https://doi.org/10.33778/kcsa.2021.21.4.059

독일의 사이버전 대응 정책변화를 통해 본 한국군 사이버전력 발전 방안에 관한 연구★

박 상 준*, 김 태 산**, 김 지 원***, 정 찬 기****

요 약

미래전장은 현대전의 주 영역인 지상, 해상, 공중과 더불어 사이버공간 및 우주영역을 포함한다. 사이버공간은 컴퓨터, 유·무선 네트워크를 중심으로 이루어져 있으며, 지상, 해상, 공중, 그리고 우주 영역에 걸쳐 있다. 사이버전은 사이버공간에서 이루어지기 때문에 사이버에 대한 전문성이 없는 사람이 사이버 상황을 인지하기는 쉽지 않다. 따라서 사이버전을 대비하여 사이버에 대한 전문적인 지식과 기술을 보유한 인력 양성이 무엇보다 중요하다. 특히 사이버전의 결과는 이를 수행하는 사이버 전투원의 능력, 사이버 시스템 성능, 사이버전 수행절차의 숙련도 등에 따라 크게 달라질 것이다. 한국군은 사이버작전사령부를 중심으로 각급 제대에 사이버전에 대응하기 위한 전력을 갖추고 있으나 빠르게 확대되는 사이버공간을 모두 방어하는 데 한계가 있다. 본 논문에서는 이러한 한계를 극복하기 위해 독일의 사이버전 대응 정책변화를 살펴보고 이를 토대로 한국군 사이버전력 발전 방안을 조직구조, 무기체계, 교육훈련체계로 구분하여 제시한다.

A Study on the Direction of Cyber Forces Development in the Korean military throu-gh Changes in Germany's Cyber Warfare Response Policy

Sangjun Park*, Taesan Kim**, Jee-won Kim***, Chan-gi Jung****

ABSTRACT

The Future Battlefield includes the main areas of modern warfare, including the ground, sea, and air, as well as cyberspace and space. Cyberspace consists of computers, wired and wireless networks, and spans the ground, sea, air, and space domains. Cyber warfare takes place in cyberspace, so it is not easy for people without expertise in cyber to recognize the cyber situation. Therefore, training personnel with professional knowledge and skills in cyber is paramount in preparation for cyber warfare. In particular, the results of cyber warfare will vary greatly depending on the ability of cyber combatants to carry it out, the performance of cyber systems, and the proficiency of cyber warfare procedures. The South Korean military has power to respond to cyber warfare at various levels, centering on the Cyber Operations Command, but there is a limit to defending all the rapidly expanding cyberspace. In this paper, to overcome these limitations, we looked at the changes in Germany's cyber warfare response policy. Based on them, the organization structure, weapon system, and education and training system of future Korean military cyber forces are presented separately.

Key words : cyber warfare, cyber forces, German Cyber-intelligence Army, weapon system, training system

접수일(2021년 09월 27일), 수정일(2021년 10월 28일), 게재확정일(2021년 10월 31일)

★ 본 논문은 육군사관학교 사이버전 연구센터의 2021년도 연구활동비 지원을 받아 연구되었음.

* 육군사관학교 전자공학과

** 육군사관학교 군사사학과

*** 국방보안연구소

**** 아주대학교 국방디지털융합학과, 교신저자

1. 서 론

미래전장은 현대전의 주 영역인 지상, 해상, 공중과 사이버공간 및 우주영역을 포함하는 다영역으로 구성될 것이다. 이 중에서 사이버공간은 컴퓨터 단말기, 유·무선 네트워크를 중심으로 이루어진다. 사이버공간에서 이루어지는 사이버전은 사람이 인지하는 것이 매우 어렵기 때문에 관련 분야에 대한 전문적인 지식과 기술을 보유한 인력의 양성이 매우 중요하다. 특히 군사작전 영역에 속하는 사이버전은 이를 운용하는 사이버전투원들의 능력과 구비된 시스템 성능과 사이버전 수행절차의 숙련도 등에 따라 그 결과는 매우 크게 달라질 것이다.

한국군은 사이버작전사령부를 위시하여 사단급 제대까지 사이버전에 대응하기 위한 전력을 갖추고 있으나 사물인터넷 기술 등 4차 산업혁명 기술의 발전으로 점점 더 확대되어 가는 사이버공간을 모두 방어하기에는 한계가 있다. 특히 북한의 사이버전 능력은 조선컴퓨터센터, 광명정보기술회사 등 약 17개의 해킹지원조직과 약 1,700여 명의 해킹실행조직이 사이버공간 상에서 심리전, 정보수집, 테러, 사이버전 분야로 나누어 활동하는 것으로 판단하고 있다[1]. 그러나 한국군은 사이버전이 새로운 전장영역으로 미래전쟁에서 매우 큰 비중을 차지할 것이라는 인식이 부족하다. 이로 인해 군단급 이상 제대에서 사이버방호 및 지원을 하는 CERT를 운용하고 있으나, 사회공학적 기법을 활용한 사이버전, 물리전과 연계한 사이버전 등 다양한 사이버전의 형태에 대한 대비가 부족한 실정이다[2].

최근 인공지능, 사물인터넷 기술 등 4차 산업혁명 기술이 무기체계에 적용되면서 전장환경은 초지능화, 초연결화되고 있고 국방환경은 빠르게 네트워크와 소프트웨어로 바뀌고 있다[3]. 이에 따라서 국방 분야의 사이버안보는 소프트웨어 개발과 보증 문제 등에 있어서 더욱 전문성이 요구되고 있다. 이러한 사회의 변화에 따라 미국, 중국, 독일, 일본, 러시아 등은 사이버사령부를 창설하고 지속적으로 사이버역량을 강화해 나가고 있다[4]. 이중 독일은 사이버전에 효과적으로 대응하기 위해 2017년 사이버정보군을 창설하여 현재 세계적으로 23개 지역에서 약 14,500여 명이 활동하고 있으며, 독일 사이버정보군은 IT 기술을 활용하는 것뿐만 아니라 전자전 분야까지도 아우르고 있어 우리군이 벤치마킹하기에 가장 적절하다고 판단된다.

