Journal of the KNST

2022; Vol.5, No.1; pp. 20-32

ISSN: 2635-4926 https://doi.org/10.31818/JKNST.2022.03.5.1.20

Check for updates

Received: 2022/01/14
Revised: 2022/03/08
Accepted: 2022/03/21
Published: 2022/03/31

*Corresponding Author:
Su-Min Kim
E-mail: anasista62@gmail.com

해군 사이버전자전 발전 방향 연구

A Study on the Development of Cyber Electronic Warfare in the Republic of Korea Navy

김수민*

해군 소령/해군 2해상전투단 235고속정편대장

Su-Min Kim*

LCDR/DCO, ROKS 235 PKM Division Command, 2nd Battle Group, ROK NAVY

Abstract

4차 산업혁명 이후 사이버공간은 새로운 전장영역으로 포함되며 그 중요성이 커져왔다. 사이버공간에서의 승리를 위해 세계 각 국가가 노력한지 10년이 되지 않은 이 시점에서 우리는 사이버전 영역과 전자전의 영역이 통합된 사이버전자전이라는 새로운 전장환경을 대비해야 하는 시대를 맞이하고 있다. 본 연구를 통해 우리가 준비해야 할 사이버전자전을 이해하고 세계 각 국가의 발전 동향을 확인하고 대한민국 해군이 나아가야 할 발전방향을 제시한다.

Since the 4th Industrial Revolution, cyberspace has been included as a new battlefield, and its importance has grown. Less than 10 years after countries around the world have worked hard to win cyberspace, we are facing an era of preparing for a new battlefield environment called cyber-electronic warfare, in which the areas of cyber warfare and electronic warfare are integrated. Through this study, we understand the cyber-electronic warfare that we need to prepare, check the development trends of countries around the world, and suggest the development directions for the Republic of Korea Navy.

Keywords

사이버전자전(Cyber Electronic Warfare),
사이버전(Cyber Warfare),
전자전(Electronic Warfare)
사이버작전(Cyber Operation),
스마트 해군(SMART Navy)

Acknowledgement

이 논문은 2022년도 한국해군과학기술학회 춘계학술대회 발표 논문임

1. 서론

4차 산업혁명 시대에 살고 있는 우리는 사회 및 전장환경에서도 사이버공간의 중요성에 대해 인식하고 있으며 이 사이버공간에서의 안전보장과 적과의 교전에서 승리하기 위해 만반의 준비를 하고 있다.

사이버공간은 5대 전장영역인 지상, 해상, 공중, 우주, 사이버 중 하나의 영역으로 포함될 정도로 최근 큰 관심과 이에 대한 대비가 중요해지고 있는 상황이다. 우리는 사이버라는 공간은 단순 LAN선을 통해 연결된 사이버공간에서 컴퓨터를 통해 적의 지휘체계를 공격하는 등의 개념으로 인식하고 있다.

이러한 사이버공간에서의 전투수행의 개념이 미 육군을 시작으로 점차 확대되어 나가고 있다. 사이버공간이 확장되는 개념이 바로 사이버전자전의 개념의 시작이다. 통상 사이버와 전자전의 영역을 분리하여 각각 대응하고 있는 것이 현재 우리 군의 실상이지만 앞으로는 이러한 영역의 구분은 점차 없어질 것이고 이 두 영역을 통합한 사이버전자전의 범주 내에서 전쟁의 승리를 위한 각종 활동이 진행될 것이다.

사이버전자전에 대한 관심이 증대된 계기는 2011년 이란 상공에서 이란의 핵시설을 정찰하던 미국 무인기 RQ-170이 이란에 의해 나포된 사건을 발단으로 시작된다. 미국의 최신 무인기가 이란의 사이버전자전 공격으로 나포되었다는 사건[1]에 충격을 받은 미국은 본격적으로 전자기 영역과 연계된 사이버전자전에 대한 발전에 집중하였고 2013년 미 육군에서 최초로 사이버전자전 교리와 제대별 부대 편성 및 교육훈련 등의 사이버전자전 수행을 위한 계획을 수립하고 발전시켜 나가고 있다.

이후 미국은 2017년 3월 발사 직전 교란 즉 Left of Launch 개념을 발표하기에 이른다. 적의 미사일을 발사하기 직전 아군의 사이버전자전인

전자기파와 사이버공격을 통해 적 지휘통제체계와 미사일 내부 전자 기기 공격으로 무기 발사를 무력화한다는 작전[2]을 구상하게 된다. 이 작전개념은 실제 북한이 2017년 6월 총 6차례에 걸친 무수단 미사일을 8발 발사했지만 이 중 1발만 성공하고 나머지 7발은 실패하게 된 사례를 통해 작전의 효과를 가늠해 볼 수 있는 기회가 되었다.

해상에서 작전을 수행하는 우리 해군은 과거부터 전자기파 영역에서의 작전인 전자전을 수행하고 있으며 지상영역에서의 작전과 달리 해상이라는 전장환경은 공중과 같이 전자기파의 직진성을 방해하는 요소가 없으며 함정의 다양한 탐지 및 무기체계에서 발생되는 전자파에 의한 전자전이 수행되고 있는 환경이다. 이러한 해군의 특수성을 고려하였을 때 앞으로 그 중요성이 커지게 되는 사이버 전자전에 대한 대비가 가장 중요한 것은 대한민국 해군이라고 생각된다.

이에 본 연구에서는 해군이 앞으로 준비하고 발전해야 할 사이버전자전의 기본 개념을 이해하고 실제 사이버전자전이 수행되었던 사례를 분석한다. 또한 주요 국가와 대한민국 육군, 공군에서 발전시키고 있는 사이버전자전의 발전 동향을 확인하고 대한민국 해군이 앞으로 나아가야 할 사이버전자전의 발전 방향을 제시하고자 한다.

2. 사이버전자전에 대한 이해

2.1 사이버전과 전자전의 기술적 환경

사이버전과 전자전의 기술적 환경을 살펴보면 Fig. 1과 같이 국제표준화기구에서 개발한 통신계층(7 layers)으로 설명할 수 있다. 이 모형은 OSI 모형(open systems interconnection reference model)로 국제표준화기구(ISO)라는 단체에서 개발하였다. 특징으로는 컴퓨터 네트워크 프로토콜 통신규약에 대한 전체적인 범주와 송수신자 상호간의 통신을 각 계층별로 구분하여 설명한 것이 특징으로 통상 OSI 7 계층(OSI 7 Layers)[3]이라고 한다.

먼저 결론적으로 통신의 7가지 계층 속에 사이버 영역과 전자기파 영역이 모두 포함되어 있음을 알 수 있다. 위의 그림에서 볼 수 있듯이 1계층은 물리계층 즉, physical layer로 전기적, 기계적, 기능적인 특성을 이용하여 통신케이블로 데이터를 전송하게 하는 계층이다. 기본적인 통신 단위는 비트 즉, 0과 1을 이용하여 통신을 하게 되고 이는 전기적으로 on, off 상태로 데이터를 구성하게 된다. 이 계층에서는 단순 데이터의 통신에 신경을 쓰고 구체적으로 통신 내용에 오류가 있는지 여부 등은 따지지 않는다.

2계층인 데이터 링크 계층은 1계층인 물리계층을 통해 송수신되는 정보의 오류와 흐름에 관리하여 안전한 정보의 전달을 수행할 수 있도록 돕는 역할을 한다. 그렇기 때문에 통신의 오류를 찾고 데이터 흐름에서 오류가 식별되는 경우(즉 송신자가 송신하였지만 통신환경 등의 오류로 인해 수신자가 정상 수신을 못 하는 경우) 재전송하는 기능도 포함하고 있다. 이는 상호간의 신뢰성 있는 송수신 통신을 보장하는 단계를 포함하고 있다.

3계층은 네트워크 계층으로 전송단위인 데이터를 최종 수신자까지 안전하게 전달하는 기능을 가지고 있다. 최초 송신자부터 최종 수신자까지 데이터가 이어지는 과정에서 걸치게 되는 여러 가지 노드들(중간지점) 간의 흐름을 통제하는 역할을 한다. 이러한 데이터의 흐름에서 각 중간지점들을 오류 없이 찾아가기 위해 지정된 주소가 바로 IP 주소이다.

