Cyber Terror의 체계분류 및 경호경비대책 방안

김 두 현 *

◇ 목 차 ◇

Ⅰ. 서 론

한반도를 중심으로 주변국이 모두 정보화사회가 완성되는 2020년 전후에는 국가능력의 정보기반 의존성이 심화되므로써 테러목표가 산업기반 및 군사시스템이기보다는 상대국의 정보기반으로 이동될 가능성이 농후하다. 따라서 다가오는 사회를 포스트(Post) 산업사회, 정보화사회, Cyber사회, 컴퓨터사회 등으로 칭하고 있다.[1] 이와 같이 정보화

* 한국체육대학교 안전관리학과 교수, 법학박사

1) 최성빈, "미래 국방과학기술의 혁신적 발전전략", 「21세기 군사혁신과 한국의 국방비전」, 한

된 국가의 총생산성의 80% 이상이 정보기반에서 생산되는 상황에서는 국익을 위해 보호되어야 할 자산은 이제까지와 같은 물리적 산업기반이기보다는 정보기반이 되어야 할 것이다.

정보시대의 테러는 컴퓨터, 센서, 통신, 위성에 의한 정보관련 기계의 우열이 좌우하게 될 것이기 때문에 해커가 테러대상의 정보시스템을 마비시키고 파괴하는 기술을 프로그램화하여 통신시스템에 침투하여 그것들을 마비시키는 것은 물론 2002년 월드컵축구대회를 개최하는 우리로서는 월드컵 데이터베이스 및 위성방송통신체계 파괴 등 대참사를 촉발할 가능성에 대비 하여야 한다.[2)]

이미 세계 120여개국 이상이 국가정보 기반구조를 타격할 수 있는 능력을 보유하고 있으며, 일부국가는 국가정보 기반 타격을 계획 중인 것으로 분석되고 있다.

미국의 경우 사이버 테러 대비를 위한 대통령직속의 특별위원회를 설치운영하고 있으며, 중국도 지난 1997년 4월부터 컴퓨터 바이러스부대를 창설한 것으로 알려지고 있다.[3)]

특히, 1998년 5월 김대중대통령이 일본을 방문했을 당시 나리타공항에 무선 해커가 출몰하여 이·착륙하는 항공기들이 추락사고의 위험에 노출되었다는 사실이 밝혀져 우리들을 놀라게 했다.[4)]

매년 기하급수적으로 증가하는 사이버 테러와 범죄의 동기는 단순히 실력을 과시하거나 호기심, 장난으로부터 시작하여 금전적 이익 또는 정치적 이상을 실현하기 위한 기업, 국가간의 정보유출에 이르기까지 그 범위가 다양하고, 이처럼 다양한 동기는 불특정 다수에 의한 무차별 침입시 위협을 상존케하기 때문에 불측사태에 대한 최소한의 보안대책이 마련되어야 할 것이다.

따라서 본 논문에서는 사이버테러의 일반적인 개념을 정립하고 사이버테러에 의한 국내·외의 피해사례를 살펴보고, 이에 따른 각국의 대비실태 및 사이버테러에 대한 대비방안을 제시하고자 한다.

국국방연구원, 1998, 582면.

2) 김두현, "2002년 월드컵축구대회에 대한 안전대책", 「경호경비연구(제2호)」, 한국경호경비학회, 1999, 57면.

3) 한 희, "정보전체계의 발전과 한국군의 대비 방책", 「21세기 군사혁신과 한국의 국방비전」, 한국국방연구원, 1998, 267면.

4) 경향신문, 1999. 3. 26일자 2면.

Ⅱ. Cyber Terror의 일반개념과 체계분류

1. Cyber Terror의 일반개념

사이버테러란 Computer가 합성한 가상현실의 세계(Cyber Space)와 가상인간의 영역과 같이 인간체계가 운용되는 공간에서의 테러로서 이는 정보화사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 System 파괴보다는 훨씬 결정적인 손실을 강요할 수 있는 총체적인 가상공간에서의 정보마비를 추구하는 테러수행방식을 의미한다. 즉, 은행이나 기업 등의 전산망을 교란시키거나, 정보를 조작해 재난을 야기시키는 조직적 테러행위로 그 기법으로는 전자우편폭탄(E-Mail Bomb), 서비스거부(Denial of Service), 논리폭탄(Logic Bomb) 등이다.[5]

따라서 국가마다 행정, 금융, 군사 등 제반분야에 관한 중요정보를 Computer D/B화하고 있기 때문에 가상공간 내의 정보 System을 파괴시킬 경우, 국가전체의 통제체계를 순식간에 마비시켜 심대한 결과를 초래할 수 있다. 사이버테러는 오류가 있는 자료를 주입할 경우 컴퓨터의 기능이나 동작이 손상되나 컴퓨터의 외관상으로는 특이사항이 나타나지 않아 운용자는 시스템이 정상이라고 생각되도록 하는 가상공간에서 수행되는 테러의 한 차원에서 미래 테러에서는 가시적 공간의 테러보다는 가상공간의 테러의 중요성이 더욱 증대될 수 있다.[6]

가. 사이버 테러리스트의 분류

사이버 테러리스트란 첨단 정보통신기술을 이용해 전산망을 침투한 해커[7]나 불순한 목적을 가지고 컴퓨터 바이러스를 만들어 뿌리는 행위를 한 자나 집단을 말한다.

사이버 테러리스트들의 테러 대상이 과거에는 대학이나 연구소시스템이었으나 오늘날은 국가안보와 국가기능 유지를 위한 핵심기반체계(비상재해체계, 수도와 연료공급체계, 물류수송체계 등) 및 국민들의 일상생활과 직결되는 의료지원시설망·제약회사·금융기관·군사기지·경찰 D/B·교통신호체계·전화교환체계·식량관련시설·발전소·정

---

5) 김두현, 전게논문, 56면.
6) 합동참모본부, 「합동 VISION 2015 합동전장운영개념서」, 1999, 78~79면.
7) 해커란 원래 컴퓨터시스템의 내부구조 및 동작 등에 심취하여 이를 알고자 노력하는 사람으로서 대개 뛰어난 컴퓨터 및 통신실력을 가진 사람을 가리킨다(한국정보보호센터, 「정보시스템 해킹 현황 및 대응」, 1996, 3면).

부행정기관 등의 파괴 또는 마비는 정치적·군사적(안보적)·경제적인 국가이익을 결정적으로 좌우하게 되는 주요기간시설들을 <표 1>과 같이 테러대상으로 삼고 있다.

<표 1> 대상별 국내 네트워크 테러(침해)현황(1997년도)

구 분	대 학	연 구 소	정부·공공기관	기 업	기 타	계
건 수	32	3	4	25	0	64
비율(%)	50	5	6	39	-	100

자료 : 송광섭, "Internet 관련 범죄의 동향과 그 대책"「경호경비연구(제2호)」, 한국경호경비학회, 1999, 102면.

물론 사이버테러에 의한 사고는 아니지만(실수에 의한 사고) 1999년 9월 30일 미 항공우주국(NASA)의 잠정 조사결과에 의하면 위성에 컴퓨터 자료를 입력시 실수로 파운드 단위를 미터 단위로 바꾸어 입력하여야 할 자료를 잘못 입력함으로써 화성기후관측위성(1억 2천 5백만 달러 : 한화 약 1천 5백억원)을 날려버리는 결과(코스를 96㎞ 이탈)를 낳게 하는 사건이 발생하였다. 이는 컴퓨터시스템에 잘못된 자료입력으로 우주선을 날리는 엄청난 결과를 초래함으로써 컴퓨터 시스템에 대한 관리의 중요성을 강조하는 좋은 계기가 되었다.[8)]

이러한 사이버 테러리스트는 다음과 같이 크게 세부류로 나눌 수 있다.

첫째, 주로 10대 청소년을 중심으로 혼자 활동하는 부류로 이들은 컴퓨터에 탐닉해 사회적으로 소외된 자신의 존재를 알리기 위해 각종 불법행위를 저지른 부류가 있다.

둘째, 범죄조직화 된 엘리트집단으로 스웨덴의 '국제해적단'과 네델란드의 '트라이던트'와 러시아의 '지하 해킹마피아' 등과 같은 대표적인 집단으로 이들은 새로운 기법을 개발해 불법 지하조직들에게 판매하는 극히 위험한 집단이다.

셋째, 정치목적을 갖고 움직이는 집단으로 정체를 좀처럼 드러내지 않는 부류가 있다.

나. 해커의 분류

해커란 다른 컴퓨터에 불법·침입하여 자료의 불법 열람, 변조, 파괴 등의 행위를 하는 침입자·파괴자[9)]를 통칭하여 해커로 부른다. 이러한 해커는 일반적인 해커와 동기에 의한 해커로 분류된다.

---

8) 중앙일보, 1999. 10. 3일자 5면 ; 동아일보, 1999. 10. 4일자 B9면.