이에 본 논문에서는 이러한 독일 연방 사이버정보군의 정책변화를 분석해 미래전에 대비하기 위한 한국군 사이버전력의 발전 방향에 대해 살펴보고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 사이버전력 발전 방안에 대한 관련 연구를 살펴보고, 3장에서는 독일의 사이버정보군 발전과 운용현황을 통해 사이버전 대응 정책변화를, 4장에서는 미래 한국군 사이버전력의 발전 방향을 제시하고, 5장 결론을 통해 요약 및 향후 추진 방향을 제시한다.

2. 관련 연구

사이버전이 하나의 전장 영역으로 자리매김해 감에 따라 사이버전 관련 연구가 활발하게 진행되고 있다. 그러나 사이버전력의 향상 방안에 대한 연구는 군사보안 유지 등의 이유로 제한적으로 진행되고 있다.

그중 한국군의 합동 사이버작전 강화방안 연구에서는 합동작전과 연계하여 한국군의 사이버작전에 대한 현상을 진단하고 작전 개념과 조직 및 운영 체계를 강화하는 방안을 제시하였다[2]. 이 연구에서는 사이버작전을 위한 조직의 역할 및 기능을 제시하면서 합참에서는 공세적 사이버작전을 제안하였고 작전사, 군단 및 사단에서는 방어적 사이버작전을 수행할 것을 제안하였다.

사이버전 위협과 우리의 대응방안 연구에서는 사이버 안보환경의 변화와 위협 행위를 분석하고, 한국군의 사이버 역량강화를 위해 수행체계, 소프트웨어 방위산업, 사이버전사 교육훈련 방안 등을 제시하였으며[3], 미래 사이버전력 획득방안에 관한 고찰에서는 사이버 심리전에 대한 대비책, 첨단기술 개발 및 인력양성과 사이버군 창설과 사이버 무기체계와 훈련체계를 작전개념에 부합되게 획득할 필요성이 있음을 주장하였다[5].

사이버전 수행절차 운영개념에 관한 연구에서는 록히드 마틴(Rockheed Martin)에서 제시한 사이버 킬 체인(Cyber Kill Chain) 모델과 국내에서 제안된 사이버 킬 체인 체계를 살펴보고 이들의 한계점을 극복

하기 위한 능동적 방어 기반의 사이버전 운영개념 프레임워크 구축방안을 제기하였다. 제시된 프레임워크는 사이버공간 정보·감시·정찰, 사이버 방어, 사이버 전투피해평가의 기능 분야와 사이버 지휘통제 기능의 상호 정보교환 및 통제관계를 정의하고 구축방안에 대한 시나리오를 제안하였다[6].

사이버공간에서의 효과중심작전 적용방안 연구에서는 걸프전 당시 미군이 항공력을 중심으로 수행한 효과중심작전의 개념을 사이버공간에서 적용하는 방안을 제기하였다. 이 연구에서는 효과중심작전 수행을 위해서 군사전략 목표·수단·방법과 공격대상 및 효과를 제시하였다. 또한 효과중심작전의 한계점을 간략하게 소개하고 향후 피해평가 측정방안에 대한 연구의 필요성도 제기하였다[7].

사이버전 훈련과 관련한 연구로는 국방과학연구소의 사이버전 모의분석 도구(CMT, Cyber Warfare Modeling Technology using LVC)가 있다. 이 모의분석 도구를 활용하여 더욱 다양한 사이버전 훈련을 할 수 있도록 훈련 시나리오 저작 방법을 발표한 연구가 발표되기도 하였다[8].

미국 軍은 사이버전문인력에 대한 효과적인 양성과 관리를 위해 국가 차원의 국가사이버보안교육체계(NICE)와 국가사이버전문인력체계(NCWF)를 표준과 근거로 활용하여 국방 사이버전문인력체계(DCWS), 국방 사이버인력 자격표준(DoDD 8140/8570) 등 군 사이버 전문인력의 임무에 특화된 통합적-유기적-체계적인 군 사이버 전문인력 양성 및 관리체계를 구축하였다[9].

이스라엘은 사이버 전문인력 양성에 대해 군 조직이 적극적으로 개입하여, 고등학생을 대상으로 최상위 영재 50~60명을 선발하여 최첨단 기술 부대를 양성하는 탈피오트(Talpiot) 프로그램 등 의무복무와 연계하여 군에서의 교육이 경력경로 구성 및 인력의 민간 활동으로 이어지는 특징을 보인다.

영국은 2016년 국가사이버보안전략을 발표하고 국가보안과 회복력을 유지할 수 있는 사이버 전문가 양성의지를 천명하였다. 이를 위해 국방부 산하의 합동사령부(Joint Forces Command)내에 사이버방어를 담당하는 군사조직인 사이버 예비군(Cyber Reserve)을 구성하고 사이버공간에서의 각종 군사활동을 추진하고 있다.