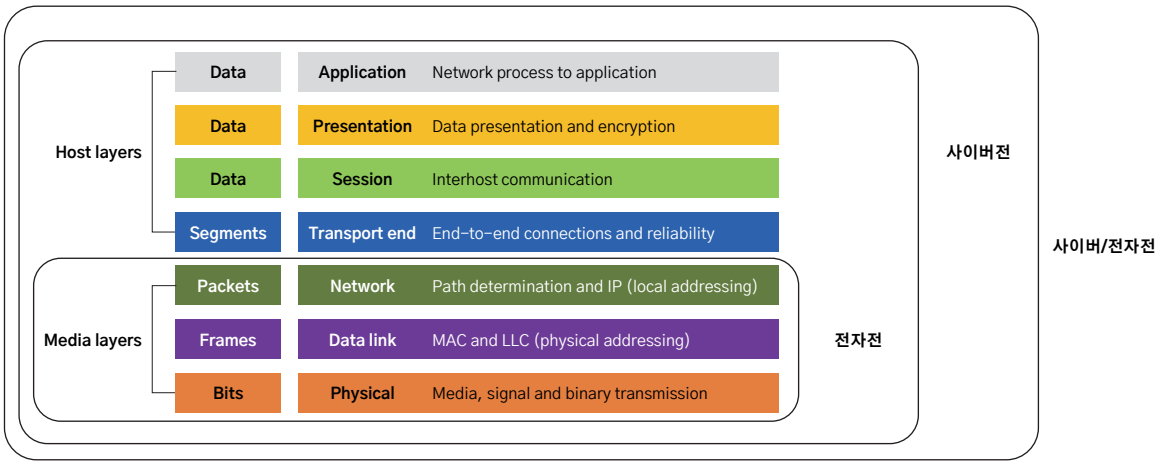


Fig. 1. 사이버전자전 기술적 환경

4계층은 전송 계층으로 통신을 활성화하기 위한 계층이다. 3계층의 상위단계로 최종 송수신자인 양 끝단(End to end)의 사용자들이 신뢰성 있는 데이터를 송수신 할 수 있도록 해주는 역할을 하며 3계층보다 더욱 신뢰성을 높이기 위해 중간단의 효율적인 데이터 전송, 전송 간 오류 검출 및 복구, 흐름제어, 데이터 중복검사 등의 기능을 수행할 수 있다. 대표적인 개념으로 TCP 프로토콜(transmission control protocol)을 들 수 있는데 우리가 주로 사용하는 인터넷 환경에서 TCP/IP의 개념을 많이 접하게 된다.

5계층은 세션 계층으로 데이터가 통신하기 위한 논리적 연결을 말하며 하위 계층에 비해 양 끝단 사용자의 응용 프로세스가 통신을 관리하기 위한 상위 개념의 관리 방식을 제공한다.

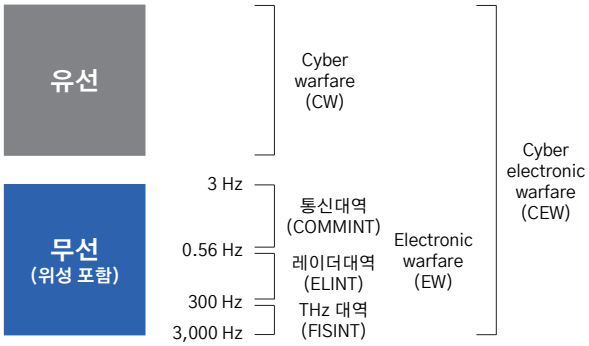
6계층은 표현 계층으로 송수신자 간의 데이터 형식의 차이를 동기화하기 위한 작업을 수행하는 계층으로 상호 데이터 표현이 상이한 응용 프로세스의 독립성을 보장하고 암호화하는 역할을 수행한다.

마지막 7계층은 응용 계층으로 우리가 실생활에 접하는 인터넷, E-mail 등 실제로 사용자가 접하게 되는 플랫폼 등을 제공하는 역할을 한다. 인터넷의 경우 HTTP, FTP 등의 개념, E-mail을 사용할 수 있는 POP3 등의 개념을 구현하는 최종 계층을 말한다. 특히 HTTP 프로토콜(hyper text transfer protocol)은 우리가 주로 사용하는 인터넷 프로토콜로 웹 상에서 웹 서버 및 웹 브라우저 상호 간의 데이터 전송을 위한 응용계층 프로토콜을 의미하며 최초에는 텍스트 기반의 송수신만 하였다면 현재는 이미지, 음성 및 비디오까지 거의 모든 형식의 데이터 전송이 가능한 수준에 이르게 되었다.

Fig. 1에서 볼 수 있듯이 우리가 크게 신경 쓰지 않고 사용했던 PC에서의 인터넷, 스마트폰에서의 웹 서핑을 위해서는 0과 1의 비트로 구성된 데이터가 유선과 무선 환경에서 여러 가지 노드 등을 거쳐 송신자로부터 최종 수신자까지 지속적으로 데이터를 왕복하는 과정을 거치게 된다.

과거에는 유선을 기반으로 하는 데이터 통신이 주가 되었다면 4차 산업혁명이 도래한 현재는 거의 대부분의 통신 환경이 무선을 기반으로 하는 통신이 주가 되었다. 우리가 생활하는 이 세상에서 컴퓨터, 스마트폰 등 각종 전자기기 등을 인터넷 및 통신을 하게 되는데 이러한 접속 과정에서 여러 데이터들이 상호간에 영향을 미치며 통신하게 된다. 상호간에 0과 1의 비트 기반의 데이터 통신을 하게 되고 이러한 데이터 통신은 유선과 무선의 모든 환경에서 통신이 이뤄지고 있다.

무선 기반의 데이터 통신(WDC, wireless data communication)은 말 그대로 둘 또는 그 이상의 지점 사이에 전기 전도체의 연결 없이 정보를 전송하는 것을 의미한다. 통신 방식으로는 공기중의 전자기파를 이용한 통신 방법과 사람이 청각으로 인지할 수 없는 초음파 영역을 이용한 통신방법, 사람이 청취할 수 있는 고주파와 합성하여 전파를 생성하여 송수신하는 등의 여러 가지 방법이 있다. 또한 각종 전자기기 리모컨과 같이 적외선(IR)을 이용하여 통신하는 방법과 위성 통신과 같이 수천 km 떨어진 곳에서 이뤄지는 등의 다양한 방법이 있다. 우리의 실생활에서는 Wi-Fi 등을 이용한 무선 네트워크 연결이 대중적으로 활용하고 있는 무선 데이터 통신 기술이다.



*COMINT(통신정보): 통신 도청에 의한 정보 수집
ELINT(전자정보): 전자파(주로 레이더)에 의한 정보 수집
FISINT(외부기기 신호정보): 주변 외부기기에 의한 정보수집

Fig. 2. 사이버전자전 네트워크(통신망) 적용 범위

이러한 무선 통신 기술은 민간 분야에서뿐만 아니라 군에서도 사용되고 있다. 주파수를 이용한 통신, 위성통신 등 여러 가지 분야에서 군 통신이 사용되고 있으며 우리 군은 무선 환경에서의 악의적 중간자 공격, 무선통신 침해 등의 시도 등에 대한 대비책과 대책이 필요한 상황이며, 반대로 우리도 이 무선통신 공간을 이용하여 적에게 타격을 입힐 수 있는 공격 방안과 무기가 개발되어야 함은 현재도 다수의 의견이 있으며 시대의 흐름에 부합된 노력일 것이라 생각된다.

즉, 과거에는 유선 환경만을 고려한 CW(cyber warfare) 즉, 사이버전에만 집중하였다 한다면 현재는 무선환경이 주 기반이 되는 EW(electronic warfare) 즉, 전자전 환경에 대한 대비도 필요하며 CW와 EW를 통합 및 융합하여 활용하는 사이버전자전에 대한 대응 개념도 발전시켜야 함은 분명한 현실이다.

결론적으로 사이버 영역과 전자기의 영역은 OSI 7 Layers라는 큰 틀 안에서는 통합된 공간에서 활동하고 있

음을 알 수 있다. 이러한 개념을 미군은 어떻게 적용하고 있는지 다음을 통해 알아보자.

2.2 미군의 사이버전자전 개념

미군에서는 미 육군을 중심으로 사이버전자전 개념이 지속 발전하고 있다. 미 육군 군사교범에서 정의하는 사이버전자전(cyber-electronic warfare, CEW)은 사이버전과 전자전의 각 영역의 제한사항을 극복하고 사이버공간과 전자기영역의 활용 및 통합을 통해 적 지휘통제시스템 또는 무기체계를 무력화하는 동시에 우군의 지휘통제시스템 또는 무기체계를 보호하는 군사활동으로 정의할 수 있다(미 육군 군사교범, FM 3-12, 2017, 1-1).

