사이버테러의 현황과 대책에 관한 연구

안 창 훈*

◇ 목 차 ◇

Ⅰ. 서 론

컴퓨터를 이용한 정보통신의 발달은 상호간에 정보의 교류를 원활히 함으로서 인류문명의 효율성 향상에 상당한 기여를 하여 왔으며, 정보혁명은 이제 실생활에 깊숙이 영향을 미치고 있다.

세계의 인터넷 사용인구는 1998년 1억600만명에서 1999년 2억7,600만명으로, 2000년에는 4억700만명을 초과하였으며, 최근 발표한 세계 인터넷동향조사 결과에 따르면 2001년 3월말 현재 전세계의 인터넷이용자 수는 4억2,900만명인 것으로 집계됐다.[1)]

한국은 2001년 6월 현재 인터넷 사용자수가 2,223만명에 이르고, 동년 2월 현재 초고속 인터넷도 4가구당 1가구 꼴로 보급되어 있으며[2)], 이러한 보급률은 경제협력개발기구

* 경찰청 사이버테러대응센터.

1) http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=188&page=3&tempfilename=sdataV.html

(OECD)에 이어 국제전기통신연합(ITU)에서도 세계 1위로 인정받았다.

인터넷의 발달 추세를 보면 정보화는 어느 나라를 불구하고 이미 거스를 수 없는 대세이며 따라서 각국 정부가 전자정부의 구현을 통하여 대국민 서비스를 강화하고, 실시간으로 정보를 교류함으로서 경쟁력을 강화하려는 시도를 하여 나름대로의 성과를 거두고 있다. 기업의 차원에서도 정보화를 도외시하고는 기업활동을 할 수 없을 정도에 이르렀으며, 각 개인들도 이제는 편지보다 e-Mail을 이용하는 것이 더욱 효율적임을 실감하고 있어 다양한 방법으로 정보화의 편리함을 만끽하고 있다. 그러나 정보혁명의 혜택만 있는 것은 아니며 역기능 역시 만만치 않다.

정보시대에 해킹 및 바이러스 등 원활한 정보의 유통을 방해하는 다양한 시도가 나타나고 있으며, 이 중 가장 광범위하고 포괄적인 역기능 중의 하나가 바로 Cyber terror이다. 정보통신부 산하 한국정보보호센터는 '해킹바이러스상담지원센터'에 신고된 국내 해킹 피해건수가 97년 64건, 98년 158건, 99년 572건, 2000년 1,943건으로 해마다 3배 가까이 증가하고 있다고 밝히고 있다. 2001년에는 8월까지만 해도 3,779건으로 확인되어 2000년 1년 동안의 두배가 되는 것으로 집계됐다.[3)]

정보혁명의 선진국인 영국의 산업연맹(CBI : Confederation of British Industry)이 조사한 바에 의하면 조사대상 기업 중 2/3가 지난해 해킹, 바이러스 공격, 신용카드 사기 등 '심각한 사건'을 경험한 것으로 나타났다.[4)]

전산화된 다양한 정보가 국제관계는 물론이고 국가 및 기업과 국민생활에서 차지하는 비중이 커질수록 이러한 정보의 효율성에 대한 결정적 저해요소인 사이버테러의 실태파악과 대책 수립의 중요성이 크다고 할 수 있으며, 이러한 사이버범죄 및 사이버테러로부터 국가기반구조를 보호함으로서 국가의 안위가 위협받거나 기업 및 국민생활에 지장을 초래할 우려를 불식시키는 것이 정보혁명의 새로운 과제로 등장하였다. 따라서 우리 정부는 2000년 초 박태준 국무총리를 위원장으로 한 '사이버테러 방지대책 장관회의'를 구성하여 해킹 및 바이러스 등에 적극 대처하기로 하고[5)] 부처별로 나름대로 대책을 추진하고 있으나 각 기업 및 개개인도 실질적이고 구체적인 대응책을 수립하고 효율적으로 대처할 수 있어야 할 것으로 보인다.

Ⅱ. 인터넷과 사이버테러의 개념 및 유형

---

2) http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata_main&index=239&page=1&tempfilename=sdata_mainV.html

3) http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=186&page=3&tempfilename=sdataV.html

4) http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=213&page=2&tempfilename=sdataV.html

5) 매일경제, 2000. 2. 18.

1. 인터넷 이용자 수와 네트웍의 특성

1) 인터넷 이용자수의 변화

인터넷은 전세계적인 컴퓨터 네트웍 시스템으로서, 사용자가 어떤 컴퓨터에 있든지 간에 그가 사용권한을 가지고 있다면 그 어떤 다른 컴퓨터에도 접속해서 정보를 얻을 수 있는 "네트웍의 네트웍"이다.[6]1오늘날 인터넷은 전세계의 수억 인구가 사용하고 있는 필수 도구이면서 가장 효과적인 정보전달수단으로 등장하였다.

2000년 현재 전 세계의 인터넷 사용자 수는 약 4억명이며, 2001년도 추정 사용인구는 5억2천만명으로서 약 30% 정도 증가할 것으로 예상하고 있다.

〈표 1〉 세계 및 국내 인터넷 이용자수

연 도	이용자수		연 도	이용자수	
	세 계	한 국		세 계	한 국
1990	1천만명	-1	1997	6천만명	163만4천명
1991	1천100만명	-	1998	1억명	310만3천명
1992	1천200만명	-	1999	2억5천만명	1천86만명
1993	1천500만명	-	2000	4억명	1천904만명
1994	1천700만명	13만8천명	2001(추정)	5억2천만명	2천223만명
1995	2천만명	36만6천명	2002(추정)	6억5천만명	-
1996	4천만명	73만1천명	2005(추정)	10억명	-

자료: Paul Budde Communication, Global Internet Market-Statistics Overviews, 2001. 4. 24.
한국인터넷정보센터(KRNIC)

국내 인터넷 이용자수 변화추이를 보면 1996년에 73만여명이었으나 2001년 6월 현재 2,223만명으로서 5년간 30배 가까운 성장률을 보이고 있다. 한국의 정보화는 발전속도와 외형에 비하여 보안상 다수의 취약점을 가지고 있어 Cyber terror의 공격대상으로서도 적합한 면이 있다고 볼 수 있다.

2) 인터넷의 특성

특정제품의 수가 그 제품의 사용자 수에 의존하는 경우, 그 제품은 Network 외부성(Network extemality) 또는 네트웍 효과(Network effect)를 갖는다. 모든 Network은 연결점(Node)과 연결(Connection)로 이루어진다. 대규모 Network은 연결점의 규모가 천천히

6) http://www.terms.co.kr

늘어나더라도 연결의 량과 질은 폭발적으로 늘어난다. 그리고 연결을 증가시키면 예상치 못한 효과가 발생한다.

참여자 수가 N명일 때, 총 연결 수는 N(N-1)이 된다. 즉 N2-N이 되는데, 이 때 N이 커질수록 N2가 아주 커지므로 전체의 연결 수도 N2에 가깝게 될 것이다. 이것의 매력은 한 사람의 참여자가 늘어날 때, 훨씬 더 많은 연결망이 생긴다는데 있다. 이처럼 Network 경제에서는 특정 임계치를 넘어서면 적은 노력으로도 커다란 결과를 낳을 수 있다. 이러한 효과는 인터넷 기술의 발달과정에 따라 상상키 어려운 폭증요소가 도입되므로 수년후의 인터넷 기술을 상상키 어려운 점이 있다. 한 예로 현재 32Bit체제의 IPv4 체재하에서는 인터넷에 연결할 수 있는 기기의 숫자가 43억개(4,300,000,000)이므로 2000년 세계 총 인구인 61억5800만명이 쓰기에도 부족한 편이나 128 Bit의 IPv6체제하에서는 IP의 숫자가 34×1036가 되므로 앞으로 인구가 증가하여 100억명이 되었을 때에도 1인당 34×1026의 IP를 사용할 수 있게 되는 것이다. 즉 현재의 43억개에 비하여 1027배가 되는 것이다. 대부분의 전자제품이 IP를 보유하고도 거의 대부분의 IP가 남을 정도의 IP가 배정 가능하며 이러한 IP로 연결된 제품들이 Control 가능한 System이 되는 것이다. 이러한 체제하에서는 모든 기기의 상호 연동가능성 여부가 가장 중요한 요소가 되며 업무용 및 가정용 기기 전부가 인터넷으로 연동가능하게 되면 모든 장비가 Cyber terror의 사정권에 들게 된다고 볼 수 있다.

〈표 2〉 IPv4와 IPv6 비교표

구 분	IP v4	IP v6
주소길이	8비트씩 4부분의 10진수 표시 예)222.222.222.222	16비트씩 8부분의 16진수로 표시 예)1234:5678:9abc:def0:1234:5678:9abc.ef11
주소개수	약 43억개	거의 무한대43억×43억×43억×43억
주소할당	A, B, C, D, E 등 클래스 단위의 비순차적 할당	네트웍 규모 및 단말기 수에 따른 순차적 할당으로 효율적
품질제어	Best effort 방식으로 품질보장이 안됨 (Type of service에 의한 일부 지원)	등급별, 서비스별 패킷을 구분할 수 있기 때문에 품질 보장이 용이 (Traffic Class Flow Label에 의한 QoS 보장
보안기능	IP sec 별도 설치	확장기능에서 기본적으로 제공
PnP	없음	자동설정 기능
Mobile IP	비효율적이고 곤란	효율적이고 용이
웹캐스팅	곤란	영역지정 필드 증가로 용이

자료: http://e-campus.co.kr

2. 사이버테러의 개념 및 특징

1) 사이버테러의 개념

테러리즘은 오늘날 국제사회가 당면한 가장 심각한 문제중의 하나임에도 불구하고 지금까지 "테러리즘이란 무엇인가?"에 대한 보편적인 정의가 존재하지 않고 있다. 그동안 서구의 여러 학자들과 전문가들의 학문적 노력에 의해 테러리즘의 정의에 관한 연구가 많은 진전을 보여왔지만 아직 모든 학자들이 전적으로 동의하는 테러리즘의 정의는 내려져 있지 않다. 이는 테러리즘의 개념 정의 자체가 난제임을 반증하는 것이다. 테러리즘의 동기, 대상, 범위, 주체, 이념 등의 포함여부 그리고 학자들과 테러리즘 전문가들의 시각에 따라 개념이 달리 정의됨으로써 테러리즘의 정의에 관한 연구와 논쟁은 끊임없이 계속되고 있다. 즉 동일한 사건을 관점에 따라 테러리즘으로 규정하기도 하고, 단순한 일반범죄로 취급하기도 하며, 다른 시각에서는 애국적인 행위로 평가하기도 한다.[7]

미 국무부는, "테러리즘은 준국가단체 혹은 국가의 비밀 요원이 다수의 대중에게 영향력을 행사하기 위해 비전투원을 공격대상으로 하는 사전에 치밀하게 준비된 정치적 폭력"이라고 정의하고 있으며[8] FBI는 Cyber Terror의 개념을 "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives... through the exploitation of system deployed by the target"이라고 정의하고 있다.

