공학석사 학위논문

범정부 차원의 사이버테러 대응 전략에 관한 연구

지도교수 김 성 운

이 논문을 공학석사 학위논문으로 제출함

2003년 8월

부경대학교 산업대학원

정보통신공학과

강 수 동

이 논문을 강수동의 공학석사
학위논문으로 인준함

2003년 6월 21일

주 심 공학박사 윤 종 락 

위 원 공학박사 박 규 칠 

위 원 공학박사 김 성 운 

A Study on Strategy for Cyber Terror Prevention in Pan-Government Scope

Su-dong Kang

Department of Telematics Engineering

Graduate School of Industry, Pukyong National University

Abstract

The improvement of communication technologies and the explosive growth of Internet have brought the importance of intranet-based national information security infrastructure for cyber terrors. In order to support a safe information-oriented society, a systematic and synthetic cyber terror prevention system should be established in the pan-government scope.

In this thesis, we analyze the problems concerned to the nation-wide cyber terror prevention system. Based on this analysis, we propose a synthetic strategy for the nation-wide cyber terror prevention in the aspects of laws, regulations and organizations, education and management, technical developments, and international cooperation for information security related.

목 차

Ⅰ. 서 론

정보통신기술의 발달로 사회의 정보화가 고도화됨에 따라 경제, 사회, 문화 등 주요 국가기반 구조가 정보통신 인프라와 결합하고 있다. 이러한 변화는 Internet의 급속한 보급과 함께 우리의 삶을 매우 편리하고 풍요롭게 만들고 있으나, 이에 부수하여 사이버공간에서 발생하는 각종 신종 범죄 또한 급증하고 있다. 이러한 사이버범죄는 컴퓨터 해킹, 인터넷을 통한 홈페이지 훼손 및 네트워크 마비 등 매우 다양하며, 최근에는 사이버테러, 사이버전쟁 등의 개념으로까지 확대되어 사회적으로 심각한 문제를 낳고 있다. 특히 고속 네트워크 인프라가 전세계적으로 발전되고 보급되면서 네트워크를 마비시키는 악의적인 공격들은 그 피해 범위가 점차 확대되고 있으며, 사회 주요 기반 시설의 정보시스템 의존도가 심화됨에 따라 사이버테러는 개인 생활 뿐 아니라 국가 안보의 위해요인으로 작용하고 있다. 따라서 안전한 지식정보사회 구현은 사이버공간에서의 안정성이 우선적으로 확보되어야 하며, 범정부차원의 체계적이고 종합적인 사이버테러 대응책이 절실히 요구된다.

현재 세계 주요 국가들은 국가적 차원에서 사이버테러 대응역량 강화에 주력하며 사이버 공간에서의 우위를 선점하기 위해 많은 노력을 기울이고 있다. 예를 들면, 미국은 주요 정보 기반에 대한 범정부적 보호체계를 구축하기 위해 대통령 훈령인 PDD(Presidential Decision Directives) 63을 제정하고 국가종합 대책인 국가정보시스템보호계획(National Plan for Information Systems Projection)을 수립하여 추진중에 있으며, 유럽에서는 유럽전기통신표준협회 ETSI(European Telecommunications Standard Institute)를 중심으로 정보보호를 포함한 각종 기준 및 표준정책 개발 등 유럽의 정보기반구조 구축을 추진하

고 있다. 또 중국의 경우에는 군과 학계와의 연계를 통해 사이버戰 전문 인력을 양성하고 있고, 일본은 국가 주요 13개 기관으로 구성된 "정보보안관계성청국장회의"를 통해 사이버테러 대응방안 강구에 주력하고 있다. 우리나라의 경우는, 2001년 제정된 정보통신기반보호법을 중심으로 국가정보원, 정보통신부, 정보보호진흥원 및 검·경찰청 등 여러 기관에서 사이버테러에 대응하고 있으나 앞에서 살펴본 세계 각국의 실태와는 달리 범 정부차원의 종합적이고 명확한 체계가 구축되지 않은 실정이다.

따라서 향후 국내 주요 기반 시설들을 대상으로 발생하게 될 사이버테러에 대응하기 위해서는 국가차원의 정보보안체계 마련이 요구되며, 그것은 정보화 시대의 흐름에 맞춰 지속적이고 체계적으로 구축되어야 한다. 이를 위하여 본 논문에서는, 국가 사이버테러 대응능력 제고를 위해 사이버테러의 현황 및 주요국의 사이버테러 대응방안을 분석하고, 효과적인 국내 사이버테러 대응체계 구축을 위한 강화 방안을 정책조직 및 법·제도 체계, 보안 교육 및 관리 체계, 정보보호기술 구축 및 개발 체계, 국제협력 체계 등 4가지 측면에서 제시하고자 한다.

본 논문의 2 장에서는 사이버테러의 개념과 기술 및 특징을 분석함으로써 국가적 차원의 사이버테러 대응체계 도입 필요성을 정리한다. 3 장에서는 지금까지 발생한 사이버테러 사례 및 현황들을 살펴보고, 이를 통해 사이버테러들의 최근 동향을 분석한다. 4 장에서는 현재 운용되고 있는 국내·외 사이버테러 대응체제 현황들을 바탕으로 국내 사이버테러 대응체계 문제점을 분석하고, 6장에서는 5장에서 분석된 문제점들을 해결하기 위해 정책조직 및 법·제도 체계, 보안 교육 및 관리 체계, 정보보호기술 구축 및 개발 체계, 국제협력 체계 측면에서의 사이버테러 대응체계 구축 방안을 제시한다. 마지막으로 7장에서는 본 연구의 결론을 맺고 향후 연구과제에 대해 정리한다.

Ⅱ. 사이버테러 개요

본 장에서는 사이버테러의 개념을 정립하고 사이버테러의 원동력이 되는 기술들을 비교 분석한다. 또한 사이터테러의 전반적인 특징들을 분석함으로써 국가적 차원의 사이버테러 대응체제가 필요한 요인을 고찰한다.

1. 사이버테러의 개념

일반적으로 테러는 "정치적 목적을 달성하기 위해 정부나 대중 또는 개인에게 위해를 가하거나 예측할 수 없는 폭력을 사용하는 조직적인 행위"로 이해되나 시대적 상황에 따라 테러의 목표와 유형 등이 변화하기 때문에 그 개념 및 성격도 함께 변화하고 있다. 따라서 수천만대의 컴퓨터가 네트워크로 연결된 정보화시대에서는 테러의 수단과 대상이 사이버세계로 옮겨가고 있고, 과거에는 없었던 정보화시대의 산물로서 사이버테러가 새로운 테러의 유형으로 분류된다. 즉, 사이버테러는 "사이버공간에서 일정한 목적을 가지고 계획적으로 정보시스템을 공격하는 행위"로, 여기서 "사이버공간"은 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집, 가공, 저장, 검색 및 송신 또는 수신하는 정보통신망을 통하여 형성된 공간이라고 할 수 있다[1]. 그러나 사이버테러라는 용어가 아직까지 우리나라 법령에 사용된 예는 없으며, 다만 "컴퓨터통신망을 이용한 정보조작 및 전산망 파괴"(국가 對테러활동지침 제2조 제1호)[2]를 테러 유형의 하나로 규정하고 있을 뿐이다.

이 때 사회적이나 국가적으로 불안감을 유발시키는 사이버테러는 단순한 해킹이나 바이러스 전달에서 그치는 사이버 범죄와는 명백하게 구별해서 사용하는데, 이는 지금까지의 테러가 주요 인물의 납치나 댐·교량

등의 물리적인 폭파를 통해 국가기능을 마비시킨 것이라면 정보화시대에 등장한 사이버테러는 국가 경제 및 사회활동의 근간이 되는 정보통신기반을 파괴해서 특정한 기능을 마비시키는 행위이어야 하기 때문이다. 즉, 다수의 피해자의 전산망에 대하여 사이버 공격을 하였더라도 심각한 결과라고 볼 수 있는 피해가 발생하지 않았다면 이를 사이버테러라고 보기는 어려우며, 반대로 1명 혹은 소수의 개인의 컴퓨터 시스템에 대한 사이버 공격이라도 만약 그것이 결과적으로 한 사회나 국가에 공포심 내지 불안감을 조성할 수 있는 정도에 도달한다면 우리는 이러한 공격행위를 사이버테러라고 간주할 수 있다.

결론적으로 위와 같은 점들과 국제사회의 사이버테러에 대한 개념규정 및 우리나라의 현행법제를 종합하여 생각컨대, 사이버테러란 대체로 해킹, 바이러스유포, 논리폭탄전송, 대량정보전송, 서비스거부공격, 고출력 전자총 등을 통신망에서 사용하는 "컴퓨터 시스템 운영방해행위" 내지는 "정보통신망 침해행위", 또는 전자적 침해행위에 의하여 "국가적이나 사회적으로 공포심 내지 불안감을 조성하는 행위"라고 정의할 수 있다. 따라서, "컴퓨터시스템운영방해행위" 또는 "정보통신망위협 및 침해행위"와 "테러리즘(terrorism)"의 결합이야말로 사이버테러의 진정한 개념요소라고 할 수 있으며, 정보화사회 도래와 함께 국가와 사회의 주요 기반시설이 정보시스템에 대한 의존도가 심화되면서 사이버공간에서 행해지는 사이버테러는 물리적인 테러 못지않게 우리 사회를 혼란에 빠뜨리고 있다.

2. 사이버테러 기술

현재 사이버테러는 다양한 기술 및 접근 방식을 통하여 이루어지고 있으며, 이용하는 기술적 특성에 따라 발생하는 피해 규모도 뚜렷한 차이를 지닌다. 따라서 이 절에서는 다양한 사이버테러 기술들을 비교 분석하고, 이를 사이버테러 대응기술 방안을 제시하기 위한 기본 자료로 활용하고자 한다.

가. 해킹기술

컴퓨터 시스템을 해킹하는 방법에는 매우 다양한 기법들이 존재하고 있으며, 그 중 대표적인 몇 가지 기법들[3]을 간략하게 살펴본다.

1) 시스템의 환경 설정 변수를 이용

인터넷에 연결되어 사용되는 컴퓨터 시스템은 매우 다양한 운용체제를 가지고 있으며, 또한 다양한 사용자의 요구를 만족시키기 위하여 각 시스템 별로 환경변수(environment variable) 들을 이용하고 있다. 해커들은 바로 이러한 환경 설정 변수들이 잘못 설정되어 있는 경우 이를 이용하여 관리자의 권한을 획득하게 된다.

2) 사용자 도용

인터넷의 각종 웹 사이트나 혹은 메일 서버와 같이 다수의 이용자가 존재하는 경우, 각 사용자들은 기본적으로 패스워드를 통해 해당 시스템에 접근한다. 이때 일부 사용자들은 패스워드를 손쉽게 기억하기 위하여 매우 단순한 방식으로 만드는 경우가 많으며, 해커들은 바로 이러한 사용자들의 아이디(ID : Identity)를 도용하여 해당 시스템을 해킹 할 수 있게 된다.

3) 경쟁조건(race condition)을 이용

유닉스 시스템에서는 한정된 자원을 여러 개의 프로세서들 또는 여러 사용자들이 공유하게 된다. 따라서 한정된 자원들을 여러 객체들이 사용하려고 서로 경쟁하는 모양을 갖추게 되며, 이러한 현상을 이용하여 일반사용자가 시스템의 관리자 권한을 획득할 수 있게 된다. 그림 1은 SUN시스템에서 /bin/mail프로그램의 경쟁조건을 이용한 해킹 방법이다.

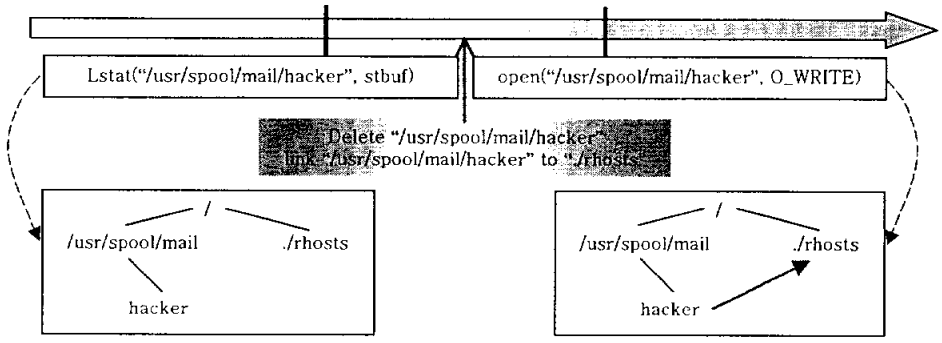


그림 1. SUN 시스템에서 /bin/mail 프로그램의 경쟁조건을 이용한 해킹

4) 버퍼 오버플로우(Buff Overflow) 취약점 이용

지정된 버퍼의 크기보다 더 많은 데이터를 입력하여 프로그램이 비정상적으로 동작하도록 만드는 방식으로, 해커는 이를 이용하여 공격하고자 하는 시스템을 파괴할 수도 있으며 관리자의 권한을 획득하여 정보 변조 및 유출 등을 시도할 수 있게 된다. 특히 이 기술은 1997 년 Phrack 49 호에 발표된 이후 해커들이 매우 자주 사용하는 공격수법의 하나가 되고 있다.

5) 네트웍 프로토콜의 취약점 이용

인터넷의 최초 구성 이유가 정보의 공유에서 출발되었듯이 인터넷 통신방식의 근간을 이루는 TCP(Transmission Control Protocol)/IP

(Internet Protocol) 프로토콜을 이용하여 해킹하는 방법은 매우 다양하며, 대표적으로 IP Spoofing 공격, SYN(Synchronize sequence Numbers) Flooding 공격, 암호 sniffering 공격 및 서비스 거부(DOS : Denial of Service) 공격 등이 있다.

먼저 IP Spoofing 공격은 신뢰관계에 있는 두 시스템 사이에서 한 시스템의 IP 주소를 해커가 도용하여 자신을 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속인 후 아무런 인증절차 없이 접근하는 방식으로, 그림 2 는 IP Spoofing 을 이용한 공격 과정을 보여주고 있다.

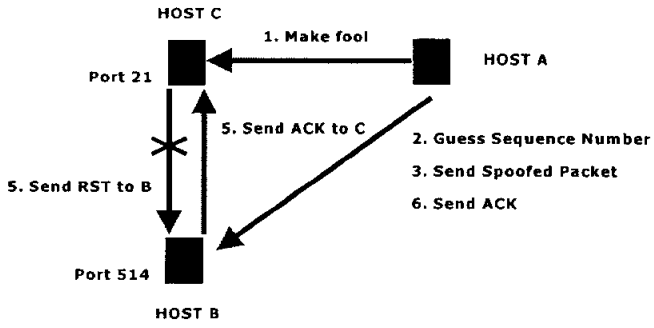


그림 2. IP Spoofing 을 이용한 공격

먼저 호스트 A 가 호스트 C 의 포트 21 번에 연결 요청을 계속 보냄으로써 호스트 C 의 포트 21 번을 마비시킨 후 호스트 A 는 호스트 B 의 포트 514 번에 연결 요청을 여러 번 보내어 sequence number 를 알아낸다. 그리고는 호스트 A 가 호스트 C 인 것처럼 자신의 소스 IP 주소 항목에 호스트 C 의 IP 주소를 써넣은 패킷을 만들어 호스트 B 에 전송하면 호스트 B 는 들어온 연결 요청이 호스트 C 로부터 온 것인 줄 알고 호스트 C 에 ACK(Acknowledgement)를 보낸다. 그러나, 호스트 C 의 port 는 이미 마비되었으므로 대답할 수 없으며, 이때 호스트 A 가 호스트 C 인 것으로 가장하여 호스트 B 의 SYN 에 대한 ACK 를 보냄으로써 호스트 A 과 호스트 B 와의 연결이 아무런 인증 없이 이루어지는 것이다.

다음으로 SYN flooding 공격은 인터넷의 주요 프로토콜 중 하나인 TCP 프로토콜의 연결설정 과정인 3-way handshaking 이라는 방법의 취약점을 이용하는 것이며, 암호 sniffering 네트워크상에서 흘러다니는 정보를 가지고 사용자의 패스워드를 등을 알아내는 공격 방법으로 매우 다양한 해킹툴들을 사용하여 손쉽게 공격대상 컴퓨터의 사용자 아이디 및 패스워드를 획득 할 수 있다.

