사이버 테러리즘 현황과 정책적 대응

조호대
순천향대학교 소프트웨어학과

우리나라는 UN의 전문기구인 ITU(국제전기통신연합)의 디지털기회지수 평가에서 2년 연속 1위를 차지하였고, IMD(국제경영개발대학원)에서 발표하는 2006년도 국가경쟁력지수 중 정보통신부문이 포함된 기술 인프라 부문에서 6위를 차지할 만큼 인터넷 강국으로 주목을 받고 있을 만큼 정치·경제·사회·의학 등 국민생활의 전 분야에서 컴퓨터와 인터넷을 통한 업무 활동이 일반화되어 있다. 이러한 정보접근의 용이성, 수많은 동시 이용자, 정보의 빠른 흐름 등과 같은 인터넷의 장점들이 점차 역기능으로 작용하여 개인적인 피해가 심각한 수준으로 증가할 뿐만 아니라 산업기밀과 국가기밀의 유출 가능성도 높아지게 되고 정보통신 인프라의 위협이 주요기반시설의 위협으로까지 확장되고 있어 국가의 안보적인 측면에서의 위험이 증가하고 있다. 또한 컴퓨터와 인터넷 발전의 역기능은 목적 달성을 위해 테러를 자행하는 집단이나 개인에게도 적용되어 테러리스트들에게 테러의 가능성을 높여주었다. 본 연구에서는 사이버테러리즘에 대한 유형과 발생현황을 살펴봄으로써 문제점을 도출하고 그에 따른 정책적 대응방안을 제시하였다.

주제어: 테러리즘, 사이버테러리즘, 국가기반시설, 사이버 안전, 정보 네트워크

Ⅰ. 서론

1970년대 초반 컴퓨터 통신이 시작되었음에도 불구하고 컴퓨터와 정보통신기술의 획기적인 발전은 비교적 짧은 시간에 초고속 인터넷의 확산을 가져와 1980년대 중반이후 인터넷을 사용하고 있는 모든 사람들이 시간적·공간적인 한계를 뛰어 넘어 전 세계의 광대한 정보를 인터넷이 연결되어 있는 곳에서는 언제 어디서나 획득할 수 있게 하였다[1].

우리나라 역시 정치, 경제 사회, 의학 등 국민생활의 전 분야에서 컴퓨터와 인터넷을 통한 업무 활동이 일반화되어 가고 있을 뿐만 아니라, UN의 전문기구인 국제전기통신연합(ITU)의 디지털기회지수(DOI)평가에서 2년 연속 1위를 차지하고, 국제경영개발대학원(IMD)에서 발표하는 2006년도 국가경쟁력 지수 중 정보통신부문이 포함된 기술 인프라 부문에서 6위를 차지 할 만큼 인터넷 강국으로 전 세계의 주목을 받고 있다.

하지만 정보 접근의 용이성, 수 많은 이용자, 정보의 빠른 흐름 등과 같은 인터넷의 장점들이 정보화 사회 선진화에 따라 역기능으로 작용하여 악성댓글, 스팸메일, 개인정보 유출, 금융적 이익을 목적으로 하는 피싱(Phishing)·파밍(Pharming)에 따른 개인적인 피해가 증가하고 있으며 불건전 정보유통, 개인 사생활 침해와 같은 부작용 등이 점차 심각한 사회문제로 대두되고 있다. 또한 네트워크의 확대보급에 따른 정보교환 및 공유로 인하여 정보의 불법적인 접근이 가능하고 이에 따라 산

1) 유비쿼터스(Ubiquitous)는 '언제 어디서나 존재한다'는 라틴어에서 유래한 의미로써, 유비쿼터스 컴퓨팅 환경(Ubiquitous Computing Enviornment)은 언제 어디서나 컴퓨터를 사용할 수 있는 환경을 의미하고 이는 차세대 정보화 사회에서 핵심적인 IT기술의 패러다임이다(조광래, 2005: 238).

업기밀과 국가기밀의 유출 가능성도 높아지고 있고, 국가중요기반시설이 점차 정보 네트워크에 의해 관리·통제됨에 따라 정보통신 인프라의 위협이 주요기반시설의 위협으로까지 확장되고 있어 국가의 안보적인 측면에서 위험이 되고 있다(국가정보원, 2007: 3-4).

컴퓨터와 인터넷의 발전의 역기능은 목적 달성을 위해 테러를 자행하는 집단이나 개인에게도 적용되어 폭탄을 가득 실은 화물트럭이나, 플라스틱 폭탄과 같은 물리적 공격 방법에서 컴퓨터와 인터넷을 사용하여 가상공간을 통해 공격하는 것으로 공격실행수단이 컴퓨터와 인터넷으로 바뀐 것이지 테러조직이나 테러리스트들의 목적은 전통적인 테러리즘과 변함이 없다.