사이버공간과 전자공간 각각의 제한사항을 극복하고 큰 틀에서 하나의 영역으로 볼 수 있는 사이버공간과 전자기영역을 통합하여 활용함으로써 각자의 노력의 낭비를 최소화하고 통합을 통한 시너지 효과를 극대화하겠다는 의미로 평가할 수 있다. 사이버전자전은 기존 사이버작전의 제한사항이었던 적의 폐쇄망 및 전장망에 대한 접근을 가능하게 하며 간접적인 접근이 아닌 전자기영역을 활용한 접근으로 직접적인 사이버작전이 가능하도록 발전시키고 있는 것이다.

미 육군의 군사교범 FM 3-12 <사이버공간과 전자기작전> 교범에 의하면, 사이버전자전을 완전히 새로운 군사작전의 영역으로 인식하고 있다. 사이버공간 상에서 무선이 아닌 유선을 통해 전송되는 전자적 정보를 통한 모든 작전은 사이버공간의 영역으로 구분하고, 사이버공간이 아닌 단순 전자기 스펙트럼에 속하는 작전은 전자전으로 구분하였다(미 육군 군사교범 FM 3-12, 2017, 1-1). 기존의 사이버작전이 유선을 통해 이뤄지는 것에서 확장되어 전자기 스펙트럼 영역인 무선 환경에서 사이버작전이 진행되는 것을 사이버전자전으로 볼 수 있는 것이다.

미 육군 및 여러 연구에서도 '사이버전자전'이라는 용어사용에 있어 관련된 여러 가지 사용과 의견이 분분하였다. '사이버/전자전', '사이버전자전', '사이버전 및 전자전' 등 다양한 용어의 사용이 각 군마다, 작전요원마다 달라 추후 용어의 통일이 필요하다.

미 육군은 위의 사이버전자전의 개념을 전체적으로 포괄하는 개념으로 CEMA(cyber & electro-magnetic activities, 사이버전자기활동)으로 정의하며 세부적으로는 사이버공간작전(CO), 전자전(EW), 스펙트럼 관리 작전(SMO)으로 구분[4]하고 있다.

Table 1. 미 육군의 사이버전자전 세부 작전

작전 구분*		목적
사이버 공간 작전 (CO)	OCO	· 사이버공간 내에서 또는 공간을 통해서 전투력을 사용하여 적을 공격하는 작전
	DCO	· 국방 또는 아군의 사이버공간의 사이버위협을 탐지/식별/대응 및 작전수행 능력을 유지/보존하는 작전
	DODINO	· 국방 데이터의 기밀성, 무결성, 가용성 확보를 위해 국방망을 설계, 구축, 구성, 보안강화, 운용, 유지보수, 운영유지하는 작전
전자전 (EW)	EA	· 적 전투능력을 수준저하, 무력화, 파괴시킬 의도로 인원, 시설, 장비를 공격하는 작전을 의미하며 전자기 에너지, 지향성 에너지, 대방사 무기 등을 사용
	ES	· 적 전자위협 탐지, 식별 및 위치 탐지 작전
	EP	· 아군 전투력을 수준저하, 무력화, 파괴하는 적의 전자기 스펙트럼 사용의 결과로부터 인원, 시설, 장비 등을 보호하는 작전
스펙트럼 관리 작전 (SMO)	SM	· 작전 임무를 수행하기 위해 스펙트럼 접근이 가능하도록 지원
	FA	· 특정 장치의 주파수 사용 권한부여
	HNC	· 작전이 수행되는 국가와 주파수 사용 협의
	Policy	· 스펙트럼 관리 규칙이 준수되도록 관리 (생명유지장치의 안정성 확보 관리 등)

*OCO: offensive cyberspace operations,
DCO: defensive cyberspace operations,
DODINO: Department of Defense information network operations,
SM: spectrum management,
FA: frequency assignment,
HNC: host nation coordination
(출처: 미 FM 3-38, 'Cyber Electromagnetic Activities' (2014) pp. 1-2.)

대한민국 육군정보학교에서는 '사이버전자전', '사이버/전자전'의 개념에 대한 정의를 다음과 같이 구분하였는데 먼저 '사이버전자전'은 사이버작전과 전자전의 개념을 통합하는 개념으로 '전자기스펙트럼(EMS)[1]을 이용하여 사이버공간 및 전자기 영역에 영향을 주는 군사활동'으로 정의, '사이버/전자전'의 용어는 사이버작전, 전자전 그리고 사이버전자전 3가지 개념이 모두 포함된 개념으로 정의한다.

육군은 이러한 사이버전자전의 개념을 ACE(activities affecting cyberspace using electromagnetic spectrum)란 약어로 정의하고 이에 대한 개념을 발전[5]시키고 있다.

[1] EMS(Electro-Magnetic Spectrum)으로 전자기파를 파장에 따라 분해하여 배열한 것으로 감마선부터 분류하는 기준에 따라 X선, 자외선, 가시광선, 적외선 등의 파장으로 배열한 것을 의미한다.

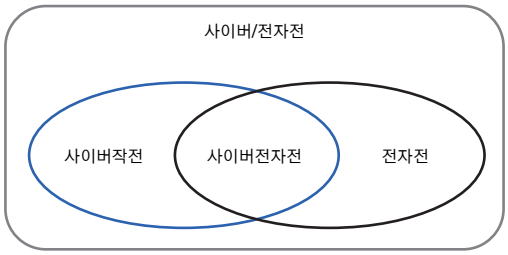


Fig. 3. 사이버전자전의 영역

지금까지 사이버전자전에 대한 개념과 적용 영역, 최초로 개념을 도입한 미군의 적용과정과 대한민국 육군에서의 정의 등을 통해 사이버전자전에 대한 이해를 높일 수 있었다. 다음 장에서는 사이버전자전을 실제로 수행하였던 사례를 통해 사이버전자전의 중요성에 대해 알아보자.

3. 사이버전자전 수행 사례

3.1. 이스라엘 공군의 시리아 핵시설 공격 작전

'과수원 작전(Operation Orchard)'으로 불리는 이 작전은 2007년 9월 6일 이스라엘 공군이 시리아 지역 내 위치한 핵시설을 공격한 작전이다. 국제원자력기구(IAEA, International Atomic Energy Agency)가 2011년 4월 시리아에 핵시설이 있는 것으로 공식 발표하였지만, 그 전까지 시리아는 해당 내용을 지속 부정하며 IAEA의 핵 사찰을 거부하고 있었다.

이에 시리아의 핵시설에 대한 위협을 느낀 이스라엘은 과수원 작전을 통해 시리아의 핵시설 제거를 결심하게 되었다. 결과적으로 이스라엘은 과수원 작전을 통해 자군의 피해 없이 목표한 시리아의 핵시설을 성공적으로 제거하였다. 이스라엘의 F-15I, F-16I 전투기, 전자정보수집기, 헬기 등이 포함된 10대의 항공기가 작전을 수행[6]하였으며 이 작전에서 F-15I 전투기에는 이스라엘 Elisra 회사에서 개발한 SPS-2110 전자전 체계가 탑재되었으며 해당 전자전 체계에는 사이버전자전 수행이 가능한 소프트웨어인 '서터(SUTER)'가 내장되어 있었다.

Fig. 4. 시리아 원전 파괴 전·후 및 이스라엘 사이버전자전 수행 전투기(F-15I, F-16I)

작전의 경과는 이스라엘 공군기를 이용하여 시리아의 radar site를 재밍하는 등 전자공격과 재래식 정밀폭격을 통해 파괴하였다. Radar site를 교란하는 과정에서 앞서 설명한 사이버전자전 무기 소프트웨어 '서터(SUTER)'가 사용된 것이다.

사이버전자전 무기 소프트웨어인 '서터(SUTER)'에 대해 구체적으로 살펴보면 '서터(SUTER)'는 BAE라는 회사에서 개발한 적 네트워크와 통신 방해를 위한 군사용 소프트웨어다. 미 공군에 의해 통제되며 적 방공망을 주요 표적으로 하는 임무수행 시 사용되는데, 단계별로 SUTER의 기능[7]이 구분되며 구체적인 내용은 아래 표와 같다.

Table 2. 사이버전자전 무기 소프트웨어 SUTER의 단계별 능력

단계	세부내용
SUTER 1	· 적 방공망 운용자의 활동 내용을 감시
SUTER 2	· 적 네트워크에 침투해 제어 및 적 R/D 통제
SUTER 3	· 시한성 표적인 대륙간 탄도미사일(ICBM) 또는 이동형 지대공 미사일 위협의 데이터링크 시스템에 침투, 체계 교란

시리아는 러시아로부터 방공무기를 구입하여 사전 배치 및 대응하였으나 방공 radar site 상 접촉사항이 없어 무방비 상태에서 핵시설에 대한 피격을 받는다. 기존 전자전 공격인 재밍 기술에서 한 단계 발전하여 전자기파를 이용하여 적의 전투체계에 대한 사이버공격을 수행한 과수원 작전을 통해 이스라엘의 사이버전자전 기술인 '서터(SUTER)'가 세상에 알려지게 되었고 이를 통해 사이버전자전과 재밍기술이 세계에 큰 관심을 얻기 시작하였다.

