국방 정보전(IA) 모델

최 운 호*, 박 상 서 **
* 경기대학교
** 국가보안기술연구소

A Model of MND Information Assurance

Unho Choi*, Sangseo Park**

1. 서 론

코소보와 보스니아 전쟁을 시작으로 현대적 의미의 정보전은 새로운 국면을 맞고 있다. 즉 1996년 미국방성 국방과학위원회(DSB : Defense Science Board)의 정보전 방어(IW-D : Information Warfare - Defense)보고서를 시작으로 정보전은 사이버전 그리고 사이버테러리즘으로 여러 용어가 혼용되어 쓰여지고 있으나 최근 2001년도 2월에 발간되어 8월에 공개된 미국방성 국방과학위원회는 "Protecting the Homeland" 라는 보고서에서 향후 핵전쟁이나 생화학전보다 사이버전이 최우선적인 위협요소 라고 정의하고 있고, 정보운용(Information Operation)과 정보전-방어(IW-D)를 동일한 개념으로 사용하고 있다.

국내의 민간 정보보호수준은 정보보호평가체계에 의한 K4등급의 침입탐지, 침입차단시스템에 집중되고 있으나, 국방부의 핵심시스템은 그 특성상 별도로 제작되거나, 국방 관련 또는 국방부의 위탁을 받은 국가 기관에 의하여 별도의 평가 과정을 거쳐 검증된 상용 제품들이 사용되어야 한다.

현재, 군에서 사용하고 있는 제품들은 대부분이 상용 제품들이기 때문에, 이들 시스템이 갖는 내재된 취약성을 시작점으로 하는 사이버전 및 사이버테러의 위협은 나날이 증가하고 있다. 이와 같은 사이버테러의 위협에 대한 위기의식 하에, 미국에서는 작년 1월 국가 주요 기반구조 보호(Critical Infrastructure Protection: CIP)를 위한 국가 차원의 계획을 수정해서 발표할 예정이며, DARPA(Defense Advanced Research Project Agency)에서는 정보 보증 및 생존(Information Assurance & Survivability: IA&S) 프로젝트를 진행하고 있고, IA&S는 정보전에 대한 미국방성의 기존 인식이 변화하면서 대두된 개념으로, 국방성, 연방정부, 공공기관 및 산업체의 정보보호 능력을 통합하고 조정함으로써 협력체제를 강화하여 국가 정보 기반구조(National Information Infrastructure: NII)를 구성, 운영 및 통제하는 정보와 정보기술을 침해로부터 보호하고, 신뢰성과 가용성을 보장하는 것을 말한다. 이는 사이버테러로부터 NII를 보호하기 위한 기술 개발은 전통적인 정보보안(INFOSEC)에서 정보 보증 및 생존성(Information

Assurance & Survivability: IA&S) 기술 개발로 변화하였다는 것을 의미한다.

본 논문에서는 국방 정보보호 발전의 한 방향을 제시하기 위하여 국방 정보보호 모델을 제안하고, 이 모델에 따라 국방 사이버 상황실 구축 방안과 국방 사이버전 조기 경보 체계 구축방안을 제시하고자 한다.

2. 국방 정보보호 추진 정책 방향 및 중·장기 추진 전략

국방정보보호체계의 기본 방향은 증가하는 공격자에 대한 방어 개념이 최우선시되어 필요시 전술적인 공격에 필요한 기본준비를 갖추는데 있으며, 다음과 같은 기본적인 요소가 가능해야 한다.

1) 적대적인 공격자에 대한 접속거부

- ○ 시스템 접속절차가 안전하게 설정되었는가에 대한 점검
- ○ 자동적으로 취약성에 대한 패치가 가능한 소프트웨어 개발
- ○ 바이러스/웜에 대한 발견/제거/복구 대책
- ○ 공격자에 대한 격리 및 네트웍의 자동재구성 방법 개발

2) 공격자의 접속 제한

- ○ 비인가접속자에 대한 제한 원칙 설정
  - ※ 예를 들어 잘못된 정보를 사용하여 호스트와 버전이 다른 명령어로 접속을 해온다면 이는 공격자로서 제한하는 원칙이 필요하다

3) 시스템에 영향을 주거나 접속가능 권리의 무력화

- ○ 침입자(intruder)가 얻게 되는 시스템 접속 등을 원천적으로 차단

4) 공격자의 의지 및 수준별 기교 증명방법 강구

- ○ 공격자가 수사에 참조할 증거를 honeypot 등에 남기면, 이를 통대로 공격자의 의지 및 수준을 판별하여 대처하기 위한 방안

5) 공격자의 존재 발견

- ○ 공격자 발견 방안
  - ※ 공격자는 자동화된 도구 등으로 대용량의 데이터나 특정 주제를 찾아다니는 특성이 있어서, 파일이나 데이터를 암호화하여 디지털 워터마킹을 걸어 놓거나 추적 에이전트를 심어 놓기 때문이다.

6) 내부관계 정의 및 공격자의 조직

- ○ 많은 네트웍부하분석에서 공격자의 근본 출발지 및 경유지를 발견할 수 있는 근거 수단 확보

7) 내부 인원 훈련

- ○ 기본적인 내부개발 도구로 훈련하여 추적이 가능한 상태로 시스템관리자나 운영자를 훈련

8) 분석 데이타의 양을 최소화 할 수 있는 기준 정립

- ○ 침해사고나 공격자의 공격개시로 분석해야 할 데이터가 무한정 증가하면, 이를 분석하여, 추적하거나 방어준비를 하는데 많은 시간이 소요됨에 따라 이를 평시에 최소화하는 기준 및 훈련이 필요함

