사이버 테러 대응 방안에 관한 연구

조 호 대
[illegible]

오늘날 인터넷의 발달로 우리는 발을 디디고 있는 현실의 공간이외에 컴퓨터와 인터넷에 의해 네트워크로 형성된 사이버공간에 살고 있다. 특히 사회의 각 분야가 업무의 효율성을 추구하면서 사이버 공간은 수십만 대의 컴퓨터들이 광섬유 케이블로 연결되어 민간과 공공기관의 주요 기반시설들의 모든 시스템들이 거대한 신경망을 형성하게 되면서 이제 사이버공간의 완벽한 보호는 국가경제와 안보를 위해 필수적인 사안으로 인식되고 있다. 이에 따라 개인이나 특정집단에서 자신들의 경제적・정치적 목적을 관철시키기 위해 사이버공간에 대한 테러를 감행하는 사례가 잦아지고 있다.

다행히 지금까지 우리나라에서는 사이버 테러를 포함한 모든 분야의 테러에서 세계의 이목을 집중할 만한 국제적인 테러리즘은 발생하지 않았으나 테러는 언제 어디서 발생할지 예측할 수가 없고 다가오는 정보화 사회 속에서는 국가기간전산망에 대한 사이버 테러는 국가안보를 좌지우지할 중차대한 일로 결코 무시할 수 없는 문제이다.

사이버 테러는 인터넷을 통해 세계를 거미줄처럼 연결한 통신망을 통해 바이러스를 유포시키거나 직접 시설물의 통제시스템을 공격・파괴함으로써 엄청난 피해를 입히고 있으며 현재처럼 빠른 속도로 변화하는 정보화 물결 속에서 국가의 주요 자료들이 집중된 기간 전산망이 타격을 받을 때는 짧은 시간 내에 회복하기 힘든 피해가 발생한다. 군사적으로는 미사일이나 전투기의 요격시스템에 대한 침투를 통해 오작동을 유도하는가 하면 은행 전산망에 침투 자료를 훼손하는 사례가 나타나고 있다.

따라서 본 연구에서는 21세기 정보화 사회에 있어서 심각한 문제로 대두되고 있는 사이버 테러리즘에 대한 기본적인 논의와 함께 대응전략을 모색하고자 하였다.

주제어: 사이버, 테러, 테러리즘, 해킹, 공조수사

Ⅰ. 들어가는 말

2005년 우리나라는 초고속인터넷 가입률 세계 1위, 인터넷 사용자 수 세계 3위 등 세계적 수준의 IT강국으로서 면모를 갖추고 있으며, 정보화 사회의 성숙기인 유비쿼터스 사회로의 진입이 가시화되고 있지만, 정보통신기술의 비약적인 발전과 함께 이를 악용한 해킹, 웜・바이러스 등 사이버 위협 또한 첨단화・다양화되고 있는 실정이다.

2003년 1월 25일 슬래머(Slammer)와 웜(Warm) 바이러스로 인한 인터넷 마비사고와 2004년 주요 국가기관 해킹사건으로 인해 세계 최강의 정보통신국가에서 세계 최악의 보안 후진국으로 전락하는 수모를 겪었고, 이는 사이버 위협의 파괴력이 과거처럼 단순한 서비스 마비나 경제적 손실을 넘어 국가안보를 위협하는 심각한 단계에까지 이른다는 것을 의미한다(국가정보원, 2005: 1).

사이버 위협은 새로운 방식의 해킹기법을 사용하거나 해킹행위의 자동화프로그램을 개발하여 선진 각국과 우리나라에서 해킹사고가 급증하고 있으며, 국가기관의 정보시스템 작동이 중단되는 사례가 증가하고 있다.

현재의 해킹은 PC뿐만 아니라 서버를 파괴할 수 있는

변형 바이러스를 이용하거나, 감염이 쉽고 피해범위가 넓은 매크로바이러스(Macro Virus), 리눅스·웹기반 악성바이러스 등의 신종 바이러스 등을 웹상에서 유포하는 형태로 확산되고 있다. 대부분의 해커들은 이러한 치명적인 바이러스를 이용하여 주로 공공기관이나 언론사, 금융기관, 군 정보지휘부 등 중요 정보통신망에 침입하여 국가정보를 유출하거나 중요자료를 삭제하는 등의 심각한 문제를 일으키고 있다.

카네기 멜론 대학의 제프리 헝커 교수가 "해킹테러 하나가 목숨을 앗아갈 수도 있고 최소한 우리 삶을 생지옥으로 만들 수도 있다(한겨레신문, 2001년 10월 15일)"고 지적한 것처럼 최근 들어 과거에는 경험하지 못한 국가와 국민의 안전을 위협하는 새로운 형태의 테러가 현실로 다가오고 있는 것이다(백영철, 2002: 78).

또한 정치적 목적을 가진 해커에 의한 불법적 해킹인 핵티비즘(Hacktivism)도 등장하여 이러한 불법적인 해킹과 치명적인 악성바이러스에 의한 사이버 테러리즘(Cyber Terrorism)은 국가기반을 위태롭게 할 수 있다.

본 연구에서는 21세기 정보화 사회에 있어서 가장 심각한 문제로 등장하고 있는 사이버 테러리즘에 대한 기본 논의와 함께 기존의 사이버 테러의 대응실태를 살펴보고 이를 분석한 후 이를 토대로 대응전략을 모색하고자 하였다.

II. 사이버 테러에 관한 이론적 배경

1. 사이버 테러의 정의

'정치적으로 동기가 형성된 폭력'이라고 정의되는 테러 또는 테러리즘이라고 불리는 테러행위는 기본적으로 수단적인 가치보다도 상징적인 정치적인 문제와 범죄로서의 폭력행위를 복합적으로 포함하고 있다(이황우 외, 1996: 75). 테러리즘은 학자들과 테러리즘 전문가들의 시각에 따라 달리 정의되기도 하며, 심지어는 한 국가내 부처마다 정의가 서로 다른 경우도 있다. 우리나라에서 대테러업무를 주관하는 국가정보원은 테러리즘을 "정치적·사회적 목적을 가진 개인이나 집단이 그 목적을 달성하거나 상징적 효과를 얻기 위해서 계획적으로 행하는 불법적 폭력행위(http://www.nis.go.kr)"라고 정의하고 있다[1].

이와 달리 사이버 테러는 "최첨단 정보통신 기술을 이용해 사회 중추신경인 전산망을 파괴하거나 해킹으로 획득한 자료들을 불순한 목적에 이용하는 행위(조병인 외, 2000: 227)", "첨단 정보통신 기술을 이용해 물리적 세계가 가상의 세계로 전환되어 있는 공간을 무차별적으로 공격하는 행위(http://terrorism.or.kr)", "해킹과 바이러스 프로그램에 의한 행위 그리고 주요 사회기반시설 내지 정보통신기반시설에 대한 테러행위로 국한시키는 견해", "사이버 공간에서 일정한 목적을 가지고 계획적으로 정보를 공격하는 행위" 등과 같이 다양하게 정의되어지나, 사이버 테러라는 용어 자체는 우리나라 법령에 사용된 예가 없으며, 국가대테러활동지침 제2조 제1호에서 「컴퓨터 통신망을 이용한 정보조작 및 전산망 파괴」를 테러 유형의 하나로 규정하고 있을 뿐이다.

이를 종합하면 사이버 테러란 『해킹, 바이러스 유포, 논리폭탄 전송, 대량정보 전송, 서비스거부 공격, 고출력 전자총 등을 통신망에서 사용하는 "컴퓨터 시스템 운영방해 행위"내지는 "정보통신망 침해 행위", 또는 전자적 침해행위에 의하여 "국가적·사회적으로 공포심 내지 불안감을 조성하는 행위"』라고 정의할 수 있고, "컴퓨터시스템 운영방해 행위" 또는 "정보통신망 위협 및 침해 행위"와 "테러리즘(terrorism)"의 결합이야말로 사이버테러의 개념요소라고 할 수 있다(이동곤, 2005: 8-10). 정보화 사회 도래와 함께 국가와 사회의 주요 기반시설

1) 테러리즘의 동의어로 테러라는 용어가 일반적으로 사용되고 있는데 두 용어의 개념에는 현격한 차이가 있다. 심리학자들에 의하면 "특정한 위협이나 공포로 인해 모든 인간들이 심적으로 느끼게 되는 극단적인 두려움의 근원이 되는 것"이라고 규정하고 있다. 즉 테러란 발생 원인이 어떤 것이든 극도로 불안한 심리적 상태를 말하며 자연적인 현상이다. 반면에 테러리즘은 테러와는 구별되는 폭력적 행위의 한 형태를 의미하는 것으로 항공기 납치, 요인 암살, 공중시설 폭파 등을 통해 사람들에게 공포를 일으키게 하는 행위를 의미하는 것이다(이진수, 2000: 8). 따라서 엄밀히 말하자면 테러와 테러리즘은 다른 개념으로 생각할 수 있다.

이 정보시스템에 대한 의존도가 심화되면서 사이버공간에서 행해지는 사이버테러는 물리적인 테러 못지않게 우리 사회를 혼란에 빠뜨릴 수 있다[2].

<표 1>에서 보듯이 사이버 테러는 주체에 따라 개인적 침해, 조직적 침해, 국가적 침해로 구분할 수 있으며, 이에 따라 목적, 대상, 공격 방법에 차이가 있다.

개인적으로 수행할 수 있는 침해 유형으로는 컴퓨터 바이러스, 해킹, 서비스거부 공격이 있고, 조직적 침해에는 개인적 공격방법을 포함하여 유·무선 도청, 정보통신망 스니퍼, 교환 시스템 동작 마비 등이 있고, 국가적 침해에는 개인적·조직적 침해방법을 포함 첨단 도청 및 암호 해독, 전자공격무기 등이 있다.

