국방 정보보호 인력 양성 방안

박상서*, 최운호**
* 국가보안기술연구소
** 경기대학교, (주) 엔에스컨설팅

요 약

우리 군도 하루 속히 사이버전에 대비한 정보보호 요원들을 양성하여 우리 사이버 국토가 외국 사이버 전사들에 의한 경유지로 활용되는 것을 차단하고, 유사시 적절히 군을 보호할 수 있는 역량을 강화하여야 할 필요성이 절실해지고 있어서 향후 국방 정보보호 인력 양성을 위하여 고려되어야 할 사항들을 제시한다.

A Scheme of Training the MND Information Security Manpower

Sangseo Park*, Unho Choi*
* National Security Research Institute
** Kyonggi Univ.

ABSTRACT

As soon as possible, our military have to trainning the information security manpower for Cyber Warfare, it should be block the foreign infowarrior to go by way of other country from our system. An emergency, we can protect our military information system and this thesis provide checkpoint about how we consider about trainning the infowarrior for future war.

1. 서 론

최근의 전쟁 양상은 걸프전과 유고전에서 볼 수 있었듯이 정보전 공격이 항상 동반될 뿐 아니라, 전시 상황이 아니더라도 사이버 무기들은 매우 유용한 공격 수단으로 인식이 되고 있다. 특히, 미공군기와 중국 전투기간의 충돌 사건 이후 미국과 중국간에 발생한 사이버전은 전시뿐만 아니라, 평시, 위기시, 분쟁시에도 사이버 전 공격 수단이 얼마나 상대국에 피해를 발생시키고 심리적인 불안을 가중시킴으로써 상대국을 교란할 수 있는지 극명하게 보여준 바 있다.

이러한 상황을 지켜볼 때, 우리 군도 하루 속히 사이버전에 대비한 정보보호 요원들을 양성하여 우리 사이버 국토가 외국 사이버 전사들에 의한 경유지로 활용되는 것을 차단하고, 유사시 적절히 군을 보호할 수 있는 역량을 강화하여야 할 필요성이 절실해지고 있다. 특히, 최근 전쟁에서의 군 정보체계 보호 즉 사이버 방어는 전쟁의 승패 및 지속에 있어서 매우 중요한 역할을 담당할 뿐 아니라, 미국, 중국 등 군사 강대국에서는 정보전 공격 수단을 염두에 둔 작전계획을 준비하고 있는 것으로 알려지고 있어 우리 군도 이에 대비하기 위해서는 정예 정보보호 전문 요원들을 시급히 양성하여야 할 때이다. 본 논문에서는 이와 같은 국내외 현실을 직시하고, 향후 중장기적 관점에서 국방 정보보호 인력을 양성하기 위한 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 제2절에서는 국방 정보보호 인력을 양성하기 위한 범위와 목표를 설정하기 위하여 인력 양성 모델을 정립하였고, 제3절에서는 인력 확보, 외부 인력 활용, 그리고 교육 훈련이라는 세 가지 맥락에서의 국방 정보보호 인력 양성 방안을 제시하였다. 제4절에서는 향후 국방 정보보호 인력 양성을 위하여 고려되어야 할 사항들을 제시하고, 제5절에서는 본 논문의 결론을 제시한다.

2. 국방 정보보호 인력 양성 모델

국방 정보보호 인력을 양성하기 위해서는 정보보호 인력이 수행하여야 할 임무와 역할, 인력의 구성, 임무 수행 부서, 인력 수급 방법, 그리고 국방 정보보호 지원에 관련된 기관에 따라 종합적인 계획이 수립되어야 한다. 이와 같은 고려사항들을 감안하여 모델화한 국방 정보보호를 위한 인력 양성 모델은 (그림 1)과 같다.

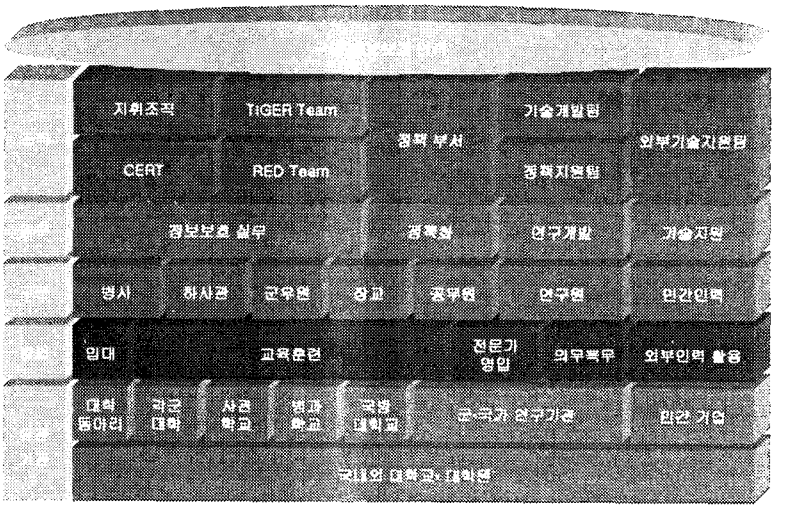
2.1 조직적 측면

국방 정보보호 인력이 배치되어야 할 조직은 다음과 같은 것이 있다.