마지막으로 서비스거부공격은 목표 대상 호스트의 마비 및 성능 저하를 일으켜 서비스를 하지 못하도록 하는 기법으로, 그림 3 과 같이 분산 서비스 거부 공격(DDOS : Distributed DOS)의 경우에는 하나 이상의 피해 시스템을 공격하기 위하여 여러 시스템이 활용된다.

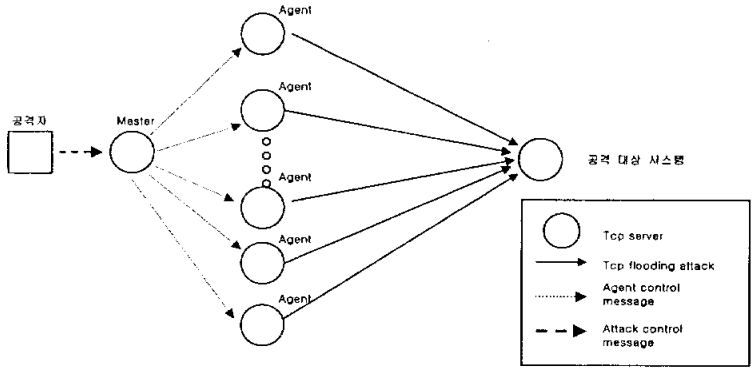


그림 3. 분산 서비스 거부 공격

즉, 공격자가 많은 수의 Agent 를 이용하여 공격할 호스트에 막대한 트래픽을 발생시켜 공격 대상 시스템을 무력화시키는 방법으로, 관리자의 권한 획득이나 데이터를 파괴 및 절취 보다는 시스템이 정상적인 서비스를 수행하지 못하도록 방해하는 목적을 지닌다. 이러한 공격법은 최근 급격히 증가하고 있는 전자상거래에서 심각하게 문제시되고 있고, 시스템 침입과 같은 다른 유형의 공격에 비해 공격의 흔적을 거의 남기지 않기 때문에 공격의 원인이나 공격자를 추적하기가 매우 힘들어 다른 공격 수단에 비해 남용될 소지가 많다.

나. 바이러스

일반적으로 바이러스는 프로그램을 변형 또는 삭제하여 주변기기에 오동작을 일으키거나 파일을 손상시키며 자기자신을 복제하는 등의 행위다. 이중에는 가벼운 것도 있지만 때로는 생명을 위협하는 독감처럼 치명적인 피해를 가져오는 경우도 있으며, 바이러스 유포에 의한 컴퓨터 시스템의 파괴, 데이터의 위/변조 등도 매우 다양한 수법들이 존재하고 있다. 이들은 감염 방법에 따라 원래의 프로그램을 파괴하지 않고 프로그램의 앞이나 뒤에 바이러스 프로그램이 추가되는 기생형, 원래의 프로그램이 있는 곳에 바이러스 프로그램이 겹쳐져서 위치하는 겹쳐쓰기형(Leprosy Virus, Lehigh Virus 등), EXE파일에 직접 감염되지 않고 같은 이름의 COM 파일을 만들어 여기에 바이러스 프로그램을 넣어두는 산란형(AIDS(Acquired Immune Deficiency Syndrome) II Virus 등), 프로그램 시작위치를 바이러스 프로그램의 시작위치로 바꾸어 줌으로써 컴퓨터 바이러스로서의 동작을 수행하게 하는 연결형(DIR-II Virus, Byway Virus 등), 윈도우(Windows) 상에서 사용되는 MS社(Microsoft Corporation) 제품의 매크로 기능을 이용하는 매크로형 등으로 구분할 수 있다. 운용체계에 따라서 분류하면 대부분의 바이러스가 속해있는 도스 바이러스, Win95/CHI, Anxiety_Poppy, Win3.1 Virus, Win32 Virus와 같이 윈도우 시스템에서 동작되는 바이러스, 어플리케이션에 내장된 매크로 혹은 스크립트 언어를 사용하여 제작된 바이러스로서 운영체제와 상관없이 해당 응용 프로그램을 플랫폼으로 하여 동작되는 어플리케이션 파생 바이러스, Linux/Bliss 등과 같은 리눅스(Linux) 바이러스, 자바(JAVA) 언어를 기반으로 동작되는 자바 바이러스 등으로 구분할 수도 있다. 감염부위에 따라 분류하면 Brain, Monkey 등과 같이 부트섹터에 자리잡는 부트

(boot) 바이러스, 예루살렘, Sunday, Crow, Win95/CHI 파일 바이러스, Invader, Euthanasia, Ebola 바이러스처럼 부트섹터와 파일에 모두 감염되는 부트/파일 바이러스, 감염 대상이 실행파일이 아니라 MS社의 엑셀과 워드 프로그램에서 사용하는 문서 파일에 감염되는 매크로 바이러스 등으로 구분 가능하다[3].

최근에는 네트워크와 연결된 컴퓨터의 주소록을 이용하여 순식간에 전세계에 e-mail을 감염시키는 웜(worm) 바이러스나 시스템내부에 잠복해 있다가 특정 요일 혹은 조건 하에서 동작하는 트로이 목마와 같은 지능형 바이러스가 점차적으로 증대되고 있으며, 특히 웜은 스스로 전파되는 악성코드로서 단시간에 수많은 시스템을 감염시켜 인터넷을 마비시킬 수 있다. 실례로, CodeRed는 2001년 7월 19일 단지 9시간 만에 25만대 이상의 시스템을 감염시켰고, 2003년 1월 25일 발생한 한국의 인터넷 마비사태도 윈도우 MS-SQL(Structured Query Language) 서버의 취약점을 이용한 새로운 웜 바이러스가 발생 원인으로 분석되었다. 또한, sadmind/IIS와 CodeRed는 웹 사이트 변경 페이로드를 가지고 있을 뿐 아니라, W32/leaves와 같은 웜은 동적으로 변형되는 능력을 보유하고 있기도 하다. 그림 4는 년도별로 웜의 진화를 나타낸 것으로 1988년 모리스 웜을 시작으로 날로 진보해가고 있으며, 현재 인터넷 기반 기설에 가장 커다란 위협을 줄 수 있는 사이버테러 기술로 꼽히고 있다[4].

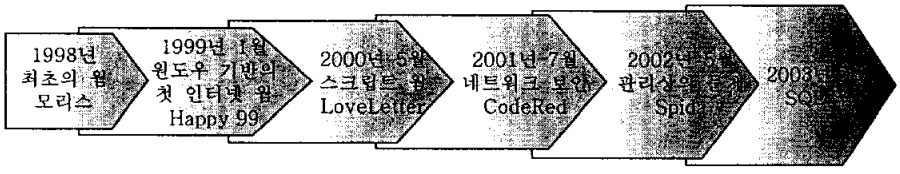


그림 4. 년도별로 본 웜의 진화

다. 해킹툴

해킹툴이란 원래 시스템의 관리자들에게 시스템의 보안 수준을 높여줄 수 있는 편리한 도구로 제공되던 것이었으나, 해커들에 의해 악용됨으로써 해킹의 주요 수단으로 발전되고 있는 추세이다. 즉, 이러한 툴들은 인터넷을 통하여 매우 손쉽게 구할 수 있기 때문에 많은 초보 해커들을 양성하는 결과를 낳았으며, 대표적인 도구들[3]은 다음과 같다.

1) 내부점검 도구

시스템의 각종 파일, 디렉토리 권한, 패스워드 및 시스템 설정 등을 알아내어 해킹 작업을 용이하게 해주는 도구로서, COPS(Computer Oracle and Password System), Tiger 및 Tripwire가 대표적이다. 특히 Tripwire은 해커들이 해킹 하고자 하는 시스템에서 그들을 은닉시키기 위한 도구로 널리 사용되고 있다.

2) 패스워드 점검도구

여러 가지 규칙과 많은 단어가 포함된 사전을 조합하여 사용자들의 패스워드를 알아내는 crack 프로그램, John 프로그램, LophtCrack 프로그램 등이 여기에 속한다. 원래 이러한 도구들은 시스템 관리자들이 사용자들의 패스워드를 좀더 강화시키고 관리할 수 있도록 하기 위해 제공되었으나 이를 악용하여 해킹에 사용하고 있는 것이다.

3) 보안 취약점 스캐너 도구

시스템의 보안 취약점들을 점검하여 알려주는 도구로서, ISS(Internet Security Scanner), SAINT(Security Administrator's Integrated Network Tool), SATAN(System Administrator Tool for Analyzing Network), nmap 및 xnmap 등이 있다. 이들 대부분은 원격지 시스템들

의 문제점들도 검사하여 보고해 주기 때문에 먼 거리에서도 해킹이 용이하게 하며, 특히 nmap과 xnmap은 원격지에서 목표 시스템이 제공하고 있는 서비스 포트들이 무엇인지를 알려주는 도구로서 현재 가장 많이 사용되고 있다.

4) 모니터링 도구

네트워크 인터페이스 상에서 데이터들을 모니터링하는 Tcpdump, Sniffit, Snoop 등이 이용된다. 즉, 패킷의 헤더 정보를 보여주는 Tcpdump와 패킷이 가지고 있는 데이터의 내용을 보여주는 Sniffit 및 현재 전송되고 있는 각종 패킷들을 분석하여 보여주는 Snoop를 이용하여 해커들은 원하는 정보를 추출하고 변경 할 수 있으며, 이러한 도구들은 각종 해킹 기술들과 함께 사이버테러의 밑거름으로 제공되고 있다.

라. 전자기적 위협

최근 많이 등장하고 있는 chipping, nano machine, HERF(High Energy Radio Frequency) Gun, EMP(Electro-Magnetic Pulse) Bombs, AWCM(Autonomous Mobile Cyber Weapon) 등 주로 하드웨어를 마비 또는 파괴시키는 사이버테러 기술들[5]을 일컫는다. 즉, 직접적으로나 간접적으로 하드웨어에 접근하여 시스템 및 네트워크를 공격하는 기술들로, 특히 주파수 및 전자기파를 이용하는 HERF Gun이나 EMP Bombs은 노출된 컴퓨터나 통신 시스템 등 주변의 모든 전자시설을 파괴할 수 있어 막대한 피해를 야기된다. 또한 AWCM은 외부의 조종이나 도움 없이 스스로 네트워크를 돌아다니며 시스템을 파괴하거나 조작하기 때문에 마치 지능을 갖춘 사이버테러 무기로 간주되어 진다

3. 사이버테러 특징

일반적으로 사이버테러는 간단한 조작, 속임수로 광범위한 피해를 유발할 수 있으며, 점진적으로 발달되는 각종 해킹 기술들에 의해 익명성, 접근성, 비대칭성, 시공초월성 및 대량 피해 등의 특징을 나타내는 것으로 요약된다. 그리고 이러한 특징들은 독립적 이라기보다는 효율적인 공격을 하기 위한 상호 의존적 특징으로 볼 수 있으며, 각 특징을 구체적으로 살펴보면 다음과 같다.

먼저 익명성[6,7]은 사이버테러의 가장 큰 위협요소로서, 사이버공간에서는 자신을 노출시키지 않은 채 활동하는 것이 가능하다. 즉, 마음만 먹으면 전 세계 네트워크에 자신을 은닉한 채 컴퓨터 조작만으로 공격이 가능하고, 공격 받은 전산망이나 기간시설이 완전 무력화되거나 정보유출 및 조작 등이 이루어진 후에야 공격 받은 사실을 감지 할 수 있다. 따라서 사이버테러에 대한 죄의식이 희박하게 함으로써 더 큰 범죄를 가능케 하고, 실제적으로 많은 사이버 공격자들이 자신에 대한 추적과 검거를 피하기 위해 익명성을 이용한 사이버 공격을 감행하고 있다.

두 번째 특징은 접근성[5]으로, 사이버테러는 물리적 수단으로 정상적으로 보호되고 있는 핵심 기반에 대해서 피해를 입힐 수 있다. 즉, 공격대상에 접근할 필요 없이 네트워크가 연결된 곳이면 지구촌 어디에서나 공격이 가능하고, 네트워크 전체를 차단하지 않는 한 예방이 어렵고 증거를 남기지 않아 공격자와 공격한 장소의 추적이 어렵다.

사이버테러의 세 번째 특징으로는 비대칭성[6,7]이다. 사이버공간에서는 개인 또는 작은 집단만으로도 네트워크에 연결되어 있는 컴퓨터를 이용하여 막대한 피해를 일으킬 수 있다. 즉, 사이버 시위와 같이 대규모 인력의 참여가 필요한 경우를 제외하고는, 굳이 대규모 인력과 장비를

투입하지 않아도 소기의 목적을 충분히 달성할 수 있다는 의미다. 또한 사이버테러를 수행하는 데 많은 비용이나 국가적 지원이 없어도 정보체계에 대한 전문 지식만 있으면 사이버테러 기술 개발이 가능하고, 개발된 기술로 네트워크를 통해 접근할 수만 있으면 엄청난 규모의 사이버테러를 가져올 수 있다.

네 번째 사이버테러의 특징은 사이버공간이 시간적 및 공간적으로 제약을 받지않는 시공초월성[8]을 갖는다는 점이다. 즉, 사이버테러 공격은 국가의 모든 기반구조가 상호 연결되어 있는 사이버공간에서 수행되기 때문에 누구든지 마음만 먹으면 별다른 어려움 없이 네트워크를 통해 접근 가능하므로 어디든지 잠재적인 전방이 될 수 있다.

마지막으로 사이버테러 특징은 대량 피해를 유발하는 것으로[8], 하나의 컴퓨터만 점령할 수 있다면 네트워크에 연결되어 있는 이웃 컴퓨터들을 쉽게 공격하는 것이 상대적으로 어렵지않다. 특히 네트워크가 전세계적으로 점차 확대되는 추세기 때문에 사이버 위협은 여러 목표를 동시에 겨냥할 수 있고, 이는 클린턴 대통령의 국가 안보 보좌관이었던 Anthony Lake에 의해서도 언급되었던 사실이다[9]. 따라서 사이버테러는 전력·통신·금융망 마비, 철도·항공·군사장비 시스템 파괴 및 군·경 비상연락망 교란 등 국가안보를 위협할 수 있는 엄청난 피해와 혼란을 초래할 수 있다.

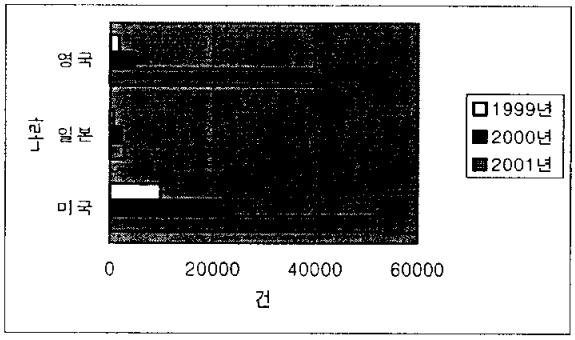
Ⅲ. 국내·외 사이버 테러 현황

해마다 사이버테러 사고가 급격히 증가하고 있고, 이는 매우 다양하고 고도화된 수법으로 사이버공간을 침투하여 전세계적으로 심각한 문제를 초래하고 있다. 따라서 이 장에서는 현재까지 국외와 국내의 사이버테러 현황 및 사례를 살펴보고, 앞으로의 사이버테러 대응체계를 위한 최근의 사이버테러 사고 특징을 분석하고자 한다.

1. 국외 사이버테러 현황 및 사례

가. 국외 사이버테러 현황

현재 사이버테러에 대한 피해는 전세계적으로, 그림 5는 침해사고대응팀협의회(CERT/CC: Digital Freedom Network-Computer Emergency Response Team/Coordination Center)에 의해 조사된 미국, 일본 및 영국의 해킹사고 현황[5]이다.



	미국	일본	영국
1999년	52,658	2,853	40,274
2000년	21,756	2,224	4,773
2001년	9,859	788	1,712

그림 5. 세계 주요국의 해킹 사고 현황

먼저 미국의 해킹 건수 변화를 보면, 1999년도 9,859건에서 2000년도 21,756건으로 221%증가하였다. 이와 같은 추세는 계속되어 2000년에 21.756건에서 2001년 52,658건으로 1년 사이에 2배 이상 증가한 것으로 나타나고 있다. 그러나 9.11 테러 사건 이후 사이버 보안에 대한 감시활동이 강화됨에 따라 미국 정부기관의 컴퓨터에 대한 해킹 건수가 감소세를 보이고 있다. 미 연방 컴퓨터 사고 보고센터(FCIRC : Federal Computer Incident Response Center)가 집계한 정부 컴퓨터의 응급상황 보고건수는 8월에 114회였지만, 9월에는 63건으로 떨어졌으며 10월광 11월에도 각각 75건, 65건을 기록했다. 이에 따라 전문가들은 앞으로의 해킹활동은 정부보다 기업 및 개인들에 집중될 것으로 내다보고 있다.

