사이버테러리즘의 대응방안에 관한 연구

A Study on the Countermeasure to Deal with Cyber Terrorism

오태곤
전남도립남도대학 경찰행정경호과

Tae-Kon Oh (otk@korea.com)

요약

오늘날 현대사회는 산업사회에서 지식정보사회로의 '페러다임의 전환기'에 직면하고 있다. 이는 지식중심의 초고속 네트워크 사회로의 진입을 의미하는 것이며, 특히 우리나라는 일찍이 IT 관련 산업에 막대한 투자를 한 끝에 몇 몇 분야에서는 이제 세계 강대국들이 우리의 기술을 벤치마킹해 가는 현실이다. 하지만 이러한 성장 일변도의 정책적 대응은 정보화의 역기능에 대한 대비가 미흡하게 되었으며, 그 대표적인 것이 사이버 테러리즘이다. 익명성을 띤 행위자가 불특정 다수에게 행하는 사이버 테러리즘은 오늘날 뉴테러리즘의 가장 대표적인 유형의 하나이다. 본 연구는 사이버테러리즘에 대한 정책적, 법적 쟁점을 중심으로 살펴보고 그 대응방안을 강구한다.

■ 중심어 : | 지식정보사회 | 초고속 네트워크 사회 | 법적 보호 | 사이버테러리즘 |

Abstract

These days, modern society is facing a 'turning point of paradigm' from industrial society to knowledge and information society. It indicates an entry to the high-speed network society centering on knowledge. Specifically, Korea has invested enormously to IT Industry and finally other advanced countries are eager to export technologies of our country through benchmarking. However, because of our growth-oriented policy, Korea is not very good at dealing with the dysfunctions of information-centered society, and one of the representative problems is cyber-terrorism. Cyber terrorism which anonymous actors do to the uncertain number of people is one of the new types of terrorism. This study aims at political and legal speculations on cyber terrorism for protection of contents and find its countermeasures.

■ keyword : | Knowledge and Information Society | High-speed Network Society | Protection of Law | Cyber Terrorism |

접수번호 : #050523-001
접수일자 : 2005년 05월 23일
심사완료일 : 2005년 06월 21일
교신저자 : 오태곤, e-mail : otk@korea.com

I. 서 론

세계적인 미래학자 앨빈 토플러는 일찍이 '제3의 물결'이라는 논고에서 산업사회에서 지식정보사회로의 전환을 예고했었다. 이는 지식중심의 초고속 네트워크 사회로의 진입을 의미하는 것이며, 특히 우리나라는 일찍이 IT 관련 산업에 막대한 투자를 한 끝에 몇 몇 분야에서는 이제 세계 강대국들이 우리의 기술을 벤치마킹해 가는 현실이다. 하지만 이러한 성장 일변도의 정책적 대응은 정보화의 역기능에 대한 대비가 미흡하게 되었으며, 그 대표적인 것이 사이버 테러리즘이다. 2003년 1월 25일 전국은 유선 인터넷은 물론 무선인터넷, 행정전산망이 완전히 불통되는 사상 초유의 재난이 발생했다. 동 사건은 특히 국내 뿐 아니라 미국, 유럽 등 전세계적으로 발생하여 각국에 엄청난 피해를 주었다[1]. 즉 몇 몇 해커들에 의한 사이버 테러리즘에 의하여 국가 기능이 잠시지만 마비가 되는 중대한 결과를 초래하게 된 것이다.

지금까지 사이버 테러리즘에 대한 연구는 각국의 현황을 분석하거나 소개하는 정도에 그치고 있는 현실이다. 이에 본고에서는 콘텐츠보호를 위해 사이버테러리즘에 대해 우리나라의 현황을 살펴보고 법적체제를 중심으로 가장 효과적인 대응방안을 강구해 본다.

II. 사이버 테러리즘

1. 개 념

테러 또는 테러리즘이라고 불리는 테러행위는 '정치적으로 동기가 형성된 폭력'이라고 정의하고 있는 데서 알 수 있듯이 기본적으로 수단적인 가치보다도 상징적인 정치적인 문제와 범죄로서의 폭력행위를 복합적으로 포함하고 있는 것이다[2]. 이 용어에 대해서는 학자들간에 달리 정의하고 있지만, 우리나라의 대 테러업무를 주관하는 국가정보원은 "정치적 · 사회적 목적을 가진 개인이나 집단이 그 목적을 달성하거나 상징적 효과를 얻기 위해서 계획적으로 행하는 불법적 폭력행위"라고 정의하고 있으며, 사이버테러는 사이버공간에서 정치적 동기나 일정한 목적을 가진 크래커가 첨단정보통신을 이용하여 계획적으로 정보시스템을 공격하는 행위라고 정의하고 있다.

