韓國公安行政學會報 – 第38號(2010): ??–??
투고일 2009.??.?? / 심사일 2009.??.?? / 게재확정일 2009.??.??

테크놀로지 발전에 따른 사이버범죄의 진화와 범죄현상의 조명 및 대응

이 병 종

(동국대학교 경찰행정학과 겸임교수)

韓國公安行政學會報 – 第38號(2010): ??–??
투고일 2010.??.?? / 심사일 2010.??.?? / 게재확정일 2010.??.??

테크놀로지 발전에 따른 사이버범죄의 진화와 범죄현상의 조명 및 대응

이 병 종*

【국문요약】

컴퓨터에 뒤이어 현대기술 발명의 상징인 '인터넷'과 '디지털' 시대로 들어옴에 따라, 오늘날 우리 인류는 정치·경제·사회·문화의 모든 영역에서 폭발적인 지식과 정보를 공유하게 됨에 따라 삶의 풍요와 생산성의 향상으로 큰 혜택을 누리고 있다. 그러나 가상공간에서의 정보 기회의 확대는 사이버범죄의 확대로 이어지게 됨으로서 일반대중은 물론이고 사회적인 두려움도 늘고 있다. 사이버범죄는 컴퓨터에 내장된 고객이나 가격정보의 불법활용과 같은 단순한 범죄로부터 디도스, 피싱과 같은 사이버테러와 인터넷웜과 같은 바이러스, 소프트웨어 해적행위, 사이버스토킹, 전자사기, 불로그 등의 음란물과 성폭력, 허위사실 유포와 악플 등의 피해뿐만 아니라 최근에는 무선통신의 발달로 휴대폰, 노트북과 개인정보 단말기 등과 관련된 디지털범죄 또한 증가하고 있는 실정이다. 따라서 전통적 범죄가 '노상범죄'라고 한하면 오늘날 21세기 새로운 범죄는 '키보드'에 의해 저질러지는 사이버범죄로 변화하고 있다고 할 수 있다.

사이버범죄는 컴퓨터가 민간 및 공공 부문에서 사용이 확대되고 1990년대 인터넷이 성행되고 디지털기술 등의 인포메이션 테크놀로지의 확대에 따라서 생성된 개념이며, 그 이론적 뿌리는 화이트칼라범죄에 기원을 두고 있다. 사이버범죄에 대해서는 그동안 단편적인 연구는 많이 존재하였으나 범죄의 개념 정립에 관한 총체적 접근이 없었기 때문에 용어의 이해와 범죄현상의 파악과 대응의 문제점이 되어 왔다. 따라서 본 연구는 사이버범죄의 진화와 개념의 정립, 범죄현상의 파악을 통해 이에 대응하는 방안을 모색코자 한다. 사이버범죄는 단일현상이라기보다는 정보네트워크와 통신테크놀로지에 의해 수행되는 것으로 가상공간이 주축이 되어 야기된다는 점을 강조하기 위한 것이다. 따라서 사이버범죄는 컴퓨

* 동국대학교 경찰행정학과 겸임교수, volcanic51@hanmail.net

터, 인터넷, 조직적인 네트워크 그리고 디지털기술과 같은 전자적 장비를 활용하여 인포메이션 테크놀로지를 이용하여 불법적 행위를 용이하게 하는 것으로 최근 디지털 기술과 관련이 늘고 있다.

사이버스페이스에서 조직범죄, 각종 극우파, 산업스파이, 전자상거래의 교란, 해커기술의 첨단화, 정보통신기술의 발전, 아동포르노그래피 그리고 테러리즘 등등에 관련된 사이버범죄들이 난무함에 따라, 사이버스페이스에 맞는 효율적인 경찰활동이 새롭게 요구되고 있다. 이에 따라 전통적 경찰활동의 역할의 변화와 함께, 사이버범죄가 증대된 만큼 사이버 경찰활동의 역량제고를 위한 '디지털실체주의'가 이루어질 필요가 있다. 범죄학 이론과 관련하여서는 지리적 경계가 없는 범죄행위지, 능력과 기술을 갖춘 범죄자 그리고 사이버범죄의 올바른 이해가 요구된다. 제도적 개선을 위해서는 사이버범죄관련 법률의 체계적 정비와 국제적 형사공조, 그리고 범죄의 신속한 대응을 위한 수사권의 확보가 필요하다. 마지막으로 현실세계에서 윤리가 정립된 것처럼 가상공간에서의 윤리의 확보가 필요하다.

주제어 : 사이버범죄, 컴퓨터범죄, 인터넷범죄, 하이테크범죄, 가상공간, 디지털

목차

Ⅰ. 서 론

오늘날 인류는 두 개의 세상에서 동시에 생활하고 있다. 그 하나는 현실세계라고 하는 오프라인 세계이고, 다른 하나는 가상세계인 온라인 세계이다. 인터넷의 발전은 세계를 일일생활권으로 만들었고 '지구촌화' 그리고 새로운 산업혁명으로 불리는 '정보화시대'를 가져왔고, 비지니즈, 소비, 레저 그리고 정치면에서 엄청난 확대를 이룩하였다. 그러나 이 같은 테크놀로지의 발전은 또한 우리들의 행복과 안전에 대한 위협이 되고 있는 것도 사실이다. 테크놀로지의 발전은 그 역기능으로 불법과 비행에 대한 기회를 제공함으로서 디도스와 같은 분산서비스거부공격의 사이버테러, 보이스피싱, 인터넷대란을 야기한 웜바이러스, 전자적 사기, 해적행위, 허위 쇼핑몰 개설, 대포폰과 대포통장을 이용한 사기, 원조교제와 성매매, 불법오락과 도박 그리고 자금세탁 등이 행해짐으로서 개인에 대한 피해의 발생뿐만 아니라 사회에 대해서도 안전, 질서, 경제번영 그리고 정치적 자유에 대한 도전이 되고 있다.

사이버범죄는 군대와 기업에서 컴퓨터가 처음으로 도입되고 기업과 대학, 정부 등에서 활용이 확대되면서 컴퓨터범죄라는 개념이 생성되게 되었으며, 1990년 인터넷의 등장으로 더욱 가속화되고, 하이테크의 상징인 디지털기술이 우리의 일상생활에서 필수요소로 등장하면서 더욱 확대 발전되고 있다. 사이버범죄는 테크놀로지의

발전과 함께 탄생된 신개념으로서 그 이론적 뿌리는 지위, 권한 그리고 전문성을 이용하여 영리를 추구하는 화이트칼라범죄 개념과 함께 진화되어 왔다. 우리나라의 2008년 사이버범죄 발생은 136,819건으로 전년 동기 대비 54%가 증대되었다. 가상공간에서의 불법과 부정행위는 날로 확대되어 범죄현상은 난무하고 있는데 이를 규제하고 연구하는 영역은 미흡한 실정이다. 또한 사이버범죄자들은 사이버범죄의 특성인 익명성과 개방성을 배경으로 하기 때문에, 범죄에 대한 죄책감이 둔화됨으로서 사이버범죄 현상에서 윤리의 확보가 큰 문제점이 되고 있다.

테크놀로지발전에 따른 가상공간에서의 불법행위는 그 범죄현상을 어떻게 파악하느냐에 따라 범죄학계에서는 컴퓨터범죄, 인터넷범죄, 하이테크범죄, 네트워크범죄, 디지털범죄 등 여러 가지 용어로 설명되고 있다. 이처럼 사이버범죄에 대한 이해가 다양하기 때문에 많은 전문가나 실무자들이 사이버범죄에 대한 이해와 대응에 있어서 혼란을 겪고 있다. 또한 지금껏 사이버범죄에 관하여 각론적으로 많은 연구들이 있었으나 정작 사이버범죄에 대한 총론적인 논의가 없었으므로 사이버범죄의 완전한 이해가 없이 단편적 사회현상만 탐구하는 오류에 빠지는 결과를 가져왔다. 따라서 이 연구는 사이버범죄의 이론적 고찰, 그 진화과정, 범죄현상의 실체와 함께 사이버범죄에 대한 정의를 세움으로서 아래와 같은 목적을 달성하고자 한다. 첫째, 테크놀로지 발전에 따른 사이버범죄의 진화를 체계적으로 고찰한다. 둘째, 사이버범죄에 대한 단편적이고 각론적인 접근의 문제점을 보완하기 위해, 총론적인 개념 정립을 함으로서 사이버범죄 개념에 대한 정확한 이해를 수립하고자 한다. 셋째, 사이버범죄의 진화에 따른 최근의 범죄현상을 조명함으로 사이버범죄의 실태를 파악한다. 넷째, 사이버범죄의 이해와 실체 파악에 따라 전통적 경찰활동의 한계를 극복함으로서 '디지털실체주의'를 수립토록 하며, 지리에 기초한 전통적 범죄학 이론인 범죄지와 범죄자에 대한 인식을 다시 함으로서 사이버범죄 이론의 수립을 목표로 한다. 다섯째, 위와 같은 연구를 통하여 사이버범죄에 대한 제도적 대응을 수립하고자 한다.

Ⅱ. 이론적 배경

전통적으로 범죄란 노상범죄인 살인, 강도, 강간, 폭행 등을 의미하였다. 그러나

서더랜드가 '화이트칼라범죄'를 밝힘으로서 그 불일치를 선언하게 되었다. 사이버범죄의 개념형성은 컴퓨터와 인터넷을 배경으로 한 네트워크 테크놀로지에 의해 형성되었으며, 그에 대한 일반적 구성은 사이버스페이스와 범죄의 결합된 이미지가 영향을 미쳤다.