일본의 경우 JP(Japan)CERT/CC에 접수된 부정 접속건수는 1999년 788건에서 2000년 2,224건으로 282% 증가하였으며 2001년에는 2,853건으로 집계되었다. 정보처리진흥사업협회(IPA: Information Technology Protection Agency)에 접수된 건수는 각각 55건, 143건 550건이었다.

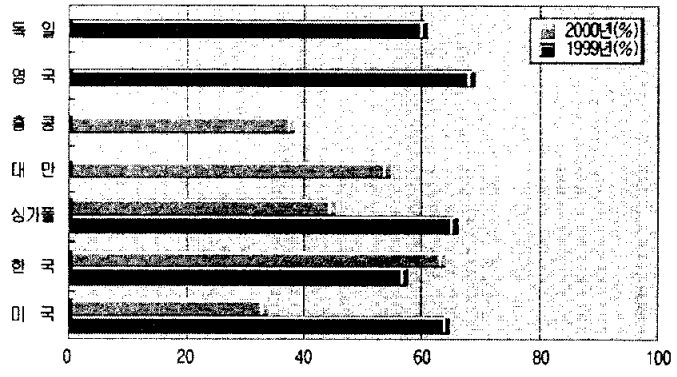


그림 6. 주요국의 바이러스 감염률

더불어 세계 각국의 바이러스 감염률 현황(IPA 및 JP/CERT의 집계)을 그림 6을 통해 보면, 1999년도 3,645건에서 2000년도 16,109건으로 해킹 증가율 보다 더 가파른 증가 현상을 보이고 있다. 그리고 영국의 경우는 무려 10배나 증가한 40,274건이 발생하였다. 또한 일본의 IPA가 1999.12~2000.11 기간동안 주요국의 300~600개 기관에 대해 바이러스 감염률을 조사한 자료에 의하면, 한국의 경우 56.8%(1999년)에서 62.9%(2000년)로 가장 악화된 것으로 나타났으며, 싱가폴의 경우 66.3%(1999년)에서 45.4%(2000년)로 개선된 것으로 파악되었고, 미국의 경우 64.5%(1999년)에서 32.4%(2000년)로 가장 크게 개선된 것으로 나타났다. 이와 같이 볼 때, 한국이 6개국 비교조사에서 가장 불량상태로 전락한 바 이에 대한 원인분석과 대처가 뒤따라야 할 것이다.

나. 국외 사이버테러 사례

1) 미공군 로마 연구실(Air Force Rome Lab) 공격[10]

1994년, 뉴욕에 위치한 미공군 로마연구실에 대한 공격이 탐지된 사건으로, 당시 16세의 영국 소년이 궁중전화를 통하여 인터넷에 연결한뒤 워싱턴, 시애틀, 뉴욕을 거쳐 로마 연구실에 공격을 시도한 것으로 밝혀졌다. 또한 이 소년은 나토 사령부, 가다드 우주 비행 센터(Goddard Space Flight Center), 라이트-패터슨 공군기지(Wright-Patterson Air Force Base) 등도 목표로 하고 있었던 것으로 알려졌다.

2) 솔라 선라이즈(Solar Sunrise)[10]

1998년 2월, 미 국방부는 솔라리스 운영체제의 취약성을 이용한 공격

을 받은 사례로, 하버드대학교와 아랍에메리터연합(UAE : United Arab Emirates)에서 시작되었다. 그 후 UAE와 유타주립대학교에서도 공격이 시도되었으며, 나중에는 독일, 프랑스, 이스라엘, UAE, 그리고 대만에까지 확산되었다.

3) 인도 원자력 연구소 침투[11]

1998년 6월, 핵 실험에 반대하는 해커 그룹 "miwOrm"이 인도의 바바원자력연구소(BARC : Bhabha Atomatic Research Center)의 컴퓨터 네트워크에 침입하여 홈페이지 일부를 변조하고 5MB(megabyte)분의 전자 메일을 다운로드한 사건으로, 이들은 미 항공우주국(NASA : National Aeronautic and Space Administration), 미 해군, 미 공군의 서버를 경유하여 BARC에 침입한 것으로 알려져 있다.

4) 유고전시 미 국방성 및 백악관 웹 페이지 공격[12]

1999년 3월 미국과 나토의 유고침공에 반대하는 전자적 침입자들이 미국방성 및 백악관 웹 사이트에 대량의 전자우편 폭탄 및 바이러스에 감염된 메일을 보내어 웹 서버를 24시간 동안 다운시킨 사례로, 이에 대응하여 미국에서는 유고 전산망에 침입하여 기존자료 삭제 및 바이러스를 침투시켜 전산망을 마비시켰다. 실제적으로 물리적 피해는 별로 없었지만 수천명의 미국인들에게 자국내 주요 기관의 보안이 미약하다는 인식을 갖게 하는 계기가 되었다.

5) 유고전시 중국대사관 오폭에 따른 미국에 대한 공격[13,14]

1999년 5월 7일, 유고의 베오그라드에 있는 중국대사관에 대한 오폭 사건이 반발하자 중국 해커들은 미국 에너지부, 내무부 및 백악관 웹사이트 공격 등 즉각적인 사이버 시위를 시작하였다. 이 때, 인터넷상의 몇 개 사이트에서는 미국 사이트에 대한 대량 컴퓨터 공격을 시도하였고, 미국 금융 사이트를 대상으로 한 컴퓨터 바이러스를 배포하기도 하였다.

6) 중동 무력충돌에 따른 사이버전쟁 [11]

2000년 9월말에 이스라엘과 이슬람과격파 사이에 무력충돌이 발생한 이후 미국과 이스라엘 및 이슬람교 웹사이트에 대한 상호 공격이 되풀이 된 사례로, 초보적인 전자메일 공격이나 크래커 집단에 의한 조직적 공격도 행해졌다. 이 밖에 웹 사이트의 변조 및 신용카드 번호나 회원기록의 도난 등도 발생하였고, DDOS 공격(예 : Smurf 공격)이나 조직적 침입행위와 같이 공격수법도 날로 격화되는 등 2001년에 들어서도 사이버 공격이 꾸준히 이루어졌다.

7) 미-중 공군기 충돌 사건에 이은 사이버 전쟁[13,14]

2001년 EP-3 정찰기 사고에 의해 촉발되어 한 달여 동안 지속된 사건으로, 중국의 해커들은 워싱턴 해군통신기지국(Washington Navy Communications Station)과 해군광역수송국(Navy Service Wide Transportation) 사이트를 시작으로 백악관 웹 사이트 마비까지 시켰다. 이 분쟁으로 미국은 1,038개의 웹 사이트가 변조되었고, 중국은 1,600개의 웹 사이트가 침입을 당하였다.

2. 국내 사이버테러 현황 및 사례

가. 국내 사이버테러 현황

인터넷의 급속한 보급으로 인해 국내에서도 사이버테러 발생이 매우 급격하게 증가하였으며, 이는 미국, 일본, 영국, 싱가폴 등 세계 각국에 비해 매우 심각한 상태이다. 따라서 이 절에서는 최근 국내 사이버테러 현황[15] 및 사례들을 다각도에서 분석하고, 이를 통해 향후 국내 사이버테러 대응방안 제시에 있어 기본 자료로 활용하고자 한다.

1) 국가·공공기관 사이버테러 발생현황

근래 정부 및 공공기관과 관련한 사이버테러가 급격히 증가하는 추세를 보이고 있다.

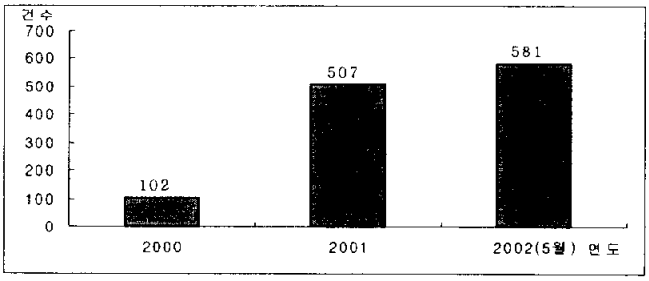


그림 7. 국가·공공기관 사이버테러 연도별 발생현황

위의 그림 7은 최근 3년간 국가 및 공공기관의 연도별 해킹사고 발생현황을 보여주는 것으로 2000년도에는 102건이었던 사이버테러가 2001년에는 507건으로 2000년에 비해 497% 증가하였다. 더 나아가 2002년 상반기에는 발생 건수가 581건으로 2001년 한해의 건수와 비슷하게 나타났

으며, 사이버테러가 매달 평균 100건 이상으로 증가하는 추세를 보임에 따라 2003년도 말에는 2천건이 넘을 것으로 예상되어진다.

발생 기관별로 살펴보면 그림 8에서 보여지듯이 2002년 한 해 동안 교육기관이 475건으로 가장 큰 비중을 차지하였고 지자체 49건, 산하기관 14건, 연구기관 12건 순으로 나타났는데, 상대적으로 보안시스템이 미비하고 실무담당자의 전산보안 분야에 대한 전문지식이 취약한 교육기관에서 사이버테러 발생 빈도가 높게 나타났다.

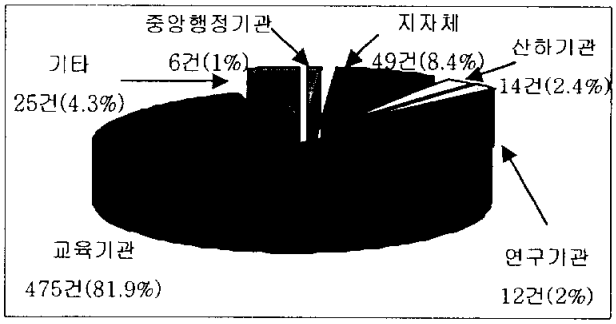


그림 8. 2002년 기관별 사이버테러 발생현황

따라서 2002년에 발생한 사이버테러 사고의 가장 큰 특징은 집중적인 보안관리 실시기관과 그렇지 않은 기관의 사고발생 비율이 현저히 차이가 나고 있다는 점을 들 수 있다. 즉, 전담관리자 및 각종 보안시스템이 설치되어 있어 상대적으로 보안관리가 철저한 중앙행정기관은 발생건수가 6건으로 전체 1%에 불과하나, 초·중·고 등 교육기관은 총 475건으로 전체 81.9%를 차지하고 있다. 그리고 산하기관 및 연구기관은 정보보호의 투자증가에 힘입어 사고발행이 중앙행정기관 다음으로 낮게 나타났다.

2) 운영체제(O/S)별 사이버테러 발생현황

운영체제(O/S : Operating System) 측면에서도 사이버테러는 해마다 양상을 달리한다. 그림 9는 2001년과 2002년도 운영체제별 사이버테러 사고 발생현황을 나타내는 것으로, 2002년의 두드러진 특징은 MS社 윈도우 시스템 계열의 사고발생이 2001년 20%에서 2002년에는 29%로 늘어나고 있는 반면, Unix는 10%에서 3%로 급감했다는 점이다. 이와 같은 현상은 최근에 MS社 윈도우에 대한 공격기법이 증가하면서 사고발생도 증가한 것으로 판단되며, 리눅스를 많이 사용하고 있는 초·중·고를 제외한 나머지 국가·공공기관에서 윈도우 관련 사고 발생 비율이 50%에 육박했다.

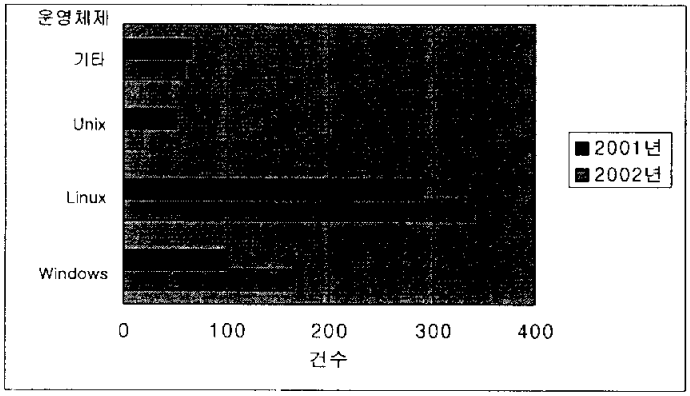


그림 9. 2001년/2002년 운영체제(O/S)별 사이버테러 발생현황

아울러, 유닉스 계열이 감소한 이유는 사용자가 감소와 함께 2002년도 들어 신규 해킹기법이 나타나지 않은 것에서 원인을 찾을 수 있다. 그리고 리눅스는 예산상 이유로 보안관리가 어려운 기관에서 주로 사용되고 있으나 지속적으로 신규기법이 나타나고 있어 사고발생 비율이 높은 실정이다.

3) 침투수법별 사이버테러 발생현황

발생 빈도 못지않게 사이버테러의 침투수법 또한 매우 다양해졌으며, 그림 10은 2002년 한 해 동안의 침투수법별 피해현황을 나타낸 것이다. 이를 구체적으로 살펴보면, 웜 바이러스 감염이 222건으로 전체의 38.4%를 차지하여 가장 많았으며 관리자 권한 도용이 125건으로 다음 순위를 차지하였고 스팸릴레이도 119건으로 세번째를 기록했다. 전반적으로 인터넷을 이용하는 공격기법인 웜 바이러스 및 스팸릴레이 등이 사이버테러의 주 요인으로 나타났으며, 특히 짧은 시간에 급속히 확산되어 막대한 피해를 유발하는 웜 바이러스 사용이 높은 것으로 분석되었다. 또한 보안 지식이 부족한 관리 인력들의 실수도 사이버테러 사고의 주요 요인으로 나타났으며, 체계적으로 보안 인력을 양성할 수 있는 교육 환경이 시급히 요구되어 진다.

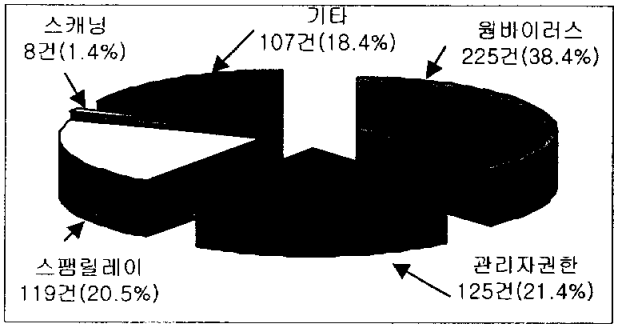


그림 10. 2002년 침투수법별 피해현황

4) 피해유형별 사이버테러 발생현황

2002년 사이버테러 사고를 피해 유형별로 살펴보면, 그림 11에서 보

여지듯이 해킹을 당한 시스템이 다른 기관을 공격하기 위한 경유지로 활용된 경우가 80.7%(435건)로 가장 높은 비율을 차지했고, 해커의 실력을 과시하거나 전시적 효과를 노린 홈페이지 변조가 7%(41건), 자료유출 1.6%(9건) 등의 순으로 나타났다. 그 외 기타에서는 여러가지 유형들 중에서도 한번 침입에 성공한 시스템에 재침입이 용이하도록 해주는 백도어(back door) 프로그램 설치가 비교적 높았는데 향후 백도어의 기술발전과 더불어 세련되고 은밀한 커널 백도어가 출현할 것으로 예상됨에 따라 이 분야에서의 사이터테러 방지 기술개발이 필요하다.