2. 특 징

사이버 테러리즘은 보이지 않는 사이버 공간에서 해킹과 바이러스와 같은 수단으로 목적하는 대상의 정보시스템에 영향을 주어 목적하는 결과를 기대한다는 점에서 여러 가지 새로운 특징을 갖고 있다[3]. 첫째 사이버테러리즘은 고도의 기술성을 요한다. 이들은 컴퓨터나 첨단정보통신을 이용하여 전산망에 침투하거나 바이러스를 침투시킨다. 이는 사이버 테러리즘 관련자를 처벌하고자 할 때, 추적도 어려울 뿐 아니라 흔적도 찾기 어렵기 때문이다. 두 번째, 해커나 컴퓨터 공학도 등의 고급 두뇌가 가담한다는 것이다. 대개 해커나 컴퓨터 공학도 출신의 사이버테러리스트들은 인터넷이나 통신망을 통해 경쟁국의 국가정보기관이나 국가중요시설의 컴퓨터시스템에 숨어 들어간다. 보안프로그램은 몇 시간이면 뚫리기 마련이어서 이들에게는 문제가 되지 않는다. 세 번째, 방대한 정보유출과 파괴행위를 수반하며 그 패해가 예측 불가능하다. 네 번째, 관련자의 적발이 어렵다. 이들은 고전적 기법보다 훨씬 빠르게 방대한 양의 치명적인 정보를 빼내고 파괴를 한다. 이러한 연유로 추적시스템을 통해 흔적을 발견하고 추적하지만 이들의 존재를 파악하기는 쉽지 않다. 마지막으로 이들은 불법적인 경제적 이들을 얻기 위한 경우도 있지만, 단순히 범죄인식이 없이 자신의 실력을 뽐내기 위한 경우도 있다.

3. 유 형

사이버 테러리즘의 유형은 기술 발전의 단계 만큼이나 복잡하고 다양하다. 이하에서는 사이버 테러리즘의 가장 대표적인 형태인 '해킹'과 '컴퓨터 바이러스'에 대하여, 그 유형과 공격방법을 일별하여 보면 다음 표와 같다[4].

표 1. 해킹의 유형 및 공격방법

유 형	공 격 방 법
사용자 도용	가장 일반적인 해킹형태로 다른 일반 사용자의 ID 및 패스워드를 도용하는 방법
S/W보안오류	컴퓨터내의 시스템 S/W나 응용 소프트웨어의 버그 등을 이용한 공격방법
버퍼오버플로우 취약점	소프트웨어 변수관리상의 문제인 오버플로우 버그를 이용하여 불법으로 명령어를 실행하거나 권한을 가지는 방법
구성설정 오류	시스템 S/W의 설치나 운영상에 오류를 이용한 공격방법
프로토콜 취약점	인터넷의 통신프로토콜인 TCP/IP의 설계취약점을 이용한 구조적인 공격기법
서비스 거부공격	시스템이나 네트워크의 정상적인 동작과 서비스를 방해하거나 정지시키는 공격
취약점 정보수집	특정의 시스템을 공격하기 전에 시스템의 취약점을 알아내고자 하는 스캔공격
사 회 공 학	관리자를 속여 패스워드를 알아내거나 권한을 얻어내는 공격

표 2. 컴퓨터 바이러스의 유형 및 공격방법

유 형	공 격 방 법
부 트 형	디스크드라이브를 인식하기 위해 처음 읽혀지는 부분을 부트영역이라고 하는데, 이 영역에 있는 운영체계를 공격하는 형태
파 일 형	프로그램을 실행하기 위해 가장 필요한 실행 프로그램 파일을 공격하는 형태
부트/파일형	부트영역의 운영체계와 실행 프로그램 파일을 동시에 공격하는 형태
매크로형	매크로 기능을 사용하는 마이크로소프트사의 워드나 엑셀 등의 자료파일을 매개체로 하여 컴퓨터 시스템을 공격하는 형태
트로이 목마형	유용한 프로그램으로 위장하여 특정일자나 특정 조건이 되면 컴퓨터 시스템이나 파일을 공격하고, 개인정보를 불법적으로 취득하는 악의적인 해킹을 주 목적으로 하는 형태
웜 형	다른 사람에게 보내는 E-mail에 자신을 첨부하여 빠른 전파력으로 인터넷 시스템, 하디디스크, 프로그램을 공격하는 형태
스크립트형	프로그래밍 언어가 아닌 언어로 작성한 짧은 프로그램이나 명령문들의 집합체를 이용하여 컴퓨터 시스템을 공격하는 형태
복 합 형	일반적인 바리어스형태에 해빙기법이 첨가되어 두가지 공격을 같이 하는 형태

III. 최근 사이버 테러리즘의 현황

최근 사이버 테러리즘의 양상은 초기의 천재적인 컴퓨터광에 의하여 자신의 실력을 과시하기 위한, 다분히 장난기 어린 형태의 침해 유형에서 점차 범죄화 되어가고 있다. 즉 초기에 메일 등에 첨부화일 형태로 바이러스를 유포하여 상대방의 컴퓨터의 사용을 방해하는 단순 형태에서, 최근에는 전국가적 · 전세계적인 네트워크의 장애를 유발하기도 하고 국가기관을 해킹하여 국가 안보와 직결되는 중요자료를 탈취하려는 시도를 하고 있다.