9) 침입자(Intruder)·파괴자(Cracker)란 테러대상의 컴퓨터에 전산망을 이용하여 불법으로 침입하여 자료를 유출, 변조, 파괴 등의 범죄적인 행위를 하는 사람을 의미한다(정기태, "해커의 이해와 해킹 대응 방안"「국방정보통신 (제16호)」, 국군지휘통신사령부, 1999, 33~34면).

일반적인 해커는 ① 시스템 탐구 등 자신의 연구목적을 위한 「학구형 해커」와, ② 타 시스템 침입만 시도하는 「침입형 해커」, ③ 시스템 침입 후 자료를 파괴하는 「파괴형 해커」, ④ 상용프로그램 암호를 푸는 「암호형 해커」, ⑤ 비밀 및 개인의 신상정보를 절취하는 「스파이형 해커」로 분류된다.

동기에 의한 해커는 ① 대부분 호기심과 영웅심리에 의한 「단순해커」와, ② 금융망 등을 대상으로 금전적 이익추구를 목적으로 하는 「범죄적 해커」, ③ 주로 내부직원에 의해 이루어진 개인이나 집단의 이익이나 동기를 추구하기 위해서 행한 「내부 불순자 해커」, ④ 혼란 및 파괴를 목적으로 개인이나 그룹이 추구하는 이상을 달성하기 위한 「테러리스트·그룹」, ⑤ 기업의 이익을 추구하기 위하여 경쟁기업의 정보를 유출하는 「기업체고용 해커」, ⑥ 국가의 이익을 추구하기 위하여 경쟁국가 등에서 정보를 유출하는 「국가고용 해커」 등으로 분류한다.[10] 그리고 스스로 시스템의 보안 문제점을 파악하거나 불법 침입프로그램을 작성할 수 있는 능력을 가진 지능형 침입자(Uebecracker)도 있다.

이와 같은 해커들의 사회적 특성을 파악해 보면 다음과 같은 공통적인 면이 있다.

먼저 해커들은 대부분 젊은 층의 남자로 17~30세가 많으며, 학업은 성공적이지 못하였으나 매우 지적이고, 자기분야에서는 정통하다는 점과, 그들 자신은 그들의 행위가 사회에 위협을 주는 존재로 인식하지 않고 있으며, 직업적으로도 컴퓨터 관련분야에서 종사하고 있으며 혼자서 하는 일의 특성을 지니고 있으나 최소한의 조직체로서 활동하는 것이 보통이다. 이러한 조직체(모임)에서는 은퇴한 해커나 보안관계 전문가들을 연사로 초빙하여 강의 및 토론을 하고 있다는 공통적 특성을 가지고 있다.[11]

다. 사이버테러의 수법

미래 테러 환경에서 예상되는 것으로써 목적에 따라 첫째, 대 센서형(antinsensor)으로 인간의 눈 또는 감시용 센서를 무력화시키기 위한 것이 될 것이다.

둘째, 기동성감속형(antimobility) 형태로서 직접적으로 차량 및 항공기 등을 움직이지 못하도록 하거나 이러한 것들의 엔진 등에 손상을 주는 형태가 될 것이다.

셋째, 대 C4I형 (Command, Control, Communication and Intelligence)으로 테러 대상의 통신장비나 정보망을 무너뜨려 경호·경비작용 자체가 불가능하게 하는 것이다.

넷째, 대 기간시설(anti-infra-structure) 무기로서 국가기간시설의 기능을 일시에 마비시키는 것이다.

---

10) 한국정보보호센터, 전게 정보시스템 해킹 현황 및 대응, 4면.

11) 원은상·하광희, "테러집단의 정보전 위협과 안보관련 시사점", 「주간국방논단(제703호, 98-5)」, 한국국방연구원, 1998, 7면.

다섯째, 대인용(antipersonnel)으로 사람에게 직접 영향을 미쳐 활동을 정지시켜 버리는 테러 등이 될 것이다.[12]

최근 고도화된 사이버테러의 수법은 ① 멀리 떨어진 곳에서 사용자 ID나 비밀번호를 알아내는 '스누핑'과 전산운영권을 완전 장악하는 '스푸핑' 등의 해킹수법, ② 사이버 스파이들에 의해 사용되는 수법으로 통신케이블에서 흘러나오는 전자파를 잡아내 그 안으로 전송되는 정보를 빼내는 '벤엑코' 수법, ③ 아일랜드 반군이 중국 금융가에 테러를 계획한 바 있는 프로그램으로 강력한 전파를 발사하여 전산망을 정지시키는 전파무기(고출력 전자총 : Herf Gun)를 사용하는 수법, ④ 강한 전자기를 내뿜는 전자기 폭탄[13]으로 국가통신망시스템·전력·물류·에너지 등의 사회 Infra를 일순간에 무력화시키는 수법, ⑤ 컴퓨터 악성 바이러스로 전산망에 침투하여 중요한 정보를 외부로 유출 또는 해당 전산망을 망가뜨리는 수법으로 최근 개발된 '칼리큘라·코드파기자'와 같은 악성 바이러스 등으로 공격하는 수법 등이다.

특히, 컴퓨터를 잡는 전자폭탄은 터질 때 폭음이나 소리가 없어 「소리 없는 폭탄」으로도 불리는 이 폭탄은 서류가방에도 넣을 수 있는 작은 크기이지만 치명적 파괴력을 가지고 있으며, 폭파대상은 모든 종류의 컴퓨터 회로이며, 고에너지로 순간적으로 마이크로웨브를 발생시켜 컴퓨터 전기회로를 파기하며, 모든 전기회로를 박살낼 수 있다.

즉, 컴퓨터 전기회로는 대부분 논리회로로 이들 회로는 저항기(R : Resistance), 유도기(L : Inductance) 용량기(C : Capacitance)를 바탕으로 구성되어 있다. RLC가 조합된 회로는 고주파를 맞으면 손상된 원리를 응용한 것이다.

2. Cyber Terror의 체계분류

사이버테러의 체계는 크게 「논리폭탄(Logic Bomb)체계」, 「웜(Worm)체계」, 「컴퓨터 바이러스체계」, 「트랩도어(백도어)체계」, 「트로이 목마(TROJAN HORSE)체계」, 「해킹체계」, 「AMCW체계(Autonomous Mobile Cyber Weapons)」, 「소프트 웨어체계 취약성 분석체계」 등으로 분류할 수 있다.

---

12) 신성택, "첨담비살상무기의 개념과 개발동향", 「21세기 군사혁신과 한국의 국방비전」, 한국국방연구원, 1998, 471면.

13) 전자폭탄은 스웨덴 국방과학연구소에서 러시아의 한 기업과 공동으로 컴퓨터 파괴용으로 만들었다. 1기당 100만kW인 10개의 원자력 발전소 전력생산량에 해당하는 1백억와트의 고에너지로 전자폭탄의 마이크로웨브 발사 가능거리는 50m정도이지만 강력한 모델을 만들면 수백m까지 연장이 가능하며, 목표물에 접근하여 소리 없이 폭탄을 발사하면 항공기, R/D기지, 전산센터, 은행, 발전소 등 어떤 목표물이든 그 안에 있는 모든 컴퓨터들을 무차별적으로 없애버릴 수 있다.

가. 논리폭탄(Logic Bomb)체계

논리폭탄체계는 물리적 무기체계의 시한폭탄과 같이 내정된 특정한 임계조건을 미리 설정하거나 명령전달에 의해 상대의 무기체계 및 정보수행시스템에 타격을 가하는 테러(공격)용 사이버무기체계로[14] 상대의 정보를 파괴 또는 왜곡하거나, 하드웨어나 소프트웨어의 동작을 방해한 체계로 ① 테러 대상에 직접 설치하여 작동시키는 「매설형체계」, ② 전자우편 및 원격지 파일 전송과 같은 우회적인 매개 경로를 통해 미리 투입되어 간접적으로 작동되는 「투입형체계」, ③ 네티워크를 통한 해킹에 의해 직접 침투하여 작동시키는 「침투형체계」 등으로 구분할 수 있다.

논리폭탄체계는 평상시에는 컴퓨터 내부에 잠복해 있다가 예정된 시간이나 특수한 명령어가 들어오면 작동하는 도화선 없는 바이러스 폭탄이다. 이는 물리적인 테러가 행해지기 전에 전산망과 통신망, 공항과 항구, 군이나 행정기관 및 경호관련기관의 컴퓨터 시스템에서 논리폭탄이 일제히 터진다면 그 파괴력은 상상을 초월한다. 우선 R/D망이 교란되고 항공기들은 무용지물이 된다. 그리고 통신망은 두절되고 기차가 탈선하거나 정지해 버린다. 병원에서는 혈액관리체계가 엉망이 되면서 응급환자들에게 손도 대지 못하고, 은행과 증권 전산망이 마비되면서 주가가 폭락하고 고객들의 예금액이 사라지며 순식간에 공황이 번지면서 극심한 사회 혼란 속에 빠져들 것이다.

