C4I 시스템 보안 로드맵 설계

이강택* · 이동휘* · 양재수** · 김귀남* · 박상민***

요 약

C4I 시스템은 군의 핵심전력이자 중추 신경계이다. C4I 시스템은 정보 그리드, 정보의 생산·분배에 사용되는 정보기반체계로 전장공간의 모든 전투요소를 정보 네트워크로 연결하여 실시간 전장정보와 인식의 공유를 가능하게 하여 과거 플랫폼중심의 전쟁개념을 네트워크 중심전(NCW)으로 근본적인 전쟁패러다임변화를 유도하였다. 이러한 군 핵심전력인 C4I 시스템이 적의 사이버 공격대상이 될 것임이 자명함에도 불구하고 그 대비책은 거의 부재한 실정이다.

본 논문은 전·평시 사이버 공격의 핵심목표가 될 C4I 시스템 보호책 마련을 위한 보안 로드맵을 설계하였다. 본 로드맵은 C4I 시스템 보호를 위한 비전과 목표에 대한 지원 프레임워크를 제시하고 있으며, 합참 및 방사청에서 적절한 프로그램을 선정하고 투자하여 신속하고 효율적인 보안시스템 구축이 가능하도록 한다.

Design of Security RoadMap for C4I System

Gang-Taek Lee* · Dong Hwi Lee* · Jae Su Yang**
Kuinam J. Kim* · Sang Min Park***

ABSTRACT

C4I system is the centerpiece of the military force. The system is an information based system which facilitates information grid, collection of data and dissemination of the information. The C4I system seeks to assure information dominance by linking warfighting elements in the battlespace to information network which enables sharing of battlespace information and awareness; thereby shifting concept of warfare from platform-centric paradigm to Network Centric Warfare. Although, it is evident that C4I system is a constant target from the adversaries, the issues of vulnerability via cyberspace from attack still remains. Therefore, the protection of C4I system is critical.

The roadmap I have constructed in this paper will guide through the direction to protect the system during peace and war time. Moreover, it will propose vision, objectives and necessary supporting framework to secure the system from the threat. In order to fulfill these tasks, enhanced investments and plans from the Joint chief of Staff and Defense of Acquisition and Program Administration (DAPA) is critical; thereby enabling the establishment of rapid and efficient security system.

Key words : C4I, Security RoadMap

* 경기대학교 정보보호학과
** 광운대학교 산학협력단
*** 인천대학교 산업경영학과

1. 서 론

정보통신기술의 급격한 발달은 전장공간의 모든 전투요소를 정보 네트워크로 연결하여 실시간 전장정보와 인식의 수평적 공유를 통해 네트워크 중심전(NCW : Network Centric Warfare) 기반의 효과중심작전(EBO : Effects Based Operation)으로 전쟁패러다임변화를 유도하고 있다. 이에 따라 우리 군은 새로운 전쟁패러다임에 부합하고 군 전력구조 및 체계 혁신을 통하여 정예 정보화 군을 양성하기 위한 합동 C4I(Command Control Communication Computer and Intelligence)체계 건설을 계획대로 진행하고 있다.

