미래 정보전에 대비한 육군전술지휘정보체계(C4I) 정보보호대책 연구

우희철*

A Study on the Army Tactical C4I System Information Security Plan for Future Information Warfare

Hee-Choul Woo*

요 약 본 연구는 현재운용중인 국방정보통신망의 운용실태와 시스템의 구조·관리, 통신선로, 선로용 보안장비, 네트워크 및 소프트웨어의 관리, 보관중인 자료와 전송자료, 우리 군(軍)의 C4I체계에 대한 전반적인 취약점에 대해 분석을 실시하였다. 특히, 이중에서도 차후 전장에서 정보전의 핵심이 될 수 있는 육군전술지휘정보체계(C4I)에 대해 중점적으로 분석을 실시하여, 제시된 취약요소를 토대로 정보보호 적용방안을 제시하였다. 첫째, C4I 체계의 취약요소에 실질적으로 적용될 수 있는 보안운용체제, 인증제도, 바이러스 및 악성소프트웨어에 대한 대비, 가상사설망(VPN), 침입차단·탐지시스템, 방화벽 등 다양한 정보보호 요소기술을 제시함으로써 네트워크, 하드웨어(컴퓨터보안), 통신측면(통신보안)에서 강구될 수 있는 방안을 마련하였다. 둘째, 최근 사회적으로 이슈가 되고 있는 해커전에 대비하기 위해 해킹수법의 분석을 통한 위협을 살펴봄으로써 육군전술지휘정보망에 대한 대응책을 수립할 수 있도록 방안을 제시하였음. 셋째, 합리적인 국방정보보호체계를 구축하기 위해서 정보보호 관련된 제도 및 규정, 조직의 정비와 보완 등 여러 가지 선행되어야 할 요인들을 제시함으로써 효율성 높은 국방정보보호 체계를 구축할 수 있는 기반을 마련하였다. 본 연구의 결과를 바탕으로 얻어진 결론을 제시하면 성공적인 정보보호체계의 구축을 위해서는, 여러 기종의 다양한 보안시스템을 통하여 침입행위를 실시간으로 탐지하고 신속한 대응을 수행하며 침입관련 정보를 수집·분석하여 적절한 구성정보를 유지하여 주는 효율적인 '통합보안시스템'의 구성·운영이 필수적임을 강조한다.

주제어 : 정보전, 국방정보통신망, 육군전술지휘정보체계, 정보보호, 통합보안시스템

Abstract This study aims to analyze actual conditions of the present national defense information network operation, the structure and management of the system, communication lines, security equipments for the lines, the management of network and software, stored data and transferred data and even general vulnerable factors of our army tactical C4I system. Out of them, by carrying out an extensive analysis of the army tactical C4I system, likely to be the core of future information warfare, this study suggested plans adaptive to better information security, based on the vulnerable factors provided. Firstly, by suggesting various information security factor technologies, such as VPN (virtual private network), IPDS (intrusion prevention & detection system) and firewall system against virus and malicious software as well as security operation systems and validation programs, this study provided plans to improve the network, hardware (computer security), communication lines (communication security). Secondly, to prepare against hacking warfare which has been a social issue recently, this study suggested plans to establish countermeasures to increase the efficiency of the army tactical C4I system by investigating possible threats through an analysis of hacking techniques. Thirdly, to establish a more rational and efficient national defense information security system, this study provided a foundation by suggesting several priority factors, such as information security-related institutions and regulations and organization alignment and supplementation. On the basis of the results above, this study came to the following conclusion. To establish a successful information security system, it is essential to compose and operate an efficient 'Integrated Security System' that can detect and promptly cope with intrusion behaviors in real time through various different-type security systems and sustain the component information properly by analyzing intrusion-related information.

Key Words : Information warfare, National defense information network, Army tactical C41 system, Information security, Integrated security system

*문경대학교 부사관과 조교수
논문접수: 2012년 7월 29일, 1차 수정을 거쳐, 심사완료: 2012년 9월 30일

1. 서론

1.1 연구의 필요성 및 목적

정보기술(Information Technology)의 발달과 함께 정보화가 급속하게 진행되고 있는 현재 우리가 운영・관리하고 있는 국가조직의 모든 영역은 하나의 단일체계로 변화되어, 국가기간 산업, 경제, 안보분야 등 국가 전반을 통제하는 주요 시스템들의 자료는 모두 공유된 컴퓨터 망으로 구축되어 관리되고 있다. 이렇게 구축되어 관리되는 자료는 발달된 컴퓨터 통신망으로 상호 연결되어 마치 하나의 덩어리인 양 사용되고 있기 때문에 이런 핵심기반 시스템이 해커 등과 같은 외부 침입시스템으로부터 불법 침입을 당하여 손상을 입는다면 그 피해는 우리가 가히 상상하기도 힘들만큼 커질 것이며 그로 인해 국가기능은 마비되고 이에 따른 엄청난 혼란은 불 보듯 뻔할 것이라는 예측은 그리 어렵지 않다. 또한, 정부가 추진하고 있는 초고속 정보통신망 구축사업에 의해 국가기간 전산망이 하나의 사이버공간에서 모든 정보의 유통이 이루어지는 것은 그리 멀지 않은 바로 우리 코앞에 닥쳐있는 현실로 인식되고 있다.

이러한 국가의 정책에 따라 국방 분야에서도 국방정보통신기반구조(DII)의 하나로 국방전산통신망을 구축하였다. 그러나 이 국방전산통신망은 많은 구간이 군 전용망이 아니라 사설망을 이용하고 있어 적이나 가상의 적 혹은 불순한 의도를 갖고 있는 인물이나 조직, 국가에 국방관련 기밀들이 노출될 수 있는 가능성이 점차 증가하고 있는 실정이다. 미래학자와 군사전문가들은 발달된 정보기술을 이용하는 미래의 하나의 전쟁형태를 정보전(Information Warfare)이라 분류하였고, 걸프전에서 정보기술을 작전에이용하여 승리를 거뒀던 미군은 걸프전에서의 전쟁양상을 연구한 결과, 정보전은 과거의 전쟁과 달리 군사분야뿐만 아니라 미디어와 발달된 정보통신망을 이용하면 심리전등과 같이 민간분야까지 공격과 방어의 대상이 됨을 인식하기에 이르렀다.

한편, 우리나라에서도 정보전이란 개념이 주목을 받기 시작하면서 군의 여러 문서와 보고서에 정보전이란 용어가 자주 등장하고 있으나 미국 등 선진국 등에 비하면 아직 시작단계일 뿐 아니라 정보전에 관련된 국방분야의 관심과 투자는 미미한 실정이라 하겠다. 즉, 우리 군은 주요 정보체계에 대한 보호대책으로 통신보안장비와 같은 암호화 기능 중심의 네트워크 기밀성 서비스 제공을 중점적으로 수행하여 왔으나, 반면에, 모든 정보가 생성・처리・저장・관리되는 사용자 LAN 환경에서의 정보보호 대책은, 현재 부분적으로 정보보호체계 및 기술들을 활용 중에 있으나, 아직까지 관리적, 물리적 보안 대책 위주로서 상대적으로 미흡하게 취급되어 왔다고 할 수 있다[10].

국방 정보화의 추진 및 정보체계 간 정보 유통 소요 증가에 따른 상호 운용성 기술발전에 따라, 이와 같은 공격에 대한 위협은 주요 국방정보체계의 마비 및 파괴에 직접적인 영향을 끼칠 수 있으므로 정보보호의 필요성은 절실히 대두되고 있다.

따라서 본 논문에서는 다양한 정보전의 유형들 중에서 미(美) 국방대학원 교수인 리비키(Martin C. Libicki)가 분류한 정보전의 유형을 살펴봄으로써 해커전과 정보전을 중심으로 우리 육군의 전술 지휘통신망(C4I)에 대한 정보전 및 해커전등 에서의 위협과 취약점을 연구・분석하고, 이 분석결과를 통해 파악된 취약점에 대응할 수 있는 실질적인 정보보호 기술들을 도입・개발함으로써 국방정보통신망 정보보호 대책을 보완・강화하여 미래 정보전하에서 임무수행간 국방정보통신망의 보호성을 높임으로써 임무수행간 반영되는 내용에 대한 신뢰성을 극대화하여 완벽한 임무 수행에 기여할 수 있는 방법을 제시코자 한다[20].

