

미국 ATE 정책 기반의 신규 사이버보안 인력양성 정책 비교 프레임워크 연구

홍 순 좌^{†*}
ETRI 부설연구소

A Study on the Framework of Comparing New Cybersecurity Workforce Development Policy Based on the ATE Programs of U.S.

Soonjwa Hong^{†*}
The Attached Institute of ETRI

요 약

미국의 사이버보안 인력양성 정책은 2010년 시작된 NICE를 중심으로 포괄적이고 체계적으로 추진되고 있다. 기존 과학·기술·공학·수학(STEM) 전문인력 양성 정책의 일환인 국가과학재단(NSF)의 첨단기술교육(ATE) 8개 분야 중 하나인 보안기술(Security Technologies)에서 사이버보안 인력양성 프로그램을 운영 중이다. 이 보안기술 분야는 NICE와 연계하여 추진되고 있으며, 5종의 세부 프로그램으로 구성된다. 본 논문은 ATE에서 지원하는 사이버보안 인력양성 프로그램 5종에 대해 세부적으로 살펴보고, 이 프로그램들과 유사한 우리나라의 정부지원 프로그램을 상호 비교하여 개선점을 도출한 후, 국가차원의 신규 사이버보안 인력양성에 대한 추진 방향을 제안한다. 이때 적용된 방법론을 체계적으로 정리한 사이버보안 인력양성 정책·평가 프레임워크를 새로운 인력양성 정책 수립 시 적용할 수 있도록 제안한다.

ABSTRACT

The US cybersecurity workforce policy is being pursued comprehensively and systematically, based on the NICE established initiated in 2010. Security Technologies, one of the eight areas of Advanced Technology Education(ATE) of the National Science Foundation(NSF) included in the STEM. This policy has been comprehensively promoted in conjunction with NICE, and this security technology field is operated with five detailed programs. In this paper, we examine in detail five cybersecurity workforce development programs supported by ATE, and compare them with the current status cultivation of cybersecurity workforce in Korea. After finding out the problems and improvements by comparison with the current situation of cybersecurity workforce development in Korea, we propose several implementations of nation-wide strategies for cultivating new cybersecurity workforce in Korea.

Keywords: ATE, NICE, FISMA, Cybersecurity Act, CSSIA, CSEC, NCC, CWW, ACE, Cybersecurity Training

1. 서 론

2000년대 들어오면서 미국 연방정부는 외국으로

부터 거세지는 사이버위협 및 공격에 대한 대응책으로 전문 인력양성을 국가차원의 핵심과제로 인식하였으며, NICE로 대표되는 관련 정책 및 프로그램도

체계적이라고 할 수 있다. 미국의 사이버보안 인력양성은 초·중·고·대학생 대상의 신규 인력양성과 연방기관에서 근무 중인 직무인력 양성으로 구분할 수 있다.

국내의 경우 정보보호, 정보보안, 사이버보안 등 많은 용어들이 구체적으로 정의되지 못하고 혼재되어 사용되고 있는 현실을 감안한다면 전문 인력양성에 대한 구체적인 정책수립과 구현은 매우 어려운 일이라고 할 수 있다.

미국의 경우 1980년대에는 컴퓨터 보안법(Computer Security Act of 1987)에서 보듯이 컴퓨터 보안과 함께 네트워크 보안이라는 용어가 사용되었다[1]. 1990년대에는 IT 용어의 등장과 더불어 정보보안(information security), 정보보증(information assurance) 등의 용어가 사용되었으며, 90년대 후반기 인터넷의 등장 및 초고속인터넷의 발전에 따라 정보전(information warfare)이라는 새로운 용어가 등장하였다. 2000년대에 들어서서 공포된 국토안보법(Homeland Security Act of 2002)은 부속절 'C-Information Security' 내에 사이버보안 강화법(Cyber Security Enhancement Act of 2002)을 제정하였다[2]. 이 법에서 보듯이 사이버보안 용어가 공식적으로 법에서 처음 등장하였으며 정보보안 내에 사이버보안을 포함시키는 개념으로 사용되었다. 이후 모든 국가 법·제도·정책 문서에서는 사이버보안(cybersecurity)이 가장 포괄적인 용어로 정리되어 사용되고 있다. 우리나라의 경우에도 더 이상 혼란을 주지 않도록 용어에 대한 재정립이 필요하다.

미국은 연방정보보안관리법(FISMA 2002)의 연방기관의 책임(\$3544)에서 직무인력을 훈련하도록 의무화하였다. 또한 정보시스템 계약자 및 기타 사용자 등 외부 인력에 대한 보안인식제고훈련(security awareness training)을 의무화하는 등 처음으로 사이버보안 기관장의 임무로 규정한 법으로서 가치를 갖는다고 할 수 있다[3].

2008년 국가사이버보안종합전략(Comprehensive National Cybersecurity Initiative, CNCI)을 기반으로 사이버보안 인력 대상으로 교육을 확대하여 인력양성 정책을 본격적으로 추진[4]하고자, 2012년 국립표준기술연구소(National Institute of Standards and Technology, NIST)를 중심으로 “국가사이버보안교육정책(National Initiative for Cybersecurity Education, NICE)”을 수립하여 민·관·군이 체계

적으로 추진하는 국가정책이 시작되었다[5]. 민간협력은 NIST, 연방정부 직무인력양성 정책은 국토안보부(DHS), 군 인력은 국방부가 주관이 되어 NICE 정책을 추진하고 있다.

NICE 등 인력양성 정책 추진의 근거를 명확히 하는 사이버보안 인력 전용의 법률인 사이버보안 인력 평가법(Cybersecurity Workforce Assessment Act 2014)이 제정되기에 이르렀다[6]. 이 법을 근거로 DHS는 산하 직무인력에 대한 인적역량 강화를 추진하고 있다. 계속적으로 제정되는 사이버보안 법률에서 인력양성을 강화해 나가고 있으며 2015년도에 국가 사이버보안을 포괄하는 사이버보안법(Cybersecurity Act of 2015)을 제정하였다. 이 법에는 유관법률 “Cybersecurity Information Sharing Act of 2015”, “National Cybersecurity Protection Advancement Act of 2015”, “Federal Cybersecurity Enhancement Act of 2015”, “Federal Cybersecurity Workforce Assessment Act of 2015”을 포함하고 있다[7].

이미 제정된 “사이버보안인력평가법 2014”는 DHS 내 직무인력으로 한정된 범위를 전 연방정부 직원으로 확대한 “연방사이버보안인력평가법”으로 강화되었다. 이와 같이 미국은 법으로 사이버보안 인력의 교육·훈련을 의무화 하는 등 사이버보안 인력양성에 대한 확고한 의지를 알 수 있다.

사이버보안 대응능력 확보는 국가 안보차원에서 더 이상 간과할 수 없는 필수정책으로 추진되어야 하는 것은 일반적인 공감대이다. 그러나 우리나라에서는 어떻게 인력양성을 추진해야 하는지에 대한 구체적이고 실질적인 방법론은 미흡한 현실이라고 할 수 있다.

사이버보안 인력양성 정책은 국가별로 교육문화, 법·제도, 경제 등이 상이하므로 직접적으로 비교하는 것은 무리가 따를 수 있다. 본 논문은 미국의 ATE 사이버보안 프로그램 5종을 상호 비교 후 프로그램별로 특성을 도출하여 인력양성 프로그램 비교 항목으로 선정한다. 이 비교항목은 유사하게 추진되는 우리나라의 사이버보안 인력양성 프로그램으로 국가정보보호백서에서 식별한 5개 프로그램과 교육부가 주관하는 정보보호형재교육원 사업의 6종을 비교한다. 정부지원 정책에서 대표적으로 수행하고 있는 정보통신기술진흥센터의 인력양성 사업 15종 내에 사이버보안 인력양성도 포함되어 있으나 본 연구에서는 사이버보안 인력양성에 대해 독립적인 사업만을 대상으로 적용하므로 복합적인 인력양성 프로그램은

연구범위에서 제외한다.

본 논문에서는 미국의 사례 연구를 기반으로 우리의 사이버보안 인력양성 현실과 비교를 통해 개선방향을 도출해 보고자 한다. 2장에서는 미국의 사이버보안 인력양성 정책인 NICE를 중심으로 살펴보고, 3장은 NICE에서 지원하는 20여종의 협력 프로그램들을 살펴보고, 그 중에 초중고 대학생 대상의 인력양성 프로그램인 ATE 사이버보안 프로그램 5종을 면밀히 분석한다. 4장에서 ATE 프로그램과 유사한 국내 사이버보안 인력양성 지원 프로그램 6종을 선정하여 ATE 프로그램과 비교하며, 사이버보안 인력양성 정책 비교·평가 프레임워크를 제안한다. 마지막으로 5장에서 결론을 맺는다.

II. 미국 사이버보안 인력양성 추진 현황

2.1 추진 경위

미국은 급증하는 사이버공격에 대응하는 인력을 양성하는 정책을 국가차원에서 마련해 오고 있으며, 이와 같은 사이버보안 교육, 훈련 및 인력 개발 요구에 효과적으로 대응하기 위해 다양한 정부지원 프로그램들이 운영되고 있다. 국가적인 차원의 일원화된 사이버보안 교육·훈련 정책은 부시정부 말인 2008년 1월 수립된 CNCI의 12개 전략 중 하나인 사이버보안 관련 교육을 확대하는 정책을 시작으로, 국가차원의 사이버보안 인력양성이 본격적으로 추진되었다[4]. 오바마 정부는 2009년 2월 취임 후 60일간의 사이버보안 정책검토를 통해 “Cyber-space Policy Review”를 발표하였다. 기존 부시정부의 CNCI 정책을 보완하여 사이버보안 분야의 중요성이 더욱 증대되었다고 평가받고 있다[8][9].

2010년 4월 CNCI의 8번째 전략인 “사이버보안 교육확대”를 기반으로 오바마 대통령은 사이버보안 중점 정책 추진 방침과 더불어 백악관 국가안전보장위원회(NSC)의 사이버보안 이사회, 국가정보국실(ODNI)의 합동유관기관 사이버 태스크포스의 결정에 따라 NIST가 전반적인 정책관리 역할을 수행하는 NICE가 공포되었다. 발표 당시 NICE는 트랙 1(국가 사이버보안 인식 제고), 트랙 2(공식적인 사이버보안 교육), 트랙 3(연방 사이버보안 인력 구조 구축), 트랙 4(사이버보안 인력 훈련 및 전문가 육성)과 같이 4가지 트랙으로 정책 방향을 수립하였다.

