Internet 관련 犯罪의 動向과 그 對策*

송 광 섭**

◇ 목 차 ◇

Ⅰ. 서 언

인터넷(Internet)이란 inter와 network의 결합어로서 "서로 연결되어 있는 네트워크의 집합체"인데, 이 인터넷을 통하여 임의의 다른 사용자에게 도달함으로써 각 사용자(컴퓨터)가 있는 각종 정보를 이용 또는 제공할 수가 있다.

미국을 포함한 각국의 정보통신기반(Information Infrastructure) 구축과 범세계적 정

* 이 논문은 1999년도 원광대학교의 교비지원에 의해서 연구됨.
** 원광대학교 법과대학 교수, 법학박사.

보통신기반(GII) 구축이 추진중인 현상황에서 인터넷은 전세계를 연결하는 중요한 정보통신기반으로 급부상하고 있다. 또한 인터넷 관련 정보기술의 급속한 발전에 따라 최근 인터넷은 무한한 잠재력과 확장 가능성을 예고하고 있다. 경제적인 면에 있어서는 급속하게 발전하는 인터넷 기술이 가져올 새로운 서비스 영역의 등장과 함께 이로 인한 새로운 이윤창출의 기회를 제공하여 향후 대부분의 경제활동이 인터넷을 매개로 하여 이루어질 것으로 예측되며, 인터넷은 모든 경제영역의 핵심 수단이 될 것이다.

미래 정보사회에서는 인터넷의 핵심기술과 서비스 영역의 우위 여부에 따라 산업 및 국가경제의 성장과 발전이 좌우되며, 인터넷을 통한 고도화된 정보통신 서비스의 개발과 보급으로 국민의 복리증진과 삶의 질의 향상도 가능해질 전망이다. 한편으로 인터넷이 급속하게 확산되면서 그에 따른 역기능의 해결이 중요과제로 대두되고 있다. 컴퓨터의 폭발적인 보급 결과에 의하여 정보의 내용과 소재에 관계없이 누구나 손쉽게 인터넷상에 방대한 정보를 올리고 내리는 것이 가능하게 되어 이를 일일이 확인하고 관리하는 것이 현실적으로 불가능하다. 이에 따라 폭력·외설·범죄·지적소유권 침해·개인정보·프라이버시에 대한 침해 등 불건전 정보의 유통이 용이하게 된다.[1] 이에 따라 바람직한 인터넷 발전을 위해 현실 세계와는 다른 새로운 가상 공간에 적합한 질서와 규범 마련이 시급한 실정이다. 인터넷과 같은 가상공간(cyber space)에서 발생하는 정보시스템 범죄의 특징은 발생시 대규모적인 피해를 유발할 뿐만 아니라 전문적 기술을 이용한 범죄이므로 범죄적발과 입증이 어렵고, 사이버 스페이스로 인한 공간의 무제약성 등으로 인해 반복성의 특징을 가지고 있다. 컴퓨터의 폭발적 보급과 그에 대한 사회적 대응의 지연은 인터넷 이용에 있어 다양한 사회문제를 발생시켰고, 이에 따라 전세계적으로 그에 대한 법적 대응, 특히 인터넷의 규제와 관련된 논의를 야기하였다. 국경을 넘은 컴퓨터네트워크인 인터넷은 종래의 PC통신망과는 차원을 달리하는 사이버 스페이스를 형성하고 있지만, 여기에는 인터넷 자체의 특성을 반영하여 종래의 범죄학, 법률학이 미처 예상하지 못한 법적 문제점을 발생시키고 있다.

따라서 인터넷상에서 발생하는 제문제, 즉 외설적·폭력적 표현, 명예훼손, 저작권침해, 프라이버시침해, 통신비밀의 침해 그리고 이러한 행위에 대한 분쟁처리기구와 분쟁처리방법 등에 관하여 적절한 법적·제도적 대책의 수립이 긴밀한 과제로 대두되고 있다.

현재 우리나라에서 인터넷과 관련하여 중요한 범죄로 거론되고 있는 것은 해킹·바이

1) 그러나 불건전 정보 유통에 대한 규제는 표현의 자유를 저해할 가능성이 크며, 개방적인 인터넷의 특성상 실효성있는 대응방안 마련에 많은 어려움이 따른다.

러스·음란물·도박·사이버 스토킹 등이다. 이러한 유형 중 이미 해킹, 바이러스, 음란물에 대한 정도는 위험수위를 훨씬 넘어선 것으로 보여지고 있다.

이하에서는 인터넷과 관련된 범죄인 컴퓨터 해킹, 컴퓨터 바이러스, 해커와 경호·경비, 국방상의 문제점과 그 대책 등에 관하여 고찰하기로 한다.

Ⅱ. 컴퓨터 해킹

컴퓨터 해킹(Computer Hacking)이란 컴퓨터를 이용하여 다른 사람의 정보처리장치 또는 정보처리조직에 침입하거나 기술적인 방법으로 다른 사람의 정보처리장치가 수행하는 기능이나 전자기록에 함부로 간섭하는 일체의 행위를 가리킨다.[2] 이와 같은 컴퓨터 해킹은 통신망의 발전과 데이터베이스 산업의 눈부신 발달에 따라 오늘날 인터넷 관련 범죄의 가장 중심적인 문제의 하나로 대두되고 있다.[3] 즉 개인용 컴퓨터가 널리 보급되고, 이는 또한 Network와의 연결을 통하여 컴퓨터가 정보전달매체의 기능을 중심으로 활용됨으로써, 이에 대한 다양한 침해가 문제되고 있는 것이다.[4]

컴퓨터 해킹은 보통 다음과 같은 3단계의 절차를 거친다. 첫번째 단계는, 목표로 한 통신망에 침입하여 쉘(shell)을 사용할 수 있는 사용자의 권한을 얻는 단계이다. 다시 말하면 사용자의 비밀번호를 알아내는 과정이다. 두번째 단계는, 침입한 통신망에서 시스템 내부의 오류 등을 이용하여 관리자(root)의 권한을 획득하는 과정이다. 세번째 단계는, 관리자로서 다음에 다시 침입하기 위한 비밀문(backdoor)를 설치하는 과정에서 범죄를 은폐하기 위한 방어적 수단을 구축하는 단계이다.[5]

이러한 절차를 통하여 행하여지는 해킹의 행위형태는 ① 프로그램이나 컴퓨터에 수록된 정보를 복사·인쇄 또는 입수하는 행위, ② 컴퓨터시스템이나 프로그램 또는 데이터를 변경·파괴하는 행위, 또는 컴퓨터시스템의 부정조작을 통하여 ③ 정상적인 컴퓨터 작동을 방해하는 행위, ④ 재산상 이익을 얻는 행위 등으로 나타날 수 있다.[6]

---

2) 최영호, 컴퓨터와 범죄현상, 컴퓨터출판사, 1995, 183면.
3) 유인모, "가상공간을 매개로 한 새로운 컴퓨터범죄와 형법," 인천대 논문집 제21호, 1996, 5면 이하.
4) 심재무, "컴퓨터해킹과 형법," 경성법학 제6호, 경성대 법학연구소, 1997, 128면.
5) 최영호, 정보범죄의 현황과 제도적 대처방안, 한국형사정책연구원, 1998, 61~62면.
6) 심재무, 앞의 논문, 129면.