1. 화이트칼라범죄

사이버범죄의 개념적 구성은 서더랜드(E. H. Sutherland)가 화이트칼라범죄를 처음으로 인용할 때로 거슬러 올라간다(최인섭·최영신, 1996: 21). 1930년대 후반 서더랜드는 기존의 노상범죄인 절도, 강도, 폭행은 대체로 노동자 계급에 의해 이루어지는데 반해, 화이트칼라범죄는 은행원, 변호사, 회계사 그리고 정부공무원과 같은 전문가들에 의해 이루어짐을 밝혔다. 왜냐하면, 이들 전문가들은 권한이나 신뢰의 남용을 수행할 수 있는 직위에 있고, 상대적으로 정보와 금전에 접근하기가 쉽고, 그들이 근무하고 있는 조직이나 은행에 관련된 법률이나 규정을 잘 이해하고 있기 때문이다. 화이트칼라범죄는 사회적 지위와 직업적 과정의 특성을 가지는 것으로 경영자와 간부직원, 정치가, 공무원 등의 사회지도층 인사들이 그들의 지위와 권한을 이용하여 영리를 추구하는 행위라고 정의된다(Sutherland, 1949: 9).

2. 컴퓨터 범죄의 출현

컴퓨터 형태의 활용은 2차 세계대전에서 미국과 동맹국들이 나치연합세력들의 암호메시지를 가로채서 해독하기 위해서 시작하였다. 1950년 후반에 은행업계에서는 간단한 자금을 이전하고, 계좌 기록을 유지하기 위해 컴퓨터를 활용하기 시작하였다. 처음 컴퓨터부정이 나타난 것은 1958년 미네아폴리스(Minneapolis)은행원에 의해 발생된 살라미기법이었으며, 미국 연방은 1966년 처음으로 은행장부의 조작에 대해 형법위반으로 기소를 하였다. 1960년대에 회사들은 컴퓨터를 활용하여 사회적·환경적·재정적 부정과 결합하는 기회가 확대 되었다. 또한 학생들은 대학에서 컴퓨터 활용법을 수업하면서 해킹과 같은 시스템 파괴기법을 학습하고 이를 수행하였으며 해커의 의미가 생성되었다. 미국에서는 전자동 장거리 전화가 소개되었고 프리커들은 전화장치에 혼선을 주는 방법으로 무료통화를 하는 전자해킹형태가 발생되었

다.[1] 돈 파커(Donn Parker)는 컴퓨터범죄 연구의 선구자로서 1976년 '컴퓨터범죄'라는 책을 출간함으로서 컴퓨터법률의 제정이 미흡한 시기에 컴퓨터 활용의 증대와 이와 관련된 전문 지식의 증대가 컴퓨터부정과 범죄로 이어진다는 점을 밝혔다(Parker, 1976).

3. 인터넷의 등장

인터넷이란 그 이름이 상징하는 바와 같이 컴퓨터 네트워크의 핵심이며, '네트워크의 네트워크'이다(Castells, 2002). 네트워크는 지금껏 기업, 정부, 군대 그리고 대학 등에서 존재하여왔으며, 컴퓨터를 연결해줌으로서 커뮤니케이션과 정보의 교환을 가능하게 해주었다. 인터넷의 전신은 1960년대 미 국방성이 냉전시대에 통신과 협동을 강화할 목적으로 '알파네트'(ARPANET)를 개발한데서 기원을 찾는다.[2] 1970년대 전자우편이 창안됨으로 통신이 더욱 확대되었으며, 알파네트에 이어 영국의 JANET(Joint Academic Network)이 개설되고, 미국에서는 'NSFNET'(미국학술재단 소속)이 등장하였다. 1990년 미국정부는 미국의 학술재단의 감독 아래 '알파네트'를 민간부문에도 공급하도록 조치하였다. 같은 해 스위스의 'CERN'물리학 연구소가 'WWW'(World Wide Web)를 개발한 이후, 1994년 처음으로 상업용 인터넷인 'Netscape'가 등장하였으며, 다음 해인 1995년 마이크로(Microsoft)사가 인터넷 익스플로(Internet Explorer)를 개시하였다.[3] 이와 같은 인터넷 브라우저의 개발은 개인용 컴퓨터(PC) 접속을 가능하게 하였을 뿐만 아니라 인터넷서비스 공급자(Internet Service Providers: ISP)들이 전화선에 연결하여 사업을 함으로서 본격적으로 시장에 참여하였다.

---

1) 해커(hacker), 프리커(phreaker), 크랙커(cracker)는 다음과 같이 구별되기도 한다. 해커는 컴퓨터를 중심으로 하고 프리커는 전화를 중심으로 발전되었지만 양자는 탐험, 정보획득 또는 호기심의 목적으로 불법적으로 타인의 컴퓨터에 침입하는 것으로 인터넷과 웹정보 그리고 정보통신기술을 활용하는 자들이다. 크랙커는 해커 중에서 함부로 시스템에 침투하여 전자정보를 절취하는 자이며, 악의적인 의미가 더 많고, 해커는 다소 선의의 의미가 있다고 주장하기도 한다.

2) 당시 미 국방성은 '알파네트'를 미국 지역의 동부 연구기관인 Lincoln, Harvard, MIT 등과 Carnegie와 Illinois를 거쳐 미국 서부의 Utah, Stanford, UCLA, Rand 등 연구소를 연결하였으며, 동 네트워크의 특징은 컴퓨터의 하드웨어 연결과 함께 프로토콜(규약)도 수립되었다는 점을 들 수 있다.

3) 스위스의 'CERN'이 개발한 'www'는 단순한 정보공유의 기능이었으나 'Netscape'와 'Microsoft'가 등장하면서 본문과 이미지를 공유하는 정교함을 갖추게 되었다.

4. 사이버범죄의 기원

오늘날 사이버범죄는 네트워크 테크놀로지에 의해 이루어지는 범죄로 널리 기술되고 있다. 사이버범죄의 기원은 공상과학소설과 영화에 기원을 두고 있다. 월(D. S. Wall)의 소설과 영화는 범죄가 사이버스페이스와 연결되고 가상환경에서 발생될 수 있음을 보여주었다. '사이버스페이스'라는 용어는 1982년 깁슨(William Gibson)이 '불타는 크롬'이라는 단편소설을 'Omni Magazine'에 게재하고 부터이고, 공상소설과 과학이 교류되는 시기는 1978~1998년 사이이다. 사이버펑크(cyberpunk)[4]를 주제로 하여 사이버스페이스와 가상환경을 배경으로 하는 Bruce Bethke의 단편소설, 깁슨의 'Neuromancer' 그리고 Stephen의 'Snowcrash' 작품에서 더욱 진화하게 되었다. 사이버스페이스와 범죄의 결합은 1980~1990년대 초기까지 사이버펑크 개념으로 등장한 드라마들이었으며, 뒤이어 사이버펑크소설과 희극관련 책들이 등장하였다.

사이버스페이스와 범죄의 융합은 사이버펑크 개념으로 구성된 해커 영화들이며, 아래와 같이 3개세대로 구분된다. 제1세대는 1969년 'Italian Job' 과 1988년 'Die Hard'로 중요기반시스템에 침입하는 해크(hack)를 배경으로 한다. 제2세대는 낭만적인 해커이야기로 대표적인 것이 'War Game'이며, 커뮤니케이션 네트워크를 이용하여 가상공간의 한계에서 해커의 활동을 묘사한 것이다. 그러나 이들은 1995년 'Johnny Mnemonic'과 1996년 'Independence'보다는 약한 도덕성을 보여주었다. 제3세대는 해크와 해커가 함께 등장하게 되고, 1999년의 'The Matrix'가 대표적이다. 이와 같은 사이버범죄 이미지의 연계는 TV영화, TV프로그램, 책 그리고 소설 등에서 재생산되게 된다.

이와 같은 과정을 통해서 사실과 가상이 뭉쳐진 이미지가 사이버범죄의 전형적인 고정관념으로 각인되게 된다. 빅토리아과학의 공상소설인 웰(H. G. Wells)과 동시대 작품들은 기술의 혁신과 이의 전환과정과 함께 또한 신기술의 위험에 직면한 사회변혁의 시대였다. 이들의 전통 유산은 현대의 Brian Aldiss, Aldous Huxley와 다른 작가들에 의해 전수되어지고 있다. 사회과학 공상소설의 대표는 Orwell의 'Nineteen Eighty Four'이며, 오웰은 디스토피아적인 미래사회를 예측하기 위해 사회이론과 사

4) 사이버펑크는 정보통신 기술의 발달과 함께 정보 독점으로 인한 불평등 문제가 제기되면서 이에 저항하는 사람들이 반체제·반문화 운동인 펑크 문화의 전통을 컴퓨터 통신망에서 구현해 독점체제를 깨뜨리고 정보를 공유하기 위한 여러 가지 활동을 전개하면서 생겨난 문화현상을 뜻하는 것으로 컴퓨터와 마약이 지배하는 폭력적이고 도시적인 미래를 그리는 공상과학소설이다.

상을 동원하여 시대적 사건들을 구성하고 있다(Wall, 2008: 46-49). 사이버범죄라는 용어는 1995년 서스맨(Sussman)과 휴스턴(Heuston)이 처음으로 사용하였으며, 1997년 미국의 '정부기간산업의 보호에 관한 대통령 위원회'의 최종보고서에서 공식적으로 인용한 후 일반인에게도 널리 알려지게 되었다(McQuade III, 2006: 15).[5)]

5. 사이버스페이스에서의 경찰활동

사이버스페이스에서 극우파, 신나치파, 백인 우월주의, 인종주의자, 파시스트 그리고 각종 사이버범죄 조직들은 이들 조직의 목표와 임무를 수행하기 위해 인터넷을 활용하고 있다. 1997년 Stern의 조사에 의하면 미국에는 300개의 극우 시스템이 존재하며, LA에만 600개의 증오(hate)사이트가 있다. 이중 35개는 미국 내에 주소를 둔 무장투쟁 단체의 소속이고, 94개는 인종 계층제를 주장하는 집단이며, 87개는 신나치주의, 35개는 백인우월주의, 51개는 테러리즘 지지 세력들의 사이트들이다(Stern, 1998: 224). 또한 상당수의 사이트는 미국의 감시망을 피하기 위하여 해외에 사이트를 개설해 운영하고 있으며, 이들 사이트로는 PatriotNet, LibertyNet, PaulRever 등이 있다(Stern, 1998: 226).

