사이버경찰의 수사한계와 수사력 강화방안

최응렬* · 황영구**

< 목 차 >

Ⅰ. 서 론

1. 연구의 목적

현재 인류는 인터넷이라는 가상공간에서 사이버범죄로 인해 새로운 위협을 받고 있다. 이 사이버범죄는 정보통신매체에 대한 의존도가 심화됨에 따라 나타난 하나의 결과라고 볼 수 있다(Scott Sullivan, 1999: 19). 인터넷이 우리에게 비춰주는 밝은 면 뒤쪽에 짙게 드리워진 어두운 그림자를 없애는 것이 이 시대를 살아가는 우리 모두가 시급히 해결해야 할 숙제일 것이다.

그렇다면 인터넷상에 짙게 드리워진 어두운 면을 해결하기 위해 어떤 노력을 하고 있으며, 그 문제점이 과연 무엇인가? 그리고 이를 해결할 수 있는 방안이 과연 없는 것인가? 이러한 사이버범죄에 대응하는 근본적인 해결책을 찾기 위해 많은 노력을 기울이고 있으나 뚜렷한 해결책이 없는 것이 현실이다.

* 계명대학교 경찰행정학부 교수
** 계명대학교 대학원 경찰행정학부 박사과정

현재 사이버범죄에 대응하기 위해 경찰청, 검찰청, 국가정보원, 한국정보보호진흥원 등 여러 기관들이 노력하고 있으나 이들을 비웃기나 한 것처럼 계속해서 늘어나고 있다.[1] 더 큰 문제는 사이버범죄가 계속해서 늘고 있는 반면에 검거율은 점점 떨어지고 있다는 것이다.[2] 검거율이 점점 떨어지는 근본적 이유는 컴퓨터 및 네트워크 기술의 고도화로 인해 범죄수법이 매우 다양해지고 있으며(오기두, 1997: 63), 범죄자 등에 의해 소거 혹은 각종 수법에 의한 은폐가 용이하다는 점, 압수의 대상인 데이터를 특정하기가 매우 곤란한 점을 들 수가 있다(英太郎, 1999: 139). 또한 사이버수사관들의 전문지식과 인력 부족, 예산부족으로 인해 첨단장비 도입과 증거확보를 위한 기술개발 미비, 즉 사이버경찰의 전반적인 시스템에 큰 문제가 있음을 잘 말해 주고 있다. 따라서 이 연구에서는 사이버수사의 방법과 절차를 설계해 보고, 사이버수사의 한계를 살펴본 후 사이버경찰의 수사력 강화방안을 모색해 보고자 한다.

2. 연구의 범위와 방법

그 동안 학계, 여러 관련기관에서 사이버범죄와 관련하여 형사정책 분야에 대해서는 많은 연구가 이루어지고 있다. 그러나 이 연구는 기존의 선행연구들과 방향을 바꾸어 사이버수사에 초점을 두었다. 따라서 이 연구에서 다루고자 하는 범위는 사이버수사의 방법과 절차를 설계해 보고, 사이버수사를 하는데 있어서 어떠한 한계가 있는지 살펴볼 것이며, 이에 따른 사이버경찰의 수사력 강화방안을 모색하는데 있다.

이 연구는 주로 관련문헌과 공식통계자료, 정부기관의 홈페이지 및 언론의 각종 보도자료를 활용하여 문헌연구를 하였다. 특히, 각종 통계자료의 객관성을 확보하기 위해 국회 행정자치위원회 및 법제사법위원회의 국정감사자료집을 활용하였다.

---

1) 경찰청 경찰백서(2002)에 따르면 2000년에 2,444건, 2001년에 33,289건으로 무려 13.6배가 증가하였다.

2) 한나라당 박종희 의원에게 제출한 '사이버범죄 발생 및 검거현황'에 따르면 사이버범죄는 1998년 394건, 1999년 1천709건, 2000년 2천444건 그리고 2001년 7월말 현재 9천520건으로 폭증하고 있는데 반해 범인 검거율은 1998~1999년에는 거의 100% 수준이었으나 2000년 70.2% 그리고 2001년 7월말 현재는 20.9%로 나타났다(인터넷 한겨레. 2001. 8. 31일자: http://www.hani.co./kr/section-003000000/2001/08/003000000200108311446752.html).

Ⅱ. 사이버수사의 방법과 절차

1. 사이버수사의 방법

수사의 방법은 크게 임의수사와 강제수사의 두 가지로 나눈다. 임의수사란 강제력을 행사하지 않고 상대방의 동의를 얻어서 수사하는 방법을 말하고, 강제수사란 상대방의 의사와 관계없이 강제로 수사하는 방법을 말한다.

형사소송법 제199조제1항에서 수사는 기본적으로 임의적 방법으로 하는 임의수사의 원칙과 법률에 특별한 규정이 있는 경우에만 예외적으로 허용하는 강제수사 법정주의 원칙, 그리고 헌법 제12조제3항에서 강제수사는 일부 법정된 예외를 제외하고 법관이 발부한 영장에 의할 것을 요구하는 영장주의의 원칙을 채택하고 있다(배종대 · 이상돈, 2004: 210).

1) 임의수사

범죄관련 전자기록 등을 압수 · 수색영장에 의하지 않고 수사에 이용할 수 있는 방법으로는 컴퓨터 관련 증거의 소지자에 의한 임의제출을 받을 수가 있다(하태훈 · 강동범, 1998: 314). 이와 마찬가지로 수사기관은 권한 있는 자의 동의가 있는 경우에는 영장 없이도 일정한 장소 또는 물건을 수색할 수 있다. 이러한 동의는 명시적으로 또는 묵시적으로 가능하다. 동의를 한 자가 동의를 거부할 권한이 있음을 알았느냐 여부는 문제되지 않는다.

그러나 컴퓨터에 대한 수색에 대한 동의가 있었는지에 관해서는 통상의 경우보다 더 복잡한 문제가 발생할 수 있을 것이다. 즉 전자게시판과 같은 복수의 사용자가 있는 경우에는 누구한테 동의를 받을 것인지, 시스템 관리자가 모든 시스템 사용의 파일에 대한 수색을 동의할 수 있는지 등의 문제가 발생할 수 있다(김상우, 1996: 227). 그리고 법원은 동의가 자발적으로 이루어졌는가를 판단하여야 하고 이를 적법하게 판단하기 위해서는 동의를 한 자의 나이, 지적 수준, 정신적 및 신체적 상태, 동의를 하지 않을 권리가 있음을 고지 받았는지 여부 등의 여러 요소들이 복합적으로 고려되어야 할 것이다

(1) 동의의 범위

수색에 대한 동의에 있어서는 그 범위가 명시적으로 제한될 수 있다. 즉 수사기관은 제한된 동의 범위를 넘어 대상물을 수색할 수 없다. 또 동의 범위는 묵시적으로도 제한될 수 있을 것이다.

피고인이 자신의 컴퓨터에 있는 정보에 대해 수색을 동의하였다 하더라도 패스워드를 통해 수사관이 보지 못하게 하였다면 이는 동의에 관한 묵시적 한계를 구성한다고 보아야 할 것이다(이종상, 2000: 42). 만약에 수사관이 피고인이 패스워드를 입력하는 것을 어깨너머 보려 한 것이 위법은 아니라 할지라도 위와 같이 알아낸 패스워드로 컴퓨터 내용 전체를 검색하려 한 것은 피고인의 동의의 한계를 넘은 것으로 보아야 할 것이다.

(2) 공동사용자에 의한 동의

오늘날 많은 컴퓨터 사용자들은 컴퓨터를 서로 공유하고 있다. 이러한 경우에는 복수의 사용자가 존재하게 된다. 만약에 컴퓨터의 수색에 대한 동의에 있어서 복수의 사용자 중의 일부만 동의를 하였을 경우에 그 동의가 유효한가, 또한 유효하다면 수사기관은 어떤 범위의 정보를 검색할 수 있는지가 문제가 된다. 이러한 문제로서 첫째, 컴퓨터 공동사용자의 동의에 대한 문제이다. 컴퓨터 수색에 있어서 공동사용자 중의 한 명이 공동영역에 개인적인 디렉토리(Directory)를 설치하였을 경우를 예로 들어보자. 이러한 경우 위와 같은 원칙을 적용한다면 별도의 디렉토리를 만드는 것만으로는 새로운 영장을 요할 정도의 프라이버시를 기대할 수 없다고 할 것이다. 그러나 설치자가 디렉토리에 패스워드 등의 접근제한 조치를 취했다면 이는 공동사용자의 동의만으로는 수색대상이 될 수 없다고 보는 것이 타당할 것이다. 따라서 공동사용자의 동의가 있었다고 하더라도 수사기관이 패스워드를 해독하여 디렉토리를 수색하였다면 이것은 위법한 증거수집으로 보아야 할 것이다.

