https://doi.org/10.33778/kcsa.2019.19.4.013

사이버작전에 대한 공통상황인식 함양을 위한 軍 사이버작전 교육체계 연구 및 방향성 제안★ -非사이버작전부대 장교 교육을 중심으로-

이 상 운*, 박 용 석**

요 약

본 연구는 사이버작전을 전문적으로 수행하지 않는 非사이버작전부대 장교들을 위한 교육체계를 개발하고 방향성을 제안하기 위한 연구이다. 사이버작전을 합동작전으로 수행하기 위해서는 非사이버작전부대 장교들도 사이버작전을 알아야하나 이들을 위한 교육체계는 현재 軍에는 없으며, 이에 대한 선행연구 또한 거의 없어 해당 분야의 연구가 필요하다. 따라서, 非사이버작전부대 장교 교육체계는 사전에 실시한 관련 문헌연구를 기반으로, 교육체계를 구성할 수 있는 5가지 항목 즉, 교육의 필요성, 교육대상, 교육목표 및 내용, 교육과정에 관한 사항을 개발하였다. 또한, 관련 전문가들에게 델파이방법으로 각 항목의 타당성을 확인하였다. 그 결과, 일부 향상의 필요성도 보였으나, 전체적으로 적합함을 보였다. 향후에는 이 연구를 바탕으로 세부 교육프로그램 개발이 개발될 수 있다.

Research and Direction of Cyber Operation Education System for Fostering Common Situation Awareness about Cyber Operation -Focusing on non-Cyber Operations Unit Officer Education-

Sangwoon Lee*, Yongsuk Park**

ABSTRACT

The purpose of this study is to suggest the educational system and direction of cyber operations officers of non-cyber operations forces who do not specialize in cyber operations. In order to carry out cyber operations as a joint operation, non-Cyber Operations officers must also know about cyber operations, but there is no education system for them at present, Since there is almost no previous research on this, research in the relevant field is necessary. Therefore, the education system was developed based on the prior literature review, that is, the education system, that is, the necessity of education, the object of education, the goals and contents of the education, and the curriculum. In addition, the relevant experts confirmed the validity of each item with Delphi method, and as a result, some improvement was needed, but it was shown to be suitable as a whole. In addition, detailed educational program development can be developed based on this in the future.

Key words: Cyber Operations, Common Situation Awareness, Cyber Operations Education System, Officer of non-Cyber Operations Force, Joint Operations, Joint Combat Development

접수일(2019년 8월 22일), 수정일(1차: 2019년 9월 21일), 게재확정일(2019년 10월 25일)

★ 본 논문은 해당 논문 저자 이상운의 석사학위 논문을 기반으로 하였음.

* 세종사이버대학교 정보보호대학원 석사과정

** 세종사이버대학교 정보보호대학원 주임교수(교신저자)

1. 서 론

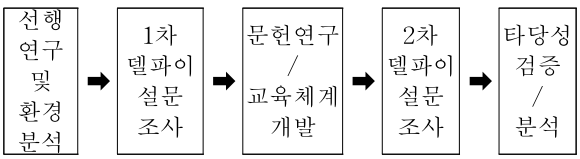
사이버전, 사이버보안, 사이버작전 교육의 중요성과 필요성은 지속 제기되어 왔다. 대한민국의 사이버전 역량은 미국・중국・러시아・북한에 비해 상대적으로 열세하여 교육 및 훈련체계는 강화해야 할 역량의 하나이며[1], 각 기관은 기관 특성에 맞는 맞춤형 사이버보안 교육훈련체계를 구축해야 한다[2]. 또한 軍의 미래 사이버작전 개념발전을 위해서는 모든 전투병과[1] 장교들에게 사이버작전을 교육해야 하고, 이를 위한 장교 양성 및 보수교육 교과체계 개편이 필요하다[3].

軍은 2011년에 국군사이버사령부를 창설하면서 사이버공간에서 사이버전을 준비해 왔다. 최근에는 부대 명칭을 사이버작전사령부로 변경하여 합동부대[2]로 지정하면서 사이버작전을 합동작전의 범주에 포함시켰다[4]. 軍이 사이버작전을 합동작전으로 수행하기 위해서는, 물리작전과 통합된 합동작전계획이 수립되고, 합동전투발전분야[3]에서 실질적인 발전이 있어야 하며, 합동작전의 주체인 지휘관이 사이버작전 개념을 제시할 수 있어야 한다[5]. 특히 임무 달성이 가능한 합동작전계획을 수립하기 위해서는 상・하제대가 작전환경, 위협의 본질, 업무절차 등에 대하여 명확한 공통상황인식을 형성하여 제대간 노력의 통일을 달성해야 한다[6]. 따라서 합동작전으로써 사이버작전을 지휘하는 지휘관, 작전계획을 수립하는 계획가, 전투발전업무를 추진하는 실무자들은 사이버작전을 이해하고 이에 대한 공통상황인식을 가져야 한다. 그러나 이들 대부분은 사이버작전을 직접 수행해 보지 않았고, 사이버작전 교육을 받지 않은 非사이버작전부대 장교들로, 물리작전 분야에는 전문가이나 사이버작전 분야에는 어려움을 겪고 있다. 따라서, 본 연구의 목적은 '非사이버작전부대 장교들이 사이버작전을 이해하고 공통상황인식을 함양할 수 있는 교육은 어떠해야 하는가?'라는 (사이버작전을 전문적으로 수행하지 않는)非사이버작전부대 장교 사이버작전 교육체계를 개발하는 것이다. 이를 위해 연구문제를 다음과 같이 5가지로 설정하였다.