사이버 테러리즘은 새로운 유형의 테러리즘으로 컴퓨터 기술의 습득과 조직적인 네트워크의 구축만으로 테러조직이나 테러리스트들의 목적 달성을 위한 공격행동에 있어서 테러리스트에게는 신체적 위험성을 확연히 줄여주고, 사이버 공간에 대한 공격만으로 국가중요산업 및 국방 분야를 마비시키고 그에 따른 일반 시민들의 정신적·신체적 파괴와 공포감을 조성할 수 있다는 점에서 테러리스트들에게 테러의 가능성을 높여주었다.

수백개의 인터넷 웹사이트에서 찾아볼 수 있듯이 오늘날 모든 테러조직은 그들만의 인터넷 기반을 구축하고 있고, 사이버 테러리즘에 대한 높은 기술을 보유하고 있기 때문에 정보기술의 발달에 따라 급격히 변화하는 사이버 테러리즘에 대한 대비는 매우 중요하다.

본 논문에서는 사이버 테러리즘에 대한 정의와 범위에 대하여 알아보고 우리나라의 사이버 테러리즘에 현황을 살펴봄으로써 사이버 테러리즘에 대한 정책적 제언을 제시하고자 한다.

II. 사이버 테러리즘의 개념적 접근

1. 사이버 테러리즘의 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, 국가 내 부처마다 정의가 서로 다른 경우도 있다. 우리나라의 대테러업무를 주관하는 국가정보원은 "정치적·사회적 목적을 가진 개인이나 집단이 그 목적을 달성하거나 상징적 효과를 얻기 위해서 계획적으로 행하는 불법적 폭력행위"(http://www.nis.go.kr)라고 테러리즘을 정의하고 있다[2].

이와 달리 사이버 테러리즘은 최근에 나타난 개념으로 "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 주요사회기반시설 내지 정보통신기반시설에 대한 테러행위로 국한시키는 견해"(국가사이버안전센터, 2004: 74), "해킹, 바이러스 등 정보통신망 자체에 대한 공격행위로서 국가 또는 사회적 혼란 또는 불안을 야기하는 행위"(양근원, 2004: 183) 등과 같이 다양하게 정의되어지나, 사이버 테러리즘이라는 용어 자체는 우리나라 법령에 사용된 예가 없으며, 국가대테러활동지침 제2조 제1호에서 「컴퓨터 통신망을 이용한 정보조작 및 전산망 파괴」를 테러리즘 유형의 하나로 규정하고 있을 뿐이다.

따라서 본 논문에서는 전자상거래 사기, 프로그램의 불법목제, 불법사이트 운영, 개인정보침해 등과 같은 개인적인 이익 취득과 목적 달성을 위한 일반 사이버 범죄보다는 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 정보통신망 자체에 대한 공격행위를 통해 이루어지는 정치, 종교, 사회, 민족적 목적 달성과 이를 위한 이득을 얻기 위해 사이버 공간을 범죄의 수단으로

---

2) 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 항공기납치, 용인암살, 공중시설 폭파 등을 통해 사람들에게 공포를 일으키게 하는 행위를 의미하는 것이다(이진수, 2000 : 8). 따라서 엄밀히 말하자면 테러와 테러리즘은 다른 개념으로 생각할 수 있다.

삼는 것을 사이버 테러리즘이라고 정의하고 겉으로 드러난 행위 자체뿐만 아니라 공격 행동으로 인해 얻어지는 이익의 효과로 그 범위를 한정한다.

2. 사이버 테러리즘의 특징

사이버테러는 전 세계에 그물망처럼 연계된 인터넷망을 통해 빛의 속도로 전개되며 소요시간도 그 동안에 있었던 일반적인 테러와는 달리 수분이내에 끝나면서도 피해규모에 있어서는 일반의 상상의 초월하고 심지어는 국가의 안보에 심각한 위협으로 나타날 수 있다. 따라서 사이버테러는 그동안 우리 인류에 커다란 위협이 되어왔던 일반적인 테러와는 그 본질을 달리하는 것으로 볼 수 있는데 통상의 테러와는 다른 사이버테러의 특징을 살펴보면 다음과 같은 점을 들 수 있다(이진수, 2000: 34).

1) 광역성 및 다양성

일반적으로 사이버테러는 테러리스트가 목표로 정한 공격지점에 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 사이버공간에 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 사이버테러를 대비하기 위해서는 과거처럼 경찰이나 군 등이 책임지역이나 건물을 가지고 독자적으로 업무를 수행할 수 있는 것이 아니고 네트워크에 연계된 각 기관들이 공동으로 상호 유기적인 협조체제를 구축하지 않고서는 적절한 대비가 어렵기 때문에 미래 인류사회의 최대의 위협이 될 사이버테러는 국제적인 협력관계 구축은 물론 관련기관간의 유기적인 협조체제 구축이 필요하다(이진수, 2000: 34).