3. 독일의 사이버전 대응 정책변화

3.1 독일 사이버안보전략의 변화

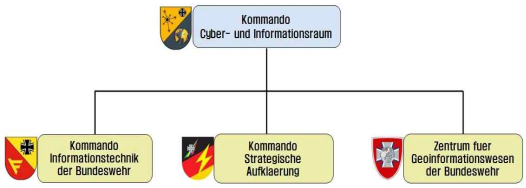
2011년 이전까지 독일의 사이버안보전략은 민간보안 영역이 주된 역할을 하고 독일 연방군은 보조적인 역할을 하는 것이었다. 그러나 사이버공격이 국가주요기관 및 기간산업, 사회기반시설 등을 위협할 뿐 아니라 군사적으로 활용될 수 있는 사례가 나타나면서 독일 정부는 사이버안보의 중요성을 인식하게 된다. 이에 2011년에 '독일 사이버 안보전략(Cyber-Sicherheitsstrategie für Deutschland)'을 발표하였다. 이는 2016년에 최신 사이버 보안 개념을 반영하여 수정되었으며, 이를 통해 독일 사이버 안보를 위한 전략적 지침이 확립되었다[10].

또한 사이버전에 효과적으로 대응하기 위한 군 조직으로 2017년에 사이버정보군이 창설되었고, 현재 세계 23개 지역에서 약 14,500명이 활동하는 부대로 발전하였다. 이 사이버정보군은 국방부 직할부대로 평시에는 전반적인 IT 시스템 운영 및 작전 수행을 위한 정보 및 첩보를 수집하고, 전시에는 각종 전자 및 정보전 임무를 수행한다. 현재 사이버정보군은 첨단장비와 전문인력 확보를 위해 매진하고 있으며, 창설된 지 얼마 되지 않았지만 현재 연방군의 주축으로 자리매김하고 있다. 또한 독일 정부는 사이버안보와 관련한 국가전략의 일환으로 사이버안보조직을 강화하기 위하여 2018년 연방 내무부와 국방부가 공동으로 '사이버안보 혁신을 위한 에이전시'를 설립하여 운영하고 있다[10].

3.2 독일 사이버정보군 조직 편성

독일 사이버정보군은 연방군의 모든 IT 시스템을 운영하며 지속적으로 검색 및 탐지 능력을 강화하여 사이버 영역을 수호하고 있다. 이와 함께 이 부대는 통신 및 전자, 전산 등을 포함한 포괄적인 정보업무를 담당하는 부대로 발전하고 있다.

현재 사이버정보군의 조직은 (그림 1)과 같이 사이버정보사령부(Kommando Cyber- und



(그림 1) 독일 사이버정보군 조직도

Informationsraum) 예하에 연방군 정보기술사령부(Kommando Informationstechnik der Bundeswehr), 전략정찰사령부(Kommando Strategische Aufklaerung), 연방군 지형정보센터(Zentrum fuer Geoinformationswesen der Bundeswehr)로 구성되어 있다. 사이버정보사령부는 사이버 관련 제반 업무를 총괄하는 지휘부로 사이버 정보군의 지휘, 인력 양성 및 보수교육을 계획하며 현재 약 670명이 소속되어 있다[11]. 연방군 정보기술사령부는 독일 연방군 IT 서비스를 총괄하며, IT 보안 및 교육업무를 담당한다. 그리고 그 예하에는 6개의 정보기술대대 및 나토의 통신대대 일부, IT 운영센터, 사이버보안 센터 등이 소속되어 있으며, 현재 약 420명이 근무하고 있다[12]. 전략정찰사령부는 각종 정보를 수집하는 임무를 수행하며 특히 파병에 관한 업무를 지원한다. 즉, 이 부대는 첩보 수집 및 정보 제공을 위한 조직으로 무선정찰, 전자전 등의 임무를 수행한다. 이를 위해 그 예하에는 전자전수행국, 기술정찰 조사부, 작전적 통신센터, 사이버작전 센터 등이 있으며, 여기에 현재 약 550명이 근무하고 있다[13]. 연방군 지형정보센터는 지형 및 기상정보를 다루는 부대로 수집된 지형 및 기상정보를 독일군 전체에 수시로 제공한다. 이를 위해 이 부대에는 생물학, 인류학, 측지학, 지구물리학 등 다양한 분야의 전문가 300여 명을 포함한 약 1,000명이 근무하고 있다[14].

사이버전과 관련된 독일 사이버정보군의 기능에는 심각한 사이버공격에 대한 방어와 민간 당국에 대한 지원, 군 체계 및 인프라에 대한 사이버위협 방어, 공격적 사이버공간 작전, 군사작전을 위한 사이버 효과 개발, 정보작전 및 전자전, 교육훈련과 인력 양성이 있다[10].

3.3 독일 사이버정보군 운용 장비

(그림 2) 독일 사이버정보군 운용 장비

독일 사이버정보군은 다양한 임무를 수행하기 위해 첨단 IT장비들을 운용하고 있다. Micro-PoP 시스템(Micro-Point of Presence), SATCOMBw 통신시스템(Kommunikationssystem SATCOMBw), 지상중계시스템(Terrestrisches Übertragungssystem, TÜtrSys), TETRAPOL 통신시스템(Bündelfunkssystem TETRAPOL Bw), BGAN Explorer 710 위성통신장비(BGAN Explorer 710), KWS RMB Fuchs 장갑차(Kampfwert-Steigerung Radio Multiband), Hummel 전파방해 장갑차(Störpanzer Hummel) 등으로 각 장비들의 형상은 (그림 2)와 같다.

Micro-PoP 시스템은 전 장병이 작전보안을 유지하며 의사소통할 수 있는 시스템으로 1세트에 8명까지 사용이 가능하다. 위성통신망을 통해 원거리 통신 및 독일연방군 IT 시스템에 접속이 가능하다[15].

SATCOMBw 통신시스템은 2Mbps의 전송속도로 음성 및 데이터 전송이 가능한 위성기지국으로 정지궤도 위성인 COMSATBw-1과 COMSATBw-2를 이용한다[16].