1. 컴퓨터 해킹의 현황

1997년 한국정보보호센터 CERTCC-KR[7]이 피해를 접수받아 지원한 해킹사고 건수와 그 밖에 검찰과 경찰에서 수사하여 발표한 해킹피해 사례를 바탕으로 1997년 해킹사고 현황을 조사하여 1996년과 비교한 통계결과를 보면 다음과 같다.[8]

<표 1> 1997년 해킹사고 피해 현황

구 분	1996		1997		계	
	건 수	비율(%)	건 수	비율(%)	건 수	비율(%)
대 학	95	65	32	50	127	60
기 업	46	31	25	39	71	34
정부·공공기관	2	1	4	6	6	3
연 구 소	-	-	3	5	3	1
기 타	4	3	0	-	4	2
계	147	100	64	100	211	100

<표 2> 1997년 해킹피해 현황(심각성정도)

구 분	건 수	비 고
큰 피해	48	자료 유출, 삭제, 변조, 시스템정지
일반 피해	3	일반 해킹으로 인한 침입
단순 피해	13	해킹시도 및 단순 해킹
계	64	

7) CERTCC-KR은 국내 전산망 해킹 등 침해사고에 대응하기 위하여 한국정보보호센터가 운영하고 있으며, 침해사고의 방지 및 예방, 해킹 등 침해사고의 접수 및 처리지원, 피해복구 등의 임무를 수행하고 있다. 또한 국내대응팀 협의회 사무국의 역할과 국제적인 해킹과 침해사고에 대응하기 위하여 국제조직과 함께 한국을 대표하여 활동하고 있다.

8) 한국정보보호센터, 정보보호뉴스, 1998년 4월호 (통권 10호) 참조.

<표 3> 1997년 해킹피해 현황(해킹수법 분류)

구 분	건 수	비 고
ID 및 비밀번호 도용	3	ID 도용
해킹프로그램 이용	5	취약점파악용 도구 등
시스템 취약점 이용	33	운영체제, 홈페이지 등
스팸, 메일폭탄	4	
기타	4	Syn Flooding, Ping 공격 등
계	49	

<표 4> 국제 해킹관련 현황

구 분	1996년	1997년
해외 ⇨ 국내	1	9
국내 ⇨ 해외	6	11

2. 컴퓨터 해킹의 처벌

오늘날 해킹으로 인한 피해가 날로 커지고 있다. 즉 컴퓨터를 이용하여 금융범죄를 자행하고, 개인정보를 침해하거나 인터넷 사기, 횡령 등 하루가 다르게 해킹의 수단과 방법이 지능화, 첨단화되고 있다. 이와 같은 해킹행위는 실정법에 위반되는 범죄행위임에도 불구하고 범죄행위라는 인식의 결여로 인하여 해킹범죄를 저지르는 경우가 늘어나고 있다.

이하에서는 해킹관련 범죄의 태양과 그에 따른 처벌법규 및 형량을 소개하기로 한다.

가. 형 법

구 분	법 률 조 항	처 벌 형 량
데이터부정 조작, 변조	제227조의 2(공전자기록등위작, 변작)	10년 이하의 징역
	제228조(공전자기록등 부실기재)	5년 이하의 징역 또는 1천만원 이하의 벌금
	제229조(위공전자기록등행사)	10년 이하의 징역
	제232조의 2(사전자기록위작, 변작)	5년 이하의 징역 또는 1천만원 이하의 벌금
	제234조(위작사전자기록등 행사)	

업무방해	제314조 제2항 (컴퓨터등 장애업무방해)	5년 이하의 징역 또는 1500만원 이하의 벌금
비밀침해	제140조 제3항 (공무상비밀전자기록등 내용탐지)	5년 이하의 징역 또는 700만원 이하의 벌금
	제316조 제2항(전자기록등 내용탐지)	3년 이하의 징역이나 금고 또는 500만원 이하의 벌금
전자기록 손괴 및 은닉	제366조(전자기록등 손괴)	3년 이하의 징역이나 금고 또는 700만원 이하의 벌금
	제141조 제1항 (공용전자기록등 손상)	7년 이하의 징역 또는 700만원 이하의 벌금
컴퓨터사기	제347조의 2(컴퓨터등 사용사기)	10년 이하의 징역 또는 2천만원 이하의 벌금

나. 전산망 보급확장과 이용촉진에 관한 법률

구 분	법 률 조 항	처벌형량
전산망 보호조치 침해, 훼손	제30조의 2(벌칙)	3년 이하의 징역 또는 3천만원 이하의 벌금
전자문서 위반, 변작, 행사	제29조 제1항(벌칙)	10년 이하의 징역 또는 1억원 이하의 벌금
타인의 정보 훼손, 침해, 도용	제30조(벌칙)	5년 이하의 징역 또는 5천만원 이하의 벌금

다. 전기통신사업법

구 분	법 률 조 항	처벌형량
통신비밀침해, 누설	제70조 제3호(벌칙)	3년 이하의 징역 또는 3천만원 이하의 벌금

라. 공공기관의 개인정보보호에 관한 법률

구 분	법 률 조 항	처 벌 형 량
개인정보 변경, 말소	제23조 제1항(벌칙)	10년 이하의 징역
개인정보 누설, 처리, 제공	제23조 제2항(벌칙)	3년 이하의 징역 또는 1천만원 이하의 벌금
부정한 방법으로 개인정보 열람, 제공	제23조 제3항(벌칙)	2년 이하의 징역 또는 700만원 이하의 벌금

마. 신용정보의 이용 및 보호에 관한 법률

구 분	법 률 조 항	처 벌 형 량
신용정보 변경, 검색, 삭제	제32조 제11호(벌칙)	3년 이하의 징역 또는 3천만원 이하의 벌금

바. 공업 및 에너지기술기반조성에 관한 법률

구 분	법 률 조 항	처 벌 형 량
산업정보 위조, 변조	제22조 제1항(벌칙)	10년 이하의 징역 또는 1억원 이하의 벌금
산업정보 훼손, 비밀침해	제22조 제2항 제1호(벌칙)	5년 이하의 징역 또는 5천만원 이하의 벌금

사. 무역업무자동화촉진에 관한 법률

구 분	법 률 조 항	처 벌 형 량
무역정보 위조, 변조	제25조 제1항(벌칙)	1년 이상 10년 이하의 징역 또는 1억원 이하의 벌금
무역정보 훼손, 비밀침해	제26조 제3호(벌칙)	5년 이하의 징역 또는 5천만원 이하의 벌금

아. 화물유통촉진법

구 분	법 률 조 항	처 벌 형 량
물류정보 위조, 변조	제54조의 2(벌칙)	10년 이하의 징역 또는 1억원 이하의 벌금
물류정보 훼손, 비밀침해	제54조의 3(벌칙)	5년 이하의 징역 또는 5천만원 이하의 벌금
전산망 보호조치의 침해, 훼손	제54조의 4(벌칙)	3년 이하의 징역 또는 3천만원 이하의 벌금

Ⅲ. 컴퓨터 바이러스

컴퓨터 바이러스는 생물학적 병원체와 같이 컴퓨터에서 컴퓨터로 옮겨 다니며 이용자의 시스템이나 소프트웨어를 교란하고 파괴하는 프로그램을 말하는 것으로 자기복사의 방법으로 증식한다. 프로그램의 실행 순서를 바꾸거나 변형하고 삭제하여 컴퓨터가 정상적인 기능을 수행하지 못하게 하는데, 대개는 일정한 조건(날짜, 명령어, 입력 신호)이 부합되면 작동하도록 프로그래밍되어 있다.