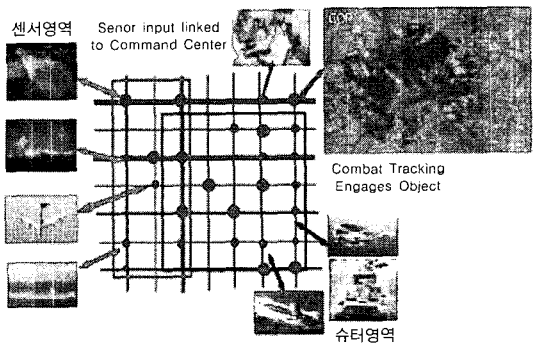
한편, 국방정보화의 추진에 따라 다양한 정보통신 기술이 활용됨으로써 정보통신기술에 내재된 취약성을 이용한 사이버 공격이 증가하고 있으며, 이에 따른 피해도 점차 증가하고 있는 실정이다. 특히 C4I 시스템을 대상으로 한 해킹 및 악성코드 살포와 같은 유형의 공격 위협은 주요 무기체계 통제의 기반이 되는 컴퓨터시스템에 대한 치명적 타격을 입힐 수 있으며, 이는 국방의 주요 정보자원 및 정보체계에 막대한 악영향을 미침으로써 전쟁을 수행할 수 없는 상황을 만들 것이다. 이처럼, 정보보호 및 사이버전 대응 능력 확보가 선진·자주 국방으로 나아가는 선결과제임에도 불구하고 상호운용성을 통한 각 군 C4I체계의 효율적 통합운용에 주안점을 두고 있을 뿐, 전·평시 적 사이버 공격의 핵심목표가 될 C4I체계에 대한 보호책 마련에는 소홀한 실정이다.

본 연구는 'Security' 보장 없는 C4I 시스템의 운용은 치명적인 결과를 초래할 수 있다는 절박한 인식하에 보안 로드맵 설계를 목표로 하였으며, C4I체계 보호를 위한 각 단계별 목표, 추진방향, 세부추진과제를 제시하였다. 이러한 전략적 프레임워크를 통해 합참 및 방사청에서 적절한 프로그램을 선정하고 투자토록 함으로써 신속하고 효율적인 사이버전 수행이 가능하도록 하였다.

2. 관련 연구

2.1 전쟁 패러다임 변화

지난 걸프전에서부터 이라크전을 거치면서 첫 고통신기술을 중심으로 하는 천담과학기술들은 기존의 플랫폼 중심(PCW : Platform Centric Warfare)에서 네트워크중심전(NCW : Network Centric Warfare)으로 전쟁개념을 바꾸어 놓았다. 군사력을 통한 대규모 물리적 파괴 중심에서 정보·감시·정찰(IRS)의 센서체계, C4I 중심의 의사결정체계, 그리고 장거리 정밀유도무기(PGM) 중심의 슈터체계를 네트워크체계화 하여 효과중심의 전쟁을 수행함으로써 적의 전쟁지속의지 무력화를 통해 전쟁목표를 조기에 달성하자는 것이다[1]. 이러한 변화에 부합하고자 우리군도 NCW 수행을 위한 센서체계와 슈터체계를 통합한 C4I 중심의 복합체계구축을 추진 중에 있다.

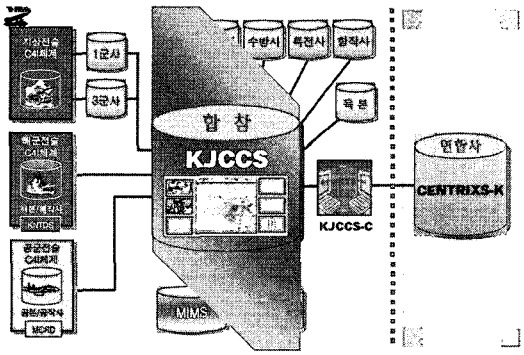


(그림 1) NCW 개념도

(그림 1)은 다양한 센서들에 의해 수집된 정보들이 네트워크 기반의 정보노드간 공유를 통해 COP(Common Operation Picture : 공통상황도)를 생성하면, 지휘본부는 COP를 통한 실시간 전장을 지휘하며, 효과적인 슈터를 운용함으로써 전쟁목표를 달성하는 NCW 수행개념을 설명하고 있다.

2.2 C4I체계 현황

NCW 수행체계를 구축하기 위하여 우리 군은 각군 전술 C4I개발 사업을 수행 중에 있으며, 합참을 중심으로 실시간 전장정보 공유, 공통작전상황 인식, 지휘결심 지원 등을 위해 합동지휘통제체계(KJCCS : Korean Joint Command & Control System) 개발사업을 추진 중에 있다.