- ○ 정책 부서: 국방부 및 각 군의 정보보호 정책을 담당할 정책 부서로서 각 군 본부의 지휘통신참모부와 국방부 국방전산정보관리소가 있다.
- ○ CERT: 1999년 12월 1일부로 창설된 군 CERT는 국방부, 기무사 및 각 군에서 정보보호에 관련된 사고 접수 및 처리 업무를 담당한다.
- ○ RED Team: 정보통신기반보호법의 제정 및 시행에 따라, 국방부 및 각 군의 주요 정보자산을 식별하고, 보호되어야 할 자산(운영체제, 시스템 소프트웨어, 응용 소프트웨어, 데이터, 데이터베이스, 정보통신망, 정보통신망 장비 등)의 취약성을 분석, 평가 및 점검하는 업무를 담당한다.
- ○ TIGER Team: 을지훈련 및 정보보호 훈련 등을 위한 임시 조직으로서 가상 적군의 역할을 수행한다.
- ○ 정책지원팀: 국방부 및 각 군의 정책 부서에서 정보보호 정책을 개발 및 제도화할 수 있도록 지원한다.
- ○ 기술개발팀: 국방부 및 각 군에서 필요로 하는 정보보호 기술을 개발하고 관련 체계를 구축한다.

○ 지휘조직: CERT, RED Team 및 TIGER 팀을 지휘하기 위한 조직으로서 합동참모본부와 각 군의 사령부(군사령부 및 작전사령부)에 둔다.

○ 외부기술지원팀: 민간의 전문가 조직 또는 업체로서 CERT, RED Team 및 TIGER team의 임무 수행에 필요한 민간 기술 및 인력 등을 지원한다.



(그림 1) 국방 정보보호 인력 양성 모델

2.2 임무 측면

국방 정보보호 인력이 해당 부서에서 수행하여야 할 임무에는 다음과 같은 것이 있다.

○ 정책화: 정책 부서에서 군 정보보호에 관련된 제도, 규정 등을 제정하며, 관련 기관 또는 조직에서 임무 수행에 필요한 예산을 반영한다.

○ 정보보호 실무: 지휘조직, CERT, RED Team 및 TIGER Team에서 군 정보보호를 위한 업무를 현장에서 수행한다.

○ 연구개발: 국방부 및 각 군의 정보보호 정책 수립을 위한 관련 제도와 정책 등을 연구하고, 실무에 활용할 도구와 기술을 개발하며 체계를 구축한다.

○ 기술지원: 국방부 및 각 군의 정보보호 실무 수행을 기술적으로 지원한다.

2.3 인력 범위 측면

국방 정보보호 인력은 다음과 같은 범위에 속한다.

○ 장교: 국방 정보보호 부서에서 근무하는 장교로서, 정보보호 실무와 정책 부서에서 정책화를 수행한다.

○ 하사관, 병사, 군무원: 국방 정보보호 실무 부서에서 근무하는 인력으로서 정보보호 실무를 담당한다.

○ 공무원: 국방 정보보호 정책 부서에서 근무하는 국가 공무원으로서 국방 및 각군 정보보호 정책을 수립/추진한다.

○ 연구원: 민관군 연구기관의 인력으로서 국방 정보보호 정책과 기술을 연구한다.

○ 민간인력: 민간 기업과 대학 등의 인력으로서 국방 정보보호 실무 수행에 필요한

기술을 지원한다.

2.4 인력 양성 방법 측면

인력을 양성하는 방법 측면에서는 다음 다섯 가지를 고려할 수 있다.

- ○ 교육 훈련: 국방 정보보호 교육 기관에서 교육을 통하여 배출한다.
- ○ 입대: 병사의 경우 입대 대상자 중 정보보호 능력 보유자를 선발/추천 등의 방법으로 확보한다.
- ○ 외부 전문가 영입: 민간 기업, 학교, 정부출연 연구기관, 타 정부부처 등에서 정보보호 전문가를 영입하여 정책 부서, 연구기관, 실무 부서 등에 배치한다.
- ○ 의무복무: 병역특례 연구 요원으로서 의무종사 기간동안 군 연구기관에서 정보보호 정책과 기술을 연구한다.
- ○ 외부 인력 활용: 민간 기업의 정보보호 인력을 국방 정보보호 취약성 분석, 사고처리 등에 활용하며, 타 정부부처(예: 경찰청 사이버테러 대응 센터 등) 또는 연구기관(한국정보보호 진흥원, 한국전자통신연구원, 국가보안기술연구소 등)과 공조체제를 구축함으로써 해당 기관의 전문 인력을 활용하여 정보보호 정책, 연구 및 실무에 투입한다.

2.5 인력 양성 유관 기관 측면

인력 양성에 관련된 기관으로는 다음과 같은 기관들이 있다.

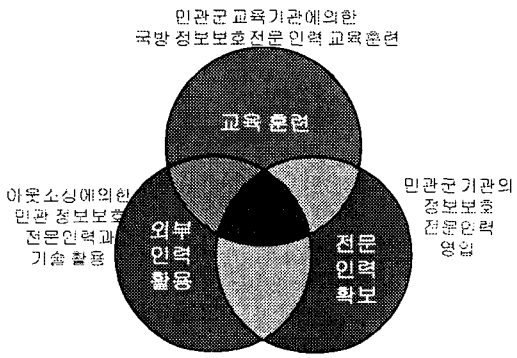
- ○ 대학 동아리: 각 대학교에서 활동하고 있는 해킹/정보보호 동아리로서 이 동아리 활동자들 중 입영 대상자에게는 국방 정보보호 관련 부서에서 근무할 수 있게 함으로써 해당 인력이 군에 복무하는 동안 민간의 인력과 기술을 활용할 수 있다.
- ○ 사관학교: 정보보호에 관련된 초급 장교를 육성하여 이들이 임관 후 정보보호 관련 부서에서 근무하도록 할 수 있으며, 전 사관생도들에게 정보보호 개념과 정보보호의 필요성을 교육함으로써 정보보호 마인드를 전군에 확산할 수 있다.
- ○ 각 군 대학: 영관급 장교들 중 정보보호 관련 업무 종사자들의 재교육 기회를 부여할 수 있고, 전 영관급 장교들에게 정보보호 마인드를 전파할 수 있다.
- ○ 국방대학교: 국방관리대학원, 안보대학원, 합동참모대학, 직무연수부 등에서 고위급 장교들에게 정보보호 마인드를 전파할 수 있으며, 재교육 차원의 실무 교육을 집중적으로 이수토록 함으로써 정보보호 실무자들을 양성할 수 있다.
- ○ 민간 대학교/대학원: 교수들을 통하여 정보보호 관련 연구를 수행하도록 함으로써 군에서 필요로 하는 기초 기술을 개발시킬 수 있으며, 정책화를 위한 조언을 받을 수 있다. 또한, 정보보호를 전공한 대학원생들을 군 연구기관에서 복무시킴으로써 정보보호 관련 연구를 활성화시킬 수 있다.
- ○ 군·국가 연구기관: 군 및 정부출연 연구기관들을 통하여 국방에 필요한 정보보호 기술과 정책을 지원받을 수 있고, 국방 정보보호 기술을 교육시키는 지정 교육기관으로도 활용할 수 있다.
- ○ 민간기업: 군에서 필요로 하는 실무차원의 민간 첨단/상용 기술과 인력을 지원받을 수 있으며, 민간 교육기관을 통하여 국방 정보보호 인력을 교육시킬 수도 있다.