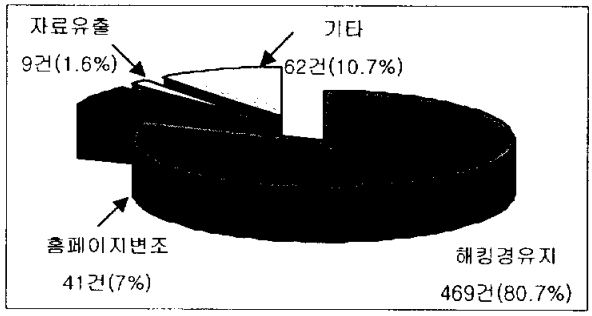


그림 11. 2002년 해킹사고 피해유형별 발생현황

나. 국내 사이버테러 사례

국내에서도 자료유출, 정보변경 및 바이러스를 이용한 각종 사이버테러 사례가 발생하였다. 1999년 전국 대학의 전산망을 관리하는 서울대 전산망에 40여건의 해킹 사고가 발생하여 보안사고에 속수 무책인 것으로 밝혀졌는데, 특히 서울대 전산망을 중간 거점으로 이용해 다른 외국기관의 전산망을 해킹하는 사고가 주를 이루어 해킹을 당한 외국대학 및 기관으로부터 항의 메일이 속출하였다[16]. 또한 1999년 3월에는 해킹 프로그

램인 백오리피스를 이용하여 국산 인공위성 우리별 3호의 중요 자료들이 유출되는 사고가 있었고, 2001년에는 4월에는 신용카드 회사의 정보망이 뚫려 47만 명의 신용카드번호 및 780만 명의 개인정보가 유출되어 전자상거래 시장을 마비시킬 수도 있는 사건이 발생했다. 이렇듯 인터넷 기업의 고객정보 관리 및 유출 문제가 심각한 문제로 대두되고 있는 가운데 2002년 7월에는 유명 인터넷증권정보제공업체 고객 5만 명의 증권정보관련 비밀번호 및 증권계좌 등 자칫 개인과 사회에 큰 혼란을 야기할 수 있는 정보들이 불법 유출되었고[17], 이는 사이버공간에서 해킹으로 인한 개인정보 유출 문제가 심각한 상태임을 보여 주고 있다. 특히, 이러한 인터넷 업체 중 10%만이 개인정보보호를 위한 보안프로그램을 사용하고 있어 그 문제는 더욱더 심각할 것으로 여겨진다.

사이버테러 사고의 두드러지는 특징 중 또 하나는 강력한 공격기능을 겸비한 각종 웜 바이러스가 출연하여 전세계적으로 많은 피해를 야기하는 것으로, 국내에서도 웜 바이러스에 의한 막대한 규모의 피해가 속출하였다. 그 사례로 2001년 7월에 "CodeRed"라 불리는 바이러스로 인해 국내 약 3만 6천 여대의 시설이 피해를 입었고, 이로 인해 대전청사 내 일부 감염기관에서는 적시에 예방조치를 강구하지 않아 몇 시간동안 정보통신망에 장애가 발생하였다. 또한 2001년 9월에는 이전의 바이러스와는 달리 첨부된 파일을 단순히 클릭하거나 미리 보기만 하여도 네트워크를 통해 시스템을 빠르게 감염시키는 "Nimda"에 의해 2만 2천 여건의 피해 발생하였으나, 이 바이러스에 대한 치료 백신 제작이 어려워 일주일간 국내 전산망을 어지럽혔다[6]. 웜 바이러스에 의한 범죄는 점점 더 심각해져 지난 1월 25일에는 전국 유무선 인터넷이 순식간에 마비되는 대형 사고가 발발했는데, 이는 "Slammer" 웜 바이러스 공격에 의해 인터넷기간 망의 DNS(Domain Name System) 서버들이 다운되면서 일어났다[18]. 이 때, 인터넷이 서비스가 7시간 가까이 중단되면서

온라인을 기반으로 하는 공공기관 및 각종 업체들이 업무가 마비되어 관련 업계가 수 백억 원대의 막대한 손실을 입었는데, 외국보다 우리나라 피해가 컸던 것은 서버 관리자의 보안의식 취약으로 외국보다 많은 SQL서버가 감염(일본의 약 7배, 중국의 약 2배)되고, 국내에 루트 DNS가 없어 국제 회선 포화에 따른 국내 DNS 과부하 및 초고속통신망의 높은 보급률에 의한 급속한 확산 때문이다. 또한 1월 30일에도 트로이 목마로 인해 전국 11개 지역의 초고속 인터넷 서비스가 4시간 여 동안 불통되는 사태[18]가 발생함으로써 국내 사이버테러 사고의 심각성이 매우 수준에 도달했음을 여실히 보여주는 계기가 되었다.

3. 최근의 사이버테러 사고 특징

최근 발생한 사이버테러 사고 유형에 따른 주요 특징을 분석하고 이에 대한 보안대책을 고찰한다.

첫 번째로 신종기법의 공개와 그에 따른 피해 확산의 가속화이다. 2002년도는 연초부터 SSH(the Secure Shell) 보안 취약성으로 인한 피해가 광범위하게 발생하였다. 이는 2001년도 말에 인터넷 보안사이트에서 소개되었을 당시에는 별로 피해가 없었으나, 국제 해커 그룹인 "teso team"에서 관련 취약성 공격프로그램을 제작하여 인터넷으로 유포한 이후 2002년도 초반부터 많은 피해가 발생하였다[19]. 즉, 신종기법이나 보안버그(bug)보다는 공격프로그램이 공개될 때 사이버테러 사고 발생이 급증하게 되며, 아직까지는 공격프로그램의 공유가 일부 고급 해커들간 제한적으로 이루어져 다행스러웠으나 최근 인터넷을 통해 신종기법의 공격코드가 공개되고 외부에 빠르게 확산되면서 전 세계적으로 피해건수가 다시 급증하는 특징을 보이고 있다. 따라서 신종기법에 대한 보안대책으로는 침입차단시스템 및 보안시스템의 보안규칙 설정에 신중을 기하고,

불필요한 포트는 닫아두며, 제공하는 서비스는 최소화하여야 한다. 그리고 운영중인 주요 시스템에 대해서는 수시로 보안 패치(patch)를 설치하는 것도 하나의 방안이다.

두 번째는 MS社 NT 및 윈도우2000 시스템에서 피해가 급증하고 있다는 것이다. 2000년도까지는 윈도우시스템이 리눅스 등 유닉스계열의 시스템보다 사고 발생이 없어 상대적으로 안전한 시스템으로 인식되어 왔다. 그러나 2001년 초반부터 해커들의 MS社 관련 시스템에 대한 공격기법 연구 및 공개가 증가하면서 피해도 급증하고 있다. 대표적인 예로 지난해 윈도우시스템의 취약성인 IIS(Internet Information Server) Unicode, IIS ISAPI(Internet Server Advanced Programming Interface) Extension 및 front page 등을 겨냥하여 웜 바이러스(예 : Nimda, CodeRed)와 해킹 기술을 이용한 사고가 지속적으로 발생하였으며, 최근에도 MS-SQL 서버 취약성을 이용한 해킹공격과 이를 활용한 "Spida" 웜 바이러스가 출현하여 피해를 유발하고 있다[4,5]. 이는 MS社 윈도우 시스템은 사용이 편리하고 시스템 내부정보를 비공개로 하여 보안적인 측면에서 많은 장점이 있었으나 해커들의 집중적인 연구 및 하나, 둘씩 발견되는 보안 취약성으로 인해 범용성이 높은 윈도우시스템이 매우 위협적인 사이버테러 요소로 자리잡고 있다. 보안대책은 보안버그 공지에 대해 관심을 기울이며 보안 패치 및 서비스 팩(pack)을 설치하고, 포트 관리 및 서비스 제어를 철저히 해야 한다.

다음으로 사이버테러 사고의 주요 특징 중 하나는 웹(Web) 포트(80번)를 이용한 공격이 증가한다는 것이다. 최근에 침입차단시스템 등 각종 보안시스템을 도입하고 운영하는 기관이 늘어나면서 과거와 같이 손쉬운 침투는 불가능해지고 있다. 따라서 해커들은 이러한 문제를 해결하기 위해 외부에 항상 공개된 웹 포트를 대상으로 한 공격기법을 지속적

으로 개발하고 있으며, 그 이유는 대부분 기관이 홈페이지를 운용하기 위해 웹 포트를 필수적으로 열어두어야 하기 때문이다. 미 보안사이트인 "SANS(System Administration, Networking, and Security Institute)"[20] 발표에 따르면, 80번 포트를 이용한 공격이 최근 가장 급증하고 있는 사이버테러 사고로 분석되었다. 관련 보안대책으로는 불필요한 웹 운영을 삼가고 게시판에서 실행 권한을 금지시키며 보안 패치를 설치해야 한다.

네 번째 사이버테러 사고의 특징으로는 각종 웜·바이러스 증가에 의해 동시다발적인 대량 피해를 들 수 있으며, 이는 인터넷의 급속한 확산과 함께 전세계적인 네트워크가 형성됨에 따라 더욱 심각한 피해를 야기하고 있다. 2001년도 3월부터 개발, 유포되면서 악명을 떨친 웜 바이러스로는 2001년도 3월 리눅스 시스템을 대상으로 한 "li0n", "Ramen" 등이 있고, 5월에는 미·중 항공기 충돌사건으로 촉발된 양국간 사이버 분쟁시 출현한 "Sadmind/IIS" 등이 있으며, 7월과 9월에는 전세계를 강타한 "CodeRed" 및 "Nimda" 웜 바이러스 등이 있다[4]. 특히, CodeRed 및 Nimda는 지금까지 개발된 그 어떤 종류보다 강력하여 전세계적으로 100만대 이상의 피해를 초래하였으며, 이 두 가지 웜 바이러스는 여전히 왕성한 활동을 전개하면서 지속적인 피해를 유발하고 있다. 또한 2002년도에도 "My Party", "Gop", "Yaner", "Klez" 및 "Spida 등 각종 웜 바이러스가 지속적으로 출현하여 수 천만건의 피해가 발생하였으며, 2003년 1월에는 "Slammer" 웜 바이러스로 인해 국내에서만 수 백억원 상당의 손실이 있었다[4,15]. 이처럼 기존의 바이러스가 소멸하고 웜 바이러스가 증가하는 이유는 인터넷을 통해 유포가 용이하고 한번의 공격으로도 자동적으로 확산되어 동시에 대규모 피해를 유발할 수 있다. 즉, 해커의 입장에서는 장점이 많은 공격수단이며, 향후에도 웜 바이러스로

인한 피해가 급증할 것으로 예상된다. 따라서 클라이언트 단계에서는 웜을 탐지하고 제거할 수 있는 백신프로그램을 이용하고, 네트워크 단계에서는 웜 바이러스가 내부로 침투를 하지 못하도록 포트제어 및 바이러스 월 등을 사용하는 것이 바람직하다.

최근 사이버테러와 관련하여 마지막 특징으로는 스팸(spam)메일을 이용한 피해 증가를 들 수 있다. 여기서 "스팸 메일"이란 사용자의 요구 없이 무차별적으로 배포되는 광고성 메일로서 대부분 송신자가 불명인 것을 말한다. 즉, 스팸메일 발송자는 제3자 시스템의 sendmail 프로그램 취약성을 이용하여 불법으로 메일서버를 통해 스팸메일을 발송하는데, 이러한 스팸메일은 광고를 위해 대용량의 이미지 정보를 전송하는 경우가 대부분이므로 정보통신망 전체에 대한 트래픽을 증가시키거나 과도한 디스크 및 메모리를 사용하게 만들어 정상 사용을 방해한다. 특히 우리나라는 보안이 취약한 초·중·고 시스템을 스팸메일 경유지로 이용하는 사례가 빈번히 발생하고 있어 외국으로부터 "스패머(spammer) 국가"라는 오명을 받는 등 외교문제로까지 비화된 적도 있다. 따라서 보안대책으로는 스팸메일 차단 서비스를 제공하는 사이트(RSL : Relay Stop List, http://relays.visi.com, ORDB : Open Relay DB, http://www.ordb.org)를 활용하고, 자신의 시스템이 스팸메일 경유지로 이용되지 않도록 메일 구동 프로그램을 최신판으로 갱신하거나 보안 패치를 설치하며, 메일서버를 운영하지 않는 기관에서는 관련 프로그램 구동을 즉시 중지시켜야 한다.

결론적으로 사이버테러 기술이 날로 발달해감에 따라 사이버테러 사고도 점점 고도화, 대규모화 및 악성화 되는 특징을 보이고 있다.

Ⅳ. 국내·외 사이버테러 대응체계

세계 주요 국가들은 21세기 정보화 사회에서 국가 경쟁력 우위학보는 물론, 매년 2~3배씩 증가하는 사이버테러로부터 자국의 정보 자산을 보호하고 미래의 사이버戰에 대비하기 위하여 조직과 제도 정비, 전문인력 양성 및 기술개발 등 사이버공간에서의 경쟁력을 지속적으로 강화하고 있다. 따라서 이 장에서는 국·내외 사이버테러 대응실태 및 체계를 비교하고 고찰함으로써 국내 사이버테러 대응체계의 문제점을 분석하고자 한다.

1. 국외 사이버테러 대응체계

가. 미국

미국은 1998년 5월 대통령 훈령(PDD63)에 따라 급증하는 사이버테러로부터 자국내 정보통신 기반구조를 보호하기 위해 범정부 차원에서 대응체계를 마련하고 이를 시행해 나가고 있다. 이를 위해 2000년 1월 국가 주요 기반구조 보호를 위한 국가 차원의 계획을 발표 하였으며, DARPA(Defense Advanced Research Project Agency)에서는 정보보증 및 생존(IA&S : Information Assurance & Survivability) 프로그램을 진행하고 있다[3]. 특히, 9.11테러 직후부터 사이버테러 발생 가능성에 대한 우려의 목소리가 높아지면서 미국은 사이버테러에 대한 대비를 더욱 강화하였으며 이는 다음과 같다.

먼저 조직 체계 측면에서는 2001년 국토안보국(Office of Homeland Security)을 설립하여 물리적 테러뿐 아니라 사이버테러 대응 및 복구에 관한 활동을 조정하는 임무를 부여하였으며, 대통령 사이버보안특별보좌

관을 임명하여 정보시스템 보안을 위한 각 부처, 연방·지방 정부의 활동을 총괄 조정하고, 침해사고 복구를 총괄하며 주요정보통신시설을 운용하고 있는 민간 분야와의 업무를 조정하고 협의하는 역할을 부여하였다. 또한, 대통령주요기반보호협의회[President's critical Infrastructure Protection Board]를 설립하고, 미국의 국가 주요 기반시설 보호를 위한 최고 정책기관의 임무를 부여하였다. 그리고 2002년에는 테러 대책을 총괄하는 새로운 부서로서 국토안보부(Department of Homeland Security)를 설립하여 국토안보 뿐 아니라 정부의 정보보안을 강화하는 임무까지 부여하여 사이버공격으로부터 미국을 보호하는 역할을 수행하고 있다[21].

법제 정비와 관련하여서는 애국법(USA Patriot Act of 2001)[22], 사이버보안연구개발법(Cyber Security Research and Development Act)[23], 전자정부법(E-Government Act of 2002)[24], 국토안보법, 및 사이버보안강화법(CSEA : Cyber Security Enhancement Act)[25] 등을 신설하였고, 이 중 사이버보안강화법은 사이버테러에 대해 개인 뿐만 아니라 국가적인 차원에서 경제 및 중요 인프라를 위헌하게 할 경우 종신형까지 처벌할 수 있도록 규정하고 있다. 또한 보안기술 강화를 위해서 현재 600만 달러 수준에 머물고 있는 사이버보안 연구지원금을 2003년에는 1억 1100억 달러로 확대하여 각 대학이 사이버 보안 전문인력을 양성하고 보안기술 연구 및 개발을 추진할 수 있도록 할 예정이다[25]. 그리고 사이버보안을 강화하기 위한 국가차원의 기획서인 사이버보안국가전략(National Strategy to Secure Cyberspace)[26]과 주요기반물리적보호국가전략(National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)[27]을 발표하는 등 다각적인 노력을 기울이고 있다.

나. 유럽

유럽에서는 유럽전기통신표준협회 (ETSI : European Telecommunications Standard Institute)를 중심으로 유럽 및 전세계 차원의 정보기반 구조의 구축을 위하여 정보보호를 포함한 각종 기준과 표준 정책을 개발하고있다. 특히 22차 ETSI 기술회의에서는 EPIISG(European Project on Information Infrastructure Starter Group)을 창설하여 각종 정보통신 분야의 프로젝트에 대한 업무를 수행하고 있으며[3], EU(the European Union) 의장국인 벨기에는 급증하는 사이버테러 피해를 최소화하기위해 유럽 차원의 보안 시스템 구축을 추진 중에 있다. 더불어 EU 각국은 자국 내 정보통신 기반구조 구축을 위해서도 활발한 활동을 수행중이며[28], 이를 몇 가지 살펴보면 다음과 같다.