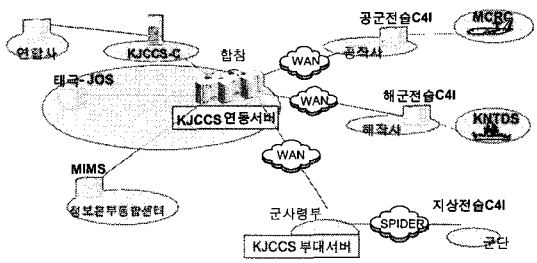


(그림 2) 합동지휘통제체계 구성도

(그림 2)는 합동지휘통제체계 구성도로서 각 군 전술 C4I체계, 군사정보통합처리체계인 MIMS, 합동 워게임 훈련체계인 태극-JOS, 그리고 연합사 C4I체계인 Centrixs-K 등이 상호 연동하게 됨으로써 합참 중심의 NCW를 수행하게 된다.

C4I체계 구축과 더불어 범국가적으로 추진하는 광대역통합망(BcN) 구축과 연계된 다양한 네트워크 기술을 수용하기 위해 ATM망 중심에서 IP망 중심으로 '국방정보통신망 ALL-IP화'를 추진중에 있다[2].

따라서 C4I체계의 네트워크 중심 설계는 IP를 이용하는 거대하고 포괄적인 정보시스템들이 상호 연결되어 다수의 자동 전송시스템을 갖게 된다. 지금까지는 비 IP 시스템과 군사용 어플리케이션, 그리고 국방망과 같은 독자적인 폐쇄망 시스템을 사용하였으나, 이제 상호운용성과 더불어 지속적인 비용 절감과 위험을 줄이기 위해 개방형 및 보호형 프레임워크를 사용해야 할 것이다.



(그림 3) 차세대 국방정보통신망 구성도

(그림 3)은 합참지휘통제체계(KJCCS)를 중심으로 하는 IP망 구성도를 나타내는 것으로 IP망간 끊임없는 정보소통을 보장하고, 생존성 및 보안성을 확보하기 위한 노력이 병행되어야 한다.

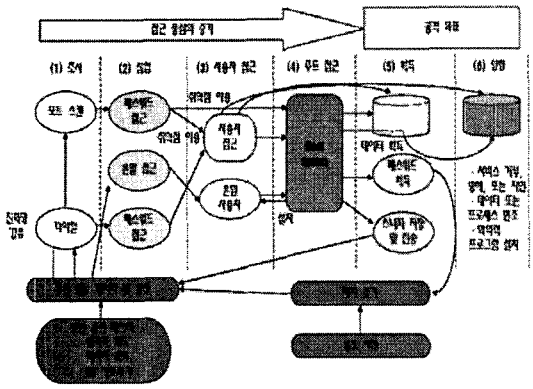
2.3 C4I체계 위협 분석

국방정보통신망의 ALL-IP망화를 추진함에 따라 군 지휘체계의 중추신경이라 할 수 있는 C4I체계는 현 독립 국방망 운용 시보다 적의 사이버 위협에 더욱 노출될 것이다.

적의 사이버 위협(공격) 행위는 바로 정보전 수행이라 볼 수 있으므로, 본 연구에서는 Edward Waltz의 "정보전-원칙과 운용" 중에서 '네트워크 공격 프로세스를 6단계' 이해를 통해 C4I체계 위협요소를 식별하였다.

(그림 4)와 같이 공격 프로세스는 총 6단계인 조사(Probe), 침입(Penetration), 사용자 접근(User access), 루트접근(Root access), 획득(Capture), 영향(Affect)이다[4].