<표 1> 테러 주체에 따른 테러 위협

구분	개인적 침해 위협	조직적 침해 위협	국가적 침해위협
주체	해커 컴퓨터 범죄자	산업스파이 테러리스트 조직화된 범죄 집단	국가 정보기관 사이버전 전사
목적	금전 획득 영웅심 발휘 명성 획득	범죄 조직의 이익 달성 정치적 목적달성 사회·경제적 혼란 야기	국가기능 마비 국가방위능력 마비
대상	민간 사설망 공중 통신망 개인용 컴퓨터	기업망 금융, 항공, 교통 등 정보통신망	국방, 외교, 공안망 등
공격방법	컴퓨터 바이러스 해킹 메일폭탄 홈페이지 변조 패스워드 유출 개인 신분위장 트로이목마 등 서비스거부 공격	개인적 공격방어 포함 유·무선 도청 정보통신망 스니퍼 통신망 교환 시스템 동작마비 공격	개인적·조직적 공격 포함 첨단 도청 및 암호 해독 전자공격 무기 고에너지 전파무기 전자기파 폭탄 등 기타, Chipping/초미세형 로봇/전자적 미생물

2. 사이버 테러의 유형 및 특징

1) 사이버 테러의 유형

사이버 테러리스트들은 컴퓨터나 첨단 정보통신에 대한 전문적인 지식과 경험을 가지고 있어 불법으로 정보통신망에 침입하기 위해서 다양한 수법을 사용하고 있다. 그 중에서 가장 대표적인 것이 컴퓨터의 기능을 방해하거나 프로그램 및 데이터를 손상 또는 파괴하는 것으로써, 점점 그 위력을 더해가고 있는 컴퓨터바이러스이다.

1990년에는 200종에 불과하던 것이 지금은 36,000종이 넘고 있으며, 하루에 10종 이상 새로운 바이러스가 생성되고 있어 PC이용자 10명중 3명이 바이러스 감염의 경험이 있고, 경험자의 50%가 1백만원 이상의 재산상 피해를 보고 있다. 정보화시대에 전염병과 같은 컴퓨터 바이러스를 만들어 내는 사람들은 자기 실력을 과시하고 싶어 하거나, 남에게 피해를 끼치려는 전문가의 소행이기도 하지만, 경쟁사의 업무를 마비시키거나 경쟁의 핵

2) 인터넷 등 컴퓨터 통신망을 이용해 가상공간에서 상대방에게 해를 입히는 행위인 사이버 테러는 국가 정보원에 따르면 중동·서남아 지역에서는 과격 테러단체와 분리주의자 등이 인터넷 웹사이트를 개설해 운영하면서 목표물에 대한 정보 입수와 자신들의 주의·주장을 선전하는 한편, 폭발물 제조법 교육 및 테러지령 하달수단 등으로 이용하고 있다. 또한 2000년 7월에 발간된 미 의회의 보고서는 "사이버 테러리즘은 빛의 속도로 전개되며 단 몇 분이면 모두 끝난다. 전기와 통신이 완전히 두절되고 월스트리트의 모든 금융거래 기록은 일순간에 사라진다. 미국의 막강한 군사력은 고철덩어리에 지나지 않을 뿐이다"라고 사이버 테러리즘의 가능성을 경고하였다. 테러리즘을 자행하는 동기는 과거와 동일하지만 시대 변화에 따라 테러의 양상도 끊임없이 변화하여 과거에는 없었던 새로운 유형의 무기들이 인류를 위협하고 있다. 과거 테러리즘으로부터 인류를 지켜주었던 정보체계, 전술, 보안절차 등은 새로운 위협에는 거의 무용지물일 뿐만 아니라 과거의 테러리즘에 대항하여 인류의 평화와 인권을 보호하던 대 테러리스트 특공대도 이 새로운 유형의 테러리즘에는 아무런 효과를 거두지 못한다.

심요소인 기업 비밀과 주요 정보를 파괴시키기 위한 수단으로 사용되기도 한다.

컴퓨터 바이러스의 대표적인 종류에는 웜(Warm)과 논리폭탄(Logic Bomb)이 있다(임채호, 1998: 221). 웜은 자기 자신을 복제하는 프로그램으로서 웜이 있는 디렉토리나 디스크에 끝없이 자기 자신을 복제, 확대, 재생산하여 기하급수적으로 늘어나게 되면 컴퓨터와 네트워크에 웜이 가득 차게 되어 컴퓨터를 마비시킨다. 논리폭탄은 프로그램 속에 숨어있는 명령집단으로서 매주 정해진 요일, 매월 일정한 날짜와 금요일과 13일이 겹치는 날 등 특정 요일, 특정 날짜와 같은 특정 조건이 만족되면 실행되는 응용프로그램이다. 이밖에 최근 개발된 칼리큘라, 코드파괴자와 같은 악성바이러스는 전산망에 들어가 중요한 정보를 유출시키면서 해당 전산망을 망가뜨리는 결과를 가져온다.

두번째로 사용하는 기법은 해킹기법으로 이는 단순히 전산망에 침투하는 것 외에도 다양한 기술이 있다. 그 중에서 가장 많이 사용하는 기술이 스니프(Sniff)로 스니프는 LAN상에서 네트워크 장비를 혼합모드로 설정할 경우 LAN상의 모든 송수신 테이터를 훔쳐볼 수 있는 기능을 악용하여 사용자 이름, 비밀번호 등을 알아내고, 송수신되는 메일 내용들을 도용하는 것이다. 대표적인 수법인 '트로이 목마 공격'은 해킹용 프로그램을 인터넷 검색 프로그램인 '익스플로러(파일명 ie0119.exe)'와 인터넷 보안용 프로그램인 '래퍼(파일명 TCP wrapper)' 등으로 위장하여 시스템에 침투시키는 방식이다. 만약 사용자가 이 프로그램을 전송 받아 자신의 컴퓨터에 설치하면 자동으로 해킹프로그램이 작동, 해커가 침투할 수 있는 길을 열어주게 된다.

해킹방법 중 다른 하나는 스푸핑(Spoofing)이다. 스푸핑은 송수신자 간의 TCP 접속시 일어나는 3방향 접속시 필요한 순서번호를 이용하여 불법접속이 가능하게 만드는 방법이다. 여러 대의 컴퓨터가 정보를 공유하고 있을 때, 그 중 한 컴퓨터가 다른 컴퓨터에 정당한 통신인 것처럼 신호를 보내고 침투한다. 침투한 크래커는 정당한 사용자에게는 엉뚱한 일을 시키고 크래커를 정당한 사용자로 착각하게 하여 사용을 허가하게 된다(임채호, 1998: 224).

또 다른 해킹방법은 S스캔방법이다. 1999년 1월 국내 처음 보고된 S스캔 공격은 원격지에서 불특정 다수의 전산시스템을 대상으로 허점을 찾아내는 프로그램인 S스캔을 이용, 취약점을 찾아 전산망에 불법 침투하는 해킹기법이다. 미국 출신의 해커로 알려진 J. S.바하가 개발한 해킹용 프로그램 'S스캔'은 다수의 인터넷의 사이트를 대상으로 운영체제의 종류와 취약점 등을 자동으로 파악하여, 공격하는 위력을 갖추고 있다. 사이버 테러리스트들은 이 프로그램으로 취약점을 발견하면 바로 시스템에 침투하여, 자료 유출이나 시스템 파괴 등의 활동을 할 수 있게 된다.

세번째는 전파무기를 사용하는 것으로 전파무기는 강력한 고출력 전자파를 발사하여 컴퓨터를 오작동하게 하거나 정지시키는 것이다. 몇 년 전 아일랜드 반군이 이 무기를 구입해 런던금융가에 공격을 가할 계획을 수립한 적이 있었다는 보도가 있었다.

네번째는 벤엑크라는 장비를 이용하는 방법으로 통신케이블에서 흘러나오는 전자파를 잡아내 그 안에서 전송되는 정보를 빼내는 방법이다. 이러한 첨단기술은 이미 실용화되어 원격지에서 전자파를 감지하여 대상 컴퓨터의 모니터 화면을 재생하는데 사용된다.

마지막으로, 전자기 폭탄을 사용하는 것으로 전자기 폭탄은 강한 전자기를 내뿜어 국가통신시스템・전력・물류・에너지 등의 사회 인프라를 일순간에 무력화시킬 수 있다. 만약 향후 미래전쟁에 이 무기가 쓰인다면 지구적 규모의 파괴력이 나타날 것이다.

그 외 사이버침해 유형으로는 논리 폭탄, 치핑(Chipping), 나노머신(Nanomachine), Jamming, HERF(High Energy Radio Frequency), EMP(Electro Magnetic Pulse)폭탄, AMCW(Autonomous Mobile Cyber Weapon) 등이 있다.

2) 사이버 테러의 특징

사이버 테러는 전 세계에 그물 망처럼 연계된 인터넷 망을 통해 빛의 속도로 전개되며 소요시간도 그 동안에 있었던 일반적인 테러와는 달리 수분이내에 끝나면서도 피해규모에 있어서는 일반인의 상상을 초월하고 심지어는 국가의 안보에 심각한 위협으로 나타날 수 있다. 따라서 사이버 테러는 그 동안 우리 인류에 커다란 위협이 되어왔던 일반적인 테러와는 그 본질을 달리하는 것으로 볼 수 있는데 통상의 테러와는 다른 사이버 테러의 특징을 살펴보면 다음과 같은 점을 들 수 있다(이진수, 2000: 34).

(1) 광역성 및 다양성

일반적으로 사이버 테러는 테러리스트가 목표로 정한 공격 지점에 직접 접속하여 공격하는 것이 아니라 네트워크가 연결된 곳이라면 세계 어느 곳이든 공격을 감행할 수가 있다. 특히 네트워크망에 대한 보안시스템이 잘 완비되고 국민들의 보안의식이 높은 선진국보다는 보안시스템이 취약한 지역・국가에서부터 출발하여 여러 단계를 거친 다음 목표하는 전산망에 접근하여 필요한 정보를 빼내가는 우회적인 방법을 선택하는 것이 일반적인 방법이다. 따라서 사이버 공간에 대한 범죄가 발생했을 경우 피해를 당한 전산망에 대한 조사권만 가지고 조사하는 것에는 한계가 있으며 그것이 국제적 테러조직에 의한 범죄일 경우 국제적인 협력이 없다면 조사자체가 불가능해지는 상황까지 발생한다.