NIST를 중심으로 NICE 세부전략을 수립하는

과정을 통해 2011년 8월 “국가사이버보안교육정책 전략 계획(National Initiative for Cybersecurity Education Strategic Plan(Draft) - Building a Digital Nation)”을 공포하였다. 관련 기관 및 참여자들의 의견 수렴을 통해 마련된 최종적인 계획 보고서를 2012년 발표하여, 사이버보안 인력양성에 대해 본격적인 추진을 할 수 있었으며 ‘트랙’이라는 용어는 ‘컴포넌트’라는 명칭으로 변경되었다[5].

Fig.1.에서 보듯이 ‘컴포넌트1’을 주관하는 기관은 국토안보부가 담당하고 있으며 국가 차원의 사이버보안 인식제고 관련 업무를 담당하고 있다. ‘컴포넌트2’는 국가과학재단(NSF)과 교육부가 주관이 되어 운영하고 있다. NSF는 기존의 과학·기술·공학·수학(Science·Technology·Engineering·Mathematics, STEM) 교육과 연계하여 사이버보안 교육 프로그램을 지원하고 있다. 또한 첨단기술교육(Advanced Technological Education, ATE) 프로그램에 사이버보안을 독립적인 분야로 설정하여 강력한 정책적인 지원을 해오고 있다[5].

‘컴포넌트3’는 국토안보부와 인사관리처(Office of Personnel Management, OPM)가 공동으로 주관하고 있다. 사이버보안 직무인력에 대한 구조화를 목적으로 추진한 결과 2017년 8월 “NICE Cybersecurity Workforce Framework(NIST SP 800-181)”를 공포하여 연방 정부차원의 표준을 마련하였다[10]. ‘컴포넌트4’는 국토안보부, 국방부,



Fig.1. NICE Structure

국가정보국실 주관으로 국가 사이버보안 인력을 육성하고 있다. 국방부와 ODNI는 자체 수급 인력에 대해 독자적인 사이버보안 인력양성 프로그램을 추진하고 있는 반면, 국토안보부는 연방기관들이 필요로 하는 사이버보안 인력을 양성하여 보급하는 정책을 주관하여 추진하고 있다.

2.2 NICE 협력 및 지원 프로그램

NICE 정책에 있어 NIST가 총괄기관 역할을 담당하고 있으며, 특히 민간분야와의 협력을 주도적으로 추진하고 있다. 미국의 사이버보안 인력양성은 연방정부, 주정부, 학계 및 산업계 등 다방면에서 추진되고 있는바 정확한 현황을 파악하는 것도 어려운 현실이다. 2012년부터 본격 추진된 NICE는 2016년에 이르러서 NIST 입장에서 추진되는 정책들의 성과, 결과, 현황 등을 요약한 분기별 eNewsletter를 홈페이지에서 발간하고 있다[11].

2016년 봄호부터 2017년 겨울호까지 8종의 뉴스레터를 기반으로 NIST 제휴 프로그램, NIST 예산

지원 프로젝트 두 가지로 구분해 볼 수 있다.

NIST 제휴 프로그램은 Table 1.에서 보듯이 약 12개 프로그램이 운영 중에 있다. 미국의 첨단기술 교육(Advanced Technological Education, ATE) 주관으로 국가과학재단(NSF) 지원을 받아 지정 운영되는 사이버보안 인력양성 관련 ATE 센터는 2017년 5종이 지정되어 있다.

NIST에서 자금을 지원하는 프로그램은 Table 2.에서 보듯이 약 8개 프로그램이 운영 중에 있다. 5개 기관은 'Regional Alliances and Multistakeholder Partnerships to Stimulate(RAMPS)'에서 수여하는 RAMPS 2016 Award를 수상하였다[11].

Table 2. NIST Funded Programs

No	Funded Programs	etc
1	NICE Challenge Project	
2	National Integrated Cyber Education Research Center(NICERC)	
3	PACET : Partnership to Advance Cybersecurity Education and Training	RAMPS 2016 Awardee
4	HRCyber : The Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance	RAMPS 2016 Awardee
5	Cin-Day Cyber : Cincinnati-Dayton Cyber Corridor	RAMPS 2016 Awardee
6	Cyber Prep Program	RAMPS 2016 Awardee
7	The Arizona Statewide Cyber Workforce Consortium	RAMPS 2016 Awardee
8	CyberSeek	

Table 1. NIST Affiliated Programs

No	Affiliated Programs	etc
1	Cybersecurity Education and Awareness Portal : National Initiative for Cybersecurity Careers and Studies (NICCS)	
2	Advanced Cyberforensics Education(ACE) Consortium	ATE Center
3	Center for Systems Security and Information Assurance	ATE Center
4	Cyber Security Education Consortium (CSEC)	ATE Center
5	CyberWatch West (CWW)	ATE Center
6	National CyberWatch Center (NCC)	ATE Center
7	Catalyzing Computing and Cybersecurity in Community Colleges(C5)	
8	CAE Community	
9	National Centers of Academic Excellence(CAE) CAE-C National Centers of Academic Excellence in Cybersecurity CAE-CD National Centers of Academic Excellence in Cyber Defense CAE-CO National Centers of Academic Excellence in Cyber Operations	
10	CyberCorps®: Scholarship for Service	
11	GenCyber	
12	K-20 Cybersecurity CECOR Project	

III. 미국 첨단기술교육(ATE)

3.1 ATE 추진 경위

미국의 ATE 역사는 1980년대 초반까지 거슬러 올라간다. 미국 주니어 및 커뮤니티 칼리지 협회는 펜실베이니아 주 하원 Doug Walgren 의원과 협력하여 NSF가 2년제 대학에 대한 보조금을 늘리는 법안들과 1989년 노스캐롤라이나의 하원의원 David Price는 과학 및 기술 문맹 퇴치 법안을 발의 하였다. 이 같은 노력을 통해 1992년 10월, 의회는 SATA(Scientific and Advanced Technology Act of 1992)로 불리는 Public

Law 102-476의 과학 및 첨단 기술 법을 통과 시켰다. 1993년, SATA 1992 법을 근거로 국가과학 재단은 첨단기술교육 프로그램을 시행하였다 [13][14].

1993년 NSF는 SATA 법을 근거로 ATE 프로그램 계획을 국가과학위원회(National Science Board, NSB)에 보고하여 승인받았고, 1993년 8월 연방 관보에 공표하여 공식적으로 추진하게 되었다[15]. ATE 프로그램의 추진 경과를 살펴보면 다음과 같이 요약할 수 있다[13].

- o 1994년, 3개 센터, 16개 기획 보조금, 39개 프로젝트에 기금 지원
- o 1994년 10월 27일, 미국 커뮤니티 칼리지 협회 첫 번째 ATE 수석 조사관 컨퍼런스 소집
- o 1998년, 11개 센터, 158 프로젝트
- o 2001년, 지역 센터 시작
- o 2007년, 247개 실행 보조금 운영
- o 1993년~2013년, 1,201개 ATE 교부금상 532개 기관에 수여, 2013년, 292개 실행 보조금 운영
- o 2013년, 292개 실행 보조금(active grants)
- o 2017년, 42개 ATE 센터 및 296개 프로젝트 운영 중

ATE 프로그램은 국가 경제·안보에 중요한 첨단 기술 산업분야의 전문인력을 육성하는 것을 목적으로 시행되고 있으며, 대부분의 전문인력은 커뮤니티 칼리지의 준 학사 프로그램과 중등학교의 관련 프로그램을 통해 자신의 직업 선택과 준비를 할 수 있도록 지원하고 있다. 2017년 현재 전국적으로 지정된 42개의 ATE 센터는 ATE Centers 홈페이지(atecenters.org)에서 확인할 수 있다.

ATE의 각종 프로그램은 학부생 및 중등학교 학생들을 위한 과학·기술·공학·수학 교육을 강화하기 위해 ‘혁신적인 교재, 코스, 커리큘럼 및 교수법을 개발하고 시험’, ‘급속하게 진화하는 기술 분야의 대학 교수 및 중등학교 교사에 대한 지식·기술력 양성’, ‘서로 다른 기술 분야에서 활용 가능한 직무 수행 인력에 대한 교육 요구 분석’, ‘직무 필요성을 충족하기 위한 학생들에 대한 교육 프로그램 및 직무 경로를 설계와 같은 다양한 활동을 지원한다[15].

3.2 ATE 프로그램 세부내용

2017년 현재 ATE 프로그램에서 지원하는 기술 분야는 ‘고급 생산 기술’, ‘농업 및 바이오 기술’, ‘에

너지 및 환경 기술’, ‘공학 기술’, ‘정보 기술(IT)’, ‘학습·평가 및 연구’, ‘마이크로 및 나노 기술’, ‘보안 기술’의 8개 분야로 구성되지만 매년 평가를 통해 조정되고 있다.

ATE 프로그램에서 지정된 ATE 센터 및 프로젝트는 혁신적인 STEM 기술자 양성을 위한 교육 프로그램을 지원하며, 해당 프로그램의 주관 대학 및 파트너 기관은 기존 또는 신기술에 관한 새로운 교육 방법을 개발한다. 이러한 구조적 연구를 통해 만들어진 결과물은 교육 모듈, 새로운 교육 과정, 인증서, 학위 프로그램이 있다. 이 프로그램을 통해 2년제 대학 강사와 중등학교 교사는 새로운 기술과 교육 방법을 배우고, 이를 통해 산업계에서 필요한 능력을 갖추도록 학생들을 육성할 수 있다.

Fig.2.는 2017년 운영 중인 42개의 ATE 센터에 대한 미국 전역의 분포도를 보여주고 있다.

