사이버보안 강화를 위한 법적 과제*

박 훤 일**

《차 례》

Ⅰ. 머 리 말

오늘날 우리는 이른바 '情報革命'의 시대에 살고 있다. 無形의 지식과 정보가 컴퓨터·통신망을 이용하여 고부가가치의 상품으로 거래되는가 하면, 기업의 경영방식이 첨단 정보기술(information technology: IT)을 이용하여 획기적으로 변모하였고 새로운 행정수요의 등장으로 정부의 기능도 크게 달라졌다. 이와 같이 개인, 기업, 정부가 컴퓨터 시스템과 통신 네트워크를 이용하여 다양한 활동을 전개함에 따라 컴퓨터와 서버, 라우터, 통신 케이블로 상호 연결되어 있는 사이버空間(cyberspace)이 새로운 기반시설(infrastructure)로 등장하였다.

이러한 사이버공간에서는 법률의 기능도 종전의 산업혁명 시대와는 현저한 차이가 있다. 産業革命의 중심 역할은 증기기관과 철도가 수행하였으나, 오늘날 情報革命의 중심축은 정보시스템과 통신망이 담당하고 있다. 산업혁명 시대에는 사회발전을 어느 정도 예측할 수 있었지만, 정보화 시대의 기술진보는 예측이 거의 불가능하다. 이에 따라 정부 나아가 법률의 기능도 종전에는 지시와 규제 중심으로 규율대상을 선도하는 입장(leader)이었으나 이제는 정책적으로 올바른 방향을 제시하고 적용대상을 유도, 권장하는 지원자(supporter)의 역할로 바뀌었다.

사이버공간이 통신, 금융, 수송, 에너지, 행정 등 각종 분야에서 핵심적인 기반시설로 등장함에 따라 사이버공간의 보안(cybersecurity)이 중요한 국가적 과제로 대두되었다.[1] 우리가 2003년 초에 경험하였던 '1·25 인터넷 대란'은 인터넷이 일시

---

* 2003.11.11 경찰청이 주최하고 한국인터넷법학회 등에서 주관한 "2003 사이버테러 대응 심포지엄"에서 발표한 자료를 논문 형태로 다시 작성한 것임.

** 경희대학교 법과대학 조교수, 법학박사.

1) 미국은 9·11 테러 사건을 계기로 미국의 사이버공간의 테러리스트들의 공격목표가 될 수 있다고 보고 사이버공간의 보안을 위한 국가전략을 수립 공표하였다. White House, *The National Strategy to Secure Cyberspace*, February 2003.

마비되어도 국가의 사회적·경제적 기능이 일순 혼란에 빠질 수 있음을 보여주었다. 그러므로 정보통신 기반구조의 경제적·사회적 비중이 커지고 있는 만큼 이를 방해·마비시키는 책동을 억제하여야 사이버공간에서의 자유롭고 원활한 활동이 보장될 수 있는 것이다. 본고는 사이버보안의 목표를 사이버공간의 평화와 질서유지, 기술진보의 촉진에 둔다고 하였을 때 사이버공간의 질서교란자, 방해자를 어떻게 억제하고 퇴치할 수 있는지 법제 개선의 관점에서 살펴보고자 한다.

II. 사이버보안의 현황 및 문제점

1. 사이버보안의 개념

사이버보안이란 정보통신망에 대한 전자적 침해행위(cyberattack)를 사전에 예방하거나 사후에 피해를 복구하는 등 정보통신 시스템이 정상적으로 가동하도록 보장(assurance)하고 정보통신기반시설을 보호(protection)하는 것을 말한다.[2] 그러나 정보기술의 발달에 따라 전자적 침해행위도 고도화되고 있으므로 이에 관한 국제적 동향을 파악하고 국제협력을 추진(정보통신기반보호법 26조)하는 것도 중요하다고 하겠다. 예컨대 OECD가 2002년 7월 채택한 「정보 시스템 및 네트워크의 안전을 위한 지침」[3]이나 미국이 2003년 2월에 공표한 「사이버공간 보안전략」이 좋은 기준이 될 것이다.

여기서 전자적 침해행위란 정보시스템의 취약점을 공격하여 시스템 내에 침투하거나 시스템을 마비·파괴하는 등의 사고를 유발하는 것을 말한다. 좁게는 정보통신기반보호법 제2조 2호에 정의되어 있는 행위유형을 의미하지만, 넓게는 시스템이 당초 설계된 기능을 발휘할 수 없는 하드웨어·소프트웨어의 사기 및 절도, 산업스파이 활동, 데이터 조작상의 오류·사보타지, 풍·수해, 지진, 화재, 정전 등의 사고를 포함한다. 미국에서는 '사이버 공격'(cyberattack) 또는 '사이버 위

2) 사이버보안은 다른 말로 사이버테러를 비롯한 사이버공격을 방지하고 피해를 최소화하며 신속히 대응하기 위한 노력이라 할 수 있다. 사이버테러란 '해킹, 바이러스 등 정보통신망 자체에 대한 공격행위로서 국가 또는 사회적 혼란 또는 불안을 야기하는 행위'라고 정의할 수 있다. 양근원, 「사이버테러의 실태와 법적 대응에 관한 연구」, 경희대학교 국제법무대학원 석사학위논문, 2003, 11면.

3) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. <http://www.oecd.org/pdf/M00034000/M00034292.pdf>

협'(cyberthreat)이라 하여 컴퓨터 시스템을 이용하여 악의적인 목적을 갖고 컴퓨터 시스템 및 네트워크로 구성된 사이버공간에 대하여 불법적·악의적으로 국가의 정상적인 기능수행에 악영향을 미치고자 하는 일체의 과정과 행위를 일컫고 있다.[4)]

사이버보안이 추구하고 있는 기밀성(confidentiality), 가용성(availability), 무결성(integrity), 진정성(authenticity)의 관점에서 본다면 實時間으로 정보를 가로채 내용을 알아보는 監聽(interception), 정보의 전송과정을 침해하는 妨害(interruption), 권한 없이 정보의 내용을 수정하는 變作(modification), 권한 없이 없는 정보를 만들어내는 僞作(fabrication)이 각각의 침해행위에 해당한다.

요컨대 전자적 침해행위는 기본적으로 컴퓨터와 정보통신망을 이용한 기술적인 문제일 뿐만 아니라, 다른 한편으로 타인의 생명과 재산을 침해하는 犯罪行爲이고, 나아가서는 국가안보에 대한 침해행위가 될 수도 있는 것이다.

2. 전자적 침해행위의 유형

사이버보안의 대상이 되는 전자적 침해행위에는 해킹, 컴퓨터 바이러스, 웜, 트로이 목마, 논리폭탄, 전자우편폭탄 및 스팸메일 등이 있다. 이 중에서 웜, 논리폭탄, 전자우편폭탄 등이 사이버테러 수법으로 흔히 이용된다.

o 해킹(hacking): 악의적인 의도로 컴퓨터 시스템이나 네트워크에 존재하는 취약점을 이용하여 시스템과 네트워크의 정상적인 작동을 방해함으로써 사용자에게 위해를 가하는 행위를 말한다.

o 컴퓨터 바이러스(computer virus): 프로그램에 잠입하여 컴퓨터로 하여금 본래 목적 이외의 처리를 하도록 하는 프로그램을 말하며 종류에 따라서는 컴퓨터 시스템에 치명적인 해를 끼칠 수도 있다. 1970년대 미 국방부 알파-네트(Alpha-Net)에서 최초로 발견된 이래 최근에는 하루에 수십 개의 새로운 바이러스가 생겨나는 것으로 추정된다. 인터넷이 널리 보급되고 초고속화됨에 따라 치명적인 바이러스에 의한 피해도 광범위하고 빠르게 확산되고 있는 추세이다.

o 웜(worm): 컴퓨터 바이러스와 같은 악성 프로그램의 일종으로 바이러스와는 달

4) 국가보안기술연구소, "미국 사이버보안 정책 동향-미국 사이버보안 국가전략을 중심으로", 2003.3, 3면.