TÜtrSys 지상중계시스템은 네트워크 노드 간 중계소 임무 수행을 위한 시스템이다. 광대역 통신장비와 라우터 등으로 구성되며, 100Mbps의 전송속도를 갖는다. 또한 최대 3개 노드와 네트워크 연결이 가능하며, 장비 외부에서 원격으로 네트워크 모니터링을 할 수 있다[17].

TETRAPOL 통신시스템은 제한된 사용자 그룹을 위한 이동형 통신시스템이다. 훈련이나 작전 시 주로 음성 통화용으로 이용되며 통달거리는 25km이다. 그룹통화 기능과 2.4kbps 전송속도로 짧은 데이터 통신 기능을 제공한다[18].

BGAN Explorer 710 위성통신장비는 휴대형으

로 안테나, 트랜스퍼, 송수화기로 구성된다. 음성 및 데이터, 화상 통신을 할 수 있으며 600Kbps의 전송속도를 갖는다. 또한 위성모뎀을 사용하여 인터넷 접속이 가능하다[19].

KWS RMB Fuchs 장갑차는 전투능력을 향상시킨 다채널 장갑차로 레이더 신호를 탐지, 분석할 수 있다. 105km/h의 속도로 800km까지 주행할 수 있어 기동성이 우수할 뿐 아니라 안테나 구동장치 등 모든 장비가 내부에 있어 적의 전자전 공격으로부터 보호받을 수 있다[20].

Hummel 전파방해 장갑차는 VHF/UHF 대역의 적 전파를 감지하고 방해할 수 있는 전자전 장비이다. 송신장치를 통해서 적의 음성 및 데이터 통신을 방해할 수 있으며, 승무원의 활동은 내부에서 이루어지므로 적의 총격으로부터 보호받을 수 있다[21].

3.4 독일 사이버정보군 훈련체계

독일 사이버정보군은 간부 및 모든 소속원의 직무수행 능력 향상을 위해 군사기본훈련, 전투준비훈련, 범국가 사이버안보훈련, 지역 및 동맹방어 훈련 등 개인훈련으로부터 부대훈련에 이르기까지 다양한 훈련을 실시하고 있다.

군사기본훈련은 사격, 행군, 방향 탐지 등의 병 기본훈련과 전문적인 주특기 훈련으로 구성되어 있다. 이러한 군사기본훈련은 부대훈련장, 사격장, 일반 야지에서 이루어지며, 순찰 및 교전요령에 관한 훈련도 포함된다.

전투준비훈련은 부여된 임무를 성공적으로 수행하기 위해서 정보 수집 및 처리, 보호 등에 관한 전문적인 IT 능력을 배양하기 위한 훈련이다. 전투준비 외에도 각종 우발 상황에 대처하기 위한 능력, 파병을 대비한 외국어 능력 향상 훈련도 병행하고 있다.

범국가 사이버안보훈련은 국가 및 주요 기반시설에 대한 사이버공격을 방호하고 연방군을 보호하기 위한 훈련이다. 사이버안보훈련은 사이버 안보와 관련된 부서 및 기관과 공조하여 훈련하며, 이를 통해 사이버전 수행 과정 및 절차를 개선하면서 긴급 상황에 신속하게 대처할 수 있는 능력을 갖추게 한다.

지역 및 동맹방어 훈련은 나토 차원에서 실시하는 훈련으로 사이버정보군에 소속된 지형 및 통신 전문가들이 정보 수집 활동을 하면서 정기적으로 단기간 경보 훈련을 수행한다. 또한 이 훈련에는 국제평화유지 임무 차원에서의 전자전 활동, IT 네트워크 운영병력 파병, 정보기술대대를 통한 지휘통신 연결 지원 등 다양한 임무를 수행하기 위한 훈련이 포함된다.

3.5 독일의 사이버전 대응 정책변화의 시사점

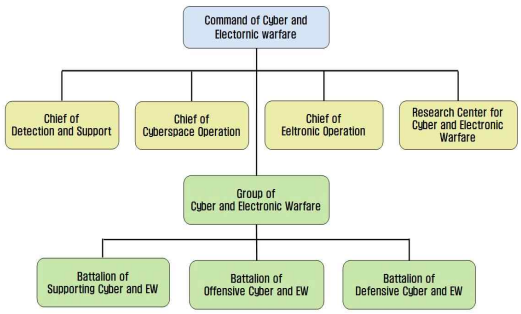
독일은 2011년 이후 사이버안보전략을 수정한 후 사이버정보군을 창설하고 사이버전 관련 대응 체계를 바꿔왔다. 독일 사이버정보군이 임무를 수행하는 전장영역은 통신네트워크 영역, 사이버공간 영역뿐 아니라 전자기영역까지도 포괄하고 있음을 알 수 있다. 즉, 독일의 사이버정보군은 사이버작전, 컴퓨터 네트워크 작전, 전자전을 하나의 조직으로 통합하여 지휘체계를 일원화하고 있다는 것이다. 이는 4차 산업혁명 기술의 발달로 미래전장에서 지능화되고 초연결 네트워크를 통해서 다양한 무인 무기체계와 전투원 및 지휘소 간 밀접하게 정보 송·수신함에 있어서 안정성을 추구하는 것이라 할 수 있다. 따라서 독일이 사이버전에 사이버정보군의 창설과 전력 보강은 미래 전장에서 제5전장으로 불리는 사이버전 영역과 전자전 영역이 밀접하게 연계되어 가고 있음을 시사한다.

4. 한국군 사이버전력 발전 방안

본 절에서는 독일 사이버정보군이 주는 시사점을 토대로 한국군의 사이버전력 발전 방향을 사이버전 조직과 무기체계, 교육훈련 분야로 구분하여 제시한다.