2017년 기준 ATE에서 지원하는 42개 프로그램은 3개 트랙으로 구분하고 있다. 트랙 1은 국가센터(National centers), 지역센터(Regional centers), 지원센터(Support centers)와 같이 세 가지 유형으로 구분하여 ATE 센터를 지정하고 예산 등을 지원하고 있다. 국가센터는 국가차원의 산업별 개혁을 리드하는 기관의 역할을 담당한다. 지역센터는 특정 지역 내의 특정 산업에 중점을 두는 기관이며, 지원센터는 하나 이상의 기술 영역에서 다양한 ATE 교육자를 지원하는 제품과 서비스를 제공한다. 트랙 2는 프로젝트가 커리큘럼 개발, 프로그램 개선 또는 교수 육성과 같은 활동에 좀 더 집중적으로 초점을 맞춘다. 트랙 3은 기술자 교육을 타겟형 연구 방식으로 추진하는 분야로서, 기술자를 교육하는 측면과 기술자 인력의 이해도에 중점을 두어 ATE 센터와

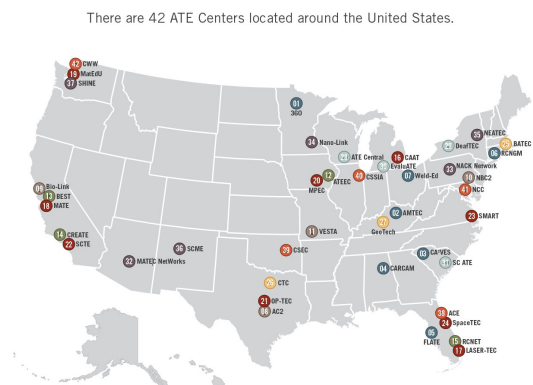


Fig. 2. 42 ATE Centers Map

Table 3. ATE Centers for Security Technology

ATE Center	Year	Type
CSSIA(Center for Systems Security and Information Assurance) www.cssia.org	2003	Regional center
CSEC(Cyber Security Education Consortium) www.cseconline.org	2004	Support center
NCC(National CyberWatch Center) www.cyberwatchcenter.org	2005	Regional center
CWW(CyberWatch West) www.cyberwatchwest.org	2011	National center
ACE(Advanced Cyberforensics Education) Consortium www.daytonastate.edu/ace/	2012	Support center

프로젝트가 산업과 학생 양쪽의 요구사항을 보다 효과적으로 반영할 수 있도록 조정 및 해결하는 방법을 연구하여 개발하는 분야이다.

2017년 현재 보안 기술 분야에는 Table 3.와 같이 5개의 주관 센터가 지정되어 있다.

3.2.1 국가시스템보안 및 정보보증센터(CSSIA, 2003년)

CSSIA는 2003년에 지정된 지역센터로서 Illinois주 Palos Hills에 위치한 Moraine Valley Community College에서 운영하고 있으며, 미국 중서부에 있는 6개의 기관과 파트너를 맺고 있고, 미국 전역의 대학 및 고등학교와 협력·제휴 관계를 유지하고 있다.

CSSIA는 중서부대학 사이버방어 경진대회(Midwest Collegiate Cyber Defense Competitions, CCDC)를 운영하여 학생들에게 사이버보안 분야의 실제 경험을 제공한다. 2006년 중서부 최초의 대회를 시작한 이래로 CSSIA는 매년 여러 주 및 지역 대회에서 300명이 넘는 학생들을 참여하고 있다. 2008년 CSSIA는 경진대회 자문위원회(Competition Advisory Board, CIAB)를 구성하여 업계 참여를 확대하고 실제 직무 경험을 할 수 있도록 해당 콘텐츠를 대회에 추가했다. 2006년부터 2011년까지 1,120명의 학생들이 이 대회에 참가했다.

CSSIA는 가상화 교육이 가능하도록 사이버보안 교육 콘텐츠를 개발하고 있다. 2011년 CCDC 대회의 효과적인 추진을 통해 CSSIA 가상화데이터센터(CSSIA Virtualization Data Center, CVDC)

가 성공적으로 정착될 수 있었다. CVDC의 가상화 기능을 통해 이 대회에 참여할 수 있는 팀 숫자를 확대할 수 있었고, 비용을 절감할 수 있도록 복잡한 경쟁 환경을 복제할 수 있는 능력을 통해 대회를 성공적으로 치를 수 있었다. 표준화된 데이터 센터의 설립으로 사이버보안 교육자들은 사이버보안 및 정보보증 관련 프로그램을 가르치고자 하는 기관에게 쉽게 배포하고 공유할 수 있는 여러 커리큘럼을 개발할 수 있었다. CSSIA 가상 환경은 5가지 코스를 지원하고 있으며 추후 윤리적 해킹, 디지털 포렌식, 보안+, Microsoft 및 Linux OS 플랫폼 강화 등의 추가 코스를 개발할 계획이다.

2017년 현재 CSSIA 가상 교육 및 학습 환경은 250개 교육 기관에서 채택되고 있으며, 이 기관들의 강사는 사이버보안 과정, 인증 프로그램 및 2년제 학위 과정에 등록한 10,000명 이상의 학생들을 가르치고 있다. 2011년 이래 293개의 고등 교육 기관에서 CSSIA 과정 중 하나 이상을 다음과 같이 개설하여 운영해 오고 있다.

- o Security+(v.2) 247개 기관 운영
- o Ethical Hacking 218개 기관 운영
- o CNSS 4011 194개 기관 운영
- o Forensics 155개 기관 운영
- o Network Security 87개 기관 운영
- o Security+(v.3) 74개 기관 운영
- o Python Security 43개 기관 운영

3.2.2 사이버보안교육컨소시엄(CSEC, 2004)

CSEC은 2004년에 지정된 지원센터로 Tulsa 대학교에서 운영 중이다. Arkansas, Colorado, Kansas, Louisiana, Missouri, Oklahoma, Tennessee, Texas 주에 있는 2년제 대학과 직업·기술 센터와 파트너십을 맺고 있다. Tulsa 대학교는 책임 훈련 기관을 담당하며 2년제 교육기관 49곳에 대한 멘토를 담당한다(Table 4.). 초기에는 오클라호마 주에 있는 8개의 기관에서 11명의 사이버보안 강사와 함께 시작되었다.

2017년 기준, CSEC 기관들은 502개의 보안학위 전공을 운영하고 있으며, 340명의 학생들은 보안 관련 인증을 받기 위해 해당 교육에 참여하고 있다. 2015년 한 해 동안 169 명의 학생들이 준학사학위(associate degrees)를 받았으며, 56명의 학생들

이 학사학위를 받고 243명이 수료하였다. 또한 CSEC 학생에게 341건의 CNSS(Committee on National Security Systems) 인증서가 발급되었으며, 심포지엄 또는 교육과정을 통해 721명의 재직자가 교육을 받았다.

CSEC이 시작된 2004년 이후 2017년 현재 1,442명의 학생들이 사이버보안 준학사학위를 받았

고 360명이 학사학위 프로그램을 마쳤다. 한편, 1,878명의 학생들이 인증 프로그램(certification program)을 마쳤다. CSEC 기관은 2004년부터 2,236개의 CNSS 인증서를 발행했으며, 많은 학생들이 CNSS 인증서를 받았다.

Table 4. CSEC Partnership Institutions in 8 States

Arkansas
<ul style="list-style-type: none"> o Arkansas State University - Beebe o Arkansas State University - Mountain Home o Northeast Arkansas Community College o Phillips Community College o Pulaski Technical College o University of Arkansas Community College Batesville
Colorado
<ul style="list-style-type: none"> o Arapahoe Community College o Community College of Aurora o Front Range Community College o Pueblo Community College o Red Rocks Community College
Kansas
<ul style="list-style-type: none"> o Butler Community College o Dodge City Community College o Hutchinson Community College o Johnson County Community College o Kansas City Kansas Community College o Manhattan Area Technical College
Louisiana
<ul style="list-style-type: none"> o Bossier Parish Community College o Louisiana Technical College - Sullivan o Bossier Parish Technical School
Missouri
<ul style="list-style-type: none"> o Metropolitan Community College o St. Louis Community College
Oklahoma
<ul style="list-style-type: none"> o Cameron University o Control System Security Sites o Oklahoma CareerTech Cyber Security Sites o Oklahoma City Community College o Oklahoma State University - Institute of Technology o Rose State College o University of Tulsa
Tennessee
<ul style="list-style-type: none"> o Cleveland State Community College o Columbia State Community College o Dyersburg State Community College o Jackson State Community College o Nashville State Community College o Northeast State Community College o Pellissippi State Technical Community College o Roane State Community College o Southwest Tennessee Community College o Volunteer State Community College o Walters State Community College
Texas
<ul style="list-style-type: none"> o Richland College o Texas State Technical College Sweetwater

3.2.3 국가사이버위치센터(NCC, 2005년)

NCC는 2005년에 지정된 지역센터로 Maryland 주 Largo에 있는 Prince George’s Community College에서 운영 중이다. NCC는 준학사학위 및 인증 프로그램을 위한 정보보증 커리큘럼을 개발한다. NCC 프로그램을 통해 커리큘럼을 연방 및 산업 지식과 기술 표준, 직무 역할과 전문 인증에 매핑하여 학생들이 2년제 및 4년제 학위 프로그램 사이를 공유할 수 있도록 모델이전경로(Model transfer pathways)를 활용하고 있다. 이 모델이전경로에는 2년 및 4년 교육 기관 간의 전환뿐 아니라 수평 및 역방향 이동이 포함된다.

수천 명의 학생들과 수백 명의 교수진이 매년 National Cyber League(NCL)에 참가하며, 이 행사를 통해 대학생 및 교수진이 사이버보안 지식 및 기술을 개발하여 실행해 본 후 검증할 수 있는 지속적인 가상교육 환경을 제공받는다. 교수진의 실제 시뮬레이션 환경에는 산업계의 인증에 부합하는 콘텐츠가 포함되어 운영된다.

국가사이버보안학생협회(National Cybersecurity Student Association, NCSA)는 학생의 교육과 직업개발을 활동, 네트워킹 및 협업으로 발전시키는 역할을 담당하고 있다[12].

NCC는 업계, 정부 및 학계 간의 협력과 혁신 문화를 조성함으로써 NCC의 리더십이 전국 대학의 사이버보안 프로그램의 수준을 향상시켰으며, 이러한 대규모 네트워크에는 고등교육기관, 공립 및 사립학교, 기업 및 정부 기관 등 200개 이상의 파트너가 참여하고 있다.

3.2.4 사이버위치 웨스트(CWW, 2011년)

CWW는 2011년에 지정된 국가센터로 Washington 주 Bellingham에 있는 Whatcom Community College에서 운영 중이다. CWW는 서부지역 14개 주에서 사이버보안 인력을 육성하기 위한 프로그램을 개발 중이다.

2011년 이후 CWW는 267명의 대학 교수진을 대상으로 17가지 기술 습득 워크숍을 제공했으며, 교육과정에 대한 주제는 공인 윤리 해커 및 포렌식 포함된다. CWW는 핵심 인프라 보안 및 복원력에 관한 13개 오픈소스 코스와 같은 새로운 커리큘럼 리소스를 웹 사이트를 통해 온라인으로 교수들에게 제공한다.