3.2 이란의 미국 무인기 RQ-170 탈취 사건

2011년 12월 4일 이란의 핵시설을 정찰 중인 미국의 무인기 RQ-170(센티널)을 이란이 사이버전자전 기법으로 공중 탈취하여 자국의 비행기지에 착륙시킨 사건이 있었다.

최초 미국 정보는 RQ-170 무인기 탈취에 대해 공식적으로 부인하였지만 미 정부의 추가적인 정보 입수와 이란 정부의 공식 발표로 인해 자국 무인기가 격추된 사실을 인정하였고 무인기 반환을 이란에 요청하였다.

무인기 탈취는 이란의 기술진이 사이버전자전 공격을 통해 미국 RQ-170의 인공위성항법장치(GPS) 좌표를 변경해 기존의 계획된 착륙지점이 아닌 이란의 비행기지로 착륙하도록 조작하는 방식이었다. 구체적으로 살펴보면

미국 무인기의 GPS 연결신호를 사이버전자전 기법인 GPS 스푸핑과 재밍을 통해 차단시키고 비정상적인 상황이 된 RQ-170은 자동비행 모드로 전환, 기(旣)계획된 착륙기지인 아프가니스탄의 미군기지로 복귀하게 초기 설정되어 있었으나 미군기지 좌표를 이란의 비행기지로 변경입력함으로써 RQ-170은 이란의 비행기지가 아프가니스탄의 미군기지로 착각하고 이동 및 정상 착륙을 통해 탈취[8]된 것이다.

이란은 2011년 탈취한 RQ-170을 이용하여 역공학적 기법(reverse engineering)으로 연구를 수행하여 2013년 해당 무인기로부터 추출한 비디오 영상을 공개, 무인기 내 수집된 모든 영상 및 각종 정보를 복호화 완료하였다고 주장하고 RQ-170을 복제하여 사용할 것임을 발표하였다.

Fig. 4. 미 RQ-170을 복제한 이란의 신형 전투무인기

이후 이란은 공식 성명을 통해 2016년 10월 RQ-170 무인기의 역설계에 성공하여 이란 혁명 수비대(Iranian Revolutionary Guard)의 신형 전투무인기인 'Thunderbolt(또는 Saegheh)를 발표[9]하였다. Thunderbolt는 이스라엘 정찰용으로 사용 중인 것으로 밝혀졌다.

이란의 미국 RQ-170 스텔스 무인기의 탈취 사건을 통해 북한도 언제든지 이러한 사이버전자전 기술을 이용, 우리군이 운용하고 있는 무인체계(무인기, 무인수상전투정 등)에 대해 공격 및 탈취가 가능할 것으로 보이며 탈취된 무인체계는 역공학 및 복제를 통해 언제든지 대한민국 및 군의 안보에 위협을 가할 수 있어 이에 대한 대비가 필요할 것이다.

3.3 사이버전자기 공간을 이용한 민간 침해 사례

위에서 살펴본 군사분야에서의 사이버전자전 사례와 더불어 민간분야에서도 종종 발생하고 있는 사이버전자기 공간을 이용한 침해 사례에 대해 살펴보자.

2015년 미국 FBI는 민간 여객기 기내에서 기내 Wi-Fi 통신망을 이용하여 항공기에 대한 물리적 침해를 시도하였던 사실을 확인하였다. 미국 덴버 소재의 IT 보안업체에 근무하는 크리스 로버츠라는 보안 전문가는 미국 유나이티드 항공기 여객기에 탑승 후 기내용 Wi-Fi 시스템을 악용하여 항공기를 20여 차례 해킹한 사실이 적발되었다. 해당인은 entertainment용 기내 Wi-Fi에 접속한 후 항공기 조종에 필요한 IT 장비의 관리자 권한을 획득하여 항공기 운항 관리 시스템에 접근, 관제탑 송수신 내역을 획득하고 항공기 엔진까지 작동할 수 있는 권한까지 획득한 것으로 확인[10]되었다.

이러한 침해는 항공기 인근에서 Wi-Fi에 접속하여 침해한 사례이지만 그 이외에 관제탑 주변에서 항공기 위치탐지시스템과 항공정보교류시스템 등 관제에 관련된 통신망에 접속하여 해킹한다면 비행 중인 항공기를 추락시킬 수 있다는 정보도 존재한다. 일부 해커는 자신이 직접 만든 어플리케이션(app)을 이용하여 운항 중인 여객기의 조종은 물론 기내 시스템까지 마음대로 조종할 수 있다고 주장하는 등 여객기 해킹이 자칫 테러에 활용될 수 있다는 가능성도 있다는 우려가 있다.

위의 사례는 운항 중인 항공기에 대한 해킹 시도였지만 더 넓게 생각하면 항공기뿐만 아니라 움직이는 이동수단에 대한 침해가 얼마든지 가능하다고 볼 수 있다. 항공기 해킹에 대해 연구하였던 미국 보안 기업 아이오인터렉티브에서는 위성 장비의 취약성을 발견하고 항공기, 선박, 군사작전, 산업시설 등에 쓰이는 통신 링크를 중간 탈취하여 혼란을 줄 수 있다고 경고하고 있다. 또한 위 업체의 직원인 루벤 산타마타 연구원은 지상에서 항공기를 관제 및 통제하는 위성에 침투하여 비행 중인 항공기 네트워크 침투에 성공하는 사례를 보이고 있다. 위성 터미널을 이용하여 기내 Wi-Fi에 접속하는 방식인 침해는 공격자가 쉬운 암호를 재설정하거나 하드코딩된 계정 정보를 활용, 위성 데이터 유닛을 통제하는 침해방식[11]이다.

항공기에 대한 침해시도 뿐만 아니라 바다 위를 항해하는 선박에 대한 해킹도 지속되고 있다. 최근 자율운항 선박 등 선박시스템에 대한 ICT 정보통신기술이 적용되면서 사이버공격에 대한 위협이 커지고 있는 실정이다. 2018년 9월, 한국 정보통신기술진흥센터에서 발행된 주간기술동향 보고서에 따르면 최근 보안 취약점을 악용한 공격으로 해운물류 시스템이나 항만시스템이 피해를 입는 사고가 실제 발생하고 있다. 영국, 싱가포르 등 세계 해운회사들이 사이버침해공격으로 선박 및 해운관련 중요 데이터가 유출되고 시스템이 다운되는 사고가 발생[12]하였다. 침해자는 선박에 사용되는 위성통신장치 시스템의 보안 취약점을 이용하여 선박 내부의 제어장치에 침투할 수 있는 것으로 이 취약점은 점차 위성통신을 이용한 선박 운항 기

술에 중요한 문제점으로 작용할 수 있으며, ICT 기술이 적용되는 민간 선박뿐만 아니라 전투임무를 수행하는 함정, 항공기 등 플랫폼 기반의 군 장비에서 해당 기법을 활용한 공격이 가능하다는 가능성은 충분히 있다고 볼 수 있어 이에 대한 대응책 마련이 필요하다.

4. 주변국 및 육·공군의 사이버전자전 발전 동향

4.1 미국의 사이버전자전 동향

2장에서도 언급하였듯이 미국은 2011년 이란 상공에서 이란의 핵시설을 정찰하던 미국의 무인기 RQ-170이 이란에 나포되는 사건을 통해 본격적인 사이버전자전에 대한 연구를 시작하게 되었다. 이후 미 육군에서 최초로 2013년 본격적인 사이버전자전 교리, 제대별 부대 편성 및 교육훈련 등의 사이버전자전 수행을 위한 계획을 수립하고 추진하기 시작하였다.

이후 2017년 3월 미 합참의장에 의해 발사 직전 교란 즉, Left of Launch 개념을 발표하였고 실제로 북한은 2017년 총 6차례에 걸친 무수단 미사일을 8발 발사하였지만 이 중 1발만 성공하고 나머지 7발은 대부분 발사 직후 폭발하거나 발사와 동시에 폭발해 발사 차량까지 손상을 입게 되었다. 이러한 실패는 미국의 Left of Launch 작전이 개입되었다는 주장[13]이 크다.