첫째, 非사이버작전부대 장교들에게 사이버작전 교육이 필요한가?(교육의 필요성)
둘째, 非사이버작전부대 장교들 중 어떤 계층을 대상으로 교육해야 하는가?(교육대상)
셋째, 교육대상에게 맞는 교육목표 및 중점은 어떠해야 하는가?(교육목표 및 중점)
넷째, 非사이버작전부대 장교들을 위한 사이버작전 교육은 어떤 내용이어야 하는가?(교육내용)
다섯째, 非사이버작전부대 장교들을 위해 적합한 교육과정은 무엇인가?(교육과정)

연구방법은 문헌연구와 델파이방법으로 5가지 연구문제에 대한 답을 각각 구함으로써 교육체계를 개발하였다. 문헌연구는 非사이버작전부대 장교 교육체계(특히 교육내용)에 대한 선행연구가 없어 기초자료 수집을 위해 실시하였다. 델파이방법은 미래에 대한 예측뿐 아니라 현재 상태에 대한 일반화 혹은 표준화된 자료가 부족한 경우 많이 사용 되고[7], 문헌연구 결과의 신뢰성을 보완하면서, 사이버작전에 대한 개념과 인식이 개인별 편차가 심하여 다수의 전문가들로부터 다양한 의견 수렴과 합의과정을 거칠 필요가 있어 적용하였다. 델파이 설문조사는 본 연구의 주제와 비교적 유사한 연구[8]를 참조하여 총 2회를 실시하였다. 델파이 설문조사를 위한 전문가는 사이버전 관련 분야에서 20년 이상 경력이 있는 석・박사급의 軍 및 민간 교수, 연구원, 현직 군 정책부서와 사이버작전부대 부서장 등 총 11명을 선정하였다.

전체적인 연구의 방법 및 절차는 (그림 1)과 같다.



(그림 1) 연구의 방법 및 절차

먼저 선행연구 및 환경을 분석하고 1차 델파이 설문조사를 실시하여 연구문제에 대한 기초자료를 수집하였다. 이후 문헌연구를 통해 교육내용을 추가로 연구함으로써 교육체계를 개발하였다. 개발한 교육체계는 2차 델파이 설문조사를 통해 그 타당성을 검증하였다.

1) 보병, 포병, 기갑, 공병, 통신, 항공, 방공, 정보

2) 국군조직법에 의거하여 합동참모의장이 합동작전을 위하여 지휘・감독하는 부대이며(대통령령 제25377호), 합동작전은 육·해·공군 중 2개 이상의 군이 공동의 작전 목적을 달성하기 위하여 상호 합동으로 실시하는 작전(군사용어사전)

3) 미래 전장에서 합동작전 수행에 요구되는 능력을 갖추기 위하여 발전시켜야 할 분야로 교리(Doctrine), 구조 및 편성(Organization), 교육훈련(Training), 무기・장비・물자(Material), 인적자원(Personnel), 시설(Facilities)로 구분함(합동・연합작전 군사용어사전, 2014)

2. 선행연구 및 환경 분석

2.1 軍 사이버작전에 대한 선행연구 분석

2015년 이전까지 국내에서의 軍 사이버작전에 관한 연구는 정보보호 역량 강화, 사이버전에 대한 인식의 변화, 사이버위협 대응전략 또는 대응방안, 사이버작전 발전방향 제시 등 대체적으로 포괄적이고 개념적인 내용을 다루는 연구들이 대부분이었다[9 ~ 12]. 2015년 이후에 들어서는 합동작전, 정보, 심리학 등의 관점으로 연구 범위가 확대되고 있는 추세이다. 합동작전의 관점에서는 사이버작전이 국방 및 합동기획체계에서 다루어지고, 다른 군사작전과 연계되어 지휘관이 사이버작전을 주도해야 한다[5]고 보았고, 정보의 관점에서는 기존에 물리전 작전환경 분석의 틀로 활용되고 있던 전장정보분석 개념을 사이버공간에서의 적용을 시도하였다[13]. 또한 사이버공간이 인간의 인식영역에 영향을 주기 때문에 사이버작전을 심리학의 관점에서도 바라보았다[14]. 2015년 이후의 연구들은 기존에 포괄적이고 개념적인 단계를 넘어 새로운 관점에서 특정 분야를 보다 심층적으로 연구할 수 있는 계기를 마련하였으나, 아직까지는 기초적인 수준으로 실제 軍 사이버작전에 활용할 수 있는 수준에는 이르지 못하고 있다.

교육의 관점에서도 연구들은 진행되어 왔다. 대체적으로 사이버전을 직접 수행하거나 국방정보시스템을 보호하는 전문 인력을 위한 교육과정과 교육소요를 도출하는 연구가 다수였고[15][16], 일반 인원들을 위한 교육 연구는 많지 않음을 확인하였다. 그 중 사관생도 교육을 위해 육군사관학교의 사이버전 교육현황을 분석하여 위관 및 영관장교 보수교육과 연계된 교육의 필요성을 언급하였고[17], 사이버전을 위한 12개의 지식영역을 도출하여 각 영역별 교육과목 명칭과 교육내용을 제시하여 육·해·공군 사관학교 특성을 고려한 정보보호 수준의 교육커리큘럼을 제안[18]하기도 하였다. 하지만, 이들 연구들을 살펴보면 사이버작전을 직접 수행하는 전문 인력을 위한 교육에 치중되어 있고, 非사이버작전부대 장교를 위한 교육에 관한 연구는 아직까지 거의 발견되지 않았다. 또한 기존에 연구된 교육소요와 교육과정도 정보보호 차원의 기술적 분야에 맞추어져 있으며, '누구에게, 무엇을, 어떻게 교육할 것인가?'에 대한 구체화는 부족하다보니 군사목표 달성을 위해 군사적 수단을 사용하는 군사작전 개념[19]의 사이버작전 교육과는 다소 거리감이 있었다.