인터넷을 활용한 이들의 위협은 아래와 같은 이유를 내포하고 있으므로, 사이버 경찰활동에 대해서 중요한 의미를 가지고 있다. 첫째, 종전에는 전혀 가능하지 않았던 것들이 인터넷을 활용함으로서 쉽게 그리고 신속하게 상호접속이 허용된다는 점이다. 둘째, 인터넷은 은밀한 커뮤니케이션과 익명성을 보장한다는 점이다. 셋째, 인터넷의 활용은 비용이 저렴하다는 점이다. 넷째, 인터넷은 극우단체들에게 힘을 향상시켜 주고 있다는 점이다. 다섯째, 극우단체들은 기성조직이 그들을 부정하더라도 인터넷을 통하여 새로운 회원을 모집할 수 있기 때문에 젊은층과 지식층을 포섭할 수 있게 된다.

이제는 사이버스페이스가 극우단체나 범죄조직에게 위험한 장이 되고 있음을 깨닫게 됨으로서, 사이버스페이스에서 보다 효과적인 경찰활동이 요구되고 있다. 경찰

5) 사이버(cyber)는 그리스어의 'kyper'(배의 조타장치를 뜻함)에서 유래된 것으로, 1984년 William Gibson이 'Neuromancer'라는 공상과학소설에서 눈으로 볼 수는 없지만 틀림없이 존재하는 영역으로 지구상의 수많은 사람들이 컴퓨터를 통해서 교신하는 또 다른 공간으로 사이버스페이스(cyberspace)라는 용어를 사용하였다(Gibson, 1984: 68). 우리나라에서는 1999년 경찰청에서 '사이버범죄수사대'를 창설함으로서 공식적으로 사이버범죄라는 용어를 사용 하였다.

활동과 관련하여서는, EU가 경찰을 포함한 사법기관이 인터넷 텔레커뮤니케이션과 관계된 범죄인 경우에는 상호 협력하도록 하였고, 1997년 유럽위원회와 'Europol'은 유럽 내 경찰은 인터넷상 불법 콘텐트를 검색하도록 하고, 국경이 중복된 경우에는 정보 교환과 함께 관련 국내법의 조율과 수사에 협조하도록 조치하고 있다(Thomas and Loader, 2003, 234-250).

영국은 2007년 상반기 악성코드에 의한 신종범죄의 협박 건은 212,101건으로 2006년 동 기간 대비 185% 증가 했다. 그러나 영국 정부가 1990년부터 「컴퓨터 오남용법」을 제정한 이후, 15년 동안 이 법에 의해 기소된 범죄는 200건에 불과 하였다. 이러한 현상은 다른 지역과 국가에도 비슷한 상황이다(Wall, 2008: 47-48). 사이버범죄의 현상이 실제 범죄발생률 보다 이 처럼 낮게 나타나는 원인으로는 익명성과 프라이버시 등의 이유로 인한 암수범죄, 범죄피해자의 낮은 피해 인식과 피해에 대한 보고의 기피, 사이버범죄자의 전형적인 특징인 자동성·간접성과 국경을 초월한 사법권의 필요 그리고 경찰의 인식 결여 등으로 볼 수 있다. 사이버범죄자의 일반적인 특징으로는 젊고, 창의력이 있고, 상당히 외톨이 성격을 가진 중산층으로 범죄 경력이 없는 자들로 전문적 지식을 가지고, 금전적 또는 기타 다양한 동기를 가진 사람들이다(Wall, 2000).

경제의 세계화와 다국적기업의 확대는 이윤을 창출하는 국제적 시장에서 기회의 확대를 의미함과 동시에 이를 파괴하는 범죄활동이 또한 증가하고, 산업스파이 문제를 야기한다. 또한 전자 상거래와 지적 재산권에서 위조와 변조 행위가 발생하며, 웹사이트와 전자네트워크에 대한 검열의 부재는 반란자와 극단주의자들에게는 매력적인 표적이 되고 있다. 조직범죄는 더욱 정교한 기술을 활용함으로서 마약매매, 자금세탁, 불법무기거래, 밀수 등을 행하고 있다. 개인 해커들 또한 금융, 무역 등에서 교묘히 침투하고 있으며, 데이터의 절도, 바이러스 심기와 트로이목마를 활용하고 있다. 사이버범죄에서 무선범죄가 증대되는 것은 디지털 기술의 증대를 말한다. 예를 들면, 무선전화기를 사용하여 은행 강도가 경찰의 송수신 내용을 가로채고, 휴대폰을 활용하여 경찰망을 빠져나가는 경우가 이에 해당한다. 가상공간에서 다중과 다중의 연결이점은 전 세계적으로 대량의 정보와 지식을 무제한적으로 살포함으로서 잠재적 위험은 물론이고 폭력을 야기할 수 있게 되었다. 사이버범죄의 초기 위협은 국내는 물론이고 국제적으로도 경제, 안보, 사회와 정치관계에 도전이 되고, 형사사법기관에도 중대한 도전이 되고 있다. 또한 통신 메시지의 코스를 변경하기 위하여 고안된 신축

성 있는 통신체제 자체가 정부통제를 더욱 어렵게 하고 있다(Loader, 1997).

아울러 정보통신 기술의 발전은 정보전, 테러리즘 그리고 범죄활동간 구별을 어렵게 하고 있다. 비정부조직과 국제적인 범죄조직의 인포메이션 테크놀로지의 활용 증대는 경찰활동의 기능 수행에 있어서도 중요한 영향을 미치고 있다. 또한 개인의 정보보호와 프라이버시보호를 위해, 허가되지 않는 디지털자료의 획득(예, CCTV) 등은 개인의 자유에 대한 간섭이란 점에서 논쟁이 되고 있다. 결국, 개인의 자유와 효과적인 법집행에서 균형이 요구된다는 점은 가상공간에서 초 국경의 경찰활동은 보호육성 되어야 함에도 불구하고, 동시에 이의 균형이 요구되고 있다는 점에서 범죄학뿐 만 아니라 경찰정책 수립에도 근본적인 문제점이 되고 있다(Davies, 1996). 이밖에도 아동포르노그래피 문제 그리고 메일폭탄, 패스워드 가로채기, 스푸핑(spoofing) 등의 수법들이 등장하고 있다. 사이버범죄에서 범죄자는 해커와 프리커, 정보장사꾼, 테러리스트, 극단주의자 그리고 불법행위자들이다.

사이버스페이스가 탄생된다는 것은 현실세계의 한계가 되었던 시·공의 제약요소들을 초월하고, 폭파하고, 압축하고 그리고 붕괴시킴을 의미한다. 그러나 사이버 범죄자들의 특성을 조명할 때는 지역적 범죄와 같은 것으로 취급함으로서 사이버범죄가 질적으로 전통적 범죄와 다른 점을 간과하기 쉽게 된다. 사이버범죄가 시·공을 초월한 '지구촌화'로 야기되는 사회학적 접근을 할 때의 논리적 근거는 가상공간의 등장으로 인하여 아무리 멀리 떨어져 있는 사람들이라 할지라도 새로운 만남과 교환이 가능하게 됨을 의미한다(Shields, 1996). 범죄학의 입장에서 보면, 이와 같은 환경의 변화는 곧 물리적 거리의 장벽이 제거됨으로서 우리들이 잠재적 약탈자로부터 취약하게 됨과 동시에 잠재적 약탈자는 위장을 통한 익명성을 유지함으로서 강력한 범죄 도구를 갖게 됨을 말한다(Sydner, 2001: 252).

Ⅲ. 사이버범죄의 진화

1. 우리나라의 사이버범죄 현황

<표 1>은 2004년부터 2008년까지 5년간 발생한 우리나라 사이버범죄현황을 나타낸 것이다. 2008년 우리나라 사이버범죄 발생은 136,819건으로 전년 동기 대비 54%나

증대되었으며, 2004년 대비 77% 증가하였다. 또한 2008년 우리나라 사이버범죄건수는 2008년 전체범죄 발생건수 2,063,737의 6.6%에 해당된다(경찰청, 2009: 89, 97). 사이버테러형범죄인 해킹과 바이러스는 전년 동기간 대비 13.6% 증가하였으며, 일반사이버범죄로는 불법복제, 판매 및 인터넷사기 등이 증가한 것으로 나타나고 있다.

〈표 1〉 사이버범죄의 발생 및 검거현황(2004-2008)

(단위: 건)

연도 \ 유형		총계	사이버테러형범죄			일반사이버범죄						
			소계	해킹	바이러스	소계	통신사기 게임사기	명예훼손 성폭력 등	개인정보 침해	불법 사이트 운영	불법 복제 판매	기타
발생	2008년	136,819	20,077	19,950	127	116,742	36,591	9,543	5,769	7,723	33,537	23,579
	2007년	88,847	17,671	17593	78	71,176	31685	10,028	4,214	5,229	8,866	11,154
	2006년	82,186	20,186	20,119	67	62,000	33,041	7,881	2,839	6,798	2,313	9,128
	2005년	88,731	21,389	21,336	53	67,342	42,675	6,642	3,759	1,836	1,257	11,173
	2004년	77,099	15,390	15,348	42	61,709	40,283	3,667	3,137	2,308	1,604	11,250
검거	2008년	122,227	16,953	16,854	99	105,274	29,290	8,690	5,129	8,056	32,084	22,025
	2007년	78,890	14,037	13,988	49	64,853	28,081	9,164	3,741	5,505	8,167	10,195
	2006년	70,545	15,979	15,934	45	54,566	26,711	7,109	2,327	7,322	2,284	8,813
	2005년	72,421	15,874	15,831	43	56,547	33,112	6,338	2,889	1,850	1,233	11,125
	2004년	63,384	10,993	10,955	38	52,391	30,288	3,751	2,065	2,410	1,244	12,633

출처: 경찰청, 2009: 97.