2) 최소의 인원으로 최대의 피해 가능성

컴퓨터 네트워크를 이용하여 적의 정보통신망에 침투하기 위한 최소한의 기술자만 있으면 사이버테러리즘은 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 타격대상이 되는 정보통신 시스템을 파괴·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 사이버테러리즘을 그리 선호하지 않을 것이라는 의견도 있다(Arquilla & 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 디지털증거에 법적 증거능력을 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 위한 증거자료를 확보하는 것에 특별한 방법과 절차를 요구하고 있다. 범죄의 혐의가 있을 때 범죄사실과 증거를 수사하여야 하는 것은 컴퓨터 관련 범죄에서도 다른 범죄와 마찬가지이나 컴퓨터와 관련된 증거를 수집함에 있

3) 컴퓨터 포렌식스(Computer Forensics)는 컴퓨터 등과 같은 정보처리기기에서 수집할 수 있는 디지털 자료가 법적증거능력을 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 증거능력을 갖게 하기 위한 절차로서의 의미는 'Digital Forensics'가 좀더 광범위하고 정확한 의미가 될 수 있으나 'Computer Forensics'가 초기에서 사용되어 왔고, 그 의미 또한 크게 벗어나지 않으므로 아직까지 통용되고 있는 실정이다.

어서는 데이터나 프로그램 그 자체로는 유기물이 아니기 때문에 형사소송법상 압수수색 대상 여부 진위와 같은 전통적 증거수집과 다른 절차상의 새로운 문제가 야기된다. 또한 사이버범죄의 주요유형중 하나인 해킹 기술이 발전할수록 보안기술도 함께 발전해 왔다고 할 수 있지만, 알려지지 않은 행위나 새로운 공격기법을 방어하기에는 역부족이고 해킹을 당한 대부분의 시스템 관리자들은 자신이 해킹을 당했는지조차 알지 못하며, 체계적인 대응방안을 세우는 데에도 익숙하지 못해 피해복구에 대한 전문적인 기술개발이나 체계적인 연구가 진행되지 못하고 있다(수사연구, 2004: 17).

3. 사이버 테러리즘의 유형

사이버 테러리즘에 대한 유형은 사이버 테러리즘을 발생시키는 주체에 의해 분류하는 방법, 사이버 테러리즘의 대상에 따라 분류하는 방법, 사이버 테러리즘에 이용되는 기술 및 방법에 따라 분류하는 방법과 같이 다양하게 적용된다.

1) 주체와 대상에 따른 유형

<표 1>에서 보듯이 사이버테러는 주체에 따라 개인적 침해, 조직적 침해, 국가적 침해로 구분할 수 있으며, 이에 따라 목적, 대상, 공격방법에 차이가 있다.

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

<표 1> 사이버 테러리즘 주체와 대상에 따른 분류

구 분	개인적 침해 위협	조직적 침해 위협	국가적 침해위협
주 체	해커 컴퓨터 범죄자	산업스파이 테러리스트 조직화된 범죄 집단	국가 정보기관 사이버전 전사
목 적	금전획득 영웅심 발휘 명성획득	범죄조직의 이익달성 정치적 목적달성 사회·경제적 혼란야기	국가기능 마비 국가방위능력 마비
대 상	민간사설망 공중통신망 개인용 컴퓨터	기업망 금융, 항공, 교통 등 정보통신망	국방, 외교, 공안망 등
공격 방법	컴퓨터 바이러스 해킹 메일폭탄 홈페이지 변조 패스워드 유출 개인 신분위장 트로이목마 등 서비스 거부공격	개인적 공격방어 포함 유·무선 도청 정보통신망 스니퍼 통신망 교환 시스템 동작마비 공격	개인·조직적 공격 포함 첨단도청 및 암호해독 전자공격무기 고에너지 전파무기 전자기파 폭탄 등 기타, Chipping/초미세형 로봇/전자적미생물

자료: 국가정보원(2004: 15).

해킹 (Hacking)은 일반적으로 다른 사람의 컴퓨터 시스템에 무단 침입하여 정보를 빼내거나 프로그램을 파괴하는 전자적 침해행위를 의미하는 것으로 사용하는 기술과 방법 및 침해의 정도에 따라 단순침입, 사용자도용, 파일 등 삭제변경, 자료유출, 폭탄스팸메일, 서비스거부공격으로 구분하고 있다.