먼저 영국은 21세기 전쟁의 주요 특징 중 하나를 비군사적인 사이버 위협으로 보고 정보통신 기반구조에 대한 안전 및 보안대책을 효율적으로 마련하기 위해 2000년 5월 "국가기반시설 보안조정기구"를 설립하였으며, 2001년 무역산업부, CSSA(Computing Services and Software Association), 전자비지니스연합회, NHTCU(National Hi-Tech Crime Unit)가 참여하여 사이버 보안단체인 "SAINT(Security Alliance for Internet and New Technology)"를 발족하였다. 또한, 강력한 보안기능을 지닌 네트워크 구축을 추진중이며, 고수준의 정보 및 컴퓨터 보안을 보장하고 원격 통신 및 사생활을 보호를 가능케 하는 기술 개발에 더욱 주력하고 있다.

프랑스는 정보통신기반구조 침해에 대비한 대응책으로서 정부 및 각 분야에서 장기적인 관점으로 정보보호정책 협력 및 보안기술 개발을 추진중이며, 재정정책면에서도 이를 뒷받침하기위한 노력을 진행하고 있다 .

독일도 사이버테러에 대응하기 위해서 컴퓨터 긴급대응팀인 "DFN (Digital Freedom Network)-CERT"를 통해 침해사고 처리, 기술지원, 정보수집·분배 및 취약성분석 등의 업무를 수행하고 있으며, 국가적 차원의 암호 방식 및 인증 기술을 지정하였다.

다. 일본

일본은 90년대 후반 인터넷의 급속한 보급으로 사이버테러가 급증하게 되자 1997년 통산성 산하에 "네트워크 보안대책위원회"를 설립하고 사이버테러 예방 및 피해방지를 연구에 착수하였다. 그 결과 사이버테러 발생시 긴급히 요구되는 보호 대책을 제시하였으며, 여기에는 정보시스템과의 접속시 보안대책, 전화 접속시의 보안대책, 무선 응용 접속시 보안대책, 네트워크 계획·설계·구축시의 보안대책, 컴퓨터 바이러스에 관한 보안대책 및 사회 공학적 측면에서의 보안대책 등을 담고 있다. 이러한 기반 위에 일본은 1999년 사이버테러에 방지를 위해 "부정접속행위금지 등에 관한 법률"을 제정하고 관방성, 경찰성, 방위청 및 금융감독청 등 구가 주요 13개 기관의 국장급으로 구성된 "정보보안관계성청국장회의"를 설치하여 국가 기반시설에 대한 사이버테러 대응방안 강구에 주력해 왔다[3]. 특히, 9.11테러 이후에는 총리가 주재하는 긴급 관계성청회의를 거쳐 생화학·핵에 대한 대응책 마련과 함께 사이버테러 대책 강화 등을 중점 추진 사항으로 의결하였으며, 이는 사이버테러를 대테러 대책의 하나로 분류함으로써 기존의 대테러 대책에서 진일보한 자세를 보여주고 있다. 또한 2001년 10월에는 사이버테러 특별행동계획에 대한 후속조치[29]를 통하여 행정, 전력, 및 교통 등 국가 주요 인프라의 사이버테러

대응협력체계를 구축하였으며, 이는 현재까지도 추진되고 있다.

더불어 전자정부 및 민간 주요 인프라에 대한 사이버테러 대책을 원활히 수행하기 위하여 2002년에는 내각관방 정보보안대책추진실에 국가긴급대응팀(National Incident Response Team)[30]을 설치하고, 정부부처 정보보안 상담대응, 사이버테러 관련정보의 수집·분석, 사이버테러 피해 확산 방지 및 복구에 대한 기술적 지원 등의 임무를 부여하였다.

한편, 방위청은 Info-RMA(Information-based Revolution in Military Affairs) 추진에 있어서 다양한 센서 등을 이용하여 다중화 및 감내화된 정보네트워크를 기반으로 육·해·공 자위대가 정보를 실시간으로 공유하고 미군과의 상호운용성을 확보하며 사태의 변화에 유연하게 대응하는 등 신속하면서 효율적으로 전력을 발휘할 수 있는 체계를 구축하기 위해 노력을 기울이고 있다.

라. 중국

현재 중국의 인터넷 인구는 약 5,660만명으로 미국에 이어 세계 2위의 인터넷 시장으로 불리고 있다. 그러나 최근 인터넷 인구가 급증하면서 금융 및 전자상거래 사이트가 잇달아 해킹 당하는 등 사이버테러가 빈번히 발생함에 따라 이에 대한 대응책 마련에 부심하고 있는 실정이다.

물론, 중국은 1985년부터 사이버戰을 대비하여 "국방과학기술정소센터"를 설립하였고, 남경, 북경, 난주군구 등에서 여러 차례에 걸친 모의 사이버戰 훈련도 실시하였다. 또한 국가안전과 방호의 측면에서 중국과학원 내 "첩보안전기술공정연구센터"에 안전응용, 비밀번호이론 및 안전관리 등의 연구분과를 설치하여 공격과 방어를 겸하는 사이버戰에 대응

방안을 추진하였다. 또한, 1997년에는 "컴퓨터바이러스부대"를 창설하여 지속적으로 미국, 나토, 일본, 인도네시아, 대만 등에 대하여 공격을 시도하여 왔고, 미 하원에 제출된 보고서에 의하면 "도상전쟁 및 훈련 시나리오상에 적 컴퓨터망의 취약점을 이용하여 오판을 유도하는 정보를 입력하고 데이터를 변경하며 컴퓨터의 작동을 중지시키는 등 적의 지휘통제체계를 공격하는 내용이 포함되어있다"고 밝히고 있다. 그리고 1999년에는 강택민 국가주석을 포함한 정부 핵심간부들이 미래 하이테크戰 수행방안을 결정하였고, 컴퓨터전문가로 구성된 전자전 특수부대인 "Net(Network) Force"를 창설하여 사이버 공격 및 정보교란 모의 훈련을 수시로 실시하였다. 최근 중국의 사이버戰 및 사이버테러 대비체제를 살펴보면, 2000년 8월 대만에 7,200여건의 사이버 공격을 실시하였고 1,000여명 규모의 사이버戰 담당기구를 창설한 것으로 알려지고 있다. 또한 일부 군부대에서는 지역대학과 군 간부 양성계획을 체결하여 졸업 후 사이버戰의 주요요원으로 활용하려는 계획도 추진하고 있다. 특히, 걸프戰 이후에는 낡은 재래식무기와 전투운용능력으로는 대만 및 미군을 이길 수 없다고 판단하여 유사시 적군의 지휘체계, 미사일 유도 및 무기 보급체계 등 정보시스템을 무력화시키기 위한 전략을 수립하는 등 사이버戰에 대비해오고 있다. 이외에도 지난 2001년에 1월부터 해킹, 바이러스 전파 및 유해정보 전파 등 컴퓨터 관련 범죄활동 방지를 위한 "컴퓨터정보시스템 안전보호등급 구분" 제정하여 시행하는 등의 제도적 체제를 정비하였고, 컴퓨터제품의 안전성을 평가하는 "국가정보 안전 측정센터"를 설립하여 자체적인 보안기술 개발에 주력하는 등 국내 보안체계 제고를 위해 다각적인 노력을 기울이고 있다[31].

마. 북한

우리나라와 인접한 북한에서도 사이버테러에 대응하는 "강성대국" 건설을 목표로 경제적이고 부가가치가 높다고 판단되는 소프트웨어 기술개발에 전념하여 해킹 및 바이러스 침투 등 사이버戰 수행 능력이 상당히 향상된 것으로 판단 되어진다. 이미 90년대 초반부터 전방부대와 인민무력부간 광케이블을 구축하였으며, 정보전·전자전·지휘자동화 분야의 전문가 양성을 위해 설립된 지휘자동화 대학은 C4I체계 연구작업을 통하여 매년 전술·전자전분야 전문인력 100명을 양성하고 있다. 또한 김일성종합대학에 1999년 컴퓨터과학대학을 설치하고, 매년 "전국 대학생 컴퓨터 프로그램 경연"을 개최하여 우수인력을 발굴하여 사이버戰 전문 인력으로 양성하고 있다. 더불어 북한은 한-미 양국군의 첨단 컴퓨터 통신망을 이용한 훈련 비중이 커짐에 따라 주요 정보기관이 경쟁적으로 미 국방부와 미국기자의 인터넷을 조회하고 있는 것으로 알려지고 있으며, 미사일 타격수단의 보유 외에 정보기술의 활용 및 확보에 노력을 기울이는 등 사이버戰에서 우수한 기술을 확보한 것으로 파악되고 있다[32].

2. 국내 사이버테러 대응체계

현재 국내 사이버테러 대응체계는 다양한 기관들의 대응 활동을 통해 크게 국가·공공 분야와 민간분야로 나뉘어 구축되고 있으며, 이 절에서는 국내 사이버테러 대응 조직과 정책 및 활동을 분석한다.

가. 사이버테러 대응 조직 및 정책

국내 사이버테러 대응 조직은 대표적으로 국가정보원, 정보통신부, 검·경찰청 및 국방부 등 네 개의 수행기관과 한국정보보호진흥원(KISA :

Korea Information Security Agency), 국가보안기술연구소(NSRI : National Security Research Institute), 한국전자통신연구원(ETRI : Electronics and Telecommunications Research Institute) 내 정보보호 기술연구본부 및 정보보호전문업체 등 다양한 지원기관을 통해 추진되고 있으며[5,33], 사이버침해에 대응하기 위한 국내 대응 조직들의 체계 및 정책은 다음과 같다.

먼저 수행기관측면에서 살펴보면, 국가정보원은 국가· 공공 기관 및 국가 안보관련 시설 정보보호와 관련된 사이버테러 대응업무를 담당하는 기관으로, 국가정보보안업무 기획, 조정 및 보안정책을 수립하고 국가기관 및 공공단체를 대상으로 정보시스템의 보안대책 지원하며 국가·공공기관용 암호장비나 보안시스템 개발 보급, 정보보호시스템의 인증업무 등을 수행하고 있다. 또한 1998년부터는 정보보안관리반 편성 및 정보보안119(NISSC : National Information Security Service Center)를 개설하여 해킹·컴퓨터 바이러스에 대한 국가·공공기관 정보통신망의 예방 활동과 사고발생시 대응방법 및 복구기술도 지원하고 있다. 이에 반해 정보통신부는 민간부문에 대한 정보보호 정책 및 법 제도를 수립하고 시행하는 기관으로, 정보화 역기능에 관한 대책, 개인정보보호를 위한 대책, 정보보호산업의 육성과 인력양성 및 정보보호시스템의 평가 등에 관한 사항들을 수행하고 있다. 다음으로 검·경찰청은 주로 사이버범죄와 관련된 대응업무를 수행하고 있으며, 이들은 컴퓨터범죄에 대한 적극적인 대응과 조직적인 수사를 위하여 대검찰청 인터넷 범죄수사센터, 22개 컴퓨터범죄 수사부 및 경찰청 사이버테러 대응센터 등을 설치하여 운영하고 있다. 이 중 사이버테러 대응센터는 95년 해커수사대에서 시작하여 2000년 7월 전문인력 및 장비의 대폭적인 보강을 통해 사이버테러 대응센터로 개편되었으며, 경무관을 중심으로 협력운영팀, 신고경보팀, 수사

팀 및 기법개발팀 등 4개 팀으로 구성되어 있다. 마지막으로 국방부는 국방 CERT, 국군기무사, 한국국방연구원 및 국방과학연구소 등을 통해 사이버테러에 대응하는 국방기본정책을 수립, 연구 및 개발하고 있으며 국방에 필요한 병기, 장비 및 물자에 관한 기술 개발도 수행하고 있다.

다음으로 각 지원기관의 사이버테러 정책을 살펴보면, 1996년에 한국정보보호센터로 출범하여 2001년 정보통신망이용촉진 및 정보보호등에 관한 법률에 따라 한국정보보호진흥원으로 개명된 KISA는 기획단, 기술단, 평가인증사업단, 기반보호사업단, 개인정보분쟁조정위원회 사무국 등으로 구성되어 주요 정보통신기반시설 보호를 지원하기 위해 정보보호시스템 평가, 해킹·컴퓨터 바이러스에 의한 침해사고 대응, 전자서명 인증체계 기반 강화, 개인정보 침해 신고센터 운영 등의 기능을 수행하고 있다 . 다음으로 NSRI는 국가 정보보안 분야의 통합 연구기관으로 2000년 ETRI 부설 "국가보안기술연구소"라는 명칭으로 설립되었다. 주요 목표와 임무는 국가정보기반구조의 안전을 위한 범국가적인 사이버테러 대응체제 구축으로, 이를 위해 기술지원팀과 침해사고처리팀으로 편성된 해킹사고대응팀(CIART : Computer Incident Assistance and Response Team)을 구축하여 국가용 암호 이론체계 연구, 암호분석 기술연구, 정보전 기술 연구, 위성·유선·무선통신보호기술 연구 및 국가 정보보안정책 연구 등을 수행하고 있다. 이와 더불어 ETRI 정보보호기술연구본부는 네트워크보안연구부, 차세대보안응용연구부 및 정보보호기반연구부 등 3개부 16개팀으로 구성된 국가연구기관으로 안전한 정보사회 건설과 전자정부 구축에 필수적인 정보보호기술의 개발 및 관련 핵심 시스템의 개발을 주목적으로 하는 연구개발 업무를 추진하고 있다. 또한 주요 정보통신기반시설에 대한 취약점 분석, 평가 및 보호대책 수립업무를 지원하는 민간업체로서 마이크로테크놀러지, 시큐아이닷컴, 시큐어소프트, 안철

수 연구소, 에스큐브, 에이쓰리시큐리티컨설팅, 에스티지시큐리티, 해커스랩 등 9개 업체를 2001년에 정보보호전문업체로 지정하였으며, 이 업체들은 향후 3년간 주요 정보통신기반시설에 대한 정보보호컨설팅 업무를 담당하게 된다.

그러나 위와 같은 조직들의 사이버테러 대응체계 및 정책들은 먼저 법·제도적기반위에서 수행되어야 하며, 이를 위해 국내 주요 정보통신기반시설을 보호하는 "정보통신 기반보호법"을 2000년에 제정하여 2001년 7월부터 시행하고 있다. 또한 민간 부문의 개인정보를 보호하기 위하여 2000년 1월 1일부터 "정보통신망이용촉진 및 정보보호등에 관한 법률"을 시행하고 있으며, 이 법은 OECD(Organisation for Economic Cooperation and Development)에서 제시한 개인정보보호 8원칙을 수용하고 EU의 개인정보보호지침을 고려하여 개인정보보호기본원칙, 정보주체의 권리, 사업자의 의무, 개인정보침해에 대한 구제 등을 규제하고 있다. 이외에 신용정보의 이용과 보호에 관한 법률(1995), 전자거래기본법(1999) 및 전자서명법(1999) 등에서도 해당 분야와 관련된 사이버테러 대응규정을 두고있고[1], 그 예로 해킹 및 바이러스 관련한 사이버테러에 경우에는 정보통신망 이용촉진등에 관한 법률과 전자거래기본법 및 형법 등의 일부 조항을 통해서 수행하고 있다.

나. 사이버테러 대응 활동

국내 사이버테러 대응은 앞에서 언급한 조직 및 기관들의 다양한 활동들을 통해 추진되고 있으며[5,33], 이는 다음과 같다.

먼저 국가.공공기관을 대상으로 국가정보원에서 운영하는 정보보안관리반은 최신기술을 이용하여 각급 기관의 정보시스템에 대한 예방활동

업무를 수행하고 있으며, 2001년에는 30여개 기관을 대상으로 네트워크 실정에 맞는 보안정책 및 안전한 보안시스템 운영방안 등 제반 보안기술 지원활동을 전개한 바 있다. 더불어 정보보안119는 국가정보원이 21세기 사이버戰 대응체계 구축 사업의 일환으로 해킹 및 컴퓨터바이러스 감염 등 정보통신망 보안사고 처리 전담반으로, 국가·공공기관에서 사이버테러가 발생한 경우에 사고를 접수하고, 피해기관을 방문하여 사고 원인을 조사,분석·및 복구하는 업무를 수행하고 있다. 이 외에도 사이버테러 예·경보 및 인증제품 소개와 정보보안 교육 및 홍보 등의 업무를 수행하고 있으며, 이미 2001년도에 국가·공공기관의 해킹사고에 대한 분석을 통한 "사이버테러 10대 예방대책"이라는 보안권고문을 작성하고 배포한 바 있다.