2. 테크놀로지의 진화에 따른 사이버범죄의 발전

홀링거(Richard Hollinger)는 현대적인 컴퓨터 해커에 수반되는 사회적 가치와 낙인을 고속도로와 열차 강도의 낙인과 비교하여 설명한다. 이들 두 집단이 처음에는 민중적 영웅으로 묘사되지만, 마침내 사회는 그들에게 낙인을 가함으로서 악마화하고 그들의 체포에 보상금을 거는 것으로 발전한다고 한다(Hollinger, 1991: 6-17). 범죄에 대한 용어의 낙인은 이처럼 기술발전과 함께 진화하는 것이며, 이로서 신종범죄의 탄생이 가능하게 된다. 사이버범죄는 컴퓨터와 인터넷, 네트워크 그리고 디지털의 발전과 밀접하게 관련되어 진화되어 왔기 때문에 테크놀로지에 대한 이해와 대응이 중요하다.

1) 컴퓨터범죄

컴퓨터범죄는 범행이 반복되고 영속성을 가짐으로서 범죄의 발견과 입증이 곤란하다는 특징을 가지고 있다. 컴퓨터범죄의 개념과 관련하여 이를 부정하는 견해도 있으나 컴퓨터범죄는 범죄의 행위자나 행위 그 자체가 종래의 전통적 범죄와는 유형을 달리하므로 컴퓨터범죄를 인정하는 것이 일반적이다(이윤호, 1993: 96). 우리나라에서는 1973년 서울 반포 AID차관 아파트의 입주권자 추첨에서 프로그래머에게 뇌물을 주고 특정인이 당첨되도록 한 것이 첫 사례이다(김경태, 1997: 118-120).

컴퓨터범죄의 분류 방식으로 가장 전통적인 것은 1984년 리차드 홀링거(Richard Hollinger)가 분류한 네 가지 방식이다. 첫째, 컴퓨터가 범죄의 목적이나 대상이 되는 경우로 고객리스트와 가격데이터가 이에 해당한다. 둘째, 컴퓨터가 범죄의 수단이 되는 경우로 현금입출금기 카드와 계정에 대한 사기와 증권거래 사기 등이 있다. 셋째, 컴퓨터가 다른 범죄에 부수적인 경우로 돈세탁, 불법금융거래, 조직범죄장부의 기록과 전자게시판 등을 들 수 있다. 넷째, 컴퓨터의 보급과 관련된 범죄로 소프트웨어의 해적행위와 위작, 컴퓨터프로그램의 저작권 침해와 장치위조 그리고 기술적인 설비의 절취 등이 이에 속한다(Carter, 1995: 21-27).

컴퓨터관련 범죄의 개념은 컴퓨터와 장거리통신 기술의 급격한 발전을 고려한 개념이고, 컴퓨터와 관련된 범죄를 수사하고 기소하는 것과 관련하여 수많은 기술과 법률의 변화를 포괄하고 사회적 함축성을 확대하기 위한 것이었다. 그러나 컴퓨터범죄의 개념 사용 후 IT의 급속한 발전으로 사이버범죄 등의 하이테크 범죄 개념이 더욱 자주 사용됨으로서 컴퓨터범죄 개념의 사용은 상대적으로 줄어들게 되었다.

2) 사이버범죄

① 해킹과 바이러스

사이버범죄는 익명성, 개방성, 비대면성, 자동성 등의 특성을 무기로 하여 한층 발전하게 되고 이의 대표적인 사례가 해킹과 바이러스라 할 수 있다. 해킹은 1980년대 패스워드 추측과 같은 단순한 형태의 공격에서 벗어나 버퍼 오버플로우, 스니핑, 세션 하이재킹, 사용자의 ID나 비밀번호를 빼내는 스누핑(snoofing), 타인의 전산운영권을 속임수로 장악하는 스푸핑(spoofing), 스팸메일, 한 사이트에 동시에 접속시켜 트래픽량을 대량으로 증대시킴으로서 사이트를 마비시키는 일명, 분산서비스 거부

공격(DDoS)[6], 고출력전자총, 스캔공격, 백오리피스, 논리폭탄 등 많은 수법이 있고, 타인의 개인정보를 불법으로 획득하는 피싱(phishing)[7] 등이 있다.[8] 또한 금융네트워크 공격과 대규모 개인정보 침해사례 등이 나타나고 있다.[9] 한편 해킹은 정치적 성격을 띠는 핵티비즘의 사이버테러를 포함하여 군사, 외교, 정부중요문서 그리고 산업계에서 산업스파이로 이용되고 있어 총성 없는 전쟁이 되고 있다.

최근 미국 국방부는 사이버테러와 사이버전쟁에 대처하기 위해 '사이버사령부'를 설치해 적극적으로 사이버전쟁에 대응한다고 밝히고 있고, 우리나라의 국방부도 사이버사령부 설치를 공표하였다(「중앙일보」, 2009.6.25: 14). 한편, 바이러스는 자기 스스로 다른 파일 및 메모리에 복제하여 자기 자신 또는 자기 자신의 변형을 감염시켜 파괴 및 은폐기능을 하는 것으로 전통적으로 예루살렘, 러브바이러스 등의 많은 바이러스가 존재하며, 겉과 속이 다른 동작을 하는 트로이목마(Trojan Horse), 시스템 과부하를 목적으로 하는 인터넷웜, 무료 프로그램에 탑재되어 정보를 유출시키는 스파이웨어, 사용자를 놀라게 하거나 속이는 '조크와 혹스' 그리고 스크립트의 실행과 함께 컴퓨터내의 정보를 손상시키는 악성스크립트 등으로 진화하였다. 또한 앞으로 신종 플루보다 더 위험한 것은 '디지털바이러스'라고 경고하고 있다. 사실 머지않은 장래에 '생물학적 바이러스'와 '디지털바이러스'가 결합된 새로운 형태의 바이러스가

6) 디도스는 2000년 이후 급속히 발전한 공격기법으로 전체네트워크를 마비시키는 경우보다는 특정한 목표를 정해서 공격하는 경우에 많이 사용된다. 국내에서의 디도스공격은 2009년 7월 7일부터 10일까지 좀비PC를 통해 악의적으로 유포된 악성코드가 주요 정부기관, 은행사이트 등을 공격하면서 사회적으로 큰 파장을 일으켰으며 그 배후에 북한이 개입된 것으로 드러나기도 하였다. 이와 같은 '7·7대란' 이후에는 중소기업에게까지 금품을 요구하고 거부 땐 수 억 원대의 피해를 입히는 사례의 디도스공격이 속출하고 있다.

7) 피싱의 한 형태인 보이스피싱은 갈수록 지능화되고 기업형 범죄로 나타나고 있다. 범죄자들은 피해자를 '콜센타'로 유인하도록 하고, '통장모집책', '인출책', '자금관리책', '연락책'을 두고 수십명 내지 수백명으로 조직적으로 운영되고 그 수법도 다양해지고 있으며, 그 대표적인 사례로는 ① 환급형, ② 수사빙자형, ③ 납치형, ④ 카드반송형, ⑤ 분실습득형 등으로 분류되고 있다(「중앙일보」, 2009, 4, 24: 29).

8) 안철수연구소에 의하면 해킹추세도 크게 발전되었다. 과거에는 네트워크나 웹사이트를 공격하던 것이 최근에는 메신저, UCC, 블로그를 직접 공격하는 추세로 바뀌고 있다. 개인이나 관리자 PC를 공격하는 악성코드도 급증했다. 신종웜은 작년 상반기 277개에서 올 상반기 423개로 52% 늘었고 신종트로이목마는 956개에서 2293개로 140%, 신종 드롭퍼(파일에 바이러스나 트로이목마를 숨겨놓는 악성코드)는 202개에서 438개로 116% 증가했다. 사용자가 메신저의 메시지를 무심코 내려받게 하는 '좀비PC'도 두드러지게 나타나고 있다(「한국경제신문」, 2007, 7, 12),

9) 미국 국토안보부 산하 컴퓨터침해사고대응센터(US-CERT)에 따르면, SI(Swine Influenza)등장과 관련하여 e-메일로 '첫 SI희생자' 또는 '미국의 SI통계'라는 제목을 부쳐 사람들의 관심을 끈 후 이메일을 열어보는 순간 악성코드에 감염시켜 개인정보를 빼내가는 수법이 등장하였다(「중앙일보」, 2009. 6. 19: 14).

출현할 가능성도 대두되고 있다.

② 일반사이버범죄

일반사이버범죄행위는 실로 다양하다. 소프트웨어 해적행위, 불법 파일의 공유, 웹사이트 파괴, 사이버스토킹, 이메일 스팸, 컴퓨터 엿보기, 전자기기를 이용한 금품 강탈 등과 가상공간을 무대로 한 사기, 명예훼손, 성폭력 등이 등장하고 있다. 또한 포탈사이트의 검색순위 조작, 온라인광고 클릭수 조작, 유해정보가 범람하는 UCC, 미니 홈피나 블로그에 음란물 등의 불법적인 정보 유포 등의 행위가 나타나고 있다(정완, 2007: 17-25). 사기행위로는 허위 쇼핑몰 개설, 대포폰과 대포통장을 이용한 사기 그리고 온라인 게임아이템 사기 등이 주류를 이루고 있다. 또한 자살과 청부살인 사이트, 원조교제와 성매매, 불법오락과 도박 그리고 자금세탁 등이 행해지고 있어 현실세계에서 일어나는 모든 범죄가 온라인상에서 일어나고 발전되어 가는 추세이다.