먼저, 1단계는 조사단계로 인터넷이나 기타 통신을 통해 접근 가능한 취약한 지점을 포트 스캔과 같은 도구를 이용해 조사하는 단계이다. 2단계는 침입단계로 가용한 네트워크의 접속점을 찾아 접속을 시도하는 것으로 이미 알려진 취약점을 이용하거나 이미 획득한 정보를 이용해 정상적인 접



(그림 4) 네트워크 공격 프로세스

근을 시도하는 단계이다. 3단계는 사용자 접근단계로 합법적 또는 시스템 취약점을 이용해 사용자 접근에 성공하는 단계로 상당한 수준의 시스템 자원의 조사와 이용이 가능한 상태에 도달하게 된다. 다음으로 4단계인 루트단계는 시스템의 루트 권한을 획득하는 것으로 악의적인 행동을 즉각 수행할 수 있는 모든 통제권한을 가진다. 그리고 5단계인 획득단계는 스니퍼 프로그램을 설치하거나 관리자용 파일 또는 암호화된 패스워드 파일 등을 탈취하고, 새로운 사용자 계정을 만들어 둘 수 있는 단계이다. 마지막 단계로 영향단계는 표적시스템 내의 정보와 프로세스를 거부, 파괴, 방해하여 의도하였던 악의적 행위의 목적 달성하는 단계이며, 차후 지속적인 공격행위 수행을 위해 악의적인 프로그램을 설치해 두는 단계이다.

이러한 네트워크 공격 프로세스는 일반 해커들의 공격 프로세스와 거의 흡사하며, 네트워크 기반의 C4I체계에 대한 공격 행위 또한 이와 같은 프로세스를 통해 수행 될 것이 확실시 된다. 따라서 지금까지 알려진 공격유형과 내용에 대해 알아봄으로써 C4I체계 및 국방정보기반체계에 대해 어떠한 유형의 공격들이 일어날 수 있는가에 대한 이해를 돕고자 한다. <표 1>은 대표적 공격유형을 정리한 것으로 센서 및 슈터, 컴퓨터 및 네트워크의 연동/통합 증가 및 유비쿼터스 환경 확대에 따라 센서, 전투원, 네트워크, 장비, 소프트웨어 등 보호대상 급증하고, 하나의 네트워크에 대한 국지적 사이버 공격이 다른 네트워크 또는 전체 네트워크로 확산이 가속화되며, 모든 전장 기능 및 전술적 구성 요소가 전자화·자동화 및 무선·이동 환경으로 변화됨에 따라 예상치 못한 공격 패턴의 등장과 피해가 급증할 것으로 예상된다[3].

제 2장에서는 C4I체계에 대한 이해와 예상되는 공격유형에 대해 알아봤으며, 다음 제 3장에서는

〈표 1〉 공격유형 분석

공격유형	내 용
내부자 공격 (Insider)	• 정보보호 처리 시스템의 물리적 경계 내에 있거나 직접적인 접근 권한을 갖고 있는 인가된 사람에 의해 수행되는 공격 (예) 데이터 및 보안메커니즘 변경, 비밀채널 설정, 물리적 파괴 등
수동적 공격 (Passive)	• 시스템 및 네트워크에서 유통되는 데이터와 이를 통해 추출 가능한 정보를 수동적으로 감시하는 공격 유형 (예) 정보의 모니터링, 스니핑, 암호문 분석 등
능동적 공격 (Active)	• 일반적으로 알려진 대표적인 공격 유형으로, 보호수단의 우회/파괴, 악성코드 삽입, 정보의 탈취·변조·삭제 등과 같이 정보나 정보시스템의 기밀성, 가용성, 무결성에 직접적인 영향을 미치는 공격 유형 (예) 정보 위변조, 사용자 가장, 서비스 거부공격 등
근접 공격 (Close-in)	• 인가되지 않은 자가 정보를 변조, 수집하거나 정보자산에 대한 정상적인 접근을 방해하기 위한 목적으로 네트워크, 시스템 또는 시설에 물리적으로 접근하여 수행하는 공격 (예) 데이터 변경/수집, 시스템 변경, 물리적 파괴 등
배포 공격 (Distribution)	• 생산에서부터 설치까지의 과정 중이나 사이트 간 이동 중에 악의적인 목적으로 하드웨어나 소프트웨어를 수정, 변경하는 공격 유형 (예) S/W, H/W의 악의적 수정, 백도어 설치 등

C4I체계 보호 및 사이버전의 효율적 수행을 위한 보안 추진중점에 대해 진단해 보았다.