국정원에서는 테러를 "정치적 사회적 목적을 가진 개인이나 집단이 그 목적을 달성하거나 상징적 효과를 얻기 위하여 계획적으로 행하는 불법적인 폭력행위"로 정의하고, 국가대테러활동지침(대통령훈령 제47호) 제2조 1호 마항에서는 "컴퓨터통신망을 이용한 정보조작 및 전산망 파괴"를 테러 유형의 하나로 규정하고 있는 바 이 규정에 의한다면 컴퓨터를 이용한 정보조작 및 전산망 파괴를 의미한다고 할 수 있다.

국방분야에서는 "전투(경쟁)에서 승리하기 위한 중요한 전략자원인 정보를 획득하고 활용하기 위하여 적(경쟁자)의 공격으로부터 우리의 정보기반구조를 보호하면서, 적(경쟁자)으로 하여금 이러한 정보를 사용하지 못하도록 적의 정보기반구조를 공격하여 전장(경쟁)에서의 정보 지배를 유지하기 위한 모든 방법"[9]이라고 규정하고 있다.

---

7) http://www.terrorism.or.kr, 한 예로 영국정부는 아일랜드 공화군(IRA)의 모든 공격을 테러리즘으로 그리고 IRA 요원들을 테러리스트로 규정하고 있다. 반면에 IRA를 추종하는 사람들이나 리비아 등 IRA를 직접 혹은 간접적인 방법으로 지원하고 있는 국가들은 IRA의 행위를 민족주의 해방운동(National Liberation Movement)으로 그리고 IRA요원들을 자유투사(Freedom Fighter)로 규정하고 있는 실정이다.

8) http://www.terrorism.or.kr

9) 조완수, "사이버테러 활용 및 대응기술", 국가보안기술연구소 주최 제1회 정보보증기술심포지움 자료집, 2001. 12. 11. p.73.

사이버테러의 개념정립이 미비된 이유 중의 하나는 이 분야의 변화가 너무 신속하여 학계에서 개념이 형성되기도 전에 사회환경이 변화함으로 또 다른 개념이 추가되어 공감대의 형성이 어려운 점이 있음을 들 수 있다고 하겠다. 이렇게 사이버테러는 아직 정확한 학문적 개념이 확립되지 않은 실무적 개념으로서 현재에도 개념상의 진화를 거듭하고 있다.

2) 사이버테러 양상의 변화

변화의 속도가 예측할 수 없을만큼 급변하는 정보혁명의 과정에 있는 현 시점에서 조만간 도래할 근미래의 사이버테러 양상에 대하여 한 번 검토해 볼 필요가 있다.

C8lyber terror의 위력은 Network을 통해 국가 기간산업과 군사·핵발전소·금융·항공기·철도 등의 통제 시스템을 순식간에 혼란에 빠뜨릴 수 있으며, 21세기 첨단기술을 최대로 활용하고 있는 테러집단들이 앞으로 어떤 식의 테러를 자행할지 정확히 예측하기란 쉽지 않다.

현실공간에서 상상만으로 그칠 일이 사이버공간에서는 실제로 가능한 경우가 많다. 그 중 한 예로 병원에 보관된 전산자료의 변조를 들 수 있다. 대량의 해킹이나 바이러스 유포가 아니고도 국가원수나 군, 관, 기업체 주요임원들의 전산기록 중 혈액형을 기록한 글씨 한자를 변경하는 행위만으로 상대국이나 경쟁기업의 체제에 변화를 줄 수 있다면 이처럼 위험부담이 적고 효율적인 테러가 있을 수 없을 것이다.

21세기의 테러는 점차 정보와 그 System에 타격을 주는 Terror의 비율이 높아질 것으로 예상되며, 앞으로는 전쟁도 군사시설에 대한 직접적인 타격보다는 그 전단계에서 군수지원시스템과 국민생활의 핵을 이루는 다양한 전산시스템에 대한 Cyber상의 공격을 선행함으로써 사회기반을 무력화하는 단계가 필수적으로 도입될 것이며 이러한 단계에서는 군과 경찰, 민관이 구별되지 않은 혼연일체의 대응체제를 구축해야 할 것이다. 현재에도 점차 분야별, 계층별, 업무별 영역의 담장이 붕괴되고 있으나 이러한 통합추세는 갈수록 가속화할 것으로 보인다.

3) Cyber terror의 특징

Cyber terror는 가상공간의 특성상 현실공간과는 다른 성격이 존재하므로 기존의 테러와 다른 다양한 특징들이 있다.[10]

가) 수행비용이 저렴하다.

Cyber terror에 필요한 장비는 PC 한대로 가능한 실정이므로 특별히 고가의 장비가 필요치 않다. 미사일 한 기만 해도 수만 달러[11]에 이르며, 폭탄테러를 하기 위하여는 자살특공대가 필요할 경우도 있으나 Network 상에서는 그러한 위험을 감수하지 않고도 상대방

10) 조완수, 전게자료, p.73.

11) 사이드와인더 미사일 1기에 41,300$, http://arms.defence.co.kr/weapon/side.htm 참조.

에 대하여 목적한 바를 달성할 수 있다.

나) 사이버공간에서는 경계가 불분명해진다.

공공과 민간, Terror와 범죄, 국가간의 지리적 국경 등의 개념이 모호해진다. network에 연결된 이상 모두가 하나이다. On line 상에서는 시공의 경계가 있을 수 없어 24시간, 전 세계가 하나로 작동된다고 볼 수 있다. Cyber상에서는 접근이 허용되는 모든 지점이 잠재적 전장이 되며, Network만 있으면 장소를 불문하고 Terror 임무를 수행할 수 있다.

다) 지각능력을 조작할 수 있는 기회가 많다.

비디오 모핑 등을 이용한 이미지 혹은 사실의 조작 및 광범위한 전파도 가능하다. www은 순식간에 별도의 비용을 들이지 않고 다수의 사람들에게 많은 량의 정보를 발송할 수 있으며 따라서 부정확한 정보를 접한 사용자들이 이러한 정보를 오판하여 신뢰하는 결과를 초래할 우려가 있다.

라) 새로운 전략 첩보의 수집 및 분석방법이 요구된다.

현재까지의 일반적인 테러방법은 새로운 체계를 개발하고 이를 사용할 수 있도록 함에 상당한 시간이 필요하였다. 하지만 Cyber상에서는 이러한 과정의 수행에 별도의 시간이 필요하지 않은 경우가 대부분이며, 따라서 상대방이 어떠한 공격방법을 구상하고 있는지 외형적으로는 전혀 할 수 없을 경우가 많다고 할 수 있다.

마) 적절한 경고시스템 및 평가방안 부재

갑자기 메일에 섞여 들어오는 Virus를 PC에서 자동적으로 구별하여 경보를 발령하는 시스템이 없으며, 백신을 구입하여 설치한 후 지속적인 관리를 하여야 하므로 Cyber terror를 예방하기 위하여는 수시로 백신을 다운받아서 검색을 하고 조치를 하여야 한다.

3. Cyber terror의 유형

1) 방법에 의한 분류

인터넷의 발달로 사이버공간상에서 필요한 정보를 획득하거나 손괴하는 것이 보다 간단해졌다. 따라서 이러한 수단을 이용하여 적국이나 상대방의 가지고 있는 중요한 정보의 무력화나 파괴가 하나의 중요한 방법으로 사용되어 왔으며, 그 주된 수단으로는 Hacking, Virus, Mail bomb, Logic bomb, AMCW 등이 있고, Off Line상의 Cyber terror용 무기로는 전자총, Chipping, Jaming, HERF[12], HPM[13], EMP[14], Nano machine,[15] 미생물무기

12) High Energy Radio Frequency Gun, 고에너지 RF를 무기로 근거리 상대방의 전자장비 기능을 마비시키는 무기

13) High Power Micro wave : 좁은 밴드역, 좁은 빔폭, 초고주파 에너지, 높은 출력을 방출하여 목표의 전자적 기능을 마비시킴

등이 있다.

가) Hacking

Cyber terror에 가장 많이 사용되는 수단이 바로 Hacking이다. 어떠한 목적에서건 시스템 관리자가 구축해 놓은 보안망의 무력화와 관련된 모든 행동을 말하며, 보통 시스템 관리자의 권한을 불법적으로 획득한 경우 또는 이를 악용해 다른 사용자들에게 피해를 주는 경우에 해당한다.[16]

〈표 3〉 연도별 해킹피해 상황

년 도	'96	'97	'98	'99	2000	2001. 9월
건 수	147	64	158	572	1,943	4,301
증감율(%)	0	-56.5	146.9	262.0	339.6	221.3

자료: http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=186&page=3&tempfilename=sdataV.html

최근들어, 해킹 형태가 더욱 복잡해지고 분산되었으며, 복수의 취약점을 노린 공격이 동시에 행해지고 있다. 해커들이 공격할 수 있는 단서를 제공해 주는 취약점 또는 취약성은 운영체제나 애플리케이션 및 네트워크 장비의 취약점을 말하는 것으로, Hacker들은 해당 제품이 발표됨과 거의 동시에 공격 코드들이 인터넷상에 발표[17]하고 있으며 Scanning, IP Spoofing, Buffer Overflow 등의 다양한 방법이 있다.

나) Virus

Virus는 컴퓨터 Virus가 아닌 Program의 구조를 다른 Porgram의 구조로 변경하거나 많은 Program에 대하여 수정을 할 수 있는 것, 어떤 Program에 행해진 수정여부를 인식할 수 있거나 위의 수정 인식후 같은 Program을 또 다시 수정하지 않는 Program으로서 이 Program에 의해 수정된 Program이 위의 4가지 특징을 만족시킨다면 컴퓨터 Virus라고 해도 좋을 것이다.[18] 이러한 Virus의 종류로는 윈도우 바이러스, 매크로 바이러스, 부트/파일 바이러스, 파일 바이러스, 부트 바이러스, Trojan, Worm, Hoax 등이 있다.

---

14) Electro Magnetic Pulse 폭탄 : 전자기 펄스효과를 사용하여 단기에 고출력 펄스 에너지를 방출, 목표의 전자적 기능을 마비시킴.

15) 초소형의 거미나 개미 등과 같은 유기체로 네트워크나 시스템에 침입하여 기능을 마비시키는 무기 (1㎚=10억분의 1m)

16) 이요섭, 공무원정보보호심화과정 교재 I (서울: 정보통신교육원, 2001), p. 2.

17) http://www.boani.com/secui/src/info/shield_detail.jsp?nodeid=231&order=hit+desc&expertid=331&rsc=1&rscid=981331705370&page=1

18) 박명순, 컴퓨터 바이러스 분석, 제작 및 처방 (서울: 집문당, 1992), p. 23.

