사이버 안보를 위한 軍 정보보호 전문인력 양성방안

이 광 호* · 김 흥 택**

요 약

우리 군의 사이버 공간은 적으로부터 지속적인 위협을 받고 있다. 이 같은 사이버 위협에 대응하는 수단은 결국 軍 정보보호 전문인력이다. 하지만 현재 우리군의 고급 정보보호 전문인력은 소수에 불과하며 체계적인 양성계획은 미비한 상태이다. 따라서 본 논문에서는 세계 주요국인 미국, 영국, 이스라엘, 그리고 일본의 사이버 전문인력 양성정책을 조사하였다. 그리고 국내 정보보호 전문인력 양성정책을 조사하여 간략하게 제시하였다. 그리고 국방 사이버안보 전문인력 양성을 위해 4단계 전문인력 양성 및 중장기 계획 수립, 단계별 교육체계 정립, 인증제 도입을 제시하였다.

Measures for Training Military Information Security Professional Personnel for Cyber Security

Kwang-ho Lee* · Heung-Taek Kim**

ABSTRACT

The Cyberspace of the Republic of Korea Army is continuously threatened by enemies. Means for responding to such cyber threats are ultimately Military information security professional personnel. Currently, however, there are only a handful of advanced information security professional persons in Republic of Korea Army, and a lack of systematic training is inadequate. Therefore, in this thesis, we surveyed the information security professional human resource policies of USA, UK, Israel, and Japan. In addition, the policy to train professional human resources specialized in defense cyber security, we proposed training of specialist talent of 4 steps and medium and long term plan, step-by-step training system sizing, introduction of certification system.

Key words : Military information security, Cyber security, Information security professional personnel

접수일(2017년 5월 25일), 수정일(1차: 2017년 6월 26일), 게재확정일(2017년 6월 30일)

* 아주대학교 NCW학과
** 아주대학교 NCW학과(교신저자)

1. 서 론

2013년 5월 삼성 SDS 등 군 전술망 네트워크 체계와 전술지휘통제 자동화 체계 관련 기술을 가진 국내 방위산업체 두 곳의 전산 시스템이 북한 또는 중국으로 추정되는 세력으로부터 해킹을 당했다[1]. 2015년 8월에는 국방부 바이러스 백신 프로그램 공급업체 하우리가 북한으로 추정되는 외부로부터 해킹을 당했다[2]. 2015년 11월에는 2015 서울 국제 항공우주 및 방위산업전시회(ADEX)에 참가한 국내외 386개 방위산업체를 대상으로 악성코드를 심은 메일이 조직적으로 발송되었으며 2016년 9월에는 국방 전산망이 북한 추정 세력으로부터 해킹을 당하여 주요 군사자료가 유출된 것으로 판단하고 있다[3][4]. 2017년 5월 12일 전 세계 150여개 국가 20만대 이상의 컴퓨터를 감염시킨 워너크라이(Wanna Cry) 랜섬웨어(Ransomeware)의 배후도 북한으로 지목되고 있다[5]. 이와 같이 최근 들어 국방 분야에 대한 지능화 및 대규모화 되고 있는 사이버 공격은 단순히 기술적 수단만이 아닌 조직, 사람을 대상으로 사회공학적 공격과 함께 APT(Advanced Persistent Threat, 지능적 지속위협)공격유형으로 치밀한 계획 하에 조직적으로 발생되고 있다. 2016년 국방백서에 따르면 북한의 사이버전 인력은 약 6800명으로 추산되고 있다. 미국 워싱턴대 국제문제연구소의 평가에 따르면 북한 해커부대 전력은 미국 사이버사령부가 보유한 4900명보다 많으며 중국에서 활동하는 해커부대원만 600~1000명 수준인 것으로 추정하고 있다. 더욱이 최근 발표에 따르면 북한 정보기관인 정찰총국이 180부대라는 사이버 전쟁팀을 운영해 각종 사이버테러에 성공하고 있다[6]. 즉 북한에 의한 국방 사이버안보의 위협이 지속적으로 발생되고 있는 상태이다. 이에 비해 국내의 정보보호 인력은 2017년 수요 132,685명 대비 공급 110,236명으로 부족인력이 22,449명에 이를 것으로 한국인터넷진흥원 조사결과 전망되고 있다[7]. 또한 금융기관이나 민간부문의 고급 보안인력의 연봉은 1억~3억원 수준으로 군의 간부 또는 군무원들의 연봉보다 높은 수준을 유지하고 있다. 국방 분야의 정보보호 전문인력은 정보통신 분야에 근무하는 인력이 대부분이며 정보보호 분야에 특화된 전문인력은 소수에 불과하다. 하지만 이와 같은 현실에도 불구하고 중급이상의 전문인력에 대한 유인책은 현실적으로 미비한 실정이다[8]. 따라서 국방 사이버 안보를 위해서는 체계적인 정보보호 교육을 통해 군내에 중급 이상의 전문인력을 양성하는 장기적인 정책 마련이 필요하다. 본 연구에서는 주요국의 정보보호 전문인력 양성정책과 국내 및 군 정보보호 전문인력의 양성정책을 확인하고 군 정보보호 전문인력의 양성방안을 제시하고자 한다.