2.2 軍의 사이버작전 합동전투발전 환경 분석

사이버작전을 합동작전으로 수행하기 위해 필요한 능력을 갖추기 위해서는 합동전투발전체계[4]의 틀에서 분야별 전투발전업무가 균형 있게 추진되어야 한다. 합동전투발전업무는 非사이버작전부대 장교들이 주축을 이루기 때문에 사이버작전 전투발전 환경의 현재 상태를 알고 이들에게 적합한 교육체계를 개발하기 위해서는 합동전투발전체계를 분석할 필요가 있다. 『합동전투발전업무훈령』[20]을 기반으로 합동전투발전체계를 재구성 및 도식화하였다. (그림 2)와 같이 ①합동개념발전, ②능력평가, ③능력요구, ④합동소요결정의 4단계로 업무가 이루어진다.

(그림 2) 『합동전투발전업무훈령』[20]기반 합동전투발전체계도

① 합동개념발전 단계에서는 합동참모본부(이하 합참)가 미래 싸우는 방법에 대한 개념과 이를 위한 요구능력을 도출하여 『미래 합동작전기본개념서』와 『합동작전요구능력서』를 작성하여 다음 단계인 능력평가의 근거를 제공한다. ②능력평가 단계에서는 합참에서 현재와 미래의 능력을 평가하여 부족능력을 식별하고 합

4) 합동성 차원에서 미래전을 준비하는 총체적인 노력으로서, 현존 전력을 극대화하고 미래전투발전 소요를 창출하는 과정. 합동전투발전체계는 '합동작전부대가 어떻게 작전할 것인가?'와 '합동작전부대의 요구되는 능력이 무엇인가?'를 제시하고, 이를 위해 전투발전분야별로 필요한 소요를 창출하는 과정(합동전투발전업무훈령)

동부대에 전투발전『소요제기지침서』를 하달한다. ③ 능력요구 단계에서는 합동부대에서 작전요구능력을 도출하여『소요제기서』를 작성한 후 합참에 제출한다. ④ 합동소요결정 단계에서는 합참에서 합동부대로부터 제기된 소요를 검토하여 결정한 후『합동군사전략목표기획서』와『합동무기체계기획서』에 반영한다. 여기에 반영된 소요들은 방위력개선사업과 전력운용사업으로 추진된다.

합동전투발전업무는 보수교육을 이수한 영관장교들이 국방부 및 합참의 관련 부서에 보직되어 수행한다. 이들은 합동전투발전업무의 ①합동개념발전, ②능력평가, ④합동소요결정 업무를 주도함으로써 '합동작전부대가 어떻게 싸울 것인가?'와 '합동작전부대의 요구되는 능력은 무엇인가?'를 구체화한다. 하지만 이들은 대부분 非사이버작전부대 영관장교들로 사이버작전을 수행해보지 않았고, 관련 교육을 받지 않은 상태에서 사이버작전을 합동작전의 개념과 실질적인 전력으로 발전시키기에는 매우 어려운 환경임을 알 수 있다.

실제로 사이버작전의 합동전투발전분야 수준을 사이버작전 전문가 12명에게 설문조사(매우 양호:5점, 양호:4점, 보통:3점, 미흡:2점, 매우 미흡:1점)한 결과, 전반적으로 '미흡'한 수준으로 평가되었다(교리 2.4점, 구조 및 편성 2.8점, 교육훈련 2.2점, 무기·장비·물자 1.9점, 인적자원 1.9점, 시설 3.2점). 또한, ①합동개념발전, ②능력평가, ④합동소요결정 업무를 추진하는 국방부 및 합참 실무자 10명과, ③능력요구 업무를 추진하는 사이버작전부대 실무자 10명에게 인터뷰를 통해 문의한 결과, 국방부 및 합참 실무자들은 사이버작전이 생소하고 어려워 업무 추진에 제한사항이 많다는 의견이 대부분 이었고, 사이버작전부대 실무자들은 국방부 및 합참 실무자들에게 작전소요를 제기하기 위하여 사이버작전을 이해시키는 과정이 매우 어렵다는 의견이 많았다. 따라서 사이버작전이 합동작전으로 발전하기 위해서는 합동전투발전업무의 주축인 非사이버작전부대 장교들은 적어도 사이버작전 개념과 사이버부대의 능력을 이해할 수 있어야 함을 알 수 있다.

2.3 軍의 非사이버작전부대 장교 교육환경 분석

사이버작전이란 사이버공간에서 군사목적 달성을 위해 사이버관련 능력을 운용하는 작전으로, 합동작전계획 수립 시 사이버작전을 전역[5] 또는 주요 작전의 일부로 계획해야 하고, 교육훈련은 일반 장교를 위한 보수교육과 사이버전문인력을 위한 전문교육으로 구분하여 실시한다[21].

현재 軍에서 시행되고 있는 장교 보수교육으로, 위관장교들은 초등군사반과 고등군사반 교육과정에서 해당 병과의 직무수행에 필요한 교육을 이수 후 중대급 이하 지휘관과 사단급 이하 제대의 참모업무를 수행한다. 영관장교들은 합동군사대학교에서 제병협동작전, 합동 및 연합작전, 국방·합동기획을 위한 교육을 이수 후 대대급 이상 전술제대의 지휘관 및 참모, 정책·기획·계획부서의 참모 업무를 수행 한다[22].

사이버작전 교육은 사이버작전을 직접 수행하는 사이버전문 인력에게는 사이버작전사령부와 각 군 정보통신학교에서 자체 교육프로그램을 구성하여 전문교육을 실시하고 있고, 일반 장교들에게는 보수교육과정에서 일반교육을 실시하고 있다. 일반교육의 경우 장성급 고위 정책관리자들을 대상으로는 국방대학교 안전보장대학원에서, 영관급 장교들은 합동군사대학교의 합동기본정규과정에서 인식제고 차원의 2~3시간 정도의 교육이 진행되고 있다. 양성교육과정에서는 육군사관학교 컴퓨터과학과에서 1·2학년 생도들에게 사이버전 기초기술 이해를 위한『컴퓨터과학 개론 및 실습』을 3~4시간 교육하고 있다[17]. 따라서 非사이버작전부대 장교들이 이러한 교육 환경에서는 사이버작전을 충분하게 이해하기가 매우 어렵다는 것을 알 수 있다.