〈표 4〉 신종 바이러스 현황

구 분	1월	2월	3월	4월	5월	6월	계
국 산	3	4	2	3	1	3	16
외 산	11	14	18	11	17	16	87
합 계	14	18	20	14	18	19	103

자료 : KISA, 2001년 상반기 해킹·바이러스 분석 보고서, p. 28.

Virus는 Software가 가진 취약점을 공격하는데 가장 많이 동원되고 있으며, 일반적으로 Program을 변형 또는 삭제하여 주변기기에 오동작을 일으키거나 파일을 손상시키며, 자기 자신을 복제하는 등의 행위를 하는 프로그램으로서 때로는 치명적인 피해를 가져오는 것도 있다.[19]

다) 기타 전자무기

Cyber terror에 동원되는 무기 중 컴퓨터 하드웨어의 취약성을 공격하는 무기이다. 대표적인 방법으로는 Tempest[20]와 EMI,[21] EMC[22] 등이 있다. 이는 컴퓨터 시스템이 내는 전자파를 수집해 정보를 입수하는 방법이다. 컴퓨터가 쏟아내는 전자파 흐름은 뇌파와 달리 일정한 규칙을 가지고 있어 컴퓨터 시스템 입출력시의 주파수와 파장을 분석하면 컴퓨터 파일의 내용을 복구할 수 있다.

(1) 전파방해 (electronic jamming)

오래 전부터 사용되는 방법이다. 적국 시스템이 송수신하는 전파의 흐름을 방해해 전달하고자 하는 정보를 없애거나 가짜 정보를 중간에 삽입하여 통신망을 교란하는 행위이다.

(2) Chipping

시스템 하드웨어를 설계할 때 Chip속에 고의로 특정코드를 삽입한 채 시스템을 공급하다가 긴급한 사유로 시스템을 공격하거나 침투할 때 사용하는 병법이다.

(3) 논리폭탄 (Logic Bomb)

---

19) 국정원, Cyber terror대응정보보안교육 교재, 2001. 04, p.4.

20) 순간전자장파동표준(Transient Electromagnetic Pulse Standard), 전화선이 없어도 컴퓨터 화면에서 나오는 독특한 무선주파를 주변사무실에서 '방향 안테나'를 통해 잡아 영상신호를 확장하면 컴퓨터 화면에 나오는 내용을 파악할 수 있다. 컴퓨터 앞에 있는 사람이 무엇을 보고 있는지, 어떤 비밀문건을 작성하고 있는지를 파악할 수 있다.
http://www.kinds.or.kr/

21) 電磁波障碍 : electromagnetic interference

22) 電磁波適合性 : electromagnetic compatibility

컴퓨터 바이러스와 비슷한 것이 논리 폭탄이다. 논리 폭탄은 적국 시스템에 일시적으로 오류가 발생하도록 시스템 내부 코드를 바꾸는 기능을 수행한다.

(4) 전자파 무기 및 미생물 무기 등[23]

미국 뉴멕시코 로스앨러모스 국립연구소는 강력한 전자기파를 만들어내는 서류가방 크기 전자 장치를 개발했다. 이 장치를 은행 주위에 설치하면 건물 안에 있는 모든 디지털 정보는 순식간에 사라져 버린다. 전자 기술과 생물학이 만나는 방법이 이용되기도 한다. 미생물체가 쓰레기나 기름 찌꺼기를 먹어치우는 것처럼 컴퓨터 부품을 갉아먹는 미생물체의 개발도 연구중이다.

2) 집단 및 목적에 의한 분류

컴퓨터 관련 범죄를 자행하는 집단은 크게 3가지 유형으로 분류할 수 있다. 첫째는 개인적으로 활동하는 해커들이다. 둘째는 범죄 조직화된 집단이다. 셋째는 정치적, 민족적 혹은 종교적인 목적을 달성하기 위해 조직된 단체나 혹은 주권국가의 사이버 테러리스트들이다. 이 중에서 가장 우려가 되는 것은 세번째 유형의 집단에 의해 저질러지는 사이버 테러리즘이다.

지금까지 발생한 대부분의 컴퓨터 관련 범죄는 컴퓨터를 이용한 사기 등과 같은 단순 범죄였다. 그러나 최근에는 단순한 해킹 차원을 넘어 정치, 민족, 종교 혹은 사회적 목적을 달성하기 위해 테러리스트들이 가상 공간을 이용하고 있다. 기존의 해커 중에서도 일부가 자기 과시나 자기 만족보다는 정치적 명분을 추구하는 사이버 테러리스트로 바뀌고 있다는 것도 사이버 테러리즘 확산의 요인이 되고 있다.[24]

6. 외국의 Cyber terror 대응현황

1) 미국

국가안보의 새로운 위협 요소인 Cyber terror에 대처하기 위해 세계 각국은 대응책 마련에 부심하고 있다. 미국에서는 1995년부터 국방부와 관련부처를 중심으로 해킹 전담팀을 구성하고 1996년부터 국방성 산하에 보안전문가로 구성된 "RED Team을 운영하고 있으며, 1998년부터 해킹을 전시에 공격수단으로 활용하는 방안까지 연구·추진하여 왔다.

1999년 10월에는 대서양 사령부를 사이버전쟁통합사령부로 운용하기 시작하였으며 셜던 합참의장이 수비위주의 전략에서 공격과 수비를 병행한 전략으로 전환하여 개념정립 특별

23) http://user.chollian.net/~jy1010/cyberwar/news-1-1.htm
24) http://www.terrorism.or.kr

팀을 구성 운영하였고, 2000년 10월에는 사이버전쟁 프로그램을 강화하였다고 한다.[25]

2) 영국

영국은 지난 20년간의 경제적 불안정성을 해소하고 경쟁력을 회복하기 위하여 지식정보화를 전략적으로 활용하고 있다.[26] 그러나 공공기관의 3분의 1이 사이버 테러리스트들로부터 해킹을 당한 것으로 조사되었으며, 이들의 거의 절반이 일명 넷스피오나지(netspionage)로 알려진 사이버 테러가 조직의 생존을 위협하고 있다고 생각하는 것으로 나타났다.

영국 통신관리협회(CMA)의 조사결과에 의하면 32%가 사이버 테러를 당한 경험이 있다고 응답하였으며, 60%는 해킹이 조직생존에 심각한 위협이 되고 있다고 시인했다. 더욱이 CMA 전문가들 중 절반이 자신들의 업체가 이같은 사이버 테러와 싸울 준비가 돼있지 않다고 대답했다.[27]

3) 일본

일본에서는 좌익 또는 우익을 표방한 일부 과격단체의 폭력이 테러범죄의 양상을 띠면서 점차 증가추세에 있는 가운데, 급속한 국제화의 진전과 더불어 국제테러의 위험 또한 증가하고 있다. 따라서 관방성 주도하에 사회기반 및 생산설비에 대한 Cyber terror 대책을 수립하고 1999년 9월 관방성, 경찰청, 방위청, 금융감독청 등 13개 부처 국장급으로 정보보안관계부처 회의체를 구성 운영하고 있다.[28]

주로 테러범죄의 예방을 위한 치안강화 및 테러발생시의 신속한 진압이나 테러대응 요령에 관한 대국민 홍보 등 행정적인 조치에 치중하고 있으며, 특히 국제테러범죄에 대하여는 국제형사사법공조나 국제적인 정보교환 등 국제협력에 적극적으로 노력하고 있다. 그러나 일본은 앞서 살펴본 국가들처럼 테러범죄에 대한 특별한 형사입법을 하고 있지는 않다.

4) 중국

아시아 유일의 핵과 중장거리 탄도미사일 보유국인 중국은 97년 약 100명 수준의 정예인력으로 구성된 해커부대를 창설했다.[29]

중국의 북경 군구는 1997년 6월 인민해방군 내에 Computer Virus 특수부대를 창설, 가

---

25) 김효식, "Cyber terror 어떻게 대처할 것인가?", 제2편, 새천년민주당 국회의원 연구보고서, 2001. 9. p.2.

26) 정보통신부, Cyber Korea 21, 창조적 지식기반국가 건설을 위한 정보화 Vision, 1999. 3, p. 3.

27) 전자신문, 2001. 4. 6.

28) 국정원, 전게서, p. 8.

29) 상게 site.

상적국의 군 지휘체제 교란 및 파괴연구를 수행하고 있으며, 1999년 10월 최대의 인터넷 전쟁훈련을 실시한 것으로 전해졌다. 같은 달 광주군구는 무한(武漢)대학과 군간부 배양계획을 체결해 대학생에게 매년 5,000위안화를 지원하고 졸업 후 인터넷전쟁의 주력으로 활용키로 하였으며, 유사시 적군의 컴퓨터망을 무력화시킬 수 있는 전자특수부대 Net Force를 육성중이라고 보도한 바 있다.[30]

Ⅲ. Cyber terror의 실태 및 문제점

Cyber terror는 Network상에서 일어나는 테러로서 정보가 유통되는 통신망이 없으면 발생될 수 없는 한계를 가지고 있다. 그러나 Network이 활성화되고 일상적인 대부분의 업무가 Network를 통하여 이루어지면서 모든 분야가 Cyber terror의 위협에 노출되어 있다고 해도 과언이 아니다. 인터넷은 무한(infinity), 불확실성(uncertianty), 가상(virtuality), 개별성(individuality), 평등(equality), 자유(freedom)의 세계이다.[31] 따라서 발생되는 현상 역시 현실공간과 대비되는 많은 차이가 있으며 이러한 부분을 감안하지 않은 실태파악과 대응전략논의는 현실성을 도외시한 대책이 될 수 있다.

1. Cyber terror의 실태

1) 국가 정보에 대한 위협

전자정부란 일하는 방법을 정보화에 맞게 쇄신하여 모든 업무처리를 전자화함으로써 행정기관간, 행정기관과 국민·기업간의 모든 업무를 전자적으로 빠르고, 투명하고, 편리하고, 효율적으로 처리할 수 있는 정부를 말한다. 따라서 전자정부가 구현되면 국민과 기업은 관청을 방문하지 않고도 한번의 클릭으로 민원을 신청하고 발급받으며, 행정기관과 계약, 거래·결제하고, 각종 세금을 신고·납부하며, 필요한 각종 정보를 획득하고, 의견을 제출하는 등 정부와 의사소통을 자유롭게 함으로써 빠르고 편리하고 투명한 정부가 구현되는 것이다.[32] 정부는 이러한 전자정부를 구현하기 위하여 「전자정부의 구현 및 운영에 관한 법률」을 마련하여 2001년 7월 1일부터 시행에 들어가게 되었다.[33]

---

30) 국정원, 전게서, p .9.
31) 장승권, 정명호, 김영수, 인터넷 지식벤처의 성공조건 (서울 : 삼성경제연구소, 2000), p. 34-39.
32) 행정자치부, 전자정부의 이해와 해설, 행정자치부, 2001, p. 5.
33) 상게자료, 2001, p. 11.

