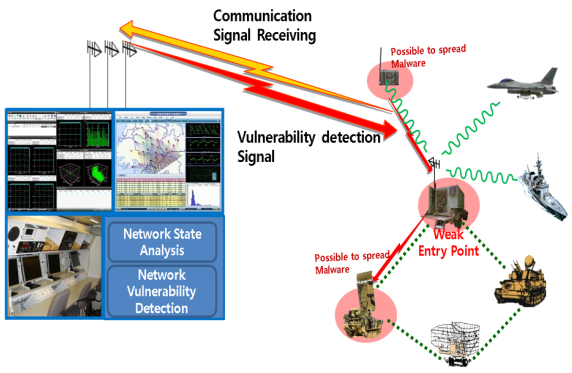


그림 8. 네트워크 취약접점 탐지 기술
Fig. 8. Network vulnerability detection technology.

될 것이다.

3-3 현실적인 위협선정과 맞춤형 공격기술

사이버전자전의 최우선 대상 위협으로는 프로토콜이 공개되거나 취약한 것으로 이미 알려진 GPS 수신기 탑재 무기체계(드론/무인기, GPS유도 미사일 등), 공개/보안취약 무선네트워크 체계, 위성체계 등이 현실적인 공격대상이 될 수 있다. 이에 필요한 핵심기술로는 진화된 위성 항법신호 교란기술, Radio Control 신호 교란기술 등이 있을 수 있다.

3-3-1 진화된 위성 항법신호 교란기술

위성 항법신호 교란기술은 항법신호로 유도되는 위협에 대응하기 위해 필요하다. 기존 전자전 기술이 잡음전파 송출로 위성 항법신호로 유도되는 드론/무인기 등을 궤도이탈/추락시켰다면 사이버전자전에서는 항법위성 메시지를 탐지/분석하고, 허위/기만 메시지를 생성하고, 송출하여 위협을 특정경로/안전지역으로 유도한다. 이는 폭발/화학무기를 장착한 물리적 사이버 위협 대응을 위해 매우 긴요한 기술이다(그림 9).

3-3-2 Radio Control 교란기술

Radio Control 신호는 RC-IED 의 기폭장치 제어 및 무인 위협들의 제어를 위해 이용된다(그림 10). 따라서 Ra-

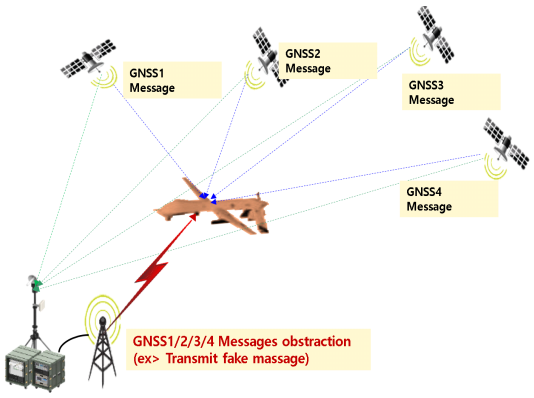


그림 9. 진화된 위성 항법신호 교란기술(예)
Fig. 9. Progressive GNSS(global navigation satellite system) obstruction technology(example).

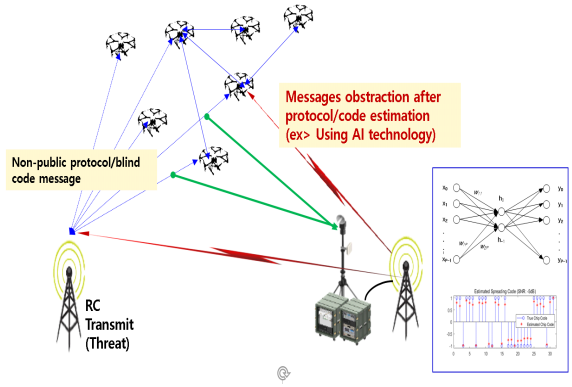


그림 10. Radio control 신호 교란기술(예)
Fig. 10. Radio control signal obstruction technology(example).

dio Control 교란기술은 Shooter(사수)의 제어신호로 유도되는 물리적 사이버 공격위협에 보다 적극적으로 대응하기 위해 반드시 필요하다. Radio Control 신호는 공개된 위성 항법신호와는 달리 비공개 프로토콜/코드 신호를 기반으로 한다. 따라서 딥러닝 등 첨단 AI 기법을 이용하여 이를 추정한 뒤, Radio Control 신호를 탐지/분석하고, 허위/기만 메시지를 생성·송출할 수 있는 사이버전자전 기술 개발과 적용이 필요하다.