바이러스(악성프로그램)는 일반적으로 컴퓨터 바이러스 또는 인터넷 웜을 의미하며 '정보시스템의 정상적인 작동을 방해하기 위하여 고의로 제작 유포되는 모든 실행 가능한 컴퓨터 프로그램'을 의미하는 것으로 보통 자기복제능력 등 각자의 특징에 따라 컴퓨터 바이러스, 인터넷웜, 트로이목마 등으로 구분하고 있으며, 법에서는 '정보통신시스템, 데이터 또는 프로그램 등을 훼손, 멸실, 변경, 위조 또는 그 운용을 방해할 수 있는 프로그램'을 악성프로그램으로 규정하고 이를 유포하는 행위 처벌하고 있다(http://www.ncsc.go.kr).

2) 사이버 공격 유형

<표 2>는 국가사이버안전센터가 2004년 7월부터 사이버 공격 및 피해유형을 최근의 사고 유형에 맞추어 새로운 기준으로 재분류한 것으로 사이버 공격 유형 기준은 웜, 바이러스, 스캐닝, 취약점 이용, 기타로 분류하였다.

<표 2> 사이버 공격 유형 기준에 따른 분류

대 분 류	내 용	유형 예시
웜.바이러스	대상 시스템에 침투하여 악성코드를 삽입하고시스템파괴와 확산을 시도하는 공격	웜.바이러스, 트로이목마 AD-ware , spyware등
스캐닝	해킹하기 전 대상 네트워크나 시스템의 취약점을 수집하기 위한 작업. DoS 공격	각종 포트 스캐닝, DoS

취약점 이용	S/W 오류. 설정상 오류, 프로그램 취약점 등을 악용한 공격이나 취약점을 이용한 권한 획득	Buffer Cverflcw, ActiveX 및 Java 악성코드, SQL 주입, 권한설정 취약. 보안설정 오류등
기타	시스템 피해가 목적이 아닌 시위나 사기 ,명예훼손 등을 위한 공격이나 위 항목에 정의되지 않는 유형과 공격시도가 없는 상태	홈페이지 접속장애, 사이버 시위, 쇼핑몰 사기, 물리적 보안 취약, 사회공학 등

자료: 국가사이버안전센터(2004: 18).

3) 사이버 피해 유형

사이버 피해 유형 기준은 경유지 이용, 웜 및 바이러스 피해, 홈페이지 변조, 자료훼손 및 유출, 단순침입 시도, 기타로 분류하였다.

<표 3> 사이버 피해 유형 기준에 따른 분류

대분류	내 용	유형 예시
경유지 이용	해킹 피해를 당한 뒤 다른 사이트를 공격하는 경유지로 활동되는 피해	해킹 경유지, 스팸 릴레이
웜.바이러스 피해	웜.바이러스 감염시도 및 전이	감염시도, 감염 후 전이 시스템 장애, 네트워크 부하 등
홈페이지 변조	취약점 등을 통하여 홈페이지의 메인 페이지가 변조되거나 사용하지 않는 페이지가 삽입되는 피해	홈페이지 변조 삽입, 삭제
자료훼손 및 유출	FTP 서버 및 PC등의 권한이나 공유설정의 취약으로 자료가 변조, 삭제되거나 유출, 열람되는 피해	자료삭제, 자료유출, 자료변조, 자료열람, 백도어, 루트킷
단순침입 시도	스캐닝 기법 등으로 시스템이나 네트워크의 취약점 점검 및 계정추측 등의 침입시도만 이루어진 피해	패스워드 추측시도, 침투시도,스캐닝
기 타	시스템이나 네트워크의 피해나 침입시도 없이 사이버 시위나 단순사기, 명예훼손 등의 사건이나 위 항목에 정의 되지 않는 피해유형	

자료: 국가사이버안전센터(2004: 19).

III. 사이버 테러리즘 현황

1. 사이버 범죄 현황 및 검거현황

<그림 1>에서 볼 수 있듯이 경찰청 사이버테러대응센터는 사이버 범죄를 사이버테러형 범죄와 일반 사이버 범죄로 분류하고 있고, 이 중 사이버테러형범죄가 본 논문에서 사이버테러리즘의 범위를 정한 것과 유사하다. 사이버테러리즘은 2001년에 10,638건이었으나 매년 증가하여 2007년에는 20,186건으로 증가하였음을 알 수 있다.

자료: 경찰청 사이버테러대응센터.

<그림 1> 최근 6년간 사이버테러리즘 발생 현황

자료: 경찰청 사이버테러대응센터.

<그림 2> 최근 6년간 사이버테러리즘 검거 현황

또한 위의 <그림 2>를 보면 사이버테러리즘 검거 현황은 발생 현황에 비해 비교적 낮다는 것을 알 수 있으며, 이는 사이버테러리즘의 수법이 갈수록 치밀하고 다양화 된다는 것을 말한다.