이란에 의한 피해와 북한을 상대로 한 성공 등 사이버전자전의 중요성을 인식하게 된 미국은 2014년 사이버와 전자전 영역을 통합한 사이버전자기 활동 개념을 도입하고 이후 사이버전자전 작전 교리를 발전시키고 있다. 2018년에는 사이버전자기 활동팀을 미 육군 군단과 여단급까지 추가 편성하며 미 육군의 전 영역 작전에 대한 사이버전자전 지원을 지속하고 있다. 사이버전자기 활동(CEMA)팀은 미 본토 활동에서 범위를 확대, 인도태평양 통합전투사령부에서 12CEWS[2] 대대를 창설하여 미군 작전에 있어 전 영역에 대한 작전지원을 지속하고 있다.

4.2 중국의 사이버전자전 동향

중국은 2015년 12월 31일 시진핑 국가주석의 지시로 '전략지원군(SSF, Strategic Support Force)을 창설하고 이 전략지원군 예하에 사이버전자전 작전을 수행하는 부대를 창설하였으며 기존의 네트워크부대, 전자전부대, 우주전 부대를 통합[14]하였다.

중국의 전략지원군의 창설 배경은 4가지로 볼 수 있는데 ① 합동작전 능력 강화를 위한 필요성 ②정보전에 대한 개념을 구현하기 위한 필요성 ③ 중국의 전장 영역이 확대되면서 전략지원부대의 필요성이 제기되었으며 ④ 사이버전자 전장환경에서 중국의 3전 중 하나인 심리전을 수행하기 위함이다. 중국의 전략지원군은 기존의 우주전, 사이버전, 전자전, 심리전과 관련된 부대들을 단일 조직으로 통합하고 통합된 부대들을 세부적으로 조정하면서 보완하는 개념으로 조직을 발전시키고 있다.

중국의 전략지원군 예하에는 총 6개의 참모부가 있으며 이중 관심 있게 봐야 할 참모부가 '네트워크시스템부'이다. 이 네트워크시스템부에는 사이버전과 전자전 분야와 심리전 분야의 조직으로 구성되어 있는데 중국은 망전일체전(網電一體戰) 즉, 사이버공간과 전자기공간을 하나의 전쟁공간으로 인식하는 개념의 접근방법인데 이 개념을 군에 적용하고자 네트워크시스템부 예하에 사이버전과 전자전 분야를 함께 구성한 것으로 평가된다.

네트워크시스템부에 대해 자세히 살펴보면 예하에 사이버자전부대와 전자전부대로 구분되며 사이버작전부대 예하에는 12개 작전조직으로 구성되어 있고 전자전부대는 전자대항부대와 전구정찰기지로 구성되어 운영[15]되고 있다.

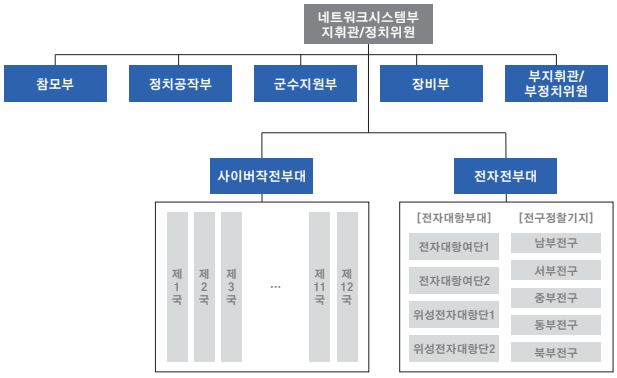


Fig. 6. 중국 전략지원부대 사이버전 관련 조직

중국은 이 네트워크시스템부에 임무를 부여하여 사이버전 전자전 등 각 전장환경의 특성을 활용하여 상대방의 네트워크시스템을 정찰하고 정보를 탈취하는 임무를 부여하였다. 또한 상대방의 네트워크에 침투하여 사이버공

[2] 12CEWS는 정보(intelligence), 정보작전(information operations), 사이버작전(cyber operations), 전자전(electronic warfare), 우주작전(space operations)을 통합하여 수행하는 부대를 의미한다.

간상에서 상대방을 공격하는 활동을 수행한다. 반대로 자국의 사이버공간을 방어하기 위해 사이버공간을 정찰하고 들어오는 공격을 방어하며 자신의 네트워크와 시스템을 보호하는 활동을 수행한다.

박남태·백승조의 논문 '중국군 전략지원부대의 사이버전 능력이 한국에 주는 안보적 함의'에서는 이러한 중국의 네트워크시스템부 예하의 사이버작전부대에 대한 세부적인 정보가 소개되어 있는데, Table 3에는 제1국부터 제12국까지의 구체적인 임무가 소개[16]되어 있다.

중국에 대한 정보는 밝혀진 자료상에 많지 않지만 위에서 소개한 바와 같이 사이버전 분야에 대한 정보는 어느 정도 공개되어 있다. 하지만 전자전에 관한 분야는 비공개가 많은 상황으로 중국은 망전일체전(網電一體戰)을 통해 전쟁에서의 우위를 달성하고자 전략지원군을 창설하였다. 여기에는 사이버전과 전자전의 통합과 발전을 하나의 전쟁수행 방법으로 지정하여 현재도 끊임없이 정보작전을 수행하고 있다. 이에 대한 우리의 대응이 절실한 실정이다.

Table 3. 네트워크시스템부 예하 사이버작전부대 세부현황

기관	임무
제1국	· 암호화, 정보 안전
제2국	· 미국, 캐나다 정보 수집, 위성사진 처리 분석
제3국	· 무선통신 수집 · 관리 사이버 통제
제4국	· 한국, 일본 정보 수집
제5국	· 러시아 정보 수집
제6국	· 위성, 고공 정찰사진, 사이버 데이터 정보수집
제7국	· 사이버공격, 우투무치 방향 위성 관리
제8국	· 유럽, 중동, 아프리카, 남미 정보 수집
제9국	· 전략정보 분석 및 데이터베이스 관리
제10국	· 중앙아시아, 러시아 정보수집
제11국	· 러시아 정보수집 및 분석
제12국	· 위성통신 차단 및 신호정보 분석

4.3 대한민국 육군의 사이버전자전 동향

대한민국 육군은 사이버공간과 전자기스펙트럼 환경하에서 사이버작전과 전자전에서의 승리를 위해 사이버전자전을 미래 지상작전 기본개념에 포함하고 차세대 게임 체인저(next game changer)로 준비하며 지속적인 연구와 발전을 진행[17]하고 있다.

Fig. 7. 대한민국 육군의 차세대 게임 체인저

육군은 2019년부터 본격적인 사이버전자전에 대한 연구를 추진하고 있으며 2019년 5월 육군본부 주도로 육군 사이버전자전 종합발전계획을 수립하여 사이버전자전 업무에 대한 기준과 방향을 제시, 육군정보학교에서는 '사이버전자전 연구 TF'를 구성하여 연구를 추진 및 발전시키는 노력을 보이고 있다.

이후 육군은 지속적인 노력을 이어나가 2019년 9월 이후에는 합참의장 보고 및 육군본부 주관의 자체 토의를 통해 사이버전자전 종합발전에 대한 경과와 진행을 지속 추진해 나가며 구체화에 박차를 가하고 있는 상황이다. 이 노력의 결과로 육군은 육군 자체의 사이버전자전 발전 방향에 대해 연구[18]하고 있으며 사이버전자전 개념을 육군에 구체적으로 적용하기 위해 교리를 발전하고 있다. 또한 육군 교육사를 중심으로 2022년 이후 <육군 사이버전자전> 교범 발간을 목표로 선행연구를 진행 중에 있다.

육군의 이와 같은 자체적인 노력에 더하여 기술개발 측면에서는 국방과학연구소(ADD)와 협력하여 핵심기술 개발을 추진하고 있으며 합참 및 군 유관부서에서 지원 중이다. 국방과학연구소는 사이버전자전에 관한 연구를 전자전특화센터에서 주도적으로 연구하고 있으며 2025년까지 구체적인 사이버전자전 핵심기술을 개발하는 것을 목표로 연구를 진행하고 있다.

4.4. 대한민국 공군의 사이버전자전 동향

공군도 항공우주군 도약을 위해 사이버와 전자전의 개념 통합에 큰 관심을 보이고 있으며 다양한 학술적·기술적 연구를 진행하고 있다. 4차 산업혁명이 불러온 첨단기술의 발전과 관련하여 공군은 "에어포스 퀀텀 5.0(Air Force Quantum 5.0)"이라는 미래 항공우주력 발전 구상 개념을 선보이며 2050년대를 준비하며 공군의 도약적 발전을 준비하고 있으며 2040년까지 공중기반 사이버 및 전자전 무기체계 능력을 구축하는 것을 목표로 구체적인 발전방향을 제시[19]하였다.