3. 국방 정보보호 인력 양성 방안

3.1 기본 방향

국방 정보보호 인력을 양성하는 것은 (그림

2)에서 볼 수 있는 바와 같이 외부 인력을 국방 정보보호 인력으로 영입하는 인력 확보, 군 외부의 전문가들을 국방 정보보호에 활용하는 외부 인력 활용, 그리고 교육을 통하여 국방 정보보호 인력을 배출하는 교육 훈련의 세 가지 측면에서 추진되어야 한다.



(그림 2) 국방 정보보호 인력 양성 기본 방향

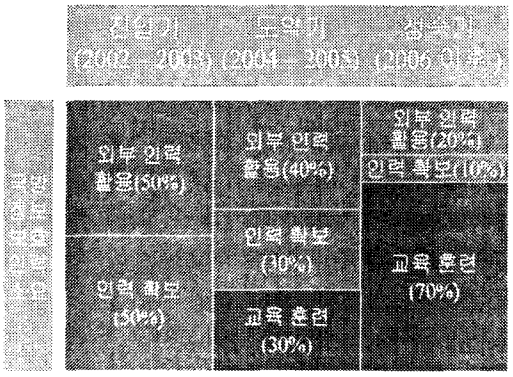
현재 군에는 정보보호에 관련된 인력이 절대적으로 부족하기 때문에, 우선적으로 민·관·군 각 기관의 정보보호 인력을 군 정보보호 인력으로 확보하여야 한다. 이를 위해서는 외부 인력의 영입과 함께, 군 내부에서 활동하는 정보보호 인력(장교, 하사관, 병사 등)을 적절하게 소집·배치함으로써 군의 전반적으로 정보보호 능력을 배가시키는 노력이 동반되어야 할 것이다.

두 번째로, 민관의 외부 인력을 적극 활용하기 위한 정책을 수립하여야 한다. 즉, 정보보호 업체, 민간 대학/대학원, 정부출연 연구기관(한국정보보호진흥원, 한국전자통신연구원, 국가보안기술연구소 등), 타 정부 부처(경찰청, 국가정보원 등) 등의 전문 능력과 기술을 활용하여 국방 정보보호 정책 및 기술을 개발함으로써 전체적인 국방 정보보호 능력을 향상시키자는 것이다.

세 번째로, 확보된 국방 정보보호 인력과 현재 국방 정보보호 업무에 종사하는 담당자 및 예정자에 대한 지속적인 교육 훈련이 수반되어야 하다. 궁극적으로, 국방 정보체계와 국방 정보통신망은 결국 군 정보보호 인력이 보호해야 할 것이므로, 중장기적으로 업무 담당자들에 대한 교육 훈련은 군 정보보호 인력 양성의 핵심이라 할 수 있다.

국방 정보보호 인력 양성 초기에는 최대한 외부 전문 인력을 영입하여 군 전문 인력으로 확보함과 동시에 외부 인력을 최대한 활용하여야 한다. 이는, 현재 군에는 정보보호 인력을 교육 훈련하기 위한 체제가 갖추어져 있지 않기 때문이며, 동시에 군 정보보호를 소홀히 할 수도 없기 때문이다. 교육 훈련에 의하여 국방 정보보호 인력이 배출되기 시작하면, 점차 인력 확보 및 외부 인력 활용을 통한 국방 정보보호 업무 수행은 그 비율이 감소되어야 한다. 따라서, (그림 2)에서 보이는 마일스톤과 같이 도약기와 성숙기에 들어서는 외부 인력 활용 비율과 인력 확보 비율을 줄이면서 군에서 배출되는 인력을 최대한 활용하는 방향으로 국방 정보보호 인력 양성이 추진되어야 할 것이다.

그러나, 국방 정보보호 성숙기에 들어선 이후에도 인력 확보와 외부 인력 활용은 그 비율을 축소하더라도 계속되어야 한다. 그 이유는 지속적인 인력 확보를 통한 기술 교류 및 도입을 활성화하고, 민간의 앞선 기술을 적극 활용할 필요가 있기 때문이다. 또한, 정보보호 전공자들을 병사, 장교 및 하사관 등으로 계속 받아들임으로써 군 정보보호 인력의 정체화와 기술적 낙후를 방지할 수 있으며, 어느 정도 공개가 가능한 부분에 대해서는 민간과 타 정부기관 및 정부 출연 연구기관의 기술력을 활용하여 체계의 구축이나 기술적 지원을 받을 필요가 있기 때문이다.