리 컴퓨터 시스템의 다른 프로그램을 감염시키는 것이 아니라 자신을 스스로 복제하는 것이 특징이다. 그리하여 네트워크를 통해 널리 전파시킴으로써 네트워크에 치명적인 피해를 입히게 된다.

o 트로이 목마(Trojan horse): 운영체제(OS)에 대한 일반적인 침투유형의 하나로 마치 정상적으로 보이는 프로그램 내부에 숨겨 놓은 프로그램을 말한다. 계속적인 불법침투가 가능하도록 시스템 내부에 부호를 생성하여 영구적으로 시스템 내부에 상주하다가 소기의 목적을 달성한 후에는 그 자취를 지워버리기도 한다.

o 논리폭탄(logic bomb): 트로이 목마의 일종으로 독립적인 형태 또는 시스템 개발자나 프로그래머가 의도적으로 프로그램에 오류를 발생시키는 프로그램 루틴을 무단 삽입한 것을 말한다. 특정 조건의 성취 또는 특정 데이터의 입력을 계기로 하여 프로그램이 전혀 예상치 못한 파국적인 오류를 범하도록 컴퓨터 시스템을 실행시키는 악성 코드이다.

o 전자우편폭탄(mail bomb): 수신인의 컴퓨터 시스템을 마비시키거나 파괴할 의도로 발송된 전자우편을 말한다. 제어문자의 특수한 배열로 단말기를 폐쇄하기도 하며, 첨부파일에 바이러스나 트로이 목마를 포함시키거나 우편의 용량을 지나치게 크게 함으로써 전자우편함의 한계용량을 초과시켜 결국 시스템을 마비시킨다.

o 서비스 거부(denial of service: DoS): 정상적인 정보통신서비스를 방해하거나 정지시키기 위해 짧은 시간에 대량의 데이터를 대상 시스템에 전송하는 것을 말한다. 악의를 가진 집단이 대상 서버에 엄청나게 많은 접속시도를 함으로써 서버의 자원을 소모시키고, 정상적인 사용자에 의한 접속을 불가능하게 만든다. 분산서비스거부(distributed DoS)는 해커에 의해 공격 프로그램이 설치된 수십, 수백 대의 컴퓨터에서 대상 서버를 행해 일제히 공격이 시도되는 것을 말한다.

o 컴퓨터 조작 오류・삭제, 내부자 사보타지: 컴퓨터 사용자가 고의나 실수로 데이터 조작의 오류나 삭제를 하는 것, 또는 정보 시스템의 기능과 특성을 잘 알고 있는 내부자가 고의적으로 시스템 손상이나 파괴를 하는 것을 말한다.

o 스파이웨어(spyware): 어떤 사람이나 조직에 관한 정보를 수집하는 도구를 말한다. 특정 사용자에 관한 정보를 수집하여 광고업체나 관심 있는 사람에게 제공할 목적으로 사용된다.

o 전자기적 위협(electro-magnetic threat): 최근 들어 Chipping, Nano Machine,

HERF Gun, EMPBombs, Electronic Jamming 등의 수단이 하드웨어를 마비·파괴하기 위해 많이 사용되고 있다.

이상의 전자적 침해행위를 침해주체별로 간추리면 다음 표와 같다. 침해주체에 따라 개인과 조직, 국가로 나누어볼 수 있으며, 목적, 대상, 침해수단에 차이가 있다.

<표 1>

침해주체에 따른 전자적 침해행위

	개인적 침해행위	조직적 침해행위	국가적 침해행위
주 체	o 해커 o 컴퓨터 범죄자	o 산업스파이 o 테러리스트 o 조직범죄집단	o 국가 정보기관 o 사이버전 전사
목 적	o 금전 수입 o 영웅심 o 명성 획득	o 범죄조직의 이익 o 정치적 목적달성 o 사회·경제적 혼란 야기	o 국가기능 마비 o 국가방위능력 마비
대 상	o 민간사설망 o 공중통신망 o 개인용 컴퓨터	o 기업망 o 금융·항공·교통정보통신망	o 국방·외교·경찰 네트워크
공격 방법	o 컴퓨터 바이러스 o 해킹 - 홈페이지 변조 - 패스워드 유출 - 개인신분 위장 o 논리/전자우편 폭탄 o 트로이 목마 o 서비스거부 공격	o 개인적 공격방법 포함 o 유·무선 도청 o 정보통신망 스니퍼 o 통신망 교환시스템 동작 마비 공격	o 개인·조직적 공격방법 포함 o 첨단도청 및 암호해독 o 전자공격 무기 - 고출력 전파무기 - 전자기파 폭탄 등 o 기타 치핑/초미세형 로봇/전자적 미생물 전파

자료: 국가정보원, 「2003 국가정보보호백서」, 2003.5, 23면.

3. 사이버보안의 현황 및 문제점

우리나라는 'IT 강국'이라고 함에도 공공부문이나 민간부문을 막론하고 정작 전문지식을 가진 사이버보안 전담인력이 배치되어 있는 곳은 드문 실정이다. 인터넷 대란 이후 정보보호에 대한 관심은 높아졌지만 정작 정보보호에 필요한 솔루션 도입 수준은 공공기관과 민간기업에서 여전히 미미한 상태이다. 다만, 정보보안제품은 널리 보급되어 있는데 인터넷뱅킹 등 중요한 전자거래의 데이터는 모두 암호화[5]되어 전송되고 있다. 정보보안제품의 이용실태를 보면 침입차단 시스템(방화벽)[6], 바이러스 백신[7], 침입탐지 시스템[8], 가상사설망[9]의 순으로 많이 이용되는 것으로 나타났다.

그러므로 우리나라 정보시스템의 안전성을 획기적으로 제고하려면 법제도 면의 개선 이전에 사이버보안에 대한 정부, 기업, 개인의 인식(awareness)을 획기적으로 제고할 필요가 있다. 정부 차원에서도 정보화 못지 않게 사이버보안을 위한 교육훈련 및 제품구입, 外注用役(outsourcing)에도 예산배정을 대폭 늘려야 한다. 일단 정보보호시장이 협소한 우리나라에서 외형적인 시장규모를 키워놓아야 사이버

---

5) 대표적인 암호기술(encryption)로는 공개키 기반구조(public key infrastructure: PKI)가 있다. 우리나라 전자서명법에서는 '전자서명생성정보'라 하여 이 방식을 기본으로 채택하였다(전자서명법 2조3호). PKI의 장점은 공개키 암호 알고리즘이 갖고 있는 송신자와 메시지의 합법성 등을 확인해야 하는 인증 문제를 해결할 수 있다는 것이다. 최근에는 지문, 홍채, 망막 등의 생체인식(biometrics) 정보를 이용한 인증기술이 실용화되고 있다. 2001년 말에 전자서명법이 개정(2002.7.1 시행)된 것도 이러한 추세를 반영한 것이다.

6) 방화벽(firewall)이란 인터넷과 같은 외부 네트워크에 연결되어 있는 내부 네트워크의 중요한 정보 및 자원을 외부 네트워크를 통한 불법적인 침입으로부터 안전하게 보호하기 위한 침입차단 시스템을 말한다.

7) 바이러스 백신(computer vaccine)은 컴퓨터의 기능을 저하시키는 악성 파일로서 최근 신종 컴퓨터 바이러스는 개인용 PC뿐만 아니라 서버까지도 감염시킬 수 있고 나아가 상대방 정보를 빼내거나 무력화시키는 고도의 해킹수단으로도 이용되고 있다. 자기복제를 통하여 대형 전산망의 서버를 공격하는 웜 바이러스가 속속 생겨나고 있다.

8) 침입탐지 시스템(intrusion detection system: IDS)은 전산 시스템과 네트워크에서 송수신되는 모든 데이터의 움직임을 감시한다. IDS는 기업정보에 대한 크래킹을 감지하고 차단하는 역할을 수행하며, 네트워크에 접속하여 전산 시스템을 이용하려는 로그온, 명령어 입력 등 모든 접속시도와 움직임을 감시한다. 시스템 로그온 기록을 저장해두고 있다가 의심이 가는 행동이 포착될 경우 즉시 침임을 차단하게 된다.

9) 가상사설망(virtual private network: VPN)이란 공중망을 통하여 데이터를 암호화해서 보내고 암호화된 데이터는 인증받은 사용자만이 해독하여 볼 수 있게 가상의 네트워크를 구축한 것을 말한다.

보안 산업이 기술개발투자에 힘을 쏟고 내수 및 수출확대에 노력할 수 있을 것이다. 사이버보안 산업의 발전을 위해서는 보안제품의 혁신 및 수요 창출, 가격경쟁력 제고, 정보보안제품의 필요성에 대한 인식의 확대가 시급히 요청된다.

1·25 인터넷 대란에서 경험하였듯이 정보화의 진전에 따라 정보시스템에 대한 침입으로 야기되는 피해는 천문학적 규모로 늘어날 수 있다. 그러므로 정부가 관련산업을 육성하고 시장에서의 수요에 따라 기술과 모범관행(best practices)을 진작시키는 것도 중요하지만 법제도 면에서 필요하다면 일정 사항은 강제해서라도 정보시스템의 안전성과 신뢰도를 제고할 필요가 있다고 생각된다.