또한 사이버 테러를 대비하기 위해서는 과거처럼 경찰이나 군 등이 책임지역이나 건물을 가지고 독자적으로 업무를 수행할 수 있는 것이 아니고 네트워크에 연계된 각 기관들이 공동으로 상호 유기적인 협조 체제를 구축하지 않고서는 적절한 대비가 어렵기 때문에 미래 인류사회의 최대의 위협이 될 사이버 테러는 국제적인 협력관계 구축은 물론 관련 기관간의 유기적인 협조 체제 구축이 최대 현안으로 떠오르고 있다(이진수, 2000: 34).

(2) 최소의 인원으로 최대의 피해 가능성

컴퓨터 네트워크를 이용하여 적의 정보통신망에 침투하기 위한 최소한의 기술자만 있으면 사이버 테러리즘은 가능하다. 물리적인 테러가 대규모 혹은 소규모라도 다수의 인원을 필요로 하는 것에 비해 목표 대상에 따라 필요 인원이 증가할 수는 있겠지만 사이버 테러를 위한 인원은 다른 어떤 물리적인 테러를 수행하기 위한 인원에 비해 적다. 하지만 이러한 경우에도 타격 대상이 되는 정보통신시스템을 파괴 또는 마비시키는 것에 따른 경제적・사회적 파급효과는 정보통신기반시설이 더욱 선진화되고 의존도가 높은 국가일수록 비례하여 커진다.

또한 컴퓨터 범죄행위는 반복 가능성, 영속성의 속성이 있으므로 한 번의 범죄행위는 그 규모나 피해가 작을지라도 계속적으로 자동적인 프로그램의 실행, 확산을 통해 피해액이 계속 증가할 가능성이 높다. 하지만 물리적 테러리즘보다 극적인 요소가 덜해 테러리스트들이 사이버 테러리즘을 그리 선호하지 않을 것이라는 의견도 있다(Arquilla and Ronfeldt, 2001: 169-172).

(3) 증거의 은닉성과 비가시성

테러리스트들은 물리적 공간이 아닌 사이버 공간의 특수성을 활용하여 수사기관의 추적을 따돌리고 증거를 변조하거나 삭제하고 있다. 이와 같이 원본과 복사본 구별이 어렵고 수사가 곤란한 디지털 증거에 법적 증거 능력을 갖게 하는 방법인 컴퓨터 포렌식스[3]는 최근 들어 크게 발전하고 있다. 수사 및 법적인 관점에서 디지털 자료는 눈에 보이지 않는 비가시성에 바탕을 두고 잠재성과 다양성・대량성 등의 특징을 가지고 있어 사법처리를

3) 컴퓨터 포렌식스(Computer Forensics)는 컴퓨터 등과 같은 정보처리기기에서 수집할 수 있는 디지털 자료가 법적 증거 능력을 갖게 하기 위한 제반 절차와 방법을 통칭하는 것이다. 포렌식스(Forensics)의 사전적인 의미는 '법정의', '변론의' 의미가 되며, 예로서 Forensics medicine은 '법의학'이라는 뜻이 된다. 따라서 디지털 자료가 증거 능력을 갖게 하기 위한 절차로서의 의미는 'Digital Forensics'가 좀 더 광범위하고 정확한 의미가 될 수 있으나 'Computer Forensics'가 초기에서 사용되어 왔고, 그 의미 또한 크게 벗어나지 않으므로 아직까지 통용되고 있는 실정이다.

위한 증거 자료를 확보하는 것에 특별한 방법과 절차를 요구하고 있다. 범죄의 혐의가 있을 때 범죄 사실과 증거를 수사하여야 하는 것은 컴퓨터 관련 범죄에서도 다른 범죄와 마찬가지이나 컴퓨터와 관련된 증거를 수집함에 있어서는 전통적 증거 수집과 달리 증거 수집 절차에 있어서 새로운 문제가 야기된다.

예를 들어 컴퓨터에 의하여 처리되고 저장된 데이터 또는 프로그램 등이 저장되어 있는 자기테이프나 디스크는 유체물이기 때문에 압수 대상이 되지만 데이터나 프로그램 그 자체로는 유체물이 아니기 때문에 형사소송법상 압수수색 대상이 될 수 있는가의 문제가 생긴다(정완, 2004: 3). 또한 사이버 범죄의 주요 유형 중 하나인 해킹 기술이 발전할수록 보안기술도 함께 발전해 왔다고 할 수 있지만, 알려지지 않은 행위나 새로운 공격기법에 대하여 방어하기에는 역부족이고 해킹을 당한 대부분의 시스템 관리자들은 자신이 해킹을 당했는지조차 알지 못하며 체계적인 대응방안을 세우는 데에도 익숙하지 못해 피해 복구에 대한 전문적인 기술개발이나 체계적인 연구가 진행되지 못하고 있다(수사연구, 2004: 17).

III. 사이버 테러 대응 실태 분석 및 문제점

1. 사이버 테러 대응 실태 분석

1) 공공분야 사이버 테러형 범죄 및 검거 실태

사이버 범죄는 크게 사이버 테러형 범죄와 일반 사이버 범죄로 구분하고 사이버 테러형 범죄는 정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스 유포, 메일폭탄, DOS공격 등 전자기적 침해 장비를 이용한 컴퓨터시스템과 정보통신망을 공격하는 행위를 말한다(한국경제, 2004. 4. 27: 8). 일반 사이버 범죄는 사이버 공간을 이용한 일반적인 불법행위로서 사이버 도박, 사이버 스토킹과 성 폭력, 사이버 명예 훼손과 협박, 전자상거래 사기, 개인정보 유출 등의 행위를 말한다.

다음은 2003년도 국가기관에 대한 사이버 테러형 범죄에 관하여 알아보기로 한다.

(1) 기관별 발생 현황

<표 2>는 2003년도 국가 공공기관별 해킹사고 발생 건수를 나타낸 것이다. 다른 기관에 비하여 교육기관, 특히 국·공립대학의 해킹사고 발생이 상당히 빈번한 것으로 나타났다.

<표 2> 기관별 해킹사고 발생건수

(단위: 건)

기관별 발생 건수	2002	2003												총계	비율 (%)
		1	2	3	4	5	6	7	8	9	10	11	12		
중앙 행정 기관	22	2	0	2	0	0	0	0	0	2	2	2	2	10	1.61
지자체	81	0	9	7	10	7	4	6	3	7	13	4	5	75	12.04
산하 기관	31	4	6	6	1	4	3	1	1	4	0	1	6	37	5.94
연구 기관	17	0	0	0	0	0	1	2	0	0	1	0	3	7	1.12
교육 기관 (교육청)	369	2	3	4	1	3	3	2	1	3	6	1	1	30	4.82
교육 기관 (국공립대)		9	9	48	95	55	32	32	64	37	28	23	15	447	71.75
기타	19	0	0	3	1	2	2	3	1	1	0	2	2	17	2.73
합 계	539	17	27	70	108	71	45	46	70	54	50	31	34	623	100

자료: 국가정보원(2004: 131).

(2) 피해 유형별 분류

<표 3>은 국가 공공기관의 해킹사고 통계를 피해 유형별로 나타낸 것이다. 가장 높은 피해 유형은 해커들이 다른 곳으로 침입하기 위한 중간 경유지로 이용된 피해가 558건으로 전체의 89.57%를 차지하고 있다.

<표 3> 피해 유형별 분류

(단위: 건)

피해 유형별 분류	02	03												총계	비율 (%)
		1	2	3	4	5	6	7	8	9	10	11	12		
경유지 이용	446	15	25	64	106	66	31	43	70	48	36	29	25	558	89.57
홈페이지 변조	36	2	0	1	0	1	9	2	0	1	11	0	7	34	5.46
자료 삭제 변조	7	0	0	0	0	1	3	1	0	1	2	0	0	8	5.46
사이버 시위	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.00
기타	49	0	2	5	2	3	2	0	0	4	1	2	2	23	3.69
합계	593	17	27	70	108	71	45	46	70	54	50	31	34	623	100

자료: 국가정보원(2004: 137).

(3) 침투 수법별 분류

<표 4>는 국가 공공기관의 해킹 사고를 침투 수법별로 분류한 것이다. 웜·바이러스가 가장 많고 그 다음이 취약점 스캐닝, 스팸 릴레이, 관리자 권한 획득의 순서로 나타났다.

<표 4> 침투수법별 분류

(단위: 건)

침투 수법	2003												총계	비율 (%)
	1	2	3	4	5	6	7	8	9	10	11	12		
관리자 권한 획득	4	4	2	0	1	8	4	2	4	19	2	5	55	8.83
웜 / 바이러스	5	12	45	63	34	13	11	40	25	3	9	10	270	43.34
스팸 Relay	4	7	10	24	24	9	9	2	1	2	2	5	99	15.84
취약점 스캐닝	3	4	4	20	11	11	19	24	18	23	16	8	161	25.84
기 타	1	0	9	1	1	4	3	2	6	3	2	6	38	6.10
합 계	17	27	70	108	71	45	46	70	54	50	31	34	623	100

자료: 국가정보원(2004: 139).

(4) 사이버 테러 수사 및 검거 실태

사이버 테러의 대표적 유형인 해킹과 바이러스와 관련된 총 범죄발생은 2000년 452건에서 2003년 14,241건으로 31배 증가하였고, 검거는 2000년 278건에서 2003년에는 무려 8,800여건으로 증가하여 사이버 테러의 위협은 더 이상 가상의 위협이 아니라 현실로 우리 곁에 있음을 보여주고 있다. 해킹의 대표적 사례는 2002년 4월 우리나라에서 발생한 해킹사건을 추적하던 사이버테러대응센터에서는 20여명의 국제적 해커들이 미국의 W사를 경유지로 이용하여 전 세계 시스템을 해킹하고 있는 것을 발견하고 면밀히 분석한 결과 이들은 95개국에서 11,222개의 시스템을 해킹하고 국내 시스템은 총 2,497개가 피해를 입은 사실을 발견했다(국가정보원, 2004: 235).

