情 報 保 護 學 會 誌
第 13 券 第 5 號, 2003. 10

Security from Cyber Crime and Terrorism
- 사이버공간 보안의 현황과 대응방향 -

하 옥 현*

요 약

정보통신기술의 발달로 지식정보사회로 급격히 전환함에 따라 Computer system과 Internet에 대한 의존도가 높아져 생활이 편리해지기도 하는 반면 여러 가지 역기능도 보여주고 있다. 특히 새로운 공간인 Cyberspace에서의 여러 형태의 범죄와 Terrorism은 날로 심각한 충격을 주고 있어 그 Security가 확보문제가 시급하다. 본고에서는 이와 관련 최근의 Cyber Security의 Trends에 대한 명확한 인식과 향후 방향 설정에 도움이 되고자 한다.

Ⅰ. 서 론 : 정보사회 (Information Society)

1. 정보화의 진전

지금 우리가 살고 있는 21세기는 그야말로 정보시대(Information Age)가 될 것이라는 점을 이제 의심하는 사람은 없을 것이다. 이는 현재 진행되고 있는 정보통신기술의 발전이 그 기술적인 차원에서 가히 혁명적이기도 하지만, 그로 말미암아 일어나는 인간사회의 변화의 폭과 성격 또한 이전의 시대와는 판이하게 달라지고 있기 때문이다.

즉, 정보화의 진전에 따라 정보의 처리, 저장 및 전송의 속도와 양이 급격하게 증가하고 있을 뿐만 아니라 이용자 중심의 편리한 접근기술과 정보매체의 발달로 그 질적 수준이 날로 고도화되고 있으며 이들을 전 세계적으로 연결하는 Internet, CATV, 무선망 등 다양한 Network가 연결되고 있다.

이러한 정보통신기술의 혁신을 근간으로 그 구조가 새롭게 변화된 사회형태를 Post-industrial society[1] 로 불렀는가 하면 진행 중인 거시적인 사회변동을 "The Third Wave"[2], "Megatrends"[3], "The Age of Discontinuity[4]" 등으로 표현하기도 하였는데 최근에는 정보사회(Information society)라고 일컫는데 어느 정도의 공감대가 형성되었다.

정보사회의 가장 큰 특징은 개인과 기업 그리고 국가의 모든 주요 시설의 Computer Networking 일 것이다. 많은 부문의 Computer Network이 상호 연동되어 작업과 통제가 이루어지면서 교통, 통신, 금융, 에너지 및 주요 시설관리, 응급구호업무, 정부기능 등 오늘날 인간 삶의 대부분이 이에 따라 이루어지고 있으며 점점 더 심화되고 있는 추세이다.

과거에는 상상하지 못했던 dot com 기업들의 출현에 의한 e-Commerce, e-Business 그리고 e-Government 등 새로운 개념과 노력들이 진전되면서 지식과 정보가 생산, 확산되고 개인과 기업 나아가 국가경쟁력의 핵심요소로 자리매김하고 있다.

이에 따라 미국, 유럽(EU), 아시아의 주요 국가들은 자국의 경쟁력을 강화하기 위하여 국가전체를 대상으로 한 국가정보화의 Vision을 제시하며 초고속정보통신망 등 정부가 뒷받침하는 강력한 정보화 정책을 계획· 추진하고 있어 앞으로도 상상을 초월할 만큼 많

1) Daniel Bell, *The Coming of Post-Industrial Society*. New York, Basic Books,1973

2) A. Toffler, *The Third Wave*, N.Y.: Bantam, 1981

3) J. Naisbitt, Megatrends, N.Y.: Warner Books, 1982

* 경찰대학교 교수부장(경무관), 전 경찰청 사이버테러대응센터 단장 (okclub@empal.com)

은 발전이 있을 것으로 보인다.

1.1. 정보통신기술의 비약적 발전

정보통신기술은 비교적 짧은 역사밖에 가지지 못하였지만 그 어느 분야보다 큰 발전을 이룩해왔다. 특히 1950년대 이후 비약적으로 발전하기 시작한 반도체 chip 기술, 신소재 기술, Microprocessor 등의 컴퓨터기술과 Fiber optics, Satellites, Digital media 등의 통신기술이 그것인데 이는 흔히 'C & C 혁명(Computer & Communication Revolution)'으로 불리기도 한다.

이와 같은 정보통신혁명은 이전의 산업혁명과 비교하면 우선 기술의 기반인 동력원이 다르고 지리적 조건의 장애 없이 세계 어느 곳에서든지 일어날 수 있으며 일방적인 기술의 수혜가 아닌 인간과 정보 기술의 지속적인 상호작용을 특징으로 한다.

Computer의 출현은 도구적 차원을 넘어 Thomas Khun의 표현대로 오늘날 Paradigm의 전환을 초래하는 중요한 기술적 진보의 축이 되어 단순히 인간 삶의 외형만 바꾸는 것이 아니라 인간존재 자체를 동요시키면서 새로운 사회변동을 가져오고 있다.[5]

정보통신기술의 변화에 대한 가장 혁명적인 특징은 컴퓨터와 통신의 개별적인 기술적 발전뿐만 아니라 BT, NT 등 다른 분야의 기술들과 서로 융합 발전되어 가고 있다는 것이다. 이와 같은 정보통신기술의 융합화 현상은 과거에 볼 수 없었던 새로운 기술과 제품 및 서비스를 계속 선보이면서 그에 따른 광범위한 사회적 변화를 유도하고 있다.

1.2 Computer기술의 발달

오늘날의 정보사회의 발전에 공헌한 가장 핵심적인 원동력은 Computer기술의 급속한 발전이라 할 것이며 Computer 기능을 응용하지 않는 분야가 없을 정도로 그 활용범위와 잠재력은 방대하고도 강력하다.

Computer의 가장 기본적인 기능은 방대한 양의 정보를 신속하게 처리 분류 조작 저장 할 수 있다는 것이다. Computer는 발명된 지 50여년밖에 되지 않지만[6] 처음 등장한 이후 급속한 발전을 거듭 하면서[7] 우리 삶의 모든 측면에 영향을 미치고 있다.

Silicon chip이 개발되어 이용되면서 덩치가 크고 강력한 Main Frame Computer 시대를 지나 1971년 Microprocessor의 발명과 1980년대의 개인용 컴퓨터(PC)[8]의 일반 상용화에 따라 더욱 발전하게 된 Computer는 현대의 가장 기본적인 엔진이며 역동적인 도구로서 일상생활의 모든 측면에 깊숙이 스며들어 엄청난 효력을 발휘하게 되었다.

특히 언제 어디서 어떤 기기로든 Network에 접속해 원하는 정보와 서비스를 이용할 수 있는 환경인 Ubiquitous or Pervasive computing 시대가 열리면 일상생활의 많은 물건에 Computer - chip 또는 sensor - 가 탑재되어[9] 인간과 물건들 간의 연결이 가시화되는 것은 이제 시간문제로 보인다.

이렇게 되면 아주 작거나 눈에 보이지 않는 Microprocessor와 Laser 그리고 값싼 Sensor들이 결합하여 우리의 존재를 감지하고 우리가 원하는 것을 알아차리고 우리의 감정까지 읽을 수 있는 그런 환경이 될 것이다.

즉, 눈에 보이지 않는 편재한 Computer들은 눈에 보이지 않는 소리 Spectrum이나 전자기 Spectrum을 통해 주변을 감지하고 우리의 손과 몸의 위치를 탐지하며 얼굴표정까지도 읽어낼 수 있을 것이다.

또한 소형 Computer screen을 안경에 포함시키는 등 Wearable Computer가 등장하여 궁극적으로 모든 사람들을 World Wide Web(WWW)의 node로 만들어 줄 수 있을 것이며 이는 진료기록, 범죄기록, 기사 자료를 검색해야 할 의사, 경찰, 기자 등의 직업에 매우 긴요하게 이용될 수도 있을 것이다.

이처럼 Compute기술의 발전은 인간의 정신적 노동을 대체·확장하는 수준을 훨씬 뛰어 넘어 더욱 가

4) P. F. Drucker, The Age of Discontinuity: Guidelines to Our Changing Society, N.Y.: Harper & Row, 1968

5) Thomas S. Kuhn, *The Structure of Scientific Revolutions*, Chicago, University of Chicago Press, 1996

6) 1833년 영국의 수리학자 Charles Babbage에 의한 현대식 computer 기술의 발상인 기계식 전산기의 논리적 구상 이래 제2차세계대전 직후인 1946년 세계 최초의 현대식 전자컴퓨터 ENIAC(Electronic Numeric Integrator and Calculator)[1]이 개발되었다.

7) Moore's law : in 18 months, the processing power doubles.

8) 1972년 Xerox PARC에서 시험용으로 역사상 최초의 Personal Computer인 ALTO를 만들었고 이어 1977년 Apple사가 이 idea를 빌려 개인용 컴퓨터를 개발하고 이어 1981년 IBM이 개인용 컴퓨터 시장에 진출하면서 본격적인 개인용 컴퓨터 시대를 열었다.

9) Microprocessor의 가격이 지속적으로 하락함에 따라 Computer산업은 더욱 발전하게 되고 모든 제품과 공장, 주거, 사무실에 이르기까지 Chip을 내장시키는 경제적 Incentive가 커질 것이다.

속화되어 궁극적으로는 인간을 대신할 수 있을 정도의 지능(Artificial Intelligence)을 갖춘 지능형 미디어로서의 Computer도 머지않아 출현하게 될 것으로 보인다.

벌써부터 양자Computer의 개발이 가시화 되고 첨단 Computer의 설계 동향은 살아 있는 생물을 모방하여 서로 대화할 수 있는 Cyber-companion[10]의 생산을 위해 노력하거나 생물의 두뇌 기능을 그대로 모방하는 인공지능(AI)을 개발하는 project[11]가 진행되고 있다.

이렇게 Computer기술이 비약적으로 발전하게 되어 실생활에 구현되면 사물들끼리 Communication도 잘 되고 인간의 생활이 편리해지는 것은 당연하겠지만 이러한 것들이 모두 Network로 연결되는 만큼 Hacking의 우려도 많아지고 각종 Malicious code들로부터의 피해도 걷잡을 수 없이 확대될 것이기에 Security에 대한 전 세계적인 협조가 불가피하게 될 것이다.

1.3 Communication기술의 발달

Communication은 인간 본능의 발전적 확장으로 그 과정에서 새로운 지식과 정보의 생산과 교류를 끊임없이 드러내며 기술적 범용성을 가지고 인간의 사회화과정에 개입하고 있다.

Communication 기술은 19세기 말 Radio와 Television에 의한 전자미디어의 대중화 실현 이래 1970년대 이후 집적회로(Integrated Circuit), Digital technology 등을 활용한 값싸고 빠른 대규모 정보처리 및 전달 체계를 갖추어 시공간의 해방과 다양한 정보의 선택을 가능케 해주었다.[12]

1990년대 이후에는 하나의 정보채널을 통해 다양한 정보유형을 통합적으로 처리할 수 있는 Media convergence 또는 Convergence of communication mode가 이루어져 그 기술적인 구조는 물론 정보의 유형과 경계가 사라지게 하고 있다.

한편 오늘날 통신기술은 Computer와 결합되면서 혁명적인 변모를 겪고 있는데 의사소통과 제어의 범위를 거의 무한대로 확장시킴으로써 Computer Network를 통해 한 방향은 물론 쌍방향 또한 1:1은 물론 多:多 등 다양한 형태의 Communication을 가능하게 하고 있다.

더욱이 최근에는 이동전화나 PDA 등의 이동통신 단말기의 보편화와 Laser나 1970년대 개발된 광섬유(Fiber Optic)[13] 등의 이용 및 인공위성(Satellite), 공중파를 통해 시공간의 제약 없이 자유롭게 의사 소통 할 수 있는 획기적인 혁신을 이루고 있다.

이동통신(Mobile Communication)은 정보의 시간성이 중요시됨에 따라 시간과 장소에 구애받지 않고 언제라도 가입자가 전체 통신망의 기능을 사용할 수 있도록 하는 수단이라는 점에서 더욱 강조되는 필수적인 System이 되었다.