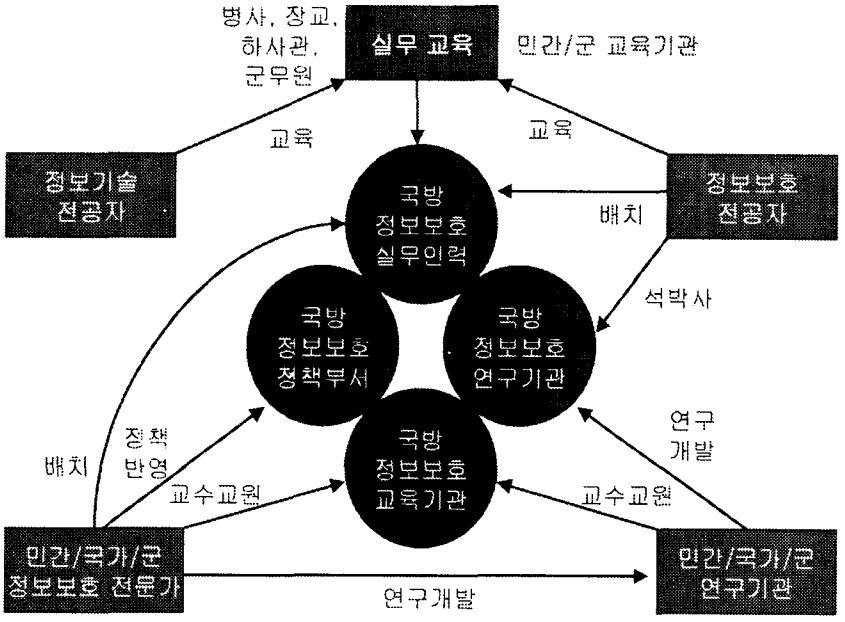
(그림 3) 국방 정보보호 인력 양성 마일스톤

3.2 국방 정보보호 인력 확보 방안

국방 정보보호 인력의 절대적으로 부족 문제를 해결하기 위해서는 외부의 정보보호 전문 인력을 국방 영역으로 흡수하여 정보보호 역량을 단기간 내에 끌어올려야 한다. 이를 위한 국방 정보보호 인력을 확보 개념은 (그림 4)와 같이 표현될 수 있다.

1) 정보보호 전공 장교 관련 부서 배치

정보보호 전공 장교를 관련 부서에 우선 배치한다. 현재, 학군장교 또는 학사장교 중에는 정보보호 분야를 전공한 장교들이 있을 것이다. 이들을 우선 실무 부서 또는 정책 부서에 배치하여 정보보호 분야의 실무 및 정책화를 담당시킴으로써 이들을 향후 국방 정보보호 전문가로 양성하여야 할 것이다. 또한, 국방대학교의 국방관리대학원 석사과정 전산정보학과에는 현재 정보보호를 연구하여 석사 학위를 취득하고자 하는 장교들이 있다. 군에서는 이들이 학위를 취득한 뒤 정보보호와 관계없는 부서에서 근무하도록 할 것이 아니라, 이들을 정보보호 관련 부서에서 근무하도록 함으로써 군에서 양성하고



(그림 4) 국방 정보보호 인력 확보 개념

있는 인력이 군을 위해 배우고 연구한 지식과 경험을 활용할 수 있을 것이다.

또한, 장교들 중 사관학교, 민간 대학교 등에서 정보기술을 전공하였거나, 현재 국방대학교 석사과정에서 정보기술을 전공하고 있는 장교들을 일정 기간 교육후 정보보호 관련 부서에서 근무하도록 할 수도 있을 것이다.

2) 정보보호 전공 병사 확보

현재 복무중인 병사 중 정보보호를 전공한 병사를 선별하여 군 CERT 등의 실무 인력으로 활용하여야 한다. 또한, 군 입영 대상자 중 재학시 정보보호를 전공하고 있거나 전공한 자, 그리고 정보보호 관련 동아리 활동자를 군에서 실무 인력으로 활용하여야 할 것이다. 이를 위해서는 객관적인 관점에서 이들의 능력을 평가하기 위한 선발 기준을 정립하고, 시험 등의 인증제도를 개발하여야 할 것이며, 이들의 국가관과 도덕성 등을 검증하기 위한 장치를 만들어야 할 것이다.

이외에도, 정보기술을 전공한 입영 대상자들에게 기초적인 실무 교육을 이수토록 한 뒤 정보보호 병사로 활용하는 방안도 함께 검토되어야 할 것이다.

3) 정보보호 전공 석·박사 확보

국방정보체계연구소의 국방과학연구소 통폐합과, 국방과학연구소 샛별부의 이관 이후, 현재 군에는 정보보호 및 사이버전 분야의 전문 연구 인력이 전무한 상태이다. 국방 정보보호 및 사이버전의 발전을 위해서는 현재 정보보호를 전공하고 있는 석·박사 과정의 학생들과 과정을 이수한 석·박사들을 한국국방연구원 또는 국방과학연구소에 입소시킴으로써 전문 인력을 확보하여야 할 것이다. 이를 위해서는 국방과학연구소와 한국국방연구원에 별도의 인력 조직을 구성하여야 할 것이며, 인력 결원 소요를 모아 별도의 팀으로 조정·편성한 뒤 인력을 확충하여야 할 것이다.

4) 정보보호 업무 경험자 특채

현재 민간 기업, 정부기관 등에서 정보보호 실무를 담당하고 있는 자를 군무원으로 특채하는 방안도 함께 고려되어야 할 것이다. 이들은 실제 업무를 담당하고 있기 때문에 곧바로 군 정보보호 실무에 투입할 수 있을 것이며, 이럼으로써 군 정보보호 능력을 단기간내에 향상시킬 수 있을 것이기 때문이다.