둘째, 같이 생활하는 배우자의 동의에 대한 문제이다. 일반적으로 배우자의 동의에 의한 수색은 아무런 문제가 없을 것이다. 결혼생활을 영위하는 가택은 배우자들 간에 공동으로 유지되고 관리되는 공간이다. 이러한 수색대상인 영역에 대하여 동의를 하는 배우자가 실질적으로 접근이 허용되지 않는다는 명백한 증거가 없는 경우에는 그 동

의의 효력은 인정될 것이다. 그러나 배우자간이라 하더라도 배우자 일방에 의해서만 사용되는 특별한 부분에 대하여 이를 사용하지 아니하는 배우자가 동의를 한 경우라든지, 배우자끼리 조화롭지 못한 결혼상태에 있으면서 일방에 대한 분노로 수색에 대하여 동의한 경우에 대하여는 적법한 동의가 있었다고 보기 어려울 것이다.

셋째, 부모의 동의에 대한 문제이다. 최근의 컴퓨터사용 인구의 상당수는 청소년이라고 할 수 있다. 따라서 컴퓨터 관련 범죄는 다른 범죄에 비하여 일반 성인들보다는 청소년들에 의하여 저질러지는 경우가 많다. 이러한 경우 부모들의 동의를 받아 자녀가 사용하는 컴퓨터에 대하여 압수·수색을 할 수 있는지 문제가 된다.

일반적으로 부모는 가족들이 거주하는 집의 공동영역을 수색하는데 대하여 동의할 권한이 있는 것은 명백하다. 특히, 미성년 자녀들에 대한 법정대리권을 가지고 있는 부모들로부터 동의를 얻은 경우에는 압수·수색이 유효한 것으로 보아야 할 것이다. 그러나 성년인 자녀들의 경우에는 그들만의 배타적인 영역을 확립하고 있다면 부모의 동의만으로 수색에 충분한 동의를 얻었다고는 볼 수 없을 것이다.

넷째, 시스템 운영자의 동의에 대한 문제이다. 현대는 인터넷 시대라 불리는 만큼 통신망이 발달되고 있으며 그 가입자가 폭발적으로 증가하고 있는 현실이다. 이러한 현실에 비추어 볼 때 누가 과연 수사에 대한 동의를 할 수 있는지, 시스템 운영자가 모든 가입자에 대한 동의가 적법한 것인지는 중요한 문제가 된다.

일반적으로 시스템 공동사용자들은 운영자가 시스템에 있는 정보를 개시할 위험을 인수하고 있으며, 비록 자신들이 프라이버시에의 기대를 갖고 있어도 운영자가 업무수행을 위해 접근하는 것을 저지할 수 없다. 따라서 운영자가 그 시스템에 대한 수사에 동의할 권한을 갖는다고 볼 수 있을 것이다. 이러한 경우 동의의 적법성을 인정받기 위해서는 시스템 이용자들이 운영자가 시스템의 전반적인 사항을 점검하기 위하여 가입자의 활동을 규제한다는 점, 또 일정부분에 대해서는 사용 중인 파일을 저장할 수 있다는 점 등 이용자들이 알고 있었다는 것을 증명해야 할 것이다.

만약에 시스템 이용자들이 이러한 점을 알지 못하였다고 주장하는 경우라 하더라도 회원 가입시 또는 평상시에 합리적인 시스템 이용자라면 시스템 운영자의 이러한 역할에 대해 잘 알고 있었을 것이라는 점을 증명할 수 있으면 될 것으로 생각된다. 그러나 시스템을 사용한다 하더라도 가입자의 사생활 보호차원에서 운영자의 동의만으로

는 접근이 허락되지 아니하는 영역이 있을 수 있다. 이러한 경우에는 운영자의 동의를 얻었다는 점만으로는 부족하고 수사관은 별도의 영장을 발부 받는 것이 옳을 것이다. 만약에 시스템 운영자가 동의를 거부하고 영장을 요구한다면 영장을 발부 받기 전까지 문제가 된 정보가 삭제되거나 조작될 위험이 있다. 그래서 수사관은 운영자에게 문제가 된 정보를 백업하여 복제할 것을 먼저 요구할 수 있을 것이며, 사후에 영장을 발부 받으면 될 것이다.

2) 강제수사

컴퓨터시스템 내에 저장되어 있거나 처리 중인 데이터를 수집함에 있어서는 컴퓨터시스템이 설치되어 있는 건조물에 들어가서 이를 수색하고 데이터를 압수할 수 있어야 한다. 그런데 현행 형사소송법 제106조, 제219조는 압수의 대상으로서 증거물 또는 몰수할 것으로 사료하는 물건을 들고 있다. 이 때 증거물 또는 물건이라 함은 일상 언어관념상으로는 유체물을 의미한다고 할 것이다. 컴퓨터에 의하여 처리되고 저장된 전자적 기록 또는 데이터는 그 자체로서는 유체물이 아니기 때문에 과연 압수의 대상이 될 수 있는지에 대해서 많은 논의가 있었다.

논의의 긍정적인 입장에서는 유체물인 데이터 전달매체를 압수하고 검사하는 권한 안에 데이터 자체를 조사하는 권한도 포함되어 있다고 보는 입장이다. 이 입장에서는 데이터 저장매체에 저장되어 있는 컴퓨터 데이터의 조사는 유체물을 대상으로 하는 전통적인 압수·수색에 의한 수사방법에 의한다 하더라도 특별한 문제점은 없다는 것이다.

부정적인 입장에서는 컴퓨터시스템을 증거물로 보아 이를 압수할 수 있다. 그러나 당해 데이터와 컴퓨터 기억매체가 일체불가분으로 결합되었다고 볼 수 없으므로 유체물에 한하여 압수할 수 있도록 규정한 현행 형사소송법상에서는 이를 압수·수색하는 것은 불가능하다고 보는 입장이다(이종상, 2000: 52-55).

현재는 정보사회로 전자상거래에서 나타나듯이, 향후 서류가 없는 사회가 올 수 있을 정도로 컴퓨터에 데이터화되어 있는 자료의 중요성은 더욱 증대될 것이다. 이미 업계에서는 물론이고 정부에서도 민정행정서비스를 위한 인터넷시스템을 구축하여 전자정부 대 국민 서비스를 실시하고 있다.[3] 이러한 때 절차법인 형사소송법의 규정이 문

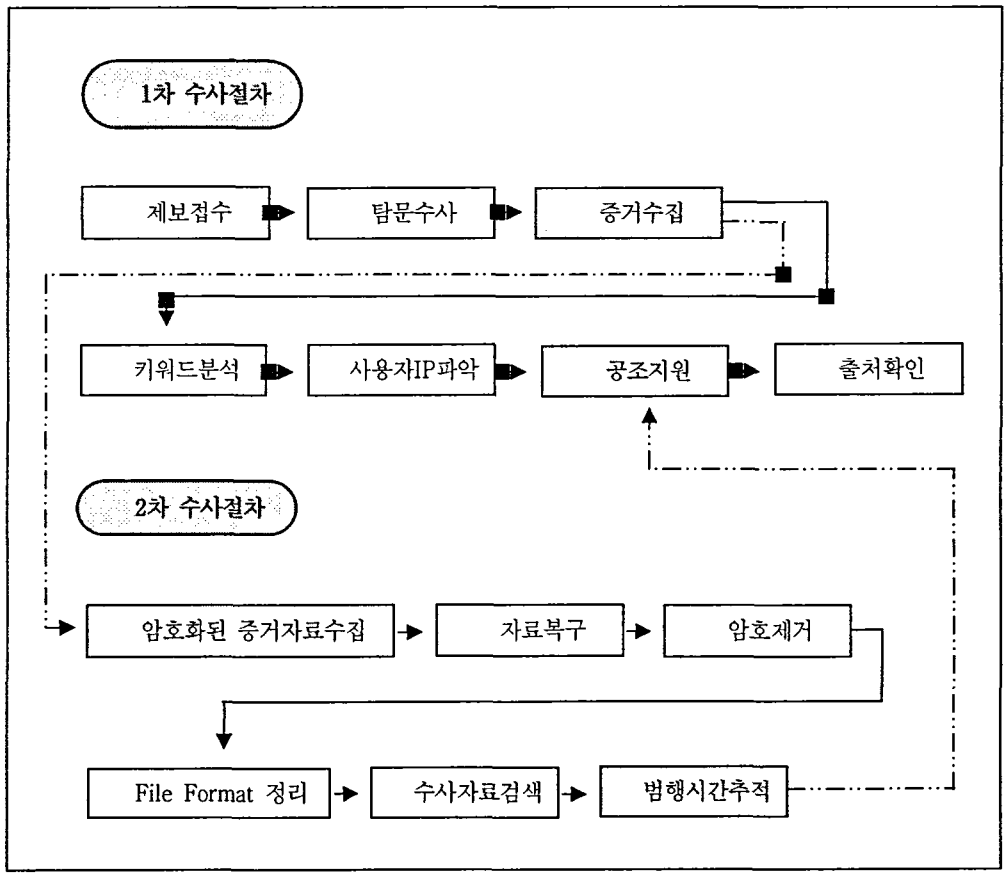
리해석상 압수·수색 대상을 유체물에 한정시키는 것처럼 해석된다는 이유만으로 데이터 등 무체정보를 압수·수색의 대상에서 제외시키는 것은 무체정보를 사법절차상의 통제 범위 밖에 방임하게 되는 결과를 초래할 것이다.