또한 개인 금융거래정보를 수집하기 위한 인터넷 금융사기 수법인 피싱(Phishing)이 등장하는 등 정보탈취 및 금전적 이득을 노리고 있는 현실이다. 이하에서는 이러한 사이버 테러리즘의 형태를 공공분야와 민간분야로 나누어 살펴본다[5].

표 3. 최근 사이버테러리즘 발생현황

분 야	구 분	2003년	2004년
공 공	웜 · 바이러스	388	2,287
	해 킹	935	1,683
	소 계	1,323	3,970
민 간	웜 · 바이러스	4,719	4,973
	해 킹	21,460	19,324
	소 계	26,179	24,297
합 계		27,502	28,267

* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

1. 공공분야 사이버 테러 현황

2004년도에 발생한 공공분야 해킹 및 웜 · 바이러스 사고건수는 3,970건으로 2003년도 1,323건에 비하여 3배 이상 증가하였다. 사고 유형별로는 웜 · 바이러스 감영 사고가 58%로 가장 많았으며 사고기관별로는 교육기관이 38%로 가장 많은 사이버 테러를 당하였다.

표 4. 2004년 사이버 테러 발생 현황

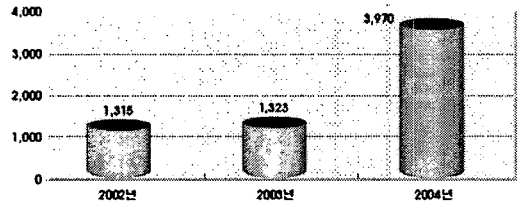
유형 / 기관	웜 · 바이러스 감염	경유지 악용	홈페이지 변조	자료훼손 및 유출	단순침입 시도	기 타	합 계
국가기관	283	37	21	34	290	133	798
지 자 체	501	22	53	8	82	35	701
연 구 소	80	11	13	8	26	17	155
교육기관	922	280	173	63	64	35	1,537
산하기관	363	15	29	9	95	47	558
기 타	138	13	8	4	13	45	221
합 계	2,287	378	297	126	570	312	3,970

* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

1.1 시기별 추이

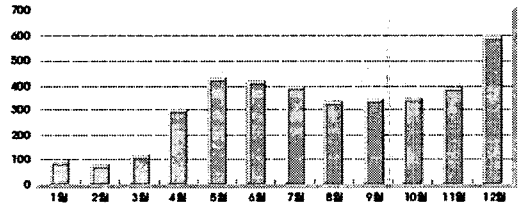
최근 3년간 공공분야의 사고 발생현황을 보면 2004

년도의 사고가 이전의 2년 합계보다 더 많이 발생한 것으로 나타났는데 이는 국가사이버안전센터가 신고위주 사고처리에서 보안관계를 통해 능동적으로 사고를 탐지한데 기인되었다고 한다. 월별로 보면, 3월부터 사고건수가 급격히 증가한 것을 볼 수 있으며 12월이 사고건수가 가장 많은 것으로 나타났는데 이는 국산 게시판 프로그램인 '제로보드' 취약점이 발표되면서 이를 악용한 홈페이지 변조사고가 많이 발생하였기 때문이라 한다.



* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 1. 최근 3개년간 침해사고 발생 현황



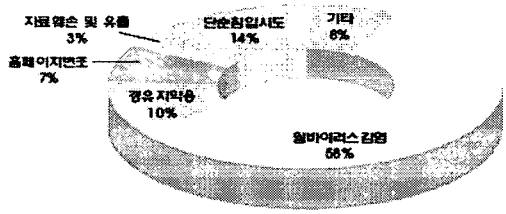
* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 2. 월별 침해사고 발생현황

1.2 사고유형별 발생 현황

2004년도 발생한 사고의 유형별 분포를 보면 [그림 3]과 같이 웜·바이러스 감염사고가 2,287건이 발생하여 전체의 58%를 차지하는 등 가장 심각한 위협이 되고 있으며 취약점 탐색을 위한 스캐닝 등의 단순 침입시도는 570건(14%)으로 두 번째 위협으로 나타났다. 그 밖에 경유지 악용 378건(10%), 홈페이지 변조 297건(7%), 자료훼손 및 유출 126건(3%)순으로 나타났다. 동 년에 웜·바이러스 감염사고가 가장 심각한 사이버 위협으로 대두되었던 이유는 웜·바이러스의 소스코드가 공개되는 등 어느 때보다 웜·바이러스 제작환경이 좋아졌기 때문이라 한다. 이는 전자우편 수신시 보안유의를 철저히 하지 않거나 각종 메신저 등 P2P(Peer-to-Peer) 프로그램을 무분별하게 사용하고 PC 보안패치를 하지 않는 등 사용자의 보안의식이 여전히 부족한 점 때문이기도 하다.