또한 주요 금융네트워크 사고를 보면 2001년 4월 한 해커가 국내 유명 신용카드회사 및 금융전산망과 전용망으로 연결되어 신용카드거래 승인·결제 업무를 수행하고 있는 신용카드 정보처리전문업체의 시스템을 해킹해 약 47만명 가량의 주민번호, 신용카드 번호 등 중요 신용정보를 유출하여 판매하려다 검거된 예가 있다. 피해사의 시스템은 이중 방화벽이 설치되어 있으며 모 보안업체로부터 보안관제서비스[4]도 받고 있는 상태였으나 피의자는 이 회사의 고급정보를 노렸다. 만약 해커가 오고가는 모든 데이터를 스니핑[5] 했더라면 국내 모든 신용카드를 다시 발급해야 했을 정도의 파급효과를 야기할 수도 있었다.

<표 5> 사이버 범죄 발생 현황

(단위:건)

구 분	계	사이버 테러형 범죄			일반 사이버범죄
		소계	해킹	바이러스	
2000년	2,444	452	449	3	1,992
2001년	33,325	10,674	10,562	112	22,651
2002년	60,068	14,159	14,065	94	45,909
2003년	68,445	14,241	14,159	82	54,204

자료: 경찰청(2004: 237).

<표 6> 사이버 범죄 검거 현황

(단위: 건,명)

구 분	계	사이버 테러형 범죄			일반 사이버범죄
		소계	해킹	바이러스	
2000년	1,715(2,190)	278(363)	275(360)	3(3)	1,437(1,827)
2001년	22,693(24,455)	7,595(8,099)	7,512(8,004)	83(95)	15,098(16,356)
2002년	41,900(47,252)	9,707(10,762)	9,707(10,762)	57(73)	32,193(36,490)
2003년	51,722(56,724)	8,891(9,992)	8,844(10,047)	47(55)	42,831(46,677)

자료: 경찰청(2004: 237).

4) 보안관제서비스는 여러 개의 네트워크 혹은 시스템 상에서 불법 침입행위가 일어나는지를 집중적으로 모아 모니터링하면서 필요시 관리자에게 대응조치를 하도록 경고를 하거나 특이 사용자들의 행태를 통보해 주는 시스템을 말한다.

5) 스니핑(Sniffing)은 시스템상에서 오고가는 데이터의 내용을 훔쳐보는 행위를 말한다.

2) 사이버 테러 관련 법 체계 현황

여기서는 관련 법규는 사이버 테러형 범죄에 해당하는 해킹과 바이러스와 관련된 법조항에 대하여 알아보기로 한다.

첫번째, 우선 국가기밀 관련 정보보호법령으로 국가보안법, 국가정보원법, 보안업무규정, 군사비밀보호법, 형법 등과 같이 주로 기밀성 위주의 정보보호 관련법령과 정보통신망상의 통신 수단 및 전자상거래 등의 발전으로 민간분야에서도 이용이 늘고 있는 비밀보호 수단인 암호의 사용과 관련된 법령으로 정보화 촉진 기본법, 전자거래기본법, 전자서명법 등이 있으며, 암호의 부정사용과 관련된 법령으로는 국가정보원법, 군 형법, 검찰사무보고규칙 등이 있다.

두번째, 정보통신망과 정보시스템의 보호조치와 관련된 법령으로는 정보화촉진 기본법, 정보통신기반 보호법, 정보통신망 이용 촉진 및 정보 보호 등에 관한 법률, 전자거래 기본법, 전자서명법, 화물유통 촉진법, 산업기술기반 조성에 관한 법률, 무역업무 자동화 촉진에 관한 법률 등이 있다. 또한 컴퓨터, 정보통신망, 정보 침해 관련 법령 형법이 개정되면서, 컴퓨터 범죄를 도입하여 처벌규정을 마련하였고, 이후 정보통신망 및 정보의 침해와 관련된 특별법이 다수 제정되었다. 현행법에서 컴퓨터, 정보통신망, 정보의 침해와 관련된 법령으로는 형법이 있으며, 특별법으로는 정보통신기반 보호법, 정보통신망 이용 촉진 및 정보 보호 등에 관한 법률, 신용정보의 보호 및 이용에 관한 법률, 통신비밀 보호법, 무역업무 자동화 촉진 등에 관한 법률, 화물유통 촉진법 등이 있다.

세번째, 개인정보보호 관련 법령이다. 정보화 역기능 중 중요한 부분을 차지하는 것이 개인정보의 침해로 최근 이에 대한 관심이 증가하면서 법령의 정비가 대폭적으로 이루어졌다. 개인정보 보호와 관련된 법령으로는 공공기관의 개인정보 보호에 관한 법률, 정보통신망 이용 촉진 및 정보 보호 등에 관한 법률, 금융실명거래 및 비밀보장에 관한 법률, 신용정보의 이용 및 보호에 관한

법률, 통신비밀 보호법 등이 있다.

네번째, 정보보호산업 육성 및 정보통신윤리 관련 법령이다. 여기에는 정보보호분야의 기술개발, 인력양성 등을 위한 정부의 시책과 정보보호 산업의 육성을 위한 규정이 정보화촉진 기본법, 전자거래기본법, 정보통신기반보호법에 규정되어 있다. 또한 최근 메일 등 정보통신서비스가 인터넷 비즈니스 활성화를 위해 활발히 이용되는 가운데, 스팸메일 등 부정적인 현상을 최소화시킬 수 있도록 2001년 1월 스팸메일 종합대책을 마련하여 법제도적인 정비를 추진해오고 있다.

이에 따라 2002년 7월 11일 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 시행 규칙을 개정하여 광고 문구를 일정규칙에 따라 '(광고)' 및 '(성인광고)'로 표시하도록 의무부과 함으로써 이메일 이용자가 원하지 않는 스팸메일에 효과적으로 대응할 수 있도록 하였다.

다섯번째, 행정절차법 중 개정법률로 전자정부 구현을 위한 행정업무 등의 전자화 촉진에 관한 법률이 제정됨에 따라 행정절차에 있어서 전자적 방식에 의한 업무처리가 가능하도록 그 근거규정을 마련하는 한편, 현행 규정의 운영상 나타난 일부 미비점을 개선·보완하기 위하여 2002년 12월 30일 개정되었다.

또한, 정보통신기반 보호법 중 개정법률로 현행 정보통신기반 보호법은 정보보호전문업체를 정보통신부 장관이 지정하도록 되어있는 바, 국문 명칭이 정보보호 전문업체로 되어 있어 정보보호 산업 전체를 포괄하는 전문업체라는 의미로 판단될 소지가 많으므로, 이 법에서 부여하고자 하는 업무나 기능에 맞게 정보보호 전문업체가 수행하는 업무가 정보보호 컨설팅 분야의 업무임을 분명히 하기 위하여 그 명칭을 정보보호 컨설팅 전문업체로 변경하기 위하여 2002년 12월 18일 개정되었다.

정보통신망 이용 촉진 및 정보보호 등에 관한 법률 중 개정법률은 현행 정보통신망 이용 촉진 및 정보보호 등에 관한 법률로는 급증하고 있는 스팸메일 등 악성 광고성 정보 전송행위와 개인정보 침해 행위에 적절히 대응하기 어려우므로, 전화·모사전송 등에 의한 영리성 광고 행위에 대한 규제 강화, 수신 거부를 고의로 회피하는 행위 금지, 연락처 자동 생성을 통한 광고 전송행위 금지, 전자우편 주소 추출행위 금지, 청소년 유해 매체물 광고 금지 등 악성 광고성 정보 전송행위에 대한 규제를 강화하고, 불법으로 개인정보를 제공받은 자를 처벌함으로써 국민의 사생활을 보호하기 위하여 2002년 12월 18일 개정되었다.

3) 사이버 테러 대응 체계 현황

현재 우리나라의 사이버 테러 대응체계는 크게 국가정보원 중심의 국가·공공분야 정보보안체계와 정보통신부 중심의 민간분야 정보보호체계로 이원화되어 있으며, 2003년 1월 25일 인터넷대란을 계기로 민·관·군에서 동시에 추진해 온 사이버 테러 대응기구들이 발족하면서 국가 사이버 테러 대응체계의 큰 틀이 갖추어지고 있다(디지털타임스, 2003. 12. 16). 국내전산망 침해사고 대응 업무를 수행하는 기구는 국가사이버안전센터를 중심으로 국방분야 - 국방정보전대응센터, 민간분야 - 인터넷침해사고대응지원센터, 교육기관 - 국가보안기술연구소, 주요 정보통신기반시설 - 분야별 정보공유분석센터가 담당하고 있으며 검찰과 경찰은 사이버 범죄수사를 맡고 있고, 이 기구들 간의 상호 의견을 조정할 비상설 총괄기구로 "사이버안보조정회의"가 국가안전보장회의 산하에 설치되어 있다.

정보통신기반보호법에 따르면 현행 국가보안업무 수행체계와 마찬가지로 국가기관 및 지방자치단체 소관의 주요 정보통신 기반시설과 도로·공항·전력·국가지도 통신망 등 국가안보에 중대한 영향을 미치는 시설에 대한 보호대책 수립과 침해사고 예방 및 복구업무는 국가정보원(국방 분야의 보호지원은 국군기무사령부) 중심으로 지원하도록 규정하였다.