나. 웜(Worm)체계

웜체계는 초급 소프트웨어 무기로 상대의 무기체계 및 정보 수집시스템에 직접적인 영향을 미치지는 않지만 자원의 사용을 남용하여 자신을 계속 복제하여 정상적인 운용을 마비시키고 교란을 획책하여 무력화시키는 교란용 사이버무기(Cyber Weapon)체계로 ① 전자우편 및 원격지 전송과 같은 우회적인 매개 경로를 통해 정상적인 운용을 가장하여 투입된 다음 간접적으로 작동되는 「기생형체계」, ② 아메바처럼 자원사용을 남용하는 자기와 동일한 웜을 복제하여 테러 대상시스템에 과부하를 일으켜 정상적인 운용을 마비시키는 「자기증식형체계」, ③ 자기 증식된 웜들이 서로 교신하며 상호협력하여 테러대상뿐 아니라 연관된 타 시스템에까지 조직적으로 침투하여 교란을 획책하는 「자기조직형체계」로 구분할 수 있다.

---

14) 논리폭탄체계를 사용한 최근 사례로 걸프전 당시 이라크가 프랑스로부터 들여온 방공시스템은 다국적국과 대치하기 시작하면서부터 제 기능을 발휘할 수 없었다. 그 이유는 대치 초기에 다국적군이 시스템에 침투시킨 논리폭탄이 가동했기 때문이다.

다. 컴퓨터 바이러스체계

컴퓨터 바이러스는 1985년 파키스탄에서 세계 최초로 등장하였다. 이러한 바이러스는 자료를 빼내는 해킹과 함께 2대 컴퓨터 범죄로[15] 우리나라의 일반 수준이 선진국대비 약 20%의 수준에 있는 것으로 알려지고 있다.

Computer Virus System은 테러대상 목표의 통신장비나 정보망을 무너뜨릴 수 있는 한가지 이상의 바이러스로 구성된다. 이는 상대의 정보체계에 침투하여 정보체계 및 정보인프라를 마비시킴으로써 상대의 기능을 마비시키며, 테러리스트의 바이러스테러로부터 자신의 정보체계를 보호함으로써 자신의 기능을 보존하여 사이버테러에 대비할 수 있는 체계로서 크게 테러용 바이러스와 대 테러용 바이러스(백신)로 구분할 수 있다. 컴퓨터바이러스는 자신을 복제할 수 있으며, 다른 프로그램에 자신을 덧붙일 수 있고, 통신선로와 데이터 통신망을 통하여 전송되어 전자교환기, 지휘통제체계에 침입하여 무력화시킨다.

컴퓨터 바이러스무기는 <표 2> 내지 <표 4>와 같이 컴퓨터 칩에 특수한 기능을 몰래 삽입하여 특정시간과 일자 조건(특정신호)에만 활동하는 기술인 「Chipping」과 컴퓨터 통신망을 통해 전달되는 패스워드를 알아내는 도구인 「슬리퍼(Sleeper)」와 명령이나 수집된 자료를 검색하여 파괴하는 「작용제(Agent)」[16]등이다.

<표 2> 매주 활동한 바이러스 현황

요일별	활동 바이러스
금	예루살렘 봉급날, 영시간, 커피숍. 1568
토	베토벤, 뽀동, 소닉
일	한국변형일요일, 일요일

자료 : 동아일보, 1999. 4. 29일자 B4면.

컴퓨터 바이러스는 백신으로부터 탐지되지 않도록 자기자신을 숨기는 「은폐(스텔스)형 바이러스」, 자신을 복제할 때마다 컴퓨터 바이러스 백신이 검색하는 부분을 다른 모

15) 경향신문, 1999. 4. 28일자 2면.

16) 컴퓨터 바이러스는 필요할 때, 충돌이 나거나 활동하기 전에 심어져야 하며, Agent는 상대의 데이터 뱅크와 파일을 통해 돌아 다니는 로보 프로그램으로 명령이나 수집된 자료를 검색한다(백용기, "정보사회화와 국방정보화 발전방향", 「21세기 군사혁신과 한국의 국방 비전」, 한국국방연구원, 1998, 605면).

습으로 변형복제하여 검색을 어렵게 하는「갑옷(조직)형 바이러스」, MS-Word·MS-Excell·배치 파일 등 응용프로그램이나 시스템의 매크로 기능을 이용하여 만들어진「매크로 바이러스」로 나눌 수 있다.

대 테러 백신체계는 ① 사이버 테러용 바이러스의 침투를 사전에 차단하는 즉, 컴퓨터 바이러스에 의한 테러로부터 자신의 체계를 보호하는(CVCM : Computer Virus Counter Measure)[17]「차단체계」와, ② 테러리스트들이 사이버 테러를 위해 침투시 이를 실시간으로 발견할 수 있는「탐색체계」, ③ 사이버테러시 이를 퇴치할 수 있는「백신체계」로 세분화할 수 있다.

미국에서는 컴퓨터 바이러스와 세균을 결합해 생명이 있는 컴퓨터 바이러스를 연구하고 있으며, 이 바이러스는 쓰레기나 기름 찌꺼기에 사는 미생물처럼 전자물질을 먹어치우며, 스스로 번식할 수 있는 컴퓨터 바이러스이다.

<표 3> 매월 활동한 바이러스 현황

일자별	활동 바이러스
1	워드매크로, 소년범, 타이머, 소닉
2	뒤집기
7	FCL
8	대만
9	IVP.548
13	IVP.928, IVP.944
14	예루살렘.EOS
16	클리퍼
18	한국변형 매독.1117
19	미니1.1010
20	NRGL.681
24	매독.955,한국변형 매독.653, 모양
25	NRGL.681
26	CIH, CIH 변종 1.4
31	미니1.751, 보자, 베토벤, FK.658

자료 : 동아일보, 1999. 4. 29일자 B4면.

17) 김병덕, "컴퓨터 바이러스를 이용한 전자전",「합참지(7월호)」, 합동참모본부, 1999, 233면.

<표 4> 컴퓨터 바이러스 캘린더

월 별	활동 바이러스
1	1일 : NRGL.946, (하드디스크 데이터 파괴)조쉬, 바로테스, 15일 : 카지노
2	2일 : 키누르기.1236, 3일 : 스크롤, 한국변형 CRI CRI 5595
3	3일 : 스크롤, KACZOR.4444, 휴일, 6일 : 미켈란젤로
4	1일 : 사탄, 2일 : 키누르기.1236, 15일 : 카지노, 26일 : CIH(하드디스크 내용삭제, 기본입출력 장치<BIOS>등 부품 망가뜨림)
5	1일 : NRGL.1065, 2일 : NRGL.1020, 16일 : 월드컵(2002World Cup Kkrea' 메시지전달)
6	4일 : 한국변형 CRI CRI .4289, 11일 : VCL.583,(하드디스크 데이터를 지움)
7	4일 : 새트리아.D, 13일 : 7월13일, 26일 : 7월 26일
8	12일 : 12일의 목요일, 13일 : 예루살렘, 15일 : 카지노, 16일 : 8월 16일, 22일 : 안락사
9	9일 : NRGL.1040, 작은 공산당, 22일 : 안락사
11	7일 : 소련복구, 15일 : 자살.843, 26일 : 리자드
11	1일 : 몰타아메바. 헬로윈, 15일 : 정주.3584, 17일 : 11월 17일, 30일 : 11월 30일
12	3일 : FCL.4228, 15~31일 : ROET.1899, 19일 : IVP.578, 24~26일 : 크리스마스인사

자료 : 안철수 컴퓨터바이러스연구소(동아일보, 1999. 4. 29일자 B4면).

라. 트랩도어(백도어)체계

트랩도어체계는 초급 소프트웨어 무기로 테러 대상자의 정보를 수집·보고하는 등의 비밀임무를 수행하는 스파이를 정보기술로 구현하는 체계로 ① 재침투를 가능하게 할 재침투 지원체계, ② 침투사실을 상대의 정보체계 운영자가 인지하지 못하도록 은폐하는 침투은폐체계, ③ 원격지의 명령을 받아서 상대의 정보체계를 마비, 파괴, 교란시킬 수 있는 오용·남용체계 등으로 구분되는 체계이다.

이들은 사이버 테러리스트가 평시에 침투한 상대의 정보체계에 트랩더어체계를 설치함으로써 테러 대상의 정보체계를 마비, 파괴, 교란시킬 수 있다. 우리나라의 트랩도어 체계는 선진국에 비해 약 5%수준에 있다.

마. 트로이 목마(TROJAN HORSE)

트로이 목마체계는 논리폭탄의 한 변종인 초급 소프트웨어 무기로 불법적으로 상대의 정보체계에 침입하여 첩보·정보를 수집하는데 이용되는 체계로, 테러대상의 컴퓨터 시스템에 시스템의 프로그램을 불법적으로 수정하여 해커가 원하는 기능을 수행하도록 하는 프로그램으로 외부적으로는 적법한 프로그램으로서 PC통신 등과 같은 네트워크를 통하여 무료로 배포하거나, 시중에 판매되는 고급 소프트웨어 형태를 띤다.

이 체계는 사용자가 그 소프트웨어에 숨겨져 있는 특정명령을 실행시키면 파일삭제, 디스크 포멧 등의 컴퓨터시스템을 파괴시키고, 잘못된 연산결과를 제시하거나, 시스템을 고의적으로 DOWN시키며, 시스템의 정상적인 동작을 방해하고, 주요 데이터나 파일 등을 사용자 몰래 외부로 반출, 프로그램을 변조시키고, 불법적인 시스템 관리자의 권한을 확보하는 등의 기능을 수행하는 체계이다.