1. 컴퓨터 바이러스의 현황

최초의 컴퓨터 바이러스는 지난 1985년 파키스탄의 한 형제 프로그래머가 제작한 '브레인' 바이러스가 시초로 알려져 있다.[9] 이들 형제는 프로그램 불법복제자들을 골탕먹이기 위해 브레인을 개발했으며, 이후 1988년에 이스라엘 예루살렘 대학에서 '예루살렘' 바이러스가 발견되었다. 예루살렘은 '13일의 금요일' 바이러스로 더 유명하다. 이후 미국과 동구권의 해커들에 의해 이를 모방한 수많은 컴퓨터 바이러스가 제작되었고, 현재까지 1만여종이 발견될 정도로 기하급수적인 발생률을 보이고 있다.

국내에서는 '브레인' 바이러스가 1988년 발견되면서 처음 알려지기 시작했으며, 1989년 최초의 국산 바이러스인 '벌꿀바이러스'가 발견된 이후 국산 바이러스의 증가율도 매

9) 전자신문, 1998년 3월 3일자 참조.

년 증가하고 있다. 1997년만 해도 2백56종의 신종 컴퓨터 바이러스가 발견됐으며, 1988년 이후 지금까지 국내에서 발견된 바이러스만 8백여종에 이르고 있다. 이렇듯 바이러스가 기승을 부리면서 실제 개인이나 기업들의 정보시스템 보안문제는 해커의 침입방지에 앞서 바이러스 방지가 가장 큰 문제로 대두되고 있다.

미국의 ICSA(International Computer Security Association)가 북미지역을 대상으로 컴퓨터 바이러스의 피해현황을 살펴본 자료에 따르면 모든 중대형 조직의 99%가 최소한 한 번 이상 바이러스에 감염된 사실이 있으며, 이 가운데 3분의 1 이상이 피해를 입었다고 응답한 것으로 조사되었다. 또 다른 연구기관 조사에서도 지난 97년 미국 내에서 발생한 정보보호사고의 3분의 2 이상이 바이러스에 의한 사고였다. 이는 외부인에 의한 시스템 불법접근, 즉 해킹이 40%였던 것에 비하면 컴퓨터 바이러스가 제일 골치 아픈 보안문제인 것으로 조사되었다.

국내에서도 지난 1996년 6월 안철수컴퓨터바이러스연구소가 5천1백99명을 대상으로 자체 조사한 바에 따르면 조사대상자의 90% 이상이 바이러스에 감염된 경험이 있으며 1백만원 이상의 피해를 본 사용자가 53%에 이르는 것으로 나타났다. 물론 이 수치는 현재 더욱 증가했을 가능성이 높다. 컴퓨터바이러스는 수적인 증가와 함께 질적으로도 발전을 거듭하고 있다. 감염 증상으로 볼 때 시스템의 성능을 저하시키거나 오동작을 유발하기도 하고 심지어 시스템 자체를 완전히 망가뜨려 소중한 데이터들을 한순간에 날려버리는 등 악성을 더해가고 있다. 바이러스 프로그램 자체로도 스스로 바이러스라는 것을 숨기기 위해 은폐기법을 사용하거나 바이러스 프로그램 분석에 절대적인 핵심부분을 암호화해 백신프로그램의 칼날을 피한다.

최근에는 다른 파일에 감염될 때마다 자신의 암호화부분을 바꿔버리는 다형성 바이러스들이 등장해 백신업체들의 분석을 어렵게 하고 있으며, 실행파일이 아닌 응용소프트웨어의 데이터 파일에 감염되는 매크로바이러스가 등장해 기승을 부리고 있다.

최초의 바이러스인 '브레인'을 만들었던 파키스탄인 형제들처럼 바이러스 제작자들은 컴퓨터시스템에 능통한 프로그래머들이다. 고도의 프로그램 능력을 갖춘 이들은 자신의 실력을 시험해 보려는 순수한 의도로 바이러스를 만들 수도 있겠지만 최근의 경향은 소영웅주의에 빠져 실력을 과시하려는 경우가 많은 것으로 분석된다. 바이러스에 자신의 닉네임이나 실명을 기재하는 경우까지 있기 때문이다. 이들은 개인적으로 바이러스를 제작, 유포하는 경우도 있지만 그룹단위로 서로 정보를 교환해 가며 실력을 쌓아 경쟁적으로 새로운 바이러스를 만들어내고 있다. 대표적인 해커그룹은 팰콘/스키즘과 핵무기(Nuke), 구토물(Puke), 트라이던트(Trident) 등이다. 이 밖에 29A, IKX, VBB, SLAM

등 세계적으로 수많은 그룹이 활동하고 있다.

국내에서도 최근 중학생이 낀 바이러스 제작그룹 'CVC' 회원 4명이 경찰에 적발되면서 그 실체를 드러냈다. 이들 외에도 유사한 그룹들이 PC통신 동호회나 사설BBS를 무대로 활동하고 있는 것으로 알려져 있다. 바이러스에 대항할 수 있는 유일한 방어체제는 현재로서 백신소프트웨어가 전부라고 해도 과언이 아니다. 물론 백신소프트웨어가 100% 완벽한 바이러스 방지 해결책은 아니지만 또 유일한 해결책인 것도 사실이다. 컴퓨터 바이러스가 등장하자 뒤이어 바이러스를 치료해 주는 백신소프트웨어도 빠른 속도로 등장하기 시작했다. 바이러스 제작자들이 신종 바이러스를 유포하면 바로 백신 제작자들이 이를 치료하는 백신을 개발해 전파한다. 이제는 바이러스 제작자와 백신 제작자 사이의 자존심 싸움으로 가고 있는 형세이다. 백신소프트웨어는 초기 공개소프트웨어로 일반에 전파되기 시작했으나 바이러스 발생률과 파괴력이 높아지면서 시장에서 절대 필요한 상품으로 성장했고, 이 분야 시장은 소프트웨어시장에서 무시 못할 규모로 거대해졌다.

한편 최근 들어서는 불특정 다수인에게 한꺼번에 E-mail을 보내는 인터넷상의 스팸메일(spam mail)을 보내는 경우가 많아지고 있다. 스팸 메일이란 광고, 비방, 음란한 내용, 컴퓨터 바이러스 등을 담은 E-mail을 불특정 다수 대중을 향해 대량 유포하는 행위로 사이버 공간의 새로운 신종 쓰레기 공해로 부각되고 있다. 이 경우에 미국 버지니아주에서는 스팸 메일 규제법을 제정하여 스팸 메일을 보내다가 적발된 사람은 500달러의 벌금에 처하고, 수시인에게 피해를 미치는 악의적인 스팸 메일의 경우에 수신인의 피해액이 2,500달러를 넘는 경우에 중범죄로 간주하여 징역에 처하도록 규제하고 있다.

2. 컴퓨터 바이러스의 처벌

가. 컴퓨터업무방해죄

인터넷 상용망에 가입한 자가 서비스에 불만이 많은 나머지 공개자료실에 소프트웨어를 올리면서 바이러스를 유포시키는 바람에 공개자료실의 서비스를 중단하도록 한 경우 컴퓨터 등 장애업무방해에 해당한다. 형법 제314조 제2항은 "컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자는 5년 이하의 징역 또는 1천500만원 이하의 벌금에 처한다."라고 규정하고 있다.

나. 컴퓨터데이터손괴죄

컴퓨터 바이러스를 유포시켜 컴퓨터 이용자의 시스템이나 소프트웨어를 교란하고 파괴하거나 컴퓨터데이터 등을 파괴하는 경우에는 전자기록등손괴에 해당한다. 형법 제366조는 "타인의 재물, 문서 또는 전자기록 등 특수매체기록을 손괴 또는 은닉 기타 방법으로 그 효용을 해한 자는 3년 이하의 징역 또는 700만원 이하의 벌금에 처한다."라고 규정하고 있다.