2014년 가을 NCL에서 학생들은 “capture-the-flag” 연습에 온라인으로 참여했다. 참가한 1,368명의 학생 중, 전년도인 2013년 보다 48% 증가한 1,040명(76%)은 적어도 하나의 깃발을 획득하였다. 이러한 대회에 참여함으로써, 학생들은 기업가에게 자신의 사이버보안 기술이 가치가 있다는 것을 보여 주게 된다.

CWW의 긍정적인 경제적 영향으로 기업주가 사이버위협으로부터 회사를 보호할 수 있도록 다양한 산업 부문과의 협력을 위해 CEO, CTO 및 인력, 회계 및 법률 부서의 직원을 포함하여 총 605 명이 참석한 2014년 개최한 사이버위협정상회의(Cyber Risk Summits)를 들 수 있다.

CWW는 매년 3개의 대학 수준의 경연대회와 1개의 고등학교 수준 경연대회를 후원하여 고등학생, 2년 및 4년 대학생이 참여하는 사이버보안 대회를 지원하는데, 그 대회는 Table 5.에서 보여준다.

CWW는 교사진과 학생들에게 사이버보안의 이해를 넓히고 탐구하도록 지원한다. CyberGirlz 및 Girls Go Tech와 같은 워크숍에서는 여중생들에게 사이버보안 및 관련 직업을 소개한다.

Faculty Graduate Program(FGP)은 자격을 갖춘 교수진이 CWW의 재정 지원을 받아 사이버보안 학위 또는 인증을 위한 대학원 수업 과정을 수강

할 수 있게 한다. Faculty Professional Development Training(FPDP)을 통해 정기적으로 교수진을 대상으로 디지털포렌식 및 교수진 멘토와 같은 주제로 워크숍을 개최하고 온라인 회원 모임에는 종종 새로운 도구 및 기법에 대한 프레젠테이션 교육 등이 포함된다.

Table 6.는 사이버방어 교육 또는 정보보증 교육에서 CAE 또는 CAE-2Y로 지정된 CWW 멤버인 19개 교육기관들을 보여준다.

Table 6. CWW Membership Institutes

Community Colleges(9)	
o	Coastline Community College, Fountain Valley, CA
o	Eastern New Mexico University Ruidoso, Ruidoso, NM
o	Estrella Mountain Community College, Avondale, AZ
o	Highline College, Kent, WA
o	Honolulu Community College, Honolulu, HI
o	Houston Community College, Houston, TX
o	Mt. Hood Community College, Gresham, OR
o	Red Rocks Community College, Lakewood, CO
o	Whatcom Community College, Bellingham, WA
Universities(10)	
o	California State Polytechnic University Pomona, Pomona, CA
o	California State University, San Bernardino, San Bernardino, CA
o	National University, La Jolla, CA
o	Regis University, Denver, CO
o	San Jose State University, San Jose, CA
o	Texas A&M University-Corpus Christi, TX
o	University of Arizona, Tucson, AZ
o	University of Idaho, Moscow, ID
o	University of Texas at El Paso, El Paso, TX
o	University of Washington, Seattle, WA

Table 5. Cyber Competitions supported by CWW

Student	Cyber Competitions
College Students	o Western Regional Collegiate Cyber Defense Competition (WRCCDC) www.wrccdc.org
	o Pacific Rim Regional Collegiate Cyber Defense Competition(PRCCDC) www.prcdc.org
	o National Cyber League(NCL) www.nationalcyberleague.org
High School Students	o CyberPatriot www.uscyberpatriot.org

3.2.5 첨단 사이버포렌식 교육(ACE, 2012년)

ACE 컨소시엄은 2012년에 지정된 지원센터로 Florida주의 Daytona 주립대학교에서 운영 중이다. 2017년 현재, ACE 컨소시엄은 4개 주에 걸쳐 멤버로 15개 기관이 지정되었으며, 주별로 1개의 수석 기관이 있다. ACE는 사이버보안 교육을 담당하는 교수진의 능력을 향상시키고 고등학생들의 사이버보안에 대한 관심도를 증대시키는 일환으로 Florida, Georgia, Carolina 주 지역의 12개 파트너 기관에서 활용할 수 있는 사이버보안 커리큘럼을 제공하였다. 이를 위해 온라인으로 교수진 전문능

력 육성, 인력 재교육을 위한 워크숍 및 인증 프로그램 개발, K-12 학교 및 기타 기관과 파트너 관계를 맺고 학생들을 참여시키는 활동들을 수행한다.

ACE의 중요한 기능은 교수진 육성으로 이들에게 사이버보안 교육을 시행하고 각 교육기관들이 학생들에게 효과적인 사이버보안 교육과정을 제공할 수 있는 도구를 제공하는 것이다. 트레이너 훈련 프로그램(train-the-trainer program)은 핵심 사이버포렌식 코스를 운영하는 것을 목표로 4가지 형태의 자기주도 온라인 과정으로 구성되어 있다. 이 과정에는 130개의 고화질 비디오 강좌, 키값이 부여된 실습 과제(hands-on assignments with keys), 퀴즈, 독서 자료 및 슬라이드가 포함된다. 2017년 현재 14명의 교수진이 이 프로그램 개발에 참여하고 있으며 이들 교수진은 비디오 강의, 과제 및 퀴즈와 같은 학습 관리 시스템에 대한 자료를 자신이 속한 교육 기관에서 ACE 참여 및 협력기관에게 제공하는 것을 담당하고 있다.

2016년 ATE Centers에서 발표한 보고서인 "Impact Partners with Industry for a New American Workforce 2016-2017"에서 발표한 내용 중 2015년 ACE의 학습관리 시스템에는 25개 주에 걸쳐 58개 기관의 110명의 교육자가 등록되어 있었다. 2012년 시작된 ACE 프로그램은 2015년까지 1,500명 이상의 대학생이 ACE에서 운영 중인 5개 코스 중 적어도 하나를 완료했다[15].

South Piedmont Community College는 2016년 6월과 7월에 이들 동안 사이버 캠프를 개최하였으며 14세에서 18세 사이의 40명의 학생들이 참가했다. North Carolina 주 Charlotte에 있는 Microsoft 건물에서 열린 5일짜리 사이버 캠프에 30명 학생(14~18 세)들이 참석했다. FBI, Microsoft, Time Warner Cable, InfraGard 등이 공동 협력기관으로 참여하였다.

Florida 사이버 얼라이언스와 공동으로 진행된 ACE 컨소시엄은 Daytona 주립대학교에서 제5회 연례 사이버 캠프(Cyber Camp, 2017)를 2017년 6월 12일~15일 동안 개최했다. 캠프 기간 동안 40명의 9학년~12학년 학생들은 사이버보안 및 사이버 포렌식에 대한 토론에서 전문가들과 만나 실제 실습과 경연에 참가했다.

Middle Georgia State University는 40명의 고등학생을 대상으로 2017년 6월 13일부터 14일까지 IT 여름 캠프를 주최했다. 주제에는 사이버보안,

로봇 공학, 게임 디자인 및 모바일 애플리케이션 개발이 포함되었다.

Trident 공과대학은 2017년 4월 제5회 Palmetto Cyber Defense Competition와 제2회 연례 Palmetto Digital Cyber Forensics Competition을 지원했다. 이 행사는 Armed Forces Communications and Electronics Association(AFCEA)와 SPAWAR SSC Atlantic가 공동 후원하였다. 2017년 7월, Trident는 중학교 여학생들을 위한 사이버 및 STEM 관련한 행사인 제4회 "Girls Day Out"을 후원했다.

Microsoft, FBI, Abagnale & Associates, FireEye, Cisco, PhishMe, Dell Secure Works, Lockfale, Wells Fargo 및 Bank of America와 같은 기업들의 개인 및 공공부문 조직들의 협력을 통해 2017년 7월1일 마이크로소프트의 Charlotte 캠퍼스에서 30명의 고등학생을 위한 2017년 InfraGard 여름 캠프를 개최하였다.

3.2.6 ATE 프로그램 비교 분석

ATE 5개 프로그램 별로 세부내용을 살펴볼 때 사이버경진대회, 온라인 교육·훈련 콘텐츠, 멤버십 및 참여 기관, 학위 및 인증 프로그램, 모임 및 행사, 경력 경로, 교수 양성 등이 비교항목으로 가능하므로, 이 항목들을 기준으로 비교하여 그 결과를 분석하고자 한다.

CSSIA는 2006년부터 CCDC를 개최하여 운영하고 있으며 CVDC를 통해 온라인 교육 및 사이버 경진대회를 운영하고 있다. 또한 온라인으로 CSSIA's Learning Video Channel을 운영하고 있으며 2017년 CSSIA 가상 교육 및 학습 환경은 250개 교육 기관에서 채택하고 있다. 2004년부터 CSSIA는 사이버보안 관련 분야에서 4,000명 이상의 교사와 대학 교수진을 양성하여 왔다.

CSEC은 8개주 43개 기관이 협력하여 운영되고 있다. 또한 학위 및 인증 프로그램 수행 결과 2004년 이래 준학사는 1,442명, 학사는 360명, CNSS 인증서 2,236개를 발행하였다. 또한 중요한 행사로 Industrial Controls Security(ICS) Summit을 개최하고 있다.

NCC는 많은 기관들이 참여하는 사이버경진대회인 NCL을 2011년 시작하여 수천명 학생 및 교수진

NCL에 참가하여 왔다. NCC는 Jones & Bartlett Learning과 함께 일련의 전자서적을 제작하여 지원 협력기관에 지원하였으며 Complete Cloud 기반 랩 솔루션을 통해 온라인 콘텐츠를 지원하였다. 웨비나 시리즈 개발 및 운영을 통해 온라인으로 콘텐츠를 포함하여 200개 이상의 파트너 기관들에게 제공하고 있다. 준학사 및 학사학위 프로그램도 운영하고 있다. NCC 지원 모임으로 NCSA를 운영하고 있고 Community College Cyber Summit(3CS)는 2014년부터 운영 중이며 400명

이상의 2년제 대학 교육자가 참여하고 있다.

CWW 참여기관들은 NCL에 적극적으로 참여하고 있으며, 대학생을 위한 경진대회 WRCCDC, PRCCDC, NCL과 고등학생을 위한 CyberPatriot를 지원하고 있다. 11개 기업 파트너십을 맺고 있으며 Cyber Risk Summits, CyberGirlz 및 Girls Go Tech, CyberPatriot Coaching Academy, GenCyber Camps, Open Source Intelligence Workshop를 운영하고 있다. 교수진 양성을 위한 FGP와 FPDT를 운영 중이다.