III. 사이버보안을 위한 법제 현황

1. 개 관

오늘날 인터넷과 같은 개방된 통신환경에서는 정보보호에 어려움이 많으므로 정보보호를 위해서는 기술적인 방법과 법제도적인 방법이 병행되어야 한다. 암호화, 방화벽의 설치 등 사이버보안 기술도 비약적으로 발전하여 왔지만, 이러한 기술의 활용을 담보하는 법제도가 시행되지 않는다면 정보보호에 만전을 기할 수 없다. 현재 우리나라의 정보보호를 위한 법률은 <표 2>에서 보는 바와 같이 크게 ① 정보의 주체 또는 전자화 여부를 떠나 정보 자체의 기밀성을 보호하기 위한 것, ② 정보를 수집·이용하는 시스템과 네트워크를 보호하기 위한 것 ③ 기본권 보장의 차원에서 강조되고 있는 개인정보를 보호하기 위한 것, 그리고 ④ 정보보호산업의 육성을 위한 것으로 나누어 볼 수 있다.[10]

---

10) 사이버보안을 위한 현행법 규정은 침해행위의 유형으로 구분할 수도 있지만, 내용적으로 시스템보호를 위한 규정과 정보 자체의 보호를 위한 규정으로 구분할 수 있다. 우선, 시스템보호를 위한 규정으로는 정보통신기반보호법상 주요정보통신기반시설의 지정 등(제8조)·취약점의 분석·평가(제9조)·보호조치명령등(제11조)·주요정보통신기반시설 침해행위등의 금지(제12조)·복구조치(제14조), 정보통신망법상 정보통신망 침해행위 등의 금지(제48조)·정보통신망의 안정성 확보등(제45조)·集積정보통신시설의 보호(제46조), 형법상 업무방해죄(제314조 제2항)·컴퓨터등 사용사기(제347조의 2) 등을 들 수 있다. 둘째, 정보 자체를 보호하기 위한 규정으로는 전자서명법의 여러 규정(특히 제4장 인증업무의 안전 및 신뢰성 확보)과 정보통신망법상 개인정보보호 규정(제4장, 제22조 내지 제32조)·비밀등의 보호(제49조)·형법상 公전자기록위작·변작죄(제227조

여기에는 일반법도 있고 기본법 형태로 제정된 법률도 있지만 대부분 규율대상의 특수성을 고려하여 특별법 형태로 제정되었으며 하나의 법률이 동시에 여러 가지 목적을 위하여 시행되고 있음을 알 수 있다. 예컨대 1995년 형법개정 시 컴퓨터범죄를 유형화하여 새로 처벌 규정을 두었으나, 그 후 정보의 침해 내지 정보통신망의 보호에 관한 특별법이 다수 제정되었다.

여기서는 논의의 대상을 정보 시스템 및 네트워크에 관한 實體法에 국한하였으므로 형법, 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률을 중심으로 문제가 되는 내용을 알아보기로 한다.

<표 2>

우리나라의 정보보호 관련법률 현황

목 적	법률의 내역
① 정보 자체의 기밀성 보호(암호)	- 국가보안법, 국가정보원법, 군사비밀보호법, 형법 - 정보화촉진기본법, 전자거래기본법, 전자서명법
② 정보의 수집·이용에 관한 시스템, 네트워크의 보호	- 정보화촉진기본법, 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률 - 전자정부구현을위한행정업무등의전자화촉진에관한법률, 전자거래기본법, 전자서명법 - 형법, 통신비밀보호법 - 화물유통촉진법, 산업기술기반조성에관한법률, 무역업무자동화촉진등에관한법률
③ 개인정보의 보호	- 공공기관의개인정보보호에관한법률, 정보통신망이용촉진및정보보호등에관한법률 - 신용정보의이용및보호에관한법률, 금융실명거래및비밀보장에관한법률 - 통신비밀보호법
④ 정보보호산업의 육성	- 정보화촉진기본법, 전자거래기본법, 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률

자료: 김문환·박훤일·황 철, 「정보통신 유·무선서비스관련 보안강화를 위한 법제연구」, 국회 과학기술정보통신위원회 용역보고서, 2003.9, 32면.

의2)·私전자기록위작·변작죄(제232조의2)·비밀침해(제316조 제2항) 등을 들 수 있다. 2003.11.11 심포지엄에서 손진화 교수(경원대학교)의 토론 요지.

2. 형 법

1995년 형법개정 시 정보기술의 발달에 따른 새로운 범죄유형에 대응하기 위하여 제314조의 업무방해죄에 컴퓨터등 장애에 의한 업무방해죄를 추가하였다.

이는 컴퓨터등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해하는 행위이다. 해킹, 바이러스 유포로 인하여 컴퓨터 시스템의 작동에 이상을 일으킨 경우가 이에 해당한다.

3. 정보통신망이용촉진및정보보호등에관한법률

정보통신망이용촉진및정보보호등에관한법률[11](이하 "정보통신망법"이라 함)은 정보통신망[12]의 이용을 촉진하고 정보통신서비스[13]를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경의 조성을 목적으로 한다(정보통신망법 1조). 이 법은 사이버보안과 관련하여 정보통신서비스제공자에 대하여 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하도록 의무화(동법 45조1항)하는 한편 정보통신망 침해행위 등에 대하여 벌칙을 적용하고 있다(동법 62, 63조).

처벌대상은 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하는 행위(동법 48조1항), 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조(예: 해킹) 또는 그 운용을 방해할 수 있는 프로그램(예: 컴퓨터 바이러스, 웜)을 전달 또는 유포하는 행위(동법 48조2항), 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법(예: DDoS 공격)으로 정보통신망에 장애를 발생하게 하는 행위(동법 48조3항), 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하는 행

---

11) 이 법은 「정보통신망이용촉진등에관한법률」을 2001년 1월 16일 법률 제6360호로 전면 개정하여 같은 해 7월 1일부터 시행하고 있다.

12) "정보통신망"이라 함은 전기통신기본법 제2조제2호의 규정에 의한 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.

13) "정보통신서비스"라 함은 전기통신기본법 제2조제7호의 규정에 의한 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.

위(동법 49조)[14] 등이다.

정보통신망법에서 사이버공간의 안전성을 확보하기 위하여 컴퓨터 바이러스 등 악성 프로그램유포죄를 규정하고 나아가 정보통신망장애유발죄를 신설한 것은 정보화시대에 부응한 시의적절한 입법이라 하겠다. 사실 컴퓨터 바이러스를 제작, 유포함으로써 타인의 컴퓨터 시스템을 파괴한 경우에 기존 형법상의 업무방해죄로 처벌할 수도 있지만 오늘날 사이버공간에서는 무차별적으로 법익침해가 이루어지고 있으므로 정보통신망의 안전을 보호하기 위해서는 별도의 처벌 규정이 필요한 것이다.

뿐만 아니라 형법상의 컴퓨터등 장애에 의한 업무방해죄는 抽象的 危險犯이지만 현실에 있어서는 컴퓨터 바이러스의 복잡한 유포경로 때문에 그의 제작·유포행위와 시스템 파괴 내지 업무방해와의 因果關係를 입증하기 어렵다는 점을 감안하여 예비적 성격의 악성 프로그램 유포죄를 신설하여 처벌을 빈틈없이 하기로 한 것이다.

다만, 이들 규정의 해석에 있어서는 주의를 요한다. 예를 들어 최근의 바이러스 프로그램의 경우 처음부터 다른 사람의 시스템을 손상시킬 목적으로 설계된 프로그램도 있지만, 遠隔 애프터서비스라 등의 목적을 위해 설계된 프로그램이 악성기능을 발휘할 수도 있기 때문이다. 최근 들어서는 이런 종류의 프로그램이 해킹 등에 자주 이용되고 있다. 또 정보통신망법에서는 악성 프로그램의 단순 전달·유포행위를 처벌하고 있는데, 특별한 犯罪意圖 없이 프로그램을 전달하는 행위도 처벌될 수 있다. 예컨대 바이러스 동호회에서 동호회 게시판을 이용하여 컴퓨터 바이러스 샘플을 전송하는 행위도 처벌될 수 있으므로 업무에 따른 정당행위는 위법성이 없다고 보아야 할 것이다.[15]

실제로 정보통신망법의 처벌 규정을 살펴보면 기존 형법의 규정과 중복되거나 일부 개정만으로 해결할 수 있는 행위들이 나열되어 있다. 예컨대 정보통신망을

---

14) 이 조항은 법정형이 무겁기 때문에 형법 제316조 제2항에서 봉함 기타 비밀장치한 … 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자를 처벌하도록 한 것과 관련하여 해석상의 논란이 있다. 또한 통신비밀보호법 제16조에서도 전기통신의 감청행위 또는 통신의 내용을 공개하거나 누설한 자에 대하여 처벌 규정을 두고 있어 이들 행위유형은 대동소이하고 보호법익에 있어서 조금씩 차이가 있을 뿐인 데도 형량은 단계적으로 높아지는 문제가 있다.