바. 해킹체계

해킹이란 컴퓨터시스템의 코드를 해독하고 침입 방지장치를 무력화시키는 행동을 총칭하는 개념으로[18] 반복적으로 이러한 행위를 일삼는 자를 해커(Hacker)라고 부른다.[19] 따라서 해커(침입자)들이 저지르는 모든 불법적인 행위들을 전산망 보안침해사고로 볼 수 있으며, 정보시스템을 물리적으로 파괴하지 않고 개인정보를 무단으로 공개하거나 조작하여 개인을 공격하는 정보테러리즘이다.

이들의 행위에 따라 해킹체계를 ① 도청으로 패스워드나 ID(식별자) 등을 알아내는 사용자도용체계, ② 운영체계의 취약점을 이용한 체계, ③ 시스템의 구조적인 문제점을 이용한 구조적 공격체계, ④ 시스템 또는 서비스의 정상적인 운영을 방해하는 서비스거부체계 등으로 구분할 수 있으며, 우리나라의 경우 세계적 수준에 있으나, 선진국에 비해 약 15%의 수준에 있다.

사. AMCW(Autonomous Mobile Cyber Weapons)체계

AMCW체계는 1996년에 개념이 발표된 것으로 정보체계에 대한 테러용 고급 소프트

18) 정기태, 전게논문, 35면.

19) 한국정보보호센터, 「정보시스템 안전운영지침서」, 1998, 4면 ; 조병인, "하이테크(High-Teck)범죄의 실태와 대책", 「21C 정보화사회와 하이테크범죄 양상」, 한국공안행정학회, 1999, 26면.

웨어인 차기 사이버무기체계로, 테러 목표를 설정하고 순항하여 특정정보 또는 컴퓨터 시스템을 필요한 체계만을 파괴하는 사이버무기이다.

이는 통달거리(기동성), 테러목표(테러대상), 파괴범위(순항능력)에 따라서 ① 단일 시스템에 단일목표로 상대의 정보를 대상으로 한 소총형, ② 상대의 패키지를 대상으로 LAN(Local Area Network : 근거리통신망)[20] 시스템으로 복수목표를 파괴하는 대포형, ③ 상대의 컴퓨터시스템을 인터넷으로 복수목표를 파괴하는 미사일형, ④ 인터넷을 통하여 다수목표로 하여 네트워크 시스템을 파괴하는 핵폭탄형 등으로 분류할 수 있다.

아. 소프트웨어체계 취약성분석체계

소프트웨어체계 취약성분석체계는 소프트웨어체계의 테러 위협을 최소화하기 위한 방어체계로, 우리나라의 경우 복구체계는 100%, 예방체계는 80%수준이다.

사이버테러에 대한 방호체계는 테러리스트들의 감시와 테러 공격으로부터 자신의 정보기반체계와 정보 대응체계를 보존하거나 거짓정보를 유포하여 상대가 잘못된 판단을 내리도록 유도하는 것으로, 대국민 홍보활동 등의 「심리적 방호체계」, 디스크 내용의 암복호, 컴퓨터바이러스 백신·침입추적·CERT·RED팀 운영 등의 「정보체계방호체계」, 통신채널 보호와 비화기 및 암호장비 설치운용과 패킷 암호화 등의 「유통체계방호체계」, 주요 방호대상 시설물과 장비에 대한 방커화 및 인터넷망과의 물리적 분리와 일반인의 접근통제를 하는 등의 「물리적 방호체계」, 음어사용 및 패킷암호화와 암호화 모듈 등의 「암호체계」, 전략·전술적 기만과 허위정보 유포 및 저장 등의 「기만체계」 등으로 구성된다.

그리고 복구체계는 테러리스트들의 테러 공격으로부터 피해를 입은 자신의 정보대응체계를 원상태 또는 최소한의 필수 기능을 수행할 수 있는 상태로 회복시키는 체계로서 물리적 피해를 복구하는 물리적 복구체계와 정보대응체계의 각종 정보를 복원하는 논리적 복구체계로 구성된다.

정보 대응체계는 정보의 손실(Loss), 피해(Damage), 파괴(Destruction) 왜곡(Distortion) 및

---

20) LAN이란 다수의 독립된 컴퓨터들이 비교적 한정된 지역 내에서 데이터통신이 가능한 시스템으로 에러율이 낮고 상당히 빠른 속도의 물리적 통신채널을 이용, 상호간 통신을 하는 네트워크를 말한다. 이는 적은 지역 내에서 다양한 통신기기의 상호연결을 가능케하는 고속의 통신네트워크이며, 같은 빌딩에 EH는 좁은 지역의 각 건물간에 컴퓨터, 워드프로세서, FAX 등을 연결하여 전화, 데이터, 영상 등 제반 정보들을 상호교환할 수 있도록 하는 소단위의 고도통신망으로 전송매체로서는 평형케이블, 동측케이블, 광섬유케이블 등이 있다(오종중, 「정보통신용어해설」, 도서출판 동서, 1997, 825면).

절취(Interception)를 방지할 수 있어야 한다. 이를 위해서는 통신채널을 통하여 정보들이 전송되는 동안 정보에 대한 불법적 접근을 허용하지 않기 위한 방안이 마련되어야 하며, 관련 하드웨어와 소프트웨어에 대한 지속적인 개선 및 개발이 요구된다.

물리적 복구체계는 부품교환, 장비교체, 장비대체, 개보수, 재시도, 수리 등의 「물리적 복구수행체계」와 복구장비, 복구인력, 부품·수리부속 및 대체장비 등의 「물리적 복구지원체계」가 있으며, 논리적 복구체계는 데이터 복원과 데이터 베이스 복원, 소프트웨어(내장 소프트웨어 포함) 재설치 등의 「논리적 복구 수행체계」와 백업체계 및 백업장비, 소프트웨어CD, 고장 허용컴퓨터 등의 「논리적 복구지원체계」로 구분된다.

Ⅲ. Cyber Terror에 의한 국내·외 사례

최근 국제적으로 타인의 정보에 대한 맹목적인 위협이 증가하고 있으며, 해킹수법 또한 나날이 고도화되는 등 해킹의 정도가 과감해지고 그 피해 수가 많아지는 경향이 있다. 특히, 보안사고의 경우 70% 이상이 내부자 혹은 외부 연고자에 의한 것으로 비인가자에 의한 자원에의 접속 및 유출, 인가자에 의한 자원 및 접속법의 유출·훼손·변질 등의 사례들이 급증하고 있다.

1. 우리나라의 피해 사례

우리나라의 컴퓨터 보급 대수가 1999년 현재 7백 30만대(가정용 컴퓨터 보급율 51.8%로 2가구 중 1가구 보급)[21]로 PC통신 이용자 수도 829만 228명(매월 3.3%씩 증가), 인터넷 이용자 수는 578만 4000명(매월 15.2% 증가 추세)으로 전용선 가입기관의 경우 3만 777개 기관, 전문업체서비스를 통한 직접접속 개인가입자 수도 91만 9천여명(매월 13.3% 증가)이다.[22]

이에 따라 사이버범죄에 의한 피해도 급증추세를 보이고 있다. 경찰청 통계자료에 의하면 1998년 1월부터 1999년 3월 말까지 적발된 인원이 618명으로, 유형별로는 사이버 성폭력 등 534명, 금융전산자료 유출 등 24명, ID 도용 16명, 해킹 9명, 컴퓨터바이러스 유포 7명, 인터넷 불법 사이트 운영 6명, 기타 22명인 것으로 나타났다.[23]

---

21) 한국정보문화센터, 국민생활 정보화실태 및 정보화인식조사 (전자신문, 1999. 10. 1일자, 1면).
22) 한국전산원, 한국인터넷정보센터(KRMIC)조사결과, 국내 인터넷 이용현황 (전자신문, 1999. 4. 27일자 1면 ; 경향신문, 1999. 5. 12일자 1면).
23) 조병인, 전게논문, 38면.