1.2 연구내용 및 연구방법

본 연구목적을 달성하기 위한 연구문제는 다음과 같다. 연구하고자 하는 본 논문에서는 넓게는 정보전을 좁게는 정보전의 한 분야인 해커전을 연구대상으로 설정하였으며, 공격대상은 국방정보통신망을 기반으로 운용 중인 모든 망으로 설정하였다. 특히. 이중에서도 우리가 현재 운용중인 C4I망에 대해 집중적으로 알아보도록 할 것이다[5]. 앞으로, 정보전의 기본 바탕은 현재 운용중인 지휘통제망이 될 것이므로 실제로 이 망에 대한 운용실태와 정보보호분야에 대한 취약점을 파악하여 이를 토대로 해킹대책과 관리적인 측면에서 정보보호 대책을 제시 할 것임. 또한, 가장 기본적인 내용으로서는 정보전의 개념, 분류, 정의, 특징, 정보전 관점에서 본 국방정보통신망의 취약점 분석 중 정보전과 해킹전에 대비하기 위한 해킹의 정의, 공격유형 등을 알아보고 결론적으로 이러한 정보・해커전에 대비하기 위한 대책을 제시함으로써 완벽한 방어적 의미의 정보전을 수행할 수 있는 대책을 수립

토록 할 것이다[1].

2. 정보전 개념[19]

2.1 전쟁양상의 변화

인류가 살아오면서 수행한 전쟁의 원인과 사용된 기술, 전략과 전술의 변화 등을 보는 관점은 연구자들에 따라 다양하게 주장되어지고 있으나 그중 대표적인 학자인 토플러 부부(Alvin & Heidi Toffler)는 “전쟁을 사회에서 부를 획득하기 위한 방법의 확장으로 보고 시대를 농업시대, 산업시대, 정보시대로 구분하여 각 시대를 제1, 제2, 제3의 물결이라 하였으며 정보전은 제3의 물결인 정보시대의 전쟁방법”이라고 하였다.

한편 Edward Waltz는 토플러 부부의 저서인 “제3의 물결”과 “전쟁과 반전쟁”을 종합하여 각 시대별 특징을 <표 1>과 같이 제시하였다[19].

〈표 1〉 문명과 전쟁의 3가지 물결

연대(구분)	5000 B.C (농경사회)	A.D. 1700 (산업사회)	A.D. 2000 (정보사회)
힘의 원천	물리력・토지	재화 / 강철	지식 / 정보
생산 원리	노동력 집중	분업원리에 의한 대량생산	지식・정보에 의한 소량 생산
경쟁력 요소	노동	자본	기술
투쟁 동기	지배자간의 충돌	지역적, 범경제적 경쟁	이데올로기와 경제간의 충돌
전쟁 핵심 원칙	보병의 소모	기계소모, 대량파괴 장갑 및 기계 계층구조	의지와 능력소모 정밀제어와 지각 복잡, 적용, 분산
핵심 기술	도구・기계	기계/에너지	시스테밍 / 네트워킹
군사 전문가	손자	나폴레옹, 클라우제비츠	설리번, 캠펜, 리비키

2.2 정보전 특징

정보전은 과거의 전쟁처럼 현대화된 장비와 그것을 이용하는 병력의 우세로 전쟁에서 승리할 수 있다는 산업 시대적 관점에서는 해석할 수 없고, 새로운 전쟁의 패러다임을 요구하고 있다고 할 수 있다. 따라서 정보전에 관한 사항을 논의할 때에는 국가전체 즉, 군과 민간분야 모두를 포함하여야만 설명이 가능해 지게 될 것이다[19]. 정보전의 특징은 <표 2>와 같다.

〈표 2〉 정보전의 특징

정보전 특징	결 과
・전쟁수행 비용이 저렴	・잠재적인 적의 범위가 확대됨
・사이버 공간에서 전통적인 경계가 불분명	・공격당하는 자, 공격자, 대응책임자 식별 곤란
・사이버 공간에서 지각능력을 조작하기 쉽다	・실제와 조작의 구별이 불가능함
・새로운 전략첩보의 수집과 분석방법이 필요	・잠재적인 적, 적의 의도와 능력 파악 곤란
・사이버공간에서 정보전 공격을 다른 사건\들과 구분할 수 있는 적절한 전술경보체계 및 공격평가 방법이 전무	・적의 공격 여부, 공격자, 공격방법의 식별 곤란
・별도의 전선이 없음	・후방도 공격대상이 되며, 방어대상 역시 증가

2.3 정보전 정의

“정보전이란 무엇인가?” 이에 대한 관점은 다양하다. 로나(Thomas Rona), 슈와르트(Winn Schwartau), 위드낼과 포글먼(Sheila E. Widnall & Ronald R. Fogleman) 등 여러 학자들과 미 합참등 다양한 조직과 개인이 정의하였으나 본 논문에서는 군과 민간의 모든 영역을 가장 잘 포함하여 정의한 미 합참의 정의를 채택하겠다.

미 합참은 정보전을 “정보전은 정보우위를 확보하기 위하여 보호적 측면에서는 아군의 정보, 정보에 기초한 프로세스, 컴퓨터 네트워크를 보호하고, 공세적 측면에서는 적의정보, 정보에 기초한 프로세스, 컴퓨터 네트워크를 공격하는 일체의 행위”라고 정의하였으며, 여기서 정보우위란 정보를 지속적으로 수집, 처리, 저장, 전송, 표시, 전파하는 능력을 나타내는 것이라고 하였다[17].

2.4 정보전 유형

정보전의 유형도 정보전의 정의처럼 다양하게 분류되고 있으나 본 논문에서는 정보전의 유형을 가장 포괄적으로 다루고 있는 미 국방대학원의 리비키의 분류를 중심으로 살펴보도록 하겠다.

미 국방대학의 리비키(Libicki) 교수는 각종 정보전의 형태를 종합하여 지휘통제전, 군사정보기반전, 심리전, 해커전, 사이버전 및 경제정보전 등으로 구분하였으며, 이들 중 어느 하나가 앞으로 발생할 수 있는 다양한 정보전 유형을 모두 설명할 수도 없기 때문에 미래의 정보전은 리비키 교수의 분류 유형의 전부 또는 일부가 복합된 모습으로 나타날 수 있다. 리비키 교수는 정보전은 현존 군사력을 중심으로 C4I 시스템이나 정보시스템에 국한된

공격 및 방어뿐만 아니라, 사이버 테러라고 하는 국가의 주요 기반시설인 정보시스템에 대한 공격을 포함하여 사이버 공간까지 확장한 광범위한 개념으로 발전되어 가고 있다고 정의하였으며, 그 유형은 아래의 <표 3>과 같다[20].

〈표 3〉 정보전의 유형

구 분	유 형	개 념
군 사 부 문	지휘통제전 (Command and Control Warfare)	· 적 지휘부의 지휘의사결정 및 지휘수단 무력화 예) 걸프전시 이라크 지휘통제 체계 파괴
	전자전 (Electronic Warfare)	· 적의 전자통신 성능을 저하시키거나 감소 예) 레이더 재머, 전자방해, 채프등
	군사정보전 (Intelligence Based Warfare)	· 군사정보 수집, 처리, 전파에 사용되는 전장감시체계 공격과 방어 예) AWACS, JSTARS 등의 전장감시체계
민·군 중 첩 부 문	심리전 (Psychological Warfare)	· 적의 민간인, 병사, 지휘관에 대한 심리조작 예) 방송을 통한 전투참가 반대 여론 형성, 선무방송
	해커전 (Hacker Warfare)	· 컴퓨터의 보안취약점을 이용하여 컴퓨터, 네트워크, 데이터 등을 공격 예) 유고의 미국·나토에 대한 조직적 해킹 시도
	사이버전 (Cyber Warfare)	· 사이버 공간에서 가상인간 사이의 분쟁 예) 컴퓨터 바이러스, 웜 등을 공격하는 정보테러
민 간 부 문	경제정보전 (Economic Information Warfare)	· 정보전과 경제전의 결합 예) 미 NSA에 의한 유럽 및 일본 기업의 이메일 도청

3. 정보전 관점에서 본 국방정보통신망의 운용현황

3.1 국방정보화 중장기 계획[8]

국방정보화를 달성하기 위한 중·장기 계획은 2015년까지 정보전 수행능력을 갖춘 정예정보화 군 육성을 기본 목표로 하며 실시간 전장관리 및 정보 유통·공유를 통한 지휘통제와 통합된 전력을 발휘하고, 효율적인 자원관리로 작지만 강한 군을 운영하는데 그 목적을 두고 있다.