〈표 5〉 전자정부의 업무범위

분야	업 무	세 부 내 용	비 고
G2C	민원처리	인허가 처리, 재증명 발급 등	
G2B	정보제공	의무고지, 예고, 고시, 기타 정보제공, 안내	
	금전지불	지불, 조세환급, 사회적 급여지급 등	
	전자거래	물품조달, 입찰 및 서비스 대가지급 등	
C2G	신청,제출	인,허가신청, 이의제기, 신고, 고발 등	
B2G	국정참여	공청회 등 의사표시, 전자투표 등	
	금전납부	조세납부, 공과금 납부, 서비스 대가지급 등	
G2G	공동이용	문서·지식관리정보 공유, DB 공동이용 등	
	의사교환	전자문서 유통 등	
	행·재정	인사·조직, 급여, 예산, 자금 등 관리	
	의사결정	전자결재, 영상회의 등	

자료: 행정자치부, 전자정부의 이해와 해설, 2001, p. 8.

그러나 전자정부 등 국가업무의 On line화는 전자적인 침투 즉 Cyber terror에 대한 대응조치가 완벽하지 않은 한 정보에 대한 위협이 증가하고 있다고 볼 수 있으며 따라서 Cyber terror의 효과 역시 극대화될 수 있는 여건이 조성되어 가고 있다. 사이버범죄는 그 실행방법을 Cyber terror에 그대로 적용이 가능하다는 점에서 Cyber terror의 직전단계로 볼 수 있다. 이같은 사이버 범죄 증가율은 5.2%에 불과한 지난해 범죄 잔체 증가율이나 일반범죄 중 가장 높은 증가율을 보인 절도(94.5%)와도 비교가 되지 않아 수년 내 발생빈도가 가장 많은 범죄로 자리잡을 것으로 우려된다.[34] 이러한 사이버범죄는 약간만 발전한다면 Cyber terror로 발전할 수 있는 가능성이 농후한 상태로 볼 수 있다.

2) 기업차원의 정보보호 현황

Cyber terror의 대상은 정보화된 자료이다. 국내에서도 각 분야에서 정보화가 진행되어 그 위력을 실감하고 있다. 증권거래의 경우 전체 증권거래 중 사이버 증권거래가 차지하는 비중은 1998년 말 약 3% 수준이었으나 1999년 말 사이버 증권거래 비중이 40%를 넘어섰으며, 2000년 말에는 60%를 넘어 2001년 7월 현재 70% 수준에까지 이르렀다.[35]
Netvalue[36]는 2001년 7월 한국에서는 560만명이 Internet Banking Site를 찾았으며 그 다음은 영국 520만명, 프랑스 330만명, 독일 320만명 등의 순으로 고객숫자 기준으로 가장

34) 국민일보 2001. 8.24. 01면, 사이버범죄 3년새 200배…폭력—절도 이어 3大 범죄로. 해킹 범죄는 2000년에는 449건이었으나 2001년 7월까지 5,397건에 달하는 등 크게 늘고 있다. 이외에 E메일 주소 도용 및 개인정보 침해(2001년 7월 말 현재 4,797건, 2000년 402건), 명예훼손(2001년 7월 말 현재 3470건, 2000년 313건), 불법복제(2001년 7월 말 현재 636건, 2000년 59건) 등이 인터넷상의 주요 범죄로 나타났다.

35) http://www.stockpia.com/its/review/view.asp?flag=&no=10&page=1&spage=1&keyword=

36) http://www.netvalue.com/

Internet Banking이 활성화된 국가로 조사되었다.[37] 그러나 어느 국가를 막론하고 정보화가 진행되면서 이러한 기업정보에 대한 위해 역시 증가하였다.

2001년 해킹피해 중 기관별로는 일반기업체가 전체 건수의 40.7%로 가장 많아 기업 시스템이 해커들의 주공격 대상인 것으로 드러났다. 이는 대부분 중소기업체가 정보보호 인식과 준비가 미흡하여 정보보호분야에 대한 투자를 꺼리기 때문인 것으로 보인다. 해킹 경로로 보면 한국을 해킹 경유지로 삼는 국외 해커들의 침투사례가 2000년 261건에서 2001년 들어서는 297건으로 급속히 늘어났다.[38] 이러한 결과는 Cyber terror에 대한 위험성 역시 지속적으로 높아지고 있음을 말해준다.

벤처에 대한 투자 중단으로 조성된 열악한 환경 역시 정보보호가 어려워진 원인의 일부를 제공하고 있다.[39] 국내에서는 파산한 닷컴이 고객정보를 판매해 문제를 일으켰던 사건이 공식적으로 발표된 바는 없지만, 대부분의 닷컴들이 암암리에 고객정보를 거래하고 있는 것으로 알려지고 있어 닷컴들의 고객정보 유출은 매우 심각한 수준인 것으로 보인다. 기업간 합병의 경우에도 자신의 정보가 제3자에게 넘어가는 것을 원치 않는 이용자의 의사가 반영될 수 있도록, 일정기간 홈페이지에서 회원탈퇴가 가능하도록 조치해야 한다. 또 합병해서 새로 탄생한 회사 역시 일정기간 회원탈퇴 장치를 마련했음에도 가입해지를 하지 못한 이용자를 위해 그 사실을 일정기간 홈페이지나 전자우편을 통해 이용자에게 알려야 한다. 파산했더라도 이용자의 동의 없이 개인정보를 제3자에게 제공하는 닷컴기업은 엄중한 벌을 받아야 하며 파산한 닷컴이 늘어남에 따라 파산한 닷컴의 고객정보 유출문제가 사회문제로 확대될 가능성이 높다. 인터넷 기업들은 개인정보에 대한 소유권이 이용자에 있다는 점을 명확히 인식해야 할 것이나 사실상 이러한 사고를 가지지 못한 CEO와 임직원들이 많은 실정이다.[40]

〈표 6〉 시대별 공개가능성과 보안

가능성 \ 시대별	과 거	현 재
공 개	선 택	필 수
비공개(보안)	당 연	선 택

37) http://www.marketcast.co.kr

38) http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=186&page=3&tempfilename=sdataV.html

39) 최근 2차 투자를 받지 못해 폐업하게 된 한 인터넷 업체의 K사장은 1년여간 사이트를 운영하면서 축적한 고객정보를 다른 업체에 팔 것인지 여부를 놓고 고민하고 있다. 요즘 테헤란밸리에는 문을 닫는 사이트만큼이나 K사장과 비슷한 고민을 하는 젊은 사장이 적지 않다. 미국의 경우, 파산한 인터넷 회사가 고객들의 개인정보를 타회사에 판매함으로써 개인정보 유출문제가 심각하게 대두됐다. 부닷컴 · 토이스마트 · 크래프트숍닷컴 등 파산한 인터넷 회사들이 내놓은 정보에는 고객의 전화번호 · 신용카드번호 · 집주소는 물론이고, 고객의 쇼핑습관에 대한 정보도 있었다. 만약 이 정보들이 악용될 경우 여러가지로 사회적 물의를 일으킬 가능성이 높기 때문에 비난여론이 비등했다.

40) http://www.dt.co.kr/dt_srcview.html?gisaid=20010814020105515740001

인터넷 시대는 공개하고 싶지 않아도 공개될 수 밖에 없는 시대이다. '공개'는 선택사항이 아니라 타의에 의한 필수사항이며, '보안'이 강요된 선택의 시대로 가고 있다고 할 수 있다. 대부분의 Server나 PC가 internet이나 intranet으로 연결되어 별도의 보안조치를 하여도 약간의 기술만 있으면 열람이 가능한 상태가 된 것이다.

3) 개인들의 정보의 보호에 대한 인식

개인정보가 기업의 이윤창출에 결정적인 역할을 하면서 개인정보의 가치가 곧 기업의 가치와 직결되는 시대가 되었다. 인터넷에서는 User 개개인의 동향이 Check되어 관련 국제기구에서 통계자료화하고 있으며, 한국의 Internet 지수가 작성되고, 이 모든 절차가 Real time으로 이루어지고 있다.

따라서 모든 기업들이 보다 많은 고객정보를 보유하기 위하여 다양한 서비스를 동원하여 개인정보의 입력을 유인하고 있는 바 그 중 대표적인 것 중의 하나가 바로 Mail 서비스이다. e-Mail 계정은 사실상 가장 중요한 개인정보이다. 미래는 자신이 거주하는 주소보다 인터넷 상의 주소인 e-Mail이 더욱 중요하다고 볼 수 있다. e-Mail은 거주지가 바뀌더라도 지장을 받지 않으며 해외에서도 열람이 가능하다. 미국이나 일본, 영국, 아프리카 등지로 출장을 다니면서도 자신에게 온 편지를 열람할 수 있으며, 또한 다른 사람에게 편지를 보낼 수도 있다. 따라서 시간과 장소의 제한을 받지 않는 사실상 거의 무제한적인 통신수단이다.

이러한 e-Mail 주소는 현실적인 주소보다 더욱 중요한 통신요소이며 앞으로는 단순한 자료전송은 대부분 e-Mail을 통하여 이루어 질 것으로 예상할 수 있다. 이러한 e-Mail은 상업적인 목적으로 사용됨은 물론 행정이나 작전시 중요사항을 전달할 수 있다. 미국에서는 실제로 e-Mail을 작전에 활용하고 있으며 앞으로 이러한 경향은 각국에도 확대될 것으로 보인다.

〈표 7〉 사이트별 개인정보 입력 항목

업 체 별	I D	P/W	주민 번호	생일	성 명		주소	전화번호			추천인	E-Mail	비고
					한글	영문		사무실	집	휴대폰			
주민정보			○	○	○		○						
다 음	○	○		○	○		○					○	
라이코스	○	○		○	○		○	○		○			
드림위즈	○	○	○	○	○	○	○	○		○	○	○	
마이클럽	○	○	○	○	○		○		○	○		○	
야 후	○	○		○	○							○	
엠 파 스	○	○	○	○	○		○		○	○		○	
핫 메 일	○	○		○	○								
오르지오	○	○	○		○		○	○				○	
네 이 버	○	○	○	○	○	○	○	○	○	○		○	
네 티 앙	○	○	○		○		○		○	○		○	
팝스메일	○	○	○	○	○		○		○	○			

한 미 르	○	○	○		○		○		○	○		○	
슈퍼보드	○	○	○		○		○			○		○	
깨비메일	○	○	○		○	○	○		○	○			
천 리 안	○	○	○		○		○		○	○		○	
하 이 텔	○	○	○		○		○			○			

자료 : 각 site 가입신청 page.