공군의 사이버전자전 발전 계획은 '디지털 매트릭스 프로젝트(일명 사이버전자기파 발전계획)'으로 미래전은 사이버 능력과 전자전 능력의 상호 의존적 운용을 통한 전영역 작전에서의 우세 확보가 중요함을 인식하고 총 3단계에 걸쳐 사이버전자전 능력을 확대하는 것을 계획으로 추진하고 있다. 1단계는 2030년까지 사이버 및 전자전 중앙집권적 통제체계를 구축하고, 2단계는 2040년까지 공중기반 사이버 및 전자전 무기체계 능력을 구축, 3단계는 2050년 전후까지 지휘통제 우세 역량을 구축하는 것으로 단계별 목표를 설정[20]하였다.

Table 4. 사이버·전자기파 발전 3단계 계획

구분	1단계 (~2030년)	2단계 (~2040년)	3단계 (~2050년 전후)
목표	사이버 및 전자전 중앙집권적 통제체계 구축	공중기반 사이버 및 전자전 무기체계 능력 구축	지휘통제 우세 능력 구축
응용기술	· 초고속 무선 네트워크 · 빅데이터	· 공중기반 지향성 에너지 기술 · AI기반 전자 재밍 기술 · 협대역 전자기 펄스 발생기술	· 완전자율 AI
목표역량	· ATO체계 내 사이버전, 전자전 작전 통합 · 전장 가시화 체계 · 방호·회복복구 체계	· 공중기반 적극 작전능력 확보 · 전자전기, EMP탄, 탄소섬유탄 · 전투기 탑재 레이저 무기 · 사이버 및 전자전 무기체계	· 선별적 우주우세 지원역량 구축 · 공중·우주 기반 사이버·전자기파 탐지·분석·대응 통합 체계

특히 공군은 공중 전장환경에서 전자전의 유용성과 전자전의 개념에 사이버전을 접목한 사이버전자전 개념에 관심을 보이고 있으며 과거 이스라엘 공군의 시리아 핵시설 공격작전(과수원 작전) 등에서 보인 사이버전자전의 효능을 예시로 삼아 사이버전자전의 중요성을 인식하게 되었으며, 공군 항공기에 사이버전자전 무기체계를 장착하여 임무수행 시 공격 및 방어작전에서 승리를 달성할 수 있는 중요한 요소로 작용할 것으로 예상하고 있다.

공군은 사이버전자전의 중요성에 대한 인식을 시작으로 구체적인 사이버전자전 발전을 위한 활동을 추진하기 위한 준비를 진행하고 있으며 사이버전자전 운영개념 정립과 교리 구축을 위한 사전 준비, 사이버전자전 조직 및 전문인력 확보, 향후 중·장기적 군사력 건설 방향에 대한 논의를 지속적으로 진행하고 있는 상황[21]이다.

5. 해군에게 주는 함의와 사이버전자전 도입 필요성

지금까지 사이버전자전의 기본 개념과 4차 산업혁명의 도래로 강조되는 전자기 스펙트럼 내에서의 사이버전자전 활동의 중요성에 대해 확인할 수 있었다. 4차 산업혁명은 앞으로 ICT 기술을 기반으로 각종 무인기술, IoT 기술을 통해 발전하고 있으며 해군을 포함한 각 군의 작전/전술적 측면에서도 활용되고 있는 상황이다.

실제로 3장의 사이버전자전 수행 사례를 통해 확인 할 수 있듯이, 전자기 스펙트럼의 공간 내에서 침투한 무기체계는 전자기 공간에서 사이버 공간까지 침투하여 적의 지휘통제체계, 무기체계를 무력화하고 적의 정상적인 교전을 실패하게 하는 등 전투에서 승리와 궁극적으로 전쟁에서 승리할 수 있는 중요한 임무를 수행할 것으로 평가된다. 앞으로 큰 발전과 전장환경에서 중요한 영향요소로 작용될 사이버전자전 분야에서 대한민국 해군은 다음과 같은 필요성이 요구된다.

해군이 전통적으로 수행해 온 전자전의 개념에 사이버전 영역을 추가/통합하여 전체적인 전자전 스펙트럼에서의 우위 달성을 위해 사이버전자전의 도입이 필요하다. 해군은 지상군과 달리 해양이라는 전장환경에서 함정, 항공기 등의 플랫폼을 통해 전투를 수행하는 군이다.

해양이라는 특수성은 지상과 달리 지형지물이 없는 환경에서 각종 항해, 무기체계 등의 작동으로 전자파를 이용한 적·아의 상호 접촉이 용이하므로 해군은 과거부터 전자파의 중요성을 인식하여 전자공격, 전자보호, 전자지원 등 다양한 범주의 전자전을 수행하고 있다. 이러한 전자전 수행 개념에서 눈에 보이지 않는 전자파를 이용한 전자전이 단지 적의 전자공격을 방해하거나 적 전파 사용을 거부하는 등의 효과에서 한 단계 발전하여 전자기파를 이용한 사이버공격까지 가능한 기술이 연구·발전되고 있다. 전자파를 이용한 사이버공격 기법이 적 함정, 항공기의 무기체계와 심지어 적 위성 등의 노드를 통해 적 지휘통제체계의 중심부에 접근할 수 있는 가능성은 충분하다고 볼 수 있다.

지상군의 경우 사이버전자전을 수행함에 있어 지형지물을 극복하기 위한 방안으로 UAV, 드론 등을 활용한 사이버전자전을 수행하기 위해 각종 교리발전, 무기체계, 전술 개발에 박차를 가하고 있다. 공군은 공중이라는 전장환경이 해군보다 오히려 지형지물의 영향을 덜 받고 전자파의 도달범위가 넓으므로 항공기를 활용한 전자전을 과거부터 수행하고 있으며 공군 에어포스 퀀텀 5.0 계획을

발표하며 전자전 영역에 사이버 영역을 통합한 사이버·전자기파 발전 계획을 수립하여 추진하고 있다.

이렇듯, 4차 산업혁명이 가져다주는 기술의 발전은 우리가 전투를 수행하는 전장환경과 전투 플랫폼의 임무 및 대응영역의 변화를 요구하고 있다. 시대적 흐름에 발맞춰 우리는 보다 효율적이고 성공적으로 전투에서 승리하고 주어진 임무를 완수하기 위해 전자전의 개념에서 한 단계 발전한 사이버전자전의 개념을 발전시킬 필요가 있다.

6. 해군 사이버전자전 발전 방향

지금까지 사이버전자전의 개념과 중요성, 군사·민간 분야에 대한 사례와 주변국, 대한민국 육군·공군 등 전반적인 발전 추세에 대해 알아볼 수 있었다. 현재까지의 연구를 토대로 앞으로 대한민국 해군이 사이버전자전의 중요성을 체감하고 발전하는 기술에 뒤처지지 않기 위한 노력의 일환으로 발전방향을 제시한다.

6.1 교리 분야

사이버전자전에 관한 개념이 미 육군에서 최초로 시작된 후 세계 국가 및 대한민국도 육군과 KIDA 주도로 점진적인 발전이 계속되고 있다. 공군의 경우도 '에어포스 퀀텀 5.0'이라는 개념을 바탕으로 사이버전자기 활동에 대한 공군의 발전을 2040년을 목표로 단계별 발전시켜 나가고 있는 상황이다.

대한민국 해군은 2020년 5월 4차 산업혁명 첨단기술 구현을 기반으로 한 'SMART Navy 종합발전계획'을 발간하며 '해군비전 2045'을 구현하기 위한 구체적인 청사진을 제시[22]하였다. 해군 사이버전자전의 발전을 위해 'SMART Navy 종합발전계획'상 제시된 안건 중 Table 5와 같이 사이버전자전과 관련된 분야가 많음을 알 수 있다.

Table 5의 내용과 같이 'SMART Navy 종합발전계획'에 사이버전자전 분야를 적용가능한 기술 항목이 다양함을 알 수 있다. 최신 기술들이 점차 무선, IoT 기반의 소형화 되어가고 있는 상황에 따라 무선 환경은 필연적으로 사이버전자기 스펙트럼이라는 공간 내에서 송수신이 이뤄지고 있다. 이에 따라 smart battleship 구현과 스마트 항만/항공기지 운영 등 최신 무선기술을 활용하기 위해서는 이 무선환경을 통해 침투하는 적의 공격을 막을 수 있도록 사이버전자기 공간에서의 방어대책이 요구된다. 물론 사이버 방호에 대한 신기술 및 소요 항목도 제시되어 있지만 사이버공간 이외의 무선 환경인 전자기 스펙트럼 공간에서의 방호는 어떻게 할 것인가에 대한 신기술 연구와 구체적인 교리 발전이 필요하다.