우리 군의 국방정보화 중장기 계획은 <표 4>와 같다.

〈표 4〉 국방정보화 중장기 계획

단 계	추 진 목 표	추 진 중 점
1단계 (1999~2005)	· 기반 및 핵심체계구축	· 정보화 환경여건 정비 · 정보통신기반(LAN, WAN) 구축 · 핵심체계(C4I, CALS)구축
2단계 (2006~2010)	· 기능확장 및 체계통합	· 국방초고속 정보통신망 구축 · 국방통합 C4I, CALS체계 구축
3단계 (2011~2015)	· 선진 정보체계 완성	· 국방초고속 정보통신망 완성 · 국방통합 C4I, CALS체계 완성 · 전자국방업무 수행체계 구축

3.2 국방정보통신망 운용현황

3.2.1 국방정보통신망 구조

국방정보통신망은 기존 전용회선의 일대일 통신망을 개선하여 군전용 단일통신망으로 통합·운용되고 있으며, ATM 및 패킷 교환 망에 의한 교환통신을 통해 단일회선에서 복수의 상대와 통신이 가능하게 되었다. 그리고 통신체계도 TCP/IP에 의한 표준 통신체계를 채택함으로써 이기종간 상호통신이 가능하게 하였고, 신속한 정보 및 자료 교환을 가능하게 하였다.

1) 국방정보통신망 토폴리지

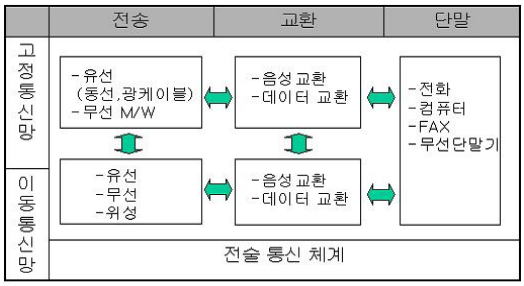
국방정보통신망은 전군의 단일 통합 네트웍으로 주요 지역에 ATM 또는 X.25 패킷교환기를 설치하고 인접 가입부대를 접속하는 형태로 구성되어 있으며 토폴러지 구성은 Connectivity가 3이상으로 생존성을 중시하였다[6].

2) 망운용 현황

국방정보통신망의 운용현황을 살펴보면 크게 고정통신망과 이동통신망으로 나누어진다.

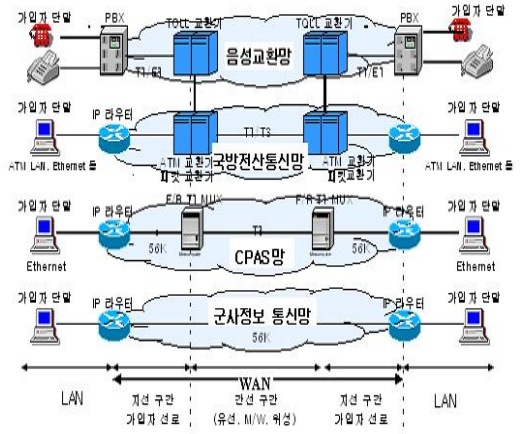
고정통신망의 전송 체계는 유선과 무선구간으로 나누어지고 유선망의 장애 발생시에 통신망의 생존성 보호를 위해 2차 통신수단으로 무선망을 운용하는 이원화 체계를 갖추고 있다.

이동통신망은 전술 통신 체계로서 이동 및 야전 위주의 지원을 담당하는 통신망으로 각 육/해/공군마다 별도의 통신 체계를 갖추고 있어 별도로 운용되고 있다. 이동통신망은 고정통신망과의 연동 혹은 상호 운용성이 지원되지 않고 각 군의 통신망과도 상호 연동되지 않는다. 국방정보통신망 운용현황은 [그림 1]과 같다[6].



[그림 1] 국방정보통신망 운용현황 개념도

현재 관리되는 고정통신망은 크게 음성망, 국방전산망으로 나뉘며 그 외에 CAPS, 군사정보통신망 등이 있으며 [그림 2]와 같이 구성되어 있다.



[그림 2] 고정통신망 구성도

국방 ATM 백본망은 한국통신의 초고속 ATM 망을 효율적으로 이용하기 위해 구축되었으나 선로용 보안 장비의 특성 때문에 이를 활용하지 못하고 있다. 선로용 보안장비는 ATM 헤더까지 암호화하므로 한국통신의 ATM 망을 통과할 수 없기 때문이다. 따라서 현재의 운용상황을 보면, 각 군부대별 음성정보는 지선구간을 거쳐 지선과 간선의 접점(Access Point)에 위치한 Toll 교환기에서 합쳐진다. Toll 스위치를 통과한 음성정보 및 IP 망을 통과한 데이터는 ATM 장비를 경유하고, 다시 광단국을 통하여 각각 별도의 채널로 전송된다. 즉 실제 전송은 한국통신의 전용선 서비스를 이용하여 전송되는 것이다.

3) 활용분야

국방정보통신망은 크게 작전지휘통제를 위한 전장관리 분야와 국방자원의 효율적 관리를 위한 자원관리 분야에 통신기반을 제공하고 있다.

3.2.2 국방 웹 기반 서비스

국방전산서비스 중 가장 대표적인 웹 기반 서비스는 국방인트라넷으로서 이에 대한 이용도 점점 활성화되고 있다. 그러나 진정한 의미의 웹 서비스라고 하기에는 확장성과 개방성이 부족하며 소규모·이동제대에 대한 서비스 제공은 현재 불가능한 실정이다[3].

3.2.3 국방정보통신망의 기반체계 및 서비스

1) 정보통신기반체계[6]

정보통신기반체계는 지휘통제체계와 자원관리체계를 효율적으로 운영하기 위한 기반체계를 제공하는 것으로서 정보체계 구축에 필요한 물리적인 요소인 컴퓨터 체계, 정보통신체계, 정보보호체계로 구성된다.

가) 컴퓨터체계

주전산기는 현재 여단급 이상 부대에 보급되어 군사자료의 통합관리와 공유·저장용으로 운용중이나 부대·기관별로 전산기 기종과 운영체계가 다양하여 상호연동과 호환성이 미흡하다.

나) 정보통신체계

국방정보통신체계는 군 작전운용 특성과 정보의 유형 및 사용환경에 따라 크게 전략 통신체계, 위성체계, 전술통신체계로 분류되어 운영되고 있으며 전략정보 통신체계 현황은 <표 5>와 같다.

〈표 5〉 전략정보통신체계 현황

구 분	현 황
국방 전산망	· 전·평시 국방자원의 효율적 관리와 운용을 위한 국방통합지원관리체계 및 사무자동화를 지원하는 망으로 여단급 이상 온라인망으로 구축·운영하고 있으나, 한국통신 전용회선을 이용하고 있어 전시 생존성 보장이 어렵다.
지휘소 자동화망	· 전략제대 지휘소자동화 체계를 운용하기 위한 데이터 통신망으로 각 군의 작전사급 이상 부대에 고속패킷교환기를 설치하여 150여 부대 및 기관이가입되어 운용하고 있으나, 한국통신 전용회선을 임차하고 있어 전시 생존성 보장과 국방정보통신망 연계 운용이 어렵다.
M / W 망	· 전략 정보통신망의 예비(Back-up) 체계로 다중경로로 격자화 되어 있어 광범위한 지역에서 운용은 가능하나 시설이 노출되어 있고 한국통신 시설을 이용하여 전시생존성이 취약하고 정보 유통 속도 충족도 어렵다.