인터넷이 어느 정도의 정보를 노출시키고 있는가를 실제 눈으로 확인하고 싶으면, www.privacy.net을 방문해보면 알 수 있다.[41] 그러나 이 site에서 노출되는 정보[42]는 단지 빙산의 일각에 불과하다. 만일 당신이 어떤 웹사이트에 회원으로 가입하여 그 사이트를 자주 찾았다면 그 웹사이트에서는 로그(Log) 분석을 통해 이미 당신이 어디에 관심이 있는가를 다 파악할 수 있다. 데이타 마이닝(Data Mining)기법을 통해 당신의 마음속에 있는 것까지 다 분석해내는 것이다.[43]

테러의 대상자가 어느 날 어디서 몇시에 무슨 일을 하는지까지 확인이 가능할 수도 있는 것이다. 따라서 자신의 정보는 자신의 정보이므로 어느 사이트에서든 자신이 관리하여야 하며, 불필요한 사이트에는 가입하면 안되는 것이다. 개인정보는 인터넷에 등재되는 순간 이미 개인정보가 아닌 것이며, 공공정보가 되는 것이다.

그 외에도 Terror 용의자가 대중의 일부인 자신을 통하여 집단의 성향, 기호, 취미, 특기 등을 분석해 낼 수 있으며, Terror의 계획 수립에 이 자료를 근거로 할 수 있는 것이다.

2.Cyber terror의 문제점

1) 국가정보화의 진전에 따른 취약성 증가

행정정보화계획이나 전자정부 계획을 보면 어느 기관도 예외가 될 수 없다. 그러나 반드

41) http://www.privacy.or.kr/ 내 정보가 얼마나 유출되나?

42) 이 site의 화면 상단을 보면 "안녕! 당신의 IP는 123.123.123.123이군요"라고 말하면서 아이비즈넷으로부터 링크되어 왔다는 사실과 함께 자세한 정보를 보려면 "Click Here"를 누르라고 한다. 실제 클릭한 후 새롭게 뜨는 화면의 하단을 보면 상당히 놀랍다. 현재 당신이 쓰고 있는 오퍼레이션시스템(OS)이 무엇인지, 어떤 웹브라우져를 쓰고 있는지, 그리고 화면의 해상도가 어느 정도인지 등을 보여 주고 있다. 그 밑을 보면 당신이 어떠한 경로를 통해 해당 사이트에 도달했는지를 보여 주고 있으며, 또 아래에서는 당신이 어떤 링크를 통해 들어 왔는지, 그리고 어떤 언어를 사용하고 있는지(한국어의 경우 ko임) 등 웹브라우져를 통해 웹사이트로 전달되는 정보들을 모두 보여 주고 있다. 따라서 당신이 접속한 웹사이트에서는 당신이 어떤 IP를 사용하고 있으며, 국적이 어디이고 어떤 경로를 통해 이곳으로 왔는지, 그리고 어느 정도의 해상도를 사용하고 있는지 등 매우 많은 정보를 알고 있는 것이다.

43) http://www.privacy.or.kr/ 내 정보가 얼마나 유출되나?

시 정보화가 장점만 있는 것인가 하는 점은 보안기능을 고려해 본다면 재고의 여지가 있다.

정통부 점검 결과 중앙 행정기관 대부분이 해킹이나 컴퓨터 바이러스 유포 등 컴퓨터 범죄에 무방비 상태인 것으로 드러났다. 정보통신부가 2000년 말 행정자치부·국가정보원과 공동으로 48개 중앙행정기관의 정보보호 추진실태를 점검한 결과, 일부 기관은 가장 기본적인 정보보호 시스템조차 구축하지 않았으며, 정보보호 시스템 운영·관리는 대부분 기관이 매우 미흡한 것으로 나타났다. 7개 기관은 가장 기본적인 정보보호 시스템인 침입차단시스템(방화벽 :Fire wall)조차 갖추지 않은 것으로 조사됐다. 침입탐지시스템(IDS :Intrusion detection system)을 설치 운영하는 곳은 법무·건설교통부·정보통신부·특허청·관세청·조달청·통계청 등 8곳에 불과했고, 암호시스템 가동 여부는 조사하지 않았으나 거의 모든 기관들이 구축하지 않은 것으로 파악됐다. 국방부·국가정보원·정통부·외교통상부 등 9개 부처를 제외한 39개 기관은 아예 전담인력조차 배치하지 않은 것으로 나타났다.[44]

2001년 9월 17일 국회 과학기술정보통신위원회 소속 한나라당 원희룡의원은 전산원에 대한 국정감사에서 국가정보원 자료를 인용, "국가 행정망에 대한 해킹이 지난 98년 18건이던 것이 올해(2001년)에는 상반기에만 328건의 해킹이 발생해 18배 이상 증가했다"고 밝혔다. 특히 원의원은 "재경부, 국방부 등 14개 중앙행정 부처의 보안시스템 구축현황을 조사한 결과 국방부와 건설교통부 단 두 곳이 안전진단시스템, 자료암호화시스템 등 보안시스템을 구축했으며 14개 부처 중 절반에 달하는 7개 부처는 아예 침입방지시스템 하나만을 설치한 것으로 밝혀져 국가행정망의 보안대책에 근본적인 문제점이 있다"고 지적했다.[45]

<표8> 최근해킹사고일지

년 월 일	내 용
2000.10.16	국회 전산망에 해커가 침입, 민주당 김효석 의원과 한나라당 원희룡 의원 홈페이지 자료 유실. ※ 두 의원은 정보보호에 관심이 많은 의원들임.
2000.10. 9	국회 국정감사에서 국내 10개 증권사의 사이버거래시스템에 대한 해킹 위험도 측정 결과, 일부 시스템의 경우 보안시스템 전무, 또한 암호화되지 않아 해킹에 그대로 노출된 것으로 지적.
2000. 9.16	현대그룹 정주영 전 명예회장의 홈페이지를 비롯한 현대그룹 계열사에 네트워크 공격이 가해짐.
2000. 9.15	2000년 상반기 동안 1,067건의 Cyber terror 행위가 발생한 것으로 발표됨.
2000. 9.13	유가급등에 항의하는 한 해커가 석유수출기구(OPEC)의 홈페이지를 공격.
2000.9. 7	한 공익요원에 의해 진주시청 홈페이지 공격 당함
2000. 7.31	국내 대학을 비롯한 공공기관-기업 등 250여 곳의 시스템이 해커들의 공격에 무력화됨.

자료:http://www.boani.com/secui/src/info/shield_detail.jsp?nodeid=231&order=hit+desc&expertid=331&rsc=

44) 조선일보, 2001. 1. 31.

45) http://www.inews24.com/php/search_news_view.php?g_serial=45252&g_menu=080400&pay_news=0

1&rscid=981331705370&page=1

사이버 테러리즘이 각광받는 이유는 물리적인 테러리즘보다 적은 비용으로 큰 효과를 노릴 수 있다는데 있다. 고도 선진화된 사회일수록 전력과 금융, 통신 및 수송망 등의 사회 기반이 네트워크로 연결되어 있는 만큼 정보망을 파괴했을 때의 파장은 예측하기 힘들 정도이다.[46] 따라서 저비용으로 순식간에 소기의 목적한 바를 달성하는데는 Cyber terror가 가장 효과적이라고 할 수 있다. 이러한 예로 볼 때 1999년 4월 26일 있었던 'CIH Virus는 국내에서만 30만대의 PC를 망가뜨렸고, 수리비와 데이터 복구에 소요된 비용만 20억원 이상인 것으로 알려지고 있으며, 전세계적인 피해액은 무려 2억5,000만 달러(추정)로 예상될 정도로 위력적이었다.

러브바이러스 등은 그 피해규모가 잘 알려진 경우이지만 카드사기, 신용사기, 돈세탁, 아동 포르노, 사이버 스토킹, 저작권침해, Cyber terror 등 잘 알려지지 않으면서 그 폐단은 알려진 것보다 더욱 크다고 할 수 있다. 시위시에도 온라인에서는 10명만 가세하면 네트워크를 마비시킬 수 있다. 이것이 바로 사이버 테러리즘의 매력인 것이다.[47] 가상전 기술은 이미 전쟁에서 활용되고 있다. 1990년 걸프전에서 미국이 승리하는 데는 정보전 기술이 크게 기여했다.[48]

2) 외형에 못미치는 기업체의 보안 인식 저하

---

46) http://www.terrorism.or.kr NATO의 중국 대사관 오폭으로 중국인들의 피해가 일어나자 일단의 중국인들이 백악관과 국무성을 비롯한 사이트를 해킹한 사례도 있었다. 이로 인해 백악관 웹사이트는 중국어와 영어로 된 각종 낙서로 도배되었으며, 24시간 동안 사용 불능 상태까지 이르렀다. 이들은 미국에서 중국이 원하는 수준의 대응책을 마련하지 않으면 MCI나 스프린트 같은 백본(Backbone)망을 해킹해 미국 전체의 인터넷을 마비시키겠다는 협박을 한 것으로 외신은 보도하고 있다. 1998년 6월 인도가 핵실험을 단행한 직후에는 네덜란드와 영국의 대학생들이 인도 핵무기연구소의 웹사이트에 핵무기를 상징하는 버섯구름 사진을 게재해 놓았으며, 1998년 9월에는 포르투갈의 해커들이 인도네시아의 40여 개 주 컴퓨터에 침입, 최근 국제사회의 이목을 집중시키고 있는 동(東)티모르 해방을 주장하고 인도네시아의 인권상황을 비난하는 웹사이트와 연결된 하이퍼텍스트를 만들어 놓기도 했다.

47) http://www.terrorism.or.kr

48) http://user.chollian.net/~jy1010/cyberwar/news-1-1.htm 미국은 전쟁 개시 10일전 이라크로 수출하는 프린터 안에 컴퓨터 바이러스를 집어넣었다. 이라크는 전운이 감돌자 전쟁 채비를 갖추기 위해 컴퓨터와 그 주변기기를 수입했다. 프린터 안에 숨어든 바이러스는 미국을 비롯해 서방 국가의 전폭기들이 출격하는 날 활동을 개시했다. 잠에서 깨어난 컴퓨터 바이러스는 이라크 전산망 안에서 엄청난 속도로 복제되었다. 연합군 전폭기가 바그다드 상공에 도착했을 때 이라크 방공망은 마비되기 시작했다. 컴퓨터 지시에 따라 발사 되어야 할 이라크 대공 화기는 손으로 조작되어 정확성이 매우 떨어졌다. 미국 공군을 비롯해 연합군 비행기의 손실이 적은 것은 그 때문이었다. 미국은 이에 그치지 않고 이라크 사담 후세인이 군대를 지휘할 수 없게 만들었다.

정보시대에는 노동이나 자본의 투입량보다는 지식과 정보의 축적과 효과적인 활용이 경제발전의 핵심역할을 수행한다. OECD 국가들의 경우 지식기반산업은 총 부가가치액의 평균 34%를 차지하고 있다.[49] 정보화가 진행되면서 다양한 정보가 전산화되어 Network상에서 접근가능한 곳에 보관되어 있다.

전자정부로 인하여 국민들이 다양한 편리성을 누리게 된 반면 Cyber terror의 위협에 노출될 우려가 있는 다양한 정보자원이 생산되었다. 전자정부의 출범에 의해 다양한 업체들이 정부관련 정보를 보유하게 되었으며, 따라서 기업과 정부간의 정보공유가 일어나게 되었다. 중요정보에 대한 보안이 정부의 조치만으로 불가능한 상태가 된 것이다. 그러나 국내기업의 고급정보에 대한 보안조치는 초보적인 수준이거나 거의 무방비상태인 것으로 볼 수 있다.