2. 사이버수사의 절차

일반적인 수사절차는 광의의 측면으로 보면 수사의 단서에서 시작하여 사건의 확정판결에 이르기까지를 의미하고, 협의의 측면으로 보면 수사의 단서에서 시작하여 공소제기까지의 시기를 의미하는 두 가지의 경우가 있다. 이러한 관점에서 볼 때 일반적인 수사절차는 수사의 단서(내사)→수사활동→공소제기→공판→판결의 일련의 과정으로 이루어진다고 볼 수 있을 것이다(박경식·천대영, 2002: 11).

그러나 사이버범죄 수사절차는 아직 정형화되어 있지 않지만, 수사의 단서→수사활동까지만 한정하여 설계해 보면 <그림 1-1>과 같다. 주요 내용을 보면 1차 수사절차 중 증거수집에서 암호화된 증거를 수집한 경우에는 2차 수사절차에 가서 암호를 제거하여 증거자료를 확보해야 한다. 그리고 증거자료를 확보한 다음 범행시간 및 위치추적을 하여 관계기관에게 수사협력을 요청하여 정확한 출처를 확인하면 된다.

3) 대한민국전자정부(https://www.egov.go.kr).



<그림 1-1> 사이버수사의 절차

Ⅲ. 사이버수사의 한계

1. 범죄의 특성에 따른 한계

사이버범죄는 인터넷기반으로 하여 컴퓨터시스템을 매개로 이루어지는 범죄이다. 사이버범죄는 현실세계의 범죄에 비해 가상공간인 사이버공간에서 범행이 이루어지기 때문에 사이버수사의 한계를 드러낼 수밖에 없는 특수성을 띄고 있다. 그 한계로써 첫째, 사이버공간은 비가시적이고 현실세계와는 달리 범죄자들이 자신의 얼굴과 정체를

노출시키지 않고 행동할 수 있다는 비대면성을 가진다는 것이다. 이러한 비대면성으로 인하여 범죄자들을 보다 과격하고 대담하게 행동을 하는 경우가 많아 사이버수사에 큰 어려움을 겪고 있다

둘째, 사이버공간은 "익명의 바다"라고 할 수 있다. 즉 사이버공간에서는 신분을 노출시키지 않은 채 활동이 가능하다는 것이다. 타인의 인적 사항이나 ID를 도용하면 자신의 익명성을 보장받을 수 있게 된다. 이러한 익명성으로 인하여 컴퓨터사용자들은 쉽게 범죄의 유혹에 빠져들고 있으며(박경식 · 천대영, 2002: 607), 또한 가해자의 대부분이 타인의 ID를 도용하는 등의 신분은닉 조치를 취하여 수사에 어려움을 주는 요인이 되고 있다.

셋째, 사이버범죄 중에는 컴퓨터와 인터넷에 대하여 약간의 지식과 기술만 익히면 범할 수 있는 것도 있지만, 컴퓨터 프로그램조작을 통한 재산취득, 바이러스 제작 및 유포, 해킹과 같은 사이버범죄는 고도의 전문적인 지식과 기술을 갖추고 있어야만 가능한 범죄가 대부분이다. 이러한 특성으로 인해 사이버수사에 어려움이 있으면, 무엇보다도 사이버수사요원의 전문성과 기술성을 요한다고 할 수 있다.

넷째, 인터넷은 TCP/IP[4]라는 공통된 통신규약을 사용하여 전 세계의 컴퓨터 통신망을 하나의 집합체로 연결하고 있어 국가간의 경계 및 지리적 제약을 해소한다. 이러한 인터넷 공간의 시 · 공간적 무제약성은 잠재적인 범죄자들에게 많은 범죄의 기회를 제공하고 있다는 것이다. 이러한 시 · 공간적 무제약성으로 인한 사이버범죄에 대처하는 데는 현실적으로 큰 어려움이 있다(貴志浩平, 1998: 118; 砂田務, 1998: 58).

2. 범죄수법에 따른 한계

사이버범죄는 통상적인 범죄와는 확연히 구분되는 익명성, 비대면성, 전문성과 기술성, 국제성 등의 고유한 특성을 가지고 있다. 또한 사이버범죄자들은 고도의 컴퓨터지식과 기술을 가지고 범행을 하기 때문에 그 범죄수법이 매우 다양하다. 이러한 범죄수법들을 살펴보면 첫째, 컴퓨터의 정보처리 과정에서 처리, 전달, 보존되는 데이터를 조작하는 부정행위이다. 여기에는 데이터의 부정변개(Data Diddling)[5], 트로이 목마수법

4) TCP/IP : 전송제어프로토콜(Transmission Control Protocol) + 인터넷프로토콜 (Internet Protocol)

(Trojan Horse)[6], 부분잠식수법(Salami Techniques)[7], 운영자로의 위장수법(Superzapping)[8], 들창수법(Trap Doors)[9] 등이 있다.[10] 형법상의 전자기록범죄에서의 특수매체기록의 위작, 변작행위와 컴퓨터사용사기죄에서의 정보처리장치에 허위정보 입력행위 등이 이러한 유형에 해당된다.

둘째, 컴퓨터에 의하여 처리, 보관, 전송되는 데이터나 프로그램을 권한 없이 습득하여 이용하는 컴퓨터스파이이다. 컴퓨터프로그램은 제작자들에게는 높은 부가가치를 창출하여 주기 때문에 범행의 대상으로서도 충분한 가치가 있다. 게다가 컴퓨터에 저장된 기업의 원가계산, 대차대조표, 고객관리서, 인사자료, 연구개발 자료, 생산공정도, 부품 설계도 등은 가장 중요한 범죄대상이다. 여기에는 쓰레기줍기수법(Scavenging)[11], 자료추출수법(Data Leakage)[12], 선로도청방법(Wire Tapping)[13], 비동기성공격(Asynchronous Attacks)[14] 등이 있다. 형법상의 기술적 수단에 의한 비밀침해죄에서의 특수매체기록의 내용을 기술적 수단을 이용하여 알아낸 경우가 이러한 유형에 해당된다.

셋째, 데이터나 프로그램이 저장된 매체를 없애거나 교란시키는 컴퓨터시스템 파괴행위이다. 이러한 파괴는 대부분 컴퓨터시스템 내에 있는 데이터나 프로그램을 파괴하는 것을 말한다. 컴퓨터의 프로그램은 일정한 규칙과 패턴에 의하여 작성되므로 아주 간단한 변경만 가하더라도 응용 프로그램과 같은 것은 아무 쓸모가 없게 된다. 프로그램 내에 이와 같은 암적인 루틴(Cancer Routine)을 반복, 복사함으로써 쓸데없는 자료

---

5) 컴퓨터에 입력된 데이터를 변개하거나 허위의 데이터를 입력하는 방법.
6) 프로그램 본래의 기능을 훼손하지 않고 은밀하게 조작해 부정한 결과가 나오도록 하는 방법.
7) 금융기관 컴퓨터시스템에 있는 프로그램을 조작하여 이자 계산시 단수 이하로 떨어지는 이자를 떼어 특정계좌에 자동적으로 입금되도록 하는 범죄수법(Donn B. Parker, 1983: 90-91).
8) 슈퍼잽(Superzap) 프로그램이 작동할 때 Password와 같은 보안장치의 기능이 상실되어 컴퓨터 주기억장치에 수록된 모든 자료에 접근이 가능하게 된다. 이 때 컴퓨터의 고장을 수리하는 것처럼 위장하여 그 안에 수록되어 있는 데이터를 조작하거나 입수하는 방법 등에 의한 범죄수법.
9) Debugging 등 프로그램을 수정할 수 있는 명령을 시스템상에서 삭제를 잊어버리거나 고의로 삭제를 하지 아니하였을 때 완성된 프로그램 내에서 이 명령을 실행하여 범죄를 자행하는 범죄수법.
10) 기타 범죄수법에 대하여는 최응렬(1990: 91-92) 논문 참조.
11) 컴퓨터시스템의 기억장치 내에 이전에 사용한 내용이 남아 있을 때 그 내용을 읽어 내거나 또 일정시간마다 그 기억장치 내에 있는 내용을 읽게 하는 프로그램을 조작하는 범죄수법.
12) 컴퓨터시스템으로부터 데이터를 다른 곳에 이전하거나 자료의 사본을 얻는 범죄수법.
13) 통신 중의 정보를 도청하는 범죄수법.
14) 컴퓨터에 수록되어 있는 Password 등 비밀장치를 뚫는 범죄수법.