다만, 이들 전문인력을 군에서 활용하기 위해서는 충분한 보수와 혜택을 부여할 수 있어야 할 것이므로, 이들의 보수체계 등에 대해서는 별도의 규정이 국방부 차원에서 수립되어야 할 것이다. 현재, 정보보호가 가장 앞선 나라인 미국에서도 민간의 정보보호 인력을 연방 정부에서 활용하기에는 그들의 현 임금 수준을 국가에서 맞추어주지 못하는 문제로 어려움을 겪다가, 그들을 위한 별도의 보수체계를 확립하여 민간 인력을 정부에서 활용하는 돌파구로 삼았다. 따라서, 우리 군에서도 당면한 정보보호 문제를 시급히 해결하기 위해서는 미국 등 선진국의 사례를 따라 별도의 보수체계를 갖추어야 할 것이다.

5) 정보보호 전문가 영입

국방부 및 각 군의 정보보호 정책화 인력을 보강함으로써 향후 국방 정보화의 기틀을 체계적으로 정립할 수 있어야 한다. 이를 위해서는 인력 확보의 또 하나 중점 사항으로서 정보보호 전문가를 공무원으로 영입하여 정보보호 및 사이버전에 대비한 정책화 능력을 강화하여야 한다. 이를 위해서는 민간, 정부부처 및 연구기관에서 소신있고 미래지향적인 정보보호 전문가이며, 투철한 국가관과 국방관을 가지고 있는 자를 선별하여 영입하여야 할 것이다.

6) 정보보호 ROTC 제도 도입

정보보호를 전공하는 민간의 대학생 및 대학원생에게 장학금을 지원하고, 이들이 병사, 하사관 또는 초급 장교로서 일정 기간 국방 정보보호에 종사하는 제도를 시행하여야 할 것이다.

3.3 국방 정보보호를 위한 외부 인력 활용 방안

시간이 지나면 지날수록 군 정보화가 가속화될 것이다. 이에 따라 국방 정보통신망도 계속 확충될 것이고, 다양한 장비와 소프트웨어도 계속 도입될 것이며, 자료의 양도 기하급수적으로 증가하게 될 것이다. 이는 곧 군에서 보호하여야 할 보호 대상이 급격히 증가하게 될 것임을 시사한다. 또한, 민간에서는 정보보호 기술이 날로 발전하게 될 것이다. 이와 같은 향후 현상을 종합해볼 때, 군 자체 인력만으로는 국방 정보보호에 한계가 있을 것임을 쉽게 예측할 수 있다. 이와 같은 난관을 극복하기 위해서는 외부의 인력을 적극 활용하여야 한다.

1) Out-sourcing으로 외부 기술력 활용

현재, 우리나라에는 약 200여개의 정보보호 업체가 있다. 이들 중에는 군에서 필요로 하는 다양한 솔루션과 기술, 그리고 인력을 보유하고 있는 업체가 상당수 있다. 따라서, 군에서는 정보보호 제품의 도입, 국방 정보보호 체계 개발 사업 참여 등을 통하여 민간의 솔루션, 기술 및 인력을 국방 정보보호에 활용하여야 할 것이다. 연구개발 측면에서는, 국가보안기술연구소, 한국정보보호진흥원, 한국전자통신연구원 등과 같은 연구기관의 기술력과 노하우, 그리고 인력을 최대한 활용하여 국방 정보보호/사이버전 정책의 개발, 요소 기술 개발 등을 수행하여야 할 것이며, 학계를 통하여 원천 기술 및 가까운 장래에 소요될 첨단 기술의 개발과, 중장기적 국방 정보보호/사이버전 대응 전략 등을 모색하여야 할 것이다.

이를 위해서는 국방 외부의 전체 전문 인력과 전문 기관을 대상으로 한 중장기적 기술 확보 방안을 수립하여야 할 것이며, 각계 각층의 전문가들을 국방 정보보호 자문위원으로 위촉하여 국방 정보보호 방향 설정을 위한 조언을 구해야 할 것이다.

2) 외부 정보보호 요원 활용

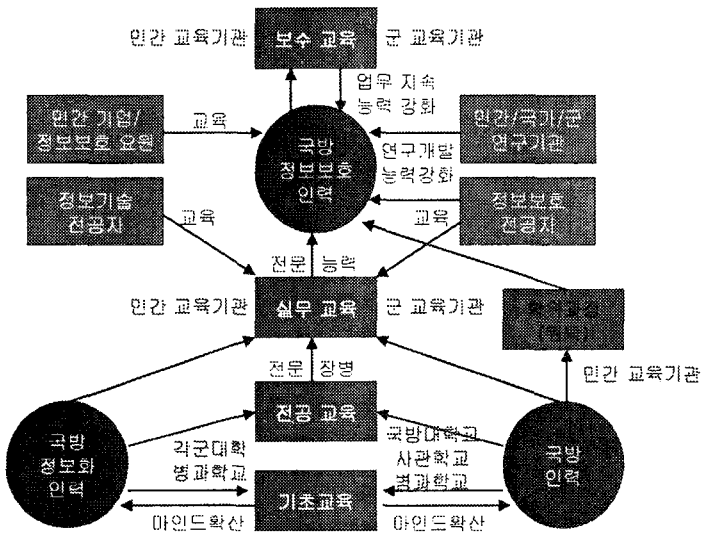
민간 및 국가 기관(연구기관 포함)의 정보보호 요원들을 활용하여 제한된 범위내에서 국방 정보보호를 위한 취약성 점검 및 위탁 관리 등을 수행할 수 있을 것이다. 현재, 군에서는 독자적인 능력으로 취약성을 점검하기가 어려운 상황이므로, 국방 정보체계에 대한 취약성 점검시 철저한 보안 지도하에 공동으로 취약성을 점검한다면 향후 군의 독자적인 능력에 의한 취약성 점검 및 보안 관리 등에 대비한 기술 축적, 노하우 전수 등의 효과가 있을 것으로 판단된다.