여기에서 손괴란 물건의 현상을 변경시키거나 그 효용을 줄이거나 또는 잃게 하는 모든 행위를 말하며, 은닉이란 물건을 숨겨 그 소재를 불명하게 함으로써 찾는데 애를 먹게 하거나 또는 찾을 수 없도록 하는 일체의 행위를 말한다.

Ⅳ. 해커와 경호·경비, 국방상의 문제

현대 정보화사회에 있어서는 사회 중추 신경인 전산망을 파괴하거나 해킹으로 획득한 비밀정보를 범죄에 이용하는 사이버 테러 등 새로운 테러 형태가 21세기 인류의 안전을 위협하는 중요 요인으로 등장하고 있다. 해커와 범죄집단이 결합할 경우에는 이들은 가공할만한 사회질서를 파괴하는 중요변수가 될 수 있다. 예컨대, 해커가 국방, 행정 등 국가 기간전산망까지 침입하여 모든 통신망을 교란시키거나 비밀정보를 훼손하는 등 치명적인 정보테러를 할 수 있고, 테러리스트들에 의하여 주요 요인의 살상, 납치 등 경호·경비상에 커다란 위험과 문제를 야기시킬 수도 있다.

1. 국가전산망에의 침입

외국에서 국내로 들어오는 통신망의 관문격인 한국통신 국제전화교환소에 외국해커가 침입한 것으로 드러났다.[10] 이 경우에 국제전화교환소에 침입한 해커가 마음만 먹었다면 국방, 행정 등 국가 기간전산망까지 침입해 비밀정보를 훼손하는 등 치명적인 정보테러를 할 수 있는 상황이었다고 한다. 1997년 국감자료에 의하면 1996년 이후 1997년 8월말 현재 국내에서 발생한 전산망 해킹사고는 192건에 달하는 것으로 밝혀졌다.

10) 한겨레신문, 1997년 8월 29일자 참조.

한국정보보호센터가 발표한 「1998 해킹사고 접수 및 지원현황」에 따르면 지난 상반기 동안 국내에서 해킹사고가 일어난 기관은 1997년 같은 기간의 64개 기관에 비하여 23% 증가한 79개 기관에 이르는 것으로 조사되었는데,[11] 이 가운데에 해외로부터 침입한 사례가 전체의 76%에 해당하는 60개 기관에 달해 1997년 상반기의 11개 기관에 비하여 급증한 것으로 분석되었다. 따라서 국가 전산망에 대한 보안 상태를 수시로 점검·관리하는 프로그램을 개발·활용하여야 한다.

2. 경호·경비상의 문제

1998년 3월 23일 USA TODAY지에 의하면 미국무부는 1997년 10월 회계감사원(GAO) 감사에서 국무부가 운영중인 국제컴퓨터망의 해외 2개 지점에 해커가 침입하여 보안상 중대한 문제가 발생한 사실을 발견하고 1997년 가을 해커가 침입한 사실이 발견된 국제컴퓨터망 일부에 대해 약 2주간 작동 중단조치를 취한 것으로 알려졌다. 국무부는 이 때문에 재외공관에 송부하여야 할 미묘한 정보 등을 컴퓨터를 통하여 배부하지 못하고, 서면으로 작성하여 인편으로 배포하여야 하였다.

1997년 4월에는 빌 클린턴 미 대통령이 참석한 행사에 수행했던 대통령 비밀경호원들의 통신내용이 해커들에 의하여 도청당한 사실도 있었다. ABC 방송에 의하면 1997년 4월 27일 필라델피아에서 열렸던 「미국의 미래를 위한 대통령들의 정상회담」에는 클린턴 대통령부부를 비롯하여 앨 고어 부통령부부, 조지 부시 및 지미 카터 전 대통령부부 등 유명인사들이 대거 참석하였는데, 이 같은 도청이 테러리스트들에 의해 저질러졌다면 이들의 생명이 위험에 처할 수도 있었다.

한편 1998년 10월 김대중대통령이 일본을 방문했을 당시 나리타공항 부근에 관제탑을 사칭한 無線해커가 출몰 이착륙하는 항공기들이 추락사고의 위험에 노출돼 있었다는 사실이 밝혀졌다. 1999년 3월 11일 일본운수성에 따르면 프랑스의 에어 프랑스 271편 점보기가 악천후로 나리타공항으로 귀항하는 도중 관제탑을 가짜 무선이 "연료를 버리고 고도를 1천5백미터로 낮추라"라는 지시를 받았는데, 당시 이 비행기는 해발 3천7백76미터의 후지산 부근을 비행하고 있었다. 이에 의심을 품은 기장이 나리타공항 관제탑에 조회한 결과 가짜 무선이었음이 확인되어 대형 추락사고의 참사를 다행히 면할 수 있었다.[12]

---

11) 전자신문, 1998년 8월 3일자 참조.
12) 중앙일보, 1999년 3월 12일자 참조.

이러한 경우처럼 컴퓨터망이 해커에게 침입당하여 대통령, 외교관 등 주요 요인의 일정 등 통상적인 활동내용들이 적대관계에 있는 국가나 단체, 개인에게 유출되면 대통령, 외교관, 시민 등 주요 요인의 납치·살상 및 테러, 국익손실 등 큰 문제를 야기할 가능성이 크다.

3. 국방상의 문제

해커들에 의한 국방부컴퓨터망에의 침입, 육군·공군·해군 컴퓨터 시스템에의 침입 등은 국방상 큰 문제를 야기할 수 있다.

미연방수사국 FBI는 1998년 2월 26일 국방부 컴퓨터망에 무단 침입한 청소년 해커 2명을 수사하고 있다고 밝혔다. 미국방부의 한 보고서에 의하면 1997년의 경우 군사컴퓨터망에 침입을 시도한 해커들이 무려 25만회에 달하며, 이 중 65%가 성공한 것으로 알려지고 있다.[13] 또한 미국방부 컴퓨터망에 해커들이 침입하여 군사위성 시스템 소프트웨어를 훔쳐내는데 성공하여 테러리스트에 팔겠다고 위협한 사건이 발생하였다. 이들은 19세에서 28세까지의 15인조로 구성되어 있었는데, 8명은 미국인, 5명은 영국인, 2명은 러시아인으로 스스로 "다운로딩의 명수들 2016216"이라고 칭하면서 소프트웨어를 훔친 사실을 국방부 보안전문가에게 인터넷 전자우편을 통해 알려왔다고 한다. 이들 해커에게 들어간 소프트웨어는 수십 개의 군사위성을 이용하여 미사일의 목표물을 겨냥 배치해 정확한 군대위치 확인 등 미 군사력의 세계 각지 배치 시스템을 조정하는 것으로 알려졌다.

또한 영국의 군사위성에 해커가 침입하여 비행궤도를 바꾸고 거액을 요구한 사실이 밝혀졌는데, 이 해커는 영국 국방부에 3백만파운드를 요구하며 이 요구가 받아들여지지 않으면 계속 위성을 방해할 것이라고 협박하였다고 한다. 문제가 된 이 군사위성은 미국과 영국의 이라크공습에 중요한 첩보수집활동을 수행해 왔는데 이번 위성통제시스템의 일시적 마비로 영국 국방부가 발칵 뒤집혔던 것으로 전해지고 있다.[14] 이렇듯 군사용 통신위성을 장악하여 통신체계를 교란시키는 경우에는 엄청난 군사상 혼란과 대가를 지불하여야 할 것이다.