국내에서 이러한 범죄행위가 테러행위로 악용될 수 있는 컴퓨터 바이러스가 3만 6천여종으로 새로운 컴퓨터바이러스가 1천 276종(1999년 현재)이 등장해 미국, 동구권과 함께 3대 바이러스 생산국의 오명을 받고 있다. 1999년 4월 26일에 CHI(체르노빌 바이러스 : 입·출력 시스템 파괴) 바이러스[24] 활동으로 청와대, 정보통신부, 산업자원부, 행정자치부, 검찰정, 금융감독원, 한국과학연구소, 전자통신연구원, 한국통신, 지방자치체(울산시청 등 30여 자치체) 등 정부의 전산망에도 피해가 발생한 바 있다.[25] CIH 바이러스에 감염된 컴퓨터 수도 전체보유 대수의 15%인 1백 10만대에 이르며, 컴퓨터기능 복구에 필요한 금액이 무려 1천억원이 넘으며, 유·무형의 재산손실을 감안하면 수천억원에 이른다. 최근 사이버테러가 정보처리장치나 정보통신망을 이용하여 다른 사람의 생명, 재산, 신체에 해악을 가할 것을 고지하거나 이러한 행위를 수단으로 경제적 이득을 도모하는 사이버테러가 심각하다. 종전에는 사이버테러에 이용되는 무기의 주종이 논리폭탄이었으나 근래에는 새로운 테러무기가 등장하여 다음 <표 5>와 같이 막대한 피해를 주고 있다.[26]

<표 5> 국내 해킹 수법별 현황(1997년도)

구 분	건 수	비 고
ID 및 비밀번호 도용	3	ID 도용
해킹프로그램 도용	5	취약점 파악용 도구 등을 이용
시스템 취약점 이용	33	운영체계, 홈페이지 등 취약점을 통한 해킹
E-메일폭탄(1995년. 6월 최초로 등장)	4	다량의 E-메일을 전송하여 시스템 마비
기 타	19	Ping(인터넷 주소를 확인하는데 사용되는 프로그램 공격) 및 비정상적 접속을 계속하여 시스템 마비
계	64	

자 료 : 송광섭, 전게논문, 103면.

24) CHI바이러스를 개발하여 올린 범인은 대만의 천잉하오(24세, 남)로 이 범인은 대북 대동공학원 정보처리학과 4학년 재학시(1998년 5월) 이 프로그램을 개발하여 인터넷에 올렸다. 천은 1998년 여름 졸업후 지금은 군에 입대해 있다. 범죄수사국은 천에게 CIH 퇴치 프로그램을 개발해 줄 것을 설득하고 있다. 이 바이러스에 의해 컴퓨터 피해를 본 국가는 한국과 터키가 각각 30만여대, 미국 1만대 미만, 중국 7천여대, 인도 1만여대 등의 피해를 입었다. 이 바이러스는 1998년 6월 대만에서 처음 발견되었다 (조선일보, 1999. 5. 1일자 31면 ; 동아일보, 1999. 4. 27일자 A21면).

25) 조병인, 전게논문, 38면.

26) 경향신문, 1999. 4. 28일자 2면 ; 전자신문, 1999. 7. 17일자 1~2면.

1999년만 보더라도 국가 기반시설인 금융·통신·전력 등의 전산망에 침투, 피해를 입히는 해킹 건수가 124건(금년 4월 작년 동기간에 비해 4배 증가, 월평균 31건 발생)이나 발생했다. 국내에서 하이테크 범죄사고의 대표적 사례는 <표 6>과 같다.

<표 6> 국내 사이버범죄에 의한 피해사례

년 도	피해대상 및 사건	테러 내용	비 고
1993	서울대학교 중앙교육전산원	전산원의 LAN에 불법침입하여 워크스테이션 6대의 디스크를 지운 사건	
1994	서강대학교	인터넷 아키(Archie)네트워크 D/B검색용시스템에 해커가 침입 각종 디스크 자료, 시스템 일부 등을 삭제	
	천리안 홈뱅킹사건	인천의 김모군이 인천지역 정보망인 인디텔에 가입한 선배의 ID를 도용, 불법으로 홈 뱅킹 계좌이체를 시도	홈뱅킹 서비스는 3, 4개의 패스워드가 요구되나 이를 모두 알아냄
1995	부산지역 해커사건	2인의 부산지역 해커가 국내 인터넷 서비스 제공업자의 시스템과 LAN을 바탕으로 부산 및 전국 주요대학의 시스템을 해킹	
1996	인터넷 홈뱅킹 사기사건	KAIST 학생이 PC통신망과 연결된 인터넷 서비스망의 서비스에 홈뱅킹 고객들의 비밀번호와 거래정보를 가로채는 변형 Telnet프로그램 설치, 여러 은행 홈뱅킹 이용자들의 ID와 비밀번호를 이용하여 계좌이체를 시도	
1997. 7	삼성 스팸 전자우편사건	삼성의 미국 현지법인 홈페이지에 관리자의 전자우편 계정을 도용하여 약 200만명의 인터넷 사용자에게 공격적인 대량의 광고 전자우편 전송	
1997. 8	시스템의 서비스 마비	오 모씨가 전자우편을 이용하여 약 20여명의 인터넷 사용자에게 약 450메가바이트 크기의 프로그램을 송신 서비스를 마비시킴	

1998. 2	국제해커 침투 사건	국제해커가 5개 교육대학에 침투하여 홈페이지 초기화면을 음란사이트로 변경	
1998. 10	해고 근로자 앙심품고 회사 시스템 해킹	PC통신회사의 시스템관리자로 근무하다 해고에 앙심을 품고 회사시스템을 해킹, 자료를 모두 삭제	3천여만원의 재산 피해

자료 : 정기태, 전게논문, 37면.

지난 1999년 3월 30일 경찰청 컴퓨터범죄수사대 발표에 의하면 최신 해킹프로그램인 「백오리피스」를 이용해 한국과학기술원(KAIST) 전산망에 침투하여 KAIST가 개발·연구중인 과학위성 「우리별 3호」의 제원·성능 등의 기초자료를 해킹당한 바 있으며,[27] 1998년 4월 PC통신 천리안 가입자 10여명의 ID를 도용하여 이들 명의로 경품 소프트웨어를 구입 재산피해(1천200만원)를 입힌 사례가 있었다.

그리고 같은 해 동년 10월에 고등학교 3학년생이 ID를 도용 ID 소유자의 명예를 훼손하는 글을 게재한 사실들을 적발한 바 있으며, 1992년도에는 부산지역 노동운동 경력자의 명단을 기업체에 유포하여 기업체로부터 취업거부 상황이 발생하는 사건이 있었다.

또한 1993년에는 경찰관 등 25명이 심부름센터에 경찰주민조회, 범죄경력조회서 등을 유출한 사건과 청와대 ID 도용사건 등이 사이버테러에 의한 대표적인 피해 사례이다.[28]

2. 외국의 피해 사례

세계 인터넷 이용자는 1억 3천만명(1998년말 추정)으로 인터넷 이용량은 3.5개월에 2배씩 늘어나고 있으며,[29] 2000년 말에는 약 3억 2천 7백만명으로 3배가 넘게 증가할 것으로 <표 7>과 같이 주요 국가별로 인터넷 사용자 수를 예측하고 있다.

27) 「백 오리피스(Back Orifice)」 프로그램은 국제적 해커그룹인 CDC클럽이 개발한 것으로 1998년 상반기부터 인터넷을 통해 확산되었다(전자신문, 1999. 4. 1일자 5면 ; 경향신문, 1999. 3. 31일자 23면).

28) 조병인, 전게논문, 38~39면.

29) 전자신문, 1999. 3. 26일자 4면(정통부 안영섭 차관 초청강연).

<표 7> 주요 국가별 인터넷 운용자 수예측 현황(2000년도)

(단위 : 천명)

순위	국 가	사용자수	순위	국가	사용자수
1	미국	132,000	2	독일	22,900
3	일본	21,900	4	영국	17,000
5	프랑스	12,600	6	캐나다	11,600
7	이탈리아	10,600	8	호주	8,000
9	네덜란드	5,400	10	브라질	5,200
11	러시아	5,000	12	스페인	4,400
13	중국	3,800	14	스웨덴	3,700
15	한국	3,200	상위	15개국	267,500
지역	유럽	102,000	총계	전 세 계	327,000

자료 : 양문승, "전자상거래 관련범죄와 대응방안", 「21C 정보화사회와 하이테크 범죄양상」, 한국공안행정학회, 1999, 93면.

이러한 추세에 따라 컴퓨터 바이러스가 1999년 5월 현재 전세계에 3만 6천여종으로 하루에 평균 10여종 이상이 새롭게 개발되고 있다.

미국의 경우 걸프전 중에 네델란드 10대의 해커가 펜타곤의 컴퓨터에 침입한 사례는 물론, 독일 해커들이 미사일정보를 해킹하여 이라크에 판매한 바 있으며, 1993년 6월, 전자해커에 의해 미 국무장관실에서 세계지도자들에게 보낸 '미국이 바그다드의 이라크 정보사령부에 미사일 공격을 가할 것'이라는 내용이 담겨 있는 전화통지문을 가로챈 사건이 발생한 바 있고, [30] 1994년 러시아의 한 해커가 시티뱅크에 침투하여 1천만불을 훔쳐가는 사건이 있었다.

1995년 통계자료에 의하면 펜타곤 컴퓨터에 총 16만회의 해커 침입이 있었으며, 해커들에 의해 NASA와 CIA의 웹페이지에 침투하여 CIA를 「Central Sutpidity Agency」로 수정해 놓고 조롱한 사건을 비롯하여, 1997년 10월 센프란시스코의 전기정전테러 사건[31], 버지니아 랭글리 공군기지의 컴퓨터 네트워크에 해커의 테러에 의해 임무수행이 마비된 사건, 그리고 1998년 9월 사이버테러리스트들이 남동부에 있는 국방부 병원의 의료 데이터베이스에 침입하여 이 부대의 혈액형 정보를 변경시킨 사건이 있었다.