ACE 컨소시엄은 2013년부터 사이버 캠프를 운영 중에 있으며, 2017년 ACE 컨소시엄은 4개 주, 멤버 15개 기관이 지정되어 있다. ACE에서 지원하는 행사들은 Train-the-Trainer 워크숍, IT 여름 캠프, Academic Cybersecurity Conference, Palmetto Cyber Defense Competition & Palmetto Digital Cyber Forensics Competition, Girls Day Out, InfraGard Summer Camp를 지원한다. 2017년 현재 130개 강좌 및 5개 과정으로 확대되었다. ACE는 5개의 핵심 사이버포렌식 커리큘럼 과정에서 자격을 갖춘 강사에게 집중적인 실무교육을 제공한다.

Table 7.은 ATE 프로그램 5종간의 종합적인 비교결과를 보여주고 있다. ATE 프로그램을 종합적으로 평가하면 학생들 대상으로 사이버 경진대회 및 캠프 등을 적극 활성화하는 측면이 있다. 또한 여러 교육기관 및 기업 등과의 적극적인 협력을 통해서 학생들을 양성하는 방향성을 보여주고 있다. 그 특성들은 강사 육성 프로그램 추진, 파트너십을 통한 공동 교육·훈련 강화, 커리큘럼 개발 및 공동 활용, 온라인 프로그램 개발 및 지원, 기업의 협력 강화, 학생 대상 캠프 및 학생 대상 사이버경진대회, 인력양성 평가 체계 강화 등을 들 수 있다.

Table 7. Comparison of ATE Programs (① CSSIA, ② CSEC, ③ NCC, ④ CWW, ⑤ ACE)

Items	Comparison
Cyber Competitions	① o organize CCDC
	③ o organize NCL
	④ o Support College student competition(WRCCDC, PRCCDC, NCL) o Support high school student competition (CyberPatriot)
On-Line Contents	① o CVDC o Video Channel
	③ o e-Book o Cloud-based LAB Solution o WEBINAR Series
	④ 250 educational institutions ② 43 institutions ③ More than 200 partners ④ 11 Business Partnerships ⑤ 4 states, 15 members
Degree & Certification	① o Associate degree 1,442 o Bachelor's degree 360 o CNSS certificate 2,236
	② Associate, Bachelor Degree
Meetings & Events	② o ICS Summit
	③ o NCSA o 3CS
	④ o Cyber Risk Summits o CyberGirlz & Girls Go Tech o CyberPatriot Coaching Academy o GenCyber Camps o Open Source Intelligence Workshop
	⑤ o Train-the-Trainer Workshop o IT Summer Camp o Academic Cybersecurity Conference o Palmetto Cyber Defense Competition & Palmetto Digital Cyber Forensics Competition o Support Girls Day Out o InfraGard Summer Camp
	③ Model transfer pathways
Career Path	③ Model transfer pathways
Teacher training	④ FGP, FPDT
	⑤ 130 lessons and 5 courses

IV. 국내 사이버보안 인력양성 정부지원 프로그램과의 비교

4.1 국내 정부지원 프로그램 현황

4.1.1 정부지원 교육·훈련 현황

ATE 프로그램 5종과 유사한 국내 프로그램은 2017년 국가정보보호백서에서 확인할 수 있다. 이

백서에 의하면 독자적인 정보보호 전문인력양성 프로그램은 과학기술정보통신부와 한국인터넷진흥원이 함께 추진하는 4건, 고용노동부, 정보통신기술진흥센터(IITP), 한국정보기술연구원(KITRI), 한국교육학술정보원(KERIS)에서 1건씩 총 8건의 프로그램이 운영 중으로 다음과 같다[16].

- 과학기술정보통신부와 한국인터넷진흥원
 - 정보보호 특성화대학 지원사업(ISCU : Information Security characterized University)
 - 대학정보보호동아리(KUCIS : Korea University Clubs Information Security) 지원사업
 - 고용계약형 정보보호 석사과정 지원사업(ISMP : Information Security Master's Program)
 - 차세대 보안리더(BoB : Best of Best) 양성 프로그램
- 고용노동부
 - 최정에 사이버보안 인력 및 산업보안 전문인력 양성사업(K-Shield)
- 정보통신기술진흥센터(IITP)
 - 대학 IT연구센터(ITRC : Information Technology Research Center)
- 한국정보기술연구원(KITRI)
 - 국가기간·전략산업 직종훈련 과정
- 한국교육학술정보원(KERIS) 4개 권역
 - 정보보호형재교육원(IISEG : Institute of Information Security Education for the Gifted)

본 논문 연구와 관련된 데이터는 2017년 국가정보보호백서와 프로그램별로 개설된 홈페이지 및 사업 주관 기관의 홈페이지에 게시된 보고서 등을 참고하여 정리하였으므로 어느 정도 오차가 있을 수 있음을 가정한다. 추진 중인 사업의 성과로 대외 파급력 등을 고려한다면 홈페이지 개설은 가장 중요한 수단이므로 여기에 제공되는 데이터를 우선적으로 적용하여 연구할 수밖에 없는 국내 환경의 개선이 필요하다고 할 수 있다.

'정보보호 특성화대학 지원사업'은 2015년 고려대학교, 아주대학교, 서울여자대학교 3개 대학이 지정되었으며, 2016년 충북대학교가 추가되어 현재 4개 대학교에서 100여 명을 교육 중이다. 이 사업은 대학과 국내의 정보보호 관련기업, 해외대학 등으로 구성된 컨소시엄을 구성하여 운영되며, 컨소시엄 참여 기업과의 산학협력 프로젝트 수행 및 산학협력중점교수 활용 등이 필수적으로 포함되어 있어 산업현장의

우수 실무형 인재발굴·육성 사업으로 평가되고 있다. 또한, 신입생 선발과정에 있어서도 입시전형과 연계한 정보보호 특기자 전형 등을 도입하여 '정보보호 분야 수능걱정 없는 대학진학'에 기여하고 있다.

'대학정보보호동아리 지원사업'은 2006년부터 10인 이상으로 구성된 전국의 정보보호 동아리를 선정하여 정보보호 교육, 세미나, 자체 연구활동 등을 지원하라는 것을 골자로 2016년에는 국내 전문대학·대학교, 대학원에 소속된 47개 동아리(회원수 약 1,6000여 명)를 선정·지원하였다.

'고용계약형 지식정보보안 석사과정'은 정보보호 기술환경 변화에 신속히 대응할 수 있는 고급인력을 양성하고자 2009년부터 운영하고 있다. 2009년도 3개 대학을 시작으로 2016년 12개 대학으로 확대하여 지원하고 있다. 졸업생을 직접 채용할 기업이 학생의 선발부터 교육내용, 인턴십 근무 및 R&D 과제 등 모든 과정에 적극 참여하는 방식을 통해 실무 중심의 교육이 이루어진다. 학생의 경우 석사과정 2년간 등록금 전액을 지원받으며, 졸업 시 석사학위를 취득하는 동시에 컨소시엄 참여 기업에 취업하는 기회를 얻어 2년간 정보보호 실무에 재직하게 된다.

'차세대 보안리더 양성 프로그램'은 한국인터넷진흥원이 한국정보기술연구원과 함께 운영하고 있으며, 1기 60명, 2기 117명, 3기 122명, 4기 136명, 5기 135명 등 총 570명이 교육을 수료하였다.

제작자 대상의 '최정에 사이버보안 인력 및 산업보안 전문인력 양성사업'은 한국인터넷진흥원은 3.20 인터넷사고와 같은 국가 사이버위기 상황에 빠르게 대응하기 위한 전문인력 양성을 목적으로 최정에 사이버보안 인력양성을 2013년도부터 매년 추진 중에 있다. 이 사업은 2017년까지 최정에 사이버보안 인력 5,000명 양성을 목표로, 다각적 사이버 공격 대응이 가능한 취약점 및 악성코드 분석, 모의침투 등의 기술력을 보유할 수 있도록 설계되었다.

'정보보안 산업전문인력양성 사업'은 지난 2008년 지식정보보안산업 진흥을 위한 정보보호 중기 종합계획의 일환으로 지식정보보안 전문인력양성계획을 수립하여 현장 중심의 실무인재 양성과 더불어 관련 산업계 인력의 수급 문제를 개선하기 위해 시작되었다. 2014년부터 사업명이 '정보보안 산업전문인력 양성사업'으로 변경되었고 2016년에는 총 9개 교육 과정을 운영하여 1,212명의 수료생을 배출하였다

'융합보안 전문인력양성 교육'은 「K-ICT 융합보안 발전 전략(2016.5)」에서 ICT 융합산업의 확대

에 따라 수요가 급증하는 융합보안 전문인력의 수급을 위해 2020년까지 2천명의 융합보안 전문인력양성 계획을 밝힌 것에 의해 추진했다.

정부가 지원하는 정보보호 관련 연구프로그램으로는 과학기술정보통신부와 정보통신기술진흥센터가 추진하는 대학ICT연구센터(ITRC)가 있다. 2016년 현재 정보보호분야 ITRC는 송실대학교 스마트서비스보안연구센터, 중앙대학교 산업보안 연구센터, 순천향대학교 IoT보안연구센터, 충남대학교 핀테크보안연구센터 등이 있다. 2016년 기준 정보보호 관련 ITRC 대학별 참여인력은 고려대학교 제어시스템보안연구센터 232명, 순천향대학교 IoT보안연구센터 218명, 송실대학교 스마트보안연구센터 499명, 중앙대학교 산업보안연구센터 326명, 충남대학교 핀테크보안연구센터 98명으로 총 1,373명이다.

과학기술정보통신부와 고용노동부가 주관하고 한국정보기술연구원에서 운영하는 '중앙부처국가기간·전략산업 직종훈련 사업'은 정보보안 산업계로의 진출을 희망하는 미취업자를 대상으로 장기(3개월 이상) 전문기술교육을 통해 정보보안 산업계의 신입인력 배출을 목표로 운영되고 있다. 2016년에는 6개 과정에서 총 208명의 수료생을 배출하였으며, 정보보호 컨설팅 과정은 보안전문기업과의 연계를 통해 신입인력의 채용을 지원하고 있다.