2. 주요국 정보보호 전문인력 양성정책

최근 전 세계적으로 정보보호에 대한 관심이 크게 증가하였으나 정보보호 업무를 효과적으로 수행할 수 있는 전문인력은 부족한 현실이다. 각국은 단편적 보안기술과 보호체계의 도입이 아닌 인력 양성에 대한 투자 확대의 필요성 증가에 따라 다양한 정책을 체계화하고 있다.

2.1 미국

미국은 2010년 4월 국가 사이버 보안 계획(National Initiative for Cybersecurity Education, NICE)을 발표하였다. 이것은 국가의 사이버 보안 수준 강화를 위한 정보보호 교육의 중요성에 따라 인력 양성에 역량을 집중하기 위한 것이다. 미국의 연방 사이버 보안 인력 양성은 2011년 국립표준기술연구소(National Institute of Standards and Technology, NIST)가 발표한 사이버 보안 인력 프레임워크(Cybersecurity Workforce Framework)로 더욱 체계화 하였다[9]. 사이버 보안과 관련된 업무 및 전문기술을 카테고리별로 분류하고 특정 업무마다 개인에게 요구되는 역량을 세밀히 분석함으로써 적재적소에 필요한 인재를 체계적으로 양성하고 있다.

2.2 영국

영국은 정보안보국 정보통신본부(Government Communications Headquater, CGHQ) 산하 정보보호 전문기관인 전자통신보안그룹(Communications-Electroics Security Groups, CESG)은 정보보호 전문인력에 대한 수요를 충족하기 위해 정보보호 전문가 인증제도를 시행 중에 있다. 전문가 인증제도는 정보보호와 관련된 직업들을 공식적으로 정의하고 각 직업별로 요구되는 기술 역량을 프레임워크 형태로 통일시켜 수치화함으로써 특정 인재의 역량을 직관적으로 판단할 수 있도록 기준을 제시하고 있다. 이를 통해 정부기관 및 기업을 위한 체계적인 인력양성 및 인재 수급 환경을 창출하는 것이 목적이다.

2 3 이스라엘

이스라엘은 자국 내 글로벌 IT 메이저 기업들이 정보보호 관련 업체에 대규모 투자에 나서는 상황을 이용하여 산업 육성 및 인력양성을 도모하는 전략을 수립하고 있다. 특히 선진기술원(Advanced Technology Park)이 이스라엘 국방부와도 연계되어 정보보호 기술 발전 및 인력 확대로 이어지는 결과를 달성할 것으로 기대하고 있다. 또한 총리실 소속 사이버국에서 이스라엘 대학의 정보보호 교육 지원, 사이버 국방 프로그램 정책 등을 추진하고 있다. 특히, 사이버 국방 인력 양성을 위한 '마그시밈 류미트(Magshimim Leumit)는 16～18세의 젊은 이스라엘 청소년을 대상으로 전문적인 정보보호 및 컴퓨팅 관련 교육 프로그램을 제공하고 차후 이스라엘 정보국인 모사드, 이스라엘 안보국 등에 취직 기회 등을 제공하여 공공분야 인력 공급을 창출하고 있다[11].