2.4 선행연구 및 환경 분석결과 시사점

軍 사이버작전에 대한 현재의 상황을 軍 사이버작전에 대한 선행연구, 합동전투발전 환경, 軍의 非사이버작전부대 장교 교육 환경을 분석하여 확인하였다. 합동사이버작전 교범에서는 일반 장교들에게 보수교육 과정에서 사이버작전을 교육하도록 명시하고는 있지만, 현재 시행되고 있는 2 ~ 3시간 정도의 인식 제고 수준 교육만으로는 사이버작전이 육상·해상·공중 공간과 함께 사이버공간이라는 영역에서 이루어지는 또 다른

5) 전역(戰役, Campaign) : 전략적 또는 작전적 목표를 달성하기 위해 부여된 시간과 공간 내에서 수행하는 일련의 연관된 주요 작전(군사용어, 육군본부, 2017)

군사작전 형태[21]임을 고려 시 교육적 효과를 통한 합동작전의 실효성을 기대하기는 어렵다. 합동전투발전 역시 그 업무의 중추적인 역할을 담당하는 영관장교들이 현재의 교육환경에서는 내실 있는 사이버작전의 발전을 기대하기는 어려워 보인다. 사이버작전 교육에 관한 선행연구 또한 많지 않은 실정이다 보니 누구를 대상으로, 누가, 언제, 무엇을, 어떻게 교육할 것인가에 대한 깊이 있는 연구가 진행되지 않아 보인다. 따라서 사이버작전을 합동작전으로 수행하면서 군사목적 달성에 기여하고, 실질적인 발전을 도모하기 위해서는 非사이버작전부대 장교들을 위한 사이버작전 교육체계가 개발되어 적용되어야 함을 알 수 있다.

3. 사이버작전 교육체계 개발결과

3.1 교육의 필요성

교육의 필요성은 첫 번째 연구문제인 '非사이버작전부대 장교들에게 사이버작전 교육이 필요한가?' 질문으로 1차 델파이 설문조사를 실시하였다. 전문가 11명 중 7명은 '매우 필요'하다고 응답하였고 4명은 '필요'하다고 응답하여 非사이버작전부대 장교들에 대한 교육은 필요한 것으로 나타났다. 교육이 필요한 이유로는, 軍이 첨단 과학기술군[6]으로의 변화를 위해서는 사이버전장환경에 대한 기본적 소양 함양이 필수이며, 앞으로의 합동작전은 사이버작전과 연계되어야하기 때문인 것으로 분석되었다.

3.2 교육대상

교육대상은 두 번째 연구문제인 '非사이버작전부대 장교들 중 어떤 계층을 대상으로 교육해야 하는가?' 질문으로 1차 델파이 설문조사를 실시하였다. 이를 기초로, 현재 교육환경의 현실적 여건과 사이버작전 발전의 시급성을 고려하여 교육대상을 '전투병과 영관장교'로 설정하였다. 현재 교육환경의 현실적 여건으로, 전투병과 위관장교들의 교육은 각 병과학교에서 분산되어 시행되고 있는 반면, 영관장교 교육은 합동군사대학교에서 일원화하여 시행하기 때문이다. 사이버작전 발전의 시급성으로, 영관장교는 합동전투발전 업무의 중추적인 역할을 수행함과 동시에 곧 대대급 이상 제대의 지휘관 임무를 수행함에 따라 단기간에 사이버작전의 발전을 견인하고 리더십 발휘가 가능하기 때문이다. 또한 전투병과 위관장교는 전략·작전적 수준의 군사교육을 받은 수준이 아닌 점을 고려하여 차후 단계적으로 교육을 확대하는 것이 바람직하기 때문이다.

3.3 교육목표 및 중점

교육목표 및 중점은 세 번째 연구문제인 '교육대상에게 맞는 교육목표 및 중점은 어떠해야 하는가?' 질문으로 실시한 1차 델파이 설문조사에서 수집된 자료를 기초로, 현재 전투병과 영관장교들은 사이버작전에 대한 교육 경험이 없어 지식과 인식 수준이 낮은 것을 고려하여 다음과 같이 설정하였다.

- 교육목표 :
  전투병과 장교들에게 사이버작전이 미래 전장에서 합동작전의 필수 요소임을 인식시키면서 사이버작전에 대한 개념을 이해
- 교육중점
  ① 사이버공간을 이해하기 위한 기술 분야의 지식 습득
  ② 사이버공간에 대한 이해와 중요성 인식
  ③ 사이버작전에 대한 이해

3.4 교육내용

교육내용은 네 번째 연구문제인 '非사이버작전부대 장교들을 위한 사이버작전 교육은 어떤 내용이어야 하는가?' 질문으로 실시한 1차 델파이 설문조사와 문헌연구 결과를 바탕으로, 교육중점인 ① 사이버공간을 이해하기 위한 기술 분야의 지식 습득, ② 사이버공간에 대한 이해와 중요성 인식, ③ 사이버작전에 대한 이해로 구분하여 설정하였다.