2017 정보보호백서에서 다루지 않은 정보보호 인력양성 프로그램으로는 교육부가 지원하는 정보보호 영재교육원 사업이 있다[17]. 2013년 7월 국가정보원은 최정예사이버 전문인력(5,000명) 발굴·양성을 위하여 「국가사이버안보종합대책」을 발표하였다. 2014년 9월 정보보호영재교육원은 정보보호에 꿈과 재능이 뛰어난 중·고등학생을 대상으로 정보보호 관련 전문 교육과 정보윤리 교육 등을 통해 윤리의식을 겸비한 정보보호 우수인재로 발굴·양성하기 위한 목적으로 영재교육진흥법 제3조(국가 및 지방자치단체의 임무), 제8조(영재교육원의 설치·운영), 영재교육진흥법시행령 제21조(영재교육원의 설치)에 의거하여 교육부에 의해 설립되었다. 접근성을 고려하여 전국 4개 권역의 대학부설로 설치된 정보보호영재교육원의 권역은 제1권역(서울, 경기, 인천, 강원), 제2권역(충북, 충남, 대전, 세종), 제3권역(경북, 경남, 대구, 울산, 부산), 제4권역(전북, 전남, 광주)로 구분되며 제주도는 모든 권역에 지원가능하다.

정보보호영재교육원은 2월에 교육생을 선발하여 3월부터 11월까지 교육을 진행한다. 선발된 교육생은

학기 중 주말교육과 방학 중 집중교육을 포함하여 총 100 시간 이상의 교육을 받을 수 있다. 학기 중 주말교육은 격주 토요일마다 진행되며 각 권역 영재교육원의 특성에 맞춰 하루 5~6시간 교육이 진행되고 방학 중 집중교육은 여름방학 기간 중 일정 기간을 정해 3~4일 합숙교육을 통한 교육이 이뤄진다.

정보보호영재교육원의 교육과정은 중학생을 대상으로 하는 중등부(3개반), 고등학생을 대상으로 하는 고등부(3개반)로 구성되고 각 교육과정은 15명의 소수정원으로 운영되므로 총 90명의 교육생이 교육을 받을 수 있다. 전체 과정은 정보보호 이론, 정보보호 실습, 현장체험 등으로 구성된다.

4.1.2 캠프 등

여름캠프로는 정보보호영재교육원의 여름방학 집중 교육이 대표적으로 볼 수 있다. 각 권역 영재교육원의 특성에 맞춰 여름방학 기간 중 일정 기간을 정해 3~4일 합숙을 통한 교육이 이뤄진다. 2016년 방학 중 집중교육기간에는 4개 권역 정보보호영재교육원이 공통으로 국가보안기술연구소 산하 사이버안전훈련센터 위탁교육을 실시하기도 하였다. 위탁교육은 실제 사이버 환경에서 발생하는 사이버 위기 대응 훈련, 미션수행 통해 학생들에게 현장 실무능력 습득 기회를 제공하였다[17].

다른 프로그램의 경우에도 방학을 이용하여 집중 교육을 실시하는 경우도 있다. 서울여대는 정보보호 특성화대학 사업 전용 홈페이지(esec.swu.ac.kr/)를 개설하였으며 하계 및 동계 기간 중 기업보안 집중교육을 실시하고 있다고 밝히고 있다.

4.1.3 사이버경진대회 등

2017년 국가정보보호백서에 의하면 국내에서 행해지는 사이버 경진대회는 화이트햇 콘테스트(WITHCON, WhiteHat Contest, 2013년 시작), 해킹방어대회(HDCON, Hacking Defence CONtest, 2004년 시작), 코드게이트(CODEGATE, 2008년 시작), 시큐인사이드(SECUINSIDE, 2015년 시작)가 있다[15]. 이 대회들은 참가대상을 따로 분류하지 않고 진행되는 사이버경진대회로서 학생들 전용은 아니다.

반면에 정보보호영재교육원 대상의 정보보안경진대회는 교육부, 정보보호영재교육원협의회에서 주최

하고, 한국교육학술정보원에서 주관하는 대회로서 학생들이 자신의 실력을 확인하고 정보보안에 대한 학습의지 향상을 목적으로 한다. 정보보안경진대회는 2015년에 처음 실시되어 2016년 두 번째 대회를 개최하였고 4개 권역 정보보호영재교육원 교육생이 모두 참여하는 개인전과 권역별 선발된 학생들이 참여하는 단체전으로 이뤄져 있다. 4개 권역이 공통으로 개최하는 정보보안경진대회를 제외하고 도 각 권역별로 학생들이 권역내의 수준을 확인하고, 자신이 부족한 분야를 알 수 있도록 모의해킹 공격·방어 대회도 개최하고 있다[17].

Table 8. Comparing Similar Programs of 2 Countries

(Item 1) Laws and Directives based programs		
US	CSSIA	
	CSEC	SATA 1992
	NCC	NSPD-54/HSPD-23(CNCI, 2008)
	CWW	Federal Cybersecurity Workforce Assessment Act of 2015
	ACE	
KR	ISCU	N/A
	KUCIS	
	ISMP	
	BoB	
	IITRC	
IISEG		
(Item 2) Target workforces of program		
US	CSSIA	high school, college
	CSEC	college
	NCC	college
	CWW	middle & high school, college
	ACE	middle & high school, college
KR	ISCU	undergraduate
	KUCIS	undergraduate
	ISMP	graduate
	BoB	middle & high school, college
	IITRC	undergraduate
	IISEG	middle & high school
(Item 3) Online Contents and Systems		
US	CSSIA	CVDC, Video Channel
	CSEC	-
	NCC	e-Book, Cloud-based LAB Solution, WEBINAR Series
	CWW	-
	ACE	-
KR	ISCU	-
	KUCIS	-
	ISMP	-
	BoB	-
	IITRC	-
	IISEG	-

(Item 4) Teacher training		
US	CSSIA	-
	CSEC	-
	NCC	-
	CWW	FGP, FPDT
	ACE	130 lessons and 5 courses
KR	ISCU	-
	KUCIS	-
	ISMP	-
	BoB	-
	IITRC	-
	IISEG	-
(Item 5) Membership collaboration program		
US	CSSIA	o organize CCDC
	CSEC	o ICS Summit
	NCC	o organize NCL o organize NCSA o organize 3CS
	CWW	o support WRCCDC, PRCCDC, NCL, CyberPatriot o Cyber Risk Summits o CyberGirlz & Girls Go Tech o CyberPatriot Coaching Academy o GenCyber Camps o Open Source Intelligence Workshop
	ACE	o Train-the-Trainer Workshop o IT Summer Camp o Academic Cybersecurity Conference o Palmetto Cyber Defense Competition & Palmetto Digital Cyber Forensics Competition o Support Girls Day Out o InfraGard Summer Camp
	ISCU	o SWU : summer · winter camp, FTBSS(Fusion Technology Business Security Symposium)
	KUCIS	-
	ISMP	-
	BoB	-
	IITRC	-
IISEG	o summer camp	

4.2 미국 ATE 프로그램과의 비교

우리나라의 사이버보안 인력양성과 관련하여 추진 현황 및 문제점을 포괄적으로 지적한 내용으로 “김동우 외” 연구에서 찾아볼 수 있으며 다음과 같이 지적하고 있다[18].

- o 정보보호 교육 중장기 계획 부재
- o 교육 프로그램에 대한 검증 부족
- o 교육기관 간의 정보 교류 부재
- o 전문 강사 확보의 어려움
- o 일반인의 정보보호 인식 제고를 위한 교육 프로그램 부재

이와 같은 문제점을 개선하기 위해 다음과 같이 개선분야를 제시하고 있다.

- 정보보호교육 마스터플랜
- 정보보호 교육 프로그램 인증제도 도입
- 정보보호 전문 인력 DB 운영
- 정보보호 교재 개발
- 교육 이수생에 대한 다양한 혜택 개발
- 사이버보안 교육장 구축
- 정보보호 인프라 강화
- 일반인에 대한 정보보호 교육 확대
- 정보보호교육 총괄기관 설립

상기연구에서 국내 정보보호교육 문제점을 도출을 통해 개선분야를 구체적으로 제시하고 있으나, 기준에 대한 설정 근거가 미흡한 관계로 정책 수립 및 실천력을 확보하는 데는 어려움이 따를 것으로 보인다.

본 논문은 미국에서 추진 중인 정부지원 정책 중에서 ATE 사이버보안 분야 5종을 기반으로 수행되는 세부 내용을 도출하여 국내 정부지원 프로그램과 상호비교를 할 수 있는 사이버보안 인력양성 비교 프레임워크를 제안한다.

- (비교 1) 법·제도 연계 프로그램
- (비교 2) 신규인력(초·중·고 및 대학생) 전용 프로그램
- (비교 3) 온라인 교육·훈련 콘텐츠(전자서적, 웨비나, 실시간 교육훈련 시스템)
- (비교 4) 전문 교육자(교수·교사·트레이너) 육성
- (비교 5) 공동 참여 프로그램(캡프, 경진대회, 심층교육, 컨퍼런스 등)

신규 사이버보안 인력양성에 해당되는 우리나라 정부지원 프로그램은 다음과 같으며, 이 프로그램들을 기준으로 미국 ATE 프로그램과 비교한다.

- 정보보호 특성화대학 지원사업 : 대학생
- 대학정보보호동아리(KUCIS) 지원사업 : 대학생
- 고용계약형 정보보호 석사과정 지원사업 : 대학원생
- 차세대 보안리더(BoB) 양성 프로그램 : 혼합
- 대학 IT연구센터(ITRC) : 대학생
- 정보보호영재교육원 : 중·고생

최정에 사이버보안 인력 및 산업보안 전문인력 양성사업(K-Shield), 국가기간·전략산업 직종훈련

과정은 직무인력에 해당하므로 본 연구의 비교대상에서 제외한다.

Table 8.은 앞에서 선정한 5개 비교항목별로 미국 ATE 프로그램 5종과 유사한 국내 프로그램 6종을 상호 비교한 결과를 보여주며 세부 내용은 4.2.1 절부터 기술한다.

4.2.1 (비교 1) 법·제도 연계 프로그램

ATE 사이버보안 인력양성 프로그램 5종은 1992년부터 시작된 SATA 1992 법안을 근거로 미국 국가차원의 정책인 STEM 교육정책과 연동되어 체계적으로 추진되어 왔다. CSSIA(2003년), CSEC(2004년), NCC(2005년) 프로그램은 국토안보법(2002년)과 FISMA 2002 법안 발효와 때를 맞춰 사이버보안 인력양성을 위해 시작된 것으로 보인다. CWW(2011년), ACE(2012년) 프로그램은 CNCI 및 NICE 정책과 같은 식에 추진되는 등 미국 연방 정부는 사이버보안 인력양성을 기존 프로그램, 법률, 정책 등에 연계하여 추진하고 있다.