2.4 일본

일본은 IT관련 정책추진에 중심적 역할을 맡고 있는 정보처리추진기구를 중심으로 정보보호 역량 강화 사업을 추진 중에 있다. 정보처리추진기구는 정보보호 역량 강화를 위한 직업 역량 프레임워크(Common Career Skill Framework, CCSF)를 마련하여 IT 인재 육성에 있어 각각의 직업군을 체계화하고 특정 업무를 수행할 인재육성에 요구되는 기술 역량의 기준을 제시하기 위한 표준을 제시하고 있다[12].

2.5 북한

북한의 사이버 전문인력 양성과 관련된 계획이 대외로 발표되거나 공개된 것은 없다. 하지만 국내 언론에서 수집 및 발표된 자료에 따르면 해커로 양성될 어린 영재들이 평양의 과학영재학교인 금성 1,2중학교에서 컴퓨터 집중 교육을 받은 뒤 '미림대학'이라고 불리는 총참모본부 산하 지휘자동화대학이나 '223'연락소'라고 불리는 정찰총국 산하 모란봉대학에서 3～5년간 '사이버전사'로 양성되는 것으로 알려져 있다. 일부는 김일성종합대학 등에서 집중적으로 IT와 해킹 기술을 습득하며 컴퓨터 인재 양성을 위해 고등교육망 내에서 특정 국가로 매해 50～60명씩 유학을 보내고 있는 것으로 알려져 있다[13][14].

3. 국내 및 軍 정보보호 전문인력 양성정책

3.1 국내 정보보호 전문인력 양성 정책

2009년 공공 부문 정부기관 사이트를 대상으로 하는 DDoS 공격 등의 사고가 잇따라 발생됨에 따라 정부는 정보보호 산업과 인력의 중요성에 주목하고, 2013년 7월 정보보호 산업 발전 및 범국가 차원의 사이버위협 대응을 위한 국가 사이버안보 종합대책을 발표하였다. 이것은 청와대 중심의 사이버안보 컨트롤타워 구축과 사이버안보를 위한 최정예 정보보호 전문인력 양성 등의 전략 방향을 제시하고 있다. 특히 업계의 높은 인력 수요를 충족시키고 정보보호 산업을 선도할 인재 양성을 위해 2017년까지 최정예 정보보호 인력 5000명 양성을 목표로 설정하였다. 이를 위해 초·중·고 정보보호 영재를 발굴하고 관련 학과 및 대학원 연구 지원 확대를 통해 석·박사급 인력을 확보하며, 우수 인재를 위한 교육 프로그램, 기업 대상 최고위과정과 보안담당자 교육 등의 전문인력 양성책을 제시 및 계획하여 추진 중에 있다.

3.2 軍 정보보호 전문인력 양성 정책

軍의 정보보호 인력 구조는 장교, 부사관 군무원, 병사로 이루어져 있으며 군무원 및 병사 외에는 별도의 정보보호 특기와 전문인력 분류가 없다[15].

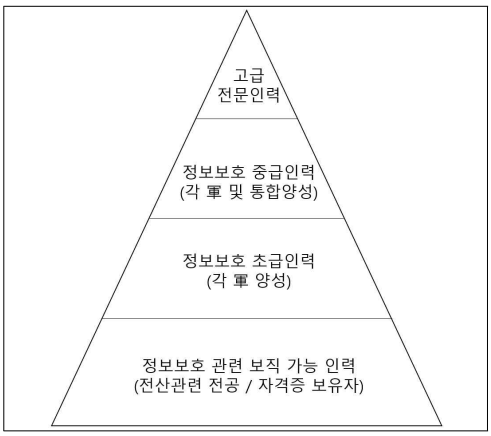
<표 1> 軍 정보보호 인력수급

계급	인력수급
장교	·정보보호병과 없음 ·단기장교의 경우 정보통신병과 장교 (전산장교) 중 전산 및 정보보호자격증 보유 인원 선발 ·2015년부터 고려대학교 사이버국방학과에서 매년 30명 양성
부사관	·정보보호병과 없음 ·고졸 / 전문대졸 이상 전산 및 정보보호 전공자 또는 자격증 보유자 중 선발
군무원	·전산 / 통신 / 정보보호직렬 공채선발 ·선발 시 자격증, 전공 등이 영향을 미침
병	·정보보호병 특기신설을 통해 선발

각 軍 교육사령부(정보통신학교)의 특기교육 과정에서 기초적인 정보보호 지식을 습득하며 부대 배치 후 국방부 예하의 교육기관을 통하여 별도의 단기 및 심화 과정을 거쳐 전문적인 정보보호 지식을 습득하고 있다.