3) 인터넷범죄

1990년대 중반에 인터넷의 상업화는 인터넷 성장을 획기적으로 가져 왔다. 1994년과 1999년 인터넷에 연결된 국가는 83개 국가에서 226개 국가로 증대되었으며(Furnell, 2002: 7), 1995년 12월 통계에 의하면 인터넷 사용자는 세계적으로 16백만 명이었고, 2002년 5월에는 전 세계 인구의 10%인 5억 8천만 명이 될 것으로 예측되었다. 또한 2005년에 10억 명과 2010년에 20억 명이 인터넷 사용자가 될 것으로 예측되었다(Castells, 2002: 3).[10] 그러나 인터넷 확대와 보급은 지역과 국가 간에 큰 차이를 보이고 있다. 예를 들면, 2002년의 경우 미국은 주민 100명 가운데 65.89대의 PC 보급율을 보이고, 영국은 40.57대 그리고 아프리카의 경우 1.3대의 보급률을 나타냈다. 인터넷사용자의 95%가 미국, 캐나다, 유럽, 호주 그리고 일본 지역에 편중되고 있다. 결과적으로 인터넷보급의 불균형은 고용, 수입, 교육, 인종 그리고 능력에 있어서 차이를 보이는 양상을 나타내고 있는데, 이러한 불균형은 범죄학의 견지에서 분

10) 한국인터넷진흥원(www.krnic.or.kr)에 의하면 2005년 전 세계 인터넷 이용자 수는 8억 7,269만 2,100명이며, 국내인터넷이용자수는 3,257만 명이다. 또한 IDC(Internet Data Center)조사에 의하면, 세계 인터넷 사용자 인구는 전체 세계인구의 1/4 수준이며, 이 수치는 2012년 19억 명을 넘어 세계인구 수준의 1/3에 도달할 것으로 예상된다고 한다. 중국은 이미 미국을 추월하여 2008년 2억7천만 명이며 2012년에는 3억7천만 명이 될 것으로 예상된다(http://markidea.net/entry/internet-population/2010.1.15.).

석해 볼 때에 잠재적 가해자와 잠재적 피해자가 될 가능성이 높기 때문에 중요한 의미를 가진다(Castells, 2002: 208-23).

인터넷의 등장은 우리 인류에게 혁명적 변화와 함께, 정보의 실시간 교류와 지식의 전달, 상거래의 활성화와 전자정부의 가속화 등 우리생활에서 많은 순기능을 가져다주었다. 그러나 이에 따른 역기능으로 학생과 주부 그리고 일반 시민에게까지 인터넷 중독증이라는 새로운 증후군이 발생되고, 인터넷게시판과 대화방, 성인방송, 광고 등에서 일탈이 성행되고 있으며, 인터넷 쇼핑몰 사기 또한 늘어나고 있다. 최근에는 취업난과 핵가족시대의 등장으로 인터넷을 통해서만 사회와 소통하는 '은둔형 외톨이'가 사회문제화되고 있다. 인터넷범죄는 인터넷과 연관된 범죄 개념이며, 사이버범죄의 일환이 된다.

4) 디지털범죄

일반적으로 디지털이란 정보(Data)를 통상 컴퓨터가 이해할 수 있는 '0'과 '1'의 두 숫자로 표현하는 것을 말하며 아날로그와 반대의 개념이다. 이러한 디지털의 특성은 식별이 불가하고, 변경이 용이하고, 유무선의 네트워크로 전송된다는 점이다(경찰대학, 2006: 39-41). 디지털과 관련된 네트워크 테크놀로지로는 개별PC를 연결해 주는 'ARCNET', 지역별로 묶어주는 'ETHERNET', 데이터 전송을 위한 광섬유연결의 'FDDI'(Fiber Distributed Data Interface), 비 동시 연결형의 'ATM'(Asynchronous Transfer Mode), Laptop과 PDA와 같은 무선접속(Wireless), 이동전화의 'Cellular' 그리고 위성중계의 'Satellite'가 있다(Casey, 2004: 365-370). 오늘날 디지털 전자적 장비로는 desktop, laptop, mini computers, cell phones, fax machine, digital camera, PDA, voice recorder, scanner 등이 이용된다. 우리들이 흔히 소프트웨어라고 칭하는 플로피디스크, 신용카드, 학생증, 호텔의 룸 키, 사무실건물의 출입증, 공중전화용카드, 지하철승차용카드 등은 플라스틱 카드 상에 마그네틱테이프나 마이크로 칩이 부착되어 판독이 가능한 것들로 모두 디지털기술과 관련된 것이다.[11]

11) 지갑속의 교통카드는 현대인의 움직임을 파악하고 있고, 지갑속의 신용카드는 어디서 누구하고 식사하고 술을 마셨는지를 알고, 휴대전화의 이용은 자신의 위치를 좌표로 표시하고, 곳곳에 설치된 CCTV는 현대인의 움직임을 알려주고 있다. 또한 멀지 않은 장래에 '인체 블랙박스' 시대가 온다고 한다. 다른 말로 하면, '라이프로그'(lifelog) 시대라고 하는데 이것은 특정인의 하루 일상사를 실시간으로 기록하는 것으로 오디오·비디오·위치·생체 등 여러 형태의 데이터로 기록하고 유지하는 것을 말한다(「중앙일보」, 2009.6.25: E1).

디지털 특성의 신용카드가 우리나라에 도입되어 우리가 '신용사회'로 진입한 것은 1980년 초이다. 신용카드가 생활필수품이 되어 우리들의 일상생활이 획기적으로 편리하게 되었으나, 그 역기능으로는 분실과 도난, 카드의 부정사용, 매출전표의 위변조, 유령가맹점의 카드 현금대출 그리고 위조카드 등의 폐해가 나타나고 있으며, 최근에는 카드판독기 출현과 컴퓨터 프로그램의 활용으로 그 폐해 또한 심화되는 현상을 보이고 있다(최응렬, 1997: 452-454).

디지털증거자료는 명예훼손, 혼인빙자간음, 살인 등 일반범죄는 물론이고 기업범죄, 금융범죄, 각종선거사범, 해킹 등 사이버범죄 수사 모두에 중요한 자료가 되고 있다(유영현·송봉규·박상진, 2009: 257). 디지털은 이와 같이 우리 일상생활에서 필수요소로 등장하여 활용되지만 디지털의 증거는 환경 등 외부적 요인이나 사람에 의해 쉽게 변질되는 특성을 가짐으로서 디지털의 증거 수집과 분석력의 향상은 유전자 감식과 프로파일링 등 과학수사력의 향상과 직결되고 있다. 오늘날 '인터넷시대'의 용어보다 '디지털시대'의 용어가 새롭게 등장되고 있는 것은 첨단 디지털 기술의 활용과 관련된 것이다. 결국 디지털범죄는 디지털기술과 관련된 것으로 컴퓨터와 네트워크 그리고 인터넷을 활용한 범죄이다(Taylor et al., 2006: xiv).

Ⅳ. 사이버범죄의 이해와 대응

1. 사이버범죄의 이해

1) 용어의 범람

사이버범죄는 일반적으로 컴퓨터범죄와 인터넷범죄로 정의되기도 하지만, 하이테크범죄, 정보범죄, 네트워크범죄, 디지털범죄와 밀접한 관련성을 갖고 있다. 이와 같은 용어의 범람은 사이버범죄의 한 단면을 크게 부각시켜서 집중 조망한 것으로 어느 것도 전체를 조망시켜 주지는 않는다. 이러한 혼란은 학자와 정부조직에서도 혼선을 보이고 있다. 파커(Parker)는 1970년대에는 '컴퓨터부정'의 용어를, 1983년에는 '컴퓨터범죄'를 그리고 1998년 이후에는 '사이버범죄'를 사용하고 있다. 또한, 미국의 전 연방 검찰총장이던 Janet Reno는 처음에는 '신시대범죄'라는 용어를 사용하였으나 1년 뒤에는 '첨단범죄'로 변경 사용하였다. 또한 2004년 법무부 소속의 '국가사법연

구원'(NIJ)과 '청소년 비행과 사법행정청'(QJJDP)은 그들의 연구보고서에서 '전자범죄' 와 '인터넷범죄'라는 용어를 각각 사용하고 있다(McQuade, III, 2006: 19). 사이버범죄의 용어 혼용은 실무형사사법기관과 각국의 사용현황에서도 알 수 있다. 우리나라의 경우 경찰은 사이버범죄의 용어를 사용하고 검찰은 첨단범죄의 개념을 사용하고 있다. 인터폴은 전통적으로는 첨단범죄로 규정하고 있으나 실무적으로는 사이버범죄라는 용어를 일상적으로 사용하고 있다. 미국은 1998년 국가기반구조의 보호를 위해 '국가기반구조보호센터'(NIPC)를 설립하였으나 2001년 9.11테러 이후 국토안보부로 이관되고 별도로 사이버부가 설립되었다. 그러나 영국은 첨단범죄라는 개념을 사용하고 있고, 일본은 첨단범죄와 사이버범죄의 양 개념을 사용하고 있다.