9) 데이터의 소음/쓰레기 데이타를 최소화

10) 방어해야할 네트웍의 기본 구조 및 백본을 명확히 파악

○ 기본적인 패치정보의 업데이트 및 백도어 제거 방안

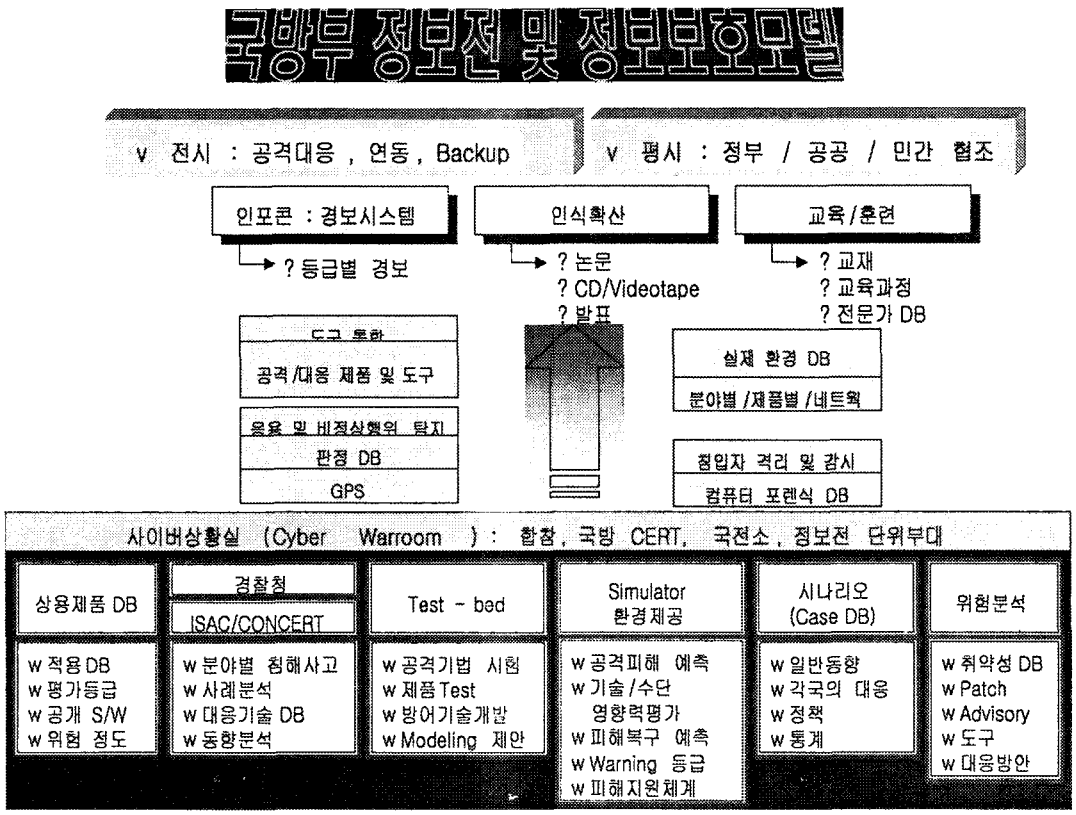
11) 공격 예상자나 조직에 대한 평시 관찰이 필요

3. 국방 정보보호 모델 및 구현 전략

3.1 국방 정보보호 모델

국방 정보전 대응체계를 건설하기 위해서는 합참 산하에 "정보전 기획단(가칭)"을 창설하여, 정보전에 관련되어 일원화된 대외 창구 역할을 해야하며, 정보전 대응체계 건설을 위한 사업, 조직, 추진계획 등을 준비하여, 각군 비전에 반영하고 특히 국방비전, 육군비전2015/2025, 해군비전, 공군비전, 방위력 개선사업으로 추진하며, 각군의 소요반영, 합참JSOP에 반영, 국방중기계획에 반영에 반영되어야 하고, 이렇게 제시된 사업 수행에 필요한 예산이 적기에 확보되어 지원되야 한다.

이를 정보전 조직구조에 반영하여, 정보전 기획체계, 수행체계, 평가체계의 소요인력을 확보



(그림 1) 국방 정보보호 모델

하고, 자주적 연구개발을 통하여 독자적인 정보전수행능력 확보 그리고 정보전대응 연구기능의 확대 및 활성화가 중요하며, 이를 뒷받침할 정보전대응 연구인력 및 예산확보가 시급하다.

이를 위해서는 기본적으로 "국방정보보호모델"을 기반으로 국방부 기본 프레임웍을 구축해야 한다. 이를 위해서는 다음과 같은 사항이 고려되어야 할 것이다.

- ○ 국방부 정보보호 대책을 전시/평시로 구분하여 수립
- ○ 중장기 계획 수립원칙 및 방향 제시
- ○ 정보보호 모델 요소별 기능 정의
- ○ 사이버상황실 구축에 필요한 기능제시

그리고, 이와 같은 고려를 기반으로 국방 정보보호 모델에 포함되어야 할 사항에는 다음과 같은 것들이 있다.

- ○ 상용제품 DB 구축
- ○ 연계대응체계 범위 설정
- ○ "정보전 훈련장" 등 테스트베드 운영환경 구성
- ○ 시뮬레이터환경 제공
- ○ 시나리오 DB 구축
- ○ 위험분석/위협평가의 방법론 제정
- ○ 도구통합환경 및 개발범위
- ○ 실제환경DB 구축
- ○ 인식 및 확산방법 연구
- ○ 교육/훈련방안 도출

앞에서 기술한 고려 사항들과 포함 사항들을 기반으로 본 논문에서는 (그림 1)과 같은 국방정보보호 모델을 제시한다.

(그림 1)에서 보인 모델을 구현하기 위해서는 다음과 같은 단계를 거쳐야 그 비젼이 조기에 구축될 것으로 판단된다.

- ○ 법/제도의 정비
- ○ 단기적 인력 확보 및 중장기 인력 양성
- ○ 조직 발전
- ○ 연구개발 강화

3.2 법/제도적 측면에서의 구현 전략

법/제도적 측면에서의 국방 정보보호 전략은 다음과 같은 것이 고려되어야 한다.