다양한 정보를 보유한 인터넷 기업들이 수많은 개인 정보를 이용하여 기업의 이윤을 창출하고 있다. 기업의 이윤이 개인정보의 양으로 결정되는 것이다. 대형 인터넷기업들이 보유한 개인정보의 수준은 <표 6>에서 보는 바와 같이 국가정보의 수준을 능가하는 양질의 정보인 것으로 나타나고 있다.

의료기관의 경우 모든 병원이 외부와 분리된 별도의 자체전산망을 보유하고 있으며 특별히 관리하고 있다고 하여도 내부에 침투한 Cyber terror리스트의 활동에 의하여 변조, 삭제, 오용될 확률은 여전히 존재한다고 할 수 있다.

금융망 역시 외부인에 의한 해킹 이외에도 가끔 내부자에 의한 범죄가 발생하는 것을 보면 Cyber terror의 안전지대로 볼 수는 없다. 잔금 인출이나 이체 정도에 끝나지 않고 망 자체를 마비시키는 바이러스를 유포할 수도 있으며, 이 바이러스에 Timer를 장착하여 일정 시간 후에 동작하도록 할 수도 있기 때문이다.

보안관련 규정이 있어도 준수하기가 쉽지 않거나 지켜도 해커의 침투로부터 완전히 자유롭다고 할 수 없다. 이렇게 기존의 중요시설에 추가하여 최신의 기술자료나 수백만에서 수천만명의 고객관련 자료를 관리하고 있는 신규 정보관련 시설이 중요시설에 편입되지 못하고 있는 것이 현실이다. 기업은 필요에 의해 장비를 구입하고 자료를 보관하고 있으나 법규가 시기적절히 대응하지 못함으로 인하여 사실상 국가적 보안의 사각지대에서 방치되고 있음을 부인할 수 없다. 또한 벤처에 대한 지원자금의 단절로 수많은 벤처기업이 기술이나 자금부족 등 여러 가지 사정으로 폐업하면서 유출된 자료는 통계가 없어 확인조차 되지 않고 있는 실정이다.

그 외에도 다양한 기업체들이 평범한 수준의 Cyber terror에도 속수무책으로 공격당하고 있는 실정이다. 정보통신부는 2001년 8월 21일부터 32개 주요민간기업 정보시스템을 대상으로 실시한 모의 Cyber terror훈련 결과 국가 안보 및 국민 경제에 중대한 영향을 미치는 금융·통신·일반 대기업 등 주요 민간기업의 상당수가 해킹·바이러스 등 Cyber terror에 거의 무방비 상태인 것으로 드러났다고 밝혔다. 더우기 이번 훈련은 사전에 대상

49) 정보통신부, 전게자료, p. 2.

기관들에게 통지해 일정과 공격시 대응요령, 훈련방법 등을 구체적으로 교육한 뒤 실시됐음에도 불구하고 각종 허점들이 노출됐다는 것은 이들의 보안관념이 어느 정도인가를 말해준다. 침입 탐지의 경우 1시간 이내에 침입 사실을 파악해 보고한 곳은 6개 업체에 불과했다. 2~3시간 이내 침입사실을 보고한 곳은 3개 업체이며 11개 기업은 3시간 이후에 보고했다. 또 5개 기업은 침입차단시스템이 설치되어 있지만 시스템이 워낙 취약해 손쉽게 침입할 수 있는 것으로 조사됐다. 금융 1곳, 통신 4곳, 일반 대기업 7곳 등 12개 기업은 침입 사실조차 파악하지 못했으며 준비도 소홀했던 것으로 조사됐다. 다른 5개 기업은 해커가 시스템의 중요한 정보를 손쉽게 빼낼 수 있을 정도로 취약했다. 컴퓨터 바이러스에 체계적으로 대처한 곳은 11개 업체에 그쳤다. 나머지 가운데 2개 업체는 모의 바이러스에 감염됐으며 11개 업체는 단순히 삭제만 하고 별도 조치를 취하지 않았고, 8개 업체는 전혀 대응조차 하지 않았다.[50]

보안제품을 개발하는 업체의 난립도 보안제품 시장의 형성을 가로막는 원인중의 하나이다. 현재 보안업체들은 몇몇 업체를 제외하고는 소규모의 다수 업체가 난립하고 있는 실정이므로 동종의 제품이라도 다양한 종류가 출시되어 인터넷 업체에서는 어느 제품을 사용하는 것이 좋은 것인가에 대하여 판단하기가 매우 어려운 실정이다.

3) 개인정보의 유가치화 및 중요성에 대한 인식부재

개인정보는 단순한 개인정보가 아니다. 인터넷 기업의 경우 개인정보를 이용하여 상상할 수 없을 정도의 가치를 창출할 수 있다. 따라서 개인정보가 단순한 개이정보가 아니며, 기업의 입장에서 보면 이윤창출의 원천인 것이다. 인터넷 시장은 User 수가 곧 기업의 Value이며, 이 기준을 근거로 기업의 가치가 결정되는 것이다. 따라서 개인정보의 위상이 종전과 달라진 것이다.

각 인터넷 기업들이 가입자들에게 사실상 필요치 않은 정보까지도 다량으로 요구하고 있으며 초기에 인터넷에 게재된 정보가 유출될 수 있음에 대한 지식이 없고 사이트의 보안실태를 잘 모르는 사용자들이 업체가 요구하는 정보를 다량으로 입력하였다.

〈표 9〉 개인정보의 가치 변화

과거 : 국제정보 > 국가정보 > 사회정보 > 기업정보 > 개인정보
현재 : 국제정보 = 국가정보 = 사회정보 = 기업정보 = 개인정보

이러한 자료를 업체에서 상업적인 목적에 이용하는 것도 본인의 허용을 득한 상태에서 가능하다고 볼 것이나 보안조치를 소홀히 하여 Cyber terror를 당함으로 문제시되었을 경

50) 대한매일, 2001. 8.24, 01면, 대기업 Cyber terror '무방비'.

우 대규모의 사용자들로부터 집단 민사소송을 당할 우려마저 제기되고 있는 실정이다. 실례로 2000년 말 650만명의 개인정보유출사건이 있은 지 불과 5개월도 안되어 780만명의 개인정보가 유출되는 사건이 발생했다. 유출 정보 중에는 성명, 주민번호, 주소, 연락처, e-메일주소 등 개인 신상정보 뿐만 아니라 신용카드번호, 은행계좌번호 또는 현금카드번호가 포함된 금융정보 및 연봉 등 소득 관련정보를 포함한 매우 심각한 수준의 정보가 포함되어 있었다. 보안이 곧 그 회사의 전부라고 할 수 있는 국내의 모든 신용카드회사와 연결돼 있는 신용카드결제 승인처리 업체가 크래킹을 당한 것이다. 그런 정도의 보안 의식을 갖고 있는 회사에 신용카드 영수증 복권 관련 업무를 의뢰한 국세청의 보안의식 역시 미비한 점이 있음을 추정할 수 있다.[51]

그러나 빈약한 보안의식에 비하여 해킹관련 사이트를 보면 해킹방법을 적나라하게 게재해 놓았으므로 이러한 분야에 약간만 관심이 있는 사람이라면 금방 습득할 수 있도록 되어 있다. 실제로 이러한 사이트는 empas에서 hacker를 주제로 검색하면 2001년 10월 9일 현재 3,015개의 사이트가 나오며, 다른 Site에서 검색하면 수백개에서 수천개의 자료가 나오는 바 그 중에는 상당히 고난도의 Hacking 기법을 소개한 사이트도 다수 존재하고 있다.

전문가의 경우 자신만의 사이트를 운영하면서 회원제로 가입을 받아 운영하나 엄선하여 가입시키므로 일반인들이 내용을 확인한다는 것을 불가능한 경우도 있다. 이처럼 해킹실력이 향상되면서 해킹이 용이하게 되자 해커들간 자유롭고 빠른 정보 교환으로 해킹기법이 점점 지능화되고 있으며, 정보시스템 운영자가 적절히 대처할 방법을 강구하기 어려울 것으로 분석된다. <표 11>의 예를 보면 Game site에서 해킹을 할 수 있도록 프로그램을 보내달라는 요청이다. 본 내용 중에는 해킹과는 무관한 Site 게시판에 올라와 있는 내용도 있다.

〈표 10〉 해킹관련 동호회 게제사례 1

해킹 초보입니다...중수님이나 고수님덜 필독! 절세미남 2001/04/28 12:38:44:107 0 내용 음...아직 초보인데여 제가 어제 첨으로 schoolbus 를 사용해보았는데요 게임방에 하라구 메뉴얼에 적혀있더군녀...근데 이거 역추적당하나요?? 글구 v3가 있스면 실행두 않되여?? 어떻하면 조심스래 역추적 당하지 않구 하는지 궁금하구여~ 그리구 스쿨버스처럼 그 컴에 가서 깔아놓지않구여~ 고수님들 처럼 ip만알아두 상대방 컴을 해킹하는법을 알구 싶습니다... 부디 고수님들 갈켜주세요~~

51) http://www.privacy.or.kr/

〈표 11〉 해킹관련 동호회 게제사례 2

[초보팁]메일을 통해 IP주소 알아내기..^^;;
IP주소 알아내기
이건 많이 알려지지 않은 정보입니다.
이 예기 할라고 이 글을 쓰는지도 모릅니다.
상대로 부터 E-Mail을 받는 것입니다.
(아웃룩을 예로 설명하자면)받은 이메일을 아웃룩으로 열어 보세요..
그리고는 [다른이름으로 저장] 해서 eml파일로 저장을 합니다.
그리고 eml파일을 메모장으로 열어 보면.. E-mail의 소스코드를 볼 수 있습니다.
소스코드 맨 위에 보낸 사람의 IP가 팍팍팍 적혀 있습니다.
그러니까 상대로 부터 E-mail을 유도하는 것이죠~
제가 최근들어 즐겨 사용하는 방법입니다.
(꼭 이런식으로 하지 않아도 멜의 등록정보를 보면 소스를 보는거나 같져)
완전 초보들의 경우는
이멜 날라온것을 오른쪽 버튼 클릭해서 등록정보를
누르면 자세히라는 탭이 있는데 그것을 보면 맨위에
아피 주소가 나와 있습니다

〈표 12〉 해킹관련 동호회 게제사례 4

백신에 안걸리게 프로그램에 합쳐서 보낼순 업산요(백오리피스)
백신에 안걸리게 합칠수는 없나요?
합쳐서 보냈더니 백신에서 바이러스 있다고 잡아서 치료해 버리던데요..
즉, 싫패했다는 이야기죠...