2) 사이버범죄 개념의 조명

사이버범죄는 시·공의 장벽을 제거함으로서 다중과 다중의 연결, 온라인 정체성의 변경 그리고 익명성·자동성·개방성·간접성의 특징을 보이는 새로운 범죄 형태를 잉태함으로서 전통적 범죄의 특징인 지리적 경계를 허무는 특징을 보이고 있다. 사이버범죄에 대한 일치된 개념규정은 어렵다. 사이버범죄를 부정하는 측은 새로운 병에 옛날의 포도주를 삽입하는 격으로 낡은 형태의 범죄라고 일축하기도 하나(Grabosky, 2001: 243-9) 대다수 학자들은 사이버범죄를 인정하고 있다. 사이버범죄의 정의와 관련하여 조병인은 "신조어로 학교, 가정, 지하철범죄와 같이 범죄가 행해지는 장소를 부각시킬 목적으로 가상의 사이버공간을 장소화하여 호칭하는 것"(조병인, 2000: 20), 허경미는 "컴퓨터와 관련된 범죄의 또 다른 명칭으로서 컴퓨터범죄와 사이버테러를 포함한 개념"(허경미, 2009: 456), 이윤호는 "사이버공간을 범행의 수단, 표적, 그리고 장소로 삼는 범죄행위"(이윤호, 2007: 178-179), 사법연수원은 "정보통신망을 그 배경, 수단, 대상으로 하는 범죄들로서 컴퓨터범죄의 한 유형임과 동시에 전통적 범죄의 정보통신망이라는 배경 아래에서의 특수한 발생 형태를 포함하는 개념"(사법연수원, 2007: 23-24)이라고 한다. 또한 Thomas와 Loader는 "사이버범죄는 세계적인 전자네트워크를 통한 불법적인 행위로 컴퓨터가 중재된 행위이며, 인터넷과 웹에 기반을 둔 정보 및 통신 테크놀로지의 다양성에서 파생된 것"(Thomas and Loader, 2003: 1-3)이라고 하고, 월(Wall)은 사이버범죄를 첫째, 해킹, 바이러스, 명예훼손과 같은 사이버침해, 둘째, 크레디트카드, 해적행위, 지적재산권의 침범과 관련된 사이버사기와 절도, 셋째, 사이버포르노그래피, 넷째, 사이버폭력으로 구분하고

있고(Wall, 2001: 3-7), 야(Yar)는 월(Wall)의 네 가지 분류에 추가하여 국가에 관한 범죄들인 테러리즘, 산업기밀누설 그리고 국가기밀의 누설에 관련된 것을 포함하고 있다(Yar, 2006: 9-11). McQuade는 "불법적 행위를 조장할 목적으로 조직적인 네트워크 또는 인터넷과 같은 정보시스템을 활용하여 컴퓨터 또는 전자적 인포메이션 테크놀로지 장비를 활용하는 것"(McQuade, III, 2006: 16)이라고 정의한다.[12]

사이버범죄의 개념은 최초에 컴퓨터범죄의 개념에서 출발하여 인터넷범죄, 하이테크범죄, 디지털범죄 등으로 호칭되고 있으며 학술상으로는 컴퓨터범죄와 사이버범죄 개념이 수립된 상태이다. 사이버범죄는 단일현상이 아니라 정보네트워크와 통신테크놀로지에 의해 수행되는 것으로 가상공간이 주축이 되어 야기되는 것으로 컴퓨터범죄를 시작으로 하여 인터넷범죄와 네트워크범죄를 거치고 최근에 디지털 기술과 결합함으로서 진화되고 있다. 사이버범죄가 불법적 목적으로 데이터를 활용하고, 접근하고, 통제하고, 그리고 조작하기 위하여 전자적 장치를 사용한다는 것은 디지털속성이 증대되는 것을 의미하며, 영상화면이 통합된 기능을 갖추고, 전선으로 네트워크되고, 동시영상화면이나 전선 없는 연결이 증대됨을 의미한다. 따라서 사이버범죄는 컴퓨터, 인터넷, 조직적인 네트워크 그리고 디지털기술과 같은 전자적 장비를 활용하여 인포메이션 테크놀로지를 이용하여 불법적 행위를 용이하게 하는 것이 된다.

2. 정책적 대응

사이버범죄 활동의 번성은 형사사법과 범죄통제에 대해서 새로운 도전이자 범죄학의 교육훈련에 대한 도전이기도 하다.

12) Wikipedia정의에 의하면 Information Technology(IT)는 인포메이션시스템의 설계, 수행, 연구 등과 관련된 종합적인 의미로 초기에는 컴퓨터의 하드웨어와 소프트웨어의 적용과 관련된 것이었으나 오늘날 IT는 전산과 테크놀로지 모두를 포함하는 개념이 되었다. 따라서 정보기술은 개인이나 단체, 그리고 국가의 정보화를 위한 모든 이론·방법론·시스템 등을 총망라한 용어로 숫자·문자·도형·사진·음성·비디오 정보 등 다양한 유형을 가진 방대한 규모의 정보를 체계적으로 분류하는 것이다.

1) 경찰활동과 형사사법에 대한 도전

① 전통적 경찰활동 기능의 한계 극복

역사적으로 경찰활동은 영토 내에서 정치적·경제적·사회적 생활과 관련된 조직이었으나 사이버범죄는 지리적 개념을 벗어나 국제적 성격을 띰으로서 다른 나라와 다른 대륙에서 가해자, 피해자 그리고 범죄의 표적이 발견되는 복합성을 띄고 있으므로 초 국경의 경찰활동이 요구되고 있다. 다시 말하면 이것은 네트워크 기술에 따른 '디지털실체주의'가 이루어져야 함을 말하는 것으로, 테크놀로지 발전에 따라 사이버범죄가 증대된 만큼 사이버경찰활동의 역량이 이에 비례할 만큼은 제고되어야 한다는 것이다. 미디어의 보도와 피해자들의 인식과는 달리 사법기관의 처리건수가 적은 이유의 하나는 피해자의 기대와 경찰의 실제 수사와의 차이에 기인하고 이러한 갭은 안이한 전통적 경찰역할의 인식에 안주한 것이 하나의 원인이다(Wall, 2008: 57). 우리나라는 IT강국이고 사이버경찰의 역량도 세계적 수준으로 평가받고 있으므로, 이와 같은 장점을 활용하여 '사이버범죄정보시스템'의 구축이 필요하고, 사이버범죄의 성장에 상응한 관리를 위해서는 현재의 '사이버테러대응센터'의 조직을 본부급으로 확대가 필요하다. 또한 경찰의 각종 교육훈련에서 최근의 해킹 수법 등 범죄사례에 대한 대응능력 제고가 요망된다.

② 자원과 전문가 부족

2001년 영국은 '하이테크범죄분석기구'를 구성하였으나 전담직원은 80명이며, 예산은 2,500만 파운드로 담당 경찰관은 전체 경찰관의 0.1% 미만이었고 예산은 전체 경찰예산의 0.5% 미만이었다. 이와 같은 현상은 'EU 하이테크범죄기관'(ENISA)도 마찬가지였다(Home Office, 2002). 우리나라의 경우도 조직과 인원의 규모를 감안하면 아직은 미흡한 실정이다. 우리나라 경찰은 경찰청의 사이버테러대응센터, 전국지방경찰청 사이버범죄수사대, 경철서 단위의 사이버범죄수사팀을 포함하여 이에 종사하는 경찰관은 924명이 근무하고 있다(경찰청, 2009: 148). 따라서 우리나라 경찰도 사이버범죄를 위한 전담요원은 전 경찰력의 1% 미만임을 알 수 있다. 우리나라 경찰은 전문인력 확보를 위해 IT전문가를 경찰관 및 연구직으로 채용하여 오고 있으며, 2009년 현재 총 203명이 근무하고 있다. 그러나 IT전문가뿐만 아니라 오늘날 사이버범죄는 국내외 금융전문가 등의 전문지식을 요구함으로서 기타 전문가 충원의 확대가 요구되고 있다.

2) 범죄학에 대한 도전

범죄학의 주요 목적은 불법행위의 원인을 탐구하는 것이며 이를 위해 많은 이론들이 개발되어 왔다. 어떤 사람들은 사회의 규정을 준수하는데 반하여 어떤 사람들은 준수를 싫어하는데 그 원천은 어디에 있는가를 밝히는 것이다. 이와 같은 설명을 위해서는 현실세계에서 발생되는 범죄기록을 근거로 분석하게 된다. 문제는 현실세계에서 수립된 이론이 가상세계에서도 적용가능한가의 문제와 어느 정도가 적용가능한가의 문제이다. 사이버범죄와 관련하여서는 아래 문제가 대두된다.

① 범죄 행위지의 문제

전통적인 범죄는 묵시적으로나 명시적으로나 생태적인 가정을 안고 있다. 범죄가 특정 지역에서 발생한다는 점은 사회적·문화적·물리적 특성과 함께 정의된다는 점을 말해준다. 이의 대표적인 이론이 '일상활동이론'으로 잠재적 범죄자는 시간과 공간을 통하여 범행을 수행할 수 있는 조건을 조성함으로서 잠재적 표적을 모색한다는 이론이다. 이와 같은 이론을 토대로 하여 범죄지도의 작성, 범죄예방과 대책 프로그램 그리고 환경설계를 통한 범죄예방방안 등이 수립되고 있다. 현실세계에서는 이웃과 지역, 도시와 교외지역, 도시와 시골 등등의 구분이 가능하나, 가상공간에서 발생되는 조직범죄, 각종 극우파, 산업스파이, 전자상거래의 교란, 해킹, 해적행위, 아동포르노그래피, 테러리즘 등등은 기본적으로 지역적 개념이 없다는 점이다. 사이버범죄에서 범죄발생지를 특정할 수 없다는 점은 지리적 특성을 가진 전통적 범죄이론이 제한적일 수밖에 없다는 점이 된다.

② 범죄자의 문제

범죄이론은 어떤 사람은 범죄를 행하지 않는데 왜 어떤 사람은 범죄를 행하느냐에 관심을 가져 왔다. 범죄통계는 범죄가 장소적인 것과 관련될 뿐 아니라 사회적·문화적·경제적·교육적 배경과 관련되고 있음을 보여주며, 박탈감이 범죄행위와 인과적 관련을 맺고 있다고 추론된다. 이와 같은 논리는 일부 비판범죄학자들은 수용을 거부하고 있으나 대부분의 범죄학자들은 범죄문제는 사회적 배척에 따른 것이 주종이란 점에 의견을 같이 하고 있다. 그러나 사이버범죄의 경우 인터넷에 접근하고 이를 활용할 수 있는 능력이 사회적으로 다르기 때문에 사회적으로 가장자리에 있는 사람들은 인터넷에 가장 적게 접근한다는 점이다.