또한, 위성통신체계는 무궁화위성 중계기와 고정・이동 지상 단말기를 이용하여 기동군단 및 작전사급 이상 부대에서 작전지휘망 및 고속 데이터망을 운용하고 있으나 상용 중계기를 이용하기 때문에 전송대역이 제한되어 원활한 정보전송이 곤란하고, 중계기에 대한 보안성, 생존성이 취약하며 저속의 전송능력으로 인해 제한된 서비스만 제공 가능하다.

그리고 군사전술정보 통신에 이용되는 전술정보통신체계는 대부분이 각 군별로 별도의 망을 구축하여 운용중이며 현황은 <표 6>과 같다.

〈표 6〉 전술정보통신체계 현황

구 분	현 황
전술 공용망	・육군에서 구축중인 SPIDER망은 향후 구축될 육군전술 C4I체계의 기간망이 될 예정이며, 공군은 MCRC망, 해군은 KNTDS망을 각각 운용하고 있다.
전술 무선망	・무선전송능력의 제한으로 전술무선망과 각 군, 기능체계간 상호운용성이 제한되어 있다.

다) 정보보호체계

현재 국방정보보호체계는 표준지정, 최신 정보보호기술 활용이 매우 미흡한 실정으로 자료유출, 컴퓨터 바이러스 침투, 해커침입에 대해 적절한 대응책이 수립되지 못하여 인터넷을 이용한 업무처리는 불가능한 실정이고, 내부 해커와 컴퓨터 바이러스로 인한 피해 가능성은 매우 높다.

2) 육군 전술지휘정보체계(C4I체계)

지휘통제체계는 전・평시의 작전운용에 필수적인 지휘통제・통신・정보의 제 요소를 통합하여 가용한 전투력을 효율적으로 운용하고, 지휘관 및 참모의 지휘결심을 보좌함으로써 전장을 효율적으로 관리하는 체계로서 합동 C4I와 각 군 전술 C4I체계로 나눌 수 있다[8].

우리 군은 지상군 전력증강의 일환으로 지난 '00년부터 군단급 이하 전술제대의 전투수행절차를 자동화하기 위한 육군 전술지휘정보체계(이하 체계라 한다)를 3단계로 구분하여 사업을 추진하고 있다. 그중 기반체계를 구축하기 위한 1,2단계사업은 성공적으로 완료하고, 3단계 사업을 동시에 추진 중에 있으며, '14년도까지 개발을 완료하고 연차적으로 전방군단에 전력화할 예정이다. 최신 상용정보기술을 군에 접목시키기 위해 순수한 국내 IT업체기술로 우리 군의 작전환경과 교리, 작전개념 등을 반영하여 한국군 특성에 맞는 우리군 고유의 체계를 개발하고 있다는 데 큰 의의가 있다.

가) 구축목표

체계 구축목표는 군단급 이하 전술제대(육군 및 해병대 포함)가 "먼저 적을 보고(先見), 먼저 결심하여(先決), 먼저 타격할 수 있는(先打)" 전투수행체계를 구축하는 것으로 신속한 보고, 처리, 전파 및 도시로 전장상황을 가시화 시키고 핵심 센서(Senser)와 슈터(Shooter)를 연결하여 실시간 타격이 가능하게 하여 전투력의 승수효과를 최대로 발휘할 수 있도록 구축하며 지휘결심에 필요한 자료를 적시에 제공하는 것이다.

이를 위한 체계구축은 여건에 따라 사업을 단계화(1차:'99~'06년, 2차:'07~'10년,3차:'11~14년)하여 점진적으로 추진하되. 먼저 '06년까지 추진된 1차사업의 목표는 피・아 전장상황의 신속한 보고・처리・전파・도시를 통하여 전장을 가시화하고, 핵심적인 감시체계(Senser)와 타격체계(Shooter)를 연결하여 실시간 타격이 가능하게 하며 지휘결심에 필요한 자료를 적시에 제공하는 체계를 구축하였다.

나) 특 성

체계 특성은 전술제대의 전장상황을 근실시간에 파악할 수 있게 지원하기 위하여 감시수단으로부터 획득된 정보 및 첩보를 체계로 획득 및 유통을 보장하고, 지휘통제 본부내의 각 기능실시간에 적시적인 정보 유통 및 공유를 지원한다. 그리고 감시 수단과 타격 수단을 연동함으로써 실시간 타격을 지원하며, 전략 C4I인 지휘소자동체계와 상호운용이 가능하도록 구성한다.

또한, 전술제대의 빈번한 이동을 고려한 기동성 있는 체계로 구성할 것이며, 상호운용성과 표준화를 고려한 개방형 체계로 확장이 용이하다.

다) 구축개념

체계구축은 군단에서 연대급까지 전술제대의 현 지휘통제실 구성을 고려 전장기능을 정보종합실, 작전실, 통합화력 지원실, 전투근무지원실 별로 통합하여 운용하도록 구성하였다. 체계연동은 전략급제대(합참-군사)에서 기 개발하여 운용하고 있는 지휘소자동화체계(CPAS)와 연동하고 일부 탐지 및 타격체계와 연동하도록 되어 있으며, 체계배치는 군단, 사단, 연대급 지휘소는 지휘통제본부를 중심으로 전산 셀터를 배치하여 LAN을 구축하고, 직할부대는 WAN으로 구성하며, 대대급은 단말기(PC)가 보급되어 연대체계의 일부로 정보를 입력하고 전

장상황을 파악하게 되며, 중대급은 무전기와 접속하여 운용되는 위치보고 접속장치로 자동적인 위치보고와 단순상황보고 및 지시위주의 간단한 전문 송·수신이 가능하다. 체계구성은 지휘통제 본부내의 운용조직을 중심으로 응용소프트웨어인 정보, 작전, 화력, 전투근무지원의 제 요소와 공통소프트웨어인 상황도 도시, 전문처리, 영상처리, 사무지원, 시스템관리 등의 다섯 개 분야와 하드웨어 및 정보보호로 구성되어 있으며, 6대 전장기능 중 기동, 방호는 작전실에, 지휘통제통신은 각 기능실에 통합하여 운용하고, 수집자산과 타격자산은 접속장치를 통해 관련 기능실과 연동되도록 구성되며, 제대간 정보유통은 전술통신 체계를 이용한다.

체계는 전술통신체계기반(MSC-500K)하에서 데이터가 유통되도록 설계되기 때문에 전술통신체계의 데이터 전송능력에 많은 영향을 받는다. 전술통신체계는 개발이 완료되어 전력화되고 있지만, 전술지휘통제체계 지원을 위해 성능개량을 동시에 추진 중에 있다.

1차 사업의 단계별 구축 목표를 살펴보면 다음과 같다.

1단계는 전장상황에 대한 보고, 지시, 전파시간을 단축하고, 상·하 제대/전장 기능간 전장상황을 공유토록 하며, UAV로부터 영상을 획득하여 관련 기능실에 전파한다.

2단계는 핵심감시 및 수집체계(AN/TPQ-36/37, TPS-830K, ES/EA, RASIT)와 연동하여 실시간으로 정보를 획득 전파하고, BTCS와 연동하여 실시간 타격명령을 하달한다.

3단계는 신속한 참모판단 및 지휘결심 자료를 제공하기 위한 기능별 업무를 부분 자동화 한다[2].

라) 주소체계

전술지휘통제 망에 대한 주소체계의 기본 운용개념은 국방 주소체계와 연계 및 상호 운용될 수 있도록 하며 전술통신체계(MSC-500K) 네트워크를 기반으로 주소체계를 정립하고 전술상황의 변화에 유연하게 대응할 수 있어야 하며, 주소의 할당 및 사용을 간명하게 함으로서 사용자 편리성을 보장하고, 향후 새로운 통신체계가 개발될 경우에 대응하도록 확장성을 고려하여 할당한다.[7]

국방 IP주소체계는 [그림 3] 과 같은 구조를 가지며 네트워크 영역중 0~63번은 LAN으로 64~223번은 WAN으로 구분하여 각각 하위계층의 주소를 부여하고, LAN 주소의 영역은 제대별(A, B), 망별(C), 가입자별(D)로 구분되며 각 가입자는 유일한 주소를 갖는다.