2. 최근 사이버 테러리즘 발생 현황

<표 4>와 <표 5>에서 나타나듯이 2005년에 비해 2006년도에 공공부문의 사이버 테러리즘 발생은 비슷하게 나타났으나 민간부문의 발생은 줄어들었다.

유형별 현황 역시 전체적으로 발생건수는 줄어들고 있는 실정으로 그동안 정보보안에 관한 법률 보완과 기술적인 측면에서의 발전이 도움이된 것으로 보인다. 하지만 2008년 들어서면서부터 조금씩 증가하는 추세를 보일 뿐만 아니라 피해가 큰 사이버테러리즘의 유형을 보인다는 특징이 있다.

<표 4> 최근 2년간 사이버 테러리즘 발생 현황

분 야	구 분	2005년	2006년
공 공	악성코드	2,504	2,548
	해 킹	2,045	1,738
	소 계	4,549	4,286
민 간	악성코드	16,093	7,789
	해 킹	33,633	26,808
	소 계	49,726	34,597
합 계		54,275	38,883

자료: 국가사이버안전센터(2006: 2).

<표 5> 최근 4년간 사이버 테러리즘 유형별 현황

구 분	2005년	2006년	2007년	2008년 03월
웜·바이러스	16,093	7,789	5,996	2,412
해킹신고처리	33,633	26,808	21,732	4,228
-스팸릴레이	6,334	14,055	11,668	1,719
-피싱경유지	1,087	1,266	1,095	315
-단순침입시도	-	3,711	4,316	1,025
-기타해킹	9,520	4,570	2,360	700
-홈페이지변조	16,692	3,206	2,293	469
악성 봇(Bot)	18.8%	12.5%	11.3%	11.1%

* 본 통계는 전세계 Bot 감염 추정 PC 중 국내 PC가 차지하는 비율임[4)]

자료: http://www.krcert.or.kr.

3. 공공분야 사이버 테러리즘 현황

<표 6>을 보면 2006년 발생한 공공분야 사이버 테러리즘 발생 건수는 지방자치단체가 1,470 건으로 가장 많았고 교육기관이 1,464건으로 두 번째로 많았으나 자료훼손 및 유출에 있어서는 국가기관이 많아 상대적으로 취약점을 노출하였다.

<표 6> 2006년 공공분야 사이버 침해사고 발생 현황

유형 / 기관	악성코드 감염	경유지 악용	홈페이지 변조	자료훼손 및 유출	기 타	합 계
국가기관	316	59	16	49	16	456
지자체	1,233	162	38	21	16	1,470
연구소	110	125	5	17	3	260
교육기관	489	821	145	7	2	1,464
산하기관	396	146	49	23	6	620
기 타	4	3	0	6	3	16
합 계	2,548	1,316	253	123	46	4,286

자료: 국가사이버안전센터(2006: 2).

4) 악성 봇(Bot) : 운영체제 취약점, 비밀번호의 취약성, 웜·바이러스의 백도어 등을 이용하여 전파되며, 해킹명령 전달 사이트와의 백도어 연결 등을 통하여 스팸메일 전송이나 DDoS 공격에 악용이 가능한 프로그램 또는 실행코드를 말함.

또한 <표 7> 사고유형별 발생건수는 악성코드 감염과 경유지 악용의 건수가 상대적으로 늘어나 향후 보완점을 찾아야 할 필요가 있다.

<표 7> 사고유형별 침해사고 발생 현황(공공분야)

구분	2005년	2006년
악성코드 감염	55%	60%
경유지악용	26%	31%
홈페이지 변조	15%	6%
자료훼손유출	3%	3%
기타	1%	1%

자료: 국가사이버안전센터(2006: 2).

<표 8> 시관별 사이버 침해사고 발생건수는 교육기관의 경우 2005년에 비해 다소 낮아 졌으나 국가기관과 지방자치단체의 경우 증가하는 현상을 보여 빠르게 진화하는 사이버 테러리즘에 적절하게 대응하지 못하고 있다.

<표 8> 기관별 침해사고 발생 현황(공공분야)

구분	2005년	2006년
교육기관	56%	34%
국가기관	7%	11%
지자체	17%	34%
산하기관	15%	14%
연구기관	4%	6%
기타	1%	1%

자료: 국가사이버안전센터(2006: 2).

4. 민간분야 사이버 테러리즘 현황

<표 9>에서 나타나듯이 민간분야 사이버 침해 발생 건수는 스팸 릴레이, 일반 해킹, 웜·바이러스 감염, 피싱 경유지, 홈페이지 변조의 순으로 나타나 민간분야의 취약성을 나타냈다.