또한 국가·공공기관의 해킹사고 급증 추세에 적극 대처하기 위해 2001년에 개설된 국가보안기술연구소의 CIART는 초·중·공 등 교육기관의 해킹사고 발생시 대응 및 복구업무를 수행하고 주요 정보통신기반구조의 피해전파를 최소화하기 위해 기술지원팀에서는 최신 해킹에 대한 기초기술 및 대응기술을 연구개발하고 있다. 아울러, 침해사고처리팀은 사고기관에 온라인 지원 및 파견지원을 수행하거나 사고현장 로그를 확보하는 등 현장에서 사이버테러 대응 및 복구조치를 수행한다.

민간분야 사이버테러 사고에 대해서는 한국정보보호진흥원의 "해킹·바이러스상담지원센터"가 개인 또는 민간의 침해사고 예방대책 등을 수행하고 있으며, 여기에는 특수번호 118을 부여하여 사람들이 언제 어디서나 쉽게 이용할 수 있도록 24시간 내내 긴급대응 및 자문상담을 해줌으로써 피해를 입은 이들의 기술적인 어려움들을 신속하게 해결하여준다. 또한 국내 피해가 확산될 가능성이 있는 사안일 경우에는 대국민 긴급경보를 발표하고, 필요에 따라 검·경찰청과도 협력한다. 더불어 함께 운

영하고 있는 침해사고 대응팀인 CERT/CC-KR(Korea)은 국내 전산망 운용기관등에 대해 통일된 협조 체제를 구축하여 국제적 침해사고 대응을 위한 단일창구를 제공하고 있으며, 이들은 2001년에 CERT 구축 및 운영을 주요 내용으로 세 차례의 기술 세미나와 한 차례의 해킹방지 워크샵도 개최하였다.

그리고 사이버범죄와 관련해서는 대검찰청 인터넷 범죄수사센터 및 컴퓨터 수사부와 경찰청의 사이버 테러대응센터를 통해 수행 중이며, 이들 중 대검찰청의 인터넷범죄수사센터는 해킹이나 컴퓨터 바이러스 유포와 같은 신종범죄 및 전자상거래를 이용한 개인정보침해 등과 관련한 수사업무를 수행하고 있으며, 22개 컴퓨터수사부서는 컴퓨터 수사장비의 확보 및 기타 검찰수사의 정보화 기반으로 컴퓨터범죄를 효율적으로 예방하고 단속하는 주요 임무를 시행하고 있다. 또한 경찰청의 사이버테러대응센터는 사이버범죄 사건 신고 접수상담과 초동조치를 담당하고 있고, 사이버범죄와 관련한 고소·고발 등을 처리하고 있으며, 사이버공간에 대한 24시간 순찰을 통해 해킹이나 바이러스유포 및 전산부정조작 등 사이버테러범죄 수사하고 지도한다.

3. 국내 사이버테러 대응체계 문제점

지금까지 국내 사이버테러 사고 현황 및 정책현황을 살펴보았고, 이는 범정부차원의 종합적이고 명확한 체계를 통해 지속적으로 이루어져야 한다. 그러나 국내 사이버테러 대응체계는 여러 기관들의 독립적인 활동을 통해 이루어지고 있으며, 이는 사이버테러에 대하여 신속하고 원활하게 대응하지 못함으로써 많은 문제점을 야기시켰다. 따라서 이 절에서는 현재 우리나라가 직면한 사이버테러 대응체계의 문제점을 분석하고자 한다.

먼저 정책조직 및 법·제도 측면에서의 문제점은 법·제도 미비로서, 사이버테러 기술이 나날이 고도화됨에 따라 법적 한계의 존재는 특히 중요하다. 물론 우리나라도 개인정보보호에 관한 법·제도적 장치는 어느 정도 구색을 갖추고 있으나, 이는 비접촉 및 비대면으로 사이버공간에서 이루어지는 불법행위를 규제하기에는 아직까지 미비한 실정이다. 더불어 현행 법 및 제도들이 갈수록 지능화, 악성화, 고도화 및 다양화되는 사이버테러 기술에 미치지 못하는 점도 문제시되고 있으며, 이러한 사이버 범죄에 대한 제반적인 사항을 규제할 수 있는 특별법 제정 및 새로운 입법 노력이 요구되어진다. 다음으로 정보보호 육성을 위한 예산 부족 및 전자정부 정보보호 정책을 체계적으로 수립하고 각 관련 기관들의 활동을 총괄적으로 조정할 수 있는 권한과 자원을 가진 최고 정책기구의 부재가 문제점으로 지적될 수 있다. 즉, 현재 사이버테러 대응 업무를 수행하고 있는 각 기관은 정보보호 전담조직도 없을 뿐만 아니라 정보보호에 필요한 예산 및 전문인력마저 확보하지 못해 정보보호를 위한 체계적이고 효율적인 대응이 어려운 실정이다. 따라서 정보보안 분야에 대한 예산과 조직의 충분한 지원이 없다면 갈수록 고도화되고 지능화되어 가는 공격자의 침투를 막아내고 대응하는 데 많은 어려움을 겪을 수 밖에 없다. 또한 침해사고시 이에 대한 적절한 방어, 경고, 복구 및 정보공유 등을 수행할 수 있는 체계적인 긴급대응체계 구축도 미흡한 실정으로, 정보보호진흥원의 118, 국가정보원의 정보보안119 및 검찰청과 경찰청의 컴퓨터범죄 담당 부서 등이 이를 다루고 있으나, 이들만으로는 폭증하는 사이버테러 사고를 감당하기가 어렵다. 따라서 사이버테러 대응정책을 체계적으로 수립하고 각 관련 기관들의 활동을 총괄적으로 조정할 수 있는 권한과 자원을 가진 최고 정책기구가 절실히 필요하다.

다음으로 보안 교육 및 관리면에서는 사회 전반에 걸친 정보보호 인식 부족을 가장 큰 문제점으로 들 수 있다. 우선적으로 최고관리자의 관심과 지원의 부족을 지적할 수 있는데, 국가 전체의 정보보호는 국가의 안보 및 국민의 생명과 재산을 보호하는 필수적인 기반임을 감안한다면, 최고지도자의 적극적인 대응체계 추진이 무엇보다도 필요하다. 특히 사이버테러 사고는 관련 기관의 이해관계와 민간부문의 기본권보장 등에서 마찰이 일어날 수 있기 때문에 최고지도자의 적극적인 관심과 지원 없이는 충분한 효과를 거두기가 어렵다. 이는 국민들도 예외가 아니며, 현재 우리나라는 사이버테러 사고의 80%가 국민들의 정보보호 인식부족으로 발생될 만큼 정보보호에 있어 국민들의 인식이 심각한 수준에 이르고 있다. 특히 정부내부에 근무하는 공무원들의 정보보안에 대한 인식부족은 더욱 큰 문제로서, 아무리 많은 자원을 투입하여 보안시스템을 갖추었다 하더라도 인식이 부족한 공무원의 부주의로 침투가 방치된다면 주요 국가기반시설이 마비되어 엄청난 혼란을 야기할 수 있다. 이렇듯 정보보호 인식이 사회전반적으로 부족한 이유는 정부와 보안전문가 및 시민이 유기적으로 연결되어 있지않기 때문으로, 정부와 정보보호전문가들 및 국민들의 연계를 통한 정보보호 교육 및 홍보가 절실히 필요하다. 더불어 정보보호가 제대로 되기 위해서는 기술적인 전문가가 우선적으로 필요한데 반해 현재 국내 보안전문인력은 매우 부족한 실정이다. 특히, 사이버테러가 사고영역이 광범위해짐에 따라 다양한 분야에서 보안 전문인력이 요구되어지고 있으나 국내 보안 인력 대부분이 유닉스 등 소형시스템에 편중되어 있어 메인 프레임의 운영체제나 제어시스템 등의 보안이 매우 취약하다. 또한 사이버범죄를 수사하는 기관에서도 자체적으로 직원을 교육시켜 컴퓨터 전문요원으로 활용하고 있음에 따라 컴퓨터공학이나 프로그램에 대한 지식이 짧은 시간에 학습되기 어려운 특성을 감안한다면, 이들이 사이버테러를 막

기에는 현실적으로 많은 문제점이 있다. 이는 민간전문보안요원의 양성하고 평가하는 인증기관의 부재가 그 요인으로, 교육 담당기관을 기반으로 한 체계적인 정보보안 교육 환경이 요구되어진다.

정보보호기술 구축 및 개발 측면에서의 문제점은 다음과 같다. 정보보호 기술은 정보보호의 기반이 되는 인증 및 암호기술과 정보보호 시스템 구축기술 및 정보보호 관리기술로 크게 나누어 생각할 수 있으며, 이들은 서로 상호 보완적으로 작용하여 정보보호 수준을 향상시켜야 한다. 그러나 현재까지는 주로 단일 목적을 가진 정보보호시스템 형태로 개발, 설치 및 운영되어 왔으며, 이러한 단일 기능 시스템은 특정한 목적과 기능을 가지고 설계되고 구현되어 다른 정보보호시스템과의 협력이 용이하지않은 편이다. 따라서 다양한 정보보호시스템 구축은 관리기능 자체도 복잡하게 만들고 있으며, 높은 수준의 보안지식을 지닌 보안전문관리자를 필요로 한다. 또한 제품개발 시 정보보호 측면이 미흡하여 정보통신 시스템 구축 후 문제점에 대한 대책을 수립하고 있으며, 이는 정보보호 제품이 취약한 S/W를 기초로 구축되어 원천적인 보안문제점이 내포되어 있다. 더불어 정보보안기술에 대한 연구 및 개발 투자도 매우 부족한 실정으로, 갈수록 보안침해기술이 발전하고 있는 상황에서 첨단 보안기술에 대한 연구 및 개발 투자가 미비하다면 적절한 대응을 취하기 어려울 것이다. 특히 최근 인터넷 환경이 널리 퍼지면서 해킹이나 바이러스 등 보안침해 기술들이 악성화, 지능화 및 고도화됨에 따라, 국가 안보 및 국가 기밀에 관한 정보보호기술을 외국에 의존하는 것은 심각한 문제를 초래할 가능성이 있으나 현재 국내 정보보호 업체 대부분이 영세하므로 정보보호기술 개발에 어려움을 겪고 있는 실정이다

마지막으로 국제협력측면에서는 사이버테러 대응체계가 자국 중심으로만 구축되어 있다는 점이다. 컴퓨터 및 통신기술의 발달로 전세계적인 인프라 구축이 용이함에 따라 사이버테러에 의한 피해 또한 전 세계적인 경제 및 사회 전반에 걸쳐 심각한 영향을 미칠 수 있다. 따라서 사이버테러 대응체계에 대한 국제적 협력 관계가 어느 때 보다 시급한 실정으로, 선진 각국은 첨단기술범죄의 수사 및 기소 역량을 강화하는 것과 범죄인도와 상호 법적 지원을 통한 국제사법 공조체제를 강화하기로 하는 국제 협력체제 구축 방안[34]을 결의하였다. 이에 비해 현재 우리나라의 사이버테러 대응체계는 국내 정보보호기반을 중심으로 추진되고 있어 사이버테러 발생시 국외 기관과의 상호 대응이 원활하게 이루어지지 않고 있다. 따라서 사이버범죄에 대한 국가간의 법적 성격이나 절차들의 차이점에 대한 국제적 조화 및 자국민의 침해 구제를 위한 국가간 협력 대처 방안이 모색되어야 한다.

V. 범정부 차원의 사이버테러 대응체계

4장에서는 현재 국내 사이버테러 사고 현황에 따른 대응체계를 살펴보았고, 이는 국가·공공분야 및 민간분야 차원에서 다양한 기관의들을 통해 수행중이다. 그러나 국가차원의 종합적이고 체계적인 형태로 추진되지않음으로써 나날이 고도화되는 사이버테러에 대해 적절히 대응하지 못하는 실정이다.

그러므로 본 논문에서는 안전한 지식정보사회 구현을 위해 범정부적인 사이버테러 대응체계 추진방향을 제시하고, 이를 토대로 법·제도 및 조직체계, 교육 및 홍보, 정보보호기술 및 국제협력 측면에서의 사이버테러 대응체계 구축방안을 제시하고자 한다.

1. 범정부적 사이버테러 대응체계 추진방향

현재 우리가 직면하고 있는 사이버테러 대응체계의 문제점을 인지하고 이를 극복하기위한 전략을 수립하기 위해서는 사이버테러 대응체계의 구조 및 과정전반에 걸쳐 지속적인 혁신작업이 일어나야 한다. 특히 정보통신의 세계는 급속도로 변하기 때문에 시대의 흐름에 따라 사이버테러 대응정책도 지속적인 변화가 뒤따라야 한다. 따라서 앞에서 살펴본 우리나라 사이버테러의 문제점을 바탕으로 그림 12처럼 범정부적인 사이버테러 대응체계 추진방향을 제시하고자 한다. 그림 12는 정책대안을 모색하기 위한 기본적인 틀로서, 사이버테러 대응체계 기본방향을 설정하고, 이를 토대로 사이버테러 대응 추진체계 및 추진기반에 대한 방안을 제시한다.

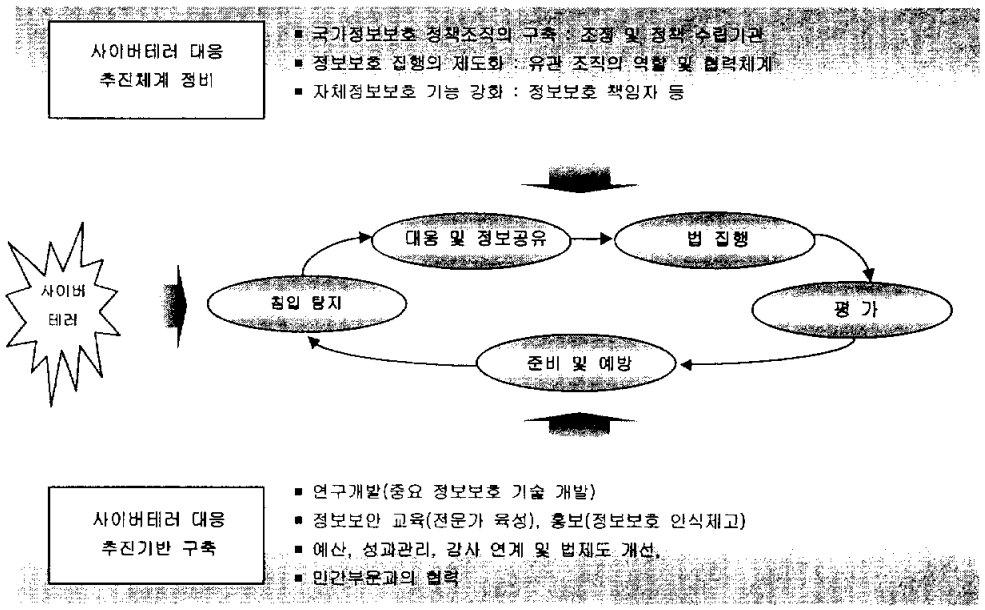


그림 12. 범정부적 사이버테러 대응체계 추진방향

다음은 사이버테러 대응체계를 구축하기 위해 필요한 세가지 기본방향을 제시한 것이다.

첫째, 체계적이고 종합적으로 사이버테러 대응체계 기능을 강화하여야 한다. 정보시스템은 수 많은 컴퓨터와 네트워크 및 사용자들로 구성되어 있기 때문에, 어느 한 부분이라도 보안이 취약하게 되면 전체 시스템이 외부공격으로부터 쉽게 침해될 수 있다. 즉, 보안은 하나의 시스템 또는 하나의 조직만 철저하다고 해서 이루어지는 것이 아니며, 갈수록 조직간 네트워크 협력이 증가되는 추세이기 때문에 조직간의 상호의존성으로 인한 보안 문제들이 더욱 증가할 것이다. 더불어 보안은 단순히 외부의 공격 뿐만 아니라 다양한 원인으로 침해될 수 있기 때문에 침해사고에 대한 탐지, 대응, 복구, 경고 및 정보공유 전반에 걸친 체계적인 대응 전략이 수립되어야 한다. 이상과 같은 이유에서 사이버테러 대응체계는 국가

전반에 걸친 체계적이고 종합적인 정책 수립을 통해 이루어져야 한다.

둘째, 사이버테러 대응체계는 관, 민, 학, 군 등 다원적 협력을 통해 구축되어야 한다. 즉, 주요 정보통신기반이 정부 외에도 민간 및 공공기관에서 운영되고 있는 경우가 많으므로 이 기관들간의 긴밀한 협력체계가 구축되어야 한다.