3-4 사이버전자전 발전방향

미래 전장은 초연결 네트워크를 이용하여 거의 모든 무기체계가 연결된 네트워크 戰이 될 것이다. 육·해·공·우주 공간이 주파수 스펙트럼으로 연결된 미래 전장에서 전자전과 사이버전 위협/주파수 영역은 점차 더 중첩될 것이고, 이에 효과적으로 대응하기 위해서는 두 기술을 융합한 사이버전자전 기술이 필요하다.

이를 위해서는 현실적이고, 점진적인 방안으로 사이버전자전에 접근해야 한다. 해외 사이버전자전 사례와 국내 기술수준을 분석해 볼 때, 대응 가능한 대상 위협은 “위성항법수신기 장착 위협”, “소형무인기”, “중대형무인기/위성통신체계”, “적 지휘통제망” 순으로 확장될 것으로 전망된다. 또한 여기에 적용될 대표적인 핵심소요기술은 “GPS수신기 기만기술”, “데이터링크 기만 기술”, “적 지휘통제망 교란/침투기술” 순으로 점차 발전될 것으로 추정된다.

Ⅳ. 결 론

본 논문에서는 초연결 사회와 사이버 위협, 전장영역 확대에 따른 전자전의 고출력 전자파송출 기술과 사이버전의 메시지 조작/교란 기술을 융합한 사이버전자전 기술을 소개하고, 위협 진화추세에 맞추어 중점 개발되어야할 주요 핵심기술들에 대해 다루었다.

결론적으로 사이버전자전의 발전을 위해서는 사이버전자전 공격에 취약한 현실적인 위협, 무기체계를 우선 식별한 뒤, 이에 필요한 핵심기술을 도출하고, 이를 중점적으로 개발하여야 한다.

References

[1] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196-248, 2020.

[2] Indo-Pacifoc Defense, "Response to improvised explosives," 2020. Available: https://ipdefenseforum.com/ko/2018/01/%EA%B8%89%EC%A1%B0-%ED%8F%AD%EB%B0%9C%EB%AC%BC-%EB%8C%80%EC%9D%91/

[3] J. S. Son, "US drones operated in the mainland... Equipped with ninja bombs to 'hit tweezers'," *Chosun*

Ilbo, 2020. Available: https://www.chosun.com/site/data/html_dir/2020/01/06/2020010600315.html

[4] N. Yasar, F. M. Yasar, and Y. Topcu, "Operational advantages of using cyber electronic warfare(CEW) in the battlefield," in *Proceeding of SPIE*, vol. 8408, p. 8408G-1, 2012.

[5] H. Kim, J. Cho, S. Kim, H. Kwak, C. Jeong, T. Kang, et al., "Smart EW: Cyber EW," *Defense New Technology Trend Analysis*, vol. 38, pp.35-40, Jan. 2016.

[6] S. Kim, "Concept of future active cyber warfare," in *Conference of the Korea Institute of Military Science and Technology*, 2017.

[7] G. I. Lee, S. G. Lee, "Cyber electronic warfare techonology development trend," *Defense New Technology Trend Analysis*, vol. 33, pp. 1-9, Sep. 2014.