4. 軍 정보보호 전문인력 양성방안

앞서 3장에서 살펴본 바와 같이 정보보호 전문인력 양성은 전 세계적인 추세임을 확인할 수 있으며 국내 역시 정보보호 전문인력 양성을 위한 계획을 수립하여 추진 중에 있음을 확인할 수 있다. 하지만 軍 정보보호 전문인력 양성을 위한 정책적 중장기적 계획 수립은 현재 다소 미비되어 있음을 확인할 수 있다. 본 장에서는 정보통신산업 진흥법 시행규칙 상의 기술 인력 자격기준이 초급, 중급, 고급, 특급으로 분류되어 있음을 참조하여 軍 정보보호 전문인력 양성을 (그림 1)과 같이 4단계로 제시하고 단계별 양성을 위한 중장기적 계획 수립, 각 기관별 정보보호 교육체계 정립, 인증제도 도입의 세 가지 방안으로 제시하고자 한다.



(그림 1) 軍 정보보호 전문인력 구조

4.1 중장기 정보보호 전문인력 양성계획 수립

현재 각 軍의 정보보호 인력은 대부분 정보통신 병과 및 직렬의 인원들로 구성되어 있으며 선발시 전공자 또는 자격증 보유자가 고려되나 인력 계획에 의거 비전공자도 선발되고 있다. 하지만 정보보호 관련 보직은 일부 계획 및 정책관련 부서를 제외하면 전문적 직무지식을 필요로 하기 때문에 비전공자는 직무에서 활용이 어렵다. 또한 단기적 순환보직이 규정된 군 인사정책에 따라 경력자의 지속적인 활용도 어려운 실정이다. 따라서 정보보호 관련 보직을 초급, 중급, 고급으로 분류하고 보직 가능한 인원을 별도의 그룹으로 관리하고 양성할 수 있는 중장기적 양성계획이 수립되어야 한다.

처음 정보보호 관련 직무에 보직된 인력은 초급인력으로 분류하고 그에 맞는 보직부여 및 직무관련 기초교육을 이수 후 즉시 활용하는 계획이 수립되어야 한다. 2~3년 이상 연속하여 정보보호 관련 직무에 보

직 시에는 중급 전문교육 이수와 함께 보다 전문성이 요구되는 보직을 순환하여 부여함으로써 중급인력으로 양성될 수 있어야 한다. 특히 각 군에서는 자체적으로 중급인력이 양성될 수 있도록 장기적인 계획 수립이 필요하다. 중급인력이 장기적으로 양성될시 현재 상급부대에 집중된 군의 정보보호 인력이 예하부대로 확산됨으로써 군의 전반적인 정보호호 수준이 향상될 것이다. 고급 전문인력 양성은 각 군에서 운영하고 있는 전문학위 위탁교육을 통해 국내외 유수대학에서 정보보호관련 연구와 석사이상의 학위를 받은 인력 및 고려대 사이버국방학과 인력, 전문사관 인력활용 계획 등을 통해 양성할 수 있다.

전문적인 교육을 통해 양성된 고급인력의 유입과 배치는 중급 이하 전문인력의 능력 및 수준이 향상될 수 있는 환경을 제공하여 군 정보보호 전문인력의 전반적인 수준이 향상될 수 있다. 따라서 이와 같은 단계적 전문인력의 양성과 배치, 활용에 대한 중장기적 계획 마련은 필수적이다.