최근에는 기존의 이동전화의 한계를 벗어나 다양한 Multimedia 통신을 구현할 수 있는 IMT-2000[14] project 추진은 물론, 케이블 대신 무선주파수를 이용· 정보의 고속 전송이 가능한 Bluetooth, 무선 주파수 대신 적외선을 사용하는 IrDA 등과 같은 Mobile Interface 기술이 발전하면서 통신 미디어의 무선화가 가속화되고 있다.

또한 기존의 동축케이블(Coaxial Cable)을 대신하는 광통신기술은 광섬유(Fiber Optics)를 이용하여 전송의 효율성이나 다양한 Multimedia 기술 유도 면에서 Data 전송기술의 일대 혁명을 이루었다.

광케이블은 가볍고 작아 설치가 용이하며 Laser 빛을 이용하여 신호를 전송하기 때문에 전송량이 동축케이블의 약 80배로 탁월함은 물론 영상, 음향 등을 실시간 전송하여 Communication의 현실감을 높이고 외부에서의 도청이 어려워 보안성이 높다.

한편 통신위성(Satellite)의 개발과 일반화[15]로

10) www.media.mit.edu/ttt

11) Japan의 'Artificial Brain Project'

12) 이러한 새로운 communication technology를 기반으로 한 새로운 환경을 "télématique" (computer + telecommunication) 혹은 "compunication" (computer + communication)이라고 하기도 한다. Simon Nora & Alin Minc, *The Computerization of Society*, Cambridge, MA: MIT Press, 1980. Antony Oettinger, *High and Law Politics : Information Resources for the 80's*, Cambridge, MA: Bllinger, 1977

13) 광섬유 한 가닥의 지름은 100-수백μm로 머리카락 굵기 정도의 원통형 유리섬유이며 이 중심부의 Core와 그 주변의 Cladding은 서로 다른 유리 성분으로 빛의 굴절률이 달라 Core를 통해서 전달되는 신호가 밖으로 유출되지 않고 Core속에서만 머무르다가 목적지까지 전송된다

14) International Mobile Telecommunication-2000은 하나의 단말기로 multimedia 정보뿐만 아니라 internet service까지 제공하는 차세대 이동통신 서비스이다.

15) 통신위성의 기원은 1900년대 초 원거리를 쏘아올린 Rocket과 2차대전후 군사목적으로 우주 진입한 Spacecraft이

가능해진 위성통신은 광역화된 통신, 다수의 수신자에게 동일한 내용의 정보 제공, 회선설정에 있어 유연성과 신속성이라는 장점을 가지고 다양한 형태의 원격통신 서비스의 핵심요소로 활용되고 있다.

이처럼 Computer와 Communication기술은 상호 상승적 관계를 맺으면서 급속하게 결합되어 가고 있으며 이것이 현대 정보통신혁명의 방향을 선도하고 있다. 즉, 컴퓨터와 통신기술이 결합되고 컴퓨터 자체의 이동성과 휴대성이 증가함에 따라 컴퓨터는 Network로 연결되고 수많은 컴퓨터 사용자들이 Internet을 통해 전 세계적 Network에 쉽게 접근할 수 있게 되었으며 이러한 연결은 정보교환능력을 획기적으로 증가시켰다.

1.4 Internet과 WWW의 발달

Computer의 보급 확대와 Network 기술의 발달에 따라 이제는 Internet을 전혀 모르거나 Internet Website에 한 번이라도 접해보지 않은 사람을 찾아보기 어렵게 되었다. 그만큼 Internet과 WWW은 누구나 이용할 수 있는 동시에 또한 누구에게나 영향을 미치는 미디어가 되었다.

1.4.1 Internet과 WWW.

Internet이란 지역별 혹은 단체별로 운영되는 지역통신망 LAN(Local Area Network)을 거대한 Network로 다시 연결함으로써 각 Network 상호간의 정보교환을 자유롭게 하는 Network of Networks이다.

Internet에 연결된 Computer는 전용 Server로부터 원격접속(telnet), 파일전송(FTP), 전자우편(e-mail), 웹(Web) 등의 각종 service를 제공받는 계층구조(Hierarchic structure)의 Client/Server System과 그러한 구조를 갖지 않고 Network 상의 모든 Computer가 Peer라고 하여 동등한 상태로 각자 스스로 Network를 관리 유지하는 Peer-to-Peer System으로 운영되고 있다.

또한 각기 상이한 Network 간에는 Host Computer와 Terminal Computer의 기술사양에 따라 Computer Operation System이 상호 다를 경우 정보유통이 불가능하므로 이를 가능하도록 하기 위해 Internet을 위한 표준통신규약인 TCP/IP (Transmission Control Protocol/Internet Protocol)[16]를 이용하고 있다.

원래 Internet은 냉전 상태가 지속되던 1960년대 말 미국과 소련간에 핵전쟁과 같은 대규모 전쟁이 일어나 어느 한 시스템이 파괴되더라도 Computer망 자체는 계속적으로 사용 가능한 분산처리시스템을 개발하려는 미국 국방부(DoD) 연구 프로젝트의 산물인 ARPANET[17]에서 출발하였다.

1969년 이 ARPANET이 개설된 이후 원격통신인 e-mail, 자료 전송을 위한 Protocol 등이 개발되면서 다수의 대학과 기업들이 연결되어 1983년 이를 통칭해 Internet이라 부르기 시작하였으며, 1990년대 초반까지만 해도 주로 정부와 교육기관이 이용하였다.

World Wide Web(WWW, W3, Web)[18]의 개발 이후로 Internet이 일반인들에게 친숙하게 대중화되고 다양한 Multimedia 정보로 발전하게 되어 on-line service가 급증하는 등 비약적인 발전을 거듭하기 시작하여 오늘날에는 Internet 그 자체로 인식되고 있을 정도다.

이리하여 Internet은 수없이 많은 Web site로 수십억의 인구를 연결하는 지구 차원의 Knowledge network로서 언제, 어디에서나 누구든지 Real-time으로 접속하여 상호 대화하거나 정보공유를 가능하게 함으로써 인간의 생활양식을 크게 재편하고 있다.

즉 Internet에서 e-Commerce, e-Government, Financial transaction, Cyber shopping center, Cyber university, Cyber library 등 지능을 갖춘 기관과 거래들이 점점 더 확산되어 현실세계만큼

며 1957년 소련이 무인 우주로켓인 Sputnik를 쏘아 올린 후 최초의 통신위성은 1962년 미국의 AT&T와 NASA에 의해 발사된 Telstar와 1963년 NASA와 Hughes Aircraft Co.의 Syncom이었다. 일반화의 계기는 1972년 미국이 '우주개방정책'을 취하면서 군사적 목적에 한정되었던 통신위성 기술을 민간에게 개방하여 그 상업적 이용이 가능해지고 산업화하면서이다.

16) TCP는 정보 전송단위인 각 packet을 순서대로 배열, 복원, checksum, control하여 신뢰성을 제고시키는 역할을 한다. IP는 packet에 client address를 부여함으로써 전송되는 경로를 지정하여 원격지 computer간의 정보교환을 용이하게 한다.

17) 1969년 미국 DOD의 ARPA(Advanced Research Projects Agency)와 RAND사가 공동으로 추진하여 하나의 회선으로 다수의 이용자가 동시에 정보를 공유할 수 있는 Packet switching technology를 개발하여 ARPANET을 운영하기 시작하였다

18) 1989년 스위스에 위치한 CERN(European Particle Physics Laboratory)의 Tim Berners-Lee에 의해 처음 시작되었는데 Internet을 통해 text, image 등 다양한 Multimedia 정보를 Web browser를 사용하여 쉽게 검색할 수 있게 해주는 GUI(Graphic User Interface)의 Distributed network system이다.

일상화되어 가고 있다.

물론 Internet 사용자와 그 복잡성의 증대로 여러 가지 장애물들이 존재하는데 정보 전송폭[19]의 병목현상(Bandwidth bottlenecks), 아직 충분히 편리하지 않은 Interface, 보다 개인의 특성에 맞춘 관리자와 Filter의 미흡, 불완전한 Security 등 많은 문제점을 야기하고 있다.

현재의 Internet 주소체제인 IPv4는 32억 개 가량의 주소를 확보할 수 있지만 그 비효율적 할당으로 실제로 쓸 수 있는 주소는 5-6억 개 정도에 불과해 Network와 PDA, 각종 가전 제품 등의 기술이 급속히 발전하면서 이들이 접속할 수 있는 Internet 주소가 심각하게 부족해져 2007년에는 고갈이 예상되고 있다.[20]

이 문제를 해결하기 위해 차세대 주소체계인 IPv6를 개발 적용하기 위한 경쟁이 치열해지고 있는 가운데 미국은 2008년까지 국방정보망을 IPv6로 전환하고 그 Security를 대폭 강화한 새로운 통신망을 구축하기로 했고 일본은 1998년부터 'WIDE'란 Project를 통해 IPv6 기본기술을 개발하고 상용서비스를 시작하였다.

유럽은 1998년부터 IPv6와 관련된 각종 연구 Project와 기술개발에 나섰고 중국도 신식산업부 주관으로 IPv6망 및 응용기술개발을 본격화하고 있으며 한국은 2001년 "차세대인터넷 기반구축 계획"을 발표하고 다양한 연구 Project를 수행하고 있다.

1.4.2 Mobile Internet과 차세대 Internet.

이동통신 기술의 발달로 음성 중심에서 Data 중심으로 변화하고 Internet 이용에서도 유무선의 경계가 무너짐에 따라 Mobile internet service가 상용화되고 있다.

Mobile internet이 가능한 이동전화와 휴대단말기의 비중이 커짐에 따라 M-Commerce(Mobile commerce)의 중요성이 부각되고 있으며 기존의 전자상거래(e-Commerce)보다 편리하여 그 영역 및 이용자가 큰 폭으로 증가하고 있다.

또한 Internet 환경이 개발 초기에 비해 엄청난 속도로 발달해와 현재와 같은 Internet의 폭발적인 발전추세를 기존의 Network 기반 기술만으로는 더 이상 감당할 수 없게 되자 각국에서는 차세대 Internet[21] 개발을 서두르고 있다.

이와 관련하여 1996년 미국의 34개 대학을 중심으로 "Internet 2" project가 제안 되었고 정부 차원에서 이를 지원하기 위해 "NGI"(Next Generation Internet) project가 착수되었으며 캐나다, 유럽 일본 등도 이를 추진하고 있다.

그러나 "Internet 2" project도 풀어야 할 기술적인 문제들이 많은데 그 중에서도 특히 발달하는 전송망과 Network 기술에 비해 인력과 필수적인 운영 Software의 발달이 미흡하다는 것이다.

2. Cyberspace의 출현

2.1. Cyberspace

정보통신기술의 혁명적 발달은 Computerization, Networking, Flexibility를 통해서 Virtual reality가 현실이 되게 시간과 공간을 초월해서 인간의 삶을 디지털화(from atom to bit)[22]하고 또 무한하게 연결시켜주는 새로운 공간인 Cyberspace[23]를 열어주고 있다.

특히 Computer는 Internet, Usenet, BBS 등의 발달을 통해 종래의 정보의 처리와 저장뿐만 아니라 정보와 의사의 교환을 동시에 가능하게 하는 종합적 Communication의 Media로 발달하였으며 Cyberspace는 이러한 Computer network의 성장을 기반으로 형성되었다.

Cyberspace는 물론 물리적인 Real world는 아니지만 하나의 공간적 은유로서 그 속에서 정보의 축적과 교류의 확대를 통하여 새로운 사회적 관계의 형성과 인지적 경험을 가능케 하는 또 하나의 사회적 공간으로서 우리의 삶에 스며들었다.

---

19) Bandwidth란 sec.당 전송될 수 있는 정보의 양(bit)으로 기본적인 기준은 4 giga byte 정도인데 이는 장편영화 한 편에 해당하는 정보의 양이다.

20) 이론상 주소 사용능력은 32bit 체계를 활용하고 있는 IPv4가 2^{32} 인데 비해 128bit 체계로 이루어진 IPv6는 2^{128} 개로 거의 무한대에 가깝다.

21) 차세대 Internet이란 세계 각국이 정부와 대학 연구소의 3각 협력체제를 갖추고 더 나은 Internet 환경을 만들고자 연구 개발하기 위해 목표로 삼은 21세기형 Internet system으로 미국의 Internet 2, NGI(Next Generation Internet), Canada의 CA*net, 유럽의 TEN-34, TEN-155, 일본의 JGN(Japan Gigabit Network) 등이 그 project이다.