[8] Wikipedia, "Operation outside the box," 2021. Available: https://en.wikipedia.org/wiki/Operation_Outside_the_Box

[9] Wikipedia, "Iran-US RQ-170 incident," 2021. Available: https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident

[10] P. Paganini, "Hacking Drones...Overview of the main threats", 2021. Available: https://resources.infosecinstitute.com/topic/hacking-drones-overview-of-the-main-threats

[11] Russia Today, "Advanced system to guard Russia from hi-tech surveillance, drone attacks," 2013. Available: https://www.rt.com/news/russia-radar-jammer-drones-864/

[12] S. Kim, "Lessons of LoL(Left of Launch) and aerospace operations application plan for CW," in *Conference of the Korea Institute of Military Science and Technology*, 2017.

[13] S. Kim, "CEW(Cyber Electronic Warfare) concept and application plan for military operation," Great Debate for Joint, Seoul, 2018.

김 소 연 [국방과학연구소/연구원]

https://orcid.org/0000-0003-4929-2924

1998년 2월: 전남대학교 컴퓨터공학과 (공학사)

1999년 8월: 한국과학기술원 전기 및 전자공학과 (공학석사)

2015년 2월: 한국과학기술원 전기 및 전자공학과 (공학박사)

2001년 7월～현재: 국방과학연구소 전자전 기술부서 연구원

[주 관심분야] 전자전 신호처리, 사이버전자전, 인공지능 등

김 성 표 [국방과학연구소/연구원]

https://orcid.org/0000-0001-8688-7412

1987년 3월: 공군사관학교 국제관계학과 (문학사)

1996년 8월: 미)오클라호마주립대 전기 및 컴퓨터공학과 (공학석사)

2004년 8월: 미)미주리대 컴퓨터공학과(공학박사)

2015년 10월 ～현재: 국방과학연구소 국방고등기술원/정책기획부 연구원

[주 관심분야] 사이버전자전, 항공우주, 미사일 방어, 인공지능 등

박 범 준 [국방과학연구소/연구원]

https://orcid.org/0000-0001-5504-7859

1994년 2월: 충남대학교 전자공학과 (공학사)

2000년 2월: 충남대학교 전파공학과 (공학석사)

2015년 8월: 충남대학교 전파공학과 (공학박사)

2001년 1월～현재: 국방과학연구소 전자전 기술부서 연구원

[주 관심분야] 전자전 수신기 설계, 초고주파 소자 설계 등

정 운 섭 [국방과학연구소/연구원]

https://orcid.org/0000-0002-3829-5743

1988년 2월: 충남대학교 전자공학과 (공학사)

1990년 2월: 충남대학교 전자공학과 (공학석사)

2007년 2월: 충남대학교 전자공학과 (공학박사)

1990년 3월～현재: 국방과학연구소 전자전 기술부서 연구원

[주 관심분야] 전자전체계 설계, 전자전 신호처리 등

추 헌 우 [육군정보학교/교관]

https://orcid.org/0000-0002-0004-7701

2006년 2월: 육군 3사관학교 프랑스어과 (학사)

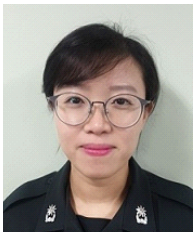
2019년 2월: 한성대학교 안보전약학과 국제안보전공 (석사)

2020년 4월～현재: 육군 정보학교 전자전 교육대대 사이버전자전 개념발전 장교 교관

[주 관심분야] 전자전 및 첨단센서 군사적 운용 및 무기체계, 사이버전자전 등

윤 정 [육군정보학교/교관]

https://orcid.org/0000-0002-3764-4067



2006년 2월: 군산대학교 전자정보공학부 정보통신전파공학과 (공학사)

2016년 8월: 아주대학교 사이버보안학과 (공학석사)

2019년 4월～현재: 육군정보학교 전자전 교육대대 전자보호교관

[주 관심분야] 전자전 군사적 운용 및 무기체계, 사이버전자전 등

김 진 용 [육군정보학교/대대장]

https://orcid.org/0000-0001-9797-4941

1995년 2월: 육군 3사관학교 전자공학 (공학사)

2002년 2월: 경희대학교 경영학과 (경영석사)

2019년 1월～현재: 육군 정보학교 전자전 교육대대 대대장

[주 관심분야] 전자전 군사적 운용 및 무기체계, 사이버전자전 등