국가사이버 안전센터의 전망에 의하면 이러한 유형의 사고는 지속적으로 발생할 것으로 보인다.

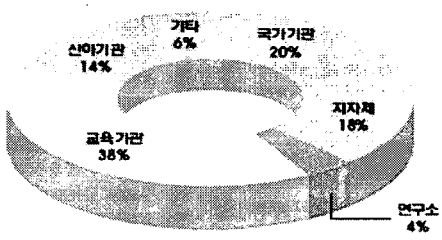


* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 3. 사고유형별 침해사고 발생 현황

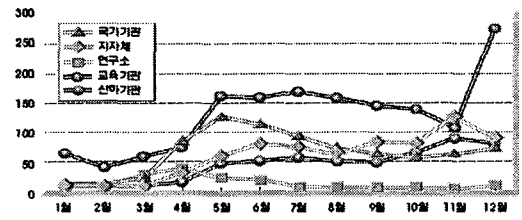
1.3 기관별 발생 현황

2004년도에 발생한 사이버 테러 상황을 기관별로 분류해 보면 [그림 4]와 같이 교육기관에서 1,537건이 발생하여 전체의 38%를 차지하여 전년도에 이어 가장 많은 사고가 발생한 분야였으며 국가기관이 798건(20%), 지자체 701(18%), 산하기관 558건(14%), 연구소 155건(4%) 순으로 나타났다. 교육기관이 사이버 공격 피해를 많이 입은 주된 이유는 교육기관의 정보보안 전담 관리자의 부재 및 교육기관의 특성상 일관된 정보보호정책 수립 및 시행이 어려운 것이 원인으로 분석되었다. 다음으로 월별 추이를 보면 교육기관과 지자체에서 지속적으로 많은 사고가 발생했으며 교육기관에 비하여 4월에는 국가기관이, 11월에는 지자체가 근소한 차이로 사고발생 비율이 앞서기도 하였다.



* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 4. 기관별 침해사고 발생 현황



* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 5. 월별 침해사고 발생 현황

2. 민간분야 사이버 테러 현황

2004년도 민간분야의 사이버 테러 발생 현황은 24,297건으로 전년의 26,179건에 비해 7.1% 감소하였다. 국가사이버 안전센터의 분석에 의하면 이는 스팸릴레이 사고건수가 60.1% 감소(8,276→3,297)하였기 때문이다.

표 5. 2004년 사이버 테러 발생 현황

일반 해킹	스팸 릴레이	일반 웜	합 계
16,027	3,297	4,973	24,297

* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

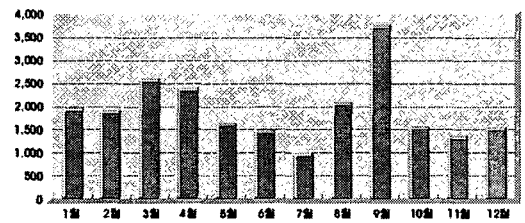
2.1 시기별 추이

최근 3년간 발생한 사고 발생현황을 보면 2003년에 대폭 증가한 발생건수가 금년에 약간 감소한 것으로 나타나고 있다.

표 6. 최근 3년간 침해사고 발생 현황

연 도	2002년	2003년	2004년
침해사고	15,192	26,179	24,297
증가율(%)	185%	72%	-7%

* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

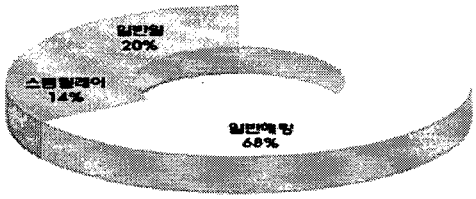


* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 6. 월별 침해사고 발생 현황

2.2 사고유형별 발생현황

사고를 유형별로 분류하면 일반해킹 68%, 일반웜 20%, 스팸릴레이 14%순으로 나타났다. 스팸릴레이 발생비율이 전년 대비 60% 수준으로 대폭 감소한 반면 일반해킹과 일반웜 사고가 증가하였다.



* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

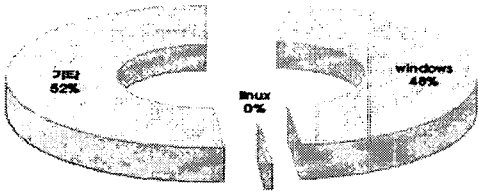
그림 7. 사고유형별 발생현황

공격유형별로 분류하면 웜이 감염 시도를 위해 스캐닝하는 유형의 취약점 정보수집(27%)이 가장 많은 것으로 나타났으며, 두 번째는 구성 설정 오류를 이용한 공격, 세 번째는 전자우편 관련 공격, 네 번째는 악성 프로그램을 이용한 공격 순이다.

* 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 8. 공격기법별 발생 현황

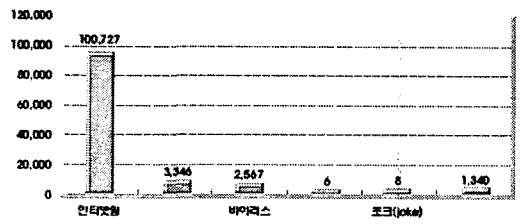
2004년 사고를 운영체제별로 분석하면 전년과 동일하게 윈도우 운영체제가 다수의 피해를 입었다. 기타는 운영체제를 확실하게 할 수 없는 시스템이지만 대부분이 웜·바이러스 피해를 입은 것으로 미루어 윈도우로 추정된다.



• 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 9. 운영체제별 발생 현황

2004년 한해 동안 웜·바이러스 등에 의한 피해건수는 총 107,994건으로 한달 평균 8,999건의 피해가 발생하였다. 전체 피해 중 상반기 동안의 피해 건수(72,225건)가 하반기에 접수된 피해건수(35,769건)보다 두배나 많았는데 이는 주로 상반기에 출현한 넷스카이, 베이글, 두마루, 마이둠, 사제르 등에 의한 것으로 파악되었다. 상반기 동안 웜·바이러스 등 악성코드로 인하여 총 72,225건 피해가 발생하였으며 주로 이메일 웜이 많았다. 관련된 주요 악성코드로는 1월에 출현한 베이글웜, 마이둠웜, 2월 넷스카이웜, 4월에는 아고봇웜, 5월에는 사세르웜, 6월에는 펍트로이안 등이 있다.

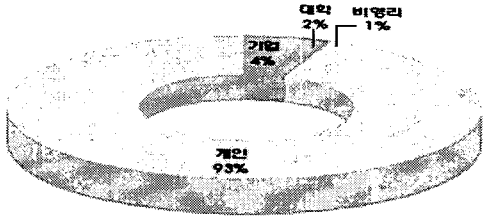


• 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 10. 웜바이러스 유형별 피해 현황

2.3 기관별 발생현황

2004년 민간분야의 사고를 기관별로 분류해 보면 개인 사용자가 93%로 가장 많은 피해를 입은 것으로 나타났다. 이는 일반 PC사용자가 백신프로그램이나 PC용 방화벽 등을 설치하지 않은 채 인터넷에 접속하여 웜·바이러스 악성 Bot에 많이 노출되었기 때문이다. 개인에 이어 기업이 두 번째 많은 피해를 입었으며 대학, 비영리기관 순서이다.



• 출처 : 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집.

그림 11.기관별 발생 현황

3. 사이버 테러리즘의 전망

지금까지 살펴본 사이버테러의 현황을 토대로 문제점을 보면 일단 기존의 운영체제 및 범용프로그램의 신규 취약점은 지속적으로 발표된 것이고 이들을 공략하기 위한 해킹프로그램이나 웜·바이러스가 출현하여 시스템 관리자들을 괴롭힐 것으로 예상된다. 또한, 기존 해킹기법의 틀을 벗어나 새로운 차원의 공격기법의 등장이 가속화 될 것으로 전망된다[6].

3.1 웜·바이러스 전파속도 가속화

인터넷 등 정보통신망의 발달은 신속한 정보 수집, 전송 등 지식기반 정보화 사회촉진에 기여하고 있으나 각종 신규 출현한 웜 또한 이를 기반으로 전파속도가 급격히 증가하면서 동시다발적인 대량의 피해를 야기하고 있다. 특히, 2003년 1월 25일 사상 초유의 인터넷 마비사태를 초래했던 슬래머웜은 376바이트 크기의 웜으로 출현 당시 단기간에 전세계 수많은 호스트를 감염시킨 바이러스로 악명을 떨쳤으며 손실액만 10억 달러에 이르는 것으로 나타났다. 이는 2001년도에 맹위를 떨쳤던 코드레드웜 보다 두배 가량 전파속도가 빠른 것이다. 전파속도가 빨랐던 가장 큰 이유는 기존의 웜이 사전 접속단계가 비교적 복잡한 TCP 프로토콜을 이용했던데 비해 슬래머웜은 사전 접속 과정이 필요 없는 UDP 프로토콜을 이용했고 MS사의 취약한 범용시스템을 공격대상으로 삼았기 때문이다. 이처럼 웜·바이러스가 증가하면서 파괴력이 강력해진 이유는 전자우편 및 프로그램 불법복제를 이용해 유포되던 기존 바이러스와 달리 자동으로 시스템의 취약점을 공격하여 유포되는 해킹기법을 적용하고 있기 때문이다. 또한 개인이 즐겨