[그림 3] 국방 IP 주소체계

네트워크영역(0~63번)은 군사급 이상제대의 LAN 주소로 할당되어 있으며, 네트워크확장(0~255)영역은 군단~여단급의 LAN 주소로 할당되어 있고, 망 구분 및 서브넷 영역은 군단~여단급의 LAN망 중에서 기능별/망별로 구분되며, 가입자 장비영역은 제대별/기능별 LAN 망 중에서 실제 가입된 장비별로 주소가 할당된다.

네트워크영역(64~255번)중 국방망은 64~79번이고, 전술망은 80~89번으로 영역이 분류되어 있으며 전술망 부분 중 지휘소자동화체계는 80번으로 할당되어있으며 육군전술지휘정보망은 81~83번으로 할당될 예정이며, 84~89는 차후에 해군, 공군의 전술망 주소체계로 할당될 예정이다.

체계의 LAN IP 주소는 TDU의 LAN포트, TDU와 암호장비 사이, 암호장비와 스위칭허브, 스위칭허브와 호스트 구간에 적용되는 IP 주소의 체계이다.[18]

네트워크 영역(0~63번)과, 네트워크 확장영역(0~255번)은 국방망에서 기 설정된 주소체계를 적용하고, 망구분/서브넷영역(C)과 가입장비영역(D) 중에서 전술지휘정보체계 망에 필요한 부분은 <표 7>과 같이 구분할 수 있다.

〈표 7〉 망 및 서브넷 구분

C영역	망구분/서브넷	운용제대	세부할당
120~223	전술 C4I (연대/대대)	A연대/대대	120~129/130~139
		B연대/대대	140~149/150~159
		C연대/대대	160~169/170~179
		D연대/대대	180~189/190~199
		지원배속/대대	200~209/210~219
		예비	220~239
224~255	예비		

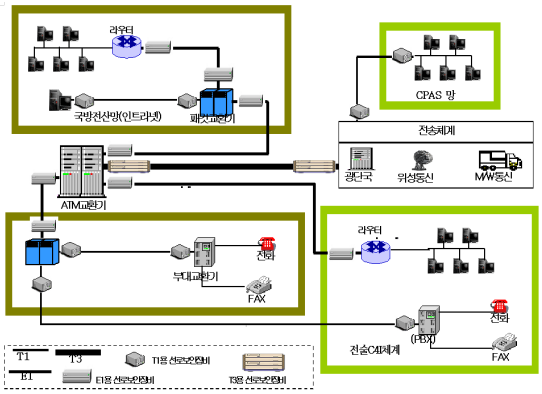
결국, LAN에서 국방망과 전술망의 구분은 망구분/서브넷("C"영역)에서 정해진다.

네트워크영역이나 네트워크 확장 영역은 여단급 이상 부대의 규모만 정해질 뿐 국방망과 전술망이 공통적으로 사용하기 때문이다. 만약, 네트워크영역(A)과 네트워크 확장영역(B)만을 네트워크부로 지정하고 나머지를 호스트로 구분한다면 구분자체는 쉬워지겠으나 상당히 비효율적인 네트워크가 될 것이다. 왜냐하면 사단급 부대의

모든 컴퓨터는 한 네트워크가 될 것이고, 가입할 수 있는 호스트 수는 65,534개(216-2)가 될 것이다. 이때 각 단말들은 브로트캐스팅 정보가 수시로 발행하는데, 이때 발생하는 브로드캐스팅트래픽을 감당할 수 없기 때문이다. 네트워크를 효율적으로 운용하기 위해서는 사용하는 호스트 수 및 조직 구성을 고려하여 적당히 나누는 것이 바람직하다. 망구분 및 서브넷 영역에서는 이를 위한 구분을 해주는 것이 목적이며 일반적으로 국방망과 전술망으로 구분하고, 각각의 망은 다시 정보, 작전, 지원 등의 형태나 1층, 2층, 3층 등으로 구분하여 망운용 유지에 가장 효율적인 형태로 운용하게 된다. WAN IP 주소체계는 전술통신체계의 IP 주소체계를 따른다[6].

3.3 국방정보통신망의 취약성 〔4〕

현재 운용중인 국방정보통신망은 전용선을 그 기반으로 하고 있으며, 이것은 우리 군에서 운용하는 국방정보체계의 전 분야에 걸친 일반적인 운용실태라고 봐도 무방할 것임. 이러한 전용망 위주의 국방정보체계를 일반국민의 알 권리를 충족시키고, 경제적인 이익을 추구함과 동시에 전산망의 성능향상을 위해서 일부를 상용선으로 분산시키는 것은 국방정보체계가 인터넷과 같은 개방성을 지니는 것을 의미하므로 이를 실현시키기 위해서는 현재 운용되는 국방정보체계의 정보보호 취약점을 완전히 해결해야하며 지금보다도 더 강력한 정보보호대책을 수립하고 동시에 우리 군 내부의 사용자들도 이에 따른 보안의식의 변화도 선행되어야 할 과제라고 생각된다[11].현재 운용중인 국방망 보안체계는 〔그림 4〕 와 같다.



[그림 4] 현재 운용중인 국방망 보안체계

3.3.1 시스템 구성문제

국방 전산시스템에 사용되는 대부분의 주 전산기는 UNIX 운영체제를 사용하고 있는데 이런 UNIX는 구성설정의 잘못으로 많은 시스템 및 망 보안 취약성을 유발할 수 있다. 또한 시스템의 사용에 대한 로그를 적절히 수행하지 않아 감사추적 자료로 활용하기 어렵다.

3.3.2 시스템 관리 문제

보안정책을 실현하기 위한 시스템 관리절차를 수립하여 철저히 시행되는 것은 비용이 소요되지 않는 가장 기본적인 보안방법임에도 불구하고 시스템 관리절차가 체계적으로 만들어져 있지 않고, 시스템을 관리하는 요원의 보안의식, 경험 및 지식이 부족하여 대다수의 사이트가 시스템관리가 제대로 되지 않고 있다.

3.3.3 통신선로상의 취약점

국방망은 물리적으로는 공중망의 선로를 사용하며, 논리적으로만 국방망 으로 구분하여 사용하고 있다. 따라서 통신선로 상에 전송되는 데이터에 대하여 도청 또는 트래픽 분석, 전자파 가로채기 등을 통한 정보의 누출 위협이 있다. 또한 누출된 데이터의 변경을 통해 데이터의 무결성이 손상될 위협이 있다. 이러한 위협에 대한 보호장치로 선로용 보안장비를 사용하도록 하고 있는데, 이런 선로용 또는 회로용 보안장비는 데이터 링크 레벨에서의 데이터의 기밀성 유지를 위한 암호화만을 제공하며, 이러한 보안장비는 선로의 속도에 따라 각기 다르게 사용하고 있다.

3.3.4 선로용 보안장비의 문제점

선로용 보안장비는 하나의 선로에 대하여 링크 계층에서 그 선로를 통하는 모든 트랙픽을 암호화하여 비밀성을 유지하는 보안장비이다. 이 장비의 문제점은 모든 선로의 양단마다 설치되어야 하므로 많은 숫자의 장비가 필요하며, 선로의 규격이 바뀌면 새로운 장비를 개발하여야 하며, 중간의 네트워크를 효율적으로 사용할 수 없으며, 보안에 취약점이 있을 수 있다.

3.3.5 네트워크 소프트웨어 및 관리문제

파일 전송서비스(FTP등)의 통제가 미흡하여 대용량 자료 유출이 가능하고 네트워크를 통한 시스템 불법침입을 모니터링할 수 있는 기능이 거의 없어 해커나 비인가

자 불법침입시 망 운영반이나 주 전산실 관리자가 불법 침입 사실을 즉시 인지할 수 없으며, 아직도 침입차단시스템과 침입탐지시스템 미설치 개소도 다수 존재한다.

3.3.6 보관중인 자료와 전송자료의 취약성

현재 대부분의 전산데이터는 시스템 성능을 이유로 제작사 에서 기본적으로 제공되는 데이터암호화 기능조차 이용하고 있지 않아 저장자료 유출과 동시에 유출된 정보의 악용이 가능하다.