3. C4I체계 보안 추진중점

보안 추진중점 분야를 정책 및 제도, 조직 및 인력, 운용체계, 그리고 기술 연구개발 등의 4분야로 진단하였으며, 각 분야별 추진목표, 추진방향, 세부추진과제를 제시하였다.

3.1 정책 및 제도 발전

먼저, 정책 및 제도 분야 발전을 통한 C4I체계 보안 추진중점은 아래 <표 2>과 같다.

〈표 2〉 정책/제도 분야 추진중점

구 분	내 용
추진목표	국방정보화 환경변화 및 미래전에 부합하는 국방정보보호 정책 및 제도 수립·발전
추진방향	• 전술 C4I체계 및 정보통신망 등 국방정보자원과 정보통신기반체계를 보호·방어하기 위한 관련 정책 및 제도 발전 • 첨단 정보보호기술 및 관련 전문가를 국방분야에 도입·활용하기 위한 정책 및 제도적 지원 기능 강화 • 사이버전 대응체제 구축을 위한 정책 및 사이버전 교리 개발
세부 추진과제	• 다차원·다계층 정보보호 정책 및 제도 수립 • 국방정보체계 안전성 수준 관리절차/제도 정립 • C4I체계 보호를 위한 기술소요 지원 정책 및 제도 강화 • 다차원·다계층 정보보호 추진전략구현을 위한 기술구조 및 참조기준 지침서 등 개발 및 배포 • 적의 사이버 공격에 대한 대응체계 구축을 위한 국가적 차원의 사이버전 수행정책 정립 및 관련 관계법령 및 제도 정비 • 합참 및 각군의 사이버전 교리 개발 및 수행 지침서/절차서 발간

정책 및 제도 분야는 C4I체계 특성상 국방망, 인터넷, 전략전술망 등의 다양한 정보통신망 환경하에서 병사용 휴대 단말기부터 첩보위성에 이르기까지 다차원의 정보센서 및 노드, 그리고 하위 제대부터 합참에 이르기까지 다계층의 정보보호대상 영역을 식별하고 이에 대한 체계적인 다차원·다계층 정보보호 추진전략 수립이 필요하기 때문에 이와 관련된 보안대책 검토, 보안성 평가, 보안측정 등 기존 정보체계 보안관리 활동을 정보체계 수명주기 활동과 유기적으로 연계시켜고, 정보체계의 안전성 수준을 제고하기 위한 관리절차 정립 및 정보체계 획득 운영시 안전성 확보를 위한 공통평가기준(CC) 수립 및 검증제도 정립 등의 정책 및 제도분야 발전을 도모하는 것이다.

3.2 조직 및 인력 강화

다음은 조직 및 인력 분야 발전을 통한 C4I체계 보안 추진중점으로 <표 3>와 같다.

〈표 3〉 조직/인력 분야 추진중점

구 분	내 용
추진목표	C4I체계 보호중심의 사이버전 수행 조직 정비 및 전문인력 보강
추진방향	• 조직 진단을 통해 중앙집중식 정보보호 조직으로 통합 • 사이버전 정책연구 및 방어/공격 대응능력 보강을 위한 기술 연구조직 신설 또는 강화 • 조직별 운용요원 체계적 전문화 관리 • 첨단 신기술 개발·유지 및 확보를 위한 자체 전문인력 양성
세부 추진과제	• 국방부 정보화기획관실 중심의 정책 전담조직 신설 • 합참 지통부 중심의 국방기반체계 보안 전담조직 신설 • 국방CERT팀 조직 강화 • 국가차원의 사이버전 수행조직 구축 • 아웃소싱을 통한 보안 연구조직 강화 • 전문교육기관 신설 또는 군내 교육기관을 통한 체계적 교육 및 전문인력 양성