자료 : http://www.hackerslab.org/cgi-bin/board/freebrd/freebrd.cgi

워싱턴 아메리칸대 전략 연구 전문가인 에밀리오 바아노씨가 최근 미국 뉴욕 테러의 수사방법에 대해 언급한 바를 보면 "미 정부는 정보수집, 감시, 현장 덮치기 및 공격, 전화통화 및 e-메일 가로채기, 공항 감시등의 방법을 총동원할 것"이라고 말했다. 그만큼 수사선상에서도 이제 e-Mail은 중요한 단서로 부상한 것이다.[52] 그만큼 e-Mail에 대한 보안도 중요한 상태로 볼 수 있으나 개인들의 e-Mail에 대한 보안 Mind는 아직 빈약하다고 볼 수 있다. e-Mail 역시 해킹에 취약한 구조를 가지고 있어 개인의 비밀이 유지된다는 보장이 없다고 할 수 있다.

52) 한국일보, 2001. 9. 27, 08면.

Ⅳ. Cyber terror 대응방안

이러한 다양한 방법의 Cyber Terror에 대하여 국가적 차원의 대응은 물론이고, 기업 자체과 개개인의 대응조치가 조화롭게 이루어져야 Cyber Terror에 대하여 어느 정도 대비를 하였다고 할 수 있을 것이다.

1.국가적 차원의 대응

미국은 지난 95년 Cyber Terrorism 전담팀을 설치하고 2002년까지 32억 달러의 예산을 배정해 놓고 있으며, 빌 클린턴 미국 대통령은 사이버 테러리즘을 비롯한 공격에 대비해 28억 달러의 추가 국방 예산을 투입할 것을 공표하였다.

국내의 사이버 테러 방지 대책은 전반적으로 아직 미미한 수준이라고 볼 수 있다. 그러나 최근 국방부, 국가정보원, 정보통신부 등 관련 부처와 민간 전문가로 구성되어 사이버 테러리즘 진압과 예방임무를 수행할 특수팀을 연내에 창설할 것으로 알려졌다. 늦은 감은 있지만 사이버 테러리즘에 대한 철저하고도 체계적인 대응과 방어책을 마련하여, 정보화 강국으로의 도약을 준비해야 할 것이다.[53]

〈 표 13 〉 미국의 Cyber terror 대응계획

개요	PDP(Presidential Decision Directive) 63을 발효 이래 2000년 1월 CIP(Critical Infrastructure Protect) 능력 확보를 위한 청사진을 제시하고자 CIAO(Critical Infrastructure Assurance Office)를 통해 국가차원의 계획서 발표	
목표	1. 준비,예방	미국의 주요정보 Network에 대한 명백한 공격가능성을 최소화하고, 공격을 당하더라도 지속적으로 운영될 수 있는 기반구조 건설 (Program 1)
	2. 탐지,대응	미국의 주요기반구조에 대한 공격을 즉각 식별하고 평가하는데 필요한 수단을 개발하는 것이며, 피해복구와 피해 시스템 재구축 포함 (Program 2-5)
	3. 강력한 기반구축	미국의 주요정보 Network에 대한 공격에 대비하기 위한 준비 및 예방과 탐지 및 대응책 수행에 기반이 되는 국가적 차원의 활동 수행 (Program 6-10)
Program	Program 1	보호대상과 상호의존성 파악 및 취약성 평가
	〃 2	공격 및 침입탐지
	〃 3	첩보 및 법적 대응능력 확보
	〃 4	경보 및 정보 공유
	〃 5	대응, 재구성 및 복구능력 확보
	〃 6	연구 개발
	〃 7	전문가 확보
	〃 8	홍보
	〃 9	Program 1-8을 수행하기 위한 법률적 지원
	〃 10	개인의 권리와 사생활 보호

53) http://www.terrorism.or.kr

자료 : 김천근, "취약점 분석기술", 국방정보마비·보호체계 발전 세미나 자료집, 2001. 6. 22. p. 7.

정부는 이에 따라 2001년 7월 정보통신기반보호법 시행에 맞춰, 정보보호책임관 제도를 도입하고, 장기적으로 정보보호직을 신설해 전담인력을 충원할 방침이다.[54] 이러한 계획에 따라 정통부는 대학내 정보보호연구센터 5곳과 정보보호 관련 학과 및 커리큘럼 개설을 지원하는 등 총 70억원을 투입해 고급인력 300명, 일반인력 4000여명을 양성할 계획이다.

한국정보보호센터 등에도 장·단기 정보보호교육과정을 개설해 산업체 정보통신인력에 대한 전환교육을 실시하고 있으며 유사시 Cyber terror에 대응할 수 있는 기술봉사요원을 확보한다는 방침을 정하여 시행중이다.[55] 또한 미국 테러사태로 우려되는 Cyber terror에 대응하기 위해 4,000여개 예·경보망을 통한 Cyber terror 경보시스템을 가동하고 있다고 2001년 9월 18일 밝혔다. 이에 따라 관계기관들이 24시간 비상대기 지원체제를 운영하고 바이러스백신을 적기에 개발·공급할 수 있는 공조체제를 유지해 나가기로 하였다고 한다. 이러한 System이 정부의 전 기관과 합동으로 효율적으로 운영되어야 할 것이다.

국방, 행정, 금융, 통신, 항공 등 주요 정보통신기반 시설에 대해선 국가정보원과 공동대응 체제를 구축했다. 이를 위해 정통부는 정보통신특별대책반을 구성하였다[56]고 하는 바 장기적인 면에서 본다면 총리산하에 실권을 부여하여 전방위적인 조직화할 필요가 있다. 이 같은 해킹피해를 막으려면 대규모 정보통신기반시설을 갖춘 기관·기업 ·단체에서는 침입차단시스템과 침입탐지시스템 등 정보보호제품을 반드시 설치하고 효과적인 해킹방지 프로그램을 사용해 지속적으로 점검하는 것이 필요하다.

2.기업차원의 대응조치

기술개발 관련 자료나 인사자료, 경영관련 자료 등 유가치하거나 보안이 필요한 기업 정보를 Cyber Terror로부터 방어하기 위하여는 다양한 보안대책을 강구하여야 한다. 가장 완벽한 대책은 Network에서 분리시키는 것이나 사실상 Web에 올려져 있는 동안에만도 다양한 중요정보들이 있어 완벽한 것은 아니다.

국내의 인터넷 보안관련 기술수준은 상당한 정도에 이른 것으로 분석되고 있으며, 중국 등지에 진출하여 기술력을 인정받고 있다. 이러한 보안관련 기술 중에는 F/W나 IDS 등 기본적인 기술 이외에 다양한 기법이 개발되어 시판되고 있다.

이러한 보안기술을 I후발국으로 수출함으로서 국내시장에서만 출혈 경쟁을 하는 일이 없어야 할 것이다. 이러한 방법을 모색할 수 있도록 정부차원에서 바람직스런 수출목표와 정책을 강구하고 업계에서 이 목표를 완수할 수 있도록 독려하는 것이 필요할 것이다.

---

54) 조선일보, 2001. 1. 31.
55) 동아일보, 2001. 5. 30, 38면. 정보통신 / 해커에도 햇볕정책.
56) 대한매일, 2001. 9. 19, 27면.

정보보호진흥원 CERT-CC에서는 미국과 아프카니스탄의 전쟁으로 국내 사이트에 대하여 Cyber terror의 가능성이 있으며, 특히 국내 정보시스템이 분산서비스거부공격 등 공격의 경유지로 이용될 가능성이 있으므로 시스템관리자는 1.정보시스템에 대한 백업 등 재난복구 계획 마련, 2.정보시스템에 대한 보안 안전진단을 실시하고, 3.분산서비스거부공격 등 해킹 및 바이러스공격에 대비한 모니터링 체제 강화를 하여야 하며, 개인 PC사용자는 PC에 바이러스 감염여부를 백신으로 점검 및 치료를 하도록 권고하고 있다.[57] IT가 발전한 만큼 이러한 분야는 정부의 홍보가 없이도 스스로 알아서 할 수 있도록 되어야 할 것이다. 기업체에서 필요한 정보보안관련 인력을 양성하는 것도 시급한 과제중의 하나이다. 하지만 이러한 인력양성이 단기간에 되는 것은 아니다. 고급 기술을 익히려면 적어도 10여년에 걸쳐 다양한 이론과 실기를 익혀야 한다. 따라서 이러한 인력을 해당기업에서 양성하여 배치하기 보다는 2001년 현재 200여개에 달하는 인터넷 보안업체를 선정하여 서비스를 받는 것이 보다 신속한 조치를 가능하게 하는 방법이다.

따라서 장기간에 걸친 인력양성을 위하여 정보통신부는 전국 대학이 동아리 지원을 현재의 45개에서 더욱 확대 선정하고 활동예산도 현재의 800만원보다 더 많은 예산을 지원할 수 있어야 할 것이다. 이러한 조치는 앞으로 계속 다양한 방법으로 연구검토되고 정부와 업계 등에서 공동으로 인력을 양성하는 방향으로 발전되어야 할 것이다. 이 동아리를 일정한 조건하에 타이커팀으로 활동시키는 등 다수의 초보적인 실전 프로젝트에 참여하게 하여 경험을 축적하는 것도 중요할 것으로 생각된다.

인력양성 이전에 기존의 개발된 서비스를 강화하는 것도 필요하다. 2001년부터 주요 정보통신기반시설에 대한 정보보호컨설팅을 전문으로 지원할 정보보호전문업체 지정작업이 본격화된다. 정보통신부는 정보보호 전문업체의 지정심사에 관한 종합 계획을 확정하고 2001년 9월17일부터 9월22일까지 신청을 접수하였으며 10월 현재 심사중이며 11월중 지정서를 교부할 계획이다.

정보보호 전문업체는 정보통신기반보호법에 따라 국가적으로 중요한 정보통신기반시설에 대한 취약점 분석 및 보호대책 수립업무를 지원하는 업체로, 정통부장관으로부터 지정받아야 하는 바 정보보호 전문업체로 지정받으려면 일정 요건[58]을 만족해야 한다.[59] 이러한 기준이 실효를 거두기 위하여는 각 보안업계가 국제적 기준에 적합한 양적, 질적 수준을 구비하도록 다소 엄격한 규정을 적용할 필요가 있다.

이 외에도 세계 최고 수준의 보안기술을 개발하고 익힐 수 있도록 다양한 기준을 만들어 이 기준에 관련학과와 업체들이 적응할 수 있도록 하는 것도 중요하다. 선진 외국의 경

57) http://www.certcc.or.kr/announce/20011008_popup.html

58) 기술인력 15인 이상, 자본금 20억원 이상, 신원확인 및 출입통제설비 등을 갖추는 것 외에도 정통부장관이 실시하는 업무수행능력심사에서 70점 이상 취득 등

59) http://www.inews24.com/php/news_view.php?g_serial=43222&g_menu=080200&pay_news=0&list_page=1

우 정부가 사전에 장기적인 목표를 설정하므로 관련 분야의 제반 사정을 고려하여 목표를 설정하고 이 목표를 업체가 달성하도록 독려함으로서 신속한 발전을 할 수 있도록 유도하는 것이 필요하다고 하겠다.