22) Nicholas Negroponte, *Being Digital*, 1995

23) Cyberspace는 William Gibson의 소설 *Neuromancer* (1984)에서 처음 등장한 용어로 현실로는 존재하지 않지만 Computer에 접속하여 있을 때 우리가 경험하는 가상(virtual)의 공간을 뜻한다

즉 Cyberspace는 물리적으로 Computer와 Computer network에 의해 창출되고 유지되는 영역이고 시간과 공간을 뛰어넘어 우리는 단지 ID(사용자 이름)를 가지고 접속할 뿐이다.

이 Virtual space에서 인간은 자신의 현실적인 사회적 위치나 Identity에 얽매이지 않고 스스로 만든 또 하나의 Identity(Dual identity)로 익명성을 유지한 채 현실 세계의 일상적인 일들을 영위하게 하고 있다.

Cyberspace의 출현은 과거 인류가 보고 느끼고 지각하지 못했던 새로운 신세계(Brand-New World)를 제시하며 새로운 질서를 창조하고 우리의 세계관을 확장시키고 있기에 우리의 생활에 미치는 충격은 훨씬 심대하다.

Cyberspace를 여론 형성의 장으로 이용하여 실제로 정부기관에서도 사이버여론을 정책결정과정에서 반영하려는 시도가 계속되고 있으며, 심지어 장관의 인선에까지 Internet을 이용한 추천 방식이 도입되기도 하였다. 2002년 대통령 선거에서도 Internet의 전파력은 기존 매체를 능가하는 영향력을 발휘했다.

2.2. Cyberspace의 특징

Cyberspace는 PC와 Internet의 확산과 함께 그에 대한 접근이 용이해지게 되면서 일반에 널리 알려지게 되었으며 기본적으로 시간적 공간적 제약에서 자유롭기 때문에 언제어디서나 접속가능하다.

또한 Cyberspace는 참여하는 개인들이 ID만 있으면 얼마든지 접속할 수 있다는 점에서 익명성이 보장되는 공간이고, 교류되는 정보의 내용을 임의로 가감·재생산할 수 있다는 점에서 고도의 편집성과 구성성을 지닌다.

뿐만 아니라 그것은 Hyper link에 의해 다선적으로 연결되는 복합적·중층적 구조를 지니고 있으며 모든 정보를 Real time으로 환원시킬 수 있어 신속성·즉시성을 지니고 있다.

그러나 Cyberspace의 가장 특징적 성격은 실물은 없지만 우리가 보고 느낄 수 있는 가상세계(Virtual world)혹은 가상현실(Virtual reality)로 엄연히 존재한다는 것이며 실제보다 더욱 현실적인 세계를 구현한다는 초현실성(Hyper-reality)일 것이다.

이러한 초현실세계로서의 가상공간은 컴퓨터 화면 속에 나타나며 그 활용여하에 따라 엄청난 효과의 창출이 가능한 것으로 현대사회의 사람들에게 새로운 활동영역을 제공함으로써 크나큰 반향을 일으키고 있다.

Cyberspace는 눈에 보이지는 않으면서도 현실적으로 존재하며 현실공간보다 많은 거래들이 Cyberspace에서 이루어지는 등 급속히 성장하고 있다. 따라서 Cyberspace는 '가상'이라는 의미보다는 눈에 보이지 않는다는 뜻에서의 '비가시성'의 의미에 중점을 두어야 한다.

특히 최근 유행하고 있는 Avatar, Cyber singer, Cyber model 등과 같이 Cyberspace에서 Character 형식으로만 존재하는 인물에 관한 것과 '바람의 나라'나 '리니지'와 같은 게임물에서의 Item의 거래나 Character에 대한 폭력 문제 등을 보면 Cyberspace에서 생활하는 '네티즌'들에게는 물리적 공간에 살아있는 생명체 못지않게 중요시하고 있다는 것을 알 수 있다.

그러나 Cyberspace는 통합적·인과적 사고보다는 분할적·조합적 사고를 고취시키며, 논리적인 사변이나 성찰보다는 무기력한 몽상과 도피·파괴심리 내지는 사이버중독을 조장한다고 비판받기도 한다.

Cyberspace에서 특정한 사람의 모습을 Character로 만들어 강간이나 끔찍한 살인과 같은 장면을 공개적으로 연출할 경우 등은 이를 단순한 '가상적'이라는 이유로 아무런 제재도 가할 수 없다면 또 다른 문제를 야기할 수도 있을 것이다.[24]

2.3. Cyberspace의 전망

Cyberspace는 최근 정보검색 등을 위한 도구적 용도를 넘어선 사회적 접촉공간으로서 새로운 생활 영역으로서의 역할을 강화시켜 가고 있다.

H. Rheingold는 컴퓨터매개 커뮤니케이션(CMC : Computer-Mediated Communication)에 의존한 사이버사회론을 제기하고 있다[25]. Cyberspace가

---

24) 경찰청 사이버테러대응센터(CTRC)에 신고되는 사건 중 네트워크 게임인 '리니지'에서 사용하는 character가 피격을 당해 살해되고 무기로 사용되는 item이 도난당했다며 범인을 잡아달라고 호소하는 경우가 많다. 그러나 현행법상 게임속의 character를 보호하기 어렵고 분실한 item도 '재물'로 보기 어려워 hacking행위와 같이 다른 특별법을 위반한 경우가 아니면 형법상의 절도죄로 처벌하기 어렵다. 이러한 설명을 하면, 많은 시간과 돈을 들이고 정열을 바쳐서 만든 게임속의 character나 item이 자신의 분신이라며 그 character가 살해될 때는 자신이 살해되는 것과 같은 피해의식을 갖게된다면서 매우 흥분하는 경우가 있는데, 이는 실제 게임에 빠져보지 않은 사람으로서는 이해하기 쉽지않은 일이다.

25) H. Rheingold, *The virtual community*, 1994.

인간의 Communication 능력을 확장시키는 영역이므로 그곳에서는 새로운 인간교류의 고리가 형성될 수 있다는 것이다.

그렇지만 인적 교류공간으로서의 Cyberspace에는 부정적인 면도 존재 한다. 즉 Cyberspace에서는 자제심을 비롯한 에티켓과 규범 등이 사라지는 일이 많아 자칫 참여하고 이용하는 사람들에게 심적 상처를 가하는 일이 종종 있음을 보게 된다.

그것은 단순히 Cyberspace 상에서 신분이 밝혀지지 않는다는 익명적 상황뿐만 아니라, 오히려 자신이 유한한 실존이라는 Identity가 Cyberspace에 들어서면서 이미 자기도 모르게 사라져 버리는 현상에서 비롯될 것이다.

그럼에도 불구하고 Cyberspace에서의 Community 형성을 지극히 낙관한다. 즉 인류 역사에 있어 공동체의 발달은 대체로 지역공동체로부터 의식공동체로 진전되어 왔으나 이제는 지역이나 의식을 지나 욕구나 관심에 근거한 인간적 유대를 지향하는 문화공동체의 형성이 Cyberspace 상에서 가능해지고 있다는 것이다.

이러한 Cyber Community의 가장 결정적 특성은 탈공간화, 즉 지역성을 초월한다는 것이므로 이는 자동적으로 Global Community를 지향하며, 또 이러한 진전은 시공간을 초월한 가상적 연대(Cyber bond)를 통한 새로운 사회통합의 가능성을 보여주고 있다.

최근 개인간의 인간적 Communication이라는 기본적 욕구에 부응하는 가상공동체를 넘어 e-Government, News group이나 Cyber university 같은 지식정보의 공유를 주목적으로 하는 기능적, 편익 추구적 공동체 형성 또는 Cyberspace 에서의 상업적 이익 추구를 위한 e-Commerce 관련 site들도 활발히 운영되고 있다.

이제 Cyberspace는 공동사회(Gemeinschaft)와 이익사회(Gesellschaft) 모두를 포괄하는 인간의 총체적 생활공간으로서 활발히 이용되고 있으며, 현실적 한계들을 해소시켜 주기도 하고 동시에 위협을 받기도 하는 새로운 해방적 대체공간으로서의 그 기능을 계속해서 확장해 나아갈 것으로 보인다.

인류 역사 중 중세까지는 지중해를, 근· 현대에는 대서양과 태평양을 지배한 민족이 세계의 지배자였다면, 앞으로는 Cyberspace의 지배자가 세계를 지배할 것으로 전망되기도 한다.

그는 선의의 시민들을 연결하는 가상공동체의 미래를 매우 희망적으로 묘사하고 있다.

3. 정보화 환경

정보화의 진전에 따라 세계적으로 Computer의 보급과 Internet user들의 급격한 증가를 보이고 있다.[26]

세계적으로 Internet user는 2002.9.로 6억 명을 넘어섰으며 한국의 PC의 보급률은 세계 9위인 1가구당 0.9대, 1개 사업체당 21.9대이고 Internet user는 약 2,670만 명으로 집계되고 있다.

Internet User 현황

구 분	1998년	1999년	2000년	2001년	2002년
한국(천명)	3,103	10,860	19,040	24,380	26,270
세계(백만명)	160.0	276.0	407.1	513.41	563.0

미국은 세계 최초로 1969년 ARPANET 이후 1992년 WWW, 1993년 Internet Browser가 등장하여 Internet Boom이 일어났다.

한국은 1982년 최초로 서울대와 ETRI간 System 연결로 Internet 통신이 시도된 이래 1994년 상용화된 이후 급속히 확산되었고 1998년 초고속Internet 서비스와 1999년 무선서비스의 개시 등으로 Internet 이용이 더욱 활성화 되었다.

특히 초고속Internet[27]은 도입 4년 만에 1,000만 회선을 넘어섰고 2002년 말에는 인구 100명당 20명이 이용하게 되는 등 국내 Internet 상용화 9년 만에 전체 인구의 58%가 이용하고 있어 단기간에 세계 최고의 수준에 이르고 있다.

이처럼 Internet user가 팽창하면서 기존의 경제활동과 산업에 막대한 가치가 새롭게 창출되었으며 정보의 공유 등으로 생활이 편리해지고 Internet투표, 사이버선거운동 등의 전자민주주의가 확산 되는 등 새로운 정보문화가 조성되고 있다.

그러나 국가 사회 및 인간생활이 전반적으로 Computer와 Internet 등 정보시스템에 대한 의존도가 심화되어 감에 따라 그에 따르는 상대적 격차(Digital Divide)와 불건전 이용행위 등 역기능 또한 만만치 않다.

26) 한국네트워크정보센터, "인터넷 이용자수 및 이용행태 조사" 2002.12.

27) 초고속 Internet은 전화선 56Kbps보다 훨씬 빠른 수 Mega bps의 service로서 ADSL, VDSL, Cable Modem, LAN, Satellite 등을 이용한다.

더군다나 Computer system과 Network 자체가 갖고 있는 본원적인 여러 취약성(Vulnerabilities)들 즉, Internet의 개방·소통 지향적 운영체계, 각종 program 등의 bug 존재, UNIX, TCP/IP 등의 Source 공개 등과 어울려 공격 Tool 습득과 사용의 용이, System Admin. 등의 보안의식과 능력 부족 등으로 공격자들에게 매우 좋은 환경을 제공하고 있다.

이처럼 충분히 완벽할 수 없는 취약성을 가진 정보시스템 상에서 상호 존중되어야 할 네티켓과 규범 및 보안의식 등이 제대로 형성되지 않은 채 종종 들이닥치는 대란으로 인한 광범위한 피해를 겪으면서 위협에 직면하고 있다.

위협(Threat)에는 물리적인 성격의 것도 있지만 Cyberspace 상에서는 개인이나 조직 또는 국가에 의해서 각기 목적에 따라 다양하게 수행될 수 있는것으로, 정보시스템에의 의존도(dependency)와 Internet user가 증가할수록 그 피해규모가 심각해져 날로 신뢰성의 위기에 처하고 있다.

이러한 Cyber threat은 악의적인 목적으로 Computer system과 Network로 이루어진 Cyberspace 자체에 위해를 가함으로써 정상적인 기능 수행을 방해하는 일체의 과정과 행위라고 할 수 있으며 이들을 Cyber Crime과 Cyber Terrorism 으로 범주화할 수 있다.