4.1 한국군의 사이버전 조직 발전 방안

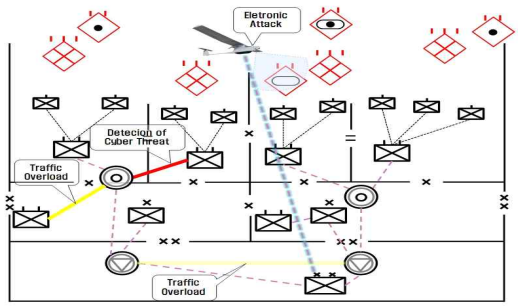
독일의 사례에서도 살펴보았듯 사이버전은 컴퓨터 네트워크 상에서만 이루어지는 것이 아니다. 최근 UAV 및 드론의 군사적 운용이 증가함에 따라 무선 네트워크 취약점을 이용하여 드론을 탈취하거나 강제 착륙시키는 등 전자전 요소를 이용하는 경우도 증가하고 있으며[22], 미국의 경우 사이버공간에서의 작전과 전자전이 연계되거나 상호 융합된 작전 개념으로 발전시키고 있다[23].



(그림 3) 한국군 사이버 조직 발전 방안

한국의 육·해·공군에서 모두 무인기의 도입을 적극적으로 추진하고 있으며, 특히 육군은 드론봇 전투체계를 전력화하기 위해 많은 노력을 기울이고 있다. 이러한 상황에서 사이버전자전 중대가 포함된 사단의 드론봇 전투대대의 편성 방안이 제기되기도 하였고 [24], 4차 산업혁명시대에 적합한 육군 사이버여단 조직 구성방안에 대해서 제안한 연구도 있다[25].

이러한 기술의 발전 및 군사작전 개념의 변화를 고려했을 때 한국군의 사이버전 조직 또한 사이버전과 전자전의 통합된 형태로 변화가 필요하다. 즉 국군정보사령부, 사이버작전사령부 등으로 구분된 조직을 전체적으로 아우를 수 있는 통합사령부가 필요하다. 이러한 통합사령부를 통해서 사단 이하 전술제대까지 사이버전과 전자전이 통합된 군사작전을 수행할 수 있도록 조직의 효율화가 필요하며 그 편성 방안은 (그림 3)과 같다. 미래전장에서는 사이버전과 전자전이 통합된 작전을 수행할 수 있도록 사이버전자전사령부 창설이 필요하다. 사이버전자전사령부에는 지원참모부, 사이버공간작전참모부, 전자전참모부와 연구센터를 두어 관련 참모업무 및 기술연구를 수행한다. 예하부대로는 사이버전자전단을 두고 사이버전자전단 예하에 지원대대, 공격대대, 방어대대를 두어 각 분야의 전문인력을 두어 작전임무를 수행할 수 있도록 한다. 사이버전자전사령부 및 예하부대는 작전술적 측면에서 임무를 수행한다. 전술제대인 군단과 사단에는 정보대대를 확대·개편하여 사이버전자전대대를 두어 사이버전과 전자전에 대한 전술적 수준의 전투임무를 수행하도록 한다. 이때 사이버전자전사령부는 군단 및 사단 예하 사이버전자전대대를 작전통제하여 통합된 군사작전이 이루어지도록 한다.

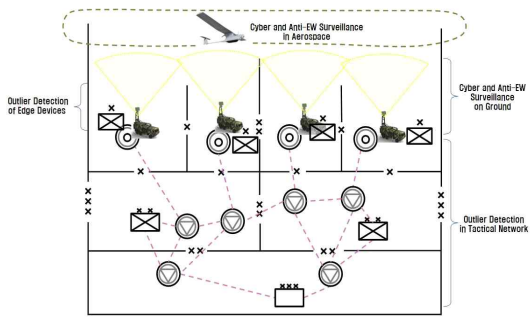


(그림 4) 사이버전 지휘통제체계 구성 방안

4.2 사이버전 무기체계 발전 방안

사이버전 무기체계는 지휘통제체계, 감시정찰체계, 공격무기체계, 방어무기체계로 구분하여 발전이 필요하다. 지휘통제체계는 사이버전자전 전반에 걸쳐 전장상황을 가시화하고 통합된 군사작전을 효율적으로 지휘할 수 있는 체계로 개발되어야 한다. 즉, (그림 4)에서 보는 것처럼 전술제대의 사이버위협 탐지, 네트워크 상태, 전자전 수행 상황 등을 가시화하여 사이버전자전 사령부 및 예하부대에서 적시에 대응조치를 할 수 있어야 한다.

감시정찰체계는 아군과 관련해서는 네트워크의 이상징후 탐지, 단말 장비(End Device)에서의 이상징후 탐지체계가 필요하며, 적군에 대해서는 네트워크 침투 및 전자전공격 효율성 향상을 위한 유·무선 네트워크 취약점 분석 및 대전자전 탐지체계가 필요하다. 사이버전 감시정찰체계는 (그림 5)에서 보는 것처럼 적군에 대한 취약점 분석 및 대전자전 탐지체계를 전술제대의 전방지역의 지상과 적 지역의 공중정찰이 가능