검색을 계속 실행하여 컴퓨터의 속도를 느리게 할 수 있다. 이러한 행위들은 컴퓨터 범죄자들이 본격적인 범죄행위를 위한 준비단계로서 이루어지는 것이 대부분이다. 또 바이러스를 제작하여 컴퓨터시스템 내에 바이러스를 감염시키는 행위, 전문 해커들에 의해 시스템 내에 해킹하는 행위도 이에 해당되며, 형법상의 컴퓨터업무방해죄에서의 정보처리장치 등 손상행위와 전자기록등손괴죄에서의 특수매체기록 은닉행위 등이 이러한 유형에 해당된다.

넷째, 타인의 컴퓨터를 사용할 권한이 없는 자가 임의로 컴퓨터를 사용하는 것이다. 컴퓨터의 보유자나 고용인에게 눈에 띠는 손실을 가져오는 것은 아니며, 그 위험성도 훨씬 경미하다. 그러나 통신요금의 부담이나 컴퓨터 장비의 과도한 사용으로 별도의 부담을 발생시키는 범죄수법이다.

위와 같이 범죄수법은 매우 다양하다. 사이버범죄자들은 이러한 다양한 범죄수법 중 한 가지 수법에 의한 범행을 하지 않는다. 즉 여러 가지 수법이 결합된 형태로 범행을 저지르는 경우가 많아서 사이버수사를 하는데 상당한 어려움이 뒤따른다.

3. 증거확보에 따른 한계

증거는 보통 디스켓, 데이터 보고서, 프로그래밍 또는 컴퓨터에 있는 정보로부터 또 다른 인쇄된 정보의 형태이다(Wayne W. Bennett and Karen M. Hess, 2001: 438). 사이버범죄로 인한 다양한 범죄수법들로 인해 수사기관이 증거를 확보하는데 상당한 어려움을 겪고 있다. 사이버범죄에 대한 수사단계에서의 증거확보는 일반적으로 피해증거와 접속기록을 확보하여 이를 분석하여 확인한 다음 피의자의 검거와 증거물 혹은 증거자료에 대한 압수절차로 진행된다. 이는 일반범죄의 수사와 유사하지만 구체적인 증거절차에서는 차이가 있다. 사이버범죄의 피해발생에 대한 증거확보를 어렵게 만드는 특징을 살펴보면 첫째, 데이터의 부정조작에 의한 범죄이다. 이는 범행 증거를 쉽게 인멸할 수 있고, 범인이 컴퓨터 운영상 실수로 데이터가 삭제된 것처럼 위장할 수도 있어 이를 증명하기가 상당히 어렵다.

둘째, 컴퓨터시스템의 기억장치에 저장된 정보량이 방대하여 관련 범행의 증거를 확보하는 것은 사실상 어렵기 때문에 수사대상이나 압수물의 명시 및 특정의 문제가 절

차상 발생하지 않는다는 보장이 없다는 점이다.

셋째, 컴퓨터시스템 내에 있는 데이터 및 프로그램을 삭제할 때이다. 컴퓨터시스템 내에 기록된 데이터 및 프로그램이 증거로 채택된 경우에는 압수·수색 등에 있어서 새로운 문제가 발생하게 된다. 통상 압수의 객체는 가동유물체인 증거물인 바 데이터가 수록된 기억장치 자체는 유체물로서 압수의 대상이 된다. 그러나 실제로 증거가 되는 것은 기억장치에 기록된 무체정보인 데이터이다. 즉 데이터만을 직접 압수의 대상으로 하여야 하므로 무체정보에 대한 압수가 가능한가 하는 문제를 고려해 봐야 한다(이철, 1995: 211).

넷째, 전자우편, 웹, 쉘 서비스 등은 각각 서로 다른 디렉토리에 별도 파일이 저장되므로 시스템 운영자에게 자료를 제공받아 증거를 확보해야 한다.

그러나 이들이 비협조적으로 나올 때는 어느 기억장치에 어떤 정보가 입력되어 있는 지, 어떤 프로그램을 사용하여 정보를 처리하였는지 수사기관이 판단할 수 없는 경우가 많다. 또한 시스템 운영자에게 자료를 제공받는 것은 국내로 제한되어 있으며, 국경을 초월하여 국가간에 이루어지는 사이버범죄에 대해서는 관련국가간의 국제수사공조와 형사관할권의 문제가 있다(이주성, 2003: 82). 이러한 문제들이 수사과정에서 얼마든지 일어날 수 있는 상황에서 객관적인 증거를 확보하는데 걸림돌이 되고 있다.

4. 현행 법규정에 따른 한계

컴퓨터와 관련된 수사에 있어서는 무엇보다도 증거확보가 가장 중요하다고 할 것이다. 컴퓨터 관련증거를 수집하기 위해 컴퓨터시스템 자체나 이에 의해서 처리된 전자적 기록, 자료(data)나 프로그램이 저장되어 있는 자기테이프나 디스켓과 같은 개별 저장매체에 대해 압수와 수색을 하는 것은 그리 어려운 일은 아닐 것이다. 그러나 데이터 그 자체나 프로그램에 대한 경우는 그리 간단한 문제가 아니다. 즉 이는 일반적으로 압수의 객체는 유체물인 증거물이기 때문에 정보가 수록된 자기테이프나 디스켓 자체는 유체물로써 압수의 대상이 되지만, 실제로 증거의 가치가 있는 것은 그 안에 수록된 무체물인 정보(data)이다. 따라서 무체물인 정보 그 자체에 대한 압수·수색에 있어 본래 물리적으로 관리 가능한 유체물을 압수·수색의 대상으로 규정하고 있는

형사소송법규칙을 그대로 적용할 수 있느냐가 문제가 된다. 이에 대해서 미국과 일본은 기본적으로 무체정보에 대한 압수·수색을 긍정하는 입장을 취하고 있지만 우리나라는 부정적인 입장을 취하고 있다.

실제로 대법원의 영남위원회 관련 국가보안법위반 사건의 판결문(대법원 1999. 9. 3. 선고, 99도2317 판결)을 보면 '컴퓨터 디스켓에 수록된 문건들에 대하여는 그 작성자 또는 진술자에 의하여 성립의 진정함이 증명된 바 없으므로 그 증거능력을 인정하여 유죄의 증거로 쓸 수 없다'고 판시하였다. 이 판결문은 디스켓 안에 있는 데이터는 압수 보관 및 출력과정에서 조작의 가능성이 있기 때문에 증거로써 인정할 수 없다는 것이다.

또 다른 문제는 인터넷이 광범위하게 사용되고 있는 현실에서 수사기관이 수사활동의 일환으로 컴퓨터통신을 어느 범위까지 허용할 것인지 문제될 수 있다. 컴퓨터 통신망에서의 뉴스 그룹 및 전자게시판(BBS)은 오늘날 또 하나의 여론형성매체로 여겨질 만큼 수많은 이용자들이 서로의 정보와 의견을 교환하고 있다. 이러한 게시판은 비록 많은 공동 이용자들에게 개방되어 있다고 하여도 ID와 패스워드를 통해서 이용자의 동일성 확인과정을 거치는 것은 그 이용이 제한되어 있어 이용이 허용되는 자 이외의 누구에 대해서도 자유롭게 접근권을 허용하고 있다고 할 수는 없을 것이다. 그러므로 컴퓨터시스템 이용자가 알지 못하는 사이에 법집행기관이 전기통신 사업자나 전자게시판 운영자의 동의만을 얻어 이용자의 전자게시판의 정보내용을 마음대로 지득할 수 있는지도 문제가 될 수 있다.

5. 제도적인 한계

앞서 살펴본 것처럼 범죄의 특성, 범죄의 수법, 증거확보, 현행 법규정에 따른 사이버수사의 한계도 있겠지만 제도적 한계, 즉 부족한 전문수사인력, 비전문적인 수사교육, 불충분한 예산 등으로 인해 사이버범죄에 대응하는데 상당한 문제점이 노출되고 있다. 여기에서는 사이버경찰의 전문수사인력, 전문수사교육, 예산으로 나누어 살펴보면 첫째, 사이버경찰의 조직은 그간의 사이버테러형 범죄수사경험을 바탕으로 수사뿐만 아니라 예방과 기법개발 등 종합적으로 대응하고자 종전의 사이버범죄수사대를 사

이버테러대응센터로 확대 개편하였다. 사이버테러대응센터로 확대 개편한 후 사이버수사시스템의 확충을 위해 컴퓨터증거분석시스템, 전국에 사이버수사네트워크 구축 등 과학적 사이버범죄의 수사를 위한 첨단 인프라를 구축하였다.[15] 그리고 전국 14개 각 지방경찰청에는 사이버수사대가 설치되어 운영되고 있다. 여기에 근무하고 있는 사이버경찰 인력현황을 보면 <표 3-1>과 같다.