현재, 국방부 정보화기획관실의 기능이 매우 미약한 실정이므로 이에 대한 보강이 우선되어야 한다. 즉 국방부 정보화기획관실 내에 국방차원의 정보보호 관련 정책을 수립 추진할 조직 신설이 필요하며, 이를 중심으로 합참 및 각군 지통부에 있는 정보보호과 조직 보강을 통해 정책 업무를 중앙집중식으로 수행하도록 해야 한다. 또한 합참 지통부 중심의 국방기반체계, 국방정보통신망 및 전술 C4I체계 등에 대한 보호를 위한 전담조직이 신설되어야 하며, 국방CERT팀은 C4I체계 특성상 다차원·다계층의 보안이 요구되는바 각군 예하부대까지 조직을 확대하여 운용되어야 한다.

국가차원의 사이버전에 대비하기 위해 국내외 유관기관간 공조체계를 구축하여 협력 프로그램 개발 및 연구개발 협력체계를 구축해 나가며, 아웃소싱을 통해 부족한 연구조직을 보완해 나가는 것이 바람직하다. 그리고 정보보호 및 사이버전 관련 전문교육기관 신설을 통해 안정적인 전문인력 양성을 통한 조직의 질 향상을 도모하고 군내 교육기관에 교육과정 개설을 통해 지속적인 정보보호인력을 획득해 나가야 할 것이다.

3.3 효율적 보안 운영체계 구축

다음은 보안 운영체계 구축을 위한 추진중점으로 <표 4>와 같다.

날로 다양화, 지능화, 첨단화되는 사이버위협에 능동적으로 대응하기 위해 보안 관련 운영체계는 지속적으로 기능 및 성능을 개선해 나가야 한다. 특히 네트워크 보안관제 중심의 현 보안관제체계를 시스템 보안관제 수준까지 확장하고 그 기능을 강화해야 할 것이다. 또한 현재 추진중인 KJCCS 및 각군 전술C4I 개발사업시 사이버위협에 대한 대응 보안관제체계가 병행되어 구축되어야 한다. 아울러 사이버전 수행역량 강화를 위한 사이버 워게임 모의모델을 개발하여 운영하기를 권장한다.

〈표 4〉 보안 운영체계 추진중점

구 분	내 용
추진목표	국방정보체계에 대한 능동적 보안 운영체계 구축
추진방향	• 기술 발전추세에 따라 관제체계, 방역체계, 인증체계 등 정보보호체계 업그레이드 추진 • 사이버 위협에 대한 정보 분석, 융합, 공유 및 의사결정 지원체계 구축 • 사이버전 수행능력 확보 및 강화를 위해 모의 모델을 활용한 모의훈련체계 구축
세부 추진과제	• 사이버위협 탐지 및 대응체계 강화 - 보안관제체계 성능 개선 - 사이버위협 예·경보 및 공유체계 구축 - 합참중심의 사이버전 의사결정지원 체계 구축 - 사이버 공격체계 구축 - 사이버전 모의훈련체계 구축 • 정보보호 기반체계 강화 - 인증체계 적용 확대 및 성능 개선 - 바이러스방역체계 성능 개선 - 유무선 네트워크 관리체계 구축

3.4 핵심기술 연구 및 개발

마지막으로 기술 연구 및 개발 분야 발전을 위한 추진중점으로 <표 5>와 같다.