세째, 지속성과 적응성을 보장하는 사이버테러 대응체계 기반이 이루어져야 한다. 정보통신기술은 급격하게 변함에 따라 해킹 및 바이러스 등 정보시스템에 대한 공격기법도 나날이 변화되고 있다. 따라서 과거의 보호기술로는 새로이 출현하는 공격에 대비할 수 없으며, 이에 따라 정보시스템에 대한 침해사고 피해가 갈수록 증가하는 추세이다. 특히, 향후에는 사이버테러가 국가간의 사이버戰으로 발전할 수 있기 때문에 사이버테러 대응체계도 체계적으로 변화되어야 한다. 따라서 정보보호기술 연구개발, 전문인력 양성, 전국민의 정보보호 인식제고 및 예산 및 법·제도적 지원 등 지속적이고 적응력 있는 사이버테러 대응체계를 구축하기 위한 기반을 마련하여야 한다.

2. 범정부적 사이버테러 대응체계 구축방안

가. 정책조직 및 법·제도 체계

1) 국가 사이버테러 대응 조직의 구축

4장에서 살펴보았듯이 우리나라 사이버테러 대응체계 추진은 여러 기관을 중심으로 수행되고 있고, 그들 간에 내부적 갈등이 발생할 경우에 실질적으로 조정할 수 있는 강력한 총괄기구가 없는 것이 문제점으로 지적되고 있다. 따라서 각 부처 산하의 사이버테러 대응 관련 기구들, 법집행을 맡고있는 검찰과 경찰, 국방관련 사이버테러를 담당하는 국방부

및 민간 부문의 사이버테러 대응 관련 기구들까지도 고려할 때 국가 전체의 사이버테러를 총괄적으로 조정하는 보다 강력한 사이버테러 대응총괄기구를 설립하여야 한다. 그리고 새로이 설립할 사이버테러 대응총괄조정기구로 선택될 수 있는 대안으로는 전자정부특별위원회의 격상을 통한 정보보호조정기능 부여, 국무총리를 위원장으로 하는 정보보호 총괄조정기구 설립 및 대통령 직속의 정보보호 총괄 조정기구 설립 등이 제시될 수 있다.

그러나 전자정부특별위원회 격상 안은 전자정부특별위원회가 전자정부구축 기능의 일부로 정보보호 업무를 다루기 때문에 상대적으로 그 비중이 약화될 수 있다는 단점이 있고, 국무총리를 위원장으로 하는 정보보호 총괄 조정기구는 그 성격상 권한과 자원의 동원면에서 대통령 직속보다는 상대적으로 약하기 때문에 신속한 정보보안체계 및 대책을 수립하고 집행하기가 미약하다. 따라서 미국의 사례에서 보듯이 대통령 직속으로 정보보호 위원회를 설치하는 것이 정부나 민간의 다양한 부처 및 기관들을 총괄적으로 조정하고 지원할 수 있는 강력한 권한과 자원의 동원능력을 갖출 수 있다는 점에서 가장 이상적인 대안으로 판단된다. 그러나 이것도 장기적으로는 대통령의 관심 여하에 따라 형식적인 기구로 전락할 가능성이 높으며, 대통령에게 너무 많은 책임을 집중 시키고 있다는 점에서 문제점이 지적될 수 있다.

따라서 사이버테러에 대한 사안의 시급성이나 초기 단계에서 강력한 권한 및 자원 동원을 통해 사이버테러 대응책을 수립하고 집행해야 하는 단기적 차원에서는 대통령직속으로 사이버테러 대응 관련 총괄조정기구를 설치하는 것이 바람직하며, 초기 단계의 사이버테러 대응정책이 어느 정도 궤도에 오르게 되면 정책들을 안정적으로 조정할 수 있는 국무총리 중심의 기구를 설립해야 한다.

2) 사이버테러 대응 기관간 연계관계 강화

성공적이고 안정적인 사이버테러 대응체계 추진을 위해서는 사이버테러 대응 기관간의 연계를 강화시키는 네트워크 구축이 요구되어진다. 이를 위해 먼저 각 정보보호 기관의 역할을 명확히 정립할 필요가 있으며, 이를 토대로 기관간의 협조 체제를 공고히 하는 대안을 마련해야 한다. 그러나 국내 사이버테러 대응체계의 문제점으로 지적되었듯이, 정보보호 관련 주요 기관들간의 이해관계가 충돌 및 업무의 관할 영역이 중복됨으로써 정책혼선 등의 문제점이 발생할 수 있다. 따라서 국가적 차원의 사이버테러 대응체계 확보하기 위한 추진 기관간의 업무영역 정립에 있어, 기본방향 및 조정방안을 그림 13과 같이 제시하고자 한다.

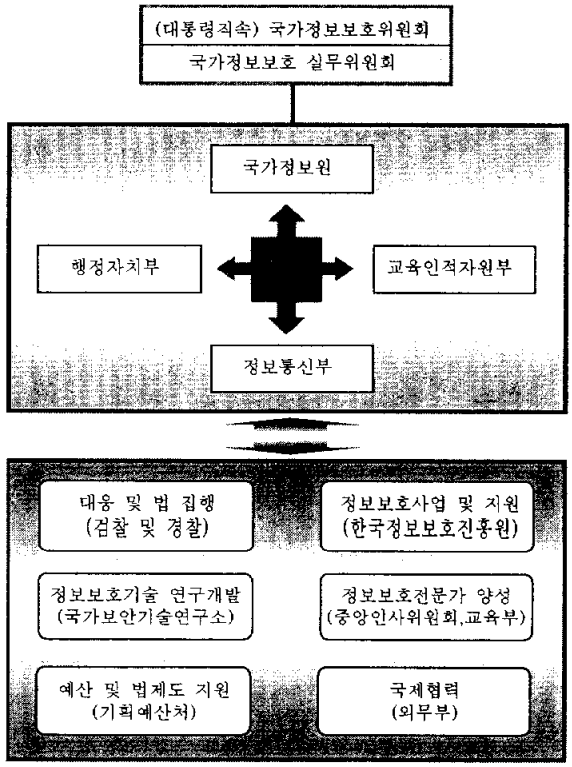


그림 13. 국가정보보호조직 체계도

우선 국가 전체의 사이버테러 관련 대응정책을 총괄 및 조정하는 기구는 앞에서 제시한 (가칭)대통령 직속 정보보호 위원회가 수행하며, 사이버테러 대응 관련 기관들의 업무 영역에 대한 갈등이 있을 경우에는 이를 조정하는 역할을 수행하여야 한다. 물론 국가정보원도 정부 및 공공기관에 대한 사이버테러 대응 총괄기구이기는 하지만, 그 핵심역량을 국가안보 및 국가기밀 관련 정보보호에 집중하여 능률성을 향상시키는 것이 바람직하다. 그리고 일반적인 정부 및 공공기관에 대한 사이버테러 사고 문제에 관하여는 행정자치부와 협의하여 자문 및 기술지원을 수행할 필요가 있다. 국가안보 및 기밀 관련 정보시스템을 제외한 일반적인 정부 정보시스템의 사이버테러 대응정책은 국가정보원과 협조하여 행정자치부에서 관리하여야 하고, 특히 상대적으로 보안이 취약한 지방자치단체의 침해사고에 대해 좀 더 많은 관심을 기울여야 한다. 또한 보안이 가장 취약한 교육기관은 교육인적자원부에서 관리하도록 한다. 그 외 정보통신부는 정부와 민간부문이 만나는 주요 정보통신기반시설에 대해서 사이버테러 대응정책을 관리하도록 하고, 이 과정에서 행정자치부 및 국가정보원과의 긴밀한 협조관계를 유지하여야 한다.

더불어 위와 같은 협조 및 조정은 "정보보호위원회" 주관으로 합리적인 방안을 도출하여야 하고, 이 때 정보통신부는 정보보호위원회와 협조하여 민간부문의 사이버테러 사고에 대한 지원 및 상담업무를 수행하여야 한다.

3) 예산· 법제도 지원 및 정책 수립

정부에서 어떤 정책을 수립하고 집행하는 데 있어서 필수적으로 확보되어야할 것이 예산과 법제도적 지원으로, 기본적인 예산이 확보되지 않

거나 법률적으로 근거하지 않은 정책은 현실적으로 효과를 거두기가 어렵다. 더구나 기존의 법률이 새로운 정책을 시행하는 데 장애가 된다면 그 정책의 성공가능성은 더욱 희박하다고 볼 수 있다. 이는 사이버테러 대응정책에서도 예외일 수 없으며, 국가정보보호위원회는 기획예산처와의 긴밀한 협의를 통해 사이버테러 대응 관련 예산을 적절히 확보할 수 있는 권한을 보유해야 함은 물론 예산확보를 위해 많은 노력을 기울여야 한다. 또한 정보화의 급격한 발전과 더불어 사이버테러 기술도 급속히 발전하고 변화하는 추세로서, 시기 적절한 법률 제정 및 개정이 없으면 사이버테러 대응을 위한 효율적인 정책집행이 어렵다. 따라서 사이버테러 법률문제를 전담하는 상임위원회를 설치하여 지속적인 사이버테러 대응 관련 법률 검토, 제정 및 개정 작업에 주력하여야 한다. 특히, 현재 급증하고 있는 스팸메일 등 악성 광고성 정보 전송행위와 개인정보 침해행위에 대한 규제를 강화하고, 개인정보 불법 유출에 대한 국민의 인권을 보호하기 위한 법률을 개정하여야 한다.

더불어 사이버테러 대응기능을 강화하기위해서는 각 부처 및 기관 자체 차원에서 사이버테러 대응정책을 수립할 필요가 있으며, 이 때 국가정보보호위원회는 관련 기관 및 전문가의 협조를 얻어 각 기관의 정책수립에 대한 지원 및 검토작업을 수행하도록 한다. 또한 영국에서 정보보호관리 국제 표준인 ISO(International Organization for Standardization)17799를 모든 정부 부처에서 도입하도록 추진하듯이 우리나라도 정부에 맞는 적절한 정보보호관리 표준을 제정하여 각 부처 및 기관이 이를 인증 받도록 권고할 필요가 있다.

나. 보안 교육 및 관리 체계

1) 정보보호 교육 및 홍보를 통한 대국민 인식 제고

사이버테러 대응강화를 위한 정책이 지속적으로 효과를 산출하기 위해서는 대국민적으로 정보보호 인식이 이루어져야 하며, 이를 위해 정보보호 교육 및 홍보 활동은 사이버테러 대응의 중요성을 전달하는 최선의 수단이다. 따라서 보안교육 및 홍보의 활성화를 위해서는, 우선 공무원들을 대상으로 한 정보보호 교육 및 홍보기능을 강화해야 한다. 즉, 모든 공무원들에게 사이버 위협을 인지하고 대처할 능력을 배양하기 위해 CD-ROM, 비디오, 워크샵, 시연회 및 온라인 교육 등 각종 시청각 교육자료와 프로그램을 활용하여 공무원에 대한 정보보호인식제고 사업을 전개한다. 또한, 정보보호자격증을 소지하고 있는 인력에게는 승진시 가산점을 부여하거나 우수한 보안전문가 및 정보보호 사례를 발굴하여 특별포상 및 승진 혜택을 부여하는 제도를 실시하는 등 전 공직자를 대상으로 보안 교육을 체계적으로 실시하여 정보보호 마인드를 심어줄 필요가 있다.

한편, 보안전문 인력을 초기부터 발굴하고 육성하기 위하여 중·고등학교 학생들과 교사들을 대상으로 한 정보보호 교육 및 인식제고 활동도 이루어져야 한다. 따라서 국가정보보호위원회는 교육인적자원부와 협의하여 중·고등학생을 대상으로 한 정보보호 교육과 홍보 계획을 수립하고 이를 지원하기 위한 방안을 마련하도록 한다. 즉, 청소년에 대한 교육을 강화하여 이들이 정보보호를 중요시하는 인식이 습관화 및 생활화되도록 해야 하며, 이를 위해 학교 및 학원의 교과 과정에 인터넷의 올바른 이용법 등 정보보호 관련 내용을 추가하여 사이버공간에서의 기본자세를 먼저 습득하도록 교육내용을 개선하여야 한다.

더 나아가 대국민 홍보 및 정보보호 마인드 확산 차원에서 관련 학회

나 연구기관을 통한 심포지움을 개최하는 등 정보보호 관련 저변 인구를 확대할 필요가 있다. 또한 일반 국민들을 대상으로 한 교육 및 홍보 기능을 강화하기 위해 정보보호 광고 및 홍보책자 발간, 정보보호백서 발간 및 인터넷이나 PC(Personal Computer) 통신을 통한 정보보호 정보제공 등 일반 국민들을 대상으로 사이버 공간에서 건전한 시민의식을 함양 시키는 운동을 전개하도록 한다.

2) 보안 전문인력 양성

사이버테러 대응체계 구축을 위해서 가장 시급히 해결해야 할 문제점으로 떠오르는 것이 보안 전문인력 충원의 문제이다. 현재 정부는 물론 민간부문에도 전문 보안인력이 절대적으로 부족하여 사이버테러에 대한 대응을 제대로 수행할 수 없는 상황으로, 신속한 사이버테러 대응을 위해서는 무엇보다도 고수준의 보안 전문인력이 필수적이다.

따라서 보안 전문인력을 시급히 양성하기 위해 다음과 같은 방안을 제시한다. 우선 단기적으로 정부에 있는 기존 IT 인력 중 보안 분야에 자질이 있는 자들을 선발하여 집중적인 교육과 훈련을 통해 보안 전문가로 양성해야 한다. 이 때 국가정보보호위원회는 중앙인사위원회의 협조 및 정보보호진흥원와 국가보안기술연구소의 지원을 받아 선발된 인력을 단기간에 정보보안 전문가로 향상시킬 수 있는 계획을 수립하도록 한다. 또한 중앙인사위원회는 정부에서 필요한 보안 전문인력의 수요 및 기술을 분석하여 보안전문인력을 모집, 선발, 배치 및 훈련하는 데 기본적인 정책자료로 활용한다.

한편, 장기적으로는 고수준의 보안 전문가 양성 및 현직 정부기관 내 보안 전문인력의 훈련을 위해 각 대학의 우수한 정보보호교육센터를 지정하고, 지정된 센터에서는 정보보호를 위한 전문 교육을 시행하도록 한

다. 이러한 맥락에서 대학 및 대학원 과정에서 정보보안 관련 과목 또는 학과를 개설하여 향후 정보기반시스템 침해대응에 필요한 전문인력을 단계적으로 양성할 수 있도록 지원하여야 하며, 추가적으로 산·학·관이 공동으로 정보보호 교육프로그램을 개발하도록 한다. 또한 미국의 경우 정보보안 전문인력을 양성 및 유치하기 위해 보안을 전공하는 대학생 및 대학원생들에게 졸업 후 2년간 연방정부 기관에서 보안 전문가로 근무할 것을 조건으로 장학금제도를 시행하고 있는데[35], 우리나라도 미국의 제도를 참고하여 각 대학의 우수 정보보호교육센터 재학생 등을 대상으로 장학금을 수여하고, 이를 토대로 우수한 보안 전문인력을 유치하는 계획을 세워야 한다.

3) 보안 관리기능 강화

앞서 제안한 보안 전문인력을 바탕으로 정부는 사이버테러 대응 기능을 자체적으로 강화시켜 주요 국가기반시설의 보안관리를 하여야 한다. 따라서 정보통신기반보호법에서 요구하는 정보보호책임관 및 정보보호책임자를 실질적인 보안관리 인력으로 채용하고, 이들은 기관 전체의 정보보호업무 뿐 아니라 그 기관과 긴밀한 연계 관계를 맺은 민간부문에 대해서도 보안 관리를 수행하도록 한다. 이를 위해 현재 정보통신기반보호법에서는 4·5급 공무원 또는 임원급 관리·운영자로 지정되어 있는 정보보호책임관의 직급을 격상시켜 이들에게 실질적인 권한을 부여하는 것이 바람직하다. 만약 정부 부처 내에서 필요한 보안 전문인력을 충원할 수 없을 경우에는 외부 정보보호전문업체나 컨설팅업체 등의 인력들을 "아웃소싱"하여 보안 전문인력 부족을 해결하도록 한다.

그리고 각 주요 부처 및 기관별로 CERT를 편성 및 운영하여, 기관이

자체적으로 정보시스템에 대해 정기적인 보안진단을 실시하도록 해야 한다. 특히 기관 내부 뿐만 아니라 정부 기관간 네트워크에 대해서도 보안대책을 수립해야 하는데, 이는 취약한 기관을 경유지로 하여 정부 전체 기관에 대한 사이버테러가 가능하기 때문이다. 따라서 각 기관간 네트워크 및 정부고속전산망이 연결되는 지점에 침입차단 및 탐지시스템 등을 설치하여 자체 보안대책을 마련하도록 한다.