경찰청 사이버테러대응센터에 69명(11.5%), 전국 14개 지방경찰청에는 71명(11.8%), 전국 경찰서에는 460명(76.7%), 총 600명의 수사관을 배치하여 사이버범죄에 대응하고 있다.[16] 전국 14개 지방경찰청을 보면 서울경찰청을 제외한 각 지방경찰청의 사이버수사요원은 3~5명에 불과하며 심지어 2명이 근무하는 곳도 있다. 또 전국 231개 경찰서를 보면 평균 2명 정도가 사이버수사요원으로 근무하고 있어 급속도로 증가하는 사이버범죄에 대응하기에는 터무니없이 부족한 인력이라고 할 수 있다.

<표 3-1> 지방경찰청별 사이버경찰 인력현황

(단위 : 명)

구분	계	서울	부산	대구	인천	울산	경기	강원	충북	충남	전북	전남	경북	경남	제주
계	531	85	33	21	20	8	64	37	26	42	32	55	52	48	8
지방경찰청	71	23	5	5	4	2	4	3	4	4	2	3	4	4	4
경찰서	460	62	28	16	16	6	60	34	22	38	30	52	48	44	4

출처) 경찰청이 2001년도 국회 행정자치위원회 하순봉의원에게 제출한 국정감사자료.

또한 전국에 있는 사이버범죄 수사요원에 대한 학력을 살펴보면 <표 3-2>와 같다. 경찰청에는 총 69명 중 61명(88.4%), 전국 지방경찰청에는 총 71명 중 38명(53.5%), 전국 경찰서에는 총 460명 중 148명(32.2%)이 4년제 이상의 학력을 소지하고 있다. 주로 일선 경찰서에는 고졸출신이 460명 중 234명으로 50.9%, 경찰청에 전문대졸 이하 8명으로 11.6%를 차지하고 있다. 상급기관으로 갈수록 4년제 이상 고급인력들이 많이 편

15) 서울, 부산, 대구, 인천, 울산, 경기, 강원, 충북, 충남, 전북, 전남, 경북, 경남, 제주 등 전국 14개의 지방경찰청에 두고 있다(경찰청 http://www.ctrc.go.kr/local/local01.jsp).

16) 대검찰청 컴퓨터수사부서의 인원 현황을 보면 대검찰청 28명, 서울지방검찰청 34명, 전국지방검찰청 87명으로 총 149명이 근무하고 있다(대검찰청 내부자료 2002 기준).

중되어 있는 것도 문제점으로 지적할 수 있겠다.

<표 3-2> 사이버범죄 수사요원 학력

(단위 : 명)

구분	계	고등학교	전문대	대학교	대학원
계	600	252	101	233	14
경 찰 청	69	4	4	55	6
지방경찰청	71	14	19	34	4
경 찰 서	460	234	78	144	4

출처) 경찰청이 2001년도 국회 행정자치위원회 하순봉의원에게 제출한 국정감사자료

둘째, 전문수사인력을 양성하는 교육기관으로서 경찰수사보안연수소가 있다. 이 기관에서는 사이버범죄 수사과정을 중급(경위 이하), 고급과정(경정 이하)을 두어 사이버 추적 수사기법 등을 배양하고 사건수사의 필수자료 획득방법 및 분석요령 및 분야별로 권위 있는 전문가를 초빙하여 실습위주의 교육을 하고 있다.[17] 그러나 경찰수사보안연수소에서 많은 전문인력을 양성한다는 것은 현실적으로 한계가 있으므로 경찰교육기관[18]간 특성에 맞는 수사교육 역할분담과 교육의 내실을 기하는 것이 무엇보다도 중요하다.

<표 3-3>에서 수사전문교육현황에서 교육내용을 보면 사이버범죄수사과정(고급), 사이버범죄수사과정(중급)이 있으며, 이 과정의 교육시간은 2주간에 걸쳐 총 57시간 교육을 받게 된다. 사이버범죄수사과정(중급)의 교육내용을 살펴보면 크게 운영체제(Unix I, Windows NT)분야, 실무(컴퓨터범죄 수사사례, 사이버범죄 증거수집 및 분석)분야, 교양(컴퓨터범죄와 법률, 최근 IT 동향 및 전망)으로 나눌 수 있다. 특히 운영체제분야에서 Unix, Windows NT를 배우는 시간은 28시간에 불과하다.

많은 사람들은 운영체제인 Windows 98/ME를 많이 사용하고 있다. 이러한 운영체제에 익숙해져 있는 상태에서 근본적으로 설계부터 전혀 다른 Windows NT를 12시간만에 모든 교육이 이루어진다는 것은 현실적으로 불가능하다. 특히, Unix 운영체제는

17) 일본은 하이테크범죄에 관한 전문인력을 육성하기 위해 경찰대학 부속 경찰정보통신학교를 운영하고 있다. 여기에서는 매년 초 500명 이상의 경찰직원(주로 기술계 직원)에게 계통적인 전문교양을 실시하여 직원 1인 1인의 능력 및 기술력을 갖춘 인재의 육성에 임하고 있다 (渡邊敏晃, 2002: 145-155).

18) 경찰대학, 경찰수사보안연수소, 경찰종합학교, 중앙경찰학교, 지방경찰학교 등

개인용 운영체제가 아니라 대형 컴퓨터와 워크스테이션에서 사용하는 기업용 운영체제라는 것을 감안한다면 이 짧은 시간에 제대로 된 교육이 이루어진다는 것은 상당히 힘들다. 따라서 이 과정들은 전문인력을 양성하는 차원의 교육이 아니라 대부분 직무수행에 필요한 단편적인 정보와 지식을 습득하는 수준에 불과하다.

<표 3-3> 경찰수사보안연수소 수사전문교육현황

교육과정	교육대상	교육내용	교육시간	교육기간	교육횟수	교육인원
사이버범죄수사과정(고급)	경정이하	1. 컴퓨터 바이러스 및 백신	9	2주	1	50
		2. 컴퓨터 시스템 보안	9			
		3. Unix II	16			
		4. 사이버범죄 증거수집 및 분석	16			
		5. 최근 사이버범죄 동향 및 수사사례	4			
		6. 최근 IT 동향 및 전망	3			
사이버범죄수사과정(중급)	경위이하	1. 컴퓨터범죄와 법률	6	2주	6	150
		2. 컴퓨터범죄 수사사례	6			
		3. Unix I	16			
		4. Windows NT	12			
		5. Net work 하드웨어의 이해	8			
		6. 사이버범죄 증거수집 및 분석	6			
		7. 최근 IT 동향 및 전망	3			

출처) 경찰청(2002). 경찰백서. 128.

셋째, 사이버경찰의 조직, 전문인력의 양성, 전문화된 교육을 감당하기 위해서는 무엇보다도 중요하고 필수적인 요소가 바로 예산부분일 것이다. 그런데 경찰치안수요의 변화와 경찰 역할의 증대에도 불구하고 예산이 절대적으로 부족한 실정이다. 이러한 예산 부족은 낙후된 경찰장비, 낮은 보수체계, 과중한 근무시간과 업무량 등으로 직결되어 경찰의 사회안전관리나 민생치안활동을 어렵게 만들고 있다.

<표 3-4>에서 보는 바와 같이 지난 10여년 동안 범죄발생건수는 1991년보다 56.9%나 증가한 반면에, 정부예산 중에서 경찰예산이 차지하는 비율을 보면 1991년 전체 예산의 5.6%이던 것이 2002년도에는 4.7%를 점하고 있다. 또한 <표 3-5>에서 경찰청 사이버수사의 예산을 보면, 2002년도 예산액은 28억 1,300만원으로 전년도보다 9억 1,500

만원이 줄어들어 24.5%가 감소되었다. 이는 당초 2002년도 예산요구액 132억 5,800만원 중 21.2%만이 예산에 반영된 것이다.

<표 3-4> 범죄발생건수 및 경찰인력 및 예산의 변화추이

구 분		1991년	1993년	1995년	1997년	1999년	2001년	2002년
경찰인력(명)		84,931	90,108	90,639	89,629	90,623	90,819	91,187
범죄발생건수(건) ('91년대비증가율%)		1,185,648	1,304,349 (10.0)	1,329,694 (12.2)	1,536,652 (29.6)	1,654,064 (39.5)	1,860,687 (56.9)	-
1인당 담당인구(명)		516	489	503	516	518	526	527
예산	경찰예산(억) (전년대비 증가율%)	1조7,643	2조3,599 (33.8)	2조9,363 (24.4)	3조6,078 (22.9)	3조4,754 (-3.7)	4조3,847 (26.2)	4조9,279 (12.4)
	정부예산(억) (전년대비 증가율%)	31조3,823	38조5,000 (22.7)	49조9,879 (29.8)	67조5,786 (35.2)	83조6,852 (23.8)	94조1,246 (12.5)	105조8,767 (12.5)
	경찰예산 /정부예산(%)	5.6	6.1	5.9	5.3	4.2	4.7	4.7

출처) 국회사무처(2002b). 2002년도 국정감사자료집(VII) - 행정자치위원회 소관: 221.