4.2 각 기관별 정보보호 교육체계 정립

각 군의 정보보호 인력은 각 군 교육사령부 (정보통신학교)에 의해 기초교육이 이루어지고 있다. 또한 각 군에서는 국방부 예하 교육기관의 교육 프로그램을 통해 전문적인 교육을 받고 있으며 일부 대외 민간기관의 교육을 이용하기도 한다. 하지만 일부 교육은 기관 간 내용이 중복되거나 개인 또는 부대별 직무 수준이 고려되지 않고 있다. 따라서 각 군의 교육사령부는 각 군의 정보시스템 환경과 정보보호체계를 고려한 직무별 기초 교육을 단계적(초급, 중급 등)으로 시행함으로써 최초 보직자가 직무를 수행할 수 있는 여건을 제공하고 각 군 초급 인력이 양성할 수 있어야 한다. 인력 양성을 위한 과목은 공통과목, 필수과목, 전문 과목으로 나누고 단계별로 교육을 이수하도록 해야 하며, 공통 및 필수과목은 일반, 정책, 이론, 기술 과목으로 분류한다. 전문 과목은 기술 및 정책에 관련된 심화과정으로 인력의 인증 유형에 따라 이수하도록 한다. 또한 2~3년 이상 정보보호 관련 직책을 수행하는 인력에 대해서는 각 군 교육 외에도 대외 민간교육을 활용한 위탁교육, 국방부 예하 교육기관에서 제공하는 중급 이상의 통합교육을 통해 중급 전문인력이 양성될 수 있는 여건을 제공해야 한다. 고급 인력에 대한 교육은 전문학위 위탁교육, 대외기관 양성교육(BoB, K-Shield 등), 상급부대 전문가 교육 등을 활용하여 시행함으로써 각 군의 교육과 연계성과 차별성을 두도록 하는 교육체계와 구체적인 과목의 정립이 필요하다.

4.3 정보보호 전문인력 인증제도 도입

정보보호 전문인력 양성의 효과를 극대화하기 위해서는 각 단계별 교육이수를 통한 인증과 인력에 대한 인증이 병행되어야 한다. 교육이수를 통한 인증을 위해서는 앞서 제시한 바와 같이 교육간 차별성과 연계성이 검증되어야 한다. 또한 양질의 교육수준을 유지하기 위해 교육 프로그램을 검증하는 인증제도가 필요하다. 검증된 교육을 이수한 인원들에 대해서는 수준 측정 평가를 실시하고 평가에 합격한 인원에 대해서만 인증한다.

인력에 대한 인증은 교육 이수 후 수준측정과 직무경력 및 기간을 합산하여 전문인력으로 인증한다 그리고 이를 DB화하여 인증된 인력을 앞서 설명한 (그림 1)과 같이 지속 관리해야 한다. 군 정보보호 전문인력은 물리적 보안을 제외한 정책, 시스템운영, 사이버전 수행의 세가지 분야에 대한 분야별 인력 인증체계가 도입되어야 한다. 또한 각 분야별 초급, 중급, 고급 전문인력으로 구분하며 고급이상 전문인력에 대해서는 인증위원회를 구성하여 심의를 통해 인증한다.

5. 결 론

앞서 살펴본 바와 같이 우리 군의 사이버 안보환경은 적 세력으로 부터 집요하고 치밀하게 위협을 받아왔다. 하지만 이와 같은 위협에 대응할 수 있는 중급

이상의 전문인력은 소수에 불과하며 중장기적인 양성 방안도 미흡한 실정이다. 또한 사회적으로도 부족하고 높은 연봉을 받는 외부의 고급 전문인력을 군내로 유입할 수 있는 유인책도 미비한 실정이다. 군 정보보호 전문인력 양성을 위한 방안으로는 인력의 구조를 4단계로 나누어 관리하는 것과 함께 중장기적 정보보호 전문인력 양성 계획을 수립해야 한다. 전산 및 정보보호 관련 전공자들을 중심으로 직책 수행이 가능한 인력부터 초급, 중급, 고급 전문인력으로 분류하고 각 단계별 필요한 교육체계를 정립하여 양성 가능한 여건과 환경을 제공해야 한다. 그리고 각 단계별 전문인력을 평가하는 인증제도를 시행해야 한다.