3) 정보보호 실무 강사진 활용

외부 정보보호 전문 요원들을 국방 정보보호 실무 강사진으로 활용함으로써, 군에서 필요로 하는 전문 지식과 기술을 전수받을 수 있을 것이다. 이렇게 함으로써, 외부의 앞선 감각과 기술을 국방 정보보호에 적용하며, 국방 정보보호 능력을 단기간내에 향상시킬 수 있을 것으로 판단된다.

3.4 국방 정보보호 인력 교육 훈련 방안

우리 군이 종합적인 정보보호 능력을 갖추기 위해서는 정보보호에 관련된 능력과 소양을 갖춘 인력의 확보와 외부 인력의 활용도 중요하지만 중장기적으로 볼 때, 현재 정보보호 실무를 담당하고 있는 군무원과 하사관의 능력을 향상시키고, 이들의 지휘통제 및 정책 수립에 관여할 수 있는 장교의 양성도 시급한 실정이다. 결국, 군의 정보체계에 대한 보호의 책임은 군이



(그림 5) 국방 정보보호 인력 교육훈련 개념

스스로 가져야 할 것이므로 국방 정보보호에 소요되는 인력의 대부분은 군 내·외부의 교육 훈련에 의한 인력 배출이 이루어져야 한다.

군 정보보호 인력의 교육 훈련의 개념은 (그림 5)와 같다. 국방 정보보호를 위해서는 각급 학교에서 전체 군 인력을 대상으로 정보보호 개념을 교육하여야 할 기초 교육이 수행되어야 하며, 정보보호 전공 교육을 통한 전문 인력 양성도 병행되어야 한다. 또한, 국방 정보보호 실무 능력을 배양하기 위한 실무 교육과 함께 국방 정보보호에 관련된 업무를 수행하는 인력을 대상으로 이들의 보수 교육도 제도화함으로써 전체 국방 정보보호 인력의 업무 지속 능력을 강화하여야 할 것이다.

1) 군 전체 정보보호 소양 교육 실시

소양 교육은 전체 장병들에게 정보보호의 기본 개념을 교육하는 것으로서 <표 1>과 같은 특성을 갖도록 구성되어야 한다. 이를 위해서, 사관학교, 각군 대학, 국방대학교 등의 전 장교 과정, 각 병과 학교 등에 정보보호 개론 과목을 개설하고, 공통 필수 과목으로 지정함으로써 전 장병들이 정보보호에 대한 기본적인 소양을 갖추도록 하여야 할 것이다.

<표 2> 국방 정보보호 기초 교육 방안

구 분	내 용
교육대상	전 장병 및 후보생 국방 정보보호 보임자
교육기관	국방대학교 육해공3군 사관학교 육해공군 대학 병과학교
교육과목	정보보호 개론
교육내용	정보보호의 필요성 정보보호 생활화 방법 등

2) 정보보호 전문 장교 양성

국방 정보보호 마인드를 가진 전문 장교들을 대거 양성함으로써 이들이 각군 본부에서 정보

보호 정책화, 기술을 보유 및 이해하는 자로서 정보보호 실무 부서의 지휘통제 및 조직 관리가 가능하도록 해야 할 것이다. 정책 부서의 장교에게는 국방 정보보호 정책 수립의 임무를 부여하며, 실무 부서(예: 각군 전산소, CERT 등)의 장교에게는 국방 정보보호 조직의 운영, 관리 및 지휘통제의 임무를 부여하여야 한다. 특히, 실무 부서뿐 아니라 정책 부서에도 정보보호에 대한 지식, 기술 및 개념을 가진 장교들을 배치시킴으로써 향후 국방 정보보호에 대한 중장기 정책 수립과 검토, 예산 반영 등의 업무를 주관하게 하여 국방 정보보호의 지속적 추진을 추구하는 효과를 얻을 수 있을 것이다.

이를 위해서는 <표 2>에서 보인 전공(학위) 교육 방안에 따라 육해공군 및 3사관학교 전산학과에 정보보호 전공을 개설하여 초급 전문 장교를 양성하여야 할 것이며, 국방대학원 석사과정에 정보보호 전공을 신설하여 중/고급 전문 장교들을 육성하여야 할 것이다.

<표 3> 국방 정보보호 전공 교육 방안

구 분	내 용
교육대상	사관생도 국방대학교 대학원생
교육기관	국방대학교 육해공3군 사관학교
교육과목	국방 정보보호론 국방 사이버전론
교육내용	국방 정보보호 기술 및 정책 국방 정보보호 추진 방향 국내외 사이버전 대비 현황 사이버전 무기체계 및 방어 등

3) 정보보호 전문 기술 하사관 및 군무원 제도 도입을 통한 전문화 지향

국방 인력 구조를 감안할 때, 국방 정보보호 전문인력을 교육훈련시키기 위한 가장 중요한 첫 번째 방안은 하사관과 군무원을 중심으로 하는 국방 정보보호 인력 구조를 정착시키는 것이다. 그 이유는 공무원들은 주로 정책 부서에 근무하고 있어 정보보호 실무에 투입하기가 쉽지 않다. 특히 이들은 국방부를 제외하고는 합참, 각군 본부, 각군 사령부 등에 근무할 수가 없기 때문에 이들을 국방부의 국방 정보보호 정책화 이외에 국방 정보보호의 핵심 인력으로 활용하기가 어렵다.