사용하는 MS메신저 eDonkey와 같은 P2P 프로그램을 통해 확산되는 등 유포경로가 다양해졌고, 네트워크의 발달로 감염 후 순식간에 확산되어 대규모 피해를 유발함에 따라 해커들이 즐겨 찾는 수단이기 때문이다[7]. 향후에도 운영체제 및 응용프로그램 취약점을 이용한 웜 · 바이러스가 급증하면서 피해도 배가될 것으로 전망된다.

3.2 윈도우시스템 피해 증가세 지속

최근에 해킹대응 분야의 특징 중 하나로 미 MS사가 개발한 NT 및 Windows 2000 운영체제를 탑재한 전산 시스템에서 피해가 지속적으로 증가하고 있다는 것이다. 2000년도까지는 윈도우시스템이 리눅스 등 유닉스계열의 시스템보다 사고발생이 없어 상대적으로 안전한 시스템으로 인식되어 왔으나 2001년 초반부터 해커들의 반미 반MS 분위기 확산을 MS사 관련시스템에 대한 공격기법 연구 및 공개가 늘어나면서 피해도 급증하고 있다.

3.3 웹 해킹사고 증가

침입차단시스템 등 정보보호시스템 설치가 각급기관에 보편화되면서 외부에 공개할 필요가 없는 서비스 포트는 외부에서 접속하지 못하도록 아예 막아버리기 때문에 더 이상 해킹툴만을 이용한 과거의 손쉬운 해킹기법은 불가능해지고 있다. 따라서 해커들은 이러한 문제를 타개하기 위해 각 기관마다 외부에 개방하여 상시 서비스하고 있는 웹 서비스 포트 80번에 대한 공격기법을 연구하고 있으며 이에 대한 피해도 급증하고 있는 실정이다. 이러한 기법의 특징은 다른 해킹도구나 스캐닝도구가 전혀 필요없고 단지 인터넷에 접속할 수 있는 웹브라우저 하나만 있으면 된다는 것이다. 또한 웹프로그램은 보통 소규모 업체에서 제작하다 보니 기능과 디자인에만 치중한 나머지 보안을 고려한 코딩에 대해서는 관심을 갖지 못하는 것이 현실이며 주기적으로 갱신이 이루어지지 못하므로 취약점이 항시 내재되어 있는 것이 특징이다. 따라서 스크립트 카드로 알려진 초보자들보다는 전문해커에 의해 악용되고 있는 실정이다.

Ⅳ. 사이버테러리즘 대응방안

1. 우리나라의 대응법제

이상과 같이 살펴본 사이버테러리즘에 대한 우리의 현행 대응법제를 일별해 보면[8], 먼저 해킹에 관해서는 정보통신망법 제48조에 의한 정보통신망 무단침입죄를 적용하고 있으며, 해킹에 의한 비밀침해의 경우는 정보통신망비밀침해죄(정보통신망법 제49조, 62조)를 규정하고 있다. 또한 해킹이 수단이 되어 불법적인 재산취득이나 타인의 자료를 무단으로 삭제하는 경우는 컴퓨터사용사기죄(형법 제347조의 2)와 정보통신망정보훼손죄(정보통신망법 제49조, 62조)에 의한 대응을 하고 있다. 다음으로 바이러스의 제조 및 전달 · 유포에 관해서는 악성프로그램 전달 · 유포죄(정보통신망법 제48조 제2항, 제62조 제4호)를 통하여 대응하고 있다. 그러나 바이러스를 제조한 경우에는 아직까지 대응규정이 없는 현실이다.

2. 정책적 과제

2.1 종합적 대응체제 구축

사이버테러리즘의 경우는 오늘날 인터넷의 탄생과 네트워크의 발달로 이제는 네트워크라는 하나의 가상공간 속에서 쫓고 쫓기는 상황이 발생하였으며 각국에서는 위 가상공간의 질서유지를 위하여 투자와 노력을 아끼지 않고 있는 것이다. 이러한 맥락에서 국가와 국가, 국가와 민간단체, 민간단체간의 유기적이고 종합적 측면의 대응은 필수 불가결한 것이다. 사이버테러리즘에 대한 대응체제를 구축하기 위한 과제는 다음과 같다. 먼저, 사이버테러리즘에 대한 '종합적 대응체제를 구축'해야 한다. 이는 한 국가 내에서의 대응체제의 확립은 물론이려니와, 관련 사건의 발생시 신속한 압수 · 수색과 이와 관련된 광범위한 전산증거자료들을 효과적으로 수집하기 위하여, 원거리 또는 국가간 협력체제가 필수적이다. 또한 민간기관과의 협조 또한 필요불가결하다. 이는 사이버테러리즘은 다른 어떠한 유형의 테러보다도 종합적인 수사체제의 확립이 중요하기 때문이다.