- ○ 정보전 수행에 필요한 국방 정보보호 훈령 또는 규정을 제정하여, 관련 법제도 정비 전에 활용
- ○ 업무 수행시 참고할 수 있는 편람 또는 지침서을 작성하여 예하 부대에 하달하고, 각 부대에서는 해당 부대의 상황에 맞게 보완하여 적용.
- ○ 정보보호 방산 업체 지정 제도 신설
  - 민간의 기술과 인력을 활용하기 위하여 정보보호 분야의 민간 기업이 국방 정보보호에 참여할 수 있도록 방산 업체 지정 제도를 신설
  - 지정 업체들의 연합체인 국방 정보보호 컨소시움을 구성
    - ※ 단, 지정업체들의 제품은 별도의 평가과정을 거쳐 국방용으로의 채택 여부 결정

3.3 인력 양성 측면에서의 구현 전략

국방부의 정보전 방어 및 정보작전(IO) 수행을 위한 인력강화 방안을 다음과 같은 원칙으로 운영할 필요성이 있다.

- ○ 대학의 사이버 ROTC 제도 (미국의 제도 응용)
- ○ 대학 전산학과 출신 공익요원의 활용
- ○ 정보산업고 및 실업고의 정보보호과 운영
- ○ 각군 사관학교 및 하사관 학교 활용

3.4 조직 발전 측면에서의 구현 전략

가) 필요 조직

- ○ 정보전 연구 개발 조직
  - ADD, KIDA의 임무와 역할 강화
  - 군 지원 기관인 국가보안기술연구소의

적극 활용
- 한국정보보호진흥원, 한국전자통신연구원 등의 기존 연구개발 조직을 최대한 활용

○ 수행 및 운영 조직
- CERT: 사고 접수 및 처리 업무 수행
- Tiger Team: 한시적인 안전진단을 위한 팀으로서, 정보전 훈련시는 Red Team으로 활용
- Red Team: 정보전 훈련 및 방어를 위하여 상설화된 조직으로 운영할 필요가 있으며, 국방부 및 산하기관/부대에 대한 정기적인 취약성 분석 및 지침을 전달할 의무를 부여

나) Tiger Team

일반적으로 타이거팀은 보안전문가나 특정한 목적을 위하여 해커를 고용하여 조직되어 운영하는 팀으로, 한시적인 목적의 운영과 상설 화된 팀으로 구분이 가능하며, 시스템을 내부나 외부에서 해킹 점검하여, 취약성에 대한 컨설팅을 하거나 보안시스템 향상 조사에 활용되는 그룹을 지칭하는 용어이다.

미 육군의 정의에 의하면 ("JARGON" US Army), 보안시스템을 침투하고 시험할 목적의 팀 혹은 스니커로서 고용된 해커타입의 기술(hacker-type tricks)을 구사하는 전문가들로, 중요방어시스템에 침투하여 "폭파", "암호코드가 분실됐음" 남기며, 이를 토대로 다음날 보안검토, 사령관이나 보안담당 장교의 조기전역을 유도한다. 최근에는, 공식감찰팀 혹은 특별소방그룹으로 지칭되며 다음과 같은 특성을 갖는다.

○ 타이거팀의 일부는 네트웍을 경유하여 원격 공격
○ 안전한 통신채널로 군사용 컴퓨터를 시험하는 전문크래커 (crackers)
○ 위대한 해커의 행위로 등급 가능(?)
○ 특별한 감각이 상업적인 컴퓨터보안범주로 도입 가능

타이거팀에는 다음과 같이 네 가지의 종류가 있다.

○ 대규모 네트웍이나 시스템을 가진 정부기관/공공기관/대기업
- 자신의 보안점검과 시험을 위하여 잘 훈련된 보안전문가나 전문해커를 고용하여 상설 조직으로 운영하는 경우
- 미국방성(DoD)은 현재 상설 타이거팀을 운영

○ 컨설팅사에서 한시적인 보안조사
- 해커나 보안전문가를 조직하여, 특정기간 동안 운영

○ 보안관련 제품개발회사에서 자사 제품의 성능시험
- 내부나 외부에서 테스트베드의 침투시험 중 운영

○ 침투시험(penetration testing)을 전문적으로 수행
- 보안점검 및 취약성을 보완해주는 타이거팀 운영

다) 레드팀

취약성 평가를 위한 레드팀(Red Team) 구성되어야 하며, 기본적인 조건과 경력은 다음과 같다.

○ 경력자 해커로서 다음조건 침투시 성공
- VM (SP, XA, HPO, ESA, ad nauseam), MVS, VMS, Unix, Windows (all flavors), OS/2, etc.
- 'Windows'박스 : 일반적인 도구없이 6분 안에 해킹 조건

○ 컴퓨터/네트웍 보안의 방어기술을 보유
- "Tiger Team", 침투시험(penetration testing.)
- 백신 및 침입탐지 소프트웨어 사용
- 침입차단시스템. 게이트웨이 등 주요 접속통제 가능
- 암호 기술 및 전자서명/인증기술 활용

- 주요 운영시스템의 패치 가능
- 위험분석 및 감리, 추적 가능
- 정보보호 정책, 인식, 구매절차 등 이해

라) 정책 조직

○ 국방부 정보화기획실 산하에 정보보호국 신설
○ 합참에 정보보호과 신설
○ 각군 지통부에 정보보호과 신설

3.5 연구개발 측면에서의 구현 전략

중장기적으로는 국방부 산하의 연구기관들이 제 역할을 충분히 수행할 수 있는 환경을 구축하는 것과 함께 단기적으로는 외부의 연구기관들을 활용하는 전략의 수립이 필요하다. 즉, 단중기적으로는 외부의 연구기관을 활용하여 정보전/정보보호 기술 및 정책의 연구 개발을 추진하면서 국방부 산하 연구기관들의 연구 능력을 확보하고, 중장기적으로는 외부 연구기관과 국방부 산하 연구기관들을 함께 활용하도록 한다. 특히, 국방 지원의 기능과 임무가 있는 기관들을 적극 활용함으로써 산하 기관이 가지고 있는 한계점을 극복한다.