Table 5. 사이버전자전 기술 적용이 가능한 신기술 소요

구분	세부내용
Smart battleship	· 해양무인 무인체계(USV, UAV, UUV) 보호
	· 체계 통합형 smart battleship 보호
	· 네트워크 기반 해상유도무기통제, 해상통합방공체계 보호
	· Smart ship 무선 네트워크 보호
	· 함정용 사이버위협 원격 관제체계
Smart operations	· 센서데이터 기반의 상태기반정비체계(IoT)
	· 스마트 항만/항공기지
	· 드론 경계감시 체계
	· IoT 기반 통합 시설물 관리체계

6.2. 무기체계 분야

사이버전과 전자전이 통합되는 사이버전자전 영역에서 도입하거나 발전시킬 수 있는 무기체계는 어떤 것이 있을까? 해양에서 작전임무를 수행하는 해군에서는 지휘통신을 위해 기본적으로 무선을 기반으로 한 다양한 통신망이 사용되고 있는데 이런 무선통신 기반의 다양한 프로토콜은 사이버전자전의 주요 공격 표적 대상이 되고 있으며 반대로 우리가 발전시킬 수 있는 공격 대상이 될 수도 있다.

적의 지휘통제 무선 통신망에 전자전 공격 기법으로 침투하여 적 지휘통제 시스템에 마비를 주고 이어서 사이버전 공격 기법으로 적의 전술통신망 및 전투체계, 나아가 지휘통제 시스템까지 악성코드를 주입, 아군의 의도에 따라 적의 전투체계 및 각종 시스템을 제어/통제하는 개념의 공격이 가능할 것으로 전망된다.

해양에서 작전임무를 수행하는 우리 전투함에서 단순 우리의 함정 무기체계, 지휘통제체계를 보호한다는 생각에서 생각을 더 확장하여 해양의 우리 함정에서 발사된 사이버전자전 무기체계로 적의 무기체계를 무력화하고 적의 육상 지휘통제체계, 나아가 적 수뇌부의 지휘통제를 마비시킬 수 있는 중요한 공격지점으로 역할을 수행할 수 있다는 큰 그림이 필요하다 생각된다.

앞서 언급했던 사이버전자기 스펙트럼 전 분야에 대해 다양한 사이버전자전 공격이 가능한데 대표적인 공격기술 사례[23]를 다음 Table 6와 같이 정리하였다.

Table 6. 사이버전자전 공격기술 사례

통신계층	공격기술	세부내용
물리 계층	PUE	· 사용무허가 공격자가 사용허가자를 사칭하여 스펙트럼 자원독점(DOS 효과)
	OF	· 공격자가 전송 매개변수를 조작하여 재계산하도록 강요하여 통신방해
	OSU	· 공격자가 네트워크에 지역적으로 인접하여 secondary 네트워크 사용자로 가입하여 primary 네트워크 피해 야기
	재밍	· 재밍을 유도하여 DOS 유도
데이터 링크 계층	SSDF	· 공격자가 잘못된 스펙트럼 센싱 정보를 주변 노드들에게 전달하여 주변 노드가 잘못된 스펙트럼 선택을 하도록 유도
	CCSD	· 동시간에 다수의 사용자가 통신을 요청할 때 공동 채널에 병목현상 유발
	CCC 재밍	· 수신자가 유효한 제어 메시지를 미수신하도록 CCC재밍(네트워크 비정상 동작)
네트워크 계층	HELLO 잠식	· 강한 세기의 신호를 모든 노드에 broadcastiong하여 공격자의 노드 주변노드로 오인하게 함으로써 패킷 포워딩
	Ripple	· 공격자가 잘못된 채널 정보를 퍼트려 네트워크 혼란 상태 유발
	싱크홀	· 공격자가 특정 노드로 가는 최적경로에 공격자 노드가 포함되도록 거짓 정보를 주변 노드에 전달하여 패킷 가로채기나 패킷 수정
	Sybil	· 공격노드가 많은 수의 거짓노드를 생성하여 네트워크에 잘못된 정보를 전송하여 네트워크의 신뢰성 저하
	웜홀	· 공격자가 메시지를 다른 네트워크에 터널링하여 메시지 재현
전송 계층	암호키 고갈	· 공격자가 반복적으로 세션을 생성하도록 유도하여 암호키 생성 패턴을 파악하여 시스템의 암호체계 공격
응용 계층	CR 바이러스	· 노드를 바이러스에 감염시켜 주변 노드에 잘못된 상태정보를 송신하고 이를 통해 네트워크가 학습하여 공격자 의도대로 오판 유도
	정책 공격	· 공격자가 부당한 스펙트럼 접근을 통해 radio 정책변경 또는 갱신불가 야기
다계층	Jellyfish	· Radio의 포워딩/라우팅 기능을 사용하여 통신 흐름을 폐쇄 루프로 만들어 통신 지연이나 패킷 로스 유도
	Lion	· 물리계층 PUE를 사용하여 TCP 연결 방해
	라우팅 정보 재밍	· 라우팅 정보 교환 전 스펙트럼 handoff 발생토록 재밍

Table 6의 내용처럼 사이버-전자 스펙트럼 영역에서 다양한 전문 공격기술이 존재하며 민·관·군이 하나가 되어 개발 및 도입해야 할 것이다. 이와 관련하여 Table 7의 내용과 같이 무기화 가능한 기술로 국방과학연구소의 핵심기술과 육군에서 중점적으로 추진하고 있는 기술[24] 등이 있다.

Table 7. ADD 및 육군의 사이버전자전 무기체계 개발 현황

통신계층	연구 무기체계	세부내용
국방과학연구소 (ADD)	머신러닝 기반 추락유도 기술	· GPS 신호기만을 이용, 적 무인기 침투 시 적 위성항법을 재밍하여 계획된 경로 이탈을 야기, 특정지역으로 추락/이동 유도
	사이버전자전 송신기술	· 적 네트워크, 통신 및 전자전 장비에 전자기파를 이용 주입할 수 있는 사이버 악성코드를 송신 및 주입하는 기술
	사이버전자전 통신망 침투접점 검출기술	· 보안이 취약한 적 통신망에 대해 침투접점을 자동 검출, 적 통신망의 상태를 분석할 수 있는 전자기파 송출 기술
대한민국 육군	전술 EMP	· 강력한 전자기파로 회선 마비
	Mobile 무기체계	· 모바일 네트워크로 기지국 장악 SNS, 메시지, 악성코드 전송
	무선 네트워크 공격무기	· 전자기파를 통한 악성코드 주입
	다기능 ES/EA	· 전자방해 및 교란 기능에 추가하여 무력화 기능 개발
	디지털포렌식 분석장비	· 컴퓨터/모바일 장비 데이터 복원 침해 시 알고리즘 분석
	전자기스펙트럼 가시화체계	· 적 전자파 분석, 제대·병종별 부대위치, 장비 등 가시화

미 육군에서 최초 발전이 시작된 사이버전자전 관련 무기체계는 국방과학연구소 주도의 핵심기술 개발이 진행되고 있으며 대한민국 육군에서는 이를 적용하기 위한 노력이 지속되고 있다. 우리 해군은 이러한 세계적인 추세에 맞추어 해상에서 적용 가능한 사이버전자전 무기체계에 대한 도입 노력이 필요할 것이다. 이를 위해 국방과학연구소 및 기타 연구부서에 적극적인 무기체계 관련 소요와 필요성을 제시해야 할 것이다.

해군은 해양작전이라는 특수성과 지상과 같이 산악지형으로 공간의 제약이 없는 해양이라는 전장환경에서 작전을 수행하고 각종 전자파를 사용하는 탐지 및 무기체계를 이용하여 전투를 수행하고 있다. 함정에는 전자전이라는 직별이 별도로 있으며 전자공격 및 전자보호, 전자지원 및 각종 전자파 수집 등 다양한 전자전 임무를 수행 중이며 전자파를 이용한 적의 R/D, 주요 자산, 시설에 대한 접근이 용이하므로 여기에 사이버공격의 영역을 접목시킨다면 해상에서의 사이버전자전은 우리 해군의 주요한 작전의 분야로 성장 가능할 것이다.