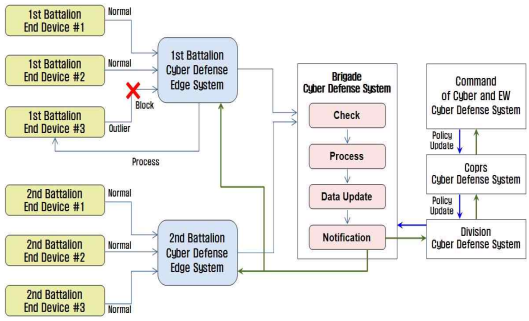


(그림 5) 사이버전 감시정찰체계 운용 방안

한 체계로 운용하여 적의 전파운용 특성과 무선 네트워크 취약점 분석을 수행한다. 아군의 방어작전 측면에서는 전방지역에서 운용하는 단말 장비를 통해 비인가 주파수를 운용하거나 동일 단말 장비에서의 네트워크접속인증 다수 실패 등 최소한의 이상치 탐지 체계를 둔다. 이러한 이상치 탐지 신호 발생시 여단급 이상 제대부터 네트워크 이상치 탐지를 강화할 수 있는 체계를 구축함으로써 사이버전에 대한 감시정찰체계를 확립할 수 있다. 감시정찰체계를 통해 탐지된 적 사이버전자전공격 징후, 적의 네트워크 취약점 분석 결과 등은 아군의 사이버전자전사령부 및 예하 부대에서 운용하는 사이버방어무기체계 및 사이버공격무기체계로 전송되도록 한다. 탐지된 이상 징후에 대한 대응이 가능하도록 다양한 전장상황에서 사람의 눈으로 식별이 어렵거나 동시 다발적인 상황으로 인해 포착이 어려운 상황을 개선하기 위한 인공지능 기반의 체계를 개발한다. 예를 들어 TOD 영상을 분석하여 감시기능을 향상시키기 위해 기계학습 기술을 활용하여 평시 발생하는 소리와 이상소리를 각각 다양한 환경에서 녹음하여 빅데이터(Big data)를 구축한다. 이 빅데이터를 기반으로 학습하는 인공지능 기반 음향 경계감시 체계를 개발한다면 감시병과 상황감시센터에 신속하고 정확하게 정보를 제공할 수 있을 것이다 [26].

사이버전 방어무기체계는 사이버공간에서 운용하는 방어무기체계와 전자전 측면에서 운용하는 방어무기체계로 구분하여 개발이 필요하다.

사이버공간 방어무기체계는 감시정찰체계의 이상치 탐지정보를 전송하는 순간부터 운용되어야 한다. 이는 적이 아군의 유·무선 네트워크에 침투한 것으로 확인되었을 때 운용되는 경우 이미 다른 단말기 혹은 네트워크로 전파되었을 가능성이 커지기 때문이다. 또한 미국 해군의 CASA(Command Architecture System Assurance)처럼 무기체계의 통제장치에서 위협정보를 임시저장 후 Push 방식으로 전송하여 실시간으로 사이버 위협을 탐지·예측하는 차세대 기술의 적용도 필요하다. 이와 같이 사이버공간 방어무기체계는 이상치 탐지정보에 대응하여 이를 원상회복시킬 수 있는 무기체계로 개발되어야 한다. 이러한 운용개념은 (그림 6)에서 보듯이 이상치 탐지 정보에 따라



(그림 6) 사이버전 방어무기체계 운용 개념도

서 악성코드 치료, 다수 네트워크접속인증 실패 단말장비 접속 차단, 이상치 탐지 부대에 대한 일시 네트워크 차단 등의 기능을 수행할 수 있는 시스템 구축이 필요하다. 대대 이하 제대에서 운용하는 단말 장비 중 하나에서 이상치가 탐지될 경우 대대의 방어무기체계에서 우선 해당 단말 장비를 차단하고 여단 체계로 자동으로 보고한다. 여단 체계에서는 문제점을 확인하여 치료, 삭제 등 문제를 해결하고 관련 데이터를 업데이트하여 예하 대대 및 상급부대로 알린다. 이렇게 보고된 적의 사이버전 공격 등 이상치에 대한 데이터는 사이버전자전사령부의 체계에서 전체적인 사이버방호정책에 반영, 업데이트한 정책을 다시 각 제대별로 통보함으로써 동일한 패턴에 대응할 수 있도록 운용되어야 한다.

전자전 측면의 방어무기체계는 적의 전자공격, 무선네트워크 취약점을 통한 공격 등에 대응하기 위해서 운용 주파수 대역에서 발생하는 고출력 전자파 탐지체계, 전자파의 도착각도(AOA, Angle of Arrival) 확인체계 등을 통해서 아군에서 사용하지 않는 전자파 출력이나 아군 부대위치와 상이한 지역에서 발생하는 전자파가 도착했을 때 해당 전자파를 차단하는 체계 등의 개발을 고려해야 한다.

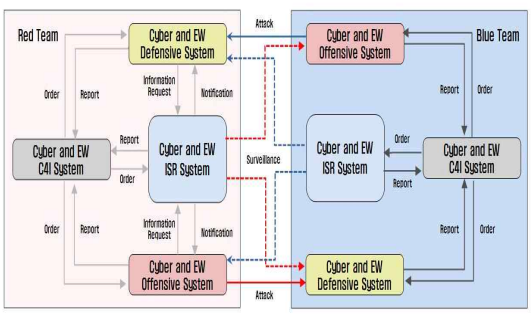
사이버전 공격무기체계는 감시정찰체계로부터 전달받은 적 유·무선 네트워크의 취약점을 통해 적의 사이버전 무기체계를 타격할 수 있도록 개발이 필요하다. 취약점은 네트워크 접속인증 방법, 보안프로그램의 취약점 등 소프트웨어 관련 취약점과 무선 주파수 운용의 취약점, 네트워크가 집중되는 특정 통신소 등 물리적인 취약점 등이 있을 수 있다. 소프트웨어 관련 취약점을 공격하기 위해서는 이 취약점을 최단시간

내에 공격할 수 있도록 자동화 공격체계를 개발하고, 물리적인 취약점을 타격할 수 있도록 드론/UAV를 활용한 고주파송출기, 초소형 EMP탄 등 전자공격 무기체계와 유·무선네트워크 인증체계 크래커(Cracker), 하드웨어 오작동 유발 SW 등 비물리적 공격무기체계를 병행하여 개발이 필요하다.