---

13) 중앙일보, 1998년 2월 28일자 참조.
14) 중앙일보, 1999년 3월 2일자 참조.

V. 향후 앞으로의 전망과 대책

오늘날의 컴퓨터 및 통신기술의 발달로 개인용 컴퓨터의 폭넓은 보급과 활용영역의 다양화가 이루어지고 있으며, 특히 PC통신이나 인터넷을 통한 정보교환이 가장 중요한 기능을 담당하게 되었다. 이와 같이 세계적으로 연결되는 인터넷의 등장으로 가상공간이라는 정보의 세계를 만들어 내게 되었으며, 이러한 정보교환시장을 중심으로 새로운 양상의 범죄들이 출현하게 되었다. 즉 종래에는 앞서 설명한 인터넷 관련 범죄의 유형 가운데 컴퓨터이용사기나 컴퓨터부정조작 등에 의한 업무방해 등이 주된 인터넷 관련 범죄양상이었으나, 오늘날은 데이터베이스범죄 또는 네트워크범죄의 형태로 나타나고 있다. 예컨대, 인터넷상의 컴퓨터해킹, 컴퓨터바이러스, 음란물, 도박 등의 새로운 유형의 인터넷 관련 범죄들은 지역적인 제약없이 음란물이나 도박, 조세포탈 또는 불법자금의 세탁과 같은 전통적인 범죄영역에까지 확산되고 있다. 또한 국가 기간전산망, 국방관련 전산망 등에의 침입을 통하여 인류와 국가·국민의 안전을 위협하는 새로운 범죄양태로까지 확대되고 있다.

그럼에도 불구하고 인터넷상의 행위들을 추적·제재하는 것은 기술적으로 쉽게 가능하지 않으며, 국제적인 형태로 나타나기 때문에 국제법으로 해결하는 것도 역시 용이하지 않다.

또한 인터넷이라는 가상세계를 통하여 행해지는 범죄행위에 대한 범죄의식 자체가 희박하여 갈수록 증가할 것으로 예상된다.

인터넷 관련 범죄는 고도의 전문성·기술성·정보유출성 그리고 지능범죄성 및 逸脫行爲(deviant behavior) 등이 복합적으로 관련된 범죄이다. 따라서 이에 대한 대책이 치밀하지 않으면 소기의 성과를 거두기 어렵기 때문에 다각적이고 종합적인 대책이 강구되어야 한다. 그러나 범죄란 항상 대책을 앞서 가는 것이기 때문에 어떻게 보면 인터넷 관련 범죄에 대한 대책은 전무하다.

우리나라의 경우 아직까지 인터넷 관련 범죄에 효과적으로 대처할 만한 입법적 장치나 기술적 발전이 많이 이루지지 않았다. 따라서 정보화사회의 역기능으로 인하여 미래범죄의 총아로 떠오르고 있는 인터넷 관련 범죄에 좀더 효과적으로 대처하기 위하여는 사전에 종합적 대책을 마련하여야 한다.

1. 법률적 대책

가. 형법의 처벌규정

형법에서 인터넷 관련 범죄에 대응하기 위한 노력이 본격적으로 논의되기 시작한 것은 1985년 6월에 발족한 형사법개정특별심의위원회에서 인터넷 관련 범죄를 신종범죄의 대표적인 예로 파악하고 이에 대한 형사법적 대처방안을 연구·검토하면서부터이다.[15] 1995년 12월 29일 개정된 형법에는 인터넷 관련 범죄에 효율적으로 대처하기 위하여 컴퓨터조작범죄의 범주에 속하는 것으로서, 전자기록위작변작죄(공전자기록위작변작 제227조의 2), 공정증서원본불실기재(제228조), 위조공문서 등 행사(제229조), 사전자기록위작변작(제232조의 2), 위조사문서 등 행사(제234조), 컴퓨터 등 사용사기(제347조의 2) 등을 신설하였다. 또한 컴퓨터파괴범죄의 범주에 속한 것으로서 컴퓨터업무방해죄(제314조 2항), 컴퓨터데이터손괴죄(제366조), 컴퓨터스파이범죄의 범주에 속하는 것으로서 컴퓨터데이터탐지죄(제316조 2항)를 신설하였고, 그 밖에 이들 범주에 속하지 않은 범죄유형으로서 권리행사방해죄(제323조)를 신설하였다.

나. 형법의 문제점 및 보완대책

개정형법이 인터넷 관련 범죄에 대하여 처벌근거들을 신설·추가하였음에도 불구하고 다음과 같은 문제점이 노출되고 있다.[16]

첫째, 개정형법은 '전자기록 등 특수매체기록'에 대하여 입법적 정의를 하지 않고 있다. 이와 같은 표현은 외연을 한정하기 어려운 막연한 규정이다. 따라서 컴퓨터의 기억(기록) 내지 정보처리방식을 중심으로 입법적 정의를 규정하는 것이 바람직하다.[17]

둘째, 개정형법은 公·私電磁記錄僞作, 變作[18]에 "…을 그르치게 할 목적으로"(제227

---

15) 미국을 비롯한 선진국들은 컴퓨터가 일반에 쓰여지기 시작한 1960년대부터 컴퓨터의 역기능에 대한 연구를 시작하였고, 그 중 가장 핵심이 되는 인터넷 관련 범죄에 대해서는 우선 이를 처벌할 수 있는 법적 근거를 마련하기 위하여 1987년을 전후하여 형법을 개정하기에 이르렀다.

16) 송광섭, 범죄학과 형사정책, 유스티니아누스, 1998, 623면 이하.

17) 일본형법은 제17조의 2에 '전자적 기록이란 전자적 방식, 자기적 방식, 기타 사람의 지각으로써 인식할 수 없는 방식에 의하여 만들어지는 기록이며, 전자계산기에 의한 정보처리에 사용하는 것'이라고 정의하고 있다.

18) 법무부 형법개정법률안 제안이유서는 '위작'이란 권한없이 전자기록 등을 작성하는 경우와 내용이 허위인 전자기록을 만드는 것이며, '변작'이란 권한없이 또는 허위내용으로 기록을 변경

조의 2, 제232조의 2)라고 목적범으로 규정하고 있는데, 이른바 해커(Hacker)라고 하는 모험심 충족을 목적으로 하는 경우와 같은 행위의 결과가 위작, 변작으로 나왔을 때 문서죄로의 처벌여부가 논란이 될 수 있다.

셋째, 컴퓨터 등 사기죄(형법 제347조의 2)에 있어서도 "컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여"로 단순화하였는데, 진실한 정보를 입력하여 불법하게 이득을 취하는 행위는 명시하지 않아 문제가 되고 있다.[19] 독일의 경우에는 컴퓨터사기죄(제263조 a)에 '진정한 데이터의 무권한 사용'을 처벌하고 있다. 이를 독자적으로 처벌하는 취지는 단순히 정보를 습득하여 컴퓨터를 기망하여 이를 이용하는 행위까지도 처벌하자는데 있다. 급증하는 CD범죄 및 그 밖의 지불거래수단 남용행위 중 '진정한 데이터의 무권한사용'이 큰 비중을 차지하고 있으며, 이에 대한 규정이 없을 경우 처벌이 곤란한 경우가 발생할 수 있으므로 우리나라도 '진정한 데이터의 무권한사용'을 처벌할 수 있는 입법적인 근거를 명백히 하는 것이 타당하다.[20]

넷째, 컴퓨터업무방해죄(형법 제314조 2항)는 이를 가중처벌하는 일본이나 독일과 달리 일반업무방해죄와 마찬가지로 처벌하고 있다. 그런데 전자기록의 중요성과 그 재산적인 가치 및 경제생활의 안정성 등을 생각할 때 그 법정형이 너무 미약하여 범죄예방적 효과가 있을지 의문스러워 진다. 또한 컴퓨터의 파괴에 대한 것은 일반 재산범죄의 개념에 포함시키고 디스크나 디스켓 등은 문서로 보아 문서범죄로 처리한다는 입법취지이다. 그러나 기업의 경우에는 경영을 위한 모든 자료처리에서부터 생산의 한 부분까지 컴퓨터가 직접 참여하고 있고, 금융기관의 경우에는 온라인에 의해 업무가 처리되고 있어 컴퓨터의 파괴로 인한 손해는 경우에 따라서는 엄청나게 커질 수가 있다. 따라서 일반파괴를 단순한 재산범죄로 처벌하는 것은 미약하고, 개정방향을 컴퓨터의 파괴에 두지 않고 업무방해의 유형으로 포함한 것은 입법적으로 충분한 검토가 이루어지지 않은 결과라 볼 수 있다.