6.3. 동맹국과의 국제협력 활동 강화

사이버전자전의 중요성이 점차적으로 커지는 가운데 미 해군 및 주변국에서도 이와 관련된 무기체계와 각종 활동이 활발해지고 있는 상황이다. 해양을 통해 동맹국 간의 상호 협력과 훈련이 이어지는 환경을 활용하여 사이버전자전 영역에서의 상호 교류와 훈련을 통해 발전을 기대할 수 있다. 한 예로 유럽의 나토 회원국들은 사이버 공간에서의 국제적 교전규칙인 '탈린 매뉴얼'을 발간하여 사이버 공간에서의 작전환경을 조성[25]하고 매년 나토 회원국 간에 사이버 방호훈련인 '락드 쉴즈(Locked Shields)'를 시행하여 사이버방호 태세를 강화시키고 있다. 우리나라는 국가정보원이 2021년 4월 처음으로 위 훈련에 참가[26]하며 사이버 방호태세 향상에 노력하고 있다. 또한 나토 회원국 간에 협약을 체결하여 회원국이 사이버공격을 받을 시 집단 자위권을 발동할 수 있는 조약을 마련하는 등 상호 보호를 위해 노력[27]하고 있다.

우리나라가 위치한 동북아시아의 경우 중국 견제를 위해 미국을 중심으로 중국견제 협의체인 '쿼드(Quad)'에 우리나라를 포함하려는 움직임이 커지고 있고, 최근 미국은 영어권 5개 나라의 정보 공유 동맹인 '파이브 아이즈(Five Eyes)'에 한국과 일본, 인도와 독일을 포함하려는 노력이 미 하원 군사위원회를 통과[28]하는 등 각종 협의체를 통한 군사 활동이 강화되고 있는 추세이다. 해양을 기반으로 동맹국과의 협력을 지속하는 우리 해군도 이러한 협의체를 적극 활용하여 사이버전자전 방호태세 강화를 위한 활동을 이어나가야 할 것이다.

7. 결론

불과 몇 년 전까지만 하더라도 '사이버전에 준비해야 한다'고 주장하며 사이버전 조직과 관련 기술에 대한 연구를 열심히 추진하였던 우리군은 또 다시 새로운 상황 즉, 사이버전자전이라는 전장환경에 직면하게 되었다.

사이버전자전이라는 개념을 이해하면서 우리는 사이버의 영역과 전자전의 영역이 사실은 하나의 큰 전자기파 스펙트럼의 범주 내에 있는 개념임을 인식할 수 있게 되었다. 먼저 본 연구의 중심이 되는 사이버전과 전자전, 사이버전자전이 모두 하나의 큰 틀 안에 포함된 개념임을 알 수 있었다. 사이버와 전자파의 영역이 거시적으로는 컴퓨터 네트워크 프로토콜의 개념인 OSI 7계층 구조 내에 포함된 개념임을 알 수 있었다.

또한 과거의 사이버전자전이 적용된 작전의 사례를 통해 사이버전자전의 중요성과 각 국가의 발전 동향을 통해 우리군도 앞으로 이 분야에 대한 준비가 정말 필요하다는 필요성도 인식할 수 있게 되었다.

우리 해군도 미 육군에서 개념발전된 사이버전자전에 대한 개념을 빠른 시일 내 적용하여 다양한 교리, 조직, 무기체계 등의 발전을 중·장기적인 관점에서 발전시켜야 할 것이다.

본 연구는 사이버전자전의 중요성과 필요성, 주요 국가의 발전동향과 대한민국 육·공군의 사이버전자전 관련 동향과 발전양상을 살펴보고 우리 해군의 현실태와 나아가야 할 방향을 제시하였다. 해군은 해양이라는 전장환경에서 작전을 수행하며 지상군과 다른 전투함정 전방으로 지형지물이 없는 개방된 공간에서 임무를 수행하는 특성이 있다. 그렇기 때문에 전자파에 의한 노출이 상존하여 과거부터 전자전에 대한 작전개념의 발전과 전력 발전이 중요하였다. 다만, 사이버전의 능력을 접목시키는 능력은 아직 걸음마 단계라 평가할 수 있다. 물론 사이버전과 전자전의 능력을 통합하려는 사이버전자전 개념은 육군, 공군 모두 시작하는 과정이다.

우리 해군이 앞으로 적용해야 할 방안에 대한 연구, 이를 중·장기적으로 발전시켜 나가야 할 정책과 추진력이 무엇보다 중요할 것이다.

후기

1945년 손에 잡히는 아무것도 없는 시절 해군의 아버지 손원일 제독의 창군정신을 생각해 봅니다. 대한민국 해군이 초심을 잃지 않고 명예, 헌신, 용기라는 정신을 이어나가 새로 맞이하는 4차 산업혁명 시대에도 필승하는 해군이 되길 소원합니다. 이를 위해 새로운 전장환경인 사이버전자전에서도 승리하기 위한 새로운 방안과 노력이 필요할 것이 분명합니다. 본 연구는 부족하지만 그 중요성을 인식하고 앞으로 나아갈 방향을 제시하였습니다. 저의 부족한 연구가 조금이나마 해군의 발전에 도움이 되길 소망해 봅니다.

참고문헌

[1] 백연상, "美무인기 포획 방법, 이란 엔지니어 주장 들어보니…," 동아일보, 2011.12.17.
[2] 이용수, "북 무수단 발사 잇단 실패 뒤엔…美 'Left of Launch' 작전 있었다," 조선일보, 2017. 3. 6.

[3] 손태종 외, “한국군 사이버전 및 전자전 통합개념 정립 방안,” 한국국방연구원, 2017, p. 35.
[4] 김형균 외, “스마트 전자전: 사이버전자전,” 국방신기술동향분석, 통권38호(2016), p. 36.
[5] 김진용, “육군 사이버전자전 발전 방향,” 군사평론 제467호(2020), p.11.
[6] 이광일, 이승근, “사이버전자전 기술 개발동향,” 국방신기술동향분석 제9권(2014) p. 24.
[7] 황성인, “항공우주군 도약을 위한 사이버전자전 발전방안 연구,” 군사과학논집 제71권 1호(2020), p. 46.
[8] 안두원, “이란, GPS 좌표 교란해 미 무인기 탈취,” 세계일보, 2011.12.16.
[9] David Cenciotti, “Iran unveils new UCAV modeled on captured U.S. RQ-170 stealth drone,” The Aviationist, 2016.10.2.
[10] 전경웅, “와이파이 가능, 여객기 해킹 무방비? 테러 위험!,” NewDaily, 2015.5.19.
[11] 김인순, “항공기도 해킹한다,” 전자신문, 2018.7.2.
[12] 김국배, “해적이 사이버 공격까지… 선박 해킹 빨간불,” 아이뉴스24, 2018.9.16.
[13] 홍기삼, “연이은 북 미사일 실패, 미 미사일무력화 사이버전 영향?,” News1, 2017.4.6.
[14] 송운수 외, “사이버억지 수단으로서의 사이버전자전 작전수행개념,” 한국군사학논집, 제77권 1호, 2021, p. 506.
[15] 박남태 외, “중국군 전략지원부대의 사이버전 능력이 한국에 주는 안보적 함의,” 국방정책연구, 통권 131호, 2021, p. 149.
[16] 박남태 외, “중국군 전략지원부대의 사이버전 능력이 한국에 주는 안보적 함의,” 국방정책연구, 통권 131호, 2021, p. 151.
[17] “미래전장 판도 바꿀 차세대 게임체인저 개발,” 연합뉴스, 2019.12.3.
[18] 김진용, “육군 사이버전자전 발전 방향,” 군사평론, 제467호, 2020, p. 9.
[19] 하수영, “[2020국감] 공군 “‘에어포스 퀀텀 5.0’ 이행력 강화해 항공우주군 도약할 것”,” newspim, 2020.10.15.
[20] 공군, “차세대 스마트비행단 구축…기지방어 작전 범위 확장,“ 국방일보, 2020.5.26.
[21] 황성인, “항공우주군 도약을 위한 사이버전자전 발전방안 연구,” 군사과학논집, 제71권 1호, 2020, p. 52.
[22] 박동선, “4차 산업혁명 첨단기술 기반의 ‘SMART Navy’ 大항해 계획,” 대한조선학회지, 제57권 제1호, 2020, pp. 7-10.
[23] 김형균 외, “스마트 전자전: 사이버전자전,” 국방신기술동향분석, 통권38호, 2016, p. 38.
[24] 전상혁 외, “육군과 사이버전자전,” 군사평론, 제469호, 2020, p.38.
[25] 이민효, “사이버전에 적용될 국제법에 관한 Tallinn Manual 고찰,” 인도법논총 37호, 2017년 12월, pp. 9-42.
[26] 홍지인, “국정원, 나토 주관 사이버 방어훈련 ‘락드실즈’ 첫 참가,” 동아사이언스, 2021.4.14.
[27] 김병수, “나토 “회원국이 사이버 공격 받으면 집단안보 발동할 수 있어”,” 연합뉴스, 2018. 4. 5.
[28] 박병수, “미국, 정보동맹에 한국 포함시킨다…하원 군사위 통과,” 한겨레, 2021. 9. 3.