또한, 병사들은 복무기간이 만료되면 제대를 하기 때문에 장기적인 기술 습득과 경험 축적이 필요한 정보보호 업무의 핵심을 맡기기 어렵다. 뿐만 아니라, 장교 역시 순환 보직 관리와 진급 때문에 장기적으로 한 부서에 근무하기가 어렵다. 따라서, 중장기적 측면에서 국방 정보보호를 지속적으로 안정되게 수행하기 위해서는 근무지/부서 이동이 많지 않고, 장기간 근무할 수 있는 하사관과 군무원을 중심으로 하는 체제를 구축하여야 한다.

우선, 해공군의 기술 하사관과 같은 개념으로서 국방 정보보호 기술 하사관으로 활용하여야 할 것이다. 이렇게 함으로써 장교의 보직 순환과 병사의 제대로 인한 인력 공백 발생, 인력 이동에 따른 전문 인력으로 양성의 어려움, 인력의 지속적 임무 수행의 어려움 등의 문제점을 해결할 수 있을 것이며, 중장기적 측면에서 볼 때 군의 정보보호를 정착시키고 지속적으로 발전시킬 수 있을 것이다. 하사관 중 정책 부서의 하사관은 정보보호를 위한 기술적 정책 수립을 뒷받침하고, 실무 부서의 하사관은 정보보호 실무를 수행하거나 기술을 숙지하고 있는 중간 관리자로서 지휘관(장교)와 (기술)병사 사이의 기술적 가교 역할 수행하도록 한다면, 병사와 장교의 이동으로 인한 공백을 충분히 완화시킬 수 있을 것으로 판단된다.

군무원들은 현재 국방 정보보호 실무의 대부분을 담당하고 있다. 그러나, 정보보호 실무 능력과 경험이 부족한 실정이다. 그러나, 이들은 하사관과 마찬가지로 교육 훈련을 통하여 실질

적 정보보호 업무의 수행이 가능하며, 군 인력 이동에 따른 여러 문제점들을 해결할 수 있는 대안이다. 따라서, 국방 정보보호를 위한 핵심 전략으로 정보보호 기술 하사관과 군무원 제도의 도입이 우선 추진되어야 할 것이다.

이를 위해서, 단기적으로는 외부 정보보호 인력 또는 정보보호 관련 분야의 병사를 전문 하사관으로 특채하고 현 실무 인력은 외부 교육기관에 위탁 교육을 통하여 기술을 습득하도록 하여야 할 것이며, 중장기적으로는 군 내부에서 체계적인 교육훈련이 가능하도록 하여야 할 것이다.

4) 군 내부 전문 교육과정 설치

기술 군무원, 기술 하사관과 함께 전문 장교의 양성, 전문 병사의 확보 및 전문 인력의 관련 부서 근무 등을 통하여 국방 정보보호에 종사하는 인력들이 자부심을 가지고 업무에 종사할 수 있도록 유도하기 위해서는 단기적으로는 외부 기관에 위탁 교육을 시켜야 하겠지만 중장기적으로는 전문 교육 과정을 설치하여 이들을 배출함으로써 기술군으로의 발전을 앞당겨야 할 것이다.

이를 위해서는 중기적으로는 <표 3>에서 보인 방안에 따라 병과학교에 정보보호 교과목을 신설하여 정보보호 기술 하사관과 군무원들이 실무 교육을 받도록 하고, <표 4>에서 보인 방안에 따라 국방대학교 직무 연수부에 보수 교육 과정을 설치하여 국방 정보보호 인력 및 보임자들에 대한 지속적인 교육훈련을 통한 업무 지속 능력을 강화하고 최신 정보보호 기술 및 능력을 습득하는 기회를 부여하도록 하여야 할 것이다. 그리고, 장기적으로는 국방 정보보호 교육센터(가칭)를 설립하여 병과학교와 직무연수부 등의 실무 및 보수 교육 기능을 흡수하여 체계적이고 일원화된 교육훈련이 가능하도록 하여야 할 것이다.

<표 4> 국방 정보보호 실무 교육 방안

구 분	내 용
교육대상	정보보호 기술 하사관/군무원
교육기관	병과학교
교육과목	국방 정보보호 실무 정보보호 기술 활용
교육내용	국방 정보보호 개념 국방 정보보호 실무 기술 국방 정보보호 체계 운영 국방 정보보호 발전 방향 등

<표 5> 국방 정보보호 보수 교육 방안

구 분	내 용
교육대상	정보보호 보임자
교육기관	국방대학교 직무연수부
교육과목	국방 정보보호 실무 국방 정보보호 원론
교육내용	국방 정보보호 개념 최신 국방 정보보호 실무 기술 최신 국방 정보보호 체계 운영 국방 정보보호 체계구축방향 등

5) 위탁교육으로 전문 지식 습득

전문 인력을 양성하기 위한 또 하나의 방법은 외부 전문 기관에 위탁 교육을 시키는 것이다. 이를 위해서는 장병이 국내외 대학 및 대학원에서 수학하고자 하여 위탁교육생 선발시 정보보호 전공분야를 우선적으로 선발하도록 제도화하여야 할 것이다.

6) 국방 정보보호 교육훈련을 위한 기관별 임무 분장(안)

임무분장(안)은 <표 5>와 같다.