3.3.7 우리군의 C4I체계 정보보호 위협요소

전문처리 기능의 정보보호 위협요소로 위조는 전문처리시 정보보호 위협 요소이며 암호화된 통신문에 대한 위협요소로는, 암호문 인지 공격방법(Giphertext Only Attack), 통신문 인지 공격방법(Known Plaintext Attack),선택 평문 공격방법(Chosen Plaintext Attcak)이 있으며, 사무자동화에 대한 정보보호 위협요소로는 C4I 체계운용시 각 기능간, 상하제대간 전자결재등 사무자동화에 따라 발생할 수 있는 위협요소는 위장(masquerade), 내용수정(content modification), 순서수정(sequence modification), 시간수정(timing modification), 부인(repudiation) 등이 발생할 수 있고, 불법침해에 따른 정보보호 위협요소로써 C4I체계도 일반적인 네트워크로 구성된 시스템의 중요한 보안문제인 권한이 없는 자가 로그온 하여 기계로 들어가려고 하거나 또는, 권한 있는 사용자인 경우 권한을 부여 받은 것 이상의 권한을 획득하려 하는 침입과 소프트웨어 불법 침해인 바이러스·벌레(WORM)가 발생할 수 있다.

3.3.8 해커 공격(해킹)의 위협

1) 해킹의 대상과 유형

이러한 해커들의 해킹대상을 데이터, 시스템 프로그램, 네트워크 등으로 분류하여 해커들이 저지를 수 있는 해킹 행위들을 불법삽입, 불법유출, 불법변조, 파괴·거부 등의 행위로 나누어 보면 <표 8>과 같이 요약할 수 있다[13].

〈표 8〉 해킹과 해킹사고 유형

	불법삽입	불법 유출	불법 변조	파괴·거부
데이터	개인의 신상에 대한 그릇된 정보 등의 제공	주요 비밀정보,개인 신상정보 등의 유출	일반자료 변조. 불법 금융거래를 노린 변조 등	일반·중요 정보의 파괴
시스템/소프트웨어	바이러스, 웜, 백도어,,트로이 목마	주요 시스템 파일의 유출	악의적 이용을 위한 프로그램/파일의 변조	프로그램 파괴, 고장 유발행위
정보 통신망	시스템 과부하를 노린 행위	시스템 제어 정보 유출	통신지연, 잘못된 라우팅 유도	접근 및 망 운영 방해

2) 해킹(Hacking) 공격 분류

해킹공격 분류방법은 정보보호 관련 학술적인 측면에서의 분류와 정보보호업체에서의 분류방법에 따라 다르게 분류되고 있으나 본 논문에서는 제 11회 정보보호와 암호에 관한 학술대회(WISC '99)에서 발표된 해킹공격 분류를 따르도록 하겠다. <표 9> 와 같이 요약할 수 있다[13].

〈표 9〉 대표적 수법 설명 및 세부 해킹 수법

대분류	수 법 설 명	세 부 해 킹 수 법	공 격 대 상
사용자도용	다른 일반 사용자의 ID 및 패스워드를 도용하는 방법	패킷스니퍼, 패스워드 크랙, 무차별 공격	운영체제 무관
SW 보안취약점	컴퓨터내의 시스템 SW나 응용 SW의 버그등을 이용	phf_CGI, rdist, sdtcm, test-CGI 등	전체 유닉스 및 특정 유닉스
버퍼 오버플로우 취약점	SW 변수관리상의 문제인 오버플로우 버그를 이용 불법으로 명령어를 실행하거나 권한을 가지는 방법	popd,imapd, named, mountd, ftpd, innd, rlogin 등	
구성설정 취약점	시스템 SW의 설치나 운제영상에 취약점을 이용한 공격	r-*명령어, tftp, NFS_export 등	전체 유닉스
악성프로그램	바이러스, 웜, 트로이 목마 등의 불법프로그램 이용	rootkit, back, orifice, CIH virus 등	전체 유닉스 및 특정 유닉스
프로토콜 오류	인터넷의 통신프로토콜인 TCP/IP의 설계 오류를 이용한 구조적인 공격	TCP Hijacking, IP Spoofing 등	전체 유닉스, 운영체제 무관
서비스 거부공격	시스템이나 네트워크의 정상적인 동작과 서비스를 방해하거나 정지시키는 공격	smurf,ping,flooding, SYN flooding 등	운영체제 무관 및 윈도우즈
E-mail 취약점	전자우편 폭탄, 스팸메일 공격	Spammail, Mail bomb	운영체제 무관
취약점 정보수집	시스템의 취약점을 알아내고자 하는 스캔공격	mscan,sscan, redbutton 등	전체 유닉스
사회공학	관리자를 속여 패스워드를 알아내거나 권한을 얻어내는 방법	전화 등을 통해 타인으로 위장하여 ID등을 알아냄.	운영체제 무관

4. 국방정보통신망의 정보보호 적용방안

본 장에서는 이런 해커 공격뿐만 아니라 각종 위협으로부터 효과적으로 대처하기 위한 군 정보통신망의 정보보호대책을 제시하여 해커전을 포함한 각종 위협으로부터의 공격에 대응하기 위한 정보보호 기술 및 적용방안, 기반조성 등에 대해 알아보고자 한다[11][16].

4.1 정보보호 요소기술[14]

4.1.1 보안운영체제의 정의 및 기능과 역할

컴퓨터 운영체제의 보안상 결함으로 인하여 생기는 위험 즉, 각종 해킹이나 기타 악의적인 행위로부터 시스템을 보호하기 위하여 기존 운영체제에 보안기능이 통합된 보안커널(Security Kernel)을 추가한 운영체제로 기능 및 역할은 <표 10>과 같다.

〈표 10〉 보안 운영체제의 기능과 역할

기 능	설 명
식별 및 인증	· 고유한 사용자 신분에 대한 인증과 검증
접근통제	· 강제적 사용통제 : 사용자의 자유재량에 상관없이 강제적으로 접근통제 · 임의적 접근통제 : 사전에 개별 사용자에게 합법적으로 부여한 재량권을 적용하여 접근통제
완전한 중재 및 조정	· 모든 접근경로에 대한 완전한 통제
메모리 재사용 방지	· 메모리에 이전 사용자가 사용하던 정보가 남아있지 않도록 기억장치 공간을 깨끗하게 정리
안전한 경로	· 패스워드 설정 및 접근허용의 변경 등과 같은 보안관련 작업을 수행할 때 안전한 경로 제공
저장파일 암호화	· 저장된 파일에 대한 암호화 지원
감사 및 감사기록 축소	· 보안관련 사건기록의 유지 및 감사기록 보호 · 막대한 양의 감사기록에 대한 분석 및 축소

4.1.2 인증[12]

1) 사용자 인증

사용자 신분에 대한 인증은 다음의 세 가지 방법 중 하나의 방법을 단독으로 사용하거나 2가지 이상의 방안을 조합하여 사용할 수 있다.

- 사용자가 알고 있는 것을 기반으로 한 식별 및 인증방법으로서 비밀 패스워드, 개인 식별번호 (PIN), 또는 암호키 등의 비밀정보 등을 이용한다.
- 사용자가 소유하고 있는 것을 기반으로 하는 식별 및 인증방법으로 ATM 카드, 스마트카드 등의 보안토큰을 이용한다.
- 사용자의 생체학적 특성을 기반으로 하는 인증방법으로서 사람을 식별하기 위해 개인의 독특한 특성 즉, 지문, 홍채, 음성 등을 사용한다.

2) 공개키 기반구조

공개키 기반구조(Public Key Infrastructure)는 전자결재, 전자메일, 전자거래의 안전성·신뢰성을 보장하기 위하여 암호기술과 전자서명 시스템을 이용하여 당사자의 신분확인, 전자업무 내용의 정보보호 및 무결성, 전자행위에 대한 부인봉쇄 기능 등을 신뢰할 수 있는 제 3자(인증기관)가 확인하여 증명할 수 있도록 지원하는 시스템을 말한다.

4.1.3 컴퓨터 바이러스 및 악성소프트웨어 대책

최근 인터넷의 폭발적인 사용증가와 더불어 인터넷을 이용한 컴퓨터 바이러스와 악성소프트웨어의 전염경로는 다변화 되었고 이로 인한 피해규모도 급속도로 증가하였다. 그리고 이러한 상황은 폐쇄망을 운영하는 국방정보통신망에서도 마찬가지가 되었다.