다섯째, 컴퓨터데이터탐지죄(형법 제316조 제2항)는 행위의 객체를 비밀로 정하고 그

하는 것이라 설명하고 있다.

19) 예컨대 타인의 CD카드를 습득하여 그 비밀번호를 알아 내어 이를 통하여 은행에서 예금을 인출하는 경우, 이를 '허위'의 정보를 입력하는 것으로 볼 수 있는가에 의문이 있다. 왜냐하면 이는 허위가 아니라 진정한 정보를 권한없이 사용하는 것이기 때문에, 이를 허위의 정보를 입력하는 행위에 해당한다고 볼 수 없다.

20) 일본형법 제246조의 2는 "다른 사람의 사용하는 전자계산기에 허위의 정보 또는 부정한 指令을 주어서 재산권의 상실, 변경에 관련하는 허위의 전자적 기록을 만들거나 재산권의 得喪, 變更에 관련되는 허위의 전자적 기록을 사람의 사무처리에 共用케 하여 재산상 불법의 이익을 얻거나 타인으로 하여금 얻게 하는 자는 10년 이하의 징역에 처한다."라고 규정하고 있다.

외양적 형태를 "봉함 기타 비밀장치"한 것으로 정하였는데, 개개의 자료로 볼 때는 비밀은 아니지만 전체자료, 즉 어떤 화일(file) 전체를 복사하여 갔을 경우에는 이를 가지고 가공·분석하면 중요한 비밀이 될 수 있는 경우라든가, 그렇지 않은 일반자료의 복사 등은 처벌할 수 없는 결과가 된다. 또한 "비밀장치"의 정의에 관한 문제에 있어서 일반적으로는 문서로 된 비밀에는 비밀문서관리규정 같은 것이 있어 그에 따라 비밀을 표시하고, 또한 일반적으로는 봉함 등을 사용하기 때문에 봉함여부로 이를 구분할 수 있으나, 전자기록이나 특수매체기록은 어떤 것이 비밀장치인지 그 구분에 혼란을 가져올 우려가 있다.

여섯째, 현행 형법에서는 컴퓨터의 부정사용[21]에 대한 처벌규정이 없다.[22] 따라서 컴퓨터의 부정사용에 관하여 형법상 적용 여부가 논의될 수 있는 것은 사용절도, 사기죄, 배임죄 등이다. 컴퓨터부정사용의 본질은 사용절도이나 형법상 사용절도는 불가벌이므로 절도죄에 의한 처벌은 불가능하다. 다만 장시간 사용할 경우나, 일시적 사용이라 할지라도 그 재물의 가치를 소비하는 형태를 수반할 때 가치소비의 의사가 있으면 영득의사가 있다고 보고 절도죄의 성립을 인정하고 있다.[23] 그리고 자기의 전기소비에 대하여 이용권한자에게 묵비함으로써 기망하고, 이에 기하여 이용권한자가 전기료를 대신 납부하게 된 것은 결국 이용권한자를 기망하여 재산적 이익을 얻는 것이므로 사기죄가 성립할 수도 있다. 또한 컴퓨터의 불법사용자가 타인의 사무를 처리하는 지위에 있는 경우에는 배임죄의 성립을 인정할 수 있고, 이러한 지위에 있지 아니한 외부인은 배임죄에 의하여 처벌할 수 없다. 컴퓨터의 부정사용에 있어 중요한 것은 컴퓨터의 전기소비나 컴퓨터의 마멸이 아니고 컴퓨터의 盜用으로 인한 행위자의 현저한 부의 증가이다. 그러므로 사기에 유사한 것이므로 급부의 사기취득에 관한 형벌규정의 입법이 필요하다.[24]

다. 기타 법규

한편 인터넷 관련 범죄에 대한 통합된 법률이 없어 일반법률에 끼워넣기식으로 만들

21) 컴퓨터의 부정사용 또는 컴퓨터의 무권한사용이란 컴퓨터를 사용할 권한이 없이 자기 자신을 위하여 컴퓨터를 일정한 시간 동안 작동시키는 것을 말한다. 이는 하드 웨어 및 이에 부속된 소프트 웨어를 부당하게 사용함으로써 그 설치 등에 따른 타인의 노력을 부당하게 탈취하는 것이므로 DP시스템의 시간절도(time-theft), 용역절도(theft of service)라고도 한다.

22) 개정 형법 제331조의 2에 "권리자의 동의없이 타인의 자동차, 선박, 항공기 또는 원동기장치 자동차를 일시 사용한 자는 3년 이하의 징역, 500만원 이하의 벌금, 구류 또는 과료에 처한다."라고 규정한 자동차 등 부정사용에 관한 신설규정과는 형평이 맞지 않는다.

23) 대판 1961. 6. 28, 61 형상 179.

24) 송광섭, 앞의 책, 625면.

어진 '누더기법률'을 적용하는 것도 문제점으로 지적되고 있다. 현재 인터넷 관련 범죄에 적용되는 처벌법규는 형법과 전기통신기본법 등 줄잡아 10여개 법률에 50여개 조항에 이른다. 법규가 일관성없이 산재해있어 법망을 교묘하게 피한 지능적인 인터넷 관련 범죄가 끊이지 않고 있다. 따라서 인터넷과 관련된 범죄에 효과적으로 대처할 수 있는 법정비가 시급한 실정이다.

또한 국제적 공조나 또는 국제적 입법의 필요성도 제기된다.

2. 형사정책적 대책

또한 법적 규제이외에 컴퓨터의 보안시스템과 컴퓨터바이러스 퇴치프로그램의 개발과 이에 대한 국가적 지원이 요청되며, 사회적으로 인터넷 관련 범죄 전담수사기관의 설치, 수사관과 법조인에 대한 체계적인 교육,[25] 그리고 인터넷 관련 범죄자들의 범죄의식전환을 위한 사회적·형사정책적 노력이 절실히 요망된다.

가. 수사의 전문성 확보

현재 우리나라의 인터넷 관련 범죄의 대책은 범죄가 급증하고 있는 면에 비하여 수사인력 양성과 종합적인 대응법규제정 등 대책은 걸음마수준에서 벗어나지 못하고 있다. 컴퓨터 보급대수 1,000만대, 국내 인터넷사용자 220만명을 돌파하면서 해킹, 바이러스 유포 등 국내 사이버범죄는 건수도 급증하고 범죄양상도 지능화하고 있지만 수사전문인력은 턱없이 모자란다. 특히 정보화분야 특성상 컴퓨터기술 발전속도를 뒤따라가기 위해서는 수사 외에 기술연구와 응용, 수사요원 교육기능도 수행해야 하지만 엄두를 못내는 실정이다. 급증하는 인터넷 관련 범죄에 효과적으로 대처하려면 해킹과 바이러스 암호해독 등 분야별 전문가를 사전에 양성해야 한다.[26]

인터넷 관련 범죄에 대한 수사는 고도의 전문성을 요하므로 일반적 수사기술로는 그 해결이 불가능하므로 인터넷 관련 범죄에 대처할 수 있는 수사능력의 배양이 필요하다.