〈표 5〉 기술 연구/개발 추진중점

구 분	내 용
추진목표	우리군 실정에 맞는 사이버전 대응 기술 연구 개발 및 적용
추진방향	• 사이버전 수행에 필요한 핵심기술 개발 • 체계 구축에 요구되는 소요기술 및 첨단기술 연구 개발 • 국내외 기관간 협력체계 구축을 통한 첨단기술 도입 및 공동연구 프로젝트 추진
세부 추진과제	• 사이버위협 탐지·대응 기술 개발 • 정보보호 기반기술 개발

정보보호 및 사이버전 관련 기술들은 다양하나, 우리군의 특수성과 실정에 맞는 핵심 기술 개발이

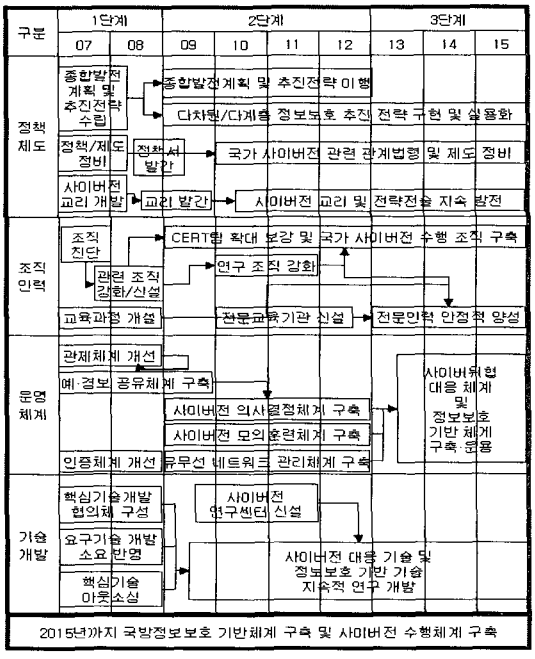
요구되며, 사이버위협 탐지·대응 기술과 정보보호 기반기술로 나눌 수 있다.

이밖에도 알려지지 않은 위협에 대응하기 위한 첨단기술 개발과 관련한 지속적인 연구와 노력이 필요하다. 특히 국정원과 정통부, 국가보안기술연구소 및 한국전자통신연구원, 정보보호학과 관련 대학 등과 지속적인 협력과 교류를 통해 첨단기술을 적극적 받아들이는 노력이 필요하다. 이를 위해 관련기관과 MOU를 통해 전문요원 상호교류, 교육과정 상호 참여, 공동연구 프로젝트 수행 등의 실질적인 활동이 이루어져야 할 것이다.

지금까지 C4I 보안을 위해 식별한 4분야 추진중점을 알아보았으며 이를 바탕으로 다음의 보안 로드맵을 설계하였다.

4. C4I체계 보안 로드맵

C4I 시스템 보안 로드맵 설계는 C4I체계를 중심으로 하는 종합적인 국방정보보호 및 사이버전 수행 체계 구축의 로드맵으로서, 정책 및 제도, 조직 및 인력, 운영체계, 기술 연구 및 개발 등의 4분야로 구분된다. 또한 단기 및 중·장기 구분하여 핵심추진과제를 제시함으로써 로드맵을 이행하기 용이하도록 하였다.



(그림 5) C4I체계 보안 로드맵

(그림 5)은 완성된 로드맵으로 1단계는 최초 시행 2년간으로 기반조성단계라 할 수 있으며, 2단계는 다음 4년간으로 내실화를 통한 역량강화 단계 및 구체화 단계라 할 수 있고, 마지막 3단계는 국방정보보호체계 및 사이버전 수행체계의 완성단계이다.

V. 결 론

과거 대량파괴 위주의 전쟁에서 정보와 지식의 네트워크화를 통한 첨단과학기술전으로 전쟁양상이 변화되고 있으며, 특히 '정보우세'는 전쟁 수행의 핵심요소로 군정보화의 중요성이 날로 높아지고 있다. 우리군도 NCW 수행을 위해 C4I체계를 구축중에 있으며, 네트워크 중심으로 국방기반체계가 설계됨에 따라, 향후 ALL-IP망을 이용하는 거대하고 포괄적인 시스템들이 상호 연결되어 운용될 것이다.