미국은 법률을 근거로 국가차원의 사이버보안 인력양성 정책을 수립하여 세부 지원프로그램을 추진하는 반면에 국내 지원 프로그램은 관련부처 정책 중심으로 추진되고 있다. 우리나라도 사이버보안 인력양성에 대한 법률을 제정하거나 관련 내용을 유사 법률에 포함하여 정책적으로 강화해 나가는 전략이 필요한 시점이라고 생각된다.

4.2.2 (비교 2) 초·중·고·대학생 전용 과정

ATE 프로그램별로 학생 기준 교육 대상자를 구분하면 다음과 같다.

- CSSIA : 고등학교 및 대학교 대상 교육 과정 운영
- CSEC : 대학교 대상 교육 과정 운영
- NCC : 대학교 대상 교육 과정 운영
- CWW : K-12(초·중·고) 및 대학교 대상 교육 과정 운영
- ACE : K-12 및 대학교 대상 교육 과정 운영

5종의 모든 프로그램은 대학생 전문 교육과정을 운영하고 있으며, 고등학교 대상교육과정은 3종 프로그램에서 운영 중이다. CWW, ACE는 K-12(초·중·고) 대상 교육과정을 운영 중이다.

우리나라 프로그램은 대학생 대상 프로그램은 3종, 대학원생 대상은 1종, 중·고생 대상은 1종, 모든 인력이 참여하는 프로그램 1종으로 구성된다. 대학생 이상을 대상으로 운영되는 프로그램이 대부분이므로 고등학생 이하 대상의 지원 프로그램이 부족한 상황이다.

4.2.3 (비교 3) 온라인 교육·훈련 콘텐츠

ATE 프로그램 5종 모두 커리큘럼 개발 및 보급은 모두 공통적으로 수행하는 내용으로 인력양성 프로그램에서 가장 중요한 역할을 담당한다.

교육·훈련 과정 참여를 원격에서 가능하도록 온라인 가상화 교육·훈련 시스템도 중요한 콘텐츠이며 CSSIA의 CVDC와 NCC의 Complete Cloud-based LAB Solution 2종이 운영 중이다.

NCC는 이외에도 전자 책(e-Books)과 웨비나를 개발하여 운영 중에 있다.

국내 6종 프로그램에서는 전문교육에 필요한 커리큘럼을 자체적으로 개발하여 운영 중이며, 다른 학교나 기관 등에게 배포하거나 제공하는 협력체계는 부족한 상황이다. 또한 국내 프로그램에서 온라인 교육·훈련 시스템, 전자책, 웨비나 등을 개발하는 등의 세부적이고 전문적인 교육·훈련 콘텐츠에 대한 내용은 부족한 측면이 있다.

4.2.4 (비교 4) 전문 교육자(교수·교사) 육성

CSSIA는 교사와 교수 육성 프로그램을 통해 2004년부터 2012년까지 사이버보안 관련 분야에서 2000명 이상의 교사와 대학 교수진을 육성하였다.

ACE 컨소시엄에서는 2015년의 경우 ACE 학습관리 시스템에는 25개 주에 걸쳐 58개 기관의 110명의 교육자가 등록되어 있었다. 2017년 현재 130개의 강좌 및 5개 과정으로 확대되었다.

국내 프로그램들은 학생대상의 인력양성에만 맞추어져 있으며, 이 학생들을 가르치는 전문 교육자에 대한 육성 과정을 설계하고 운영하는 프로그램 확충에 대해서는 매우 미흡한 상황이다.

4.2.5 (비교 5) 공동 참여 프로그램(캠프, 경진대회)

사이버경진대회는 CSSIA가 운영하는 CCDC와 CWW가 운영하는 ICCDI(International

Collegiate Cyber Defense Invitational) 대회 2종이 있다. 또한 CWW는 대학생 대한 경진대회 WRCCDC, PRCCDC, NCL과 고등학생 대상인 CyberPatriot 대회를 지원하고 있다.

또한 학생들이 직접 참여하는 캠프도 다양하게 운영되고 있다. CWW는 GenCyber Camps를 운영하고 있으며 ACE는 가장 다양한 캠프를 운영 및 지원하고 있다. 고등학생 대상의 Cyber Camp, 30명의 9학년~12학년 학생들 대상의 2일 IT 여름 캠프, 5~12학년 100여명 참석의 5일 Palmetto Cyber Security Summer Camp, 중학교 여학생들을 위한 Girls Day Out, 고등학생을 위한 InfraGard 여름 캠프 등이 운영된다.

국내 프로그램 중 유일하게 정보보호영재교육원이 4개 권역을 대표하는 학생들이 참여하는 정보보안경진대회가 유일하다.

캠프의 경우에도 정보보호영재교육원의 방학 중 집중 교육이 대표적이며 국내 정부지원 프로그램을 수행 중인 학교별로 방학 중 국내·외 연수, 교환학생 등의 자체 프로그램을 운영하기도 한다.

4.3 국내 사이버보안 인력양성 정책 제언

4.3.1 ATE 기반의 국내 신규 사이버보안 인력양성 정책 제언

ATE 기반의 사이버보안 신규 인력양성 프로그램과 우리나라의 정부지원 신규 인력양성과 비교해 볼 때 우리나라의 부족한 점이 결국 개선사항이 된다. (비교 1)의 경우 ATE 프로그램은 미국 교육정책인 STEM을 기반으로 추진되어 오다, 2012년 수립된 NICE 추진전략에 의거 NICE 체계와 협력관계를 맺어 포괄적으로 추진되는 프로그램이다. 이와 같이 국내 지원 프로그램도 국가차원의 교육 정책과 연계하는 것이 필요하며 미국 OMB(Office of Management and Budget)와 같이 예산권을 행사하는 강력한 컨트롤타워를 통해 별도 사이버보안 인력양성 정책을 수립해야 한다.

우리나라의 신규 인력양성 프로그램의 경우 주로 대학생 이상에 초점을 맞추고 있다. 미국 ATE 프로그램은 초·중·고 학생 대상의 프로그램도 다양하게 운영하고 있다. 이는 사이버윤리 등의 기본 소양부터 시작하는 사이버보안 교육의 중요성을 인식하고 교육에 적용하는 것으로 우리나라의 인력양성 프로그램에

서도 반드시 적용해야 할 것으로 생각된다.

미국은 전자서적, 웨비나, 실시간 온라인 교육·훈련 시스템 등 교육·훈련 콘텐츠 개발 및 보급에 큰 비중을 두고 있다. 우리나라는 이와 같은 특성을 면밀히 검토하여 효율적인 커리큘럼 개발과 각종 콘텐츠 개발에 대한 연구·개발을 적극적으로 추진할 수 있는 투자가 절실한 상황이다.

(비교 4)에서 보듯이 미국 정부는 교수, 교사, 강사 등 전문 교육자 육성을 매우 중요하게 생각하고 있는 반면에 국내의 경우에는 거의 확인할 수 없는 정책이다. 인력 육성에는 교육자의 수준이 매우 중요한 일반적인 개념에도 국내에서는 이 분야를 소홀히 여기는 것 같다. 현재 추진되는 지원사업의 경우에도 추진 성과가 만족스럽지 못한 원인을 이 문제점에서 찾을 수 있지 않을까 판단된다. 이제라도 사이버보안 교육자의 수준제고 및 확대를 위한 노력이 시급하므로 이에 대한 투자가 절실하다고 할 수 있다.

(비교 5)에서 보듯이 학생들이 몸소 체험할 수 있는 공동 참여 프로그램인 캠프, 경진대회, 심층교육 등이 많이 운영되고 있다. 우리나라는 이에 대한 대책이 매우 미흡하므로 이에 대한 관심과 투자가 필요하다.

4.3.2 국내 신규 사이버보안 인력양성 포괄적인 정책 방향 제언

미국의 사이버보안 인력양성을 위한 추진체계에 대한 포괄적인 검토를 통해 국가차원의 정책 방향을 크게 3가지 범주로 나누어 검토해 볼 수 있다.

- (범주 1) 사이버보안 인력양성 법안(Act)
- (범주 2) 사이버보안 인력양성 정책(Initiatives)
- (범주 3) 사이버보안 인력양성 지원(Support)

첫 번째 범주는 강력한 법률 제정을 통해 국가차원의 사이버보안 인력양성을 추진할 수 있는 법적 근거를 마련하는 것이다.

국내의 경우 정보보호에 관련된 법은 시대적인 요구사항에 따라 단편적으로 제정되어 온 측면이 있다. 2017년 국가정보보호정책에 의하면 다음과 같이 5가지 분야로 구분하여 설명하고 있다[16].

- (분야 1) 정보통신망 및 정보시스템의 안전한 이용
- (분야 2) 침해행위의 처벌

- (분야 3) 국가기밀보호 및 중요 정보 국외유출 방지
- (분야 4) 정보보호 여건 구축
- (분야 5) 개인정보보호

미국은 2015년 연방사이버보안인력평가법에서 사이버보안 인력양성을 의무화한 단일법으로 제정되었다는 것은 우리나라에 시사하는 바가 매우 크다고 할 수 있다. 국가차원의 정책 수립 및 실천에 있어 관련 법은 매우 중요하므로 하루속히 사이버보안 인력양성 및 강화할 수 있도록 노력을 해야 할 것이다.

두 번째 범주는 인력양성 정책으로 미국은 CNCI를 기반으로 NICE를 수립하여 국가 사이버보안 인력양성을 위해 일관된 목표를 달성할 수 있는 추진체계를 운영하고 있다. 빠른 시간 내에 우리나라도 법률을 기반으로 강력하고 실천적인 사이버보안 인력양성 정책을 수립하여 1년 단위의 정기적 평가를 반복하여 지속적인 성과를 측정하고 잘못된 점을 고쳐 나갈 수 있도록 노력해야 한다.

세 번째 범주는 인력양성 지원 프로그램 강화로서 미국 NIST가 주관하는 제휴 프로그램(Affiliated Programs) 12종, 예산 지원 프로젝트(Funded Projects) 8종 등 20종 이상이 운영 중이다. 우리나라는 기껏 신규 인력양성은 6개 정도로 매우 미미한 실정이다. 법적근거 및 정책 등과의 연계도 매우 느슨하여 인력양성의 효과 제고에도 한계가 있을 수밖에 없다.