사이버범죄의 수행은 기술과 자원이 요구되므로 고용, 소득 그리고 교육수준이 높은 중산층으로 해커와 프리커, 정보장사꾼, 테러리스트, 극단주의자 그리고 기타 불법행위자들이다. 결과적으로 사이버범죄의 사회적 패턴이 전통적 범죄의 지리적인 것과 상이하므로 사이버범죄자는 전통적 범죄자의 기대와 다르게 된다. 따라서 기존의 전통적 범죄행위를 설명하고 있는 사회적 배척과 가장자리 개념은 사이버범죄의 실체를 설명하는 데는 한계가 있게 된다.

③ 사이버범죄 용어 이해의 문제

정확한 용어의 정의가 부재하고 이러한 문제들의 완전한 이해가 없는 경우에는 사람들은 주어진 상황을 이해하고 있다고 착각하기 쉽고, 또한 타인들도 그와 같이 생각하는 착각 속에 빠지게 됨으로서, 결과적으로 사회현상이나 문제에 전혀 조치를 취하지 않는 결과를 낳게 되거나 부적절한 조치를 취하게 됨으로서, 사회적 손실을 야기하게 된다. 이러한 점에서 정확한 용어의 정의가 중요하게 되고, 가능한 최선의 용어를 정립하는 것이 장차 발생하게 될 사이버범죄와 정보보안 시스템에 혼란을 줄일 수 있게 된다.

3) 사이버범죄의 대응을 위한 제도적 정비

① 관련 법률의 체계적인 정비

IT의 급속한 발전에 따라 사이버범죄는 급증하고 있으나 이에 따른 법적 규제는 기술과 범죄의 속도를 따라가지 못하고 있다.[13] 사이버범죄에 대한 법률제정은 또한 기본권과 정치적 이유로 지연되기도 한다. 미국은 1996년 「통신품위유지법」을 제정하였으나 헌법에서 보장된 언론과 표현의 자유에 위배된다는 이유로 상당 부분이 수정되어야 했다. 정완은 법제도적 대응으로 사이버모욕죄와 인터넷실명제의 도입, 성매매를 위한 인터넷 루어링(Luring)금지, 사이버도박죄 도입, ISP의 책임강화와 디지털 증거에 대한 형사절차법의 마련을 들고 있다(정완, 2009: 212-219).

사이버범죄의 규제에 대해서 형법의 적용은 기본이나, 그 구체성과 기술성 때문에 특별법의 제정이 요구되고 있다. 우리나라의 경우 「정보통신망 이용촉진 및 정보보

13) 시간과 기술의 변화에 따른 범죄개념이 변화한 사례는 미국의 '애국법'(The USA Patriot Act) 제정 과정에서도 잘 나타나고 있다. 사이버테러리즘의 경우 9.11테러이전에는 범죄에 해당하지 않았거나 주법에 위배된 정도였으나 9.11테러 이후 연방법인 '애국법'에 의해 규제되도록 조치되었다.

호 등에 관한 법률」, 「컴퓨터프로그램보호법」, 「전기통신기본법」, 「정보통신기반보호법」, 「전기통신사업법」, 「저작권법」, 「청소년법」, 「신용정보의 이용 및 보호에 관한 법률」 등등이 존재하고 있으나 산발적 규정이라는 비판이 제기되어 왔으며, 이의 통합이 요구되어 왔다.

「스토커처벌특례법(안)」은 1999년 국회에서 제안되었으나 회기종료로 폐기된바 있으며, 인터넷의 성행으로 최근 사회문제화가 되고 있는 아동포르노그래피 등은 아예 입법문제가 제기되지도 않고 있는 실정이다(유용봉, 2005: 437). 산발적 규정의 미비점을 보완하기 위해서는 사이버범죄에 대한 총괄적 법률과 「스토커처벌법」등의 제정이 필요하다. 사이버모욕죄와 인터넷실명제의 도입과 관련하여서는, 사이버공간에서의 개인의 프라이버시 보호 대 표현의 자유보장이란 상반된 주장으로 찬반론이 대립된 상태에 있다. 이에 관한 논의는 정치경제에 관한 분야로 사이버스페이스의 장악과 관련된 이해관계자들의 권력 투쟁이 투영되고 있다. 그러나 인터넷상의 허위사실 유포와 악플 등 피해도 더 이상 간과할 수 없는 심각한 수준에 이름에 따라, 사이버모욕죄와 인터넷실명제의 도입이 요구된다.

② 국경을 초월한 수사권 확보와 국제형사사법공조

사이버범죄의 광범위한 발생도 문제지만 실제적으로 이를 해결하기 위한 수사권 발동에도 환경적 제한은 많다. 사이버범죄의 특성상 국제적인 연관을 가진 경우가 많아서 수사기관이 범죄자를 추적함에 있어서 관련국가의 협조를 얻어야 함에도 불구하고 이를 실현하기란 쉽지 않다. 예를 들면, 보이스피싱으로 인해 수많은 사람과 수십억원의 피해 사례가 발생되고 있으나 그 범죄단의 배후가 중국이나 대만 등과 연계되어 국내에는 자금책과 행동대를 설치하여 운영되고 있으므로 이들 국가의 공조를 받기가 쉽지 않다. 특히, 범죄인인도조약, 국제형사사법공조조약, 단속법규의 차이, 상호주의 원칙 적용 그리고 심지어 국가이익을 내세워 돈세탁행위를 두둔하거나 산업스파이를 지원하는 경우도 발생하고 있다. 또한 국내의 경우 정보통신업체에 대하여 수사기관이 수사 자료를 이용하는 데에도 한계가 있다. 한국통신은 전화번호 사용내역만 보관하고, PC통신사는 모뎀접속에 따른 IP내역만 보관하기 때문에 양쪽의 자료를 모두 입수해도 IP에 연결된 전화번호를 특정하기가 어렵다(조병인, 2000: 137-146).

우리나라는 2005년 말 현재 범죄인인도조약을 체결한 국가는 19개 국가이고 국제형사사법공조를 체결한 국가는 13개 국가이다. 그러나 체결국가의 숫자적 제한 뿐

아니라 실제로 이를 실현하기에는 제약조건이 많다. 'EUROPOL', 'INTERPOL'과 'EU 하이테크범죄기관'(ENISA) 등과 우리나라 경찰청의 '사이버테러대응센터'가 이에 관한 업무를 전담하고 있으나, 이들이 조정기능만 하고 있어 그 역할을 다하지 못하고 있다. 그러므로 인터폴의 국제적 기능이 강화되어야 하며, 국가 간 IT발달과 사이버범죄 처리 능력 등의 편차 또한 극복해야 할 과제이다.

4) 사이버윤리의 확립

가상공간과 현실세계의 윤리적 혼란은 가상공간에서 삶의 패턴을 실제상의 현실로 받아들이는 위험성이 존재하고, 가상현실에 탐닉함으로서 윤리적 문제를 야기하고 있다. 예를 들면 컴퓨터 소프트웨어의 가상체험을 현실에 옮기기 때문에 비인간화되고 폭력, 그리고 심지어 성폭력 등의 문제가 현실세계로 옮겨서 발생되고 있다(김홍진, 2000: 169-196). 그러므로 사이버공간에서 기본윤리를 확립하기 위해서는 인증제를 통한 기술적 장치와 통신윤리교육 등이 요구된다(조찬식, 2001: 198-200).

사이버공간에서의 윤리교육의 강화를 위해서는 첫째, 사이버공간에 대한 올바른 이해를 위해 청소년, 교사, 학부모, 사업자 등의 윤리교육이 중요하다. 둘째, 유관기관인 정보통신윤리위원회, 검찰, 경찰 등의 협력체제가 필요하다. 셋째, 인터넷 사업자, 민간업체 등의 협력체제가 필요하다. 넷째, 인터넷을 이용하는 기관인 학교, 직장 등에서 자체 지침서를 마련하여야 한다(정완, 2009: 211-212). 사이버윤리의 확립을 위해서는 시민들의 역할도 중요하다. 시민들이 사이버범죄에 대한 즉각적 신고와 함께 모니터링 시스템을 활용하고, 기술설치와 활용을 통해 범죄기회의 가능성을 사전에 차단하는 것이 필요하고, 개인정보의 보호의식과 함께 네티즌들의 자정능력 또한 요구되고 있다. 또한, 현재 학교에서 실시되고 있는 윤리교육과정에서 가상세계의 윤리성 제고를 위한 방안이 더욱 강화될 필요가 있다.

V. 결 론

전통적 범죄는 살인, 강도 등 노상범죄를 의미하였으나 서더랜드가 화이트칼라의 범죄개념을 도입한 이후 군대, 은행, 기업 그리고 정부 등에 의해 컴퓨터범죄의 개념이 나타나고 1990년대 인터넷의 등장과 활용, 인포메이션 테크놀로지의 진화, 디지

털기술의 급속한 발전에 의해 사이버범죄가 늘어나고 있다. 사이버범죄가 처음 등장하였을 때는 '살라미' 기법과 같은 단순한 형태로 금전적 이익을 취하는 것이었으나, 오늘날 사이버범죄는 가상세계의 특성인 비대면성과 익명성, 죄책감의 결여 등으로 인해 스누핑, 스팸메일, 디도스공격, 피싱 등의 사이버테러와 인터넷웜, 트로이목마 그리고 악성스크립트 등의 바이러스로 더욱 진화하고 있다. 또한 통신 및 게임사기, 개인정보침해, 불법사이트운영, 불법복제 그리고 성폭력과 명예훼손 등 그 범위가 넓어지고 현실세계의 모든 범죄가 재현되고 있다.