먼저, ① 사이버공간을 이해하기 위한 기술 분야의 지식은 교육대상이 사이버작전을 전문적으로 수행하지 않는 非사이버작전부대 장교임을 감안하여, ⓐ정보통신기술과 정보보호에 관한 기본개념 이해와 ⓑ사이버공간에서의 활동을 기술적 시각에서 이해, 두 가지로 설정하였다. ⓐ정보통신기술과 정보보호에 관한 기본개념

6) 국방개혁2.0에서는 국방개혁 목표를 '평화와 번영을 힘으로 뒷받침하는 강한 군대 조기 구현' 으로 설정하였고, 이를 위해 군 구조 분야는 병력 집약적 구조에서 '전방위 안보위협 대응이 가능한 첨단과학기술 기반의 군 구조로 발전' 할 것임을 명시.

을 이해하기 위한 교육내용은, 사이버전 수행을 위해 12가지의 지식영역을 구분하여 이에 맞는 교육과목을 제시했던[18] 내용을 참조하여 정보보호론, 소프트웨어 공학, 암호학, 정보보호제도 및 정책, 시스템보안, 네트워크보안, 소프트웨어응용보안, 시큐어코딩, 디지털포렌식의 9가지로 설정하였다. ⓑ사이버공간에서의 활동을 기술적 시각에서 이해하기 위한 교육내용은 <표 1>과 같이 설정하였다.

<표 1> 사이버공간 활동을 기술적 시각에서 이해[23]

구 분	내 용
사이버공간의 사이버공격	• 사이버공격 행위자 * 핵티비즘, 사이버범죄・테러 개념, • 공격자가 활용하는 기술(용어 이해) • 공격주체 식별의 어려움 • 특정 목적을 위해 수행되는 APT공격
사이버공간의 사이버방어	• 사이버방어의 기본개념 * 서명, 방화벽, IPS/IDS, 백신 등 • 방어자가 활용하는 기술(용어 이해) • 완전방어의 어려움 • 회복력의 개념과 중요성 • 정보공유와 협력의 중요성

다음으로, ② 사이버공간에 대한 이해와 중요성을 인식시키기 위해, ⓐ사이버관련 정책 및 전략과 ⓑ군사적 시각에서 보는 사이버공간의 이해, 두 가지로 <표 2, 3>과 같이 설정하였다.

<표 2> 사이버관련 정책 및 전략

구 분	내 용
주요국의 사이버안보 전략	• 사이버공간에 대한 주요국 인식과 태도 • 위협에 대한 인식, 국가적 대응을 위한 개념, 기관들의 역할 및 책임
사이버전쟁 이해	• 국가별 사이버전쟁을 정의하는 시각 • 스턱스넷 등의 사례를 통해 보는 사이버무기의 개념 • 사이버무기의 확산 위험성과 새로운 군비경쟁의 가능성
사이버공간 정책/전략 이해	• 국가안보전략, 국가사이버안보전략, 국방전략, 국방사이버전략(훈령) 등
사이버작전 수행을 위한 전략적 환경	• 국가정책과 정치, 외교 환경을 고려 시 수행 가능한 사이버작전 수준과 범위 • 정책, 전략, 전략지시 분석결과 사이버공간을 통한 군사작전 시 고려사항
사이버조직	• 국내 사이버조직 (역할 및 책임, 기관별 정책 및 전략) • 국방 사이버조직 및 부대 (역할・책임, 지휘 및 지원관계)
기타	• 합동 사이버작전 기획체계 • 방어적 사이버작전 분야와 공세적 사이버작전 분야에서 군의 능력

<표 3> 군사적 시각에서 보는 사이버공간의 이해

구 분	내 용
사이버작전 특성	• 리버스엔지니어링 가능, 단일국가/국제 소유권 없음, 협력 어려움, 저비용, 휘발성, 의도치 않은 효과
사이버공간 분류	• 계층에 의한 분류(물리/논리/페르소나) • 소유권에 의한 분류(청색, 회색, 적색)
사이버공간 위협	• 위협을 발생시키는 주체 * 국가, 비국가, 단체, 개인으로 구분하여 각 주체의 위협 특성을 이해 • 북한의 사이버위협
사이버공간 군사작전 시 도전요소	• 사이버공간의 익명성, 책임귀속의 어려움 • 지리적 도전(군 또는 국가 소유가 아닌 공간에서 작전의 어려움) • 기술적 도전(취약점에 대한 이해)
軍 사이버공간 이해	• 국방사이버공간의 구성 • 군의 사이버공간 의존성 • 군 정보보호체계의 이해

마지막으로, ③ 사이버작전을 이해하기 위해서는 ⓐ 사이버작전의 개념과 ⓑ사이버작전의 계획 수립 및 시행, 두 가지로 <표 4, 5>와 같이 설정하였다.

<표 4> 사이버작전의 개념

구 분	내 용
사이버전 사례 / 교훈	• 이라크전, 시리아전 등 군사작전 시 사이버작전이 물리전과 통합된 사례
사이버공간 내・외부의 사이버작전	• 사이버공간 내부에서 시행되는 작전 • 사이버공간을 통한 정보작전 • 사이버공간 내부를 통해 물리공간에 영향을 주는 작전
수준별 사이버작전	• 전략・작전・전술적 수준의 사이버작전
합동기능과 관계	• 지휘통제, 정보, 기동, 방호 등 합동기능과 사이버작전과의 관계
사이버공간에서 활동	• 사이버보안, 사이버방어, 사이버공격(거부, Manipulate) 구분
사이버공간 임무	• 특정 목적을 위해 시행되는 방어적, 공세적 사이버작전
사이버작전 효율성과 적법성 보장	• 효율성 보장을 위한 정부부처 협력 • 적법성 보장을 위한 국내법과 상충되는 작전 제한사항과 우방국과의 협조요소