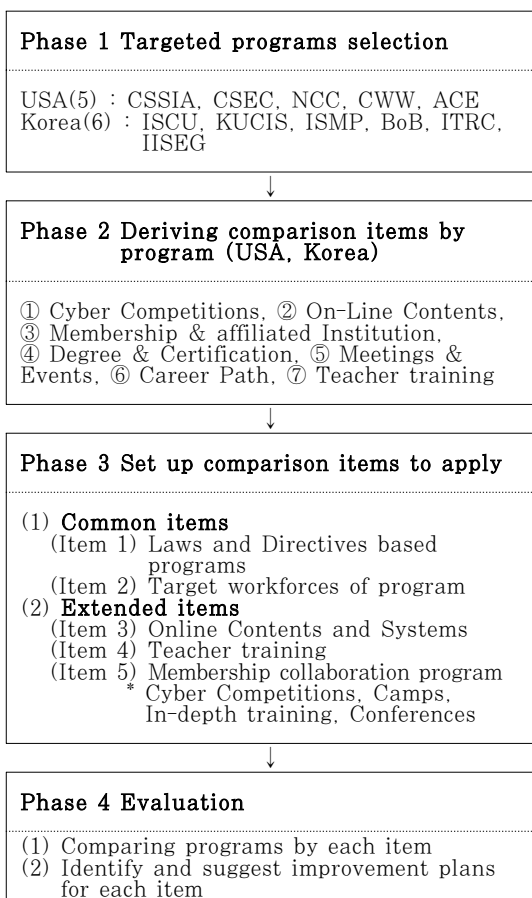
우리나라 사이버보안 신규 인력양성을 위해서는 다음과 같은 방향으로 법, 정책, 지원을 강화해 나가야 한다.

- 사이버보안 인력양성 법안 강화 및 제정
- 국가 교육정책과 연계한 인력양성 정책 수립 및 추진
- 사이버보안 인력양성 지원 프로그램 체계 개선

4.4 실용적인 사이버보안 인력양성 정책 비교·평가 프레임워크

사이버보안 인력양성 정책의 실질적인 결과를 보기 위해서는 많은 시간이 요구되며 이에 대한 측정 및 평가에 대한 연구가 미흡하다. 본 논문은 10년 이상 일관성 있게 추진되어 온 미국 ATE 프로그램 5종을 기준으로 국내 유사 프로그램 6종과 비교하여 국내 프로그램의 발전 방향을 식별하고자 하였다. 이와 같은 절차를 방법론적인 시각으로 새로운 방법론

Table 9. Cybersecurity Workforce Policy Comparison and Evaluation Framework Draft



을 제안하고자 한다.

Table 9.은 인력양성 프로그램 비교 평가 프레임워크로서 앞에서 비교 분석한 결과를 도식적으로 정리한 방법론으로서 제안하고자 한다.

첫 번째 단계는 비교 하고자 하는 인력양성 프로그램 선정 단계로서, 미국은 ATE 프로그램 5종을, 우리나라는 유사한 프로그램 6종을 선정하였다.

두 번째 단계는 ATE 프로그램과 비교할 수 있는 국내 프로그램을 찾아본 결과 4.1절에서는 정부지원 프로그램 전체를 검토 후, 4.2절에서 신규 인력양성 프로그램 6종을 선정하였다.

세 번째는 상호 비교할 항목 5종을 선정하였다. 네 번째 단계는 이 비교항목을 기준으로 미국과 한국의 프로그램을 비교 평가하여 4.3절에서 기술된 개선방안을 제안하는 방식으로 본 연구를 진행 하였다.

현재는 NICE 협력 및 지원 프로그램 20여종 중

ATE 관련 5종을 제한적으로 적용하였으나 상기 비교평가 방식을 기반으로 분석한다면 보다 효과적이고 실증적인 개선방안을 도출 할 수 있을 것으로 생각된다. 이와 같은 비교평가 방식을 “사이버보안 인력정책 비교·평가 프레임워크”로 제안하며 향후 추가 연구에서 이 방법론을 보다 실증적으로 증명하여 개선할 수 있을 것으로 예상된다.

V. 결 론

자율주행자동차, 무인기, 로봇 등 IT 발전에 따라 사이버위협은 더욱 정교해지고 그 피해는 사람의 생명을 위태롭게 할 수 있기 때문에 사이버보안의 중요한 요소인 인력양성은 더욱 중요해지고 있다. 전 세계적으로 선진국들은 기술개발 추진과 함께 사이버보안 인력양성에 힘쓰고 있다.

미국의 NICE 정책은 사이버보안 인력양성을 가장 체계적으로 추진하고 있다고 평가받고 있다. 사이버보안 인력의 경우에도 신규인력과 직무인력으로 구분하여 효과적인 지원정책을 추진하고 있다. 본 연구에서는 신규 인력양성 관점에서 NICE가 지원하는 20여종 이상의 사이버보안 인력양성 프로그램 중 가장 역사가 깊은 NSF가 지원해오고 NICE와 협력을 하고 있는 ATE 프로그램 5종을 비교 대상 프로그램으로 선정하였다. 국내의 경우 정부지원 프로그램 중 ATE 프로그램과 유사한 신규인력 양성 프로그램 6종을 선정하여 비교하여 우리나라 사이버보안 신규인력 양성 프로그램의 문제점을 식별하여 개선방안을 도출하였다.

Table 10.은 미국과 우리나라의 사이버보안 인력양성에 대한 독립적인 법, 정책, 지원 프로그램에 대한 전반적인 수준을 비교한 포괄적인 비교표이다. 법에 있어서 미국은 “Computer Security Act of 1987”, “Homeland Security Act of 2002”, “Cyber Security Research and Development Act of 2002”, Federal Information Security

Table 10. Comprehensive comparison of cyber security workforce development laws, policies and programs in the U.S. and Korea

Items	U.S.	Korea
Legislation	High	N/A
Initiatives & Strategies	High	Low
Support Programs	High	Moderate

Management of 2002 등에서 사이버보안 직무인력에 대한 교육 및 훈련을 의무화하였으며 “Cybersecurity Workforce Assessment Act of 2014”, “Federal Cybersecurity Workforce Assessment Act of 2015”과 같은 신규 인력양성을 의무화한 법을 제정하기에 이르렀다. 이에 비해 우리나라의 경우 비교할 수 있는 법률이 거의 없는 실정인데, 미국 하원이 2015년부터 사이버보안 인력양성을 위한 법안인 “Cyber Security Education and Federal Workforce Enhancement Act”가 지속적으로 발의하고 있는 상황은 우리에게 시사하는 바가 크다고 할 수 있다[19].

인력양성 정책의 경우에도 독자적으로 제안된 정책에 대해서만 비교한다면 국내의 경우 매우 미흡하지 않을까 생각되는 부분이다. 국가차원의 정책은 정권이 바뀔 때 특정 부처 중심으로 발표되는 계획의 일부로 포함되는 상황이 반복되어 왔다. 이제 우리나라도 사이버보안 인력양성 정책을 장기적이고 지속적으로 추진할 수 있는 체계가 요구된다고 할 수 있다.

인력양성 지원 프로그램의 경우에는 법, 정책에 비교해서 양적인 면은 비교가 가능한 정도이며 앞에서 미국 ATE 프로그램과 비교한 결과와 제안된 발전방향을 결합하여 개선한다면 상대적으로 가지적인 성과를 얻을 수 있는 가능성이 높은 분야이다.

본 연구에서 인력양성 정책에 대한 비교 평가를 위해 추진하는 방법론을 “실용적인 사이버보안 인력양성 정책 비교·평가 프레임워크”로 제안하였으며, 이는 지속적인 연구의 분석 틀로 활용할 수 있을 것으로 예상된다. 향후 연구는 NICE의 신규 인력양성 프로그램을 추가하여 국내 프로그램의 개선사항을 추가로 식별하여 국내 법·제도의 개선방안과 효과적인 사이버보안 신규 인력양성 정책을 설계하여 제안할 수 있을 것으로 기대한다.

References

- [1] Computer Security Act of 1987, Public Law No. 100-235 (H.R.145), Jan. 8, 1988.
- [2] Homeland Security Act of 2002, Public Law No. 107 - 296 (H.R.5005), Nov. 25, 2002.
- [3] E-Government Act of 2002, Public Law No. 107-347 (H.R.2458), Dec. 17, 2002.
- [4] The White House, “Cybersecurity Policy(NSPD-54/HSPD-23),” Jan. 8, 2008.
- [5] NIST, “National Initiative for Cybersecurity Education(NICE) Strategic Plan”, Apr. 2012.
- [6] Cybersecurity Workforce Assessment Act, Public Law 113-246 (H.R.2952), Dec. 18, 2014.
- [7] Consolidated Appropriations Act, Public Law 114-113 (H.R.2029), Dec. 18, 2015.
- [8] DHS, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” 2009.
- [9] Cristin Flynn Goodwin & J. Paul Nicholas, “Developing a National Strategy for Cybersecurity”, Oct. 2013.
- [10] NIST, “NICE Cybersecurity Workforce Framework,” NIST SP 800-181, Aug. 2017.
- [11] NIST, NICE eNewsletter 2016 Spring ~ 2017 Winter, 2017.
- [12] NCSA, “National Cybersecurity Student Association 2016 - 2017 Annual Report”, 2017.
- [13] Internet Scout Research Group, “ATE@20: Two Decades of Advancing Technological Education,” 2013.
- [14] Scientific and Advanced Technology Act of 1992, Public Law 102-476 (S.1146), Oct. 23, 1992.
- [15] ATE Centers, “Impact Partners with Industry for a New American Workforce 2016-2017,” 2016.
- [16] National Intelligence Service, Ministry of Science and ICT, Korea Communications Commission, Ministry of the Interior and Safety, Financial Services Commission, “2017 National Information Security White Paper,”

- Apr. 2017.
- [17] Bo-Ram Yun, "Analysis and Improvement of the Institute of Information Security Education for the Gifted", Master Thesis, Kongju National University, Feb. 2017.
- [18] Dong-woo Kim, Seung-woan Chai, Jae-cheol Ryou, "A Study on Domestic Information Security Education System", Journal of the Korea Institute of Information Security and Cryptology, 23(3), pp. 545-559, Jun. 2013.
- [19] Cyber Security Education and Federal Workforce Enhancement Act, Introduced in House (H.R.1981), Apr. 25, 2017.

〈저자소개〉

홍 순 좌 (Soonjwa Hong) 정회원
 1989년 2월: 숭실대학교 전산과 졸업
 1991년 2월: 숭실대학교 전산과 석사
 2005년 8월: 충남대학교 컴퓨터학과 박사
 1991년 2월~2000년 1월: 국방과학연구소(ADD) 선임연구원
 2000년 2월~현재: 한국전자통신연구원 부설연구소 책임연구원
 <관심분야>사이버보안 인력양성 정책, 미래 IT·보안기술, 사이버보안 기술·위협 분석, 국내외 정보보호 법·정책