<표 9> 2006년도 민간분야 침해사고 발생 현황

해 킹				웜·바이러스 감염	합 계
피싱 경유지	스팸 릴레이	홈페이지 변조	일반 해킹		
1,266	14,005	3,206	8,281	7,789	34,597

자료: 국가사이버안전센터(2006: 2).

<표 10>은 최근 3년간 해킹사고 발생 현황으로 2005년에 비해 2006년에는 21%가 감소 한 것으로 나타났으

나, 발생건수 대비 피해 규모는 큰 것으로 조사되었다.

<표 10> 최근 3년간 해킹사고 발생 현황(민간분야)

연 도	2004년	2005년	2006년
침해 사고	24,297	33,633	26,808
증가율(%)	-7%	+38%	-21%

자료: 국가사이버안전센터(2006: 2).

<표 11>은 2006년도 민간분야 사고유형별 발생 현황으로 스팸릴레이와 일반해킹, 웜·바이러스의 순으로 높은 비율을 나타내었다.

<표 11> 2006년도 사고유형별 발생 현황(민간분야)

사고 유형	스팸 릴레이	일반 해킹	웜· 바이러스	홈페이지 변조	피싱 경유지
발생 현황	40%	24%	23%	9%	4%

자료: 국가사이버안전센터(2006: 2).

<표 12>는 2006년도 민간분야 기관별 발생 현황으로 개인이 78.3%로 거의 대부분을 차지하고 있으며, 기업(13.8%), 대학(4.1%)의 순으로 나타났다.

<표 12> 2006년 기관별 발생 현황(민간분야)

기 관	개인(기타)	기업	대학	비영리	네트워크
발생현황	78.3%	13.8%	4.1%	2.7%	1.1%

자료: 국가사이버안전센터(2006: 2).

IV. 사이버 테러리즘에 대한 문제점 및 정책적 대응방안

1. 법제도 정비

지금까지는 각 기관간 역할이나 국가 차원의 대응체계를 고려하지 않고 소관부처 중심으로 업무수행이 이루어져 정보공유와 업무협조에 있어서도 소극적일 수 밖에 없었고, 사이버 테러리즘으로 인한 침해 사고와 관련한 민간기업의 정보제공, 정보보호안전진단 등 침해사고 최소화방안이 미흡하였다(양근원, 2004: 19).

이러한 문제점들을 개선하고 실질적인 대응업무를 마련하고 정착시키기 위해서는 관련 법제도의 개선이 필요하지만 보안관련 규정의 제정 및 개정은 매우 어려운 것이 현실이다. 정보보호 및 사이버 테러리즘 발생 시 그 피해가 막대하고 복구가 어렵다는 것을 인식하면서도 여러 공공기관 및 비정부민간기구의 반대와 같은 주변 여건으로 말미암아 상당한 진전을 보이고 있는 기술적인 측면을 법제도에서 뒷받침해주고 있지 못하다.

최근의 상황을 최대한 반영하고 법적 안정성과 예측가능성, 체계성을 갖춘 사이버 테러리즘을 포함하는 대테러방지법을 조속한 시일 내에 제정하여 국가안보와 국민의 안전에 위협이 될 수 있는 요소들을 예방하고 제거해야 한다.

2. 사이버 테러리즘 대응 조직 구축

사이버 테러리즘에 대한 범 국가적 차원에서의 대응태세 확립을 위해 국가안전보장회의(NSC)를 중심으로 '국가사이버안전센터'는 국가·공공분야, '국방정보전대응센터'는 국방분야, '인터넷침해사고대응지원센터'는 민간분야, '국가보안기술연구소'는 교육분야, '정보공유분석센터'는 통신·금융분야, '사이버범죄 수사기구'는 사이버 범죄행위에 대한 수사 활동의 대응업무를 각각 지원하면서 사이버 테러리즘 정보 분석을 통한 경보를 발령하고 상호간에 전파하고 있다. 그러나 핵심적인 조정역할을 담당하고 있는 국가안전보장회의 내에는 정보보안 문제를 통괄하고 조정할 수 있는 전문가 그룹이 부족한 것이 현실이고, 각 기관별 대응센터 간 정보공유 및 협조체제 역시 미미할 뿐만 아니라 실무 주도기관이 부재한 실정이다(조광래, 2005: 255).

이를 극복하기 위해 유사시 신속하고 피해를 최소화할 수 있도록 하여야 하며, 평상시에는 사이버 테러리즘에 대한 정보 수집과 예방, 네트워크 안전성과 보안기술 등에 대한 연구개발에 힘쓰는 각종 공공부문 정보공유센터와 민간부문의 컴퓨터 침해사고 대응팀까지 아우르는 실무 주도기관이 법적인 근거를 바탕으로 정비되어야 한다.