<표 3-5> 2002년도 경찰청 사이버수사의 예산현황

(단위 : 백만원)

구 분		2001년			2002년		예산증감	
		요구	예산안	예산	요구	예산	증감	%
계		19,177	3,728	3,728	13,258	2,813	▽915	▽24.5
청별	경 찰 청	18,029	3,321	3,321	8,461	2,285	▽1,036	▽31.2
	지방경찰청	1,148	407	407	4,797	528	△121	△29.7
항목별	자산취득비	14,352	2,500	2,500	11,425	2,255	▽245	▽9.8
	연구개발비	2,733	200	200	231	-	▽200	▽100
	운 영 비	1,510	983	983	1,340	538	▽445	▽45.3
	시설비, 기타	581	46	46	262	20	▽26	▽56.5

출처) 국회사무처(2002b). 2002년도 국정감사자료집(VII) - 행정자치위원회 소관: 182.

정보통신 및 해킹기술의 급격한 발달에 대비한 수사장비의 지속적인 보강을 위한 예산이 대폭 삭감됨으로써[19], 사이버범죄수사에 필수적인 장비구축과 이에 따른 원활

19) <표 3-6> 2002년도 대검찰청 컴퓨터수사반 예산현황

(단위 : 백만원)

2001년 결산				2002년 예산
예산액	전년도 이월액	예산현액	지출액	
2,072	147	2,219	2,219	2,049

출처) 국회사무처(2002a). 2002년도 국정감사자료집(II) - 법제사법위원회 소관: 214.

한 수사활동에 큰 차질을 초래하고 있다. 또 주요장비의 효율적 운영을 위하여 필요한 관련 프로그램 개발에 필수적인 연구개발비의 부족으로 향후 디지털 증거의 파괴, 손실, 혼란 등 사이버범죄에 효과적으로 대응하기 어렵게 만들고 있다.

Ⅳ. 사이버경찰의 수사력 강화방안

1. 관련법규의 정비 및 보완

사이버범죄에 대해 현행 법률만으로 증거의 확보 등 여러 가지 문제점을 해결하는데 한계가 있다. 대표적인 문제점을 살펴보면 테러리스트들이 인터넷상의 각종 암호기술과 소프트웨어를 이용하여 테러공작정보를 일반 채팅룸을 통해 교환하는 경우와 같이 인터넷 암호사용시 수사가 곤란하며, 인터넷 카지노를 통하여 불법자금을 합법적 자금으로 세탁하는 행위에 대한 수사상 대응문제, 형사소송법상 압수수색물의 대상물을 물건(유체물)에 한정하고 있어 사이버 공간상에서 발생하는 증거조사방법상 애로사항이 바로 그것이다.

현재 우리 현행법과 특별법으로는 이러한 문제점을 해결하기에는 부족한 부분이 너무 많아 사이버 범죄의 전 분야를 포괄할 수 있는 일반법적인 성격을 가진 사이버범죄 기본법을 제정하는 것이 필요하다.

또한 컴퓨터 성능과 기술의 발전에 따라 개인이나 기업이 그 목적에 따라 다양한 형태로 컴퓨터를 이용하고 있는 현실에서 컴퓨터의 대용량화, 네트워크화 등 여러 가지 환경으로 컴퓨터 하드웨어를 압수하는 것이 점차 어려워지고 있는 실정이다. 압수된 자기테이프나 디스켓 그 자체는 유체물로서 압수대상이 된다는 것은 당연하다. 그러나 자기테이프나 디스켓 안에 저장된 데이터나 프로그램은 무체물이기 때문에 그 자체로서는 압수의 대상이 될 수 있는지에 대해서는 앞서 전술한 바가 있다.

일본의 형사소송법 제199조의 해석에 있어서 학설은 무체정보도 압수의 대상이 되며, 또한 증거능력을 인정하고 있다고 한다(이철, 1995: 211). 그러나 앞서 살펴보았듯이 영남위원회 관련 국가보안법위반 사건에서 대법원은 증거로 인정할 수 없다는 판결을 내려 증거능력을 부정한 바 있다.

그러나 영국의 경찰 및 형사증거법 제19조제4항과 제20조를 보면, 범죄에 관한 증거로서 은닉, 개변, 또는 파괴를 막기 위하여 필요하다고 믿을 만한 합리적인 근거가 있을 때에는 컴퓨터에 내장되어 있어 당해 장소로부터 접근할 수 있는 모든 정보에 대하여 이를 취거하거나 읽을 수 있도록 출력할 것을 요구할 수 있다'고 규정하고 있다(이종상, 2000: 12). 따라서 무체정보를 영국과 같이 증거확보에 있어서 수사관이 정보입력자에게 데이터의 내용을 읽을 수 있도록 출력을 요구할 수 있는 법적 장치를 마련하는 것도 한 가지 방법이 될 수 있을 것이다.

근본적으로 컴퓨터 전자기록에 대한 압수·수색 절차와 방법, 인터넷의 주소(IP address)에 대한 압수·수색, 압수된 전자기록의 증거로서의 가치부여 등 컴퓨터와 관련된 제반 규정을 둠으로써 입법론적으로 문제를 해결하는 것이 가장 바람직할 것이다.

2. 전문수사인력 양성 및 확보

사이버범죄를 담당하는 수사요원들은 상당한 수준의 컴퓨터지식과 정보통신기술분야의 높은 지식과 숙련된 경험이 필요하며, 이러한 지식과 경험을 바탕으로 문제를 해결해 나갈 수 있는 능력을 지닌 사람이라야 한다. 한 특정분야에서의 높은 지식과 숙련된 경험을 지닌 전문인력을 양성하고 확보하는 것은 경찰수사력 강화와 관련하여 매우 중요한 일일 것이다. 따라서 교육과 훈련을 통한 내부전문인력 양성과 특정한 분야에 전문지식을 갖춘 외부인력의 활용 측면에서 살펴보면 첫째, 세계화와 정보화가 촉진되면서 경찰이 미처 전문인력을 키워내지 못한 분야에서의 범죄발생은 증가할 것이며, 기존에 발생하고 있는 많은 범죄들을 해결하기는 더욱더 어렵게 될 것이다. 이러한 전문인력을 양성하는데는 교육과 훈련을 통한 내부 인력을 양성하여 전문화시킬 필요가 있다.

전문인력을 양성하는데 무엇보다도 전문교육과 훈련이 제일 중요하다. 앞에서도 살펴본 것처럼 현재 경찰수사보안연수소에서 대부분 담당하고 있다. 그러나 사이버수사 전문인력을 양성하는데 경찰수사보안연수소에서 모두 감당하는 것은 불가능하다. 그래서 국내외 전문기관의 위탁교육을 강화할 필요가 있다. 현재도 다양한 형태의 위탁교

육이 실시되고 있다.[20] 경찰업무와 관련성이 높은 특수전문분야 위주로 위탁교육을 실시한다는 입장에서 대상자를 비교적 엄격하게 선발하고 있으며, 위탁교육 이후 교육이수자를 관련부서에 배치하는 등의 사후관리를 하고 있다(김병준 · 이승현 · 이동규 · 장영길, 2002: 69).

그러나 2001년도 교육기관은 국방대학원을 포함한 15기관이며, 피교육자는 경무관에서 순경에 이르기까지 모두 3,851명에 달한다. 그러나 국내 위탁기관의 교육과정을 보면 일반적인 경찰직무수행에 필요한 단편적인 교육 이외에 사이버범죄수사와 관련된 전문교육과정이 없어 사이버범죄수사의 전문인력양성과는 거리가 멀어 보인다. 또 해외연수는 장기위탁교육[21]과 단기해외연수[22]로 나눌 수 있다. 이러한 위탁교육과정이나 단기해외연수의 대상은 경사~총경까지이며, 교육기간은 2월~2년 6월까지이며, 횟수는 1번, 인원은 1명에 불과해 장기와 단기를 합쳐 1년에 20명 남짓 파견하는 것으로 되어 있다.