사회의 기술 변화 속도는 시시각각 빠르게 진화하고 있으며 사이버 위협도 함께 진화하고 있다. 하지만 A.I 또는 빅데이터와 같은 최신 기술이 접목된 정보보호체계의 도입만으로는 대응에 한계가 있다. 결국 사이버 공간에서 위협의 주체는 사람이고 그것을 막는 것도 사람이기 때문이다. 또한 군의 특수한 환경은 사회의 정보시스템 및 정보보호 환경과는 다른 특성을 지니고 있으므로 군에 특화된 정보보호 전문인력의 양성이 중요하다. 직무에 맞는 교육여건 제공과 인증제도를 통해 군에 특화된 초급~중급 정보보호 전문인력을 양성하고 외부에서 전문적인 교육을 받은 고급 전문인력과 함께 직무를 수행함으로써 전반적으로 능력이 향상될 수 있는 환경과 여건을 제공해야 한다. 이를 통해 중장기적으로 국방 사이버 안보 전문인력이 양성된다면 군은 물론 국가와 사회에도 기여하게 될 것이다.

우리는 혁신에 성공한 적의 위협에 노출되어 있다. 혁신은 두마리의 말이 끄는 마차를 네마리의 말이 끌도록 하는 것이 아니라 자동차를 만드는 것이다. 국방 사이버안보 전문인력 양성은 사이버 공간에서 국민의 자유와 민주주의를 보호할 것이고 자스민 혁명과 같이 이 자유를 확산하는데 기여하게 될 것이다. 국방 사이버안보 전문인력 양성을 위한 혁신이 필요한 때이다.

참고문헌

[1] 중앙일보, http://news.joins.com/article/18631228 2015년 9월 10일

[2] 경향신문, http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201508120600025 2015년 8월 12일

[3] 한국일보, http://www.hankookilbo.com/v/2f84f7d377ec42f99c38bee8bf1e8cd4 2015년 11월 19일

[4] JTBC뉴스 http://news.jtbc.joins.com/article/article.aspx?news_id=NB11462936 2017년 5월 2일

[5] 허핑턴포스트코리아, http://www.huffingtonpost.kr/2017/05/16/-_n_16631008.html 2015년 5월 16일

[6] 이데일리 http://www.edaily.co.kr/news/NewsRead.edy?SCDJF31&DCD=A00603&newsid=02053286615931216 2017년 5월 21일

[7] 한국인터넷진흥원, 2014년 정보보호 인력수급 실태조사 및 분석전망 결과보고서, pp.47, 2014년 12월

[8] 지디넷코리아, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20121031165342 2012년 10월 31일

[9] NIST. (2010). National Initiative for Cybersecurty Education.

[10] http://www.slate.com/

[11] 한국인터넷진흥원, 주요국 사이버보안 인력 양성 정책분석, 2014년

[12] VOA, http://www.voakorea.com/a/3375411.html 2016년 6월 14일

[13] 임종인·권유중·장규현·백승조, “북한의 사이버 전력 현황과 한국의 국가적 대응전략” 국방정책연구, 29(4): 9-45, 2013.

[14] 2012 국방정보보호컨퍼런스, 국방 사이버 보안 인력 현황 및 양성, 이동훈

[15] 이대성·안영규·김민수, “북한의 사이버전 위협에 대한 분석과 전망”, 융합보안 논문지, 제16권 제5호, 2016.

[16] 전정훈, “국내 정보보호의 체계적인 교육을 위한 대학교육과정에 관한 연구”, 융합보안 논문지, 제16권 제4호, 2016.

[저 자 소 개]

이 광 호 (Kwang-ho Lee)
2007년 육군3사관학교 국방경제학 학사
2016년 연세대학교 정보보호학 석사
2017년 현재 아주대학교 NCW학과 박사재학
2015년 3월~2016년 2월 연세대학교 바른ICT연구소 연구원(석사과정)

email : loveney@naver.com

김 흥 택 (Heung-Taek Kim)
1981년 육군사관학교 전자공학 학사
1990년 US Naval Postgraduate School Master of Science(전산학 석사)
2000년 한국과학기술원 전산학 박사
현 재 아주대학교 NCW학과 교수

email : kkimht@hanmail.net