---

25) 1998년 11월 26일 개최된 정보통신망침해사고대응팀협의회(CONCERT)의 워크숍에서 다년간 정보범죄를 수사해온 일선 수사검사는 "정보화의 진전에 따라 컴퓨터범죄가 날로 늘어나고 있는데도 불구하고 정작 이에 대처해야 할 사법계에서 수사 및 판결의 난맥상을 노출하고 있다.", "국내에는 전산에 대한 기본적인 지식과 수사경험이 있는 검사가 극히 적을 뿐더러 판사는 아예 없는 실정이며, 컴퓨터범죄 사건의 경우 검사의 기소내용을 판사가 그대로 받아들이는 것이 관례가 되고 있는 형편"이라고 토로한 바 있다.

26) 미국 FBI의 경우 인터넷 관련 범죄의 분야별 전문가가 50~60명에 이른다.

인터넷 관련 범죄는 고도의 전문기술적 범죄이기 때문에 범인의 적발, 범죄의 확증, 증거의 확보가 곤란하다. 따라서 수사관의 전문적인 지식이 없이는 이러한 인터넷 관련 범죄를 효율적으로 수사할 수 없으므로 전문수사요원의 육성이 절실하다. 이를 위하여는 현 수사요원 중에 인터넷 관련 범죄에 지식이 있는 수사요원을 선발하여 집중 교육시키거나, 인터넷 관련 전문가를 전문수사요원으로 특별히 채용하는 것도 한 방법이 될 것이다.[27]

또한 인터넷 관련 범죄에 대한 수사의 일관성을 유지할 수 있도록 인터넷 관련 범죄를 다룰 수 있는 전담부서의 신설과 확충이 필요하다.[28] 현재 우리나라에서는 대검찰청 정보범죄대책본부, 서울지검 정보범죄수사센타, 경찰청 컴퓨터범죄수사대 등을 설치하여 인터넷 관련 범죄수사를 담당하게 하고 있다.[29]

나. 행형제도의 개선

인터넷 관련 범죄는 전문인에 의한 일종의 화이트칼라범죄라고 할 수 있기 때문에 일반범죄자를 위주로 하는 현행의 형벌 및 행형제도가 인터넷 관련 범죄자에게는 그 범죄억지력이 의문시된다. 따라서 이들을 효과적으로 교화시키기 위하여 재판과정에서의 양형의 균형은 물론 이들에 맞는 형벌을 강구하고, 교정 및 처우프로그램의 개발이 요청된다.[30]

다. 범죄의 인식제고와 윤리교육

인터넷 관련 범죄는 일반범죄에 비하여 범죄의식이 약한 편이므로 인터넷 관련 범죄에 대한 범죄의식을 먼저 고취시키는 것이 필요하다. 최근 급증추세인 컴퓨터 해킹범죄에 대하여 일반인은 그 해커행위를 범죄행위로 인식하기보다는 컴퓨터 전문가 또는 컴퓨터 영웅으로 보는 관대한 시각이 많다.[31] 우리나라 검찰의 엄벌방침과는 달리 사법부는 관대한 판결을 선고한 경우가 있다. 예컨대, 서울지검 정보범죄수사센터에서 1996년

---

27) 미국에서는 연방수사국의 경제담당과에서는 인터넷 관련 범죄의 전문지식을 습득하도록 교육을 실시하고 있다.

28) 인터넷 관련 범죄 전담부서에서는 인터넷 관련 범죄에 관한 정보와 자료를 수집·분석하여 향후 인터넷 관련 범죄의 수사시 수사자료로 활용할 수 있도록 통계체제를 구축하여야 한다.

29) 송광섭, 앞의 책, 626면.

30) 송광섭, 앞의 책, 626면.

31) 미국방부와 항공우주국(NASA)의 컴퓨터 체제에 침투했던 이스라엘 10대 해커인 테넨바움에 대해 이스라엘 국내에서는 "컴퓨터의 영웅"으로 칭송받고 있다.

4월 16일 서울대 전산망과 정보통신부, 청와대 등 10여개 국가기관 전산망에 침입 가입자들의 비밀번호를 해독하고 일부자료를 빼낸 혐의(전산망보급확장 및 이용촉진에 관한 법률위반)로 구속 기소된 추모피고인에 대하여 징역 10월 집행유예 2년을 선고하였는데, 판사는 판결문에서 "피고인이 대학교 전산망에 무단 침입해 정보를 빼낸 사실은 인정된다.", "그러나 국가 전산망 침입 부분은 비밀번호 파일을 해독하거나 외부에 유출하지 않아 공소사실에서 빠진 점과 고졸학력이 전부인 피고인의 명문대에 대한 동경심과 지적 호기심으로 인한 범죄로 볼 수 있는 만큼 형집행을 유예한다."라고 판시하고 있다. 이 같은 법원의 판결은 비록 범죄를 저질렀더라도 중대한 피해를 끼치지 않은 경우라면 컴퓨터 전문가를 복역하게 하는 것보다도 사회에 이바지하는 것이 바람직하다는 것으로 풀이되나, 향후 인터넷 관련 범죄는 개인사생활의 침해는 물론 국가기능의 마비 및 파괴까지 몰고 올 수 있는 무서운 범죄이므로 해커행위를 중범죄로 다루는 것이 타당하다.

또한 정부, 언론, 교육기관, 가정이 합심 협력하여 정보화사회의 역기능 방지를 위한 공조체제를 갖추고, 인터넷 관련 범죄에 대한 피해의 경각심의 인식과 컴퓨터에 대한 정당한 이용을 교육시키며,[32] 컴퓨터종사자에 대한 윤리교육[33]을 철저히 하여야 한다. 아울러 국가와 사회가 공동으로 컴퓨터안전대책기구나 인터넷 관련 범죄 연구기관과 같은 기구를 설치하는 것도 장래의 인터넷 관련 범죄에 대처할 수 있는 능력을 키우는 것이라 생각한다.[34]

라. 한국정보보호센터

정보화사회에 진입함에 따라 개인정보의 유출, 정보통신시스템의 비인가 사용, 전산망 해킹 등이 무차별적으로 이루어지고 있다. 따라서 정부는 정보화에 따른 역기능에 효율적·체계적으로 대처하기 위하여 1995년 8월 4일 정보화촉진기본법을 제정·공포하여 한국정보보호센터를 출범시켰다. 한국정보보호센터에서는 정부·공공기관, 민간기관 및 개인을 위한 각종 법적·제도적인 정보보호대책을 마련하고, 인터넷 관련 범죄·프라이

32) 컴퓨터 교육을 시킬 때 컴퓨터에 대한 기술을 습득시키는 데에 급급한 나머지 컴퓨터를 사용하는 이유와 컴퓨터를 사용하면서 다른 사람에게 피해를 입히지 않도록 하는 윤리교육을 등한시하고 있다.