세계화 추세와 전문화 추세에 비추어 볼 때 경찰행정의 환경변화를 고려하여 해외파견인원을 늘리는 동시에 전문교육기관과 교육과정[23]을 다양화하고 교육기간을 늘리

---

20) 2001년 서울지방경찰청 사이버수사대의 위탁교육을 살펴보면 한국정보보호진흥원(구 한국정보보호센터) 주관 「제7회 정보통신망 정보보호 워크숍」 10명 참석(2001년 4월 17일~18일), 서울시내 31개 경찰서 사이버 수사요원 62명 사이버수사 직무교육 실시(2001년 4월 19일~5월 11일), 경찰청 주관 전국 사이버수사요원 직무교육 참석(2001년 4월 25일~4월 26일), 한국과학기술원(KAIST) 주관 Infosec Olymfair 2001 WORKSHOP 10명 참석(2001년 5월 16일~5월 18일), 정보통신교육원 주관 공무원정보보호교육과정 10명 참석(2001년 6월 11일~7월 6일), 제2차 공무원정보보호교육과정 교육 24명 실시(2001년 7월 9일~8월 3일), 사이버수사 특채요원 5명 수사직무학교 교육 실시(2001년 9월 17일~9월 29일), 정보통신교육원 주관 제2기 공무원 정보보호교육 심화과정 2명 이수(2001년 10월 8일~10월 27일), 경찰청 주관 전국 사이버수사요원 직무교육 및 사이버테러대응 심포지엄 17명 참석(2001년 10월 23일~10월 24일), 하이텔 정보보호교육센터 주관 Mobil Internet Security 세미나 6명 참석(2001년 10월 27일)(서울지방경찰청 사이버수사대 홈페이지 http://www.cybercrime.go.kr/intro/intro_03.htm).

21) 미국(한국적 특성에 적합한 경찰제도의 개선방안, 사이버범죄 대응방안, 민간경비 활성화 방안, 국제성범죄 협력방안의 4개 과정), 영국(범죄발생현황 및 추세분석 연구의 1개 과정), 일본(국제성범죄 공조수사방안, 정책연구대학원의 2개 과정), 프랑스(사법경찰관의 지위와 권한 연구의 1개 과정), 독일(통일과정에서의 경찰조직 개편의 1개 과정), 중국(중국의 자치경찰제도의 1개 과정), 싱가폴(범죄발생현황 및 추세분석의 1개 과정), 칠레(경찰학 간부과정의 1개 과정) 등 총 12개 과정(김병준 · 이승현 · 이동규 · 장영길, 2002: 71).

22) 미국(FBI 국립학교, 연방위난관리국, 미시간주립대), 호주(NSW 경찰청), 독일(베를린대학, 뮌헨대학), 일본(경시청), 중국(인민공안대학, 정법대학) 등이다(김병준 · 이승현 · 이동규 · 장영길, 2002: 71).

23) <표 4-1> 한국정보통신교육원 교육과정

는 등의 작업이 선행되어야 할 것이다.

둘째, 현재 경찰인력은 오프라인범죄에 초점이 맞추어져 있다. 그러나 현재 일어나고 있는 사이버범죄의 유형을 살펴보면 오프라인에서 일어나는 범죄유형이 사이버공간에서도 많이 일어나고 있는 추세이다. 이러한 추세에 맞추어 오프라인범죄 수사인력 중에서 컴퓨터지식을 갖춘 경찰인력을 선발해서 사이버범죄를 담당하게 하는 것이 바람직할 것이다. 그러나 현실적으로 사이버범죄를 수사하기 위해서는 고도의 컴퓨터지식과 기술이 요구된다. 이러한 전문적인 인력을 내부에서 선발하여 교육시킨다면 많은 교육시간과 비용이 수반될 것이다. 따라서 이러한 문제를 해결하기 위해서는 외부로부터 전문인력을 적극 활용하는 것이 더 바람직할 것이다. 외부 전문인력 확보의 주요 통로가 되는 것은 특별채용제도라 할 수 있다.

일본에서도 정보통신기술이 뛰어난 민간기술자의 채용, 경찰과 기업간의 인사교류 등에 의해 우수한 전문인력을 확보하고 있다(後藤啓, 2000: 17). 실제로 일본에서는 수사요원의 탄력적 채용시스템을 도입하여 1993년부터 컴퓨터 회사에 근무하던 중견전문인 3명을 경찰관으로 특채하여 성공을 거두자 사이버범죄 수사요원 확보에만 국한하지 않고 석·박사학위 소지자, 외국어에 능통한 자, 컴퓨터소프트웨어 개발이 가능한

구분	과목	주요내용
일반과정	정보보호입문	정보보호개론 정보보호 동향
	운영체제 보안	Linux/UNIX 운영체제 및 활용기법 Windows98/NT/2000, Linux/UNIX 운영체제의 보안 취약점 데이터보호, 관리 및 추적기법
	네트워크 보안	네트워크개론 및 TCP/IP 해킹 및 컴퓨터바이러스 동향 침입차단시스템(Firewall) 개요, 기능 및 설치 운용 침입탐지시스템(DS) 개요, 기능 및 설치 운용 VPN 해킹 대응분석 및 사례연구 전자메일 보안 전자서명 컴퓨터바이러스 동향 및 치료기법
	보안시스템구축	정보보호 구축방법 및 사례분석
전문과정		각 부처의 요구에 따라 별도의 교과과정의 편성
심화과정	사이버수사기법 등	각 부처의 요구에 따라 별도의 교과과정의 편성

출처) 한국정보통신교육원(http://www.aiit.or.kr).

자 등을 특채하였다. 그리고 이들을 컴퓨터수사관, 재무수사관, 국제수사관 등으로 적극 활용하고 있다(조병인, 2000: 158-159).

그러나 우리 나라에서는 특별채용시 순경 또는 경장으로 채용하는 것이 대부분이다.[24] 특히 전문인력 확보와 관계가 깊은 사이버수사요원의 특채에 있어서도 마찬가지다. 사이버수사요원의 특채는 2000년도 경사 3명, 경장 24명, 2001년도 경장 48명이 특채되었다. 보다 전문적인 인력을 확보하기 위해서는 일반적인 특채방식만을 통해 전문인력을 확보할 것이 아니라 스카우트 방식을 도입해 관련전문회사로부터 특정한 분야에 정통한 전문인력을 적극적으로 확보할 필요성도 있을 것이다. 또한 이들에 대해 현실적인 처우가 뒤따라야 할 것이다. 현실적인 처우가 뒤따를 때 외부 전문가들로부터 많은 관심을 받게 될 것이고, 이들을 확보하는데 큰 어려움이 없을 것이다. 물론 이러한 우수한 능력을 지녔다고 해서 무조건 범죄수사에 능한 것은 아닐 것이다. 오히려 첨단기술능력을 수사능력으로 발전시키지 못하면 고급인력의 낭비와 국가 예산만 낭비될 가능성도 크기 때문에 신중한 검토도 함께 뒤따라야 할 것이다.

3. 사이버범죄 수사예산의 확충 및 체계적 집행

경찰청에는 사이버테러대응센터를 비롯하여 전국 14개의 지방경찰청에 사이버수사대를 두고 있으며, <표 3-5>에서 본 바와 같이 2002년도 132억 5,800만원 요구에 28억 1,300만원 예산이 책정되었다. 그리고 대검찰청에는 인터넷범죄수사센터를 비롯하여 전국 14개의 지방검찰청에 컴퓨터수사부·반을 두고 있으며, 2002년도 20억 4,900만원 예산이 책정되었다.[25]

사이버공간에서의 역기능 제어를 위한 실무적 종합 대응기구라 할 수 있는 경찰청 사이버테러대응센터의 특수성과 경찰의 효율적인 사이버범죄예방 및 범인 검거 활동

---

24) 경찰청 인사교육과 내부자료(2001)에 따르면 과거 10년간(1992~2001) 전체 특채인원 2,677명 가운데 순경이 1,176명으로 44%를 차지하고 있고, 경장이 1,319명으로 전체의 약 49.3%를 차지하고 있다. 경정 이상으로 채용된 경우는 전체 31명으로 1.2%를 차지하고 있다.

25) 뒤늦게 경찰청은 신규사업비로 이메일 추적기법개발비 3억원, 지방경찰청 장비구입비 1억 2,600만원, 경찰서 장비구입비 2억 2,000만원, 무선인터넷이용범죄 수사장비구입비 4억 6,300만원의 예산을 편성하였다(안병옥, 2002: 61).

을 위해서는 현재의 예산으로는 사이버범죄수사에 어려운 점이 많다. 또한 경찰청 사이버테러대응센터와 대검찰청의 인터넷범죄수사센터는 유사한 기능을 수행하고 있다. 이러한 유사한 기능을 수행하는 검찰과 경찰의 양 기관이 합해서 연간 50여억원의 예산을 사용하고 있는 것은 비현실적인 예산운영이라 하겠다.

현실성 있고 체계적인 예산확보가 이루어져야 할 것이다. 정보통신 및 해킹기술의 급격한 발달에 대비하기 위해서도 그렇게 되어야만 비로소 사이버범죄 전담수사요원의 교육, 국외연수, 수사장비의 첨단화 및 지속적인 수사기법의 연구개발 등이 제대로 이루어질 수 있을 것이다. 그럼에도 불구하고 관련 예산이 제대로 반영되지 않아 날로 지능화·국제화되고 있는 사이버범죄에 효과적으로 대처하고 적정한 수사활동이 이루어지는데 차질이 빚어지고 있는 현실이다.

우선적으로 최소한 근무여건 조성, 장비의 현대화, 전문인력 확보를 위한 관련 예산의 확보와 지원이 우선되어야 할 것으로 보인다.