이를 위한 연구개발 단계별 세부 기술과제 도출 방법은 다음과 같다.

○ 1단계: 체계적 기술분류 및 기술별 중요도 평가

국방정보보호 및 정보전 기술을 공통기반, 시스템·네트워크보호, 응용서비스보호 기술 세가지로 분류하고 전문가평가를 거쳐 기술별 중요도 산출

○ 2단계: 중요기술 Grouping 및 단위 연구개발 기술 도출

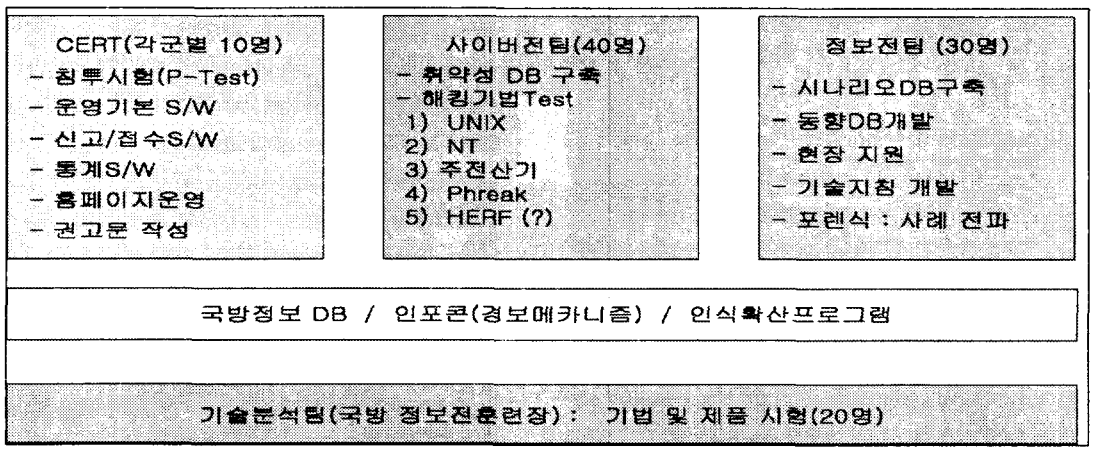
이전단계에서 "우선순위" 가 높은 기술만 선택하여 선택된 기술의 특성과 연관관계를 고려한 단위연구과제 도출

○ 3단계: 단위 연구개발기술별 기술특성 분석 및 개발 주체 선정

기술의 특성이 상호 혼재되어 있는 경우는 수행기관간 공동연구 수행

○ 4 단계 : 소요예산 및 확보방안 결정

공통기반 / 시스템·네트워크 / 응용서비스 분야별로 2002년부터 2004년까지의 국방부 예산 투자계획 작성. 이때, 도출기술의 중요도, 우선순위, 정책적 고려사항 등 종합적으로 고려하여 예산배분



(그림 2) 레드팀 구성안

4. 국방부 사이버상황실(CyberWaroom) 구축 방안

국방부 사이버상황실은 전시 및 평시의 국방부의 사이버전을 지휘하는 핵심지휘관들이 모여서, 의사결정을 신속히 내릴 수 있도록 지원해 주는 각종 첨단 장비 및 관련 데이터베이스를 운영하는 것을 말하며, 이를 기반으로 인포콘이 운영되어야 한다.

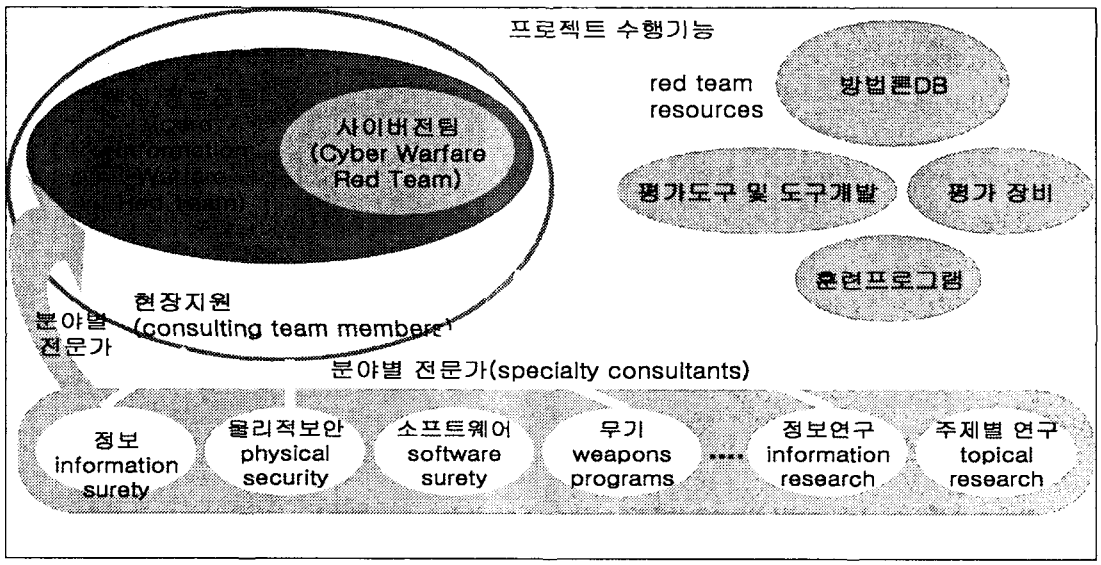
사이버상황실 구축시 고려되어야 하는 정보는 다음과 같다.