3. 전문 인력의 양성 및 확충

사이버 테러리즘에 대응하기 위한 인력은 사이버공간이라고 하는 상황 하에서 특수한 기술적이고 전문적인 지식을 갖추어야 할 뿐만 아니라 사이버범죄와 테러리즘이라고 하는 보안 분야에서의 전문적인 이해도 갖추어야

한다.

각 기관별 대응센터 및 사이버범죄 수사기관의 전문 인력은 공공분야와 국방분야, 민간분야 할 것 없이 모두 절대적으로 부족한 실정이다. 따라서 국가기간전산망을 사이버 테러리즘과 같은 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 전문성을 갖춘 인력을 신규채용하고, 지속적인 전문 교육훈련을 통해 빠른 기술적인 변화를 보충하도록 하여야 하며, 시스템을 운영하는 직원의 전문성을 최대한 보장해주고 보수 등에 있어서도 인센티브를 제공하는 것이 필요하다.

4. 국제적 정보교류 및 공조체제 구축

사이버공간은 국경이 없는 공간이고, 사이버 테러리즘은 초고속 인터넷을 통해 짧은 시간에 이루어 질 수 있기 때문에 외국에서 발생하는 바이러스와 해킹 등이 일순간에 전 세계로 유포되어 국가안보에 커다란 위협요소로 작용하고 있다. 통상 국가간의 형사사법 공조관계는 외교통상부를 경유하여 상대 국가의 법집행기관의 형사사법업무의 공조를 요구하는 것이나 이런 경우 너무 많은 시간이 소요되어 소기의 목적을 달성하기 어렵다는 점을 감안하며 국제협력분야에 있어서 인터폴 사이버범죄관련 기구 및 국제컴퓨터침해사고대응협의회(FIRST)[5], FBI 컴퓨터 범죄회의・정보보호 전문가 그룹 등과의 지속적인 협조체제와 인적교류를 강화하는 것이 무엇보다 중요하다(오태곤, 2005: 100). 특히 지난 1991년 제정된 국제형사사법공조법이 시간을 다투는 사이버테러와 같은 범죄현실에 전혀 맞지 않는 상황이므로 유럽의회 사이버범죄조약에 가입함으로써 사이버범죄에 대응하는 실효성을 높여 나가야 한다.

5. 공공과 민간부문의 공동협력 강화

최근의 해킹, 바이러스 관련 정보통신의 환경적 특징은 소프트웨어 및 네트워크 취약점의 급속한 증가, 해킹의 지능화 및 고도화 그리고 보안 취약점을 이용한 제로데이(Zero-day)공격의 증가, 웜·바이러스의 급속한 확산과 융합·복합화에 따른 피해의 증폭을 들 수 있다.

특히 이러한 사이버 테러리즘은 민간부문 뿐만 아니라 공공부문까지 이어져 커다란 사회적 이슈로 등장하였고, 우리나라는 국방, 건설, 의료, 식품 등 각 분야에서 유비쿼터스 사업을 추진하고 있고, 유비쿼터스 환경에서 대표적으로 사용되는 RFID와 USN 서비스는 소형반도체 칩을 이용해 사물 등의 정보를 무선으로 전송하여 처리하기 때문에 정보흐름 도청, 비정상적인 트래픽 발생, 정보 위·변조, 위장 리더, DoS·DDoS공격, 개인정보의 불법 수집 등의 문제가 발생할 수 있다(국가정보원, 2007: 26).

공공부분에 있어서도 국가안보라는 전통적 개념에 과학기술이 접목됨으로써 사이버테러리즘이 국민생활의 안위와 국가 안보의 중요한 영역으로 대두된 것이다. 사이버 공격이 복합화, 악성화되고 개인 간의 통신채널을 전파경로로 이용하게 되었다는 것은 사이버 공간에 연결된 민간부문의 사회 각 계층 전반이 거의 일시에 공격 대상이 된다는 것을 의미 한다(양근원, 2004: 18).

오늘날 사이버 테러리즘은 공공부문과 민간부문을 구별하지 않고 있으며, 정부만의 단독 대응으로는 한계점을 지니고 있고, 네트워크망을 통하여 취약지점을 통하여 다른 부문으로의 침투가 용이하게 변모해 가고 있으므로 공공부문과 민간부문의 공동협력체제가 구축되어야 한다(오태곤, 2005: 101).