이와 관련하여 국정원은 제8국(대테러보안국)을 중심으로 1999년 1월부터 컴퓨터 보안 전문요원으로 '국가전산망 보안관리반'을 편성해 국가·공공기관 전산망에 대한 보안진단 및 보안시스템 운용기법 등 실무차원의 보

안기술 지원활동을 하고 있다. 국정원은 1999년 8월부터 국가·공공분야의 사이버 테러 예·경보 및 해킹사고 신고 접수 및 피해 복구를 전담하는 '정보보안 119'(www.nis.go.kr//nissc)를 확대 개편하여 국가사이버안전센터를 설립하였다. 이 밖에 2001년 7월부터 시행한 정보통신기반보호법상의 주요 정보통신 기반시설의 보호 및 침해사고 예방 및 복구에 관한 기술적 지원을 하는 전문기관으로는 한국전자통신연구원(ETRI) 부설 국가보안기술연구소와 한국정보보호진흥원이 있다. 1980년대 초부터 국가 공공기관의 보안 시스템 개발업무를 담당해 온 한국전자통신연구원의 부호기술연구부와 국방과학연구소(ADD)의 정보보호부를 통합하여 지난 1월 한국전자통신연구원 부설연구소로 설립된 국가보안기술연구소는 우리나라의 사이버전 대응기술과 관련해 외국이 가장 주목하는 곳이다. 그 때문인지 이 연구소가 수행하는 모든 연구 프로젝트는 국가기밀로 분류되었고, 홈페이지조차 공개하지 않을 만큼 보안을 유지하고 있다. 한국정보보호진흥원(http://www.kisa.or.kr)은 민간 차원의 침해 대응기술 지원기관으로 민간기업의 침해사고 복구를 지원하는 '사이버 118'을 운영하고 있다(주간동아, 2001. 8. 2: 8)

(1) 사이버테러대응센터

경찰은 1995년 국내 최초로 사이버 범죄 수사기구인 해커수사대를 창설한 것을 시작으로 1997년 컴퓨터범죄수사대, 1999년 사이버범죄수사대 등 사이버 전담조직을 확대 개편해 왔으며, 해킹 바이러스의 급증과 날로 심각해지는 사이버 테러의 위험성에 대한 범정부 차원의 종합적 대응체제 필요성이 제기되면서 2000년 7월 사이버테러대응센터를 창설해 운영 중에 있다. 사이버테러대응센터의 구성은 협력운영팀, 수사1팀, 수사2팀, 기법개발실 등 3개팀 1실로 조직되어 있으며, 사이버 테러 종합대책 수립시행, 전국 사이버 수사요원 교육, 국제 공조 수사 활동, 24시간 사이버 순찰을 통한 초동조치 및 대 국민 경보발령, 주요 사이버 테러 사건 수사, 사이버 테러 수사 기법 개발 및 기술 지원 등 종합적인 업무를 수행하고 있다.

(2) 인터넷범죄수사센터

우리나라에서 사람들의 주목을 끈 컴퓨터 범죄는 1973년 10월에 발생한 이른바 반포 AID 아파트 입주권자 부정추첨 사건이었다. 그러나 이때까지만 해도 간헐적으로 발생하는 컴퓨터 범죄에 대한 체계적 대응이 마련되지 않고 있다가, 컴퓨터 및 네트워크 범죄가 뚜렷해진 1995년 4월 서울지검에 독립된 수사조직이 처음 설치되었다(정동섭, 2001: 3). 이후 1996년 6월 대검찰청 중앙수사부 수사기획관실내에 정보범죄대책본부를 설치한 것을 시작으로 1999년 4월 정보범죄대책본부를 컴퓨터범죄전담수사반으로 개칭하고 2000년 2월에 중앙수사부 내에 컴퓨터 수사과를 신설하였으며, 2001년 2월에 대검찰청 인터넷범죄수사센터로 확대·개편하였다. 인터넷범죄수사센터는 대검찰청과 서울지검에 각 설치되어 있으며 대검찰청 중앙수사부 컴퓨터수사과와 서울지검 컴퓨터수사부에서 이를 각각 운영하고 있으며, 해킹, 바이러스 유포, 개인정보 침해, 컴퓨터 이용 사기, 전자상거래 사기, 명예·훼손, 음란물, 도박 등 각종 인터넷 범죄에 대한 수사활동을 벌이고 있다. 특히 통신, 에너지, 운송, 자원 등 국가기반 정보통신시설을 대상으로 이루어지는 사이버 테러 행위와 전자상거래 사기, 개인정보 침해와 같은 국민생활과 직결된 컴퓨터 범죄를 중점 단속분야로 선정해 두고 있다.

(3) 국가사이버안전센터

민·관·군에 대한 사이버 보안 위협 정보를 종합 수집·분석하는 등 범국가적 사이버 테러 대응역량 강화를 위하여 기존 국가정보원의 '정보보안 119'를 확대·개편하여 국가사이버안전센터가 설립되었다. 국가사이버안전센터는 국방분야와 민간분야 및 공공분야의 사이버 보안 위협 정보를 공유·분석하여 위험도를 산정, 예·경보를 발령하는 등 국가 사이버 테러 대응 업무를 총괄한

다. 특히 공공분야 CERT로서 국가·공공기관에 대해 정보보안 기술을 지원하고, 사이버전 모의훈련을 실시하는 등 예방활동과 함께 사고 발생 시 각급 기관 및 분야별 CERT/ ISAC 등으로부터 사고접수 및 상담을 수행하고 사고조사 및 복구지원 업무를 수행한다. 특히 1.25인터넷 마비 사태와 같은 국가적 재난이 발생할 경우에는 범국가차원에서 민·관·군 합동 '사고조사반'과 '복구지원반'을 편성 지원한다.

(4) 국방정보전대응센터

국군기무사에 설치된 국방정보전대응센터는 국방분야의 사이버 테러 대응 역량강화와 군의 주요 정보체계에 대한 보호지원을 위해 사이버 테러 대응팀과 정보통신 기반보호팀으로 구성되어 있다. 국방정보전대응센터는 국방분야에 대해 사이버테러 예·경보를 발령하고 국방전산망에 대한 24시간 위협정보 탐지·분석과 침해사고 예방활동, 사고발생 시 원격·현장 피해복구지원 및 국내외 정보전·사이버전과 관련된 정보 분석 등의 업무를 수행한다. 또한 정보작전 방호태세 훈련 중 모의공격과 국방 정보통신 기반시설에 대한 취약점 분석·평가, 정보 시스템 보안측정 및 진단, 정보통신 보안 컨설팅 등의 업무를 수행한다.

(5) 인터넷침해사고대응지원센터

민간분야의 사이버 테러 대응 역량 강화를 위하여 한국정보보호진흥원(KISA)내에 인터넷침해사고대응지원센터가 설치 운영되고 있다. 인터넷침해사고대응지원센터는 인터넷 서비스 제공자(ISP), 인터넷 데이터 센터(IDS) 등 민간분야 전산망에 대한 사이버 테러 예·경보를 실시하고, 침해사고 발생시 침해사고 원인을 분석하여 신속 정확한 대국민 대응 요령을 전파하며, 사고지원 업무를 수행하는 등 민간부분의 CERT 역할을 수행한다. 센터 내에는 분석대응팀, 인터넷모니터링팀, 침해사고대응협력팀으로 나뉘어 있으며, 분석대응팀에서는 침해사고 긴급대응 및 기술지원, 현장조사 지원 및 바이러스 샘플 채취, 해킹 바이러스 대응 기술 연구 등을 담당하고 있고, 인터넷모니터링팀에서는 ISP네트워크 상황모니터링, 국내외 침해 사고 초동 대응 및 접수 상담, 국내외 주요 사이트 모니터링 등의 업무를 담당하고 있으며, 침해사고 대응협력팀에서는 FIRST, AVAR, 국가 CERT 협력, APCERT, CONCERT 사무국 운영, 국내 ISP, IDC, ISAC 협력체계 구축운영 등을 담당하고 있다. 그리고 국가사이버안전센터, 국방정보전대응센터 등과도 연계하여 민간분야의 각종 사이버 위협 정보를 공유하며, 백신업체, 소프트웨어 개발자 등과도 협력하여 인터넷 침해사고 정보 보안 패치 정보 등을 수집·전파하는 업무를 수행한다.

(6) 국가보안기술연구소(NSRI)

방대한 전산망과 시스템을 운용중인 교육기관의 중요성을 감안, 교육분야의 인터넷 침해 사고 대응 역량 강화를 위해 국가보안기술연구소내에 교육기관침해사고 대응센터를 구성·운영 중이다. 국공립 대학 및 초·중·고를 대상으로 대응업무를 수행 중이며, 인터넷 침해 사고 처리 뿐 아니라 인터넷 보안 취약점 연구, 홍보와 교육 활동 등을 수행하고 있다. 또한, 교육기관침해사고대응센터는 최신 해킹 및 보안 취약점에 대한 분석을 통하여 기반기술을 확보하고 분석자료를 바탕으로 사고대응 기술을 연구·개발, 침해사고에 적극 대응하고 있다.

(7) 정보공유분석센터(ISAC)

정보통신기반보호법 제16조를 근거 규정으로 주요 정보통신 기반시설에 대한 보호업무를 수행하는 정보공유분석센터[6]는 현재 통신부문과 금융부문에서 운영중이다. 2002년 1월 설립된 통신분야 정보공유분석센터는 KT, 데이콤, 하나로통신 등 국내 통신사업자들을 회원사로 하여 정보보호위원회를 운영하고, 회원사 정보, 침해사고, 취약점 등에 관한 자료 조사 및 DB를 구축, 운영하

6) 국가 전산망에 가해지는 사이버 테러 대응 전략의 핵심은 정보공유분석센터이다.

면서 회원사들에 대하여 On-Line 정보제공 및 침해 사고 처리 등의 업무를 수행하고 있다. 2004년 현재 통신사업자연합회 소속에서 KISA로 이관되어 운영 중에 있다. 2002년 12월 설립된 금융정보공유분석센터는 금융·증권 관련 회원사 간 침해사고, 취약점 등에 관한 자료조사 및 DB를 구축·운영하고 회원사에 보안 정보를 제공하며 금융증권 분야 주요 정보통신 기반시설에 대한 취약점 분석·평가 및 보호대책 수립 지원 등의 업무를 담당하고 있다.