- ○ 구축시 용도에 따라 국방부에 설치되는 상황실과 사령부 및 군단, 메가센터 등에 설치될 소규모 상황실이 고려
- ○ 이러한 상황실은 안전한 정보보호 및 네트워 대책이 지원
- ○ 운영요원은 정예화된 전문가들로 "Red Team"을 조직하여 운영을 전담케하며
- ○ 평시에는 워게임을 통한 실전을 예상한 시나리오대로 훈련을 하도록 하고, 개발에 필요한 기술 및 대책을 수립

국방부는 이러한 미래 정보전을 예상한 시뮬레이션 모델을 훈련기법으로 도입하고, 훈련용 시뮬레이터를 개발해서 보유해야 한다.

국방 사이버 상황실에서 제공되어야 하는 정보는 아래와 같다.

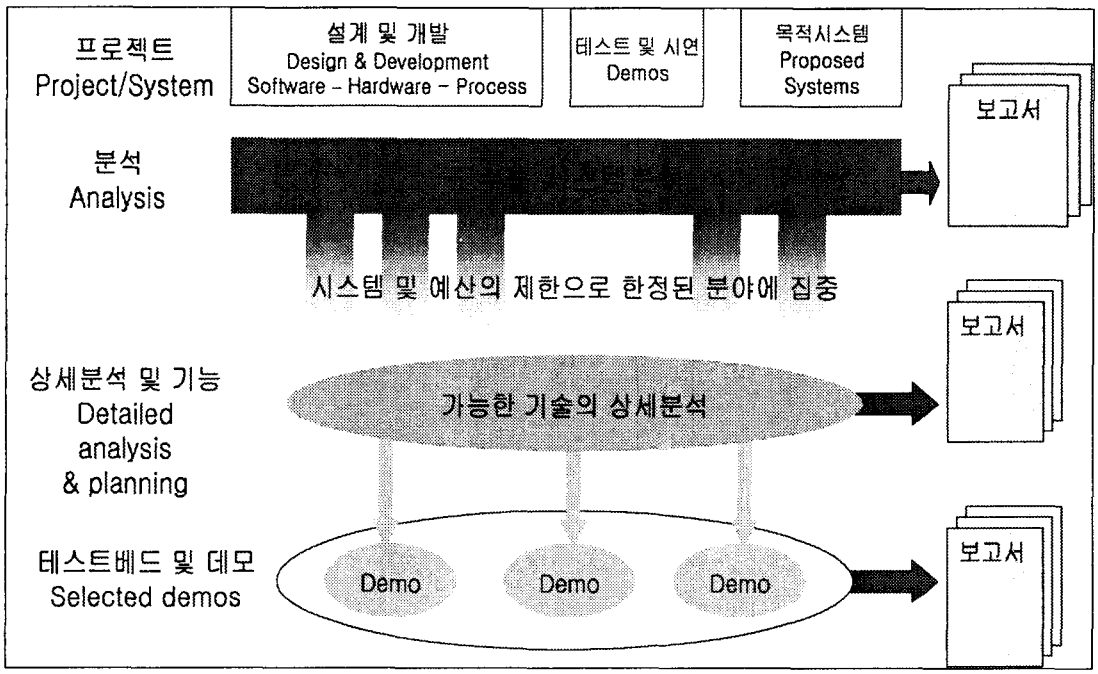
- ○ 다양한 시각의 전술적 데이타(Tactical data)
- ○ 지도베이스(Map-based)와 높은 고해상도 지원
- ○ 임무 요약과 지휘관의 최근 지시
- ○ 실시간 정보가 게시되고, DB에 저장된다.
- ○ 경보/권고문/권고사항 등 게시
- ○ 현재, 충돌이 일어나는 계획
- ○ 지원이 필요한 사항
- ○ 예상치 못한 사태에 대한 보고
- ○ 기존 계획
- ○ 응답시간 마지노선 관리
- ○ 효과 요약
- ○ 자원관리 현황



(그림 3) 레드팀 임무 분장안

○ 협조 도구상황(통신 연결 상태, 이메일 등)

사이버상황실의 종합상황판은국방부 합참, 육/해/공군, 기무사 등이 각각의 정보를 실시간으로 제공하며, 모든 상황이 한눈에 모니터링이 가능하게 구현되야 한다.



(그림 4) 레드팀 업무 수행 체계

사이버상황실에서 국방부의 정보통신망 및 시스템에 접근하는 것을 정당한 사용자는 시스템에 접근시키고, 적대적인 행위가 가능한 행동자는 일명 "Fishbowl" 혹은 "Honeypot"이라는 상대방의 행동을 어항속에 든 물고기처럼 관찰하다가 격퇴 혹은 추적하는 모니터링을 수행해야 한다.

사이버상황실을 운영할 "Red Team"의 구성(안)은 (그림 3)과 같다.

○ 정보전팀(IWRT : Information Warfare Red Team)
- 정보전 수행시 시스템 수준 평가
- 평가 절차 및 도구 자체 개발

○ 사이버전팀(CWRT :Cyber Warfare Red Team)
- 네트웍, 운영체제, 소프트웨어, 정보시스템 운영에 전문지식 보유
- 사이버 공격에 대한 상세한 지식과 도구 운영기술 보유

○ 기술분석팀
- 실제 정보전팀과 사이버전팀에 연구 및 기술을 분석하고, 기법을 테스트하여 전달하는 역할

○ 타이거팀(Tiger Team) : 한시적 특수용도 가동조직

국방부 전체 정보통신망에는 미국의 경우처럼 자동화된 침입탐지 및 침입차단 그리고 최종적으로 격퇴할 수 있는 시스템의 설치가 필요하다.

5. 국방부 조기경보(인포콘) 구축 및 운영 방안

현재 운영중인 인포콘 제도를 보완하여 사이버상황실에서 운영할 조기경보체계의 구축 기본원칙은 다음과 같다.