4.3 사이버전 교육훈련체계 발전 방안

사이버전 교육훈련체계는 전문인력 양성을 목표로 발전해야 한다. 사이버전 전문인력은 개인의 능력 및 성향에 따라 감시정찰, 공격, 방어 분야로 구분하여 교육훈련이 이루어져야 한다. 사이버전의 특성상 고도의 기술이 요구되는 경우가 많다. 물론 사이버공격과 사이버방어는 서로의 기술적 특성들을 알고 있어야 한다. 그 이유는 공격 기술에 보다 좋은 능력을 갖춘 경우, 방어 기술에 보다 좋은 능력을 갖춘 경우가 있기 때문이다. 개별 분야에서도 물리적 무기체계, 소프트웨어적 무기체계에 우수한 능력을 갖추는 경우가 있다. 따라서 사이버전 전문인력을 세분화하여 분류할 수 있는 사이버전문인력 식별체계의 개발이 필요하다.

이렇게 분류된 각 분야의 전문인력들이 실제 군사작전으로써 사이버전에 대한 개념이해, 실전 연습이 가능하도록 교육훈련체계를 개발해야 한다. 군사작전으로써 사이버전에 대한 개념이해는 이론적 부분으로 군사교리를 의미한다. 즉 기본교리인 「사이버전」을 기반으로 하여 「사이버전 지휘통제체계 운용」, 「사이버전 감시정찰체계 운용」, 「사이버전 공격체계 운용」, 「사이버전 방어체계 운용」 등 운용교리를 개발하여 사이버전을 군사작전 중 하나의 영역으로 자리 잡을 수 있도록 해야 한다.



(그림 7) 사이버전 교육훈련체계 운용 개념도

군사교리 개발과 병행하여 사이버전 교육훈련 장비 또는 시뮬레이터를 개발하여야 한다. 교육훈련 장비 또는 시뮬레이터는 지휘통제체계, 감시정찰체계, 공격무기체계, 방어무기체계로 구분하고, 각 분야의 전문인력이 통합된 훈련을 하도록 (그림 7)과 같이 구성한다. 훈련은 청팀과 홍팀으로 구분하여 실시하여 사이버전 전문인력이 자신의 담당분야인 지휘통제, 감시정찰, 공격 및 방어 시스템을 운용하여 훈련을 수행한다. 감시정찰체계를 담당하는 전문인력은 ISR 체계를 이용하여 상대팀의 공격 및 방어체계에 대한 감시정찰을 수행하고 그 결과를 지휘통제체계, 공격 및 방어체계로 보고 및 통보한다. 지휘통제체계를 담당하는 전문인력을 전체적인 상황을 모니터링하면서 작전을 지휘하는 훈련을 수행하고, 방어체계 운용팀은 적의 공격에 대해서 사이버 방어작전을 수행하며 공격체계 운용팀은 적의 방어체계에 대해 공격작전을 수행한다. 이때 각 체계는 실제 운용하는 전자전 장비를 비롯한 사이버전 장비를 모두 모델링하여 훈련 모의가 가능하도록 시스템 개발이 이루어져야 한다.

사이버전 관련 군사교리로부터 교육훈련체계를 통한 모의훈련까지 실시한 각 분야의 전문인력들은 사이버전자전사령부 및 각급 제대에 편성되는 사이버전 관련 부대 및 부서에서 근무하게 된다. 사이버전 관련 기술은 급격하게 변화하므로 사이버전자전 사령부 예하의 연구센터에서 개발한 감시정찰, 공격 및 방어 기술을 교육훈련체계에 반영하고 각 분야의 전문인력들이 주기적으로 보수교육을 받을 수 있는 체계를 구축한다면 사이버전 전문인력은 고도의 전문성을 유지할 수 있을 것이다.

5. 결 론

사이버전은 미래전장 중 하나의 영역으로 자리매김하고 있으며 4차 산업혁명 기술의 발달로 지상, 공중, 해상, 우주 영역에 이르기까지 첨단 IT 기술의 비중이 급증하고 있다. 따라서 사이버전에 대한 위협 또한 급증하는 추세이다. 최근에는 인공지능 기술을 이용하여 유사 악성코드의 생성이 급증하고 있어 이에 대한 대응 또한 자동화, 지능화하고자 하는 연구가 활발하게 이루어지고 있다. 또한 드론 및 자율주행차량, 자율무

기체계 등의 연구개발도 활발하게 이루어지고 있어 무선 네트워크 취약점을 이용한 사이버공격도 증가할 것이다.

이러한 기술발전 및 전장환경의 변화에 맞추어 독일은 사이버안보전략을 수정하여 사이버전과 전자전을 하나의 통합된 작전으로 보고 사이버정보군을 창설하여 지휘체계를 일원화하여 대비하고 있다. 독일뿐 아니라 미국, 러시아, 중국 등도 사이버전과 전자전에 대한 조직, 능력의 통합을 강화하고 있다. 따라서 IT 강국이라 일컬어지는 한국군의 사이버전력 또한 이에 맞추어 발전시켜야 한다. 본 논문에서는 이를 위해 사이버전자전 사령부를 비롯한 조직구조, 무기체계, 교육훈련체계의 세 분야로 구분하여 미래 한국군의 사이버전력 발전 방안을 제시하였다. 한국군 사이버전력의 발전을 위해 다양한 의견제시 및 논의를 통해서 IT 강국으로써 한국군의 사이버전 역량이 증대되어 사이버공간 및 전자기영역에서 우위에 설 수 있기를 기대한다.