2. 사이버 테러 대응에 관한 문제점

1) 관련법 체계의 미흡

사이버 테러는 물리적 공간의 테러와는 달리 초단위로 이루어지는 신속성과 세계 어느 곳에서든 지리적 거리를 뛰어넘어 공격할 수 있는 광역성 등에 비추어 볼 때 사이버 공간에서 벌어지는 각종 범죄행위에 대응하기 위해서는 국제적 공조와 함께 체계적인 법정비가 필수적으로 요구되고 있다. 특히 최근의 범죄는 온라인의 기술적 특성과 오프라인의 범죄적 특성이 결합되는 추세이며, 사이버 공간의 특성상 한 나라에 국한된 것이 아니라 국경을 넘어 여러 국가가 관련되는 국제적 범죄 행위가 되는 경우가 많다(문화일보, 2004. 4. 15: 12). 이에 따라 지난 2001년 유럽의회에서는 약 45개국이 사이버범죄협약을 체결하여 공동대응하기로 함에 따라 전 세계에 사이버 범죄 대응 모델로 자리잡고 있다. 이 법을 살펴보면 각종 사이버 범죄에 대한 실체법적인 대응책과 함께 초국경성, 익명성 등 사이버 범죄의 특성을 감안하고 실체법의 실효성을 담보하기 위한 절차법 규정과 국제협력 방안을 마련해 두고 있다. 그런데 우리나라의 사이버 범죄 처벌규정들은 실체법 규정도 형법, 정보통신망법, 정보통신기반보호법 등에 산재되어 있으며 서로 별개의 행위가 아니라 비슷한 행위 양상들을 결과 혹은 보호대상에 따라 별도의 법에 각각 적용하고 있어 사이버 범죄에 대한 대응이 국제적 동향과 차이를 보이고 있다. 또한 2001년 9.11테러 이후 미국은 뉴테러리즘에 대응하는 테러방지법인 '패트리어트법(USA PATRIOT)'을 도입했고 많은 국가들이 이와 비슷한 테러방지법을 제정하거나 테러 관련법의 강화를 서두르고 있다. 당시 월드컵 등 중요한 국제적 행사를 앞둔 우리 정부도 예외가 아니어서 동년 11년 6일 국무총리실에서 테러방지 종합 대책을 발표하고, 이어 12일 국가정보원에서 테러에 효율적·체계적으로 대처하여 국가의 안전을 보장하고, 국민의 생명과 재산을 보호해야 한다는 명분으로 테러의 예방·방지 및 범인색출 등 전 과정을 규정한 테러방지법안을 입법 예고[7]했으나 인권·사회단체를 위시로 대한변호사협회 등에서는 테러 범죄의 개념과 범위가 모호하고 추상적이어서 국정원의 자의적인 해석에 따른 인권침해가 우려되고, 테러범죄에 대한 예방과 처벌은 현행법으로도 충분하다는 등의 문제가 제기되면서 답보상태에 놓여있다.

또한 정보통신기반 보호법에 따라 국무총리 산하에 정보통신기반보호위원회가 설치되어 있으나, 이는 국가안보·행정·국방·치안·금융·통신·운송·에너지 등 주요 정보통신 기반시설의 보호정책에 관한 사항에 한하여 기관간 조정업무 등을 수행하고 있어, 개념 구분이 불분명한 사이버 테러리즘을 포함한 광범위한 사이버 범죄의 예방·수사·소추 및 이를 위한 정보의 관리 등 광범위한 정책집행에까지 여력이 미치지 못하는 실정으로, 기관간의 정보교류 및 공동대응을 위한 구심적 역할을 수행할 상설 집행기구의 마련이 시급한 상황(김원준, 2002: 93)이고, 정보통신부와 KISA의 자체 조사결과에 따라 당초 2003년말 지정되기로 한 제3차 주요 정보통신기반시설[8]의 지정이 부처간의 협의 지연을 이유로 미루

7) 2001년 11월 12일 입법예고 후 인권·사회단체의 반발에 부딪치자 11월 20일 참고인 구인·유치 조항과 구속기간 연장 조항을 삭제하고 불고지죄 조항도 완화하고 국정원의 테러수사권을 명시적으로 규정한 부분도 삭제한 개정입법안을 내놓았고 이후 11월 22일과 26일 차관회의에서 당초 입법예고안에서 총 15개 조문에 대한 수정과 삭제를 거쳐 27일 국무회의에 상정되었고 현재는 정부입법으로 국회 정보위원회에 상정되어 있다.

8) 제3차 주요 정보통신 기반시설은 전자정부 11대 과제 중 사회간접시설과 해양수산부 등 관련 시설을 말한다.

어져 있다.

2) 사이버 테러 대응 전문화의 부재

사이버 범죄의 폭발적 증가와 함께 사회 모든 기반시설이 빠르게 네트워크화 되면서 국가경제와 안보에 대한 위협의 크기가 증대되고 있고, 전산망 자체에 대한 공격이나 네트워크 분야에 고유한 범죄 행위에서 비롯된 사이버 범죄의 범위는 기존 off-line 범죄와 점점 구별이 불분명해지고 있으며 오히려 서로 융합 혼재되는 추세에 있다. 사기의 수단으로 인터넷이 이용된 것은 이미 오래 전이며, 인터넷 게시판이나 e-mail을 통해 불법의약품이 거래되거나 음란물이 유통되는 등 거의 모든 범죄에 인터넷이 수단으로 혹은 범죄장소로 이용되고 있다. 특히 대부분의 사이버 범죄는 국내에만 국한되지 않고 전 세계로 연결되어 있어 첨단장비를 바탕으로 정보수집 및 국제적으로 공조 강화의 필요성이 그 어느 때보다 강조되고 있다. 그러나 정보통신부가 사이버범죄에 대한 사법경찰권을 갖겠다[9]고 법개정을 요구한 것처럼 사이버 범죄에 대한 주도권을 두고 부처간 이해가 상충되면서 국가 전체의 사이버 범죄 대응력을 떨어뜨리는 요인이 되고 있다. 이는 사이버 치안 환경에 신속히 대처하기 위해 중앙수사기관에 사이버 범죄 전담기구를 편성하는 세계적인 추세에도 역행하는 일이다.

또한 기술적인 요소가 매우 큰 비중을 차지하는 사이버 범죄를 담당하는 수사관의 육성문제이다. 우리나라에서 사이버 범죄라고 할 만한 사건을 본격적으로 수사하기 시작한 것은 아직 10년이 되지 않아(경찰청, 2003: 19) 전문인력 양성이 기존 수사요원에서 선발하는 방법과 컴퓨터 전공자를 특채해, 일반수사 출신자에게는 컴퓨터 기술을 컴퓨터 전공자에게는 수사기법을 교육시켜 사이버 수사관으로 양성하고 있으나 인력 운용의 효율성 측면에 문제가 있다.

3) 통합적 관리체계 미흡

국가 중요시설이나 사회안전망을 보호하기 위해서는 유관기관의 종합적인 협력체제가 이루어져야 한다. 경찰은 2002년까지 370억원을 투입하여 사이버 테러리즘에 대한 대응조직인 '사이버테러대책본부'를 설립하였다(경찰청, 2000: 142). 국정원, 국방부, 검찰청, 정보통신부 등 관계기관별로 대책이 추진되고 있는 실정을 감안한다면 사이버 테러리즘에 대한 대응비용은 기하급수적으로 증가할 것이다.

그리고 사이버 테러리즘에 대한 규제입법이 이루어진다고 할지라도 이를 집행하는 법 집행기관의 철저한 대처, 즉 집행에 필요한 지식이나 기술을 갖추지 못한다면 사이버 테러리즘 대책과 입법대책의 목적을 달성하지 못할 것이다. 사이버 범죄의 대부분은 해커나 컴퓨터 공학도 같은 고급 두뇌에 의해서 이루어지고 범죄의 발각과 증명이 어려우며 암수범죄가 많기 때문이다. 또한 사이버 테러리즘을 발각한다고 하더라도 컴퓨터에 대한 지식의 결여로 수사기관 또는 법원에서 불기소 또는 무죄로 되는 사례가 많이 나타나고 있다(신각철 외, 1997: 327). 이러한 이유로 수사관의 수사능력의 배양, 검사·법관의 컴퓨터 지식 배양 문제는 오늘날 사이버 테러리즘의 극복을 위한 중요한 과제가 되고 있다. 즉 정보보호 관련 전문요원들에 대한 재교육과 수사관들의 교육지원이 뒤따라야 할 것이다. 우리나라의 경우를 살펴보면 각기관별로 교육지원을 하고 있는 실정인데 비해서 외국의 경우는 수사기관, 검사·판사 등의 형사 사법기관에 근무하는 인원들에 대한 컴퓨터 교육은 컴퓨터 범죄 연구기관과 긴밀한 협조관계에서 이루어지고 있다. 예를 들면 Freiburg 대학부설 형사정책 및 경제법연구소(Institut für Kriminologie und Wirtschaftstrafecht der Universitat Freiburg), 미국의 Stanford Research Institute의 컴퓨터범죄에 대한 연구소가 유명한데 이들 연구소에서

9) 정보통신부가 사이버 범죄 대부분을 직접 수사할 수 있도록 하기 위해 법 개정을 추진 중인 것으로 확인됐다. 이에 대해 시민단체들은 정통부의 사법경찰권 확대 요구는 "경찰국가로의 후퇴"라며 강력반발하고 있다. 정통부는 현재 무선 설비·전자파 장애기기에 관한 범죄, 전기통신 설비·기자재에 대한 범죄, 프로그램저작권 침해에 관한 범죄 등의 분야에서 사법경찰관을 행사하고 있다(연합뉴스. 2004. 5. 7).

수사기관 요원과 형사정책 담당자들을 교육시키고 있는 것이다(김홍근, 1999: 2). 따라서 우리나라에서도 이러한 산・학・연 합동의 컴퓨터 범죄 연구소 모델이 필요한 실정이다.

우리나라 사이버 테러 대응체계는 민간과 공공분야에서 다양한 형태의 사이버 테러 대응체계를 갖추어 운영해 왔지만 2003년 1월 25일 인터넷 대란을 통해 그 허점이 드러났다. 주요 정보통신 기반시설에 대한 침해사고가 발생할 경우 국가적으로 가동하기로 되어 있는 정보통신 기반 침해사고 대책본부가 만 하루가 지나서야 구성됐지만 활동이 미흡하다는 평을 받고 있다. 더욱이 정부와 인터넷 서비스 제공업체(ISP), 한국정보보호진흥원(KISA) 등 연구기관, 보안업체, 수사기관 간 공동대응은 고사하고 정보공유와 같은 기본적인 협조도 거의 이루어지지 않았던 것으로 지적되고 있다(디지털타임스, 2003. 12. 16: 8).