II. 사이버 범죄와 테러 (Cyber Crime & Terrorism)

1. Cyber crime & terrorism의 개념과 의의

최근 일상생활에 Computer가 널리 보급되고 Internet이 광범위하게 이용됨에 따라 사이버공간이 중요한 생활공간으로 등장하면서 인터넷의 익명성, 비대면성, 우회성과 탈시공간성을 이용한 많은 범죄들이 출현하고 있다. 이처럼 Cyberspace에서 발생하는 모든 범죄를 총칭해서 넓은 의미의 Cyber crime이라 한다.[28]

이러한 Cyber crime은 Computer가 널리 보급되면서 또는 이들이 Networking 되어 Cyberspace가 형성되면서 새롭게 등장한 것으로서 종래의 범죄행위와는 그 수법이나 그들에 대한 수사기법은 물론이고 정책적인 면에서도 달라 특별히 'Cyber crime'이라는 Category를 정하여 연구하고 대응책을 마련할 필요성이 높아지면서 등장한 개념이다.[29]

Off-line에서의 범죄와는 달리 취급해야 할 필요성과 복잡성 그리고 이들을 둘러싼 정책적 대응 등의 환경이 급속히 변화되고 있기 때문에 새롭게 등장 하는 이러한 현상을 신속하게 포착하여 일관성 있게 다루는 작업이 필요하게 되었다.

이 Cyber crime은 크게 두 가지 유형으로 나누어 볼 수 있는데 하나는 통상 쓰이는 좁은 의미의 Cyber crime이고 다른 하나는 최근 주목을 끌기 시작한 것으로 Cyberspace를 구성하는 Computer system이나 Information and Communication Infrastructure에 대한 의도적인 공격으로 Cyberspace 자체의 Security를 위협하는 Cyber terrorism이다.

1.1. Cyber crime

좁은 의미에서의 Cyber crime은 Cyberspace라는 새로운 공간을 이용하여 전통적인 범죄행위를 저지르는 경우를 말하며 Cyber gambling, Cyber stalking과 성폭력, 사이버 명예훼손과 비방, Internet을 통한 사기·매매춘·음화판매·마약밀매 등이 있다.

이러한 범죄들은 전통적인 범죄와 본질적으로 다를 바가 없는 것처럼 보이지만 피해정도나 확산 속도는 물론이고 그 행위를 입증할 증거확보, 제시나 수사기법에서 전혀 다른 특성을 보이고 있기 때문에 종래와 같은 접근방법으로 다루기 어렵다.

---

28) Cyber crime and terrorism과 관련된 문제들을 논의할 때 아직 혼란을 느끼는 경우가 많이 있다. 그 이유는 Cyberspace의 출현 자체가 최근의 일이어서 익숙하지 않은데다 현대의 정보통신기술에 의해 형성된 생활공간이기 에 기술적인 어려움들이 혼란을 가중시키고 있으며, 그 변화의 속도가 너무나 빨라 따라 잡기가 쉽지 않기 때문일 것이다. Cyberspace는 시간과 공간의 제약이 완화되고 익명성과 비대면성이 보장되며 다량의 정보가 손쉽게 처리될 수 있어 이에 대한 대응에 새로운 준비가 필요시 되고 있으며 특히 Privacy, Information security, Information warfare 등의 측면에서 새로운 주목을 받고 있다.

29) Cyber crime과 유사한 개념으로서 Computer crime, Computer-related crime, High-tech crime, Information crime 또는 Internet crime 등이 실무상 사용되면서 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록과 관련된 범죄행위 또는 Internet을 통하여 이루어지는 범죄라는 개념으로 사용되었다. 그러나 이러한 개념은 초점이 독립적인 '컴퓨터 등 정보처리장치', '전자기록 등 특수매체기록' 또는 'Internet'이라는 범행도구나 범행대상에 맞추어져 있어 새롭게 등장한 Cyberspace에서 발생하는 다양한 범죄현상을 망라하기 어렵고, 좀더 포괄적이고 유연한 개념을 사용할 필요가 있다는 점에서 종래의 개념들을 포괄하여 Cyberspace에서 발생하는 모든 범죄행위를 총칭하여 Cyber crime이라는 개념을 사용한다.

1.2. Cyber terrorism

Cyber terrorism은 Cyberspace와 Terrorism의 결합 형태로 그 개념을 파악할 수 있다.

즉, Cyber terrorism은 개인이나 조직 혹은 국가가 정치적, 사회적, 민족적, 종교적 목적 등의 달성을 위해 Computer system, Network 등 정보통신수단에 위해를 가하여 이를 교란, 마비, 파괴 시키거나 유통·저장되는 정보를 저해함으로써 사회의 불특정다수인에게 불안감·공포심·혼란 등을 조성하거나 인식과 정책의 변화 등을 기도하는 행위를 말한다.

또한 비록 정치적 목적 등이 분명하지 않거나 약한 공격이라 할지라도 단순한 장난으로 넘기기에는 terrorism에 상당한 형태를 띠고 있는 경우 그러한 공격들이 의도되었거나 심각한 손해를 입혔거나 국가에 의해서 지원되었다면 Cyber terrorism으로 볼 수 있을 것이다.

Cyber terrorist들은 이러한 목적 달성을 위해 여론을 환기하고 상대방에 타격을 가하려고 Privacy 침해로부터 조직이나 사회 공동체의 분열과 불안감 조성, National security 위협 등 다양한 형태의 공격을 가하고 있다. 전기와 통신, 교통의 두절은 물론 금융업무의 마비, 막강한 군사력 운영의 무용지물화 등이 그러한 일례이다.

Off-line에서의 Terrorism은 폭력, 암살, 인질극, Hijacking 등 이를 계획 준비하고 실행하는데 막대한 경제적 비용과 생명의 위험이 따르는데 비하여 Cyber terrorism은 경제적으로 저비용이고 원거리에서 실행할 수 있어 인적 위험이 없으며 직접적으로 폭력을 행사하지 않는다.

최근에는 이 Cyber terrorist들이 각종 범죄조직, 군 또는 정보기관 혹은 각 국 정부에서 양성, 지원 되거나 또는 대리인으로서 Cyber terrorism을 수행하고 있다는데 더 큰 심각성을 자아내고 있다. 이들은 Hacking, 암호해독, 각종 Malicious code 제작 기술 등을 가지고 Target이 되는 상대방의 Network나 저장된 정보에 침해를 가하여 정치적 군사적 경제적 목적을 달성하기 위하여 치열한 물밑 Information Warfare를 벌이고 있다.

2. Cyber crime and terrorism의 특징

Cyber crime and terrorism은 현실공간에서 발생하는 전통적인 범죄와 많은 면에서 차이가 있어 이들 차이점을 분명하게 인식하고 이에 대한 적절한 대응책을 강구해야 할 필요가 있다.

2.1. Cyber terrorism의 목적과 수단의 고도화

자기과시, 자기만족, 경제적 이익추구 등 통상적인 Cyber crime과는 차원을 달리 Cyber terrorism의 경우에는 확실한 정치적, 사회적, 민족적, 종교적 목적 등을 가지고 국가 사회 전반의 혼란을 초래할 수 있는 무차별적 공격을 Cyberspace에 가하는 경향이 있다.

국가 사회의 정보통신 Infrastructure를 침해함으로써 이를 담보로 또한 전 세계 대다수의 Internet user들을 대상으로 그들이 추구하는 목적을 알리고 정당화시키며 인식과 정책의 변화를 기도하거나 목적에 따른 실리를 추구하고 있다.

공격 수단 또한 기술의 발전과 함께 날로 고도화되어 흔적을 남기지 않아 System Administrator 자신들도 침입 사실을 모르게 하거나 추적에 곤란을 주는 수단들이 개발 되어 이용되고 있다.

2.2. 신속한 수행, 전파능력과 막대한 피해규모

Computer와 통신이 발달하면서 많은 정보와 운영이 집중관리 되고 대량으로 신속한 전달이 가능하게 되었다. Internet이 연결된 곳이면 어느 곳에서라도 자세한 정보검색이 가능하며 또한 그 방대한 자료들을 일순간 Download하거나 전달 또는 침해할 수 있다.

그에 따라 그 전파력과 피해규모 또한 추산하기 어려울 정도로 매우 광범위하게 미친다. 2002.2 미국 Amazon, Yahoo, CNN, eBay 등에의 DDoS 공격, 2001.7 Code Red worm, 동년 9월의 Nimda worm 등에 의한 사고가 그러한 사례들이며, 최근 '2003.1.25. Internet 대란'으로 보도되고 있는 Internet 접속 불능사태의 발생도 사실은 작은 Worm virus인 'Slammer Worm'이 단 10분만에 Internet의 전파력을 타고 전세계에 퍼져나가 큰 피해를 주었다.

은밀한 사생활을 담은 Video tape나 유명 연기자의 정사장면을 담은 동영상(O양, B양의 비디오 등) 그리고 목욕탕이나 화장실, 심지어 모텔과 같은 곳에 설치된 몰래 카메라에 의해 제작된 Video tape가 Internet의 전파력을 타고 단기간내 퍼져나가 개인적, 사회적으로 큰 반향과 피해를 일으키기도 하고 때로는 검증되지 않은 정보의 유통, 유언비어 유포의 진원지가 되기도 한다.

이러한 이유로 인권이나 Privacy와 관련 새로운

문제가 나타나고 있다. 과거에는 개인정보 침해가 주로 국가나 공공기관에서 운용하는 대형 Database에서 발생하여 문제가 되었으나, 최근에는 개인이나 기업 등에서 개인정보를 쉽게 수집하여 판매하는 사건이 종종 등장하고 있다.

특히 일부 기업들은 고객의 직업, 연봉 등 상세한 신상정보를 입수하여 영업에 이용하고 있는데 경우에 따라서는 이를 유출시키거나 이에 대한 관리를 소홀히 하여 범행에 의한 막대한 양의 고객정보 유출 위험에 노출되고 있어 또 다른 불안을 주고 있다.

2.3. Cyberspace의 특성으로 인한 특징

A. Cyberspace의 비대면성 관련

Cyberspace의 가장 큰 특징으로 Cyberspace에서는 현실 세계와는 달리 사람들이 활동하면서 직접 대면할 필요가 없다는 것이다. 정보의 검색, e-mail, chatting, shopping, 금융거래 등이 상호 만날 필요가 없이 이루어지고 있는 불가시적인 생활공간이다.

이러한 비대면성은 많은 이용자에게 편익을 제공하지만 범죄자에게도 자신의 모습을 드러내지 않고 범죄행위를 할 수 있는 이점을 제공한다. 피해자의 입장은 아랑곳없이 적나라하거나 대담한 표현과 행위들을 쉽게 하기도 하며 자신의 행위로부터 별다른 죄책감도 느끼지 못한다.

B. Cyberspace의 익명성(Anonymity) 관련

Cyberspace는 자신의 신분을 노출시키지 않은 채 ID와 IP Address 또는 Domain Name을 중심으로 접속 운영되고 있어 행위자가 실제로 누구인지 파악하기 어려운 경우가 많다. 더구나 Internet café(PC방)나 실습실, 공중PC의 경우에는 Computer 사용자 특정이 더욱 곤란하다.

이러한 익명성이 보장되는 환경은 범인 추적을 어렵게 하고 쉽게 범죄 유혹에 빠지게 하여 Hacking, Malicious code 유포, Internet 사기, 음란물 유통 등 많은 범죄행위의 증가요소로 작용한다.

C. Cyberspace의 탈시·공간성 관련

Cyberspace는 언제 어디에서나 접속이 가능함 으로써 시간과 공간의 제약을 없애주고 있다. 즉 24시간 원격접속이 가능해 범죄를 꾀하는 사람에게는 아무 때고 범행 가능한 시간이며 남몰래 신분을 위장할 필요도 없이 국경을 넘나들며 Network를 얼마든지 이용할 수 있다.

한국정보보호센터 발표에 의하면 우리나라에서 발생하는 해킹사건의 87%이상이 외국에서 침입하고 있다고 한다. 따라서 Cyberspace에서의 국경 개념은 사라지고 국가간 상호협력이 요구되고 있다.