또한 사이버범죄의 용어는 일반인에게도 친숙한 용어로 회자되고 있지만 그 개념의 다양성으로 혼란을 주고 있다. 사이버범죄는 컴퓨터범죄, 인터넷범죄, 하이테크범죄, 정보범죄, 네트워크범죄, 디지털범죄 등의 용어로 사용되고 있다. 그러나 사이버범죄는 단일현상이 아니라 정보네트워크와 통신테크놀로지에 의해 수행되는 것으로 가상공간이 주축이 되어 야기된다는 점을 강조하기 위한 것이며, 최근 디지털 기술과 관련된 것이 증대되고 있다. 그러므로 사이버범죄란 컴퓨터, 인터넷, 조직적인 네트워크 그리고 디지털기술과 같은 전자적 장비를 활용하여 인포메이션 테크놀로지를 이용하여 불법적 행위를 용이하게 하는 것이라고 할 수 있다.

변화하는 사이버스페이스의 치안환경에 효율적으로 대응하기 위해서는 다음과 같은 경찰활동 방안이 제안된다. 첫째, 법적분야로 사이버범죄에 관련된 법률을 체계적으로 정비할 필요가 있다. 현재는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「컴퓨터프로그램보호법」 등이 산재되어 있으므로 이들의 체계화가 요구된다. 둘째, 제도적인 측면으로는 먼저 전통적 경찰활동의 역할의 변화가 필요하다. 테크놀로지 발전에 따른 사이버범죄의 증대를 따라잡기 위해서는 사이버경찰활동의 역량이 제고되어야 한다. 또한 사이버범죄는 초 국경의 경찰활동이 요구되므로 인터폴 등 국제적 협력기반의 강화가 요청된다. 다음으로는 IT전문가와 국·내외 금융전문가 등의 전문 인력의 충원이 뒤따라야 한다. 셋째, 범죄학이론이 재조명되어야 한다. 기존의 범죄학은 사회적·문화적·물리적 특성인 '일상활동이론'이 주를 이루었으나 사이버범죄는 시·공을 초월함으로서 전통적 이론의 한계에 대한 보완이 요청된다. 또한 전통적 범죄자는 사회의 배척자나 가장자리에 머무르는 사람들이 대부분이었으나 사이버범죄자는 기술, 교육, 소득이 상당한 중산층이란 점이 고려되어야 한다. 넷째, 사이버윤리의 확립이 시급하다. 정부, 정보제공자, 정보통신서비스 제공자 그리고 이용자 간 책임성의 확보가 필요하다.

참고문헌

〈국내문헌〉

경찰대학. (2006), 「사이버범죄수사론」, 광문당.

경찰청. (2009), 「경찰백서」.

김경태. (1997), "컴퓨터범죄에 대한 법적 고찰," 중앙대학교 법과대학, 「법정논총」 32(1): 118-133.

김홍진. (2000), "사이버스페이스에서의 기독교사회 윤리적 과제," 「기독교사회윤리」 3: 169-196.

사법연수원(2007), 「신종범죄론」, 성문인쇄사.

유영현·송봉규·박상진. (2009), "디지털포렌식(Digital Forensic) 전문인력의 필요성과 양성방안", 「한국경찰학회보」 11(4): 253-2284.

이윤호. (1993), "컴퓨터범죄의 대응방안", 「한국공안행정학회보」 2(1): 95-108.

_____. (2007), 「범죄학」, 박영사.

유용봉. (2005), 「인터넷범죄와 형법」, 21세기사.

조찬식. (2001), "사이버공간에서의 네티켓과 일탈행위에 관한 연구," 「정보관리학회지」 18(2): 187-202.

정 완. (2007), "사이버범죄의 현상", 「형사정책」 19(2): 9-32.

_____. (2009), "사이버범죄의 실태와 동향 및 대응책," 홍익대학교, 「홍익법학」 10(1): 195-224.

조병인. (2000), 「사이버경찰에 관한 연구」, 한국형사정책연구원.

최응렬. (1997), "신용카드범죄의 실태와 대책", 「한국공안행정학회보」 6(1): 452-475.

최인섭·최영신. (1996), 「화이트칼라범죄에 관한 연구」, 한국형사정책연구원.

허경미. (2009), 「현대사회와 범죄」, 박영사.

〈국외문헌〉

Carter, D. L. (1995), "Computer crime categories: How techno-criminals operate", *FBI Law Enforcement Bulletin*", 64(7): 21-27.

Casey, Eoghan (2004), *Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet*, London: Elsevier Academic Press.

Castells, M. (2002), *The internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford: Oxford University.

Davies, S. (1996), *Big Brother: Britain's Web of Surveillance and the New Technological Order*, London: Pan Books.

Furnell, S.(2002), *Cybercrime: Vandallizing the Information Society*, London: Addison-Wesley.

Gibson, W. (1984), *Neuromancer*, New York: Ace Books.

Grabosky, P. (2001), "Virtual Criminality: Old Wine in New Bottles?", *Social and Legal Studies* 10: 243-9.

Hollinger, R. C. (1991), *Hackers: Computer Heroes or electronic highwaymen? Computers and Society*, 2(1): 6-17.

Home Office (2002), *Home Office Annual Report 2001-2*, at http://www.homeoffice.gov.uk/docs./2010.1.15.

Loader, B. D. (1997), *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, London: Routledge.

McQuade, Samuel C. III (2006), *Understanding and Managing Cybercrime*, New York: Pearson Education, Inc.

Parker, D. B. (1976), *Crime by Computer*, New York, Charles Scribner's Sons.

Shields, R.(ed.) (1996), *Cultures of the Internet: Virtual Space, Real Histories, Living Bodies*, London: Sage.

Stern, K.(1998), *A Force Upon The Plain – The American Militia Movement and the Politics of Hate*, Norman and London: University of Oklahoma Press.

Sutherland, Edwin, H.(1949), *White Collar Crime*, New York, Dryden Press.

Snyder, F.(2001), "Sites of Criminality and Sites of Governance," *Social Legal Studies*, 10: 251-6.

Taylor, R. W. Caeti, T. J., Loper, D. K., Fritsch, E. J., Liederbach, J.(2006), *Digital Crime and Digital Terrorism*, Upper Saddle River. New Jersey: Pearson Prentice Hall.

Thomas, D. and Loader, B.(2003), *Cybercrime: law enforcement, security and*

surveillance in the information, London and New York: Routledge.

Wall, D. (2000), "Policing the Internet: maintaining order and law on the cyber-beat," in Y. Akdeniz, C. P. Walker and D. S. Wall (eds), *The Internet, Law and Society*, London: Longman.

_____. (2008), "Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime," *International Review of Law Computers & Technology*, 22(1-2): 45-63.

Yar, Majid(2006), *Cybercrime and Society*, London: Sage publications.

〈기타〉

「중앙일보」, 2009. 4. 24 : 29

_____, 2009. 6. 19 : 14

_____, 2009. 6. 25 : 14

_____, 2009. 6. 25 : E1

「한국경제신문」, 2007. 7. 12.

http://markidea.net/entry/internet-population/2010.1.15.

www.krnic.or.kr /2010.1.15

【Abstract】

Comprehension and Countermeasure in the Evolution of Cybercrime and its phenomena in accordance with technology development

영문 이름 없음

The rapid development of technology has brought in their wakes them significant changes, a lot of benefits and enhancement of productivity in the ways we work, trade, study, play, consume, communicate and interact. Politicians, businessmen, police and citizens now have a new jargon with which to identify such dangers: hacking, spoofing, phishing, viruses, Trojans, malware, piracy, downloading, spyware, cyberstalking, cyber obscenity, cyber fraud, and so on. In this point, a dramatic paradigm shift from crime on the street to crime by keyboard has been occurred.

Although we say the word, cybercrime in common nowadays, it has been not so long since we have used the word because computers were put into force in the seventies and internet was born in nineties. The concept, Cybercrime is fused and mingled with the usages of other similar words, for example, computer crime, internet crime, hitech crime, intelligence crime, network crime, credit crime, eavesdropping, not understood throughly and not unified in its meaning. Therefore, unfortunately, law enforcement, public and private are confronted with a new set of crimes, criminals, and techniques for that they are not well prepared. In this respect, how to understand, explain, respond and manage the cybercrime are regarded to be crucial aspects not only to overcome the epidemic crime but also to catch up with the on-going development of technology. In this regard, managing and establishing policies against the cybercrime and training for the people concerned are not well controled. Bearing in mind the said problems, the

following steps are reviewed to redefine what the cybercrme is and will be in the coming years not only to cope with but also to solve the problems mentioned : first, chronological and theoretical review of the cybercrime, second, the evolution of cybercrime and its' current phenomena, third, the redefining of related terminologies to the cybercrime, fourth, comprehension and countermeasure in the evolution of cybercrime and its phenomena.

The theory of cybercrime is rooted in the meaning of white color crime by Sutherland in the late 1930. The term 'cybercrime' is widely used today to describe the crimes or harms that result from opportunities created by networked technologies. Its origins lie in science fictions across the cyberspace. As a result, it is born in the midst of fiction and science and finally anchored with the mixture of terms such as computer crime and other terms. On conclusion, cybercrime can be defined use of computers, internet, organizational networks, digital technique via information technology to facilitate illegal behaviors.

To comprehend and countermeasure in the evolution of cybercrime and its phenomena in accordance with the technology development, the following steps are recommended: First, the traditional pattern of policing and criminal justice be adapted to the new role for them because the new crime, cybercrime demolishes the current geographical boundaries of the world. Second, experts for IT as well as other professional gurus including finance be recruited to catch up with the rapid increase of cybercrime. Third, the current criminology be adjusted to the new challenges that the current theory of routine activity based on the real world may be not applicable in the virtual world due to the abolishment of time and space barrier in the virtual world. Fourth, it be focused that the traditional criminals are from poor background in society but criminals in the cyberspace are relatively educated with skills and good incomes. Fifth, laws and regulations which are related with the cybercrime be systemized because the concerned laws are scattered here and there, remaining no law concerning cyberstalking is enacted. Last, cyber ethics be established as early as possible like the ethics on the mundane world with all the concerned parties such as government, internet service provider, citizens participating.

Key Words : cyber crime, computer crime, internet crime, hitech crime, cyber space, digital