3. 개인차원의 정보보안조치

최근에는 해커들이 다양한 방법으로 타인의 전자우편까지도 Hacking하고 있는 것으로 알려지고 있다.[60] 따라서 개인정보침해에 대한 대응은 각 개인들이 스스로 가능한 방법을 전부 동원하여야 한다.

ID나 어떠한 경우에도 다른 사람에게 알려주거나 노출하여서는 안되며, 이름, 주민등록번호, 전화번호, 주소 등 추측해 내기 쉬운 단어나 숫자를 사용하여 만들어서도 안된다. PW는 주기적으로 변경하고, 이러한 DB를 기록한 서류는 다른 사람이 발견할 수 있는 장소에 기록해 두거나 놓아두어서는 안된다. 또한 이용자는 타인이 자신의 ID 및 패스워드를 이용하도록 해서는 안되며, 다른 사람의 ID를 사용해서도 안되도록 하고 있다.

한국의 경우 주민증록번호와 금융실명제라는 두가지 제도로 인해 모든 국민이 크래킹의 위험에 그대로 노출되어있다. 정부는 국민들에게 자신들의 행정편의주의를 위해 주민번호를 부여하고 관리를 하지만 이로 인한 부작용과 위험에 대해서는 국민 각자의 위험부담을 안을 것을 요구하고 있다. 특히 인터넷 사이트들은 이런 정부의 행정편의주의에 편승하고 상업주의와 결탁하여 제대로 관리도 못하는 개인정보를 받아 사용자들을 위험 속에 빠트리고 있는 것이다.

정부는 이런 대규모 개인정보 유출에 대해 고작 비밀번호를 수시로 바꾸고 생년월일이나 전화번호를 비밀번호로 사용하지 말라는 정도의 유치한 수준의 크래킹 방지 방법을 홍보하고 있다. 구조적인 문제로 발생하고 있는 정보유출 구조에서 비밀번호를 아무리 바꾸고 어렵게 써봐야 별다른 도움이 될 것 같지 않다.

정부가 온라인 시대에 걸맞도록 일반적인 다른 선진국가처럼 주민등록번호 같은 제도를 철폐하고 금융실명제에 대한 디지털적인 재정비를 하는 것이 이런 사건을 방지하는 기본적인 바탕을 만드는 시초라고 생각되며 각 사이트들도 실제로 사이트 운영을 위해 주민번호와 같은 개인정보를 반드시 받아야 하는지에 대한 고민이 필요한 시점이다.[61] 개인 컴퓨터 사용자들이 자신의 PC를 방어할 수 있는 해킹방지책을 사용해 보는 것도 좋다.
해킹방지 SW를 설치하고, 트로이 목마 등 Hacking 프로그램을 조심하며, 외국SW 평가판을 함부로 설치하지 않고, e메일은 암호화해서 전송하는 등의 다양한 방법이 Web상에 올라와 있으므로 약간의 관심만 있으면 얼마든지 자위조치를 취할 수 있다.

---

60) 한겨레, 2001. 10. 8, 20면.
61) http://www.privacy.or.kr/

V. 결 론

테러는 항상 당시의 환경에 의해 그 수단이 변경되어 왔다. 기존의 테러가 전통적인 무기와 방법을 사용하여 자행되어 왔으나 최근 테러는 최근의 무기를 사용하여 테러를 행해왔다.

2001년 9월 뉴욕 무역센터 등의 대한 테러는 설계목적상 무기가 아닌 일반 장비를 이용하여 테러를 하였으며 이러한 방법에 의한 테러는 과학의 발전에 따라 고효율의 에너지가 집적된 시설이나 장비있는 한 사전탐지가 어렵고 그 결과는 훨씬 더 위력적임을 말해준다. Cyber terror 역시 전통적인 Hacking Tool의 사용에서 벗어나 일반 관리자들이 기기관리상 사용하는 Tool이 Hacking에 사용되거나 관리자가 Hacker에게 권한을 탈취당하였을 경우 보다 위력적인 해킹도구로 사용될 수 있음을 보여주고 있으며 실제 해킹 역시 이러한 방법으로도 이루어지고 있다.

바이러스도 기존의 단순한 기능만이 아닌 강력한 전파기능이 추가되거나 해킹기능이 추가된 상태로 최단시간내에 확산될 수 있도록 설계되어 유포되고 있다.

정보시대의 Cyber terror는 연령이나 복장 등에 구애받는 것도 아니며, On Line에 연결된 PC 한 대만 있으면 어느 장소에서 언제든 가능한 것이다. 이러한 위험성을 가지고 있음에도 국내 사이트의 대부분은 중요 자료가 보관되어 있지 않음을 기화로 보안조치를 하지 않은 경우가 대부분이라고 할 수 있다. 심지어는 수백만에서 천만 이상의 회원이 가입한 Site를 운영하고 있는 회사마저도 예산을 이유로 보안조치에는 소홀한 경우가 있으며 이러한 기업이 보유하고 있는 정보가 해킹을 당해서 유출된다는 것은 국가가 보유하고 있는 행정자치부 주민전산망보다 등급이 높은 정보가 유출됨을 의미한다.

많은 수의 기업이 운영부실로 기 가입받은 고객의 정보를 고의 또는 과실로 유출시키거나 정리해고된 기업의 근로자들이 자신이 근무하던 기업체의 고객 DB를 불법유출하여 음성적으로 거래하고 있음도 역시 정보사회의 우려할만한 역기능 중의 하나라고 할 수 있다. 사이버상의 테러가 아닌 기존의 방법으로도 정보통신망에 테러를 가할 수 있는 많은 방법이 있으며, 이러한 부분에 대한 조치를 게을리 한다면 Cyber terror보다 더한 위협이 될 수 있다. 사이버 테러는 백업된 자료의 복원이나 기타 프로그램상의 조치로 순식간에 복구가 가능할 수 있으나 정보통신망 자체에 가해진 물리적인 테러는 복구에 시간적 여유를 필요로 할 뿐 아니라 불가능한 경우도 생각해 볼 수 있다.

On-line상에서 이루어지는 Terror는 Network에 연결되어 있는 한 취약시간과 장소가 지정되어 있는 것이 아니며 24시간, 어느 장소에서도 이루어 질 수 있다. 따라서 모든 시간대, 모든 컴퓨터에 대하여 대테러대책이 이루어져야 한다.

Cyber terror에 대한 민간의 대응력을 높임은 물론 정부 차원에서도 다양한 대응책을 강구하여야 할 것이다.

우선 최초로 Cyber terror 상황에 접하는 KISA나 경찰의 Cyber terror 대응능력이 저하될 경우 사이버범죄의 시간적 특성상 증거보건이 곤란하므로 범행의 증거를 확보할 수 없는 경우가 있을 수 있으며, 이 후 검찰이나 법원에서는 시간 관계상 증거확보가 더욱 곤란하여 죄를 범한 범인을 알면서도 증거불충분으로 처벌하지 못하는 사례가 발생할 우려가 있다. 따라서 경찰이 Cyber terror에 효율적으로 대응치 못할 경우 검찰, 법원에서 유죄판결이 어려운 법집행체제의 도미노현상이 발생될 우려가 있다고 할 수 있다. 이러한 제도적인 면은 정부 각 부처가 전체가 합심하여 대처함으로 시너지를 창출할 수 있도록 하여야 할 것이다.

參 考 文 獻

▣ 국내문헌

국정원, Cyber terror 대응정보보안교육 교재, 2001. 04.
김천근, "취약점 분석기술", 국방정보마비 · 보호체계 발전 세미나 자료집, 2001. 6. 22.
김효식, "Cyber terror 어떻게 대처할 것인가?", 제2편, 새천년민주당 국회의원 연구보고서,2001.
박명순, 컴퓨터 바이러스 분석, 제작 및 처방, 서울: 집문당, 1992.
이요섭, 공무원정보보호심화과정 교재, 서울: 정보통신교육원, 2001.
장승권, 정명호, 김영수, 인터넷 지식벤처의 성공조건, 서울 : 삼성경제연구소, 2000.
정보보호진흥원, 2001년 상반기 해킹 · 바이러스 분석 보고서, p. 28.
정보통신부, Cyber Korea 21, 창조적 지식기반국가 건설을 위한 정보화 Vision, 1999.
조완수, "사이버테러 활용 및 대응기술", 국가보안기술연구소 주최 제1회 정보보증기술심포지움 자료집, 2001.
행정자치부, 전자정부의 이해와 해설, 2001.
Paul Budde Communication, Global Internet Market-Statistics Overviews, 2001.
http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=188&page=3&tempfilename=sdataV.html
http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata_main&=index=239&page=1&tempfilename=sdata_mainV.html
http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=186&page=3&tempfilename=sdataV.html
http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=213&page=2&tempfilename=sdataV.html
http://e-campus.co.kr
http://www.terrorism.or.kr
http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=186&page=3&tempfilename=sdataV.html
http://www.boani.com/secui/src/info/shield_detail.jsp?nodeid=231&order=hit+desc&expertid=331&rsc=1&rscid=981331705370&page=1
http://user.chollian.net/~jy1010/cyberwar/news-1-1.htm
http://www.terrorism.or.kr
http://www.stockpia.com/its/review/view.asp?flag=&no=10&page=1&spage=1&keyword=

http://www.netvalue.com/
http://www.marketcast.co.kr
http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=186&page=3&tempfilename=sdataV.html
http://www.nic.or.kr/cgi-bin/EnterBoard2/enboard.cgi?ActionID=12&dbname=sdata&index=186&page=3&tempfilename=sdataV.html
http://www.privacy.or.kr
http://www.boani.com/secui/src/info/shield_detail.jsp?nodeid=231&order=hit+desc&expertid=331&rsc=1&rscid=981331705370&page=1
http://www.inews24.com/php/search_news_view.php?g_serial=45252&g_menu=080400&pay_news=0
http://www.hackerslab.org/cgi-bin/board/freebrd/freebrd.cgi
http://www.certcc.or.kr/announce/20011008_popup.html
http://www.inews24.com/php/news_view.php?g_serial=43222&g_menu=080200&pay_news=0&list_page=1

ABSTRACT

Countermeasures against Cyber terror in Korea

by An, Chang Hoon

Koreans are the most avid Internet surfers in the world according to Nielson/NetRatings(Reuters, August 2001) and most Internet connections are made through high-speed connections like Digital Subscriber Lines (DSLs). The result of such internet fervor is a nation that is fertile in both hackers and software companies (over 200 in the field of network security alone).

However, by-product of Internet activity is cyber crime and the need to protect innocent users from the dangers of cyber criminals and cyber-terrorists be they are individuals or organized groups. Hence the Cyber Terror Response Team (CTRT) was organized in late 2000 with the mandate to fulfill that role. In these contexts, this study analyzes the actual conditions of cyber terror and suggests the countermeasures against cyber terror in Korea.