참고문헌

[1] 사이버작전사령부, "북한의 대남 공작 사이버전사 현황," 국방백서, 2018.

[2] 송재익, "한국군 합동 사이버작전 강화방안 연구-합동작전과 연계를 중심으로-," 한국군사, 제2호, pp. 147-186, 2017.

[3] 손영동, "사이버전 위협과 우리의 대응방안," 군사논단, 제98호, pp. 36-57, 2019.

[4] 이용석, 권헌영, 황석중, "독일 연방 사이버군 창설 계획과 한국군 적용방향," 국방정책연구, 제33권, 제1호, pp. 203-244, 2017.

[5] 이재환, 김도영, "미래 사이버전력 획득방안에 관한 고찰," 국방과 기술, 제455호, pp. 136-147, 2017.

[6] 김성중, 유지훈 등 5명, "사이버전 수행절차 운영개념에 관한 연구," 인터넷정보학회논문지, 제21권, 제2호, pp. 73-80, 2020.

[7] 장원구, 이경호, "사이버공간에서의 효과중심작전 적용방안 연구," 인터넷정보학회논문지, 제21권, 제1호, pp. 221-230, 2020.

[8] 송의현, 김동화, 안명길, "계층적 사이버전 훈련 시나리오 저작," 인터넷정보학회논문지, 제21권, 제1호, pp. 191-199, 2020.

[9] "사이버전문인력 육성을 위한 교육 개선 및 개선방안 연구," 고려대학교 산학협력단, 2017.

[10] 김주희, "독일 사이버안보 국가전략: 안보화를 넘어 군사화로," 한독사회과학논총, 제30권, 제2호, pp. 3-32, 2020.

[11] Bundeswehr, "Kommando Cyber-und Informationsraum", https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum (검색일 : 2021.1.18.).

[12] Bundeswehr, "Kommando Informationstechnik der Bundeswehr", https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-informationstechnik-der-bundeswehr (검색일 : 2021.1.18.).

[13] Bundeswehr, "Kommando Strategische Aufklärung", https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung (검색일 : 2021.1.18.).

[14] Bundeswehr, "Zentrum für Geoinformationswesen der Bundeswehr", https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/zentrum-fuer-geoinformationswesen-der-bundeswehr (검색일 : 2021.1.18.).

[15] Bundeswehr, "Micro-Point of Presence", https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/cybersysteme-bundeswehr/micropop (검색일 : 2021.1.18.).

[16] Bundeswehr, "Via Satellit: Das Kommunikationssystem SATCOMBw", https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/cybersys-

teme-bundeswehr/satcombw (검색일 : 2021.1.18.).
[17] Bundeswehr, "Das Terrestrische Übertragungssystem", https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/cybersysteme-bundeswehr/terrestrisches-uebertragungssystem (검색일 : 2021.1.18.).
[18] Bundeswehr, "Das Bündelfunksystem TETRAPOL Bw", https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/cybersysteme-bundeswehr/tetrapol-bundeswehr (검색일 : 2021.1.18.).
[19] Bundeswehr, "Der BGAN Explorer 710", https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/cybersysteme-bundeswehr/bgan-explorer-broadband-global-area-network (검색일 : 2021.1.18.).
[20] Bundeswehr, "KWS RMB: Ein Panzer, der Radarsignale ortet", https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/land-systeme-bundeswehr/transportpanzer-fuchs-kws-rmb (검색일 : 2021.1.18.).
[21] Bundeswehr, "Der Störpanzer Hummel", https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/land-systeme-bundeswehr/stoerpanzer-hummel (검색일 : 2021.1.18.).
[22] 조성민, 서승현, "드론 보안에 적용된 암호기술 현황," 정보보호학회지, 제30권, 제2호, pp. 11-19, 2020.
[23] 최승철, 조준형, 권오진, "사이버전 연계 전자전 전투피해평가 지표 산출을 위한 연구," 인터넷정보학회논문지, 제21권, 제1호, pp. 201-210, 2020.
[24] 류창수, 김명환, 정영진, "드론봇 전투부대 편성 및 운용개념에 관한 연구," 국방과 기술, 제480호, pp. 70-81, 2019.
[25] 전서인, "4차 산업혁명시대 육군의 사이버작전 수행체계 발전 방안," 군사혁신저널, 제2호, pp. 1-32, 2019.
[26] "국방 인공지능(AI) 실증 기획 연구," 광주과학기술원, 2018.

〔저자소개〕

박 상 준 (Sangjun Park)
2000년 2월 육군사관학교 학사
2010년 2월
한국과학기술원 정보통신공학 석사
2020년 3월 ~ 현재 아주대학교 국방디지털융합학과 박사과정
2019년 11월 ~ 현재
육군사관학교 전자공학과 조교수
email : sigpsj13438@naver.com

김 태 산 (Taesan Kim)
1998년 2월 육군사관학교 학사
2006년 2월 서울대 서양사학 석사
2014년 1월 독일 포츠담대 사학 박사
2018년 ~ 현재 육군사관학교 군사사학과 부교수
email : kimtaesan@mnd.go.kr

김 지 원 (Jee-won Kim)
2002년 2월 동국대학교 학사
2016년 8월 연세대학교 정보보호 석사
2021년 2월 아주대학교 공학박사
2019년 10월 ~ 현재 국방보안연구소 선임연구원
email : jeewonkim@ajou.ac.kr

정 찬 기 (Chan-gi Jung)
1986년 공군사관학교 전자공학 학사
1994년 플로리다공대 전산공학 석사
2001년 플로리다공대 전산공학 박사
2016년 9월 ~ 현재
아주대학교 국방디지털융합학과 교수
email : ckjeong@ajou.ac.kr