또한 1997년 10월 다운로딩 / 2016216의 대가들이란 해커 그룹이 국방성 컴퓨터에 침

30) 신성택, 전게논문, 473면.
31) 김두현, 전게논문, 57면.

입 군사위성시스템에 관련된 소프트웨어를 절취한 뒤 1998년 4월에야 이를 테러분자들에게 판매하겠다고 위협하는 사건이 발생하는 등 지금도 미국방부 웹사이트에는 하루 평균 80여차례 정도 사이버테러를 당하고 있으며, 특히 코소보사태 중(1999. 3. 24~6. 9)에도 유고(세르비아) 해커들에 의해 NATO군(북대서양조약)과 관에 주둔한 미군기지의 전산망에 침입하여 테러함으로써 일시적 기능중단 및 역정보를 유포하는 테러가 계속되자 사이버테러리즘의 대책으로 사이버특수부대를 창설하기도 하였다.

특히, 유고사태시 나토군의 공습 4일만에 세르비아계 해커들이 나토군 웹사이트에 침입, 서버작동이 중단되는 사례가 발생하여 시스템이 다운되고, E-메일(세르비아 해커 중 1명이 나토군에 1일 2천통을 보냄)을 보냄으로써 인터넷 정보처리에 어려움을 겪었으며, 3월 말에는 세르비아계 해커모임인 「검은 손(Black Hand)」의 침입에 의해 미 백악관 웹사이트가 1개월 동안 중단되는 사태가 발생하였다.[32]

미 회계감사원(GAO)의 보고서에 의하면 1995년도에 발생한 전산방해 건수는 559건에서 년간 증가율을 고려하면 1999년도에는 25만건에 것으로 전망하고 있다.[33] 그리고 미국이 두려워하는 해커는 외국의 해커들보다도 미국 내에서 교육을 받는 자들이다.[34]

중국의 경우 최근(1999년 7월) TMD(Theater Missile Defense : 전역미사일방어)계획과 관련하여 중국과 대만간(양안사태) 긴장 고조시 중국의 해커들에 의해 대만정부기관의 홈페이지에 중국과 대만이 공중전을 하고 있다는 허위 메시지를 올림으로써 대만 증시가 폭락하는 사태가 발생, 이에 대응하여 대만 해커들에 의해 중국의 증권감독원 등 주요 기관의 홈페이지에 대만 국기와 국가가사를 게재하는 테러를 단행함으로써 중국이 대 혼란에 빠진 바 있었다.[35]

인도네시아에서는 동티모르(Timor)사태와 관련하여 동티모르 사태에 대하여 인터넷 가입자들의 관심을 유도할 목적으로 1997년 2월 10일과 17일에 포르투갈인 해커들이 인도네시아 외무부의 웹 페이지를 침입하여 서문을 「Welcome to Fascise Republic of INDONESIA」라 수정하고 외무장관의 사진을 게시한 바 있다.[36]

---

32) 합동참모본부, 「코소보전쟁종합분석」, 1999, 61면 ; 중앙일보, 1999. 4. 7일자 10면.
33) 국방과학연구소, 「국방기술정보(제3권 제11호 통권28호)」, 1997, 26면.
34) 미국의 컴퓨터 공학과 안보분야 박사들의 60%가 외국계이며, 그중 3분의 2가 이슬람국가와 인도에서 온 자들이다.
35) 전자신문, 1999. 9. 21일자 51면.
36) 한국국방연구원, 「주간국방논단(제703호 98-5)」, 1998, 6면.

Ⅳ. 각국 Cyber Terror의 대비 실태 및 경호경비대책 방안

1. 각국 Cyber Terror의 대비 실태

가. 우리나라의 대비 실태

한국전산원의 감리결과 자료(1999. 9월)에 의하면 정부행정 및 관계 산하 연구기관의 전산망에 대한 감리결과 85%정도가 해커에 무방비한 실태인 것으로 조사되었다.

기관별로 살펴보면 국무총리실 산하 비상기획위원회 등 22개 정부기관의 85개 전산망 중 15.3%인 13개 전산망만이 적정판정을 받았으나 그 외의 전산망은 사이버테러에 취약한 상태로 <표 8>과 같이 나타났다.

<표 8> 정부행정(연구)기관 전산망 감리결과(1999년도)

기 관 명	대 상	부적절/보통	적 절	비 고
비상기획위원회	6	4	2	· 총 85개 전상망 · 적정판정 : 13개망 (13.5%) · 보통 : 24개망 (28.2%) · 부적절 : 48개망 (56.5%)
행정자치부	5	3	2	
국방부 조달본부	4	3	1	
한국국방연구원	7	2/5	0	
법무부 출입국 관리소	4	2	2	
서울시	5	3	2	

자료 : 중앙일보, 1999. 10. 1일자 2면.

우리나라의 컴퓨터 기술이 선진국 대비 68.1% 수준으로, 컴퓨터바이러스 백신프로그램 실태는 세계 '톱3' 대열에 있다. 따라서 우리정부도 날로 급증하는 사이버테러에 대한 대응책을 마련하고자 범 부처차원에서 해킹 대응팀과 컴퓨터바이러스만 전문적으로 다루는 한국정보보호센터 등과 같이 전담조직을 만들고 있다.[37]

37) 문화일보, 1999. 4. 28일자 11면 ; 우리나라의 주요과학기술조사(1999), KISTEP(전자신문, 1999. 9. 17일자 2면).

민간단체에서도 사이버테러에 대한 대응책을 마련하기 위하여 보안전문가들이 모여 「정보통신망 피해사고 대응팀 협의회(CONCERT)」를 결성하여 보안관리 및 정책연구회, 침입차단 및 탐지연구회, 해킹대응연구회 활동을 위하여 한국정보보호산업협회(KISIA), 한국통신정보보호학회, 금융감독원, 검찰, 경찰 등과의 연계를 통하여 정보보호대응체계의 확산에 참여한 민간단체로 해킹기술을 악의적으로 활용되는 것을 막고 기술수준 향상을 위하여 CONCERT가 주축이 되어 시스템 취약성 진단과 정보보호 컨설팅 차원에서 해킹기술을 활용하는 일종의 타이거팀, 즉 전산망안전진단회 등이 결성될 전망이다.[38]

특히, 1996년 3월에 경호관련 학과가 개설된 대학의 교수들을 중심으로 학계·군·경·교도·소방전문가, 민간경비협회 등 경호관련 전문가를 회원으로 하여 창립된 「한국경호경비학회」에서는 경호경비에 관련된 학술세미나 및 연구를 통하여 사이버테러에 대한 대비 방안들을 제시하고 있다.[39]

일반 민간 개인연구소인 안철수 바이러스연구소, 백신프로그램업체인 하우리컴퓨터, 시만텍코리아, 명정보기술 등에서 최신 프로그램을 개발하고 있다.

그리고 검찰청에 컴퓨터범죄 전담수사체제 구축을 위하여 1996년 6월 대검찰청에 「컴퓨터범죄전담수사반」을 설치하고, 광주지검(1997. 4)을 비롯하여 10개청에 전담수사반을 설치·운영 중이며, 2000년까지 전국청에 설치 예정으로 현재 전담수사반 설치 현황은 <표 9>와 같다.[40]

<표 9> 컴퓨터범죄 전담수사반 설치 현황(1999. 10월 현재)

설치년도	설 치 청	설치년도	설 치 청
1995. 4	서울지검	1996. 6	대검찰청
1997. 4	광주·부산·대구·대전지검	1998. 6	전주·창원·청주·수원·인천지검

자료 : 양문승, 전게논문, 147면

38) CONCERT는 1996년 40여대의 회원기관으로 출발하여 1999년 현재 213개 회원기관이 되었다(전자신문, 1999. 4. 1일자 5면).

39) 김두현, "경호학의 발달과 공경호의 전문화방안에 관한 고찰", 「교양교육연구소논문집(제3호)」, 한국체육대학교 교양교육연구소, 1998, 180면.

40) 양문승, "전자상거래 관련범죄와 대응방안", 「21C 정보화사회와 하이테크범죄 양상」, 한국공안행정학회, 1999, 146면.

나. 외국의 대비 실태

미국의 경우 점증하는 테러리즘의 위협에 대처하기 위해 1998년 5월 대통령 결의안 제62조에 서명하였다. 이 결의안을 통해 21세기의 테러 위협을 제거하는데 기여할 것이다. 미국은 국제 테러범들에 대한정책의 원칙으로 ① 테러리스트들을 용납하지 않으며, ② 테러리스트들을 지원하는 국가들에 대해 모든 압력을 가하고, ③ 모든 법적 장치를 동원하여 테러리스트를 응징하며, ④ 다른 국가들의 테러 퇴치 능력 향상을 지원하는 등이다.