4) 국제 공조체제의 비효율성

국경을 초월한 사이버 테러리스트들의 활동을 규제하기 위해서는 국제 공조체제의 구축과 사이버 테러리즘 대응 국제기구에 대한 적극적인 가입과 참여가 필요하다. 1997년 12월 9일부터 10일까지 미국 워싱턴 D.C.에서 개최된 "선진 8개국 법무・내무장관회의(미국, 영국, 독일, 일본, 이탈리아, 캐나다, 프랑스, 러시아 - Meeting of Justice and Interior Ministers The Eight)"에서는 첨단 기술범죄의 수사・기소 능력을 강화하고 범죄 인도와 상호간 법적 지원을 위한 국제 협력을 강화하기로 하는 내용의 공동발표문을 발표하고, 정보시대의 범죄에 대처하기 위하여 공동발표문 부칙으로 10개의 원칙과 10개 항의 행동계획을 합의한 바 있으며, 또 1998년 1월 29일부터 30일 까지 영국 Birmingham에서 개최된 "EU 내무・법무장관회의"에서는 "EU 회원국간 인터넷범죄 대처방안"을 논의한 바 있는데, 컴퓨터 범죄에 대한 국제적 대처를 위한 노력이라 할 것이다. 마지막으로, 기술적 측면에서 살펴보면 현재 모든 국가 중요시설과 정부기관 시스템에 대한 방화벽(Fire Wall)과 같은 기본적인 정보보호 기술의 적용도 이루어지지 않은 것이 사실이다. 우리나라의 정보화를 책임지고 있는 정보통신부 홈페이지가 해킹을 당한 사실을 보면 다른 기관의 정보보호 기술도 허술한 것을 알 수 있다(세계일보, 2000. 8. 29: 13). 그리고 관련 중요 데이터는 암호화하여 보관할 필요가 있다. 미국은 이미 1977년 7월에 IBM의 암호방식을 채택하여 미국 연방정부의 데이터 암호규격(DES: Data Encryption Standard)으로 채택하였다. 우리나라에서도 이러한 암호체계를 전 사업분야로 채택하여 안전하게 데이터를 보관해야 할 것으로 보인다. 정보보호 프로그램도 갖추지 못한 현실에서 암호화 시스템까지는 아직 요원한 것이 사실이다. 하지만 정보화의 역기능은 과거 어느 때보다 심각하기 때문에 결코 낭비적인 요소는 아니다.

그리고 사이버 테러리스트의 침입을 유도하여 역추적을 한 후 검거하는 해커트랩과 같은 기술 활용이 부족하다. 지금 대다수의 국가 중요기관이나 사회안전시스템망에는 해커트랩이 설치되어 있지 않다. 따라서 사이버 테러리스트나 컴퓨터범죄자가 지금도 무방비로 뚫려 있는 국가 중요 전산망을 침투하는 것이 현실이다.

IV. 사이버 테러 대응방안

1. 현실에 맞는 법률 개선

암호기술을 필두로 한 정보보호를 위한 기술적 방법은 현재 상당한 진전을 보이고 있으나, 기술의 활용을 담보할 수 있는 법제도적인 방법이 병행하지 않는다면, 정보보호의 완전성을 기하기는 어렵다.

형사처벌과 관련된 법률은 단순하고도 명확하게 적용될 필요가 있으며 가급적 일원화된 체제로 정비되어야 예측 가능성을 높일 수 있다. 미국의 사이버 테러 관련 실체법적 규정을 보면 1984년도에 제정된 컴퓨터 사기 및 오용 방지법을 기본으로 하여 시대적 상황을 반영하여 조문 개정작업을 거쳐 오늘날 사이버 테러범죄에 대응하고 있는 것은 시사하는 바가 크다. 그에 반해 우리나

라의 경우 컴퓨터 범죄 현상과 관련한 규정을 1995년 형법 개정시 반영하였으며, 기타의 사이버 테러 관련 실체법 규정들은 기존의 형법의 규정을 개정하기 보다는 정보통신망법, 정보통신기반보호법 등 새로운 법을 만들어 특별법의 특별법 역할을 하게 하는 등 법적 안정성, 예측가능성, 체계성을 크게 훼손하고 있으므로 우리 법도 일원화된 체계를 갖는 것이 필요하다. 또한 테러방지법은 최근 상황을 최대한 반영함으로써 사이버 테러에 대한 부분까지 포함시켜 국가안보에 위협이 될 수 있는 모든 테러 상황에 대비할 수 있는 법으로 제정하는 것이 필요하다고 생각한다.

2. 사이버 테러에 대응하기 위한 전문성 추구

현재 우리나라의 상황을 보면 사이버 공간에 대한 투자는 일부 대기업과 중앙행정기관을 중심으로 이루어지고 있으며 그나마도 관련 인력도 없이 장비만 들여다 놓고 정보보호 제품만 구입하는 수준이다(국가사이버안전센터, 2004: 124).

국가 기간 전산망을 사이버 테러 등 각종 위기상황으로부터 안전하게 운영하기 위해서는 보안시설과 장비에 대한 지속적인 투자도 중요하겠지만 관련 인력의 전문성을 높이는 일이 다른 분야보다 최우선 과제로 논의되고 보완되어야 한다. 기술 인력이 일반 행정부서 직원에 비해 승진에 있어서 불이익을 받고 다방면에 걸친 팔방미인형 인력을 요구하는 현행 제도를 과감히 개선하여 전산시스템을 운영하는 직원의 전문성을 최대한 보장해주고 보수 등에 있어서도 인센티브를 제공하는 것이 필요하다.

또한 현재 사이버 범죄 수사의 중추적 역할을 하고 있는 사이버테러대응센터의 인력은 특채를 통한 사이버 수사인력 확충과 기존 수사요원을 선발하여 전문교육을 통해 전문성을 강화하고 있으나 앞으로 고도로 진전된 정보화 사회에서 사이버 범죄자들에 대해 효과적으로 대응하기 위해서는 일반수사는 수사부서 등에서 선발된 인력의 재교육을 통해 전문성을 키운 일반 수사관이 진행하도록 하고 컴퓨터 전공자는 현재 사이버 수사에서 중요하게 요구되고 있는 디지털 증거 확보에 전문성을 가진 증거분석관으로 육성하는 방안 등을 검토해야 한다. 특히 민간 정보보안 전문가 육성에도 관심을 가질 필요가 있다. 컴퓨터 보안사고는 처음에는 범죄에 의한 것인지 여부가 분명하지 않은 경우가 많기 때문에 초기에 자체 전담요원으로 하여금 사고에 대한 적절한 대응을 맡기는 것도 필요하다(Kevin Mandia & Chris Prosise, 2002: 293).

마지막으로, 공공기관의 보안의식 제고와 함께 최근 사회 일각에서 사이버 윤리를 정식 교과목에 채택하자는 의견까지 대두되고 있는 만큼 학생들을 상대로 한 사이버 보안 교육이 절대적으로 필요하다.

3. 사이버 테러 대응 통합 관리기구 설치

우리나라의 주요 국가 기간 전산망은 모든 사항을 책임지고 통합하는 기구가 없이 해당 부처 책임 하에 관리되고 있다. 주요 정보통신 기반시설의 경우 정보통신기반 보호법에 따라 국무총리 산하에 정보통신기반보호위원회가 설치되어 있으나, 이는 국가안보・행정・국방・치안・금융・통신・운송・에너지 등 주요 정보통신 기반시설의 보호정책에 관한 사항에 한하여 기관 간 조정업무 등을 수행하고 있어, 개념구분이 불분명한 사이버 테러리즘을 포함한 광범위한 사이버 범죄의 예방・수사・소추 및 이를 위한 정보의 관리 등 광범위한 정책 집행에까지 여력이 미치지 못하는 실정이다(김원준, 2002: 93).

물론 2003년 1월 25일 인터넷 대란을 겪으면서 이러한 문제를 해결하기 위해 금년 초 국가정보원에 국가 사이버 보안의 실질적인 총괄기구라고 할 수 있는 국가사이버안전센터를 두었지만 이 또한 국가안보에 관한 최고의결기구인 국가안전보장회의 산하에 '사이버안보조정회의'와의 역할에 명확한 규정이 부족해 보여 유사시 혼선이 우려된다. 또한 국가사이버안전센터가 총괄기구로서 역할을 하려면 인터넷침해사고대응지원센터와 국방

정보전대응센터를 비롯해 각종 정보공유분석센터와 일반 기업의 컴퓨터 침해 사고 대응팀(CERT)까지 아우르는 정보공유 체제가 구축되어야 하는데 현재는 이에 대한 명확한 법적 근거가 없다. 따라서 인터넷 사고 재발을 막고 피해를 최소화하기 위해서는 2003년 1월 25일과 같은 대규모 위기 발생 시 현재 국가사이버안전센터에 민·관·군 합동 조사팀과, 복구지원반이 구성되게 되어 있지만, 이를 상설화 하여 평시에는 네트워크 안전성과 보안기술 등에 대한 연구개발을 강화해야 한다.

또한 해킹, 바이러스 등 사이버 테러 대응 기술은 선진국과 3~5년, 암호 알고리즘 등의 원천 기술은 미국, 이스라엘 등과 5~10년의 격차가 있는 만큼(삼성경제연구소, 2003: 20), 정부만의 노력으로 사이버 공간의 범죄 행위와 역기능을 방지할 수 있는 것이 아니라 적극적인 민간의 참여가 있어야 한다. 따라서 정부, 기업, 언론, 사용자, 백신 소프트웨어 개발업체 등 모든 분야를 포괄하는 공동의 협의체를 구성함으로써 민간분야에서는 사이버 공간 보호를 위한 보안기술 개발과 연구, 네트워크 사용자 모두에게 적용될 수 있는 자율적인 규제방안을 마련하는 부문을 맡고, 정부에서는 관련된 예산을 지원하고 공동협의체에서 나오는 의견을 수렴해 정책으로 뒷받침한다면 사이버 공간에서의 범죄 행위를 예방하는 데에 커다란 힘을 발휘할 수 있을 것이다.