15) 동 규정은 차라리 형법 제314조 제2항의 컴퓨터등 장애에 의한 업무방해죄에 미수범 처벌 규정을 두어 해결하는 것이 합리적이라는 견해가 있다. 백광훈, 「사이버테러리즘에 관한 연구」, 형사정책연구원, 2001, 219면; 양근원, 전게논문, 2003, 44면.

이용한 악성프로그램유포죄, 명예훼손죄, 음란죄 등은 일반 국민의 금지되는 행위에 대한 올바른 인식을 돕기 위해 일반법인 형법에서 규정하는 것이 바람직하고, 초고속 인터넷이 일반화된 오늘날 굳이 정보통신망을 이용하였다 하여 특별취급을 할 필요가 없기 때문이다.[16]

4. 정보통신기반보호법

가. 주요 내용

정보통신기반보호법은 주요정보통신기반시설을 전자적 침해행위로부터 보호하기 위해 2001년 1월 제정되어 2001년 7월 1일부터 시행되고 있는데, 동법의 보호대상은 국가안전보장, 행정, 국방, 치안, 금융, 통신, 운송, 에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망법 제2조 1항 1호의 규정에 의한 정보통신망[17]을 망라하는 정부와 민간이 운영·관리하는 정보통신기반시설을 망라한다(동법 2조 1호).

중앙행정기관의 장은 정보통신기반보호위원회의 심의를 거쳐 전자적 침해행위로부터 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정한다(동법 3조, 8조). 관리기관의 장은 정기적인 취약점 분석과 평가를 통해 그 결과를 바탕으로 기관별 보호대책을 수립하고, 보호대책을 종합·조정하여 소관분야의 주요 시설에 대한 관계 중앙행정기관별 보호계획을 수립하여야 한다(동법 9조).

한편 동법은 주요정보통신기반시설의 보호를 위한 범정부적 대응체제를 구축하기 위해 국무총리 소속 하에 정보통신기반보호위원회를 두고(동법 4조), 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우에는 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 限時的으로 위원회에 정보통신기반 침해사고 대책본부를 설치할 수 있게 하였다(동법 15조).

정보통신기반보호법은 금융·통신 등의 분야별로 정보통신기반시설 간의 취약

---

16) 미국에서 1984년에 제정된 컴퓨터사기및오용방지법(Computer Fraud and Abuse Act: CFAA)을 수 차례 개정한 끝에 1996년에는 정보기반보호법(National Information Infrastructure Protection Act)을 마련하는 등 기본법 형태로 법제를 정비하고 있다.

17) 두 법률의 관계를 살펴본다면, 정보통신망법은 전기통신기본법에서 정의하는 전기통신설비(전기통신을 하기 위한 기계·기구·선로 기타 전기통신에 필요한 설비)를 이용하여 정보를 처리하는 시스템 및 네트워크를 규율대상으로 하며, 정보통신기반보호법은 그 중에서도 주요정보통신기반시설로 지정된 것에 대하여 규정하고 있다.

점 및 침해요인과 대응방안에 관한 정보를 공유하고 침해사고가 발생하는 경우 실시간 정보를 교환·분석하는 체계를 갖추기 위한 정보공유·분석센터(Information Sharing and Analysis Center: ISAC)를 설치하도록 하였다(동법 16조). 정보통신시스템은 금융, 통신, 운송, 에너지 등 분야별로 시스템의 특성이 다르고, 이에 따른 보호체계 및 대책도 상이하기 때문에 외국에서도 ISAC의 운영을 적극 지원하고 있다. ISAC은 각 분야별 산업체가 자율적으로 설치할 수 있으며, 이를 운영할 사업자를 선정하여 아웃소싱 형태로 운영하면서 취약성 및 전자적 침해행위 정보를 기업 상호간에 공유하게 된다. 이와 아울러 정부는 정보공유·분석센터 설립을 장려하고, 전자적 침해행위 및 취약성 정보를 기업에게 제공하는 등 그 기준 및 환경 등에 대한 사항을 지원하게 된다.

정보통신기반보호법의 벌칙(동법 28조)에 의하면 다음의 행위(동법 12조)를 한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

o 접근권한을 가지지 않은 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위(예: 해킹, 컴퓨터 바이러스에 의한 주요정보통신기반시설의 교란, 마비, 파괴)

o 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스, 논리폭탄 등의 프로그램을 투입하는 행위

o 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위(예: 웜, 논리폭탄, 전자우편폭탄 등에 의한 DoS 또는 DDoS)

이상의 행위는 앞에서 살펴본 정보통신망법상의 행위가 주요정보통신기반시설에 대해 행해질 경우 한층 加重처벌하도록 한 규정이다.

나. 정보통신기반보호법의 문제점

(1) 법체계상의 문제

정보통신기반보호법의 집행에 있어서는 개별적으로 주요정보통신기반시설을 관리하는 기관이 있고, 소관분야의 주요정보통신기반시설을 관할(통할·조정)하는 중앙행정기관이 있으며, 정보통신부는 통일된 시설보호의 지침과 기술지원을 담당하고 이들을 종합·조정하는 국무총리 소속 하에 정보통신기반보호위원회를 두고 있다. 그 결과 행정조직법 측면에서 보았을 때 주요정보통신기반시설의 보호에 관한 업무를 직접 처리하지 않는 국무총리실에 심의기관을 두고 그 아래 실무위원

회가 있는 기형적인 모습을 하고 있다. 국무총리는 본법에서 규정하고 있는 업무와 관련된 정보나 현안을 잘 파악하고 있지 못하기 때문에 결국 심의회의 안건은 실무위원회에서 좌우하게 될 것이다.

그러나 우리나라의 행정현실에 비추어 실제 운용에 있어서는 정보통신부가 民·官 협력체제를 통하여 이니셔티브를 행사하고, 정부는 국무총리가 국정의 종합·조정을 통해 이를 뒷받침하는 형태로 운영하는 것이 타당하다고 생각된다.

또한 동법 제8조 제7항에서 주요통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항을 대통령령에 위임하고 있는데 이는 그 지정효과를 고려할 때 법률로 정할 사항을 포괄적으로 시행령에 위임한 것이다. 정보보호컨설팅전문업체의 지정(동법 17조 4항), 지정취소(동법 21조)에 관한 규정도 마찬가지이다.

(2) 보호대책의 충분성

국가의 주요정보통신기반시설에 대한 공격은 일상적으로 공격지와 대상지가 직접 연결되어 일어나는 방식은 극히 드물다. 대개의 공격자들은 수많은 경유지를 이용하여 추적과 공격 소스를 파악하지 못하도록 하며, 대부분 국내외 취약한 다수의 시스템을 이용하고 있어 이들에 대한 보안 및 추적활동은 필수적이며 선행적인 활동임에도 이 법에는 이들과 관련된 어떤 절차적 규정도 없다. 따라서 공격의 예방과 대응에 한계를 지닐 수밖에 없다. 따라서 법이 실제적인 효용성을 가지기 위해서는 단순히 보호대상에 따른 법규정이 필요할 뿐만 아니라 사안의 성격에 따라 관련되는 시스템들에 필요한 조치를 취할 수 있는 법규정이 필요하다.

(3) 취약성 분석·평가 주체의 문제

주요정보통신기반시설에 대한 예방대책은 취약성 분석·평가에서 비롯된다. 주요정보통신기반시설로 지정된 경우 각 전문기관의 지원을 받을 수 있는데 취약성 분석·평가의 주체로서 한국정보보호진흥원, 정보공유·분석센터, 정보보호컨설팅전문업체, 한국전자통신연구원 등이 열거되어 있다(동법 9조3항).

이 규정만 놓고 본다면 시설의 취약성 분석·평가를 함에 있어 어느 기관이나 선택하여 의뢰할 수 있는 것처럼 보인다. 특히 이 법의 지원을 받고 있는(동법 17, 24조) 정보보호컨설팅전문업체는 기술적 능력이나 비용 면에서 경쟁력을 갖고 수임을 할 것으로 예상된다. 그러나 주요정보통신기반시설은 국가 운영의 핵심시설이 많고 정당한 권한을 가지고 보관된 정보의 등급에 따른 비밀취급인가가 없으면 접근 자체가 불가능한 영역이다. 따라서 어떤 목적으로든 이 영역에 접근하기

위해서는 오프라인에서의 접근권한 이상의 자격이 있어야 할 것이다.[18]

물론 국가안보에 중대한 영향을 미치는 도로·지하철·공항, 에너지·수자원시설 등 주요정보통신기반시설에 대하여는 국가보안업무를 수행하는 기관에 우선적으로 기술지원을 요청하게 되어 있다(동법 7조2항). 국가의 핵심시설에 대한 취약점 분석·평가에 있어서는 공무원에 준할 정도의 비밀취급인가를 받은 사람에 한하여 접근권한을 부여할 필요가 있다.