다. 정보보호기술 구축 및 개발 체계

1) 종합적인 정보보호 시스템 구축

통신기술의 발달과 인터넷의 확장으로, 다양하고 새로운 응용분야들이 출현함에 따라 사이버공간의 위협 요소도 다양해지고 있다. 그러나 현재 정보보호시스템 대부분은 특정한 단일 목적 및 기능 차원에서 사이버테러 대응을 수행하고 있고, 이는 각 정보보호시스템의 특성을 정확히 파악하고 운용하는 보안 전문가 확보가 어려울 뿐 아니라 시스템 기능의 중복이 심화되는 등 많은 문제점을 드러내고 있다. 따라서 정보보호시스템들을 하나의 시스템으로 묶는 "정보보호통합시스템"이 차세대 정보보호시스템으로 요구되어지며, 이를 위해 그림 14와 같은 정보보호통합관리 모델을 제시한다.

이는 각각의 정보보호 기능들을 Agent화 하고 관리 시스템을 Master로 구축하는 Master-Agent 기반의 통합관리 모델로서, 침입차단시스템인 Internal 및 External Firewall과 침입탐지시스템인 IDS(Intrusion Detection System) 등 여러 개의 보호시스템이 독립적으로 존재하면서 통합 인터페이스에 의해 보안 관리가 통합적으로 이루어지므로 확장성 및 분산성이 뛰어나다.

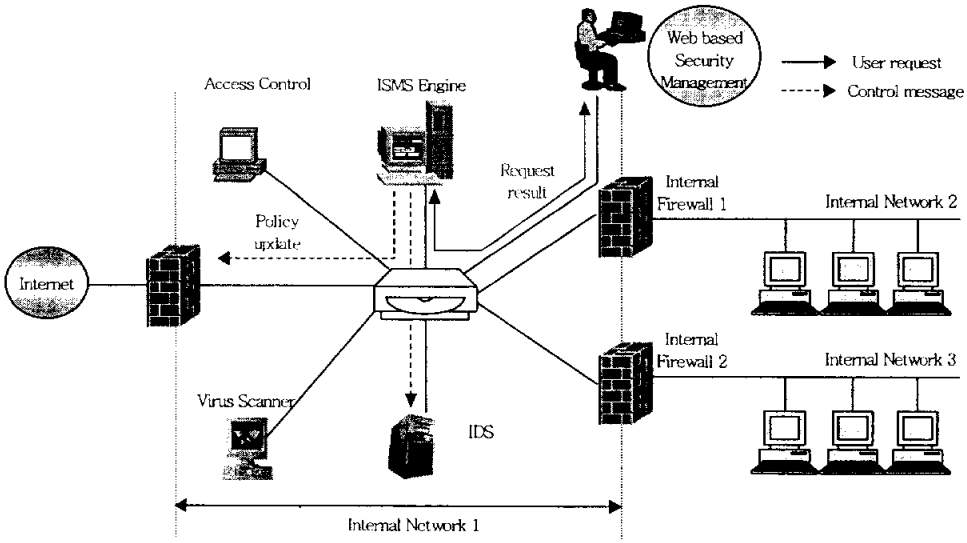


그림 14. 정보보호통합관리 모델

즉, 여러 정보보호시스템들의 기능들이 통합 인터페이스를 통해 ISMS (Information Security Management System) Engine에서 종합적으로 관리 및 운영되고, 사용자의 요청이 있을 경우 ISMS는 각 보호시스템들에게 "Policy update message"를 보내어 이들을 제어한다. 이 때, Access control과 Virus scanner는 통합 인터페이스에 맞물려 각 보호시스템들의 접근 제어 및 이들 시스템에 대한 침해 여부를 모니터링한다.

2) 보안기술 연구 및 개발 강화

사이버테러에 대응하기 위해서는 정책적 및 관리적 대책도 중요하지만, 중요 핵심기술의 연구개발도 무시할 수 없다. 특히 사이버戰 등 국가적 차원의 사이버테러 대응을 위해서는 자체적인 보안 기술을 보유하는 것이 매우 중요하나, 현재 우리나라가 보유하고 있는 정보보안 기술로는

급격하게 발전하는 사이버테러 기술에 대응하기에는 많은 한계점들을 가지고 있다.

따라서 보안 기술에 대한 적극적인 지원과 관심 및 연구가 필요하며, 이를 위해서는 체계적이고 효과적으로 연구개발 투자를 추진할 수 있는 보안기술연구총괄기구를 지정해야 한다. 현재 우리나라는 보안 기술연구가 분산적으로 수행되어 기술 개발이 제대로 이루어지지 않은 실정이므로, 신속히 보안기술연구총괄기관을 선정하여 전략적이고 체계적인 연구개발투자가 이루어지도록 하는 것이 바람직하다. 또한 기존에 수행하고 있는 국가 및 공공기관의 보안 기술연구를 지속적으로 수행할 뿐만 아니라 민간분야에서 개발이 불가능하나 꼭 필요한 보안기술에 대해서도 투자를 하도록 하며, 이 때 각 부처별로 진행되는 보안 기술 개발을 국가적 차원에서 통합적으로 관리하도록 한다. 더불어 사이버테러는 향후 국가간의 사이버戰 형태로 발전할 가능성이 높기 때문에, 미국의 NSA (National Stuttering Association)나 영국의 GCHQ(Government Communications Headquarters)와 같이 국가 안전을 위한 암호화정보 수집, 분석 및 대응하는 기관도 설립해야 한다. 그러나 아직까지는 국내 기술 및 예산 정도가 선진 각국에 비해 상대적으로 열세이기 때문에 선진 각국의 연구기관과 국제적인 제휴를 맺어 보안기술 및 정보를 습득하고 발전시켜 나가도록 해야 한다.

더불어 앞으로 우리 삶에 전개될 홈 네트워크 및 Telematiescommerce 등의 분야에서도 사이버테러를 대비한 보안 기술이 조속히 개발되어야 하고, 이들은 생체, 인공지능, 센서 및 로봇분야 등 최첨단 기술들을 기반으로 이루어져야 할 것이다.

라. 국제협력 체계

최근 인터넷을 통해 국경을 초월한 사이버테러가 빈번히 발생하고 있으며, 그 추세는 날로 갈수록 증가하고 있다. 특히 국내 인터넷 보급이 급속도로 이루어지면서 국내 침해사고의 상당 부분이 국외 크래커에 의해 이루어지고 있다. 따라서 국경을 넘어 행해지는 사이버테러에 적절히 대응하기 위해서는 국제 기구들과의 협력체계를 강화해야 한다. 이를 위해서는, 먼저 국외의 사이버테러 대응 관련 기관들로부터 체계적이고 지속적으로 침해사고 및 취약점 등의 정보를 수집할 수 있는 시스템을 구축하여 이들 기관과의 제휴 강화를 추진해야 한다. 즉, 정보보안의 선진국이라 할 수 있는 미국의 정보보호기관인 NSA, NIPC(National Infrastructure Protection Center) 및 CERT/CC 등 국제적인 기구들과 제휴관계를 맺어 신속한 보안정보 수집, 분석, 공유, 대응 및 정책수립 등을 향상시켜야 한다. 한편, 사이버범죄자에 대한 국제적인 공조 수사체제도 이루어져야 하며, 관련되는 법규와 범죄자 인도법 등을 상호 체결하여 국제적인 사이버범죄에 적절한 대응하도록 한다. 또한 국제컴퓨터침해사고대응협의회(FIRST: Forum of Incident Response and Security Teams)와 긴밀한 협조체계를 구축하여 세계 각국의 암호기술 및 해킹기술 정보를 교환하고, 이를 토대로 국제적인 크래커를 퇴치할 수 있도록 하여야 한다. 더불어 정보보안정책의 국제동향을 신속히 파악하고, 우리나라의 입장을 반영하기 위한 각종 정보보호관련 국제회의를 주도적으로 유치하여 국가적 위상을 강화하도록 한다.

Ⅵ. 결 론

정보통신기술의 발전과 더불어 주요 국가기반시설들이 정보 인프라로 구축됨에 따라 안전한 지식정보사회 구현은 사이버공간에서의 안정성이 우선적으로 확보되어야 하며, 범정부차원의 체계적이고 종합적인 사이버테러 대응책이 절실히 요구되어진다.

본 논문에서는 국· 내외 사이버테러 현황 및 대응체계들을 비교 고찰하여 국내 사이버테러 대응체계 문제점들을 분석하였고, 이를 바탕으로 국가 전반에 걸친 체계적이고 종합적인 사이버테러 대응체계 구축을 위한 법·제도 및 조직체계, 교육 및 홍보, 정보보호기술 개발 및 국제협력 측면에서의 추진 방안을 제시하였다.

먼저 법·제도 및 조직체계 측면에서는 국가 전체의 사이버테러를 총괄적으로 조정하는 강력한 사이버테러 대응총괄기구를 중심으로 국가 사이버테러 대응조직 구축 방안을 제시하였다. 또한 구축된 사이버테러 대응기관간의 연계를 강화를 위해 각 추진기관 간의 사이버테러 대응영역 방향 및 조정 방안을 제시하였고, 이를 원할히 수행할 수 있도록 예산· 법제도 지원방안 및 사이버테러 대응정책 추진 방안도 제시하였다.

이러한 사이버테러 대응정책이 지속적으로 효과를 산출할 수 있도록 보안 교육 및 관리체계 측면에서는 각계 각층의 정보보호 교육 및 홍보를 통한 대국민 인식 제고 방안을 제시하였다. 이와 더불어 학계와 대응기관간의 협력을 통한 보안 전문인력 양성 추진 방안을 단기적 및 장기적인 관점에서 각각 제시하였고, 양성된 보안 전문인력을 바탕으로 사이버테러 기능을 자체적으로 강화시키기 위한 주요 국가기반시설의 보안관리 책을 제시하였다.

또한 나날이 고도화되는 사이버테러 기술에 효율적이며 능률적으로 대

처하기 위해서 정보보호통합관리 모델을 제시하였고, 이는 기존의 여러 정보보호시스템들이 통합 인터페이스를 통해 ISMS에서 종합적으로 관리 및 운영되는 형태이다. 더불어 미래의 사이버戰을 대비하여 자체적인 정보보호 기술을 연구 및 개발하고 이를 지속적으로 추진할 수 있는 방안을 제시하였다.

마지막으로 국경을 초월하여 발생되고 있는 사이버테러에 신속히 대응하기 위해서는 무엇보다 국제적인 협력이 이루어져야 하며, 이를 위해 국제 사이버테러 대응 관련 기관들과의 제휴 강화 추진 방안을 제시하였다.

본 논문에서 제안한 강화 방안들은 법· 제도 및 조직체계 정비를 통한 체계적인 대응체제 구축, 정보보호 인식 제고 및 전문인력양성을 통한 자율적인 사이버테러 대응능력 배양, 자주적인 정보보호기술 개발능력 확보 및 국내외 유관 기관들과의 협력을 강화시켜 국가 차원의 사이버테러 대응 능력을 제고 함으로써 안전한 21세기 지식 정보화 사회를 구현할 수 있다.

향후 과제로는 과학적으로 사이버테러를 입증하기 위한 법적 증거물 확보를 위해서 소프트웨어 포렌식스를 이용한 사이버범죄 적용 시스템이 구현되어야 한다.

참고 문헌

[1] 행정자치부, "관계법령집", 1999.2

[2] 류시조 외, "사이버 공간의 법률문제," 부산외국어대출판부, 1999

[3] 서동일 외, "사이버테러 기술 및 대응방안의 현황 분석," Telecommunication Review, 제 10권 5호, pp.974-990, 2000.9/10

[4] 정관진, 이희조 "인터넷 웜과 바이러스의 진화와 전망,"정보처리학회지, 제 10권 제 2호, pp.27-37, 2003.3

[5] 국가정보원, "국가정보보호백서,"2002

[6] 박상서, 박춘식, "정보전 위협과 사례," 한국정보보호학회지, 제 12권 6호, pp.12-20, 2002.12

[7] Ed Sborocco et al., "Cyberterror: Potential for Mass Effect," IA Newsletter, Information Assurance and Technology Analysis Center, vol.4, no.4, 2001

[8] 박상서, 박춘식, "정보전 개념과 주요 동향,"정보처리학회지, 제 10권 제 2호, pp.47-57, 2003.3

[9] Anthony Lake, "6 Nightmares: Real Treats in a Dangerous World and How America Can Meet Them, Little, Brown and Company, Boston, 2000

[10] Steven A. Hildreth, "Cyberwarfare : CRS Report for Congress," Library of Congress, June. 2001.

[11] 정보처리진흥사업협회 시큐리티센터, "정보 시큐리티의 현상," 2002.5

[12] http://abcnews.go.com/sections/tech/DailyNews/whhack990511.html

[13] 박상서, "중국네트워크 보안위협," 국가보안기술연구소 TM, 2002

[14] Vigilinx, "The People's Republic of China Network Security Threat Assessment, 2001

[15] http://www.nis.go.kr

[16] http://www.linuxlab.co.kr

[17] http://www.wins21.com/

[18] 삼성경제연구소, "인터넷 강국의 취약성과 대응과제," CEO Information, 2003.2

[19] www.hauri.co.kr

[20] http://www.incidents.org

[21] 김현수 외, "9.11 테러이후 미국·일본의 대응 동향,"국가보안기수연구소 내부 TM, 2002. 6

[22] USA Patriot Act of 2001, http://www.ala.org/alaorg/oif/usapatriotact.html,2001.

[23] Cyber Security Research and Development Act, http://www. the orator. com/bills107/s2182.html,2002.

[24] E-Government Act of 2002, http://www.ala.org/washoff/egovact.html, 2002

[25] 조화, "국외 기술 · 정책 동향," 정보보호뉴스, 63호, pp.33-34, 2002.12

[26] National Strategy to Secure Cyberspace, http://www.ala.org/washoff/egovact.html,2002.

[27] National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2002.

[28] http:// www.kisa.or.kr

[29] http://www.kantei.go.jp/jp/it/security/tyousakai/dail/susume-kata.html

[30] 이철원 외, "주요국 정보전 대응 체계와 동향,"정보보안학회지, 제

12권, 6호, pp.22-30, 2002.12

[31] 이영길, "중국군의 정보전 능력," 국방저널, 제 324호, 2000.12

[32] 박종화, "미래전은 정보 과학전이다," 국방저널, 제334호, 2001.10

[33] 신영진, "국가·공공기관 해킹사고 현황 및 지원," 제6회 정보보호 심포지움, 2001

[34] 정보통신부 "안전하고 건전한 지식정보강국 구현을 위한 중장기 정보보호 기본계획(안)", 2002

[35] 정휴봉, "미국 정보보호 인력양성 정책동향," 제6회 정보보호 심포지움, 2001

감사의 글

이 작은 논문이 나오기까지 여러 사람의 도움이 있었습니다. 먼저 논문이 완성되기까지 많은 지도 편달과 조언을 해주시며 부족한 저를 이끌어주신 김성운 교수님께 감사 드립니다. 그리고 부족한 본 논문의 심사를 맡아 세심한 관심과 조언을 아끼지 않으셨던 윤종락 교수님, 박규칠 교수님께도 감사드리며, 아울러 지난 2년간의 석사시절동안 많은 가르침을 주신 정보통신공학과 모든 교수님들께도 머리 숙여 감사 드립니다.

논문을 쓰는 동안 물심양면으로 도와준 프로토콜연구실의 배정현 학우와 바쁜 가운데서도 세심하게 배려해준 프로토콜 연구실 방장을 비롯한 모든 학우들에게도 감사의 마음을 전하며, 미래에 보다 좋은 일들만이 생기기를 바랍니다.

직장생활 가운데서도 학업을 할 수 있도록 시간과 격려를 아끼지 않은 동료들에게도 진심으로 감사 드리며, 이제까지의 제 삶에 영향을 주신 저를 아는 모든 분들께도 깊은 감사의 마음을 전합니다.

마지막으로 학업을 수행할 수 있도록 헌신적인 뒷바라지를 마다하지 않고 함께해준 아내에게 감사를 드리며, 늦게까지 공부하는 아빠를 위해 옆에서 힘이 되어준 착한 딸 세빈이에게 고마움을 표시하며 이 한편의 논문을 바칩니다.

2003년 8월

강 수 동