따라서 네트워크화 된 국방전력이 적의 사이버 공격 대상이 될 것은 너무나 자명한 사실이며, 적의 사이버 공격에 의해 국방정보체계가 작전 불능 상태로 된다면 상상할 수 없는 심각한 결과를 초래할 것은 분명하다.

그럼에도 불구하고, 군은 사이버전의 중요성과 그 피해의 심각성을 제대로 인식하지 못하고 있으며, 각군 전술 C4I체계 구축사업 등 국방정보화를 추진함에 있어 정보보호 대책이 병행되어 이루어지지 않음에 따라, 심각한 적의 잠재적 사이버위협을 내포하고 있는 실정이다. 또한, 아직 국방정보보호와 관련한 종합적인 추진 전략 및 정책이 미흡할 뿐만 아니라, 사이버전에 대비한 인프라 구축이 미비한 실정이다. 즉, 정보보호 및 사이버전 수

행 전담 조직 및 전문인력이 매우 부족한 것이 현실이며, 체계적인 관련 기술 개발 및 연구가 미흡하고, 정보보호 운영체계가 부족하여 단위 목적별 또는 부분별로 보호체계를 도입·운용하고 있는 실정이라고 할 수 있다.

본 연구의 핵심 성과물이라 할 수 있는 'C4I 시스템 보안 로드맵 설계'는 C4I체계를 중심으로 하는 종합적인 국방정보보호 및 사이버전 수행 체계 구축의 로드맵으로서, 정책 및 제도, 조직 및 인력, 운영체계, 기술 연구 및 개발 등의 4분야로 구분하였다. 또한 각 분야별 추진목표, 추진방향, 세부추진과제 등을 제시하였으며, 단기 및 중·장기로 구분하여 로드맵을 이행하기 용이하도록 하였다.

끝으로, 본 로드맵의 적극적인 이행으로 최종목표인 '2015년까지 국방정보보호 기반체계 및 사이버전 수행체계 구축'이 완성되어 군 리더의 민·군·관 공조체계 구축을 통해 국가 사이버전 수행되며, C4I체계 중심의 NCW가 안전하게 수행되길 고대한다.

참 고 문 헌

[1] 합참, 합참 비젼 2015 합동전장 운용개념서, 1999.

[2] 국방부, 국방정보보호 발전 기본계획, 2002.

[3] 남길현, "사이버테러와 국가안보", 국방연구 제45권, 제1호, 국방대학교, 2002.

[4] Edward Waltz, *Information Warfare Principles and Operations*, 1998.

이 강 택

1988년 공군사관학교 전자계산학 (이학사)

2002년 포항공과대학교 정보통신학과 (공학석사)

2006년 경기대학교 정보보호기술공학과 (공학박사)

이 동 휘

2000년 경기대학교 전자계산학과 (이학사)

2003년 경기대학교 정보보호기술공학과 (공학석사)

2004~현재 경기대학교 정보보호학과 박사과정

양 재 수

1981년 한국항공대학교 통신공학과 (공학사)

1985년 건국대학교 전자공학과 (공학석사)

1993년 미국 NJIT 전기및컴퓨터공학 (공학박사)

1982~2006년 KT중앙지사장

현재 광운대학교 산학협력단 전담교수

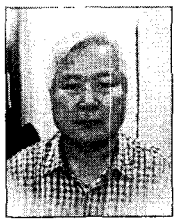
김 귀 남

미국 캔자스대학 수학과(응용수학사)

미국 콜로라도주립대학 통계학과(통계학석사)

미국 콜로라도주립대학 기계산업공학과(기계·산업공학박사)

현재 경기대학교 정보보호학과 교수



박 상 민

1970년 한양대학교(공학사)

1983년 한양대학교(공학석사)

1990년 한양대학교(공학박사)

2002년~현재 동북아전자물류연구센터 소장

현재 인천대학교 산업경영학과 교수