2.4. Cyber terrorism의 심각화

과거에 Cyber terrorism은 상당수준의 Computer 지식과 기술이 있어야 가능한 것으로 인식되었으나 최근에는 Internet에 들어가서 Hacking 방법이나 Virus 제작과 관련된 세련되고 자동적인 Tool들을 얼마든지 무료로 얻어 이용할 수 있기 때문에 초보적인 실력과 의지만 있으면 누구나 쉽게 할 수 있게 되었다. 따라서 범행을 기도하려는 자들에게는 Internet의 정보공유 환경과 개방적 구조가 자신의 목적을 이룰 수 있는 좋은 환경을 갖춰준 셈이다.

필요로 하는 해당 정보가 저장된 Network을 뚫고 들어가 국가기밀이나 산업기밀, 개인정보 등을 빼내갈 수 있고, 항공망을 교란하여 비행기가 공중에서 충돌하는 사고를 일으킬 수도 있으며, 병원의 환자 진료기록을 변경함으로써 과실을 유도하여 환자에게 치명적인 위해를 가할 수도 있다.

2003. 1. 25. 한국의 Internet 사용을 일시에 중단시킨 'Internet 대란'은 이러한 Cyber terrorism의 심각성을 실감케 한다. 동일 14:10분경부터 Internet 접속지연 현상이 발생하면서 시작된 이번 사고는 'Slammer Worm'이 단 10분만에 전세계로 전파되는 역사상 가장 확산속도가 빠른 Internet Worm Virus였으며 특히 한국에 대규모의 피해를 안겨주었다.

Internet Data분석협력협회(CAIDA)의 보고에 따르면 'Slammer Worm'은 1. 25. 05:30 (GMT) 처음 출현, Microsoft사의 Data Base용 S/W인 SQL Server의 취약점을 공격하기 시작해 매 8.5초마다 두 배로 확산되는 가공할 전파속도를 가지고 있었다. 이에 따라 10분 만에 취약한 Host의 90%가 감염됐으며 출현 후 3분경 Worm의 전파속도가 최고조에 달한 시점에선 Network를 통해 Worm이 5,500만회/sec의 DNS quarry를 보낸 것으로 되어 있다.

'Slammer Worm'이 Computer에 피해를 주는 악성 명령어를 포함하지는 않았고 단지 Network의 엄청난 확산속도를 악용하고 있다는 점에서 그 심각성이 노출되었다. Internet이 가져다주는 편익 중의 하나가 바로 이러한 빠른 전파속도인데 'Slammer Worm'은 이 장점을 그대로 역이용하였다. 이처럼 Cyberspace

공격자들은 Internet의 구조적인 허점(Security hole)을 찾아 공격하고 있는 것이다.

2.5. Cyber war, Net war, Information warfare

Cyberspace에는 우리의 삶에 유익한 양질의 정보가 많이 있는가 하면 범죄를 유발하거나 도구로 쓰일 수 있는 해로운 정보도 많이 떠다니고 있다. 또한 Cyberspace에는 국경이 없어 아군과 적군, 전방과 후방의 구별 없이 모두가 같은 공간에서 함께 공존하고 있다.

Cyber terrorism은 점점 전쟁과의 구분이 모호해지고 공격의 주체는 물론 누가 공격을 당하고 있는지도 파악하기 힘들며 Network을 통해서 접근할 수 있는 곳이면 어디든지 전장이 될 수 있는 전선없는 전쟁이 되어가고 있다.

이제 Cyber terrorism은 몇몇 특정 국가만의 문제가 아니고 점점 더 확산 일로에 있어 그 위협은 매우 심각한 상황에 이르고 있다. 기존의 Hacker들이 자기과시나 경제적 이익보다는 정치적 명분을 추구하는 Hacktivist로 활동하거나 Cyber terrorist로 바뀌는 것도 그 확산 요인이 되어 새로운 국제적 불안을 조성하고 있다.

또한 국가나 특정 집단간에도 쉽게 Cyber war 또는 Net war로 진입하는 것을 종종 볼 수 있다. 1991년 Gulf war 발발 전후 미국 등의 연합국 측에서 미리 상대국인 이라크의 방공망을 마비시켜 전쟁을 승리로 이끌었고, 1998. 6. 인도가 핵실험을 단행한 직후에 네덜란드와 영국의 대학생들이(Hacker group : miwOrm) 인도 바바원자력연구소(BARC)의 Web site에 핵무기를 상징하는 버섯구름 사진을 게재하였으며, 1998.9. Portugal hacker들이 Indonesia 40여개의 주 Computer에 침입 East Timor의 해방을 주장하며 Indonesia의 인권상황을 비난하였고, 1999년 Kosovo 전쟁에서 미국에 대항해 Yugoslavia의 많은 Hacker들이 미국의 White House 등 Internet site를 집중 공격하여 마비시킨 바 있으며, 2001.5. 미국의 EP-3 정찰기 사고에 의해 촉발된 중국 Hacker들이 미국의 White House 등 주요 site에 Cyber war를 감행하였다.

3. Cyber crime and terrorism의 수법

Cyber crime과 Cyber terrorism에 이용되는 수단은 다양하며 새롭고 강력한 기법들이 계속 시도되고 있는데 특히 날로 발전하며 큰 피해를 주고 있는 Cyber terrorism과 관련된 대표적인 수법을 살펴보면 다음과 같다.

3.1. Hacking 또는 Cracking 기술

가장 많이 쓰이는 기술로 Computer system이나 Network의 취약점(vulnerability)을 이용하여 불법적으로 접근한 후 자료의 유출, 위,변조, 삭제, 시스템 장애 및 마비를 유발시키는 공격이다. 주로 UNIX 계열 OS나 Microsoft의 Window 95, 98, NT system 등을 공격하거나 CGI(Command Gateway Interface)의 취약점을 이용하여 Web server나 Homepage를 공격하는 등 다양하고 복잡한 기법을 사용한다.

가장 손쉬운 방법으로 시스템의 기본적인 환경설정 변수(Environmental variables)나 각종 응용 S/W의 Bug들을 이용하는 경우이다. 정상적인 다른 사용자의 ID나 Password를 도용하여 당해 system을 이용하거나 Internet에 연결되는 다양한 운용체제의 환경설정 변수들의 오류 또는 공유 환경과 FTP, Telnet, SendMail, Web program 등의 Bug들을 이용하여 Root 권한을 획득한 후 당해 system을 Hacking하게 된다.

또한 Security 취약점 점검을 위해 개발된 Tool들을 오히려 Hacker들이 악용하여 hacking을 위한 수단으로 사용되고 있다. Monitoring tool인 Tcpdump, Sniffit, Snoop, Ethereal과 Password 점검 Tool인 password crack, L0phtCrack, 내부 취약성 점검 tool인 COPS(Computer Oracle and Password System), Tiger, Tripwire,과 원격 점검 tool인 ISS, SAINT, SATAN, Shadow Scan, Sscan and mscan, Nmap and Xnmap 그리고 Back Oriffice, School Bus, Net Bus, Subseven, Peekerbooty, Camera/Shy 등이 그러한 대표적인 Tool 들이다.

3.2. Internet Network Protocol의 취약성 이용 기술

Target이 되는 Computer system을 공격하기 위해 여러 System을 Master와 Agent로 활용하여 동시에 대량의 Data를 보내어 과부하가 걸리게 함으로써 당해 System이 정상적인 서비스를 하지 못하도록 무력화시키는 (분산)서비스거부(Distributed Denial of Service)공격, IP Spoofing 공격, SYN Flooding 공격, Buffer Overflow 공격 등이다. 주로 Worm과 같은 자동화된 공격도구를 사용하여 수 만개의 System

에 쉽게 침입하여 Agent를 설치하고 제어한다.

2000. 2.7 Canada의 15세 소년(Mafiaboy)이 미국의 Yahoo.com, Amazon.com, eBay.com, CNN.com등과 같이 접속빈도가 높은 대표적인 site에 공격을 가하여 정상적인 업무를 마비시키고 세상을 불안케 하였던 것도 이 DDoS Attack을 사용하였다.

3.3. Malicious Code

A. Compuer Virus

Compuer virus란 마치 생명체인 Virus와 같이 자기 복제를 하면서 전파되어 Computer에 오동작을 일으키거나 File을 손상시키는 등의 행위를 하는 Program이다.

Compuer Virus는 강한 전파성을 가지고 있어 일단 제작 전파된 연후에는 순식간에 기하급수적으로 감염되므로 퇴치가 힘들어져 Computer와 Program이 존재하는 한 계속되어 그 위험성이 대단히 높다.

1970년대 미 국방부 AlphaNet에서 처음 발견된 이후 매일 새로운 종류의 Virus가 만들어지는 것으로 알려지고 있는데 Internet의 성능과 속도가 향상되면서 현재에는 불과 몇 시간이면 전 세계적 으로 확산된다.

최근에는 Melissa, PAPA처럼 e-mail을 이용한 Macro Virus가 널리 퍼졌으며 한국에서 1999. 4.26. 있었던 CIH Virus는 당시 널리 알려져 있었음에도 예상을 초월한 큰 피해를 초래하였다.

얼마 전까지만 해도 Computer Virus는 자신을 은폐하거나 encryption하는 정도의 기능을 가진 것이 주류였으나 점차 발전하여 2001년 출현한 Code Red나 Nimda의 경우에는 Web site, Network, System의 취약점을 통해 전파되었으며 변종인 Code Red Ⅱ는 Trojan horse file까지 생성하는 등 더욱 지능화되었다.

B. Worm

Worm은 Virus와는 달리 File을 감염시키지 않으며 e-mail이나 Internet 등의 Network를 타고 스스로 전파되는 악성 코드이다. 1988.11.2 최초로 발견된 Morris Worm은 Network에 침입하여 Computer, Network, User 등에 대한 정보를 입수한 뒤 취약한 다른 System에 침투하고 자신의 복사본을 만들어 또 다른 System으로 옮기는 방법으로 수 천대의 Computer들의 정상적인 동작을 방해하였으며 Internet을 며칠간 마비시켰다.

Worm은 DoS Attack을 위한 payload를 내장하기도 하고(Code Red) Web site 변경 payload를 가지고 있기도 하며(sadmind/IIS, Code Red) 동적 configuration 능력을 가지고 있는 경우도 있다(W32/Leaves). 그러나 Worm들의 가장 큰 영향은 Internet의 많은 부분에서 서비스 거부를 효과적으로 조장하는 전파력과 치명적인 손실이다

최근 들어 Worm은 더욱 Upgrade 되어 자동화되었고 상대적으로 이용 가능한 취약성들이 광범위 하기 때문에 몇 시간이면 수많은 System에 침투하면서 큰 피해를 줄 수 있다.

2000.5. 출현한 LoveLetter는 수 많은 변종으로 수백만 대의 Computer와 수십억 달러의 피해를 입혔으며, 2001.7.19. 출현한 Code Red는 9시간만에 25만 대 이상의 System에 침투하였다.

C. Trojan Horse

정상적인 Program 내부에 숨어서 System이나 Network에 피해를 입히는 공격으로 상대방의 의심없이 실행시키게 하여 원격지에서 정보를 수집하고 해당 Computer를 control한다.

System의 Security 취약성 점검 Tool인 SATAN (System Administrator Tool for Aalyzing Networks)과 같은 형태로 위장이 가능하여 자신의 존재를 사용자들이 알아보지 못하게 작성되어 있고 또한 쉽게 탐지될 만한 피해도 입히지 않기 때문에 찾아내기 매우 어렵다.

D. Logic Bomb

Trojan Horse의 일종으로 Programmer에 의하여 독립적인 Program 내에 의도적으로 삽입된 Code의 형태를 가지고 있다. Logic Bomb은 무조건적 수행을 하는 Trojan Horse와는 달리 평상시에는 아무런 활동을 하고 있지 않다가 시간, 주파수, 사용자수, Hard disk의 여유 공간 등 활동을 위한 일정 조건이 갖추어지면 작동을 개시한다.