(4) 분석자료 비밀유지 문제

취약성 평가·분석 후의 자료취급에 있어서 그 자료가 유출되었을 경우의 파장은 상상할 수 없을 정도로 중요하다. 따라서 그 정보는 비밀에 준하여 관리되어야 한다. 특히 민간업체나 연구기관에서 보관하는 경우에는 문제가 될 수 있다. 나아가 전문업체가 폐업하는 경우 보관하고 있던 자료에 대하여는 그의 폐기, 이관 등 비밀취급에 만전을 기할 필요가 있다.

(5) 民·官協力 및 정보공유의 문제

이 법은 공격에 대한 징후 또는 관련정보를 공유하기 위해 금융·통신 등 분야별로 정보공유·분석센터(ISAC)를 구축하도록 장려하고 있다(동법 16조). 정보공유·분석센터는 취약점 분석·평가의 지원기관으로서의 역할도 수행한다. 그러나 주요정보통신기반시설에 대한 공격의 징후는 한 두 개의 네트워크에만 해당하는 것이 아니고 대규모로 여러 네트워크에서 일어나는 경우가 많다. 이런 경우에는 여러 개의 정보공유·분석센터와 수사기관, 정보통신관련기관이 가지고 있는 정보를 종합하지 않으면 사안에 대한 정확한 판단이 불가능할 것이다.

따라서 관련기관이 예방, 기술적 대응, 법 집행에 있어서 유기적으로 대응할 수 있도록 기관 상호간의 자료 및 정보, 기술의 공유와 협력이 필요하다. 그러나 통신상의 프라이버시권(헌법 17조)을 침해할 우려가 있으므로 명확한 범죄적 징후, 대규모 피해발생의 우려, 다른 네트워크에 대한 연속공격 가능성 등 구체적 요건과 절차를 해당 법률에 명확히 규정할 필요가 있다.

---

18) 정보보호컨설팅전문업체의 지정절차를 보면 그 구성원에 대하여 단순히 일정한 기술적·전문적 능력을 요건으로 하고 있을 뿐 정책적인 고려나 인적 구성에 대한 신뢰성을 검증할 수 있는 장치는 미흡한 실정이다(동법 17조). 실제 우리나라에는 많은 정보보호업체가 난립하고 있으며 단지 해킹 기술이 탁월하다는 이유로 담당자의 윤리의식에 대한 검증 없이 보안업체의 연구원으로 채용되는 예도 많다.

IV. 사이버보안 관련법제의 개선방안

1. 사이버보안 강화의 목적

정보통신의 보안을 강화함에 있어서는 다음 목적에 유의하여야 할 것이다.

첫째, 1·25 인터넷대란과 같은 대규모 보안사고가 재발하지 않도록 해야 한다. 그것은 초고속 인터넷 통신망이 발달한 우리나라의 정보통신 시스템에 불법적인 의도로 침투하여 통신망을 교란시키려는 것을 방지하는 것은 물론 南北 긴장상태가 해소되지 않은 현 상황에서 적성국의 사이버 공격에도 대비해야 한다. 또한 경쟁국의 산업 스파이가 은밀하게 산업정보를 절취하는 것도 방지하여야 한다.

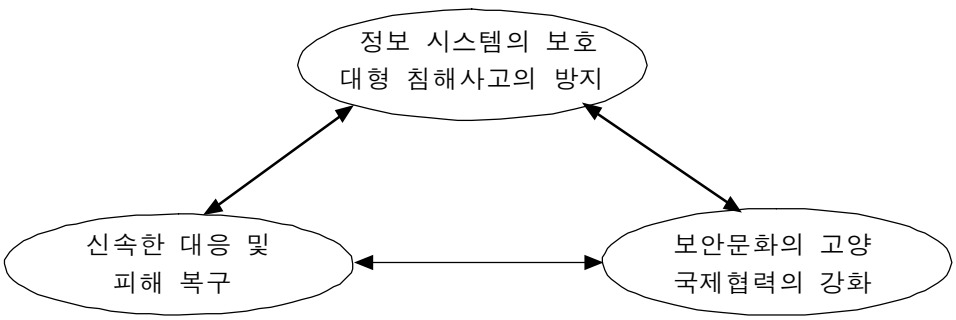
둘째, 정보 시스템에 대한 대규모 침해사고가 발생하였을 때 신속하게 대응하여 피해를 복구하고 경제적 손실이나 사회혼란이 더 이상 확대되지 않도록 한다. 오늘날 국가안보, 행정, 치안, 금융, 통신, 운송, 에너지 등 주요 시스템이 인터넷을 통하여 전자적으로 제어·관리되는 상황에서 정보 시스템의 마비는 가공할 만한 피해를 가져온다는 것을 경험적으로 확인한 바 있다.

셋째, 정보통신의 보안은 정보 시스템을 보호할 뿐만 아니라 이를 보안문화(culture of security)의 수준으로 고양시키고 국제협력을 강화하여야 한다. 이를 위해 사이버보안에 있어서도 국제표준을 설정해나가는 작업을 서둘러야 할 것이다.

이상 세 가지 목적은 상호 긴밀하게 연결되어 있다. 예컨대 정보 시스템에 대한 침해사고를 방지하기 위하여 법제를 완비한다 해도 정부와 정보보호업체, 정보통신망 이용자들의 보안문화가 확립되지 않았다면 실효를 거두기 어려울 것이다.

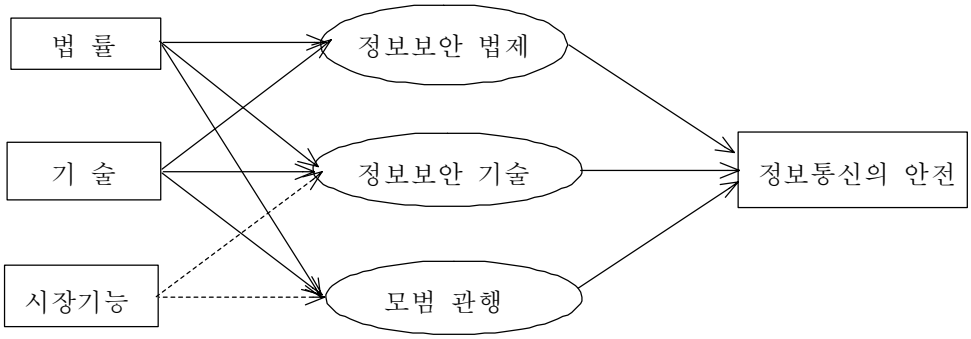
<그림 1>

정보통신 보안 강화의 목적



<그림 2>

정보통신 보안의 상호의존적인 모형



2. 사이버보안 강화의 수단

<그림 2>에서 보듯이 사이버보안의 강화를 위해서는 세 가지 측면을 함께 고려하여야 한다. 그것은 정부가 주도적으로 사이버보안에 관한 법률제도를 정비하는 것도 중요하지만 그 못지 않게 市場에서도 정보보안 관련업체들 상호간 그리고 정보통신망 이용자들과의 사이에 정보보안에 관한 모범적인 관행이 정립되는 기능(market forces)이 작동하여야 한다는 것을 의미한다. 아울러 사이버보안 기술에 있어서도 최적의 해결방법(solution)[19]이 모색되어야 한다.

다시 말해서 정보통신의 보안은 기술적으로만 해결할 수 있는 것이 아니다. 정부가 법률제도 상으로 정책목표 및 사이버보안의 기준을 설정하고 정부기관이 정보통신의 안전성에 대한 일차적인 책무를 부담하는 동시에 사이버보안 관련기업 및 이용자들이 이에 협조해야 하는 것이다. 또한 정보통신의 보안은 개인의 프라이버시 보호와 대립관계에 있기 때문에 양자의 균형을 도모하는 것도 중요하다. 뿐만 아니라 사이버보안 관련업체, 보안관리담당자, 이용자들이 사이버보안의 중요성을 인식하고 스스로 이를 지켜나가는 자율적인 행동규범이 마련되어야 한다.