<표 5> 국방 정보보호 교육훈련 기관별 임무 분장(안)

학교 \ 교육 과정			기초	실무	전공	보수	학위	과목	비고
사관학교 (육해공3군)	공통필수(전생도)		√					정보보호개론	과목개편
	전공필수(전산학과)				√			정보보호론, 정보전론	과목신설
각군 대학	공통필수(전체)		√					정보보호 개론	과목개편
	보수과정(보임자)					√		국방 정보보호론 등	과목신설
병과학교	공통필수(전체)		√					정보보호 개론	과목개편
	실무과정(보임자)			√		√		국방 정보보호 실무 등	과목신설
국방대학교	안전보장대학원	정책과정(전체)				√		국방 정보보호 원론 등	과목신설
		석사과정			√			국방 정보보호 전략 등	과목신설
	국방관리대학원	정책과정				√		국방 정보보호 원론 등	과목신설
		석사과정			√			국방 정보보호 기술 등	전공신설
	합동참모대학	전과정				√		국방 정보보호 원론 등	과목신설
	직무연수부	국방정보화과정		√		√		국방 정보보호 실무 등	과정신설
군교육기관	국방 정보보호 실무과정			√		√		국방 정보보호 실무 등	과정신설
민간교육기관	대학원 전산학과/정보보호학과						√	정보보호 기술 등	위탁교육
	한국정보보호진흥원 등			√		√		정보보호 기술 등	위탁교육

4. 국방 정보보호 인력 양성을 위한 고려 사항

중장기적 측면에서 국방 정보보호 인력을 양성하기 위해서는 앞에서 기술한 사항들 이외에도 다음과 같은 사항들이 고려되어야 한다.

1) 교리 개발 강화

각군 교육사령부 또는 전투발전단에 정보보호 및 사이버전 교리 개발팀을 편성하고, 개발된 교리가 교육 과정 및 교재에 구체적으로 포함시키도록 한다.

2) 교육 과정 개발 및 표준 교재 개발

사관학교, 병과학교, 직무연수부 등 국방 정보보호 교육기관에 적용할 기초 교육 및 실습 과정, 국방 정보보호 실무 교육 및 실습 과정, 사관학교, 국방대학교 등 전공 교육 과정, 그리고 보수 과정의 세부 교육 과정을 개발한다.

또한, 각 기관 및 과정에서 사용할 표준 교재를 개발한다. 표준 교재는 전군 공통으로 사용할 기초 교육용 정보보호 개론, 사관학교 정보보호 전공 생도용 정보보호론 및 정보전론, 국방대학교 석사과정 전공용 국방 정보보호 전략 등, 직무연수부 보수(정책)과정용 국방 정보보호 정책 등, 그리고 병과학교 실무 교육용 국방 정보보호 기술, 국방 정보보호 실무 등을 개발한다. 또

한, 2-3년마다 주기적으로 교재를 보완 및 개정하여 최신 기술과 변화된 국방 환경에 적합한 교육이 이루어지도록 한다.

3) 교수요원 확보

민관군의 정보보호 전문가를 국방 정보보호 교수 요원으로 확보한다. 이를 위하여 국방대학교, 사관학교 및 각군 대학에서는 단기적으로는 국내 민관군 연구 기관 및 교육 기관의 전문가를 겸임 교수로 초빙하고, 중장기적으로는 국내외 전문 교육을 이수한 박사급 장교를 임용한다. 병과학교 등에서는 단기적으로는 민간군 전문 연구기관의 실무자를 외래강사로 초빙하고, 중장기적으로는 군의 실무 경험 인력을 임용한다.

4) 예산 확보

외래 교수요원 인건비, 교재 개발 및 인쇄비, 그리고 위탁 교육비는 경상비를 활용하도록 하고, 투자비를 이용하여 실험실습실 구축 및 기자재 구입에 사용할 수 있도록 예산을 반영한다.

5) 외국군과의 연계 강화

미국 등 외국 군 CERT에서 정보보호 실무 교육을 받을 수 있도록 하고 국내에서 활동하는 미군 CERT와의 공식적 채널을 구축함으로써 신속한 자료 및 정보 공유가 가능하도록 하며, 사건 접수, 사고 처리 등 업무처리 절차, 지침, 조직체계 등에 관한 정보를 교환함으로써 국방 정보보호의 체계화와 선진화를 꾀할 수 있도록 한다.

또한, 주한 미군에 의한 국내 사이버테러 사건 발생시 공동 대응 방안을 모색하며, 한미연례안보회의 및 한미군사위원회 의제로 제시함으로써 한미 공조가 가능하도록 한다.

6) 국방 정보보호 교육센터(가칭) 설립

장기적으로, 가칭 국방 정보보호 교육센터를 설립하여 표준 교재 및 교육 과정 개발, 평가 기준 및 방법론 개발, 각급 교육기관의 정보보호 교육 지원 등이 일원화 되도록 하며, 병과학교의 실무 및 보수 교육 기능 이관을 통해 국방 정보보호 교육의 체계화가 가능하도록 한다.

5. 결 론

사회 정보화가 진전되면서 정보화 선진국을 중심으로 정보시스템 해킹, 컴퓨터 바이러스 유포, 불건전 정보 유통, 인터넷을 이용한 신종 범죄 확산 등 정보화 역기능이 급격히 증가하고 있다. 따라서 국방정보체계의 완벽한 안전성을 보장함으로써 정보화 역기능을 최소화하고 국방 정보화를 지속적으로 추진할 수 있도록 국방 정보보호를 종합적이며 체계적인 대책 마련에 대한 필요성이 증가하고 있는 실정이다.

이와 같은 대책 수립의 한 축으로서 본 논문에서는 국방 정보보호 인력 양성 방안을 제시하였다. 먼저, 국방 정보보호 인력의 임무, 인력 구성, 유관 부서, 인력 수급 방법, 그리고 관련 기관에 따른 모델을 제시하였고, 국방 정보보호 인력 양성의 핵심 정책으로서 인력 확보, 외부 인력 활용, 그리고 교육 훈련 방안을 제시하였다. 본 논문에서 제시된 여러 가지 방안들이 국방부 정책에 반영되어 향후 국방 정보보호 대응을 위한 전문 인력 양성에 도움이 되기를 기대한다.

참고문헌

[1] 최운호, 박상서 외 2인, "국방정보보호 모델 정립 및 정보전 대응체계 구축방안에 관한 연구", 국방부, 2001