<표 5> 사이버작전의 계획 수립 및 시행

구 분	내 용
사이버작전 계획수립	• 합동작전 계획수립절차에 의한 사이버작전 계획수립
사이버작전 계획수립 고려사항	• 의도하지 않은 효과 방지대책 • 사이버공간의 물리계층, 논리계층, 사이버 페르소나 계층에서의 시스템 사용자와 적대적 요소와의 관계 규명 • 위협 주체의 다양성 (개인, 단체, 비국가, 국가) • 통제하기를 요망하는 사이버공간과 위협주체의 지정학적 위치와의 불일치성 • 적대세력이 활용하는 사이버공간은 국내외 민간 법인 소유일 가능성 • 작전유형별(공세, 방어 등) 적용이 될 수 있는 법적 고려사항
민간 소유 사이버공간 작전 시 고려사항	• 정확한 표적을 정의, 표적 접근 방법 개발 • 작전을 위해 상부기관으로 건의사항 도출 • 정부 부처 조정사항 도출 • 작전의 정당성, 합법성 보장 위한 조치
사이버공간 표적화	• 표적화 절차 • 사이버공간 표적화 시 고려사항 • 사이버공간 표적화 제한사항 및 해결책
기 타	• 평시 사이버작전 시행절차 (침해대응, 정보작전방호태세) • 유사시 사이버작전 시행절차 (군사작전 목표달성 중심)

3.5 교육과정

교육과정은 다섯 번째 연구문제인 '非사이버작전부대 장교들을 위해 적합한 교육과정은 무엇인가?' 질문으로 실시한 1차 델파이 설문조사 결과를 기초로, 현행 영관장교 보수교육 과정에 사이버작전 교육을 포함하는 것으로 설정하였다. 모든 소령급 전투병과 장교들을 교육하기 위해서는 합동기본과정을 활용하고, 중·대령급 전투병과 장교들을 교육하기 위해서는 합동고급과정을 활용하되, 非기술분야 위주로 교육하고 기술 분야는 사이버작전부대에서 전담하여 전문성에 바탕을 둔 교육 실시로 설정하였다.

4. 교육체계 타당성 검증

4.1 타당성 검증방법

非사이버작전부대 장교들을 위한 사이버작전 교육체계를 5가지 연구문제인 교육의 필요성, 교육대상, 교육목표 및 중점, 교육내용, 교육과정에 대하여 개발하였다. 개발한 결과는 1차 델파이 설문조사에서 검증된 교육의 필요성을 제외하고 5점 Likert 평가 척도(5=매우 적절, 4점=적절, 3점=보통, 2점=부적절, 1점=매우 부적절)의 폐쇄형 질문으로 구성하여 2차 델파이 설문조사를 추가로 진행하였다.

설문조사 결과는 SPSS 통계프로그램(IBM SPSS statistics version 22)으로 평균, 중앙값, 표준편차, 분산, 1사분위수, 3사분위수 값을 구하였다. 이를 기초로 연구자가 제시한 교육체계가 적절한지를 검증하기 위해 수렴도, 합의도, 내용 타당도 비율, 변이계수를 산출하였다. 수렴도와 합의도는 전문가의 의견 수렴 및 합의 정도를 분석함으로써 연구자의 설문조사가 타당한지를 확인하기 위해 산출하는데, 수렴도는 0, 합의도는 1에 가까울수록 타당함을 의미한다[24].

수렴도=$\frac{(Q_3 - Q_1)}{2}$, 합의도=1-$\frac{Q_3 - Q_1}{Mdn}$

(Mdn=중앙값, Q1·Q3= 1·3사분위수)

내용 타당도 비율(CVR, Content Validity Ratio)은 연구자가 질문한 문항이 타당한지를 판단하기 위해 Lawshe(1976)가 제시한 값을 기준으로, 응답자 수에 따른 CVR 최소값 이상일 때 타당도가 있으며, 10명의 응답자일 경우 CVR 최소값은 0.62를 나타낸다.

CVR=$\frac{N_e - N/2}{N/2}$

(Ne=중요하다고 응답한 사례수, N=응답자수)

변이계수(CV, Coefficient of Variation)는 반복되는 설문과정에서 패널들의 설문응답의 편차가 적어 응답의 일치성을 보여 안정도가 확보되었는지를 알기위해 산출한다. 변이계수가 0.5 이하인 경우 추가적인 설문이 필요 없으며, 0.5~0.8인 경우 비교적 안정적이며, 0.8 이상인 경우 추가적인 설문조사가 필요하다[25].

변이계수=$\frac{\text{표준편차}}{\text{산술평균}}$

연구자가 개발한 내용이 적절한지에 대한 것은 수렴도가 0.5 이하, 합의도 0.75이상, 내용 타당도 비율(CVR) 0.62 이상, 변이계수(CV) 0.5 이하에 해당하는지를 기준으로 평가하였다.

4.2 타당성 검증결과

개발한 교육체계의 2차 델파이 설문조사 결과와 이에 대한 통계분석결과는 <표 6>과 같다.

<표 6> 2차 델파이 설문조사 결과 및 통계분석결과

구분		설문조사 결과					통계 분석결과
		매우 적절 (5점)	적절 (4점)	보통 (3점)	부적절 (2점)	매우 부적절 (1점)	
교육대상		3명	4명	1명	-	2명	수렴도 1.25 합의도 0.37 CVR 0.4 CV 0.42
교육목표 및 중점		2명	7명	1명	-	-	수렴도 0.125 합의도 0.938 CVR 0.8 CV 0.138
교육 내용	①	3명	5명	2명	-	-	수렴도 0.625 합의도 0.685 CVR 0.6 CV 0.179
	②	5명	4명	1명	-	-	수렴도 0.5 합의도 0.778 CVR 0.8 CV 0.158
	③	4명	5명	1명	-	-	수렴도 0.5 합의도 0.75 CVR 0.8 CV 0.157
교육과정		5명	4명	-	1명	-	수렴도 0.5 합의도 0.778 CVR 0.8 CV 0.221