그러나 이것만으로는 부족하다. 정보통신의 안전을 침해하는 기술이 발달하는 만큼 이에 대응하는 정보보호 기술의 진보를 위해서는 안정적인 시장이 확보되어야 하는 것이다. 다시 말해서 사이버보안 기술의 제일 큰 수요자인 정부기관들이

19) 이것은 技術法(*Lex Informatica*)의 형식으로 네트워크 구조에 기술표준, 프로토콜, 디폴트 환경설정을 심어놓는(embedded in network architecture) 방안도 가능할 것이다.

선도적으로 구매를 함으로써 기술의 발달을 촉진하고 이 과정에서 개발된 신기술이 주변 영역으로, 다른 나라로 파급되도록 하는 善循環이 이루어져야 한다.[20]

이를 위해서는 다음과 같은 행동계획(Action Plan)을 실천에 옮길 필요가 있다.

첫째, 정부는 정보통신의 보안을 위한 법제를 정비한다. 정부의 정보보호 조직은 특정 기구를 중심으로 개편하기보다 운영의 묘를 살려 현행 조직을 보다 유기적으로 연결하는 것이 바람직하다. 사이버 공격을 처벌하는 실체법은 기본법으로 일원화한다. 사이버 공격을 수사하기 위한 절차는 인권 및 프라이버시의 존중을 위해 법원의 심사를 받도록 하되 비상사태 발생 시에는 사태가 해소될 때까지 한시적으로 미국 애국법(USA Patriot Act)[21]과 유사한 제도를 도입한다.

둘째, 주요정보통신기반시설의 보호를 위하여 정부는 하드웨어, 소프트웨어를 포함한 정보보안 시스템 기타 제품을 우선적으로 구매하도록 한다. 정부가 앞장서서 구매할 때 정보통신 보안관련 업체는 시장의 확대에 따라 기술개발투자의 여력이 생기고 內需와 輸出도 증가하게 될 것이다.

셋째, 우리나라가 비교우위를 가진 바이러스 백신, PKI 암호기술, 가상사설망 등 전략적인 정보보호산업을 육성한다.

넷째, 기업과 개인의 사이버보안의식을 제고함으로써 국내 정보보안시장을 확장될 수 있는 풍토를 조성한다.

다섯째, 정보보호산업의 국제표준화 및 수출을 지원한다.

---

20) 일본정부 산하의 통신종합연구소는 2004년 1월 NTT, KDDI, 니프티, NEC가 설립한 Telecom ISAC Japan과 공동으로 '정보시큐리티센터'를 발족시켜 해커의 침입이나 바이러스 발신원을 빠른 시간 내에 역탐지해 방어할 수 있는 기술을 개발하기로 했다. 이 같은 민·관 공동 대응은 전자정부 관리기반을 강화하고 전자상거래 등을 안심하고 이용할 수 있는 환경정비에 의의가 있으며, 공동으로 해커·컴퓨터 바이러스의 공격에 대항할 수 있는 기술을 개발하게 된다. 일본 총무성에 따르면 일본내 해커 및 컴퓨터 바이러스 관련 피해액은 4000억엔 정도로 추산되고 있다. 전자신문, "일본, 민관 공동 사이버테러 방지 기술 개발", 2003.12.26.

21) 미국에서는 9·11 테러 사건이 발생하자 정부와 의회가 초당파적인 對테러 법안을 마련하였다. 하원과 상원의 「Patriot Act」와 「USA Act」 법안을 통합·조정한 「USA Patriot Act」(Uniting and Strengthening America + Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act: 일명 "애국법")은 2001년 10월 26일 부시 대통령의 서명을 얻어 공포되었는데 기존 전기통신프라이버시법(CFAA는 1996년 국가정보기반보호법(National Information Infrastructure Protection Act)으로 전면 개정되었음) 등을 개정하여 사이버 공격의 수사에 따른 절차 요건을 대폭 완화하고 수사기관의 권한을 강화한 것이 특색이다. 이 법은 2005년 12월 31일까지만 발효되는 限時法이다.

3. 사이버보안을 위한 조직의 정비

현재 우리나라는 2001년 7월부터 시행 중인 정보통신기반보호법에 의하여 기관별로 사이버 공격에 대한 대응업무를 수행하고 있으며, 해당 관리기관장의 책임하에 사이버보안 업무를 수행하고 있다. 실제로는 크게 국가부문과 민간부문으로 나누어 각각 국가정보원과 정보통신부가 정보보호에 관한 총괄적인 책임을 맡고 있다. 그러나 신속하고 광범위하게 동시·다발적으로 발생하는 침해사고에 효율적으로 대처하기 위해서는 범국가적 대응체제에 입각하여 각급 국가기관과 공기업, 기간통신사업자, 연구기관, 학계, 정보보호업체가 상호 유기적으로 공조활동을 벌일 필요가 있다.[22]

그리고 정보보호 시장을 공공부문과 민간부문으로 나누어 전자는 신규 수요를 창출하고 신기술을 도입하는 데 주력하는 한편 후자는 차별화된 기술과 제품을 가지고 경쟁을 벌임으로써 사용자들의 선택의 폭을 넓히도록 함으로써 해결하는 것이 바람직하다고 본다.

보다 심각하게 제기되고 있는 문제는 2003년 8월 14일 미국 북동부 지방과 캐나다를 엄습한 대규모 정전 사태를 거울삼아 우리나라에서도 주요정보통신기반시설에 대한 보호대책을 새롭게 마련해야 한다는 것이다. 우리나라에서 사이버공간의 재난 대책은 정보통신기반보호법상 정보통신기반보호위원회를 중심으로 정보통신부 산하의 인터넷침해사고대응지원센터(KISA CERT), 국방부 컴퓨터침입사고대응반(CERT), 경찰청 사이버테러대응센터(CTRC) 등의 기구가 담당하게 되어 있다. 현재 국무총리가 위원장인 정보통신기반보호위원회를 대통령 직속의 합의제 행정기관으로 격상하는 방안, 위원회가 아닌 행정관청 형태의 「정보보안국」을 설치하는 방안이 거론되고 있다.

그러나 조직체계를 강화한다고 하여 당면 문제가 해결될 것으로 보이지 않는다. 왜냐하면 미국의 경우 9·11 테러 사건으로 국토안보(homeland security)에 대한

---

22) 국가정보원은 「2003 국가 정보보호 백서」에서 국가의 사이버테러 대응 및 정보보안 업무를 체계적이고 종합적으로 수행하기 위해서는 통치권 차원에서 사이버 안전보장을 위한 종합계획이 수립·시행되어야 한다고 주장했다. 국가정보원은 또 사이버테러를 예방하기 위해서는 보안관제 및 예·경보체계의 구축·운영이 필요하다고 보고, 현재 운영중인 '정보보안 119'와 '분야별 침해사고대응센터'(Computer Emergency Response Team: CERT) 및 '정보공유·분석센터'(ISAC)의 연계를 본격적으로 추진하는 한편 한국정보보호진흥원(KISA)이 설립하는 민간분야의 인터넷침해사고대응센터와의 연계도 모색하기로 했다. 디지털타임스, "사이버테러 대응 일원화", 2003.6.20자.

위기감이 고조되어 비상 대처방안으로 시행된 것이고 이에 대한 미국내 반론도 만만치 않은 실정이다.[23]

그러므로 새로운 기구를 만드는 것보다 기존 대응체계가 유기적으로 기능을 발휘하게 하는 공조 시스템을 강화하는 것이 보다 중요하다고 생각한다. 미국이 2003년 8월 북동부 지방의 정전사태를 비교적 큰 혼란 없이 극복할 수 있었던 것은 9·11 사건 이후 한층 강화된 위기관리 시스템이 가동되었고, 무엇보다도 오래 전부터 전력 시스템의 붕괴에 대비한 대처요령이 마련되어 있었기 때문이다.[24]

우리나라는 정보통신부가 2001년 정보통신기반보호법을 시행하면서 금융, 통신 분야의 정보공유·분석센터(ISAC)를 설립했으나, 전력, 에너지 분야까지 망라한 종합적인 대응체계가 갖춰져 있지 않은 실정이다. 따라서 우리나라도 새로운 조직을 만들기보다는 현행 대응체계의 문제점을 지속적으로 개선해나가면서, 가상훈련을 통해 취약점을 파악하고 이를 시정하는 것이 급선무라고 생각된다. 이러한 방안은 현행 정보통신기반보호법의 운용의 묘를 살려 실제 상황을 방불케 하는 도상훈련을 정기 또는 수시로 실시함으로써 소기의 성과를 달성할 수 있을 것이다.