컴퓨터 바이러스와 악성소프트웨어로부터 정보체계를 안전하게 보호하기 위해서는 관리와 기술적인 측면의 대책이 동시에 수립되어야 한다. 먼저 관리적인 대책은 효율적 컴퓨터 관리를 위해 장비의 도입단계에서부터 운영단계까지 수시·정기적인 바이러스 검사를 수행하고, 유사시 피해복구를 위해 시스템의 하드웨어 및 소프트웨어에 대한 상세 정보를 남겨두어 만일의 사태에 대비한다.

기술적인 측면에서는 사용자가 스스로 최신버전의 백신을 주기적으로 다운받아 사용하고, 중요자료 및 프로그램에 대해서 반드시 백업 받아 유사시 업무상 지장을 초래하지 않도록 해야 하며 소프트웨어 사용은 정품을 사용하되 설치 전에는 반드시 바이러스 검사를 실시하여야 한다.

4.1.4 가상사설망(VPN : Virtural Private Network)

가상사설망이란 인터넷과 같은 공중망을 이용하면서도 사설망을 이용하는 것과 같은 효과를 만들어 내는 네트워크를 말한다. 즉, 인터넷과 같은 공중망 사용자간에 터널링(tunneling) 기술을 이용해 터널을 형성함으로써

사용자들에게 공중망을 이용하면서도 사설망을 이용하는 것과 같은 효과를 만들어 낼 수 있는 네트워크를 말한다. VPN에 대한 장점인 우수한 확장성과 망 운영비 절감 측면에서 VPN의 군전산망 적용은 분명고려해 볼 가치가 있다. 특히, 현재 구축되어 있는 각 부대별 LAN을 기반으로 LAN to LAN VPN을 구축 시 한국통신 망 임대료를 절약할 수 있으며, 신규 가입부대에 대한 초기 투자비를 절감할 수 있고, 훈련, 출장 등의 사유로 부대를 이탈 시 에도 망에 접속하여 해당 업무를 처리할 수 있다.

그러나, 군사적 자료의 특성상 보안에 중점을 두지 않을 수 없으므로 현재 민간 기업에서 적용하는 VPN의 기능에 추가적인 보안대책이 필요하다. 즉, 국방부에서 구축 계획인 국방인증기관의 인증, 암호화 기능을 이용한 보안기능 강화 등의 조치가 필요하다.

4.1.5 침입차단시스템

침입차단시스템의 사용목적은 외부 네트워크의 해킹과 같은 정보보호 위협으로부터 내부 네트워크를 보호하는 것으로 내부 네트워크에 허가되지 않은 사용자가 정보에 접근하는 것을 방지하고, 허가된 사용자들이 별다른 어려움 없이 네트워크 자원을 이용할 수 있도록 보장해준다.

일반적인 침입차단시스템의 장·단점은 <표 11>과 같다.

〈표 11〉 침입차단시스템의 장단점

장 점	단 점
· 취약한 서비스에 대한 보호 가능 · 호스트 시스템에 대한 접근 제어 가능 · 로그와 통계자료 유지 · 내부 네트워크상의 모든 자원들에 일관된 보안정책 적용 가능	· 제한된 서비스 제공 · 침입차단시스템을 통과하지 않는 트래픽은 제어불가 · 악의적인 내부자들로부터 시스템 보호 곤란 · 바이러스 및 새로운 형태의 위험에 대한 방어 곤란

4.1.6 침입탐지시스템(Intrusion Detection System)

침입탐지시스템은 내부 사용자 및 외부 침입자의 컴퓨터 시스템과 네트워크 자원 불법사용이나 주어진 권한 밖의 자원 접근 시도를 사전에 탐지하여 그 피해를 예방하는 시스템이다.

일반적인 침입탐지시스템의 장·단점은 <표 12>와 같다.

〈표 12〉 침입탐지시스템의 장·단점

장 점	단 점
· 해킹에 대하여 침입차단시스템보다 적극적인 방어 가능 · 내부 사용자의 오·남용 탐지 및 방어가능 · 해킹사고 발생시 어느 정도의 근원지 추적 가능	· 대규모 네트워크 상에서는 사용곤란 · 관리 및 운영 어려움 · 새로운 침입기법에 대한 즉각적인 대응 곤란 · 보안사고에 대한 근본적인 대책은 되지 못함.

4.1.7 방화벽(FireWall)

방화벽이란 2개의 네트워크 사이에서 접근제어 정책을 구현할 수 있도록 하는 시스템이나 시스템들의 집합이다. 방화벽에서 가장 중요한 요소는 네트워크의 접근과 차단의 규칙을 정해놓은 "방화벽 정책"수립으로서 얼마만큼 방화벽 정책을 부대환경에 맞게 설정하느냐에 따라 보호 수준이 달라질 수 있다. 방화벽 정책은 주요 기능인 네트워크 접근여부를 결정하는 규칙 테이블로, 네트워크 보호수준을 결정하는 중요한 요소이다. 방화벽 정책은 모든 것을 허용할 것인지, 모든 것을 거부할 것인가부터 결정을 한다.

4.1.8 통합보안관리시스템

통합보안관리시스템(Enterprise Security Management System)은 침입차단·탐지시스템, 바이러스 월 등 다른 기종의 보안 솔루션을 중앙에서 통합 관리하는 시스템으로 솔루션간 상호연동을 보장하고 시스템 전체에 대해 보안정책 수립과 이행이 가능하도록 지원하는 보안 솔루션이다. 우리 군의 국방정보체계 정보보호 능력 강화를 위해서는 다양한 보안솔루션 사용은 필연적이므로 다른 기종의 보안솔루션간의 상호운용성 보장과 효율적 관리를 위해서 통합보안관리시스템 도입이 반드시 요구된다.

4.2 해커전에 대비한 정보전 대응 정책수립

해커전에 대응하기 위해서는 국방정보통신망의 데이터를 어떻게, 어떤 수준까지 보호할 것인가에 대한 방어적 의미의 정보전 대응책을 수립해야 하는데 이것을 정보전의 의미로 본다면 방어적 의미의 정보전이라 할 수 있다. 이 대응 단계를 3단계로 구분하면 ①보안정책(Security policy)수립, ②보안계획(Security planning) 수립, ③계획 구현(Inplement the Plan)으로 볼 수 있다. 이

와 같은 계획에 의해 대응책을 수립한다면 군 정보통신망을 보호 할 수 있을 것이다[15].

4.2.1 해킹방지 대책

해킹에 대응하기 위해서 시스템 관리자는 두 가지 관점에서 시스템을 점검할 수 있는 능력을 갖추어야 한다.

첫째, 관리자 관점에서 시스템 로그파일을 분석하여 비정상적인 활동을 파악할 수 있어야 하며, 주요서버의 로그정보 분석에서는 접속로그나 에러로그 파일을 점검하여 외부 침입자가 시스템내의 주요 파일을 가져갔는지 파악한다.

둘째, 공격자 관점으로 트로이목마 등의 프로그램을 점검하여 /bin, /usr/bin,/usr/local/bin 등의 실행 파일을 담고 있는 디렉토리 파일들에 대한 변형유무를 점검하고, 숨겨져 있는 디렉토리를 확인한다.

한편, 각종 서버의 원격취약점검으로 시스템의 취약점을 해커의 관점에서 점검하고 최신 해킹기법의 습득을 위해 해킹그룹사이에서 교환되는 관련 프로그램을 확보한다.

또한 발견된 해킹프로그램들은 데이터베이스화 하여 지속적으로 관리한다. 주요 해킹 수법별 방지대책은 <표 13>과 같다.

〈표 13〉 주요 해킹 수법별 방지대책

수 법 분 류	대 책
사용자 도 용	· 사용자 도용의 대표적인 공격인 크랙 및 스니핑에 대응하기 위해 Shadow/일회용 패스워드를 사용하거나 암호화된 패스워드를 사용하며, 사용중인 패스워드는 유추할 수 없도록 작성한다.
버퍼 오버플로우 취약점	· 우선 프로그램 작성시 버퍼 오버플로우가 일어나지 않도록 하는 것이 가장 중요하며 수동적인 방법으로 시스템회사에서 작성한 패치를 이용하는 것도 있으며, 운영체제의 커널을 수정한다.
악성 프로그램	· 네트워크 트래픽 모니터링, 점검, 파일시스템을 주기적으로 점검하여 최신 백신소프트웨어를 사용하고 물리적 보안활동을 강화한다.
취약점 정보수집	· 보안취약점 점검도구가 급속도로 전파되고 있는 상황에서 뚜렷한 대책은 없으나 자신의 시스템을 주기적이며 지속적으로 점검하여 발견된 취약점을 수정한다.