이러한 Trojan Horse와 Logic Bomb에 대한 불안은 미국의 MS Windows와 UNIX 같은 S/W들에 대한 의구심으로 나타나 중국과 프랑스 등에서는 Linux 또는 Open source solution을 선호하는 정책을 취하고 있다. 실제로 R. E. Haeny는 "MS Windows나 UNIX와 같은 S/W들은 대부분이 미국에서 작성되므로 미국은 Trojan Horse를 숨긴 S/W를 외국에 수출하도록 할 수 있다. Logic Bomb에는 'War against USA' 문구가 있는 문서가 발견되는 경우 Hard disk

를 format하거나 CIA로 보내는 기능이 숨겨져 있을 수 있다."[30]고 했으며 전직 CIA요원이었던 Wayne Madison은 상용 S/W 제품들에 Backdoor가 심어져 있을 가능성이 높다고 경고 하였다.

E. Mail Bomb & Spam Mail

가장 쉬운 무기인 Mail Bomb과 Spam Mail은 공격대상에게 악의적 또는 별 의미 없는 다량의 e-mail을 보내 상대방의 System의 용량을 초과하여 Computer와 Network를 마비시키거나 장애를 초래하는 공격이다.

1999.3. Yugoslavia에 대한 NATO의 공습이 시작되자 Yugo 정부는 국민들에게 NATO의 무력행사를 비판하고 Serbia의 입장을 호소하는 메시지를 e-mail을 통해 전 세계에 띄우도록 지시했다.

이에 따라 Serbia의 Hacker들이 e-mail로 NATO Web site를 무차별 공격했고 White House Web site도 하루 종일 Shutdown 되었으며 미국 해군기지에는 발신처가 Yugo의 Beograd인 e-mail이 계속적으로 수신되었다.

3.4. Electromagnetic Weapons 등

A. Chipping.

Chip의 일부분에 시간, 주파수 등 특정 조건이 만족되면 작동하는 기능이나 회로를 H/W적으로 삽입하여 공격하는 방법이다.

B. Nano Machine.

작은 크기의 Robot으로 돌아다니다가 상대방 Computer의 slot 등의 틈을 통해 잠입한 뒤 H/W를 파괴하는 무기이다.

C. Jamming.

상대방 통신장비간의 통신 채널을 방해하는 방법으로 정보통신망을 통해 전달되는 Packet들의 유통을 전자적으로 방해 또는 내용을 변경하는 무기로 사용된다.

D. HERF(High Energy Radio Frequency) Gun.

전자회로로 이루어진 Computer가 고출력 전자파를 받으면 오작동하거나 정지되는 약점을 이용한 방법으로 일시에 고출력전파를 발생시켜 전자 장비들을 마비 도는 파괴시키는 무기이다. 이 무기는 원격으로 조정하여 전파체계를 교란시킴으로써 Computer 통신은 물론 방송, 금융거래 등 국가기간전산망을 일시에 Shutdown 시킬 수 있어 특히 위험한 공격 방법이다.

E. EMP(Electro Magnetic Pulse) Bomb.

EMP는 핵폭발이 발생하는 것과 동일한 수준의 전자기파를 발생시킴으로써 이 전자파에 노출된 Computer나 통신 System의 모든 전자회로들이 파괴된다.

F. AMCW(Autonomous Mobile Cyber Weapon).

외부의 도움없이 Network를 따라 스스로 돌아다니며 Virus 기술 등을 이용하여 상대방의 Computer system이나 Network를 파괴하거나 정보를 조작하는 무기이다.

4. Cyber crime과 terrorism의 동향

4.1. 발생 동향

4.1.1. 공격의 효과

Cyberspace 공격자들은 각종 수단을 사용하여 목적을 달성하려 하며 여기에 희생당한 취약한 System들에게나 막대한 손해를 입힐 뿐만 아니라 사회적으로도 바람직하지 못한 영향을 미칠 수밖에 없다. 이러한 공격들로부터 일어날 수 있는 효과들을 살펴보면 다음과 같은 것들로 요약될 수 있다.

우선 제일 광범위하게 영향을 미칠 수 있는 것으로 서비스 거부 내지 불능을 들 수 있으며 Comuter system의 불법 사용과 Data 또는 S/W의 변경·손실, 재정적 손실, 인간 생활의 위험·손실, Computer나 Network에 대한 신뢰성 상실, 대중적 확신의 상실 등 실로 불안과 위기를 가져다 줄 수 있다.

4.1.2. 미국의 CSI/FBI Survey

미국의 CSI(Computer Security Institute)와 San Francisco FBI Computer Intrusion Squad가 공동으로 수행한 2003 Computer Crime and Security Survey[31]에 의하면 가장 중요한 결론은 Cyber attack의 위험은 지속적으로 높은 수준을 유

30) R. E. Haeni, *Information Warfare : An Introduction*, George Washington University, 1997

31) CSI/FBI, Computer Crime and Security Survey, 2003. 해마다 실시하는 조사로 2003년 보고서는 미국의 530여의 기업 보안실무자, 정부 요원, 금융기관, 병원, 대학 관계자를 대상으로 실시하였다.

유형별 발생현황 (2000~2003.7)

구분 / 연도	총 계	사이버테러형 범죄			일반사이버범죄				
		소 계	Hacking	Virus	소 계	사기	명예훼손	개인정보	기타
2000	2,444	452	449	3	1,992	747	204	28	1,013
2001	33,289	10,638	10,526	112	22,651	14,172	1,992	1,109	5,378
2002	60,068	14,159	14,065	94	45,909	31,109	3,155	2,496	9,147
2003.7	40,042	8,061	8,015	46	31,981	22,329	1,798	1,616	6,238

연령별현황 (2000~2003.7)

구분 / 연도	계	10대	20대	30대	40대	50대	기타
2000	2,190	675	665	404	135	49	262
2001	5,052	2,193	1,661	777	242	87	92
2002	21,817	8,205	6,876	3,743	1,881	563	549
2003.7	17,866	6,222	6,621	3,126	1,304	344	249

직업별현황 (2000~2003.7)

구분 / 연도	계	무직	학생	회사원	IT전문직	자영업	전문직	기타
2000	2,190	465	601	203	18	477	43	383
2001	5,052	1,398	2,039	735	76	404	47	353
2002	21,817	6,763	6,598	2,876	283	2,129	415	2,753
2003.7	17,866	6,764	5,122	2,001	99	1,474	203	2,203

지하고 있고 상당한 보안기술을 적용한 조직조차도 큰 손실을 입고 있으며 더구나 수사기관에 신고 된 사건의 비율이 아직도 낮다(30%)는 것이다.

이로 인한 연간 총 손실액은 약 2억170만 달러로 작년 4억5,500만 달러보다 감소되긴 하였지만 2001년 이전의 수치와 일치하고 있으며, 가장 큰 손실은 지적재산권 등 사유 정보의 절도, 서비스 거부 등으로 인한 손실이었고 금융 사기로 인한 손실은 낮아졌다.

연간 총 손실액의 감소에도 불구하고 중대사고의 전체적 수는 작년과 거의 동일하게 유지되고 있는데, 가장 빈번하게 공격 또는 남용 유형은 Virus 사고(82%)와 내부자에 의한 Network 접근 남용(80%)이었다. 또한 교화한 Hacker의 Consultants 고용 여부에 관해서는 15%만이 고용할 것이라고 했고 68%는 고용할 의사가 없다고 하였다.[32]

조직을 보호하기 위해 채택한 보안기술로는 Anti virus S/W(99%)와 침입차단 System(98%)을 사용하고 있으며 대다수의 조직들(91%)이 Computer와 정보자산의 보호를 위해 특정한 유형의 물리적 보안을 채택하고 있으며 이 중 대부분은 Access control을 채택(92%)하고 있고 Biometrics(생체인식)는 그리 많이 사용하지는 않고 있다(11%).

4.1.3. 한국의 CTRC Report

한국에서도 Internet을 비롯한 정보통신 Infra의 급격한 확산과 더불어 Cyber 관련 범죄는 최근 들어 폭증하게 되었는데 경찰청 사이버테러대응센터(CTRC : Cyber Terror Response Center) 자료에 의하면 2000년 2,444건 발생 신고 되었던 것이 2001년 33,289건 2002년에는 60,068건으로 나타나고 있다.

2000년에 비해서 2001년에 13.6배로 급증한 것은 사이버테러대응센터가 창설되고 e-mail로 24시간 365일 신고를 받으면서 그동안 암수화 되었던 사소한 범죄가 모두 드러나게 된 것으로 판단되고 2002년에는

32) Reformed Hacker의 고용 여부에 대한 반응은 1999-2003 동안 거의 비슷하여 Yes:14-20%, No:61-68%, 나머지는 Don't Know였다.

전년도에 비해 2배로 증가하였는데 이는 Internet 이용인구의 증가 등으로 인해 통신과 게임 관련 사기, 명예훼손, 개인정보 침해 등의 범죄가 급증한데 그 원인이 있는 것으로 판단된다.

Hacking 등의 수법을 이용한 초기 침해사고의 경우 1993 서울대 전산센터 침입, 1994. 한국전산원 KRNIC침입, 1999. KAIST 우리별3호 제어시스템 Hacking, 20여종의 Virus를 제작하여 Computer 통신망 및 사설게시판에 게재한 Virus 제작그룹 CVC 사건 등이 있었으나 당시까지만 해도 Cyber terrorism 적인 성격은 약했다.

2000년대에 들어서면서 8월 강릉 소재 한 PC방의 Computer에 Trinoo master program을 설치하여 국내 100 여 site에 대한 침입과 Backdoor 설치 등 공격기지화, 9월 국내 Security 전문 업체에 의한 집단 Hacking 사건 등으로 Cyber terrorism에 대한 인식과 불안감이 확산되기 시작하였다.

2001.4. Cyber terrorism의 전 단계로서 수많은 Web server들을 hacking하여 Backdoor를 설치하고 그 상황을 그룹에 보고하다가 국제 hacking group WHP(We Hate People) member인 주한 미군이 검거된 적이 있으며 2001. 5 신용카드 정보회사와 Internet Portal사의 Web server의 취약점을 공격 이에 보관된 47만 명의 신용정보와 방화벽 내부의 DB Server를 공격 700만 명의 개인정보를 유출하여 불안케 하였다. 그 외 대부분은 게임 관련 Item 또는 사이버 머니, 사이버 증권과 비밀번호 관련 Hacking을 끊임없이 시도하고 있다.

연령별로는 2002년에 10대가 37.6%, 20대 31.5%, 30대 17.2%로서 20대 이하가 전체의 69.1%에 이르러 Off-line과는 달리 저연령층이 주류를 형성하고 있다.

2000년에는 30대도 상당한 부분을 차지하였던 것과는 대조된다.

직업별로는 2002년에 무직 31%, 학생 30%, 일반 회사원 13% 순이었으며 무직과 학생층이 전체의 61%를 차지하였으며 이는 최근 몇 년간 비슷한 현상이며 회사원과 자영업자들도 상당한 부분을 차지하고 있다.

한 가지 유의할 점은 한국에 성행 중인 Internet café(PC방)의 PC를 이용하여 이루어지는 범죄가 상당히 큰 부분을 차지하고 있는데 이는 손쉬운 접근과 이동성 그리고 추적의 어려움을 이용하려는 것으로 보이며 특히 음란물, 게임, 명예훼손, 성폭력 등과 관련된 것일수록 이러한 장소를 많이 이용하였다.

4.2. 최근 동향

4.2.1. 인적 및 환경적 동향

A. 환경적 동향

전 세계적으로 정보통신기반이 갖추어지고 이에 대한 의존도가 높아지며 e-Commerce, e-Business, e-Government가 진전되면서 Internet user들이 급격히 증가하는데다가 여러 가지 기술과 제품들이 개발되어 사이버 공격자들에게는 더없이 좋은 환경을 만들어 주고 있다.

더구나 사회의 주요 Infrastructure들의 운영이 Internet, Protocol, Application 등에의 의존도가 심화될수록 그들의 복잡성은 더욱 더 증대되어 Security hole은 그만큼 더 많아지고 Information security에 대한 충분한 지식과 인식의 결여로 이에 대응할 조화된 노력이 사실상 부족한 실정이다.

또 한 번 Computer가 손상되면 전체적으로 검증해 보아야 하는데 이러한 Integrity를 쉽게 검증할 만한 S/W나 Configuration files 등이 제대로 구비되지 않은 Site들이 대부분이며, 많은 Site들이 Host나 Network 관련 Logging 또는 Monitoring을 제대로 하지 않아 그 침해의 발생 원인을 추적하는데 어려움을 주고 있다.