4. 사이버 테러에 대한 국제 공조 수사 개선

UN의 '컴퓨터 관련 범죄의 방지와 통제에 관한 보고서'는 현대사회의 경제시스템이 기본적으로 국제적인 정보의 교환과 공유를 필요로 하는 등 정보에 의존하는 영역이 더욱 넓어짐에 따라 컴퓨터 관련 범죄는 국제적으로 발생할 것이라고 주장하면서 국제 공조(International Cooperation)의 필요성을 강조하고 있다. 즉 국제 금융시스템과 항공 등이 국제 정보통신 네트워크를 이용하여 서비스되고 있고, 전자상거래[10]의 활성화에 따라 UN 국제상거래위원회(United Nations Electronic Data Interchange for Administration, Commerce and Transportation: UN/ EDIFACT)가 EDI(Elect ronic Data Interchange)의 기준으로 활용될 수 있는 모델법을 제정하는 등 오늘날 국제사회의 변화를 고려할 때 컴퓨터 범죄는 국제법에 있어서 새로운 도전이 되고 있다.

사이버 범죄 피해자들이 피해 사실을 신고하는 곳을 보면 해당 인터넷업체 신고센터에 51%, 경찰청 17.1%, 정보통신윤리위원회 11.4%, 한국정보보호센터 11%, 기타 6.8%, 검찰청 2.7% 순을 보이고 있다(이민식, 2000: 87). 또한 경찰청 사이버테러대응센터는 지난 1995년 창설이후 지금은 세계적 수준의 사이버 수사능력을 보유하고 있다는 평가를 받고 있다. 따라서 사이버 수사는 경찰청 사이버테러대응센터가 중심이 되어 각 유관기관별 공조체제를 구축하는 것이 업무의 효율성과 전문성 확보에 기여할 것이다. 또한 사이버 공간은 국경이 없는 공간이기 때문에 외국에서 발생하는 바이러스와 해킹 등이 일순간에 전 세계로 유포되어 국가안보에 커다란 위협요소로 작용하고 있다는 점을 감안하면 국제 협력 분야에 있어서 인터폴 사이버 범죄 관련 기구 및 국제컴퓨터침해사고대응협의회(FIRST)[11], FBI 컴퓨터범죄회의·정보보호 전문가 그룹 등과의 지속적인 협조체제와 인적교류를 강화하는 것이 무엇보다 중요하다. 특히 지난 1991년 제정된 국제형사사법공조법이 시간을 다투는 사이버 테러와 같은 범죄 현실에 전혀 맞지 않는 상황이므로 유럽

10) 1989년 미국 Southern California 대학의 연구 보고서에서 처음 사용되기 시작한 전자상거래(Electronic Commerce)는 디지털 정보의 전자적 교환을 통해 이루어지는 상거래, 공동의 표준을 사용하여 전자화한 상업적 거래 또는 전자공간·가상공간에서 컴퓨터 통신망을 이용하여 팩스, EDI, EFT 등 전자적 방식에 의해서 이루어지는 상거래를 말한다(Tayer, EDI FORUM, Vol.8, No.1, p.12: 공업 및 에너지기술 기반조성에 관한 법률 제2조 제5호 NIST(National Institute of Standards and Technology), Trust and Traceability in Electronic Commerce(http://niinist.gov/pubs/trust-1.html).

11) FIRST: 1988년 미국에서 조직되어 2년 후에 국제협의체로 발전하여 1999년 현재 북미 48, 유럽 26, 아태 4 등 78개 기관이 회원으로 가입되어 있으며 한국정보보호센터도 1998년 가입하여 공동 대처하고 있다. 사이버 침해 사고와 파괴 문제를 해결할 수 있는 능력을 갖춘 기관이 회원으로 동참함으로써 국가와 기관간에 공동으로 사이버 침해 문제를 해결한다는 기능을 가지고 있다.

의회 사이버범죄조약에 가입함으로써 사이버 범죄에 대응하는 실효성을 높여 나가야 한다.

V. 결론

이상에서 21세기 정보화 사회에 있어서 가장 심각한 문제로 등장하고 있는 사이버 테러리즘에 대한 기본적인 논의와 함께 기존의 사이버 테러에 관한 몇 가지 대응방안을 살펴보았다. 정보보호의 필요성은 시간의 흐름, 기술 발전, 사회 변화에 따라 변화하고 있다. 국가기간전산망 구축 사업 초기인 1990년대만 하더라도 정보보호나 사이버 테러와 같은 정보화의 역기능은 그다지 큰 비중을 차지하지 못했으나 우리나라는 물론 세계의 모든 컴퓨터가 네트워크로 연결되고, 최근 잇따른 웜·바이러스 감염과 해킹을 겪으면서 사이버 공간의 정보보호는 국가안위와도 연결될 수 있는 상황이 전개되고 있다. 따라서 사이버 공간에 대한 보안체계 확립이 그 어느 때보다 중요성이 높아지고 있는 상황에서 사이버 테러에 대하여 공통적으로 추구하는 것이 있다면 변화하는 현실에 맞는 법을 제정하고, 사이버 테러에 대응할 통합 상설기구를 설치하여 전문적 기술방안 마련과 전산망 운영시스템의 보완, 그리고 전문 인력의 양성과 국제공조의 강화로 요약된다.

우리나라는 앞으로 정보화 사회가 진행됨에 따라 현재까지 발생한 사이버 테러보다 훨씬 강력한 피해를 안겨줄 사건들이 재발할 것이 예상되므로 국가기간전산망을 포함한 모든 정보통신 기반시설에 대해 기관간의 정보교류 및 공동대응을 위한 구심적 역할을 수행할 상설집행기구가 시급히 마련되어야 할 것이며, 국제적으로 발생하는 사이버 테러에 대응하기 위한 관련 국가간의 교류 및 정보공유가 수반되어야 하며, 국제 공조 수사가 현실에 맞게 이루어져야 할 것이다.

<참고문헌>

▷ 강동범. 2000. 사이버범죄와 형사법적 대책. 한국형사정책연구원 제25회 형사정책세미나.

▷ 경찰청. 2004. 경찰백서. 서울: 경찰청.

▷ 경찰청사이버테러대응센터. http://ctrc.go.kr.

▷ 국가보안기술연구소. http://www.nsri.re.kr.

▷ 국가사이버안전센터. http://www.ncsc.go.kr.

▷ 국가사이버안전센터. 2004. 2003 사이버침해사고 사례분석집. 서울: 국가정보원.

▷ 국가정보원. 2004. 국가정보보호백서. 서울: 국가정보원.

▷ 국가정보원. 2004. 테러, 이것만은 꼭 알아둡시다. 서울: 국가정보원.

▷ 국가정보원. 2004. 국가사이버 안전메뉴얼. 서울: 국가정보원.

▷ 국방정보전대응센터. http://www.dsc.mil.kr.

▷ 김문일. 1989. 컴퓨터 범죄론. 서울: 법영사.

▷ 김홍근. 1999. 컴퓨터 시큐리티. 한국정보보호센터.

▷ 남길현. 1999. 해킹 피해 및 대책. 정보화역기능방지대책공청회.

▷ 노연후. 1992. 컴퓨터 범죄. 하이테크정보 1992.

▷ 대검찰청인터넷범죄수사센터. http://icic.sppo.go.kr.

▷ 박종국. 1998. 정보화의 세계적 추세와 우리의 대응방안. 세계경제연구원.

▷ 백영철. 21세기 신종테러양상과 월드컵 대테러 방안. 대테러연구 24.

▷ 신각철·김문일. 1997. 최신 컴퓨터 범죄론. 서울: 법영사.

▷ 신의기. 1996. 유엔의 국제조직범죄 규제방안. 서울: 형사정책연구원.

▷ 이민식. 2000. 사이버공간에서의 범죄피해. 한국형사정책연구원.

▷ 이황우. 2000. 사이버테러의 실태와 대응방안. 대테러연구 23. 경찰청.

▷ 인터넷침해사고대응지원센터. http://www.krcert.or.kr.

▷ 임채호. 1997. 신종해킹기법 출현 현황 및 대책. 제3회 정보보호심포지움SIS'98. 정책연구원.

▷ 장석헌 외. 1999. 사이버테러리즘의 본질과 전망. 한국공안행정학회보.

▷ 정동섭. 2001. 한국컴퓨터범죄수사의 실태와 방향. 한국형사정책연구원.

▷ 조규정. 1994. 컴퓨터 범죄. 법무부 법무실 법무자료 제56집.

▷ 조병인. 2000. 사이버 경찰에 관한연구. 한국형사정책연구원.

▷ 최영호. 1995. 컴퓨터와 범죄현상. 서울: 컴퓨터출판사.

▷ 한국정보보호센터. 2002정보시스템 해킹·바이러스 현황 및 대응. 서울: 한국정보보호센터.

▷ 한국정보보호진흥원. http://www.kisa.or.kr.

▷ Caelli, William, Dennis Longley and Michael Shain. 1991. *Information Security Handbook*. New York: Stockton Press.

▷ Hoffman, David. 2000. Russian Tourts Computer Virus as Weapon. *World in Brief*, May 9, 2000.

▷ Koob, Gary M. 1999. Internet Information Survivability. DAPRATech '99, Jun.

▷ Tapscott, Don. 1998. *Growing up Digital-The Rise of the Net Generation*. McGraw-Hill.

▷ UN. ACCIS. 1993. *Information System Security Guidelines for the Unitd Nations Organizations*. New York.

趙皓昊: 2002년 동국대학교에서 경찰학 박사학위를 취득하고(논문: 재난관리상 경찰의 역할에 관한 연구), 대불대학교 경찰행정학과 교수로 재직하였고, 현재 순천향대학교 경찰행정학과 교수로 재직중이다. 주요 관심분야는 위기관리, 경찰운용, 경찰인사 등이다. 주요저서로는 경찰부패방지 가이드(2006)이며, 주요논문으로는 우리나라 해양경찰의 교육훈련 개선방안에 관한 연구(2003), 한국 경찰의 범죄피해자보호에 관한 연구(2004), 학교폭력에 대한 경찰역할 강화방안(2005), 한국 경찰의 수사전문화 방안(2006) 등이 있다.(jhd30@hanmail.net)