4.3 정보전에 대비하기 위한 대책

합리적이고 실질적인 국방정보보호체계가 구축되기 위해서는 기술적 대책 뿐만 아니라 정보보호 관련된 제도 및 규정의 정비, 정보보호 조직의 정비와 보완, 정보전 관련 담당 조직 및 담장자 임명, 정보전에 대한 인식변화, 침해사고 대응 종합상황실 운영, 정보전 대응 훈련의 정례화, 교육 및 훈련 등의 정보전 대응체계 구축을 위한 과제를 우리는 가용한 범위 내에서 단계적으로 선정하여 추진해 나가야만 효율성 높은 국방정보보호체계를 구축할 수 있을 것이다[9].

5. 결론

전통적으로 군은 정보보호의 중요성을 인식하고, 관련된 활동이나 기술, 체계를 개발, 구축, 운용하여 왔다.

그러나 군 정보화의 추진과 군 정보화 추진에 따른 군내 정보화가 확대되는 현실에서, 최근 증가되는 정보침해의 위협은 전통적인 정보보호의 범위 및 수준에 대해 새로운 인식 변화와 활동의 필요성이 커지고 있으나, 아직 정보보호에 대한 종합적인 대책이 미흡한 실정이다.

현재, 군은 정보보호를 위한 조직 및 전문 인력이 매우 부족한 현실이며, 체계적인 기술개발 및 체계 구축 계획 수립이 부족하여 단위 목적별 보호체계를 도입, 운용하고 있는 실정이라고 할 수 있다. 따라서 정보보호는 미래 정보전 수행능력 확보차원에서 단계적, 체계적으로 추진되어야 할 것이다. 정보전 수행에 적합한 조직을 단계적으로 구성하여야 하며, 전문 인력은 특별프로그램을 통하여 확보하고 유지하여야 할 것이다.

또한 이와 더불어 정보통신 기반체계를 개발할 때 핵심적으로 고려해야 할 사항이 보안대책이다. 여기에서는 공개, 고유 및 분산 능력을 유지하면서 보안기능이 이루어져야 한다. 망의 이동, 망의 재구성, 가입자의 이탈 및 재 가입 등이 수없이 이루어지는 상황 하에서도, 또 이를 지원하기 위해서, 특별한 보안대책을 마련해야 할 것이다. 현재, 우리 군은 비화망과 비비화망 구분에 대한 명문화된 기준이 없으므로 용도별 데이터통신망(CPAS망, 국방정보통신망, 군사정보망)을 물리적으로 구분하여 구축 및 운영하고 있다. 따라서 통신망간 정보 유통 및 공유가 제한되고 별도 통신망구축에 따른 중복투자 요소가 상존하고 있다. 용도별 데이터통신망의 장거리 전송구간은

동일한 비화장비를 사용하여 비화를 수행하고 있다.

단기적으로 용도별 데이터통신망의 장거리전송구간은 별도의 백본망을 구성하지 않고 ATM 기반의 국방 정보통신망으로 통합 및 수용하여 ATM 기반 가상 사설망(VPN)으로 구성, 용도별 통신망의 보안성을 유지하고, 부대내 통신망 구간에서 정보보호 체계를 도입하여 개별적으로 구축된 용도별 통신망간 상호연동을 추진하되 상호연동은 정해진 지점에서만 가능하도록 하여 중앙 집중적인 보안통제를 보장해야 한다.

중/장기적으로는 WAN과 LAN 전 구간에서 통합된 단일의 통신망 상에서 용도별 데이터통신망을 고도의 정보보호체계(다단계 보호체계, 가상사설망, 가상 LAN 기술 등)를 통하여 논리적으로 구분, 운영하는 방향을 발전시켜야 한다. 현재까지 국방통신망은 전용회선 서비스를 이용, 상용통신망과 분리되어 있었고, 군 내부에서도 각 군/기관/기능별 통신망을 각각 전용회선 서비스를 이용하여 구축 및 운용해 왔으므로, 암호화를 위한 보안장비 이외에 침입방지체계(방화벽), 침입탐지체계와 같은 접근통제기술을 적극적으로 활용할 필요가 없었다. 하지만 국방정보통신망은 다양한 사용자 통신망을 상호 연동 및 통합하는 방향으로 발전하고, 중/장기적으로는 인터넷과 같은 민간 통신망에도 연동될 것이다.

따라서 상이한 용도 및 비밀등급의 정보가 상호 연동된 통신망을 통하여 유통될 것이고, 인가되지 않은 사용자가 컴퓨터 자원, 통신자원 및 정보자원 등에 불법적인 접근과 훼손을 시도할 수 있으므로,암호화를 위한 보안장비 이외에 방화벽, 사용자 인증체계와 같은 침입방지체계, 침입탐지체계와 같은 수세적 정보보호체계를 적극적으로 도입하여 용도별 통신망간 정보 유통 및 공유를 보장하면서 컴퓨터 자원, 통신자원 및 정보자원을 보호해야 한다. 또한, 보안기록파일 등을 이용한 보안감사 추적체계 도입과 정보전 공격에 대한 적극적 대응능력을 갖춘 공세적 정보보호 조직을 구성하여 정보전에서 군 내부와 외부의 가상 적에 대한 적극적인 공격과 방어가 가능하도록 정보보호체계를 발전시켜야 한다.

참 고 문 헌

[1] 국군기무사령부(2012), 군사보안업무 시행규칙 해설집

[2] 국방과 기술(2005), 지휘 및 통제무기체계 발전방향(육군 전술지휘통제체계) 55-74.

[3] 국방대학원 논문(2001), WEB 환경에서의 국방정보통신망 정보보호체계 구축에 관한 연구

[4] 국방대학원 논문(2004), SSE-CCM을 이용한 해군 전술 C4I 사업 정보보호감리지침에 관한 연구

[5] 국방과학연구소(2002), C4ISR 최근 동향

[6] 국방부 정보체계국(1998), 국방정보통신망 관리지침

[7] 국방부(1993), 전산통신망 프로토콜 구조

[8] 국방부(2002), 육군 C4I 사업전략

[9] 미 해군 E.A. Smith, Jr. 박사, 네트워크중심전쟁 : 무엇을 얻고자 하며 어떻게 얻을 것인가?

[10] 우희철 (2006). 미래정보전에 대비한 국방정보통신망 정보보호대책 연구. 석사학위논문, 아주대학교.

[11] 육군 교육 사령부(2004), 정보보호체계 구현 방안

[12] 정보통신부(1996), 네트워크 보안관리 지침서

[13] 한국전자통신연구원(1999), “21세기 정보전을 대비한 정보보안체계 구축 전략,” WISC '99논문집,

[14] 한국정보보호센터(1999), 통신망 정보보호대책 연구

[15] 한미연합사령부(1999), 한반도 정보작전

[16] 합참 작전참모부(1996), 국가 정보화 발전전략,

[17] 합참(2001), 미군의 C4I 전략 / 사업,

[18] 합참(1998), 합동 C4I 체계

[19] Edward Waltz(1998), Information Warfare Principles and Operations, Artech House,

[20] Martin C. Libicki(1995), What is Information Warfare?. National Defense University,

우 희 철

- 2007년 8월 : 육군 소령(정보 병과) 전역
- 2000년 2월 : 서울시립대학교 국제관계학과(정치학사)
- 2006년 8월 : 아주대학교 정보통신대학원 C4I/정보보호과(공학석사)
- 2009년 8월 : 명지대학교 북한학과(정치학 박사)
- 2012년 10월 현재 : 문경대학교 부사관과 교수
- 관심분야 : 북한학, 군사학, 정보전
- E-Mail: leewhc@yahoo.co.kr