- ○ 민간/국방 사이버 상호협력방안이 동시에 진행
- ○ 조기경보시스템 개발 및 구축 방법이 논의
- ○ CERT : 해킹 등 침해사고 접수반

그리고 Red Team의 업무 수행 체계는 (그림 4)와 같아야 한다.

- ○ 정보통신기반보호법의 침해사고대책본부와 연계
- ○ 국방부의 침해사고대책본부 참여방안
- ○ 합참 인포콘경보제도와의 연계방안 도출
- ○ 국메가센터의 정보전상황실 설치 및 연동 고려

※ 미국은 정보전상황실(Information Warfare Cyber Waroom)을 우주전사령부에 설치 운영중이며, 주관부서는 JTF-CND임.

정보전에서의 "조기경보 및 위협평가 프로젝트" 신설이 필요하다. 가령 해상에서 태풍이 불어오면, 1급 혹은 2급 태풍인지 그리고 한반도를 경유할 것인가에 대해서 기상예보자는 항상 촉각을 곤두세우게 된다. NATO와 영국의 대학/기업이 참여한 "정보전 공격 평가 및 조기경보" 프로젝트에 근거하면, 정보전 공격도 이렇게 사전에 경보되거나 분석되지 않으면 그 파장은 말로 설명할 수가 없다.

5.1 목적

국방부 예하 하부조직에게 사이버 공격을 예보하는 방법론 및 소프트웨어를 개발하여, 사이버상황실에서 테스트하는데 있다. 이 프로젝트는 이러한 예보를 통해서 최종 시스템 관리자가 이러한 분야에서 정보시스템을 보호하고 하부조직 활동자의 행동을 이해하는 방법론을 제공할 것이다.

5.2 산출물

- ○ 최종사용자에게 개발된 정형화된 사이버공격 방어 방법론 및 대응 기술(수집, 조사, 분석)과 방법론 애플리케이션에 대한 청사진제공
- ○ 사이버 공격 및 방어 연구와 방법론 개발 절차, 방법론 개발과 애플리케이션 진행에서의 중요 기술
- ○ 사이버 공격 및 방어 무기 및 도구에 대한 수집, 조사 분석과정의 실질적인 결과물 기술 ; 즉 사이버 공격방법과 하부조직행동자의 동기에 대한 결론 그리고 대응방법/솔루션 등

5.3 배경

정보시스템 및 정보보호영역에서, 사이버 위협과 취약점을 참고하여 지능적 방법론 연구와 공공정책영역에 기초한다. 이러한 일의 시작은 인터넷과 같은 개방형 구조의 증가로 취약점이 증가했기 때문에 외부그룹의 위협으로부터 주의를 더욱더 기울여야할 필요성이 제기 됐으며, 지배적인 위험 관리 파라다임은 대개 취약성, 위험방정식의 영향요소 (위험방적식: 위험=위약성*영향*위협)에 초점을 맞추고 있다. 위협에 한에서는 대개 이러한 방정식()의 가능성 부분에 초점이 맞춰져 있다. 이것은 정보보호정책의 공식화와 정량화가 어렵다는 것을 의미한다. 동시에 풀리지않는 문제는 정보전 공격과 공격의 본질과 벡터의 예보에 대한 지시자와 경고를 제공하는 것이다. 이것은 유력한 패라다임(방해, 보호, 발견, 대응, 복구)이 한번 진행중인 공격의 발견에 의존한다는 것을 의미한다.

5.4 한계

사이버 위협은 잠재적으로 광범위한 행위자로부터 발생하며, (국가, 범죄자, 개인, 조직화된 해커, 해커 그룹) hacktivists와 사이버 테러리스트 / 정보전을 수행하는 정보전사가 주요한 요인으로, hacktivists는 컴퓨터를 해킹하는 조직화된 그룹(정치적이든 개인적인 이슈든)이고, 사이버테러리스트는 해킹을 하는 무장된 그룹이라기 보다는 정치적인 목적을 위한 운동세력에 보조수단으로 무장된 그룹이며, 정보전사는 정보전을 목적으로 조직되고 운영되는 일종의 군인이다. 자체적으로 이러한 그룹의 사이버행동성격에 확실한 집합으로 한정된다. 조지타운대학의 Denning에 따르면 이러한 정의는 인터넷공격행동패턴에 다른 것이다.

향후 국방부 사이버상황실은 전시 및 평시에 국가중요정보기반구조인 금융, 통신, 에너지, 전력, 공항 등의 주요 정보시스템에 인포콘 경보를 발령하는 형태로 발전해 나가는 것이 바람직하다. 이는 미공군이 금융을, 미해군이 에너지, 정보통신, 급수, 수송을 담당하는 것처럼 군의 업무 분장이 조정되야 한다.

6. 국방 정보체계 보호 대상 식별 및 위협요소 분석

국방부 중요정보기반구조에 대한 보호대상이 먼저 설정되야 그 중요도에 따라 위협요소 식별 및 정보보호 정책이 우선 순위에 의해서 연차적으로 정해져 중장기적으로 대처할 수 있다.

이를 위해서는 조직이 구성되어야 한다. 이 조직은 특별위원회를 구성하여, 전체 대상식별 및 분류, 우선순위 평가기준 등이 정립되고 나서 위협요소 분석이 가능해 진다.

6.1 국방정보체계 보호대상 식별 및 위협요소 분석절차(안)

국방 정보체계 보호 대상을 식별하기 위해서는 다음과 같은 중요 정보자산의 대상 및 식별, 지정방안이 도입되어야 한다.