4. 형사처벌 규정의 一元化

앞에서 살펴본 바와 같이 우리나라의 사이버 침해행위에 대한 처벌 규정은 형법, 정보통신망법, 정보통신기반보호법 등에 산재되어 있다. 이들 규정은 유사한 태양의 행위에 대해 결과 또는 보호대상에 따라 조금씩 다르게 罰則을 정하고 있다.

---

23) 미국의 경우 정보보호 및 사이버테러 대응업무를 국토안보부(DHS)로 일원화한 사례에 비추어 초고속인터넷 인프라가 완비된 우리나라에서는 강력한 통합조직이 필요하다는 주장이 설득력을 얻고 있다. 그러나 우리나라의 행정경험에 비추어 볼 때 기구를 격상한다 해도 실제로 그 기능을 수행하는 것은 일선 관리기관이므로 실효를 기대하기 어려울 뿐만 아니라 시민단체와 언론에서 새로 설치되는 정보보안국에 대해 "사이버 중앙정보부"(Cyber CIA)라며 강력히 반발하고 있다.

24) 미국의 경우 9·11 사태 이후 국토안보부(DHS)를 신설하여 주요정보기반보호에 관한 권한을 부여하고 이에 관한 업무를 총괄 운영토록 하였다. 이에 따라 연방컴퓨터사고대응센터(Federal Computer Incident Response Center), 국가기반시설보호센터(National Infrastructure Protection Center), 주요기반시설보장국(Critical Infrastructure Assurance Office), 국가통신체계(National Communications System)가 DHS로 이관되었다. 미국은 이미 클린턴 대통령 시절부터 전력붕괴 시나리오를 만들어놓고 유사시에 에너지부, 국방부, FBI, 주정부가 어떤 역할을 수행할지 명확히 하였다. inews24, "미 정전사태의 교훈... 한국도 종합대응 필요", 2003.8.18.

특히 형사처벌에 관한 법률은 가급적 일원화하여 단순·명료하게 규정하여야 예측가능성과 실효성을 높일 수 있다. 특별법상의 벌칙은 일반법으로 처리할 수 없는 특별한 경우에 예외적으로 인정되는 것이 타당하다. 미국의 사이버 공격에 대한 처벌 규정을 보면 1984년 컴퓨터사기및오용방지법(CFAA, 18 U.S.C. §1030)을 기본으로 기술의 발달, 시대상황 등을 고려하여 조문을 손질함으로써 사이버공간에서의 각종 범죄에 대응하고 있는 것은 시사하는 바 크다.

반면 우리나라의 경우 새로운 유형의 컴퓨터 범죄를 1995년 형법개정 시 반영하였으나 그밖의 사이버 침해행위에 대해서는 기존 형법 규정을 개정하기보다는 새로운 특별법에 벌칙을 규정하는 등 법적 안정성, 예측 가능성, 체계의 일관성을 해치고 있다. 따라서 다음과 같이 가급적 일원화된 체계를 갖는 것이 필요하다고 생각된다.

가. 刑法 등 처벌규정의 정비

우선 기존 형법의 개정만으로 충분한 범죄 유형은 특별법의 처벌 규정을 없애고 형법으로 일원화하도록 한다.

특히 사이버테러 범죄의 경우 형법상 컴퓨터등 장애 업무방해죄에 접근권한 초과행위 금지 및 미수범 처벌규정을 두고 보호대상에 따라 형량을 차별화한다면 정보통신망법의 '정보통신망 침해행위등의 금지'(동법 48조) 관련 조항과 정보통신기반보호법의 '주요정보통신기반시설 침해행위등의 금지'(동법 12조) 관련 조항은 이에 포함시킬 수 있을 것이다.

또한 형법상의 비밀침해죄(형법 316조) 규정을 개정하여 '정보통신망상의 정보 및 비밀침해' 행위를 추가한다면 정보통신망법 제49조의 '비밀등의 보호' 규정을 커버할 수 있고, 비밀의 종류별로 각각의 처벌 규정을 둠으로써 비밀보호의 수준에 따라 형량이 모순되는 것도 바로 잡을 수 있을 것이다.

나. 정보통신기반보호법의 정비

정보통신기반보호법은 국가적으로 핵심적인 정보통신기반시설에 대한 공격의 예방 및 대응절차, 처벌 규정 등 실체법적인 내용을 포함시키되 관련업체의 육성·지원에 관한 부분은 전기통신사업법 등의 사업법에 통합하거나 별도의 법령을 제정하는 것이 타당하다고 본다.

이와 관련하여 주요정보통신기반시설에 대하여 정보보호 컨설팅을 하는 경우에는 핵심시설의 민감성을 감안하여 접근 가능한 인적자원의 선별 조치가 요구된다.

국가공무원도 중요한 자료에 대한 접근은 보안등급 별로 제한되어 있는 점을 감안할 때 민간 보안전문업체가 국가의 주요기반시설에 대한 정보보호 컨설팅을 수행하는 것은 현실적으로 쉽지 않을 것이다. 따라서 정보통신기반보호법상 정보보호컨설팅전문업체를 지정할 경우 컨설팅 참여 직원들에 대한 신원조회 등 비밀취급인가 자격 검증에 버금가는 절차적 보완이 선행되어야 한다.

정보통신기반보호법에는 공격에 대한 징후 또는 관련 정보를 공유하기 위한 여러 가지 제도가 마련되어 있지만 어느 한 기관의 활동만으로는 사이버 공격에 대해 효과적으로 대응할 수 없다. 따라서 관련기관간의 정보·기술의 공유 및 협력을 촉진하는 규정이 보완되어야 할 것이다.

다. 정보통신망법의 정비

2003년 정기국회에서 정보통신망법 개정안이 통과되었다. 개정의 취지는 인터넷의 안전성·신뢰성을 확보하고 인터넷을 이용하는 각 당사자의 책임과 역할을 명확히 하기 위한 것이다. 이번 정보통신망법 개정법률은 인터넷 침해사고의 방지와 정보보호의 강화를 목적으로 하는데, 前者에 관한 개정법률의 골자는 다음과 같다.

- 인터넷 정보보호를 강화하기 위하여 전국적으로 정보통신망접속서비스를 제공하는 자 등[25]에 대하여 정보보호지침의 준수를 의무화하고 매년 정보보호 안전진단을 받도록 함(45조 4항 및 46조의3 신설).
- 중대한 침해사고가 발생하여 정보통신망에 심각한 장애가 발생할 우려가 있는 경우에는 集積정보통신시설 사업자(IDC)가 당해 서비스 제공의 전부 또는 일부를 중단하는 긴급조치를 할 수 있도록 함(46조의2 신설).
- 주요정보통신서비스제공자는 정보통신망에 중대한 침해사고가 발생하여 정보통신망등에 심각한 장애가 발생할 가능성이 높은 경우에는 이용자에게 보호조치의 권고등을 할 수 있도록 함(47조의2 신설).
- 정당한 권한 없이 또는 허용된 접근권한을 초과하여 부정한 목적으로 타인의 정보통신망에 침입을 시도한 자도 처벌할 수 있도록 하는 등 벌칙을 강화함(63

25) 주요 인터넷서비스제공자(ISP)·인터넷데이터센터(IDC)·대형 온라인쇼핑몰 등 다중이용시설은 매년 정보보호컨설팅전문업체로부터 진단을 받아야 하며, 이를 게을리 한 때에는 과태료가 부과된다. ISP·IDC는 정보통신부 또는 KISA에 사고 유형별 통계, 데이터 소통량 및 접속경로별 이용통계 등 통계자료를 제공하고 사고 발생 시 즉시 정통부·KISA에 신고해야 한다.

조 2항 신설).

이번 개정법률은 1·25 인터넷 대란이 종전의 사이버 공격과는 달리 네트워크가 공격을 받아 전체 인터넷망에 장애를 일으켰다는 점에 주목하고 무엇보다도 정보 시스템 및 네트워크를 이용하는 정부·기업·이용자 등 관련자 전원이 유기적으로 공조하게 하는 데 주안을 두었다. 정보통신망법 개정법률은 '음성통신시대를 넘어 데이터통신시대에 맞는 정보보호 관련법'이라는 평가와 함께 시장 논리에 따라 민간이 주도하는 인터넷 기반의 데이터통신에 적합한 모범관행(best practices)을 규범화한 것으로 여겨지고 있다.

그러나 정보통신기반보호법에서 규율해야 할 사항을 규정하고 있는 것, 심각한 네트워크 장애가 발생할 우려가 있는 경우 IDC가 개인 이용자의 접속을 제한할 수 있도록 한 것, 해킹이나 바이러스 유포행위의 미수범을 처벌하기로 한 것 등은 상당한 논란을 불러일으키고 있다. 사이버공격 미수범을 처벌하는 규정 역시 과잉입법이라는 비판을 받고 있는데, 이는 사이버공간에서는 언제 실행행위의 착수가 있었는지를 확인하기가 어렵고 처벌대상자를 규명하기도 쉽지 않을 뿐더러 '인터넷 상의 표현의 자유'를 침해할 우려가 있다는 주장이 제기되었다.