현재 우리 경찰에서는 사이버테러 대응센터를 창설하여 해킹관련범죄와 바이러스관련범죄를 담당하는 수사

관, 협력관과 연구관을 두고 있다. 사이버테러 대응센터는 국내외 컴퓨터 통신망에 대한 24시간 검색·분석 및 수사체제를 구축하여 해킹이나 바이러스 범죄 등 전문적, 기술적 범죄사건은 직접 수사하고, 일반 사건은 각 지방청에 하명하여 수사를 하고 있다. 또한 국가정보원에서도 행정전산망 등 국가기간전산망의 보안에 각별한 관심과 노력을 기울이고 있고 주로 전산망 암호체제의 규제에 관한 외국의 동향을 예의 주시하고 이에 대한 국내의 문제점 등을 찾아내고 이의 개선방안이나 외국의 해킹 등에 대비한 대응방안 등을 강구하고 있다.

정보보호의 주관부처인 정보통신부는 정보화기획실 아래에 있는 정보보호과에서 정보화 역기능 방지 업무를 담당하고 있고, 정통부산하기관인 한국정보보호센타와 정보통신윤리위원회가 정보화 역기능 방지를 위한 지원업무를 담당하고 있지만, 사이버테러리즘에 대해서는 아직 그 개념조차 확립이 되어 있지 않은 현실이다.

2.2 전문인력의 확충

다음으로 사이버테러를 대응하기 위한 전문인력이 확충되어야 한다. 사이버테러리즘의 경우에는 테러리즘적 특성과 사이버범죄 특성의 양면성을 지니고 있다. 이는 테러리즘에 대한 개념적 정의조차 완비되지 않은 작금의 현실에서 비추어 보면 관련 전문인력은 컴퓨터에 관련된 전문지식을 갖추어야 함은 물론이고 아울러 테러리즘에 대한 전반적인 이해도 선행되어야 할 것이다.

2.3 민간부문과의 협조체제 강화

민간분야의 컴퓨터보안기구와의 상호협조체제의 구축 및 강화도 필요하다. 이는 주로 사이버테러가 컴퓨터를 통한 전산망을 중심으로 행해짐으로써, 전산망 보안기술에 관한 전문가조직, 예를 들어 사이버테러대응센터(Ctrc), 전산망보안센터(Certcc)나 인터넷 침해사고대응센터(CERT-Korea) 등으로부터의 전문적인 기술지원협력도 중요하다. 이러한 민간 분야의 역동적인 기술발전과 전문지식을 충분히 활용함으로써 사이버테러의 피해를 최소화하고 사회방위 책임을 완수할 수 있다. 따라서, 외부 자문위원을 위촉하여 적극적으로 활용하고, 한국정보보호센터 등 유관기관과 업무협조체제를 상호 잘 유지하고, 또한 사이버 공간에서 활동 중인 연구기관, 민간단체 또는 자원봉사자를 적절히 활용하여야 할 것이다.

2.4 국제적 정보교류 및 공조체제 구축

마지막으로, 국제적 정보교류 및 수사공조에 대한 협조체제 구축이다. 앞서 살펴본 바와 같이 사이버테러의 특징은 초고속 전산망을 통하여 국제적으로 국경을 초월하여 벌어진다는 점이다. 통상 국가간의 형사사법공조관계는 외무부를 경유하여 상대방 국가의 법집행기관의 형사사법업무의 공조를 요구하는 것이나 이런 경우 통상 1개월 이상의 상당한 기간이 소요되어 통상의 국제형사사법공조절차는 현실적으로 소기의 목적을 달성하기 어려운 것이 대부분이다. 사이버테러의 대응에 있어서는 보다 국제적으로 신속한 수사협력체제의 구축이 필요하기 때문에 각국 유관기관간의 국제적 공감대 형성과 구체적인 협력방안 협의가 시급한 과제인 것이다. 아직 테러리즘에 대한 국제적 논의가 진행중인 현상황에서는 과도기적으로 인터폴을 활용하는 것도 좋은 방법 중의 하나가 될 것이다. 국제적으로는 현재 국가간의 협약으로 체결하여 운영되고 있는 인터폴 내에 사이버테러만을 전문적으로 공조하여 처리할 수 있는 기구를 별도의 협약을 통하여 설치하고, 이를 운영하면서 서로의 정보교류 및 수사공조의 활성화를 모색할 수 있다.