B. 인적 동향

예전에는 장난이나(Script kids) 과시적· 오락(Recreation) 또는 경제적인 이득을 보려는 공격자들이 많았다면 최근에는 상대방의 정보를 몰래 빼내려 하거나 분명한 목적과 명분 등을 가지고 의도적으로 위해를 끼치려는 지능적인 범죄적 공격자들이 증가하고 있다.

공격자들은 e-mail, Web site, IRC, DEF CON, 2600.com 등을 이용하여 미리 예비하거나 조직화하고 사용하기 쉬우며 광범위한 공격력을 갖춘 정교한 Tool들을 이용해서 보안의식이 약하거나 적절한 훈련이 결여된 사용자 및 관리자들을 공격한다.

많은 공격들이 정당한 권한(Authorized access)을 가진 내부자에 의해서 비롯되고 있으며 정책에 반함에도 그 편리성 때문에 modem을 사용하거나 잘 모르는 사이에 malicious code를 실행시키기도 한다.

Security에 대한 지식과 전문가들 그리고 대응 조직들이 점점 늘어나고 있기는 하지만 Internet user들의 증가에 비하면 그 비율과는 비교할 수 없으며 자신들의 기술을 손쉽게 시도할 수 있는 공격자들은 계

속 늘어가고 있다.

4.2.2. 기술적인 동향

예전에는 Hacking 기술과 Virus 기술이 서로 독립되어 이용되었으나 1999년 이후 이 둘이 통합되어 복잡한 형태의 공격이 나오기 시작하였고 특히 Worn, DDoS, DRDoS(Distributed Reflection DoS) 등과 같이 전체 Network에 피해를 주는 공격 방법들이 등장하고 있어 갈수록 확산되고 있는 Internet과 Mobile 기기들에 대한 위험도 그만큼 커질 것으로 보인다. 이들 최근의 기술적 동향을 살펴보면 다음과 같다.[33]

A. 공격Tool의 자동화(Automation)

공격Tool들이 갈수록 자동화되고 속도가 빨라져 System 대한 scanning을 수행하면서 취약성을 탐지할 수 있어 훨씬 신속하게 전파하고 2000년 이후에는 스스로 공격을 진행시킬 뿐만 아니라 1999년 분산 공격Tool의 등장에 따라 많은 Internet system에 분산 배치된 공격Tool들을 관리 조종한다.

이에 따라 스스로 전파되는 Code Red와 Nimda는 18시간도 안되어 전 세계적으로 확산될 수 있었고 System에 분산된 공격Tool들은 취약한 system을 scanning 하고 취약점을 이용하여 더욱 효율적으로 서비스 거부 공격을 할 수 있게 되었다.

B. 공격Tool의 정교화(Sophistication)

공격Tool 개발자들이 예전보다 고도의 기술을 구사하여 분석을 통해 공격Tool의 징후를 탐지하기가 어려워지고 Antivirus S/W나 IDS를 통해 발견하기도 어려운 실정이다. 중요한 3가지 특성이 있는데 새로운 공격Tool을 분석하기 어렵게 하거나 시간이 많이 걸리게 하는 등의 Anti-forensics, 예전처럼 하나의 정해진 순서에 의하지 않고 임의로, 미리 정해진 혹은 공격자의 선택에 따라 패턴이 달라지는 Dynamic behavior, 그리고 과거처럼 한가지 유형의 공격만을 수행했던 것과는 달리 Upgrade 하거나 Tool의 배분을 달리하여 쉽게 변할 수 있고 여러 운영체제에서도 실행될 수 있는 Modularity of attack tools 등이 그것이다.

C. 취약점의 신속한 발견(Faster discovery)

최근에는 취약성들이 빠르게 보고되어 Patch 하기에 바쁘고 매년 새로운 종류의 취약성들이 발견되고 있다. 새로운 취약성을 가진 제품의 기존 Code를 검사하기 위해서는 수백 개의 다른 S/W 제품 들을 시간이 걸리면서 반복 검사하게 되는데 종종 침입들이 개발자보다 먼저 발견하기도 한다.

D. 증가된 방화벽 침투(Permeability of firewalls)

방화벽은 침입자로부터 1차적인 보호수단으로 여겨지지만 대개 내부자로부터의 공격을 막지 못하며 Internet Printing Protocol이나 Web-based Distributed Authoring and Versioning처럼 전형적인 방화벽 configurations를 통과하는 기술들이 디자인 되고 있다. 또한 실제로 방화벽과 어울리는 몇몇 protocol들이 그렇게 설계되어 있어 Host security의 요구를 해결해주지 못하고 있다.

E. 점증하는 비대칭적 위협(Asymmetric threat)

Internet 상에서의 Security는 그 특성상 서로 연관되어 있으므로 각 system의 공격 노출은 전 세계 Internet에 연결된 나머지 모든 system들의 보안상태에 달려 있다. 공격기술의 발전에 따라 공격자 한 명이 한 system을 효과적으로 공격하기 위하여 대규모의 분산 system을 손쉽게 이용한다. 배치의 자동화와 공격Tool관리의 정교화에 따라 위협의 비대칭성은 계속 증가할 것이다.

F. 기반 공격에 따른 위협 증가(Infrastructure attacks)

기반 공격들은 Internet의 핵심 구성요소들에게 광범위하게 영향을 미치는 공격이어서 일상의 업무로 Internet에 의존하는 많은 조직과 이용자들의 관심이 증대되고 있다. 이 기반공격의 4가지 유형은 DDos, Worm, DNS 공격, Router 공격 등이 있다.

이러한 기반 공격이 증가함에 따라 항상 몇 가지 문제점을 안고 있다. 위협의 비대칭성으로 인해 Denial of service는 공격자들에게 적은 노력으로 많은 효과(high-impact, low-effort)를 내는 공격방법으로 이용될 것이고, Sircam처럼 file로 감염되는 Virus들로 인해 Sensitive information들이 외부로 유출되기도 하며, 공격자들이 news site를 변경 하거나 허위 보도자료를 돌리는 등 Misinformation 할 수 있음은 물론 보안사고 처리에 엄청난 Time and Resources를 소모토록 한다는 것이다.

33) CERT/CC. "Overview of Attack Trends", May 2002.

Ⅲ. Cyber Security 확보 방안

1. 국내 대응체계 구축

1.1. 국민인식 향상과 전문인 교육훈련 (Awareness & Training)

한국은 급속한 산업화에 이어 재빠른 정보화 정책을 추진하여 상당한 정보통신 Infra를 갖추었으나 Cyber-space에 대한 건전한 규범 인식과 이용에는 커다란 관심을 가지지 못하였고 특히 Cyber security에 대한 인식과 기술, 전문가(experts)들은 부족하였다.

거의 2000년대에 들어오면서 Hacking과 Virus, Worm 등 Malicious code 그리고 DDoS 공격들에 의한 Cyber terrorism이 Issue화 되면서 주의를 환기 시켜 그 중요성을 인식하고 가시적인 대응책을 마련하고 활동하기 시작하였다.

그러나 아직도 사용자나 관리자들의 인식 수준이 낮을 뿐만 아니라 어느 정도 알고 있는 것마저 실제 실천으로 옮기지 않고 있는 경우가 허다하다. Patch나 Anti virus S/W 등에 대해서도 무관심 하고 심지어 사용하고 있는 Computer나 Password 등에도 소홀히 하는 경우가 많이 있다.

갈수록 복잡해지는 System과 Network의 Security를 관리나 Computer Forensics 연구를 위한 전문 인력이 필요한데 전문 교육기관이나 프로그램 등이 아직 충분하지 못하며 기술력을 갖춘 청소년 그룹을 효과적으로 활용하는 방안들이 마련되지 못하고 있다.

각종 NGO 등 시민단체의 활동도 필요하나 정부나 관련 전문 조직들이 최근의 상황, 새로운 공격과 대응 방법 관련 신뢰성 있고 편견없는 자료들을 제공하고 Training course를 만들어 적극적으로 전문인을 양성해 나가야 한다.

1.2. 국내 협력체제 강화 : Coordinated Response

빠른 시간 내에 효율적으로 대응하기 위해서는 국내 모든 관련 조직들의 협력과 대응이 필요하다. 정부 내에서도 어느 한 기관에서 전담하기에는 너무 방대하고 또 Hegemony를 쥐듯이 해서는 오히려 협력에 어려움이 있을 수 있다. 따라서 모든 관련 조직들이 함께 참여하는 협의체를 구성하여 수시로 당면 문제를 해결하며 정보공유를 하고 장기적인 대응전략을 세우는 등 협력을 유도하여 나가야 할 것이다

Cyber Security는 이제 국민의 삶과 국가의 안보(National Security)가 걸려있는 문제이기도 하므로 범국가적으로 대처해서 Security incidents나 Major events에 대한 Solutions을 얻기 위해서는 가능한한 많은 전문가들이 공동 참여하여 지혜를 모아야 할 것이다.

Sponsor로서, Partner로서, Collaborator로서 같이 작업하고 Information과 Data를 공유하며 공격자들의 활동을 규명하는 것만으로도 상당한 효과를 거둘 수 있다고 보기기 때문이다.

1.3. 법과 제도 등 정비· 확충

시대 상황은 급변하고 그 변화에 신속하고 효율적으로 대응할 필요가 있는데 기존의 법규, 제도, 행태 등은 아직도 제대로 마련되지 못하거나 여러 가지 선결해야 할 문제들로부터 벗어나지 못하고 있는 실정이다.

한국의 경우 2001. 1. 정보통신기반보호법과 정보통신망이용촉진및정보보호등에관한법률이 제정되어 그동안 미비 되었던 부분을 시급히 마련하여 일단 공백을 메꾸기는 했지만 불합리한 부분이 있어 아직도 체계화되려면 많은 이해와 노력이 필요하다.

문화적인 차이나 새로운 현상에 대한 적극적인 해석과 타결 방법을 모색하기 위해 우리와 비슷한 외국의 경우도 참작하고 양식있는 네티즌들과도 상호 토의 과정을 거쳐 의견을 수렴하면서 완급을 가려 전체적인 법체계적·제도적 기반을 잡아 나가야 한다.

또한 정보통신망 이용자의 침해행위의 처벌적 측면만을 강조해서는 안되고 System과 Network의 보호조치를 성실하게 이행하지 않아 침해사고가 발생하도록방치한 ISP 측에 대한 고려도 아울러 해야 할 것이며 계속 발전되고 있는 기술을 감안하여 너무 성급하게 앞서가는 것은 자제할 필요가 있다.

그리고 날로 복잡하게 증가되어 가고 있는 Cyber crime과 Cyber terrorism에 대한 분석을 위하여 정확한 통계가 필요한데 침해사고의 신고가 필요하고 현재는 각 기관별로 분산 수집하고 있는 통계도 통일된 기준에 의해 작성되거나 통합되어 제대로 이용되어야 한다.

1.4. 정보보호산업·기술 육성

정보보호산업이나 정보보호기술은 21세기 고부가가치산업인 첨단 산업·기술이어서 각국은 경제적으로 상호 경쟁적인 관계에 있을 뿐만 아니라 주요 핵심 부분은 극비로 통제하고 있다. 이는 Cyber terrorism 또는 Information warfare 등에 의해 National

Security에 직접 연결되기 때문에 국가에서 중점적으로 지원하고 육성할 필요가 있다.

정보 시스템과 제품들의 취약성과 Malicious code들에 대한 분석, 각종 침해로부터의 차단 탐지 대응 복구 기술, 새로운 방어방법과 대책 관련 기술 등과 이를 위한 제품의 생산과 표준화 및 수출 등에 대해 관련 기능들 간의 국가적인 합의를 도출하여 효율적인 지원 육성책을 시행하여야 한다.

또한 Encryption Algorithm, PKI, Electronic Signature 등 핵심 기술 확보 및 표준화를 촉진하고 Ubiquitous computing, Mobile Communication과 관련되는 보안기술들의 개발과 대외경쟁력 확보를 위해지원을 강화해야 할 것이다.

1.5. Security Plan에 의한 철저한 관리 (Policies and Procedures)

평상시 국가기관, 기업 등 모든 주요 관계 조직들이 자체 Information security system에 대한 점검과 면밀한 사전 관리, 대응, 복구 등 일련의 계획을 수립하고 이에 의한 철저한 관리와 연구 및 Feedback으로 전체적인 Security management 수준을 끌어올리는 노력을 꾸준히 하여야 한다.