따라서 해외의 테러리스트들은 미국에 침입할 수 없고, 이들을 발본색원하고 자금줄을 차단하기 위해 가용한 모든 공법적 장치들을 동원하고 있으며, 정보·외교·군사·사법기구들간의 협력은 긍정적 효과가 있으며, 미 행정부는 의회를 통해 테러 방지를 위한 기관과 인력의 보강에 필요한 예산증가를 위해 노력하고 있다. 2000년까지는 모든 국가들을 국제 반테러협약에 가입시키기 위해 외교적 노력을 강화하고 있으며, 테러리스트들의 대량살상 공격과 전자, 통신망 등 주요 기간시설에 대한 테러를 억제하고, 그 기술을 탐지하기 위하여 노력하고 있다. 또한 직접적인 테러공격뿐만 아니라 중요한 국가기간시설, 전력이나 수송 등을 네트워크를 통해 사이버테러 할 가능성에 주목하고 있다.[41]

이러한 측면에서 대서양사령부 예하에 사이버특수부대를 1995년부터 사이버해킹전담반을 설립 배치·운영하고 있다. 특히, 미 공군에서 컴퓨터바이러스, 해커 및 정보테러에 대해 면역성을 가질 수 있도록 포괄적인 예방접종을 실시하고자, 미 공군과 국방고등연구원(DARPA)은 컴퓨터로 하여금 인간의 면역체계와 유사한 체계를 갖도록 하는 소프트웨어를 개발하여 자신과 침해자를 구별하는 법을 가르침으로써 바이러스를 퇴치하고자 하는 계획(1백만달러 예산)을 1997년도에 이미 착수하였으며, 이는 현재 사용 중인 컴퓨터 바이러스 보호 소프트웨어는 바이러스를 색출하기 위해 전산파일을 검색하고 또 새로운 바이러스나 전산방해 기술이 개발될 때마다 이에 따라 개량되지 않으면 안된다.

이와는 달리 현재 개발하려고 하는 소프트웨어는 유행성독감 예방접종처럼 바이러스 보호 소프트웨어와 달리 이 소프트웨어는 여하한 비정상적인 것이라도, 또 예전에

41) 이 결의안은 테러 퇴치를 담당하는 기관의 임무를 강화하여 광범위한 반테러 프로그램에서의 그들의 역할을 명시하고 있다(미국 백악관, "새로운 세기를 위한 국가안보전략", 「국가전략(제5권 1호)」, 세종연구소, 1999, 343~350면).

경험하지 못한 것이라도 이를 위협으로 인식하게 「컴퓨터 바이러스 퇴치용 일괄 백신 프로그램」을 2000년까지 개발할 계획이다.[42]

최근 들어 불특정 다수인에게 한꺼번에 E-Mail을 보내는 인터넷상의 스팸메일(Spam mail)을 보내는 경우가 많아지자 버지니아주에서는 Spam mail규제법을 제정하여 적발된 자는 500달러의 벌금에 처하고, 수신인에게 악의적으로 피해를 줄 경우 수신인의 피해액이 2,500달러를 넘을 경우 중범죄로 간주, 징역에 처하도록 규제하고 있다.[43]

또한 미국은 사이버테러에 적극적으로 대처하기 위하여 정부의 공공기관 및 연구기관만으로는 컴퓨터와 인터넷이 보편화된 세상에 사이버테러에 대비하는 데는 자체 기술개발만으로 한계가 있다고 판단하여 CIA가 필요로 하는 각종 정보장비와 기술을 개발할 벤처기업을 캘리포니아주 폴로 알토에 「IN-Q-IT(인큐잇)」[44] 회사를 설립(2천 8백만 달러 투자비)하여 직접 발굴·육성하고 있다. 역점분야는 현대 첩보전에 응용할 수 있는 인터넷 기술과 비밀보호기술, 자료탐색기술, CIA컴퓨터 시스템 개선사업 등이다.

그리고 미국의 정보보호 감시기관인 정보보전감시국(ISOO)은 최근 해커들이 온라인망을 타고 시스템에 침입해 시스템을 다운시키고, 데이터를 파괴하거나 바이러스를 퍼뜨리는 크랙커(Crakor)들에 대비하기 위하여 비밀서류보호를 한층 더 강화하는 특별액세스프로그램(SAP)을 책정해서 종래의 최고 단계였던 I급 비밀보다 높은 단계로 하는 것을 검토하고 있다. 이는 이미 세계목표암호(RSA)가 파괴되어 전자서명 등을 위조하는 방법들이 등장함으로써 사이버테러들에 의해 이용된다면 자금이나 시간이 많이 소요되므로 이를 적극적으로 대비하기 위한 것이다.[45]

일본의 경우 경찰청과 우정성, 통산성 등은 네트워크가 국제적으로 확산되고 있으나 관련규제법에 해커를 처벌한 근거가 없어 타인이 컴퓨터 네트워크에 불법적으로 접근하는 해킹 등의 범죄를 처벌하는 「부정액세스행위금지등에관한법률」[46]을 개정하여 대

---

42) 국방과학연구소, 전게서, 26~27면.

43) 송광섭, 전게논문, 108면.

44) IN-Q-IT는 CIA를 지칭하는 첩보(Intelligence)와 정보기술(Information Technology) 007제임스 본드 영화에서 신기한 장비를 만드는 기술요원 Q에서 각각 따왔다(중앙일보, 1999. 10. 1일자 13면).

45) 국방일보, 1999. 10. 5일자 8면.

46) 이 법은 목적에서부터 벌칙에 이르기까지 9개 조문으로 구성, 대상은 전기통신회선으로 연결된 네트워크에 접근해 사용자가 자신의 식별부호(ID, 패스워드, 음성 등)를 입력해서 작동하는 액세스 제어 기능이 탑재된 컴퓨터, 전용회선망, PC통신이나 인터넷에 접속되어 있는 기업, 개인, 회선공급자, 대학연구기관, 기업의 근거리통신망 내의 컴퓨터, 즉 식별부호 도용과 시스템 약점을 이용해서 침입 등 2가지 유형을 부정액세스로 간주 금지하고 있으며, 타인의 패스워드 등을 무

응하고 있으며, 1996년 10월 컴퓨터 부정사건에 대처하는 전문조직으로서 「컴퓨터긴급대응센터」를 개설하여 운영하고 있다.

중국의 경우 대만의 TMD계획과 관련하여 대만 해커들의 보복대응에 충격을 받아 사이버테러에 대비하기 위하여 일반해커들을 뽑아 군사학교에서 사이버테러에 대한 특수교육을 시킨 바 있다.[47] 특히, 1997년 초 중앙군사위원회를 통해 「컴퓨터바이러스특수부대」를 창설하였다.

2. Cyber Terror에 대한 경호경비대책 방안

사이버무기는 세계적으로 공개적 개발이 제한되고 자국의 이익을 보호하기 위하여 유출이 금지된 기술이다.

우리와 대치하고 있는 북한은 공개된 정보자료에 의하면, 사이버테러무기에 대해서 1991년도 걸프전과 유고사태시의 양상을 연구·분석하고, 1998년도에는 북한과 관련된 기관에서 주한미군의 인터넷사이트 자료 검색이 최다로 이 분야에 관심을 기울이고 있으며, 이미 기술적으로 능력을 갖추고 있는 것으로 추정하고 있다.

최근 귀순한 이무철씨의 증언에 의하면, 평양 미림에 전자전대학교를 설립 후 전자전 무기체계 및 기술을 집중적으로 개발하고 있으며 유사시 우리의 국방전산망을 교란하기 위해 해킹기술 습득 및 전자전 대비 기술개발을 하여 첨단 컴퓨터통신망과 지휘체계를 무력화시킬 수 있는 사이버테러를 준비하고 있고 소프트웨어 기술(특히, 응용소프트웨어 부분)도 예상 외로 발전한 것으로 알려지고 있다.

김일성종합대학, 김책공업종합대학, 평성리과학대학, 조선컴퓨터센터, 평양정보센터 등에 컴퓨터 관련 우수인력이 몰려 있어 이곳에서 국가가 필요로 하는 소프트웨어를 개발하고 있으며, 이 중 조선컴퓨터센터는 우리나라의 전자통신연구원처럼 지문식별체계, 지문출입관리시스템, 사무자동화시스템 등의 소프트웨어를 개발하는 북한 최고의 정책연구기관으로 연구사가 1,000여명 정도 있는 것으로 알려지고 있다.[48]

이러한 능력을 갖춘 북한의 사이버테러 가능성에 대비하기 위하여 다음과 같이 방안을 제시하고자 한다.

첫째, 미래 사이버테러를 대비하기 위하여 소수·정예 자원으로 정부산하 연구기관에

단으로 다름 사람에게 제공하는 행위도 금지하고, 이를 위반한 자는 1년 이하의 징역이나 50만엔 이하의 벌금을 부과하도록 규제하고 있다(전자일보, 1999. 4. 17일자 4면).

47) 전자신문, 1999. 9. 21일자 51면.

48) 경향일보사, Newsmaker (통권 315호), 1999. 4. 15일자 135면 ; 전자신문, 1999. 9. 21일자 51면.

사이버테러 연구팀 편성과 경호경비관련기관 및 유관기관에 사이버테러 대응팀을 구성 운용하여야 한다.