V. 결 어

오늘날 현대사회는 하드웨어적 기술개발의 성과에 더불어 관련 제품의 저가화에 이은 소형화, 휴대화의 경향에 발 맞춰 관련 기술의 개발에 많은 노력을 경주하고 있다. 일례로 한국영화 초유의 천만명 관객동원 돌파의 신기록을 세우고 외국으로 수출하여 외화를 획득하는 등 우리의 영상산업을 한단계 끌어 올렸다는 평가를 받는 '실미도'나 '태극기 휘날리며' 등의 영화에서도 이러한 기술력에 기반한 '특수효과'가 없었다면 아마 불가능하였을 것이다. 이러한 순기능과 더불어 2003년 초에 발생한 슬래머웜으로 비롯된 인터넷 대란은 우리나라 초유의 대형 사고였으며, 정보화 강국이란 명성에는 어

울리지 않게 아직도 사이버테러리즘에 대한 대응은 아직 그 인식조차 확립되지 않은 현실이다. 이에는 많은 이유가 있을 수 있으나, 먼저 불법 복제품을 사용하는 것에 전혀 범죄의식이 없으며, 개인이나 조직이 영리나 조직 생존에 집착하여 보안을 소홀히 하거나 형식적인 보안관리가 만연하고 있고, 국가안보 차원의 공동 대응 개념을 간과함으로써 기관 · 단체별 정보공유나 협력체제가 발전되지 않은 것이 무엇보다도 큰 원인이라 할 수 있다. 이러한 사이버 테러리즘에 대응하기 위하여 먼저, 개별 기관별로 분산되어 있고 서로 유기적인 작용을 하지 못하고 있는 정책들을 통합하여 국가 사이버안전 보장을 위한 기본전략 수립하여야 한다. 이에는 범국가적 사이버테러 예 · 경보체제가 마련되어야 할 것이다. 지난 인터넷 대란의 경우에 슬래머웜이 발생한지 십여 분만에 미국 · 일본 등 전세계에 감염됨으로써 사고 이후의 수습 조치보다는 전자적 침해에 대한 사전 예방대책 강화가 무엇보다도 중요하다는 가장 큰 교훈을 알려 주었다.

따라서 앞서 살펴본 바와 같은 기관간의 정보공유분석의 연계 확대가 본격적으로 추진되어야 하며, 범국가적 예·경보 체계를 마련하여 사이버공격 기법을 수집·분석하고 사이버공격을 사전에 인지하거나 징후를 탐지하여 각급 기관에 신속히 경보하는 한편, 최신 사이버테러 대응관련 동향을 수집·분석·전파하여 예방대책 강구에 전력해야 한다. 정보화가 진전될수록 국가와 국가, 국가와 민간간의 네트워크 구성은 확산될 것이고, 이에 따라 보안취약 요인의 증가는 필연적이라 하겠다.

오늘날 사이버 테러리즘의 양상은 국가기관과 민간기관을 구별치 않고 있으며 또한 네트워크망을 통하여 취약지점을 통하여 다른 부분으로의 침투가 용이하게 변모해가고 있으므로, 이러한 대응체제들을 통하여 사이버테러리즘 예방활동을 강화하고 관련 첨단기술을 확보해야 하며, 무엇보다도 간과하지 말아야 할 것은 전문인력의 양성과 관련 산업의 육성 시에 철저한 보안의식의 함양은 물론 향후 더욱더 진일보해갈 사이버 시대에 걸맞는 윤리의식을 함양시켜야 한다.

저 자 소 개

[1] 동아일보, 2003.1.25. 1면.

[2] 남길현, 사이버테러와 국가안보, 국방연구 Vol.45. No.1, p.2, 2002.

[3] 이윤구. 사이버테러리즘의 실태분석과 대응방안. 한국경찰학회보 Vol.3, pp.5-8, 2001.

[4] 이강래, 사이버테러 현황과 대처방안 연구, 국정감사 정책자료집, 국회입법자료실, 2000.

[5] 국가사이버 안전센터, 2004년도 사이버 침해사고 사례집, 2005.

[6] 권선필, 지식정보사회의 향후구도와 한국의 효율적 정보화 전략 수립 방안 연구, 전자신문사, 2001.

[7] 국가정보원, 국가정보보호백서, 2004.

[8] http://ctrc.go.kr/rule/index.html.

저 자 소 개

오 태 곤(Tae-Kon Oh) 정회원

- 2000년 2월 : 조선대학교 법학과 (법학사)
- 2003년 2월 : 조선대학교 대학원 (법학석사)
- 2005년 2월 : 조선대학교 대학원 (법학박사)
- 2003년 3월~현재, 전남도립남도대학 경찰행정경호과 초빙교수, 조선대학교 법과대학 시간강사

<관심분야> : 컴퓨터범죄, 테러리즘