그러나 컴퓨터의 서기 2000년 인식 오류 문제 'Y2K 소동'으로 막을 연 21세기에는 사회의 모든 부문이 인터넷을 기반으로 움직이고 있다. 전체주의와 공산주의의 부상과 몰락을 목격한 20세기에는 '자유와 권리'가 중시되었으나, 21세기 네트워크 사회에서는 일부 이용자의 악의적 행동이 전체의 기능마비를 초래할 수도 있으므로[26] 20세기형 자유와 권리의 개념을 그대로 인정할 수 없는 실정이다. 그런데 사이버범죄는 누가 저지른 것인지 알기 어렵고 당초 의도와 전혀 다른 사이버공간 침해상황을 야기할 수도 있으며, 전세계에 걸쳐 동시적으로 침해행위를 전파할 수 있는 데다 조사를 한다 해도 원인행위자를 추적하기 어렵고 시간도 많이 걸리는 특성을 고려할 필요가 있다. 사이버공간에서는 아무리 지성적이고 평범한 사람일지라도 악의적인 바이러스 유포자, 테러리스트로 표변할 수 있는 것이다.[27]

---

26) 이를테면 어느 천재적인 컴퓨터 이용자가 누구를 공격하려는 특별한 의도 없이 자신의 실력을 과시하기 위해 바이러스를 유포시킨 것이 사회 전체의 정보통신망을 마비시키는 결과를 가져올 수도 있다. "서울에서의 나비의 날개짓이 지구 반대편 뉴욕에서는 폭풍을 몰고 올 수 있다"(butterfly effect)는 '카오스 이론'과 비슷하다.

27) 유나바머(Unabomber)는 1978년부터 17년 동안 대학교와 항공사에 폭발물을 넣은 소포를 보내 3명을 살해하고 23명을 부상시키는 등 미국 전역을 공포에 몰아넣은 테러범의 별명이다. 1996년에 체포된 그는 평소에는 대학교수 테오도르 카진스키로서 행세했지만

그렇다면 사이버공간에서는 '새로운 게임 법칙'(Rule of Game)을 적용하기로 하고, 이상의 규제는 사이버범죄에 한하여 적용된다고 하더라도 국민의 기본권을 침해하는 부작용은 없을 것으로 생각된다.

이러한 견지에서 IDC・ISP의 이용자접속 제한, 침해행위의 미수범 처벌은 일정 요건 하에 허용될 수 있는 것이다. 그 조건이란 민・관・산・학의 유기적인 공조가 이루어지고, 객관적인 행위유형에 비추어 침해사고가 합리적으로 의심(reasonable doubt)되는 상황에서 보호조치로 인하여 일부 이용자가 입는 피해보다 전체의 이익이 압도적으로 큰 경우라야 할 것이다. 또 이용자의 피해를 최소화하기 위해 이용자에게 책임을 지우고 무조건 접속을 중단하기보다는 용이하게 안전조치를 이행할 수 있게 하거나 자동으로 안전조치를 이행하게 하는 등의 기술적인 해결방안을 모색하도록 해야 할 것이다.

사이버범죄의 미수범을 처벌하는 것은 유럽회의의 사이버범죄방지협약[28]을 따른 것이다. 동 협약의 제3조(불법감청), 제4조(데이터손괴), 제5조(시스템손괴), 제7조(컴퓨터관련위조), 제8조(컴퓨터관련사기) 등은 미수범 처벌 규정을 두고 있다. 우리나라가 유럽의 여러 나라, 미국, 캐나다, 일본 등이 이미 가입한 이 협약에 가입하려면 그에 부합된 규범의 정비가 필요함은 물론이다.[29]

주제어: 컴퓨터, 통신망, 사이버공간, 정보통신기반시설, 전자적 침해행위, 사이버보안, 보안문화, 정보공유・분석센터

Key Words: computer, telecommunication network, cyberspace, information infrastructure, electronic incidents, cybersecurity, culture of security, Information Sharing and Analysis Center(ISAC)

남 몰래 과학기술을 응용한 테러를 자행했던 것이다. 지금도 얼마든지 "제2의 유나바머"가 나올 수 있는 상황이다. 박성래, "사이버테러 대비하자", 한국경제신문 다산칼럼, 2003.1.27자.

28) 유럽회의(Council of Europe)는 1990년대의 준비기간을 거쳐 2001년 11월 각료위원회에서 「사이버범죄방지협약」(Convention on Cybercrime)을 채택하였다. 이 협약은 43개 유럽회의 회원국은 물론 미국, 캐나다, 남아프리카공화국, 일본 등의 옵서버 국가들도 가입해 있다.

29) 이영준・정 완・금봉수, 「사이버범죄방지조약에 관한 연구」, 한국형사정책연구원 연구보고서 01-30, 2001, 89면 참조.

참고 문헌

김문환・박훤일・황 철, 「정보통신 유・무선서비스 관련 보안강화를 위한 법제연구」, 국회 과학기술정보통신위원회 용역보고서, 2003.9.

김현수, "9・11 이후 미국 국토안보정책 현황 분석-조직정비와 사이버보안 강화법제를 중심으로", 2002.

백광훈, 「사이버테러리즘에 관한 연구」, 형사정책연구원, 2001.

_____, 「인터넷범죄의 규제법규에 관한 연구」, 한국형사정책연구원, 2000.

양근원, 「사이버테러의 실태와 법적 대응에 관한 연구」, 경희대학교 국제법무대학원 석사학위논문, 2003.

이영준・정 완・금봉수, 「사이버범죄방지조약에 관한 연구」, 한국형사정책연구원 연구보고서 01-30, 2001.

조병인, 「사이버범죄에 관한 연구」, 한국형사정책연구원, 2000.

국가보안기술연구소, "미국 사이버보안 정책 동향-미국 사이버보안 국가전략을 중심으로", 2003.3.

국가정보원, 「2003 국가정보보호 백서」, 2003.5.

정보통신부, 「정보보호 강화대책 수립을 위한 정책토론회 자료집」, 2003.3.

Joel R. Reidenberg, "Privacy Protection and the Interdependence of Law, Technology and Self-Regulation", 23rd International Conference of Data Protection Commissioners, Sept. 25, 2001.

Lee M. Zeichner, *Cyber Security and Corporate Liability, Business Law Monographs Corporate Series*, Volume C10, Matthew Bender, LexisNexis, 2002.

OECD Working Party on Information Security and Privacy, "Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards A Culture of Security", 2002.
<http://www.oecd.org/pdf/M00034000/M00034292.pdf>

The White House, *The National Strategy to Secure Cyberspace*, February 2003. <http://www.whitehouse.gov/pcibp/cyberspace_ strategy.pdf>

주요 경제지/전문지 기사 : 한국경제신문, 전자신문, 디지털타임스, inews24 등

국회통과 새법률 사이트 <http://www.assembly.go.kr/> [2003.12.31]

<Abstract>

Legal Issues on the Enhancement of Cybersecurity

Park, Whon-Il

In this Information Age, it is quite true that knowledge or information is traded like tangible goods through the Internet. Businesses, big or small, are employing information technologies to enhance their competitiveness. The government adapts itself to the quickly developing e-environment.

The role of law is also changing in the course of information revolution. It has to suggest a new direction and is ready to support IT businesses with various incentives.

The cyberspace consists of millions of computers, servers, routers, communication cables, etc. and functions as a pivotal infrastructure of the nation. So the cybersecurity is first and foremost important in the daily operation of computer systems and networks. As we witnessed during the worm virus-driven Internet fiasco in January 2003, the breakdown of the nation's online networks for a half day would cripple our socio-economic life to the uncontrollable extent.

Therefore, various kinds of cyber-attacks or threat should be prevented and suppressed to maintain the telecommunications infrastructure and to secure the cyberspace of the nation. This article delves into the proposed possible amendment to the current laws concerning information systems and communication networks.

The pertinent substantive laws are the Criminal Code, the Information and Telecommunication Infrastructure Protection Act and the Act to Promote Information Telecommunication Networks and to Protect Personal Information among others. This article stresses a concerted approach to punishment against the same kind of electronic offenses. In other words, the relevant provisions of the Criminal Code should be firstly invoked as a general law rather than the special laws in case of electronic offensive incidents. Also this article calls for harmonized efforts and systematic cooperation by the government, IT-related businesses and individual Internet users to secure the cyberspace.