연구·개발 분야는 민간능력을 최대 활용할 수 있도록 위탁하되 완전 민영화(Privatization)가 아닌 외주활용(Outsourcing) 형식을 채택함으로써 민간의 이익 극대화 속성상(신속, 기술, 총력적) 성과의 극대화와 경제성[49]을 최대 활용하고, 행정기관 산하 연구기관에서는 기획과 감독 업무만 수행하고 연구·개발업무는 순수 민·학·산을 중심으로 이루워 질 수 있도록 하여야 할 것이다. 특히 경호작전을 지원할 수 있도록 군사작전과 연계하여 군 조직에 사이버테러대응사령부 창설이 필요하다.

사이버테러 예방을 위한 체계 연구개발을 군사작전과 연계하여, 방호체계를 구축할 수 있도록 방호벽, 컴퓨터바이러스 백신, 침입탐지체계, 침입 역추적체계, 보호공학체계 등을 개발하고, 완벽한 복구체계를 구축하기 위하여 소프트웨어 복구체계, D/B 복구체계, 고장허용컴퓨팅시스템과 감시체계인 유·무인감시용 소프트웨어 및 통신망 패킷모니터링 시스템개발 등을 산·학·관 합동으로 연구·개발이 필요하다. 아울러 미국과 같이 외부에서 불순한 침입자들이 침입시에는 자체에서 이를 거부할 수 있는 컴퓨터바이러스에 의한 테러를 퇴치할 수 있는 <표 10>과 같은 일괄 백신 소프트웨어를 국책사업으로 개발하는 등 근본적인 예방책을 세워야 할 것이다.

<표 10> 사이버테러 방호·복구·예방 및 감시체계 개발

구 분	방호체계	복구체계	감시체계	예방체계
개발 체계	· 방호벽 · 컴퓨터바이러스 백신 · 침입탐지체계 · 침입 역추적체계 · 보호공학체계	· 소프트웨어 복구체계 · D/B복구체계 · 고장허용컴퓨팅 시스템	· 유무인 감시용 소프트웨어 · 통신망 패킷 모니터링 시스템	· 컴퓨터바이러스 퇴치용 백신 소프트웨어

둘째, 민간경비업체에 시설경비뿐만 아니라, 사이버테러에 대한 예방경비체계를 도입하여 컴퓨터바이러스에 의한 피해를 범국민적 차원에서 예방할 수 있도록 민간 경비업법을 제도적으로 보완하여 사이버테러에 대한 순수 민간경비업무를 수행할 수 있도록 하되 정부부처(경호관련 기관)의 감독을 받을 수 있도록 제도화하여야 한다.

49) 민간 기업관계자는 자신들의 경영 노하우를 통하여 추정된 비용의 30% 이상 절감이 가능하다고 주장한다(한국국방연구원, 「주간 국방논단(제778호)」, 1999, 9면).

셋째, 방송 및 언론매체를 통하여 사이버테러에 대한 사전 바이러스 주의보 발령제도를 도입하여 충분한 시간적 여유를 가지고 대처할 수 있도록 제도화하고 이러한 기능을 수행할 수 있는 기구를 편성하여 기상 예보제와 같이 정기 방송프로그램화를 조기 정착화 할 필요가 있다.

넷째, 해커규제법을 일본 수준으로 제정하고, 컴퓨터를 구매하는 일반소비자들에게 바이러스 백신(프로그램)에 대해 선택(사양)프로그램이 아니라 법적·제도적으로 필수구매 소프트웨어로 지정하여 컴퓨터 바이러스에 의한 피해를 차단하여야 할 것이다.

V. 결 론

이상에서 본 바와 같이 정보화시대의 사이버테러는 국가 정보기간망을 마비시키는 것을 의미하므로, 행정· 군사·금융 등에 관한 중요 정보를 컴퓨터 D/B화하고 있기 때문에, 그 정보시스템의 파괴로 국가의 기본기능을 순간적으로 마비시킬 수 있다.

이러한 위협에 대비 사이버테러에 대해 보호 및 방책을 발전시키고, 적극적인 대비를 위하여 본문에서 제시한 ① 소수 정예자원으로 구성된 사이버테러 대응 연구팀을 정부산하 연구기관(즉, 정통부 산하 한국정보보호센터, 국방부 산하 국방정보체계연구소 및 ADD 등)에 설치하여 운영하되, 연구·개발은 민·학·산이 중심이 되어 성과 위주의 연구·개발이 이루워 지도록 제도적으로 발전시켜야 하고, ② 민간경비업체에 사이버테러 예방에 따른 업무를 수행할 수 있도록 민간 경비업법을 제도적으로 보완하고, ③ 사이버테러에 대한 주의보 발령제도를 조기 정착화하는 것이 요구되며, ④ 해커에 대한 규제법을 제정하고, 컴퓨터바이러스 백신 프로그램을 필수로 구매토록 하는 법적인 보완책인 강구되어야 한다.

끝으로 위에서 제시한 방안에 대해서 조기에 시행 및 착수함으로써 사이버테러에 의한 피해를 최소화 할 수 있을 것이다.

그러나 이와 같은 사항들이 현실적으로 반영하기 위해서는 앞으로도 많은 노력이 필요할 것이며, 무엇보다도 경호경비가 국가 안보와 직결된다는 점에서 이와 관련된 의사결정자들이 사이버테러에 대한 인식을 제고하고, 사이버테러 대응체계를 위한 조직구성 및 자원제공에 최대한의 노력을 기울여야 할 것이다.

테러에 대한 좋은 예방책만이 경호대상자는 물론 경호요원의 생명을 구할 수 있음을 다시 한번 강조하지 않을 수가 없다.

參 考 文 獻

▣ 국내문헌

권태영, "한국군의 군사혁신 비전과 선택", 「21세기 군사혁신과 한국군의 국방비전」, 한국 국방연구원, 1998.

국방과학연구소, 「국방기술정보(제3권 제11호 통권238호)」, 1997.

김병덕, "컴퓨터 바이러스를 이용한 전자전", 「합참지(7월호)」, 합동참모본부, 1999.

김두현, 「경호학개론」, 도서출판 쟁기, 1999.

———, "2002년 월드컵축구대회에 대한 안전대책", 「경호경비연구(제2호)」, 한국경호경비학회, 1999.

———, "경호학의 발달과 공경호의 전문화방안에 관한 고찰", 한국체육대학교 교양교육연구소, 1998.

미국 백악관, "새로운 세기를 위한 국가안보 전략", 1999.

백용기, "정보화사회화와 국방 정보화 발전방향", 「21세기 군사혁신과 한국의 국방비전」, 한국국방연구원, 1998.

세종연구소, 「국가전략(제5권1호)」, 1999.

송광섭, "Internet관련 범죄의 동향과 그 대책", 「경호경비연구(제2호), 한국경호경비학회, 1999.

신성택, "첨단 비살상무기의 개념과 개발 동향", 「21세기 군사혁신과 한국의 국방비전」, 한국국방연구원, 1998.

양문승, "전자상거래 관련 범죄와 대응방안", 「21세기 정보화 사회와 하이테크범죄 양상」, 한국공안행정학회, 1999.

원은상·하광희, "테러집단의 정보전 위협과 안보관련 시사점", 「주간국방논단(제703호 98-5)」, 한국국방연구원, 1998.

오종중, 「정보통신 용어해설」, 도서출판 동서, 1997.

정기태, "해커의 이해와 해킹 대응방안", 「국방정보통신(제16호)」, 국군통신사령부, 1999.

조병인, "하이테크(High-Tech)범죄의 실태와 대책", 「21세기 군사혁신과 하이테크범죄 양상」, 한국공안행정학회, 1998.

최성빈, "미래 국방과학기술의 혁신적 발전 전략", 「21세기군사혁신과 한국의 국방비

전」, 한국국방연구원, 1998.
최영호, "정보범죄의 현황과 제도적 대처방안", 한국형사정책연구원연구보고서, 1998.
한국경호경비학회, 「경호경비연구(제3호)」, 1999.
한국국방연구원, 「주간 국방논단(제778호)」, 1999.
한국정보보호센터, 「정보시스템 해킹 현황 및 대응」, 1996.
————————, 「정보보호현황」, 1996.
————————, 「전산망 정보보호」, 1996.
————————, 「정보보호총서」, 1996.
————————, 「정보시스템 안전운영지침서」, 1998.
한 희, "정보전체계의 발전과 한국군의 대비 방책", 「21세기 군사혁신과 한국의 국방비전」, 한국국방연구원, 1998.
합동참모본부, 「합동VISION 2015, 합동전장운영개념서」, 1999.
————————, 「합참지(7월호)」, 1999.

ABSTRACT

Classification of Cyber Terror & Counterplan against It.

by Kim, Doo-Hyun

I study on the classification of cyber terror & counterplan against cyber terror

The paper, purporting to consider security counterplans, comprise five chapters.

Chapter I which introduction is followed by chapter II, dealing largely with the general definition and classification of cyber terror.

Chapter III concerns the domestic & foreign cases of damages by cyber terror.

Chapter III consider the condition of world nations against cyber terror and its actual condition.

It is followed by concluding observation made in chapter V.