즉, Security에 대한 경각심을 높이고 그 Policy를 홍보, 교육할 뿐만 아니라 공격 등 침해에 있어서 준수사항, 팀원들의 역할, 고객· ISP· 사법기관 등 정보공유 조직들에의 연락망에 대한 숙지는 물론 Security plan에 대한 위험분석과 정기적인 절차 테스트, 공격받았을 때의 상황계획 등을 마련하고 철저히 관리하여야 한다.

Security가 잘 유지되는 환경을 창출, 유지한다는 것은 힘들고 많은 비용이 소요되는 복잡한 문제이다. 예방이 물론 최우선이지만 Risk 평가, 통제수단의 선택과 시행, Monitoring, Detection, Incident Response, 지속적인 개선조치 등이 함께 고려되어야 한다.

특히 각 조직의 CIO 또는 CISO들이 자신과 자기 조직에 대한 영향과 관련 자료의 민감성 때문에 사법기관과 정보공유하기를 주저할 수 있다는 것을 이해하지만 함께 정보공유를 통해서만이 공격, 침해자를 찾아내고 새로운 Cyberthreat을 알 수 있으며 Critical Infrastructure에 대한 공격을 예방할 수 있으므로 상호 협력, 공동 대응해야 한다.

Physical, S/W, H/W Controls 상의 제조치를 취함은 말할 것도 없을 뿐만 아니라 Fire Wall, IDS, Encryption, Hacker trap 등 새로운 기술에 의한 다양한 제품의 활용과 시설은 물론 기존의 운영방식 등에 대한 재검토(Periodic review)를 해 나감으로써 새로운 문제점을 도출하고 이를 해결하기 위해 공동 노력하는 체제가 갖추어져야 한다.

2. 국제 협력(International Cooperation)

2.1. 외국의 정책 동향 분석

각국의 주요 기반시설들의 정보통신기술에의 의존도가 점차 심화됨에 따라 또는 Information warfare를 방어하거나 공격하려는 의도에서 Cyber security에 대한 지대한 관심을 갖고 각국의 실정에 따른 정책들을 실시하고 있다.

특히 미국은 1998. 5. 발표된 Clinton 행정부의 Presidential Decision Directive 63으로 National Critical Infrastructures에 대한 보호와 이를 뒷받침하기 위한 National Infrastructure Protection Center를 창설하여 운영해 왔다. 2001. 9.11 미국 WTC, Pentagon 등에의 Terrorism 이후에는 물리적인 공격과 Cyber 공격을 포함한 Terrorist의 위협과 공격으로부터 미국의 안전을 보장하기 위한 노력을 하고 있다.

우선 총괄부서로서 강력하고 많은 기능을 망라한 Department of Homeland Security를 신설하고 Cyber 안보담당 대통령 특별 보좌관(Special Adviser to President for Cyberspace Security), 국가기반자문회의(National Infrastructure Advisery Council), 주요기반보호대통령협의회(President's Critical Infrastructure Protection Board)등을 조직하여 각종 정책들을 검토 수립하며 USA Patriot Act 등 각종 법제도를 정비하였다.

특히 위 PCIPB는 2003. 2. 미국의 정보통신기반을 보호하기 위한 "The National Strategy of Secure Cyberspace"을 수립하여 국가 사이버보안 대응 시스템(National Cyberspace Security Response System), 국가 사이버공간 위협 및 취약성 축소 프로그램(National Cyberspace Security Threat and Vulnerability Reduction Program), 국가 사이버보안 인식제고 및 훈련 프로그램(National Cyberspace Security Awareness and Training Program), 정부 사이버공간 보호(Securing Government's Cyberspace), 국가안보 및 국제 사이버공간 보안 협력(National Security and International Cyberspace Security Cooperation)

등 5가지 국가적 우선순위(national priority)를 기초로 전략을 구체화하고 있다.

일본은 1997. 8. 정부 주도하에 정보보안대책실을 설치하고 국가적 정보보안대책을 추진하여 1998. 6. '하이테크범죄 중점추진 프로그램' 발표, 1999. "부정 ACCESS행위의 금지등에관한법률' 제정 시행하고 있으며 경찰에 Net Force를 창설 대처하고 있다.

9.11 테러 이후에는 Cyber Terror 대책 강화 등을 중점 추진사항으로 하여 "사이버테러 특별행동계획"과 그 후속조치를 마련하는 등 진일보한 대책을 서두르고 있다.

2000.5 Paris에서 열린 G-8 정상회담 이후 2001. 11 EU 이사회에서 채택된 Cyber crime 방지를 위한 Convention은 상당한 성과라고 할 수 있다. 또한 2004.1.부터는 EU 15개 국가가 날로 기승을 부리는 사이버 범죄에 공동으로 대처하기 위해 전담기구인 〈The European Network and Information Security Agency〉를 설립하여 4년간 운영하기로 하였다. 이 전담기구 관리위원에는 정부, 산업계와 민간단체가 참여하게 되는데 EC위원회와 유럽이사회에서 각 5명, 유럽의회 2명, 산업계 4명, 소비자단체 2명으로 구성되며 자문위원회도 갖추게 된다.

중국은 1997년부터 중앙군사위원회에 Computer virus 특수부대를 창설 운영하며 미래의 Information Warfare에 대비 전국적인 훈련을 실시해오는 것으로 알려지고 있다. 북한과 러시아도 상당한 수준의 기술능력을 보유한 것으로 알려지고 있고 중동아시아 제국 및 동유럽 국가들도 뒤따르고 있다.

OECD, G-8, AFEC 등 국제조직들도 각자의 실정과 목적에 따라 Cyber Security에 관한 정책과 제도를 운영하고 있기 때문에 이에 대한 관심과 연구를 참고 하여 한국의 정책과 방향을 설정해 나갈 필요가 있다

2.2. 국제적 공동 대응 노력

국경이 없는 Computer system과 Network의 속성으로 인해 Cyber crime을 통제하기 위해서는 세계의 모든 정부, 사법기관 등의 조직, 기업, S/W제작자, 연구계, 실무자들은 모두 새로운 Risk에 대한 책임을 같이 나누는(Shared responsibility) 전방위 대응(Full range of Response)이 필요하다.

그러나 각국의 정보화 수준, 국가의 정책, 법 제도의 준비, 문화의 차이, 공동 사법기관의 부재 등으로 인해 이러한 도전들을 예방, 추적, 처벌하며 전 세계적인 협력과 신뢰관계를 형성하는데 매우 큰 어려움이 따르게 된다.

하지만 우선 가능한 방법으로 CERT, ISAC, Interpol, 지역간 협조체제, 공식 및 비공식 조직들 간의 상호 긴밀한 협력, 협약, 조약 등을 통해 정보의 공유, Security incidents에 대한 공동 대응, 침해자의 추적 등 점진적으로 공조 노력을 해나가야 할 것 이다.

경찰청에서는 1995년 '해커수사대'의 발족을 시작으로 1997. '컴퓨터범죄수사대' 1999. '사이버범죄수사대'로 이어져 오다가 2000년 들어 국제적으로 Cyber terrorism의 양상이 심각해짐에 따라 국가 사회 정보통신기반을 보호하고 미래에 대비하기 위해 Cyber terrorism에 대한 예방과 분석, 추적수사 그리고 대응기법개발 등 종합적인 대응체제를 갖춘 Cyber terrorism 전담기구인 '사이버테러대응센터(Cyber Terror Response Center)'를 창설하여 운영해오고 있다[34].

Ⅳ. 결 론

본 고에서는 정보통신기술의 비약적인 발전에 따른 현대 정보사회에서 새로이 대두된 Cyberspace의 Security 문제를 Cyber Crime and Terrorism의 측면으로부터 살펴보았다. Computer system과 Network이 점점 더 복잡해지고 Ubiquitous computing, Mobile 시대가 오면 더욱 더 Security hole은 많아지고 공격자들은 광범위하고 파괴력이 큰 Tool을 이용하게 되어 인간과 사회가 안는 Risk는 그만큼 더 커질 것이다. 또한 범죄와 전쟁간의 구분도 모호해지며 Information warfare를 위한 각국의 방어 공격체제 경쟁도 한층 더 격화될 것이다.

이에 대한 대비로서 한편으로는 적절한 대응을 위한 준비와 처리 능력을 배양해야 하겠지만, 다른 한편으로는 인류가 오랜 역사 속에서 꽃피워낸 첨단 과학기술들이 보다 더 인간의 삶의 질(Quality of Life)을 높이고 행복을 추구(Pursuit of Happiness) 하

34) 필자가 2000.1.부터 창설 구상을 하고 2월 경찰청을 방문한 당시 국무총리께 창설 필요성과 규모 예산 등에 대해 직접 공식 Briefing한 뒤 조직과 예산의 확보 작업을 거쳐(인원 128명, 예산 370억원 요구하였으나 1차년도에 하향 조정된 채) 7.11 공식적으로 출발하였다. CTRC는 단장을 중심으로 협력운영팀, 신고경보팀, 수사팀, 기법개발팀 등 4개의 Team으로 구성되었다. 또한 일선 지방 경찰관서에 사이버범죄수사대를 설치하여 일반 사이버 범죄 수사를 전담 처리토록 하였다.

는데 이용될 수 있도록 사회-정치-경제적 대책과 인간성(Humanity)을 회복하는데 관심과 노력을 경주해야 할 것이다.

참 고 문 헌

[1] Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books,1973

[2] A. Toffler, *The Third Wave*, N.Y.: Bantam, 1981

[3] J. Naisbitt, Megatrends, N.Y.: Warner Books,1982

[4] P. F. Drucker, The Age of Discontinuity: Guidelines to Our Changing Society, N.Y.: Harper & Row, 1968

[5] Thomas S. Kuhn, *The Structure of Scientific Revolutions*, Chicago, University of Chicago Press, 1996

[6] H. Rheingold, *The virtual community*, 1994.

[7] R. E. Haeni, *Information Warfare : An Introduction*, Washington DC, George Washington University, 1997

[8] Anonyme, *Sécurité Maximale des Systèmes et Réseaux*, Paris, CampusPress, 2003

[9] Daniel Martin, Frédéric-Paul Martin, *Cybercrime: menaces, vulnérabilités et ripostes*, Paris, PUF, 2001

[10] Winn Schwartau, *Information Warfare*, New York, Thunder's Mouth Press, 1996

[11] Donn B. Parker, *Fighting Computer Crime*, New York, John Wiley & Sons, Inc. 1998

[12] Nicholas Negroponte, *Being Digital*, 1995

[13] Donald L. Pipkin, *Information Security*, HP Professional Books, 2000.

[14] Lawrence Lessig, *Code and other Laws of Cyberspace* , New York, Basic Books, 1999

[15] Mandy Andress, *Surviving Security*, Indiana polis, 2002

[16] Gerald Ferrera, *Cyber Law*, South-Western College Publishing, 2001.

[17] Dorothy E. Denning, *Information Warfare and Security*, New York, ACM Press, 1999

[18] Edward Waltz, *Information Warfare Principles and Operations*, MA:Norwood, Artech House, Inc.

[19] Bruce Schneier, *Secrets and Lies : Digital Security in a Networked World*, John Wiley Sons, Inc.

[20] Charles P. Pfleeger and Sharie Lawrence Pfleeger, *Security in Computing*, 3rd edition, New Jersey, 2003.

[21] Cécile Bernat, *Les autoroutes de l:information*, Paris : LGDJ, 1997.

[22] Manuel Castelles, *La société en réseaux*, Paris, Fayard, 1998.

[23] Philippe Boure, "Internet et la Lutte contre la Cybercriminalité", Gazette du Palais, 2003.1.22

[24] CSI/FBI, "Computer Crime and Security Survey", 2003.

[25] CERT/CC, "Overview of Attack Trends", May 2002

〈著者紹介〉

하 옥 현 (HA Ok Hyun)

1978. 2. : 성균관대학교 정치외교학과

1980. 8 : 서울대학교 행정대학원 (석사)

1998. 8 : 프랑스 사회과학대학원 (EHESS) 박사과정(DEA 취득)

관심분야 : 과학기술과 사회, Ubiquitous Computing, Information Security, Cyber Terrorism & Information Warfare