33) 영국의 컴퓨터협회는 직원들의 윤리의식을 고취시키기 위해서 ① 직원 각자의 자기업무에 수반하는 책임의 수용, ② 직원들의 윤리적 행동, ③ 직원들의 자기 업무자료에 대한 기밀의 유지, ④ 직원들의 공평한 행동 등 윤리규범을 시행하고 있다.

34) 송광섭, 앞의 책, 626면.

버시보호 등의 사업을 내용으로 하고 있다.[35]

또한 한국정보보호센터에서는 전국 주요 대학에서 활약중[36]인 최고수 해커 50여명이 참여하는 보안진단전문가그룹인 「타이거 팀(Tiger Team)」[37]을 발족·운영하고 있다.

3. 인터넷 관련 시스템 안전대책

인터넷 관련 시스템에 대한 각종의 범죄 및 사고는 개인·사회·국가적인 차원에서 커다란 타격과 피해를 주기 때문에 그 예방과 방지대책이 무엇보다도 중요하다.

인터넷 관련 시스템에 대한 안전대책을 물리적·관리적·기술적 대책으로 나누어 고찰한다.

가. 물리적 대책

인터넷 관련 시설에 대한 완벽한 보안대책의 수립은 불가능하나, 인터넷 관련 시설에 대한 천재지변·폭동·테러 등에 대하여 사람과 재산을 보호하기 위한 물리적 대책마련이 필요하다. 즉 건물에 대한 안전조치, 물리적 재해에 대한 보호조치, 컴퓨터실 및 보관장소에 대한 출입통제, 컴퓨터기기·프로그램·데이터파일 등에 대한 백업(back-up) 및 비상사태발생에 대한 계획수립 등이 있어야 한다.[38]

한편 미국방부는 「사이버 테러리스트」에 의한 미국 내 정부기관 또는 민간기업에 대한 공격에 대비하기 의하여 「사이버 특수부대」를 창설할 계획이다. 이 부대는 대서양사령부 관할 아래 각 군과 정부기관에서 차출받은 컴퓨터 전문가들로 구성, 사이버 테러에 대비하기 위한 부대이다. 우리나라도 최첨단 정보화전에 대비한 특수부대의 창설을 시급히 검토하여야 한다.

---

35) 송광섭, 앞의 책, 627면.

36) 해커를 제도권으로 끌어들이게 될 타이거 팀은 정보범죄예방은 물론 정보보호기술개발에도 많은 도움이 될 것으로 기대된다.

37) 「타이거 팀」이란 미국의 군사용어로 적군으로 위장하여 아군진지에 침입해 작전과 경계상의 문제점을 찾아내는 전문침투조를 말한다. 그러나 1990년대 이후 전산망 보안진단 전문팀이란 일반명사로 굳어지면서 영국, 남아프리카공화국 등 미국 이외 다른 나라에서도 타이거팀이란 이름의 보안진단팀을 운영중이다.

38) 송광섭, 앞의 책, 627면.

나. 관리적 대책

인터넷 관련 범죄를 예방·방지하기 위하여서는 물리적 대책과 병행하여 컴퓨터업무에 대한 관리대책이 필요하다. 즉 직무권한의 명확화와 분리, 프로그램의 개발·운용의 통제, 문서화(documentation), 액세스(access) 제한, 철저한 패스워드관리, 증거기록의 확보체계구축, 고객과의 협력을 통한 감시체제, 온라인 입출력자료의 관리, 컴퓨터시스템감사,[39] 안전기준의 설정 등이 있어야 한다.[40]

다. 기술적 대책

인터넷 관련 범죄의 방지를 위한 기술적 대책은 컴퓨터 처리에 의하여 데이터취급자를 규제·견제하여 데이터를 보호하는 것이다. 데이터를 도청·무단복제·파괴·改變·가공하여 데이터를 컴퓨터시스템에서 유출시키는 행위를 방지하는 것은 데이터를 암호화하고, 사용자·사용시간에 대한 암호화가 필요하다.[41]

4. 결 언

정보화사회에 있어서 인터넷 관련 범죄 행위들 중 어떠한 행위들을 범죄화하여 처벌해야 하는가와 어떠한 행위들을 처벌하지 말아야 하는 것도 문제이다. 물론 이러한 정보사회에서도 형법의 보충성 원칙 또는 최후수단성이 적용되어야만 한다.

또한 정보사회가 가지는 특수성으로 인해 기존의 기준들이 정보사회에서도 그대로 적용될 수 있는가, 적용될 수 있다면 그 근거가 무엇이고 구체적으로 어떻게 적용되는가의 문제, 그리고 적용될 수 없다면 새로운 기준을 어떻게 마련할 것인가는 여전히 앞으로의 숙제로 남아 있다.

---

39) 컴퓨터시스템 감사는 컴퓨터시스템 주변감사, 컴퓨터처리과정 감사, 컴퓨터이용감사 등이 있다.
40) 송광섭, 앞의 책, 627면.
41) 송광섭, 앞의 책, 628면.

參 考 文 獻

송광섭, 범죄학과 형사정책, 유스티니아누스, 1998.

최영호, 컴퓨터와 범죄현상, 컴퓨터출판사, 1995.

심재무, 컴퓨터해킹과 형법, 경성법학 제6호, 경성대법학연구소, 1997.

유인모, 가상공간을 매개로한 새로운 컴퓨터범죄와 형법, 인천대논문집 제21호, 1996.

최영호, 정보범죄의 현황과 제도적 대처방안, 한국형사정책연구원, 1998.

ABSTRACT

The Trend of Internet Related Crimes and their Solution

By Song, Kwang Soub

Internet related crimes are a crime which is inter-related with high specializatio n · technicality · leakage of information · intellectual-offence and deviant behavior. Without the accurate countermeasure, we can't achieve the desired end. So we should find out multilateral and general measure.

Always crimes go in advance of the measure, so the counter measures against, computer crime can not be final. Nevertheless, we can't be careless in making the measure, but we should always consider a counter measure.

1995. 12. 29. our country revised criminal law and consolidated direct provisions, especially on the computer-hacking. But, inspite of the revision, especially on the computer-hacking. But, inspite of the revision, we have many problems. So, first of all, through the positive and empirical study, we should revise criminal law and computer crime related provisions systematically.

As the aspects and techniques of internet related crimes are always changing with the development of computer technology, there will be many problems with principle of legality, when we apply the existing abstract provisions to the new crime.

We can not be lazy in studying the emerging internet related crimes and taking concrete shape of the provision. And it will be a big help to that desirable to import the foreign provision without consideration of our reality. Without the positive and empirical study on internet related crimes, sometimes important crime will be out of reach of the punishment.

Due to these day's development of computer and technology of communication, the personal computers are widely supplied and especially PC communication and

exchange of the informations became the most important function. With the advent of internet, new aspects of crimes are appearing. Up to now, the fraud by using the computer or the interference in the execution of duty by the illegal operation of computer was the leading aspects of computer crime, but nowadays with the advent of internet, database crime or network crime like the computer hacking became the important aspects of internet related crimes. These new aspects of internet related crimes are defusing into domains of traditional crimes. Nevertheless to follow and punish the acts on the internet is not technically easy, and as it is emerging international shape, to settle it by international law is not that easy.

Harmful acts in the information-oriented society are very diverse in kinds and aspects, and it is difficult to enumerate. The point is that among the new acts in the information-oriented society we should decide which acts are to be punished and which acts are not to be punished. It is needless to say that the criminal law should be the last resort.

But owing to the characters of the characteristics of the information-oriented society, when the traditional standards can be applied, the question of what is the basis and how it can be applied in a concrete way is not settled. And if it cannot be applied, how can we make new standard is also an unsettled question.