교육대상은 연구자가 제시한 결과에 대하여 매우 적절하다는 의견으로부터 매우 부적절하다는 의견까지 다양하게 제시되어, 통계분석결과는 수렴도・합의도・내용타당도(CVR) 모두 기준에 부합하지 못하였다. 매우 부적절한 이유로는, 사이버작전을 군사작전의 하나로 생각한다면 교육대상을 전투병과 장교들로 한정하는 것보다는 모든 장교・부사관・병들을 대상으로 하는 것이 타당한 것으로 분석되었다. 교육목표 및 중점은 통계분석결과 수렴도・합의도・내용타당도(CVR) 모두 기준에 부합하여 연구자가 제시한 결과가 적절하였다. 교육내용으로 ① 사이버공간을 이해하기 위한 기술 분야의 지식 습득을 위해 개발한 내용은 통계분석결과 수렴도・합의도・내용타당도(CVR) 모두 기준에 부합하지 못하여 교육내용의 보완이 요구되었다. 그 이유로는, 사이버공간을 이해하기 위한 정보기술 분야의 교육내용으로는 대체적으로 잘 선정되었으나, 교육대상이 전투병과 영관장교임을 고려 시 교육수준의 조절이 필요하고, 기술적 이해가 반드시 필요한 것인지는 재고할 필요가 있다고 분석되었다. 다음으로 ② 사이버공간에 대한 이해와 중요성 인식, ③ 사이버작전에 대한 이해를 위해 개발한 교육내용은 통계분석결과 수렴도・합의도・내용타당도(CVR) 모두 기준에 부합하여 연구자가 개발한 결과가 적절하였다. 교육과정은 통계분석결과 수렴도・합의도・내용타당도(CVR) 모두 기준에 부합하여 연구자가 제시한 결과가 적절하였다.

추가적인 설문 여부를 확인하기 위하여 도출한 변이계수(CV)는 모든 요소들이 0.5 이하를 보여 3차 델파이 설문조사는 불필요하였다.

5. 결론 및 방향성 제안

非사이버작전부대 장교들을 위한 교육체계를 이를 구성할 수 있는 5가지 항목 즉, 교육의 필요성, 교육대상, 교육목표 및 중점, 교육내용, 교육과정에 대하여 연구하였다. 연구결과, 합동작전으로 사이버작전을 발전시키기 위해서는 非사이버작전부대 장교들에게 사이버작전 교육이 필요하다. 교육대상은 전투병과 영관장교로 한정하기 보다는 위관장교까지 포함할 것이 요구되었다. 교육목표 및 중점과 교육내용, 교육과정은 연구자가 개발한 결과가 적절하였으나, 교육내용 중 기술적 분야는 교육대상별로 그 수준을 조절하거나 필요성에 대한 재고가 요구되었다.

전쟁의 양상은 농업사회, 산업사회, 지식정보화사회로 시대가 변화해감에 따라 변화해왔고, 미래의 전쟁양상은 지상·해상·공중·우주·사이버에서 진행되는 5차원 전쟁으로 변화·확대될 전망이다[26]. 미국은 사이버공간의 중요성을 인식하여 사이버공간을 우주공간과 함께 전쟁의 영역으로 설정하였고, 사이버능력을 보다 치명적인 전력(Lethal Force)으로 구축 중에 있다[27]. 북한의 사이버위협은 對美・對南 억제력을 넘어 이미 도발을 위한 공격력 수준이라고 평가되고 있으며, 사실상 핵무기를 보유하고 있다고 추정되는 상황에서 핵전략과 함께 사이버전을 결합하여 도발할 경우 이는 대한민국의 안보에 매우 위협적이다[26]. 이러한 상황에서 우

리 軍의 사이버작전은 물리작전과 연계된 합동작전으로 발전하는 것이 중요하다.

사이버작전이 합동작전으로 발전하기 위해서는 합동작전을 계획하고 합동전투발전업무의 주축을 이루는 非사이버작전부대 장교들에게 사이버작전을 교육해야 한다. 이를 위해서 앞선 연구를 기반으로 다음과 같은 방향성에 대한 결론을 가지게 되었다. 즉 1) 학교기관에서는 전투병과 위관장교 및 영관장교들이 사이버공간을 이해하고, 사이버공간의 중요성을 인식하며, 사이버작전을 이해시킬 수 있는 교육내용을 현재 시행되고 있는 합동군사대학교의 영관장교 교육과정(합동기본·고급과정)과 각 병과학교의 위관장교 교육과정에 교육프로그램으로 반영하여 계급별 수행 임무에 적합한 교육을 단계적으로 적용해야 한다. 2) 또한 야전부대에서는 전투력을 직접 운용하고 있는 지휘관에게 '사이버작전 임무' 를 부여하여 부대별 직무교육 및 전술토의를 활성화함으로써 사이버작전에 대한 교육훈련 소요를 창출할 수 있도록 해야 한다. 3) 한편, 현재 미군 합동사이버작전 교범을 기초로 발간되어 있는 합동사이버작전 교범을 우리 군의 특성에 맞도록 구체화하면서, 전술적 수준의 교범으로 발간하여 군사작전 계획 수립의 이론적 토대를 마련해야 한다.

본 연구는 기존 연구가 없어 일반화되지 않은 非사이버작전부대 장교들을 위한 사이버작전 교육체계를 문헌연구로 개발하여 전문가들로부터 델파이 설문조사를 통해 그 타당성을 확인함에 따라 향후 세부 교육프로그램 개발을 위한 기초 자료로서는 가치가 있을 것으로 사료된다. 하지만, 교육대상이 모든 장교가 아닌 전투병과 영관장교들로 한정되어 있고, 개발한 교육내용이 아직까지는 軍에서 표준화된 개념이 아니라는 점에서 학교기관의 교육프로그램으로 적용하기에는 한계가 있다. 또한 본 연구에서 얻어진 결과는 문헌연구와 일부 전문가들과의 델파이 설문조사를 통해 얻어진 것이기 때문에 일반화하기에는 어려움이 있다.