- ○ 국방정보통신기반시설 지정 지침(안)
- ○ 국방정보통신기반시설의 지정평가를 위한 기준표
- ○ 당해 시설을 관리하는 기관 및 부대가 수행하는 업무의 국방업무적 중요성 점검표
- ○ 정보통신기반시설에 대한 의존도 점검표
- ○ 다른 정보통신기반시설과의 상호연계성 점검표
- ○ 침해사고 발생시의 피해규모 및 범위 점검표
- ○ 침해사고 발생가능성 또는 복구의 용이성 점검표

6.2 국방정보체계 보호대상 식별 및 위협요소 분석 방법론

국방 정보체계 보호 대상은 Layer별 Approach를 적용하여, 장기적으로 정보보호에 필요한 단계별로 대상이 충분히 보호되어야하는지를 점검해야 하며, 다음과 같이 분류가 가능하다.

- ○ 일반적인 시스템
  - 네트워크 : 통신망 구조, 구성요소(광케이블 등) 등 파악 필요
  - 시스템 : 시스템 종류 등 파악
  - 운영체제
  - 어플리케이션: 통합군수정보체계(탄약, 보급, 장비정비 등), 인사정보체계 등
  - 데이타
  - 라우터/교환기
  - 방화벽
- ○ 특수 시스템
  - C4I 시스템, C3I 시스템
  - MCRC, NTDS 등

6.3 국방정보체계 위협요소

1) 국방정보시스템에 접근할 수 있는 해커들의 수준과 분류

"해커" 라는 단어의 의미는 해킹을 시도하는 레크레이셜날한 해킹을 시도하는 사람을 의미하고, 흔히 알고 있는 "크래커(cracker)" 와 반대되는 좋은 의미나 뛰어난 실력의 실력자는 아니다.

현재 국내에서 연구된 해커가 구사할 기술 수준분류는 다음과 같지만, 정보전에 쓰이는 고급 기술로 위성해킹, GPS해킹, 전자전 장비 해킹 등을 구사할 수 있는 수준의 분류는 인터넷에도 어느 문헌에도 이들의 실력수준은 나와 있지 않으며, 군에서 별도로 작성한 정보전사 수준(안)을 만들어서 독자적으로 측정해야 하지만 일부 수준은 다음과 같이 제시할 수도 있다.

가) 해킹 수행 코드 작성 가능

해킹 수행 코드 작성 가능이란 의미는 난이도가 낮은 간단한 취약점을 이용하는 해킹 수행 코드 뿐만 아니라 버퍼 오버플로 공격이나 포맷 스트링 공격 등과 같은 프로그래밍 상의 오류를 이용한 공격과, 각종 프로토콜 상의 문제점을 이용한 해킹 수행 코드를 작성할 수 있는 경우를 의미한다.

새로운 취약점을 발견하고 그에 대한 해킹 수행 코드를 만들 수 있는 해커는 최고 수준의 해커라고 볼 수 있다. 이 수준의 해커는 자동화, 에이전트화, 은닉화, 분산화된 해킹 도구를 제작할 수 있는 능력을 가지고 있으며, 시스템에서 수행되는 여러 작업간의 유기적인 문제를 이해하고 있다.

기존에 발견된 취약점에 대한 해킹 수행 코드를 작성할 수 있는 해커는 여러 OS에 대해 각각의 시스템 구조를 자세하게 이해하고 있으며, 복잡한 네트워크 프로그래밍이 가능하고, 시스템에서 제공하는 서비스 및 각종 프로토콜과 프로그램 등의 구조적인 문제를 이해하고 분석할 수 있는 능력이 있다.

나) 해킹 수행 코드의 수정 사용 가능

이미 인터넷에 공개된 해킹 수행 코드를 수정하여 해킹하고자 하는 시스템에 적용할 수 있고, 여러 가지 운영체제에 대한 낮은 수준의 시스템 구조를 이해하고 있으며 각종 프로토콜을 이해하고 있다. 또한 어느 정도 수준의 네트워크 프로그래밍이 가능한 수준으로 해킹 수행 코드자체를 이해하고 각각의 코드들이 어떤 동작을 하는지 알고 있다. 만약 원하는 해킹 대상 시스템에 기존에 발표된 취약점이 존재하고, 이에 대한 해킹 수행 코드가 존재한다면 해킹이 가능하다.

다) 해킹 수행 코드를 수정하더라도 해킹 성공률이 낮은 수준

이 수준의 해커는 해킹하고자 하는 시스템에 해킹 수행 코드를 적용하기 위해 몇 가지 간단한 내용을 수정하지만 해킹 성공 가능성은 매우 희박한 수준이다. 비록 해킹 대상 시스템에 대한 취약점 점검을 통해 어떤 취약점이 있는지 확인하고, 해당 취약점에 대한 해킹 수행 코드를 찾을 수 있는 능력은 있지만, 만약 얻은 해킹 수행 코드가 해킹하려는 시스템에 정확히 일치하는 것이 아니면 해킹에 성공할 확률이 낮은 해커이다. 그러나 이러한 수준의 해커는 일반적인 시스템 프로그래밍이 가능하고 대부분의 해킹기법을 이해하고 있다.

라) 해킹 수행 코드 및 해킹 프로그램의 단순 사용

공개된 해킹 수행 코드나 각종 해킹관련 사이트에서 얻을 수 있는 각종 프로그램을 단순히 사용하는 수준의 해커를 말한다. 물론 이 수준의 해커는 해커라고 불리지 않는다. 대부분 크래커라고 불리거나 과거 분류에 따라 스크립트 키디(script kiddie), 혹은 워너비(want to be, wannabe, 해커가 되고 싶은 사람)라고 불린다. 획득한 해킹 수행 코드를 수정 없이 실행하거

나, 단순한 스크립트들을 수행시키는데, 이러한 수준의 해커는 해커라고 불리지 않는다. 이들은 획득하게 되는 각종 GUI 형태 및 UNIX 기반 해킹 프로그램을 단순히 설치하여 실행할 뿐이다. 기존에 알려져 있는 시스템이나 각종 서비스의 취약점에 대해 여러 명령어들을 이용하거나 웹 브라우저 상의 단순한 코드 조작으로 해킹할 수 있는 능력은 있으나, 해킹 수행 코드 자체를 이해하지는 못한다.