V. 결론

우리나라는 2003년 1월 25일 슬래머(Slammer)와 웜(Warm) 바이러스로 인한 인터넷 마비사고와 2004년 주요 국가기관 해킹사건, 2006년 온라인 게임 사용자에 대한 대규모 명의도용 사건, 2008년 초 옥션사이트에 대한

5) 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 공동대처하고 있다. 사이버침해사고와 파괴문제를 해결할 수 있는 능력을 갖춘 기관이 회원으로 동참함으로써 국가와 기관간에 공동으로 사이버침해 문제를 해결한다는 기능을 가지고 있다.

해킹사건, 인터넷 검색 사이트 다음에 대한 해킹사건, 국내 최대의 증권사 미래에셋에 대한 해킹 사건, 그리고 최근 옥션에 대한 해킹으로 인한 최대의 개인 정보유출로 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.

미국 CIA가 미국 경제연합위원회 보고서에 "정보기술(IT) 혁명은 산업혁명 이후 전 세계적으로 공통된 변화를 이끌어낸 최대한의 혁명"이라고 기술했듯이 정보기술(IT)과 디지털화는 현대사회를 구성하는 필수요소일 뿐만 아니라 개개인에게 하루를 생활하는데 가장 중요한 요인이 되고 있다.

하지만 정보기술의 중요성이 점점 증가하는 만큼 정보기술 시스템을 변형시키고 파괴함으로 인해서 경제와 국방 그리고 국가안위를 침해하려는 테러리스트들의 노력 또한 증가하고 있다.

이들 테러리스트는 컴퓨터와 인터넷 네트워크 자체를 테러를 저지르기 위한 공격의 매개체로 사용하거나, 공격 그 자체로서의 수단 또는 무기로 사용할 뿐만 아니라 우리의 시스템에 대한 취약점을 알아내기 위해 지속적인 연구와 노력으로 사이버 공간을 통한 테러리스트들의 공격은 미래에도 계속 될 것이 예상된다.

따라서 사이버 테러리즘에 대한 정보를 수집하여 실행하기 전 예방에 힘쓰고, 만에 하나 발생 했을 시 그 피해규모가 최소화 할 수 있는 방안을 마련해야 한다.

<참고문헌>

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

▷ 경찰청. 2007. 경찰백서. 서울 : 경찰청.

▷ 국가사이버안전센터. 2007. 2006 사이버침해사고 사례분석집. 서울: 국가정보원.

▷ 국가정보원. 2007. 국가정보보호백서. 서울: 국가정보원.

▷ 국가정보원. 2007. 테러, 이것만은 꼭 알아둡시다. 서울: 국가정보원.

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

▷ 김문일. 1989. 컴퓨터 범죄론. 서울: 법영사.

▷ 김홍근. 1999. 컴퓨터 시큐리티. 한국정보보호센터.

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

▷ 노연후. 1992. 컴퓨터 범죄. 하이테크정보.

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

▷ 백영철. 2002. 21세기 신종테러양상과 월드컵 대테러 방안. 대테러연구. 24.

▷ 신각철 · 김문일. 1997. 최신 컴퓨터 범죄론. 서울: 법영사.

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

▷ 양근원. 2004. 사이버테러의 실태 및 대응방안. 정보통신윤리.

▷ 오태곤. 2005. 사이버 테러리즘의 대응방안에 관한 연구. 한국콘텐츠학회논문지. 5(3): 93-101.

▷ 이민식. 2000. 사이버공간에서의 범죄피해. 한국형사정책연구원.

▷ 이황우. 2000. 사이버테러의 실태와 대응방안. 대테러연구. 23: 93-130.

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

▷ 장석헌외. 1999. 사이버테러리즘의 본질과 전망. 한국경찰회보. 1: 219-242.

▷ 정동섭. 2001. 한국컴퓨터범죄수사의 실태와 방향. 한국형사정책연구원.

▷ 조광래. 2005. 정보환경변화시대의 사이버테러 양상 및 대응체계에 관한 연구. 경호경비연구. 9: 237-260.

▷ 조규정. 1994. 컴퓨터 범죄. 법무자료. 56.

▷ 조병인. 2000. 사이버 경찰에 관한연구. 한국형사정책연구원.

▷ 최영호. 1995. 컴퓨터와 범죄현상. 서울: 컴퓨터출판사.

▷ 한국정보보호센터. 2003. 2002정보시스템 해킹·바이러스 현황 및 대응. 서울: 한국정보보호센터.

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

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

▷ 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.

▷ 경찰청사이버테러대응센터: http://ctrc.go.kr

▷ 국가보안기술연구소: http://www.nsri.re.kr

▷ 국가사이버안전센터: http://www.ncsc.go.kr

▷ 국방정보전대응센터: http://www.dsc.mil.kr

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

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

▷ 한국정보보호진흥원: http://www.kisa.or.kr

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. 주요 저서로는 경찰부패방지 가이드(2006)이며, 주요 논문으로는 "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).