후속 연구를 위한 제언으로, 교육대상을 계급 및 직책별(위관장교, 영관장교, 장군, 지휘관, 참모)로 구분하여 교육체계를 보다 세분화할 필요가 있다. 또한 연구자가 제안한 교육체계의 효과성은 실제 교육프로그램으로 구성하여 적용하거나, 추가적인 연구를 통해 검증해 볼 수 있다.

참고문헌

[1] 박찬수, 박용석, “사이버전의 역량평가 개선과 역량 강화 방안에 관한 연구”, 한국정보통신학회 논문지, Vol. 19, No. 5, pp.1251-1258, 2015.

[2] 엄정호, “효과적인 사이버보안 교육훈련을 위한 교육과정 문제점 및 개선방안”, 보안공학연구 논문지, 제46호, pp.337-350, 2015.

[3] 이수진, “미래 지상군의 사이버작전 개념발전 방안”, 한국전략문제연구소 전투발전 2014, 제3장, 2014.

[4] 국군조직법제9조3항에 따른 전투를 주 임무로하는 각 군의 작전부대 등에 관한 규정, 대통령훈령 제29561호, 2019.

[5] 송재익, “한국군 합동 사이버작전 강화방안 연구 합동작전과 연계를 중심으로”, 한국군사문제연구원 한국군사(2), pp.147-186, 2017.

[6] 합동참모본부, “합동교범 5-0 합동기획”, 2018.

[7] 김영욱, 김광호, “뉴스미디어의 미래:델파이 조사와 시나리오 기법을 통한 탐색”, 한국언론진흥재단, 2010.

[8] 안유진, 손은경, “델파이 연구방법 중심 아동 교육연극 프로그램 개발 기초연구”, 예술인문사회융합멀티미디어논문지, 7권, 11호, pp.315-328, 2017.

[9] 박상서, 최운호, “국방 정보보호 인력 양성 방안”, 융합보안논문지, 제1권, 제1호, pp.69-81, 2001.

[10] 손태종, 김영봉, “국방사이버전 수행 발전방향”, 주간국방논단 제1431호, 2012.

[11] 김귀남, “국가 사이버전 대비방안 연구”, 융합보안논문지, 제6권, 제4호, pp.141-151, 2006.

[12] 박상돈, 김인중 “사이버안보 추진체계의 제도적 개선과제 연구”, 융합보안논문지, 제13권, 제4호, pp.3-10, 2013.

[13] 고성훈, “사이버전 전장정보분석 항목 개발에 관한 연구”, 중앙대학교 대학원 융합보안학과 산업보안전공 석사학위 논문, 2018.

[14] 김기범, “사이버작전 수행을 위한 사이버 국방 전문인력 교육체계 연구”, 고려대학교 정보보

호대학원 사이버안보학과 석사학위논문, 2016.
[15] 김원철, “사이버전 전문인력 양성 교육에 관한 인식 연구”, 고려대학교 정보보호대학원 공공보안정책학과 석사학위논문, 2014.
[16] 서상원, 오우진, 김호길, “AHP 기법을 적용한 국방정보시스템 보호를 위한 사이버전 교육 방안 연구”, 보안공학연구논문지, 제44호, pp. 109-120, 2015.
[17] 신규용, 전병진, 강정호, 박복기, 이인수, 유진철, “효과적인 사이버전 수행을 위한 육군사관학교 사이버전 교육현황 분석 및 발전방향 연구”, 한국군사학논집, 제72호, 2권, pp.131-167, 2016.
[18] 박명환, 김득수, 김동한, 설현주, “사이버 전문가 양성을 위한 사관학교 교과과정”, 한국군사학논집, 제74호, 제1권, pp.33-53, 2018.
[19] 육군본부, “야전교범 1-1 군사용어”, 2017.
[20] 국방부, “합동전투발전업무훈령”, 국방부 훈령 제2068호, 2017.
[21] 합동참모본부, “합동교범 3-24 합동사이버작전”, 2016.
[22] 국방부, “국방교육훈련 훈령”, 국방부 훈령 제2270호, 2019.
[23] P.W.싱어, 알란프리드만 공저, 박인철, 정우석 공역, “모두가 알아야 할 것들 사이버보안과 사이버전쟁”, ㈜프리렉, 2014.
[24] 이종성, “연구방법 21 : 델파이 방법”, 서울교학사, 2001.
[25] 노승용, “알기 쉬운 연구방법론 7 : 델파이 기법(Delphi Technique): 전문적 통찰로 미래 예측하기”, 국토연구원, 국토 2006, pp.53-62, 2006.
[26] 김강녕, “미래 전쟁양상의 변화와 한국의 대응”, 한국과 국제사회, 제1권, 제1호, pp.115-152, 2017.
[27] UNITED STATES AMERICA DEPART OF DEFENSE, “Summary of the 2018 National Defense Strategy of The United States of America”
[28] 이상운, 박용석, “사이버작전에 대한 공통 상황인식과 군사작전과의 통합성 발휘를 위한 軍 교육훈련 발전분야 연구”, 한국IT서비스학회 2018 추계학술대회논문집, pp.458-461, 2018.

〔저자소개〕

이 상 운 (Sangwoon Lee)
1994년 3월 육군사관학교 물리학과 학사
1994년 3월~현재 육군
2017년 3월~현재 세종사이버대학교 정보보호대학원 석사과정
email : kmacaptain@daum.net

박 용 석 (Yongsuk Park)
서강대학교 컴퓨터학 (학사)
뉴욕(Tandon/POLY)대 (석사, 박사)
AT&T (Bell) Labs, 삼성전자
현재 세종사이버대학교 정보보호대학원 주임교수
현재 세종사이버대학교 IT학부 교수
email : yongspark@sjcu.ac.kr