해킹 수행 코드라는 것이 무엇인지 이해하지 못하는 수준으로 해킹 사이트 등에서 얻어낸 각종 해킹 프로그램을 단순히 사용하는 수준이다. 이제 막 해킹 기법을 익히기 시작한 이들은 Unix시스템을 사용해본 경험이 있고, 몇몇 시스템 명령어를 사용할 수 있으며, 네트워크와 시스템에 대한 약간의 지식을 가지고 있지만 해킹에 적용시킬 능력은 없다.

DoS 프로그램이나 패스워드 크랙 도구만 있으면 모든 사이트를 해킹할 수 있다고 생각하는 사람으로, 네트워크나 시스템에 대한 지식이 전무하며, 단순히 얻게 된 해킹 프로그램을 설치하여 실행해 본다. 또한 이런 류의 사람이 사용하는 프로그램은 GUI형태의 해킹 프로그램으로, PC방 등에 트로이잔 형태의 프로그램을 설치하고 해킹에 성공했다고 생각하는 사람이다.

2) 위협요소 분석

정보전에서 주로 공격으로 대상으로 삼는 정보시스템과 서비스에는 다음과 같은 주요 위협이 있다.

- O 비인가 접속을 하여 데이터를 변조, 이동 혹은 삭제하는 행위
- O 전자적인 공격(electronic attack (EA))으로 시스템의 작동불능, 운영중단 그리고 서비스의 연속성 중지 등으로 이용되는 전자기파공격(electromagnetic pulse (EMP))
- O 항공기, 군함 혹은 이동중인 수송기 등의 지리정보시스템(GPS)에 대한 해킹, Jamming 등
- O 내부자(Insiders)의 접속으로 내부 및 외부인이 허락받지 않은 상태에서 접속을 하는 것
- O 사이버테러리스트가 물리적인 파괴를 포함한 불법접속으로 국민의 경제적인 생활에 방해되는 주요시스템을 위협하는 것

4) 네트워크 측면에서의 위협

- O 컴퓨터네트웍공격 (Computer Network Attack (CNA))은 운영에 장애가 되는 중단, 거부, 정보의 파괴 등을 초래하도록 컴퓨터와 네트웍을 공격
- O 수동적인 차단공격 (Passive Intercept Attack)은 트래픽 모니터링, 복사, 분석, 암호해독, 패스워드 등 인증수단 가로채기
- O 공격적인 네트웍기반공격 (Active Network-Based Attack)은 정보를 악성코드를 사용하거나 중간에서 가로채는 수법으로 백본이나 전송중의 트래픽을 대상으로 하며, 원격으로 주로 시행됨
- O 내부자 공격(Insider Attack)은 직원이나 운영요원이 친분을 바탕으로 시스템에 접속하거나 패스워드 등 인증도구를 알아내어 정보도청, 절도, 위험한 정보 및 코드의 삽입 등을 수행
- O H/W, S/W분배공격(Hardware /Software Distribution Attacks)은 사전에 악성코드나 프로그램이 삽입된 형태로 배치되어 수행하는 공격

7. 결 론

본 논문에서는 국방 정보보호 발전의 한 방향을 제시하기 위하여 국방 정보보호 모델을 제안

하고, 이 모델에 따라 국방 사이버 상황실 구축 방안과 국방 사이버전 조기 경보 체계 구축방안을 제시하였다.

정보전은 이제 전통적인 정보보안 에서 중요 정보기반구조 보호 및 정보보증과 생존성으로 변화하고 있다.

현실적인 우리 군의 국방 정보전 대응체계를 건설하기 위해서는 합참 산하에 "정보전 기획단(가칭)" 을 창설하여, 정보전에 관련되어 일원화된 대외 창구 역할을 해야할 것이다. 또한, 정보전 대응체계 건설을 위한 사업, 조직, 추진계획 등을 준비하여, 각군 비젼에 반영하고 방위력 개선사업으로 추진되어야 할 것이다. 그리고 이러한 계획은 각 군, 합참 JSOP 및 국방중기계획에 반영에 반영되어야 하고, 이렇게 제시된 사업 수행에 필요한 예산이 적기에 확보되어 지원되어야 할 것이다.

참고문헌

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

[2] Haeni, R.E., "Information Warfare: An Introduction," The George Washington University, 1997.

[3] GAO Report to Congressional Requesters, GAO/AIMD-96-84, May 1996.

[4] Alberts, D.S., "Defensive Information Warfare," NDU Press Book, National Defense University, Aug. 1996.

[5] Schwartau, W., "Class III Information Warfare: Has It Begun?," Terrorism-List, 1996.

[6] Department of Defense Directive(DoDD) S-3600.1 Information Operations(IO), Dec. 9, 1996.

[7] Libicki, M., "What Is Information Warfare?," Strategic Forum, No. 28, May 1995.

[8] Defense Science Board, "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," Nov. 1996.

[9] Christopher Null, How to Hire a Hacker,

[10] Fogleman, R.R. and S.E. Widnall, "Cornerstones of Information Warfare,

[11] Thomas, T.L., "Russian Views on Information-Based Warfare,

[12] Rathmell, A., et al., "Information Warfare Attack Assessment System(IWAAS),

[13] Steven Lavy, et. al., Hungint the Hackers, News Week, Feb. 21, 2000.

[14] Melinda Liu, Cyber Rattling, News Week, Mar. 20, 2000.

[15] Annual Report on the Military Power of the People's Republic of China, Jun., 2000.

[16] GAO, "Information Security - Computer Attacks at Department of Defense Pose Increasing Risks,

[17] Shalikashvili, J.M., "Joint Vision 2010