4. 사이버수사기법 개발 및 최첨단 장비 도입

사이버범죄자들은 고도의 컴퓨터·네트워크 전문기술을 가지고 범죄를 행한다. 이러한 사이버범죄에 대응하기 위해서는 끊임없는 노력이 필요한데 여기에서는 수사력강화를 위한 방안으로 첫째, 현재 경찰청의 기법개발실(팀)에서 다양한 수사기법을 개발하여 대응하고 있다. 그러나 사이버범죄자들은 상당한 컴퓨터지식과 기술을 가지고 범행을 저지르기 때문에 그 수법이 복잡하며, 여러 가지 원인으로 인해 사이버범죄수사가 불가능한 사건도 허다하다.

2003년 경찰청 소관 예산안 검토보고서(안병옥, 2002: 62)에 따르면 2002년 1월~8월까지 사이버범죄수사가 불가능한 사건은 로그부재(679건), 공중인터넷망(882건), 외국IP(219건), 기타(1,391건) 등 총 3,171건에 달한다. 이러한 사이버범죄수사가 불가능한 사건의 구체적 원인은 일부 인터넷 서비스 제공업체(ISP)의 경우 비용부담 등을 이유로 접속로그기록을 보존하지 않거나 로그확인은 가능하나 용의자 위치가 PC방, 도서관 등 공중인터넷망을 이용하거나 또는 범죄용의 IP가 외국일 경우 사실상 수사가 불가능하기 때문이다.

'뛰는 놈 위에 나는 놈 있다'는 말도 있듯이 우리의 현실세계에서는 '나는 놈'이 범죄자의 범죄수법이라면 '뛰는 놈'은 수사기관의 수사기법이라 할 수 있다. 이러한 현실에서 '나는 놈'의 범죄수법들을 대응하기 위한 수사기법들을 개발하는 데는 경찰의 힘만으로 해결될 문제가 아니다. 물론 경찰수사기관의 최우선 노력이 있어야 되겠지만 다양하면서도 고도의 기술적 수사기법을 개발하기 위해서는 경찰과 검찰, 한국정보보호진흥원·한국전산원·시스템 공학연구소(SERI)의 정부산하 연구기관, 한국전산망 협의회(KNC)의 협회, 삼성 데이터시스템(SDS)·LG-EDS의 민간 기업들과 종합적인 연구체제를 구축하여 지속적으로 사이버범죄의 수사기법들을 연구해야 할 것이다.

둘째, 최근 들어 사이버범죄자의 연령도 점점 낮아지고 그 수법도 악랄해지고 있어 범죄수사의 어려움은 날로 커지는 반면, 피해규모는 눈덩이처럼 커지고 있다. 그러나 사이버범죄를 담당하는 수사관들은 범죄자들에 대한 대응수단이 부족해 어려움을 겪고 있다.

사이버범죄자들은 고도의 컴퓨터지식과 기술을 바탕으로 범행을 저지르고 있기 때문에 우수한 인력과 최첨단 장비의 도입 및 활용이 무엇보다도 중요하다. 아무리 우수한 인력이 많아도 범죄자를 추적하고 증거를 확보하는데는 최첨단 장비의 도움이 필수적이다. 사이버범죄자들을 추적하고 증거를 확보하는데 기본적인 장비로서는 인터넷 서버, 라우터 등 통신장비, 해커추적 수사장비, RAID 백업장비, 수사용 노트북, 업무용 프린터, 칼라평판스캐너 등이 필요하다. 특히, 범죄자들이 컴퓨터시스템 내에 있는 데이터가 파괴될 경우, 이를 복구하고 추적할 수 있는 근거가 사라지므로 범죄수사가 어려워진다. 물론 범죄자들이 고의로 데이터를 파괴하지 않더라도, 컴퓨터시스템의 기억장치에서 데이터가 유실되는 경우가 허다하다. 컴퓨터시스템은 수많은 반도체들로 이루어져 있다. 여기에서 데이터를 기억하는 장치들, 즉 하드디스크(HDD), 플로피디스크(FDD), 주기억장치(DRAM), 플래쉬 메모리, 컴팩트디스크 등에서 데이터 파괴 및 유실이 될 때 데이터 복구시스템을 이용하면 된다.

사이버범죄수사를 위해서는 장애 유형별로 복구 책임자를 선정하고 담당자들의 배치와 수행 업무 등에 대해 여러 가지 시나리오를 미리 계획해야 한다. 또한 유사시 담당자들의 효율적인 복구업무 수행을 위해 필요한 장비 및 수행업무에 대한 자료 등도 적절한 곳에 배치하는 세심함도 필요하다. 심지어는 IT공급업체와의 업무 연계와 직원

들 상호간의 비상연락망 등 전시체제로 곧바로 돌입할 수 있는 모든 준비가 되어 있어야 할 것이다. 또 사이버테러를 미연에 방지하기 위해 인터넷상의 위협요소를 사전에 수집·분석하고, 해킹 공격유형 자료를 분석해 해킹이나 바이러스에 대한 피해를 최소화하는 '사이버테러 조기탐지 및 분석시스템'을 도입하여 전국 14개 지방경찰청의 네크워크에 탑재해 활용할 필요가 있다.

V. 결 론

이상에서 사이버수사의 방법, 아직 비 정형화된 사이버수사의 절차를 설계해 보고, 사이버범죄의 수사상 한계와 사이버경찰의 수사력 강화방안을 몇 가지 제시해 보았다.

우선 새로운 형태로 변화해 가는 사이버범죄행위를 단속하고 효율적으로 수사하기 위해 경찰청의 사이버테러대응센터의 조직을 전문화된 조직으로 개편하는 것도 중요하겠지만 무엇보다도 사이버범죄를 수사하는 수사요원의 끊임없는 수사기법개발과 노력이 먼저 선행되어야 할 것이다. 그러나 아무리 훌륭한 수사기법을 가지고 범죄를 검거하고 증거를 확보한다고 할지라도 현행 법규정의 미비로 수사절차상 많은 문제가 발생하고 있어 시급히 현행 법규정을 보완할 필요가 있다.

그리고 현재 사이버범죄가 급속히 증가하고 있는 반면에 이에 대응하는 전문인력은 턱없이 부족한 실정이다. 물론 내부인력 중 적격자를 선발하여 전문인력을 양성해야 하겠지만, 이렇게 할 때 너무 많은 시간과 비용이 수반하므로 특정분야에 전문지식을 갖춘 외부전문인력을 적극적으로 스카우트를 하여 활용하는 것도 한 가지 방안이 될 것이다.

마지막으로 사이버공간에서의 역기능 제어에 체계적이고 종합적으로 대응하기 위해서는 현재의 예산으로는 어려운 점이 많아 현실성 있는 예산확보와 집행이 필요하다. 즉 최소한 근무여건 조성, 수사장비의 첨단화, 수사기법 연구개발비, 수사요원의 교육지원비 등 전문인력 확보를 위한 관련예산의 확보와 지원이 우선되어야 할 것이며, 사이버범죄수사의 효율성 제고를 위해서도 국가예산을 체계적으로 집행하여야 할 것이다

그러나 사이버범죄를 근원적으로 줄이기 위해서는 사후 조치보다는 사전 예방조치

에 초점이 맞추어져야 할 것이다. 또한 수사기관의 단속, 처벌 등 타율적 규제가 아닌 인터넷서비스 제공자나 이용자 스스로의 자율적 규제를 통한 건전한 사이버문화가 정착될 수 있도록 다 같이 노력해야 할 것이다.

참 고 문 헌

경찰청(2002).「경찰백서」. 서울: 경찰청.

국회사무처(2000). 2000년도 국정감사자료집(Ⅵ)-행정자치위원회 소관. 국회사무처 예산정책국. 329-338.

국회사무처(2001). 2001년도 국정감사자료집-행정자치위원회 소관. 국회사무처 예산정책국. 163-175.

국회사무처(2002a). 2002년도 국정감사자료집(Ⅱ)-법제사법위원회 소관. 국회사무처 예산정책국. 212-217.

국회사무처(2002b). 2002년도 국정감사자료집(Ⅶ)-행정자치위원회 소관. 국회사무처 예산정책국. 172-182.

김병준·이승현·이동규·장영길(2002). 경찰전문인력 확보 및 운영대책 (연구보고서 02-02). 용인: 치안연구소.

김상우(1996). 미국에서의 컴퓨터에 대한 압수·수색 개관. 해외연수검사연구논문, 12, 219-264.

박경식·천대영(2002).「경찰수사학」. 용인: 경찰대학.

배종대·이상돈(2004).「형사소송법」. 서울: 홍문사

안병옥(2002). 2003년도 경찰청 소관 예산안 검토보고서. 국회 행정자치위원회.

오기두(1997).「형사절차상 컴퓨터관련 증거의 수집 및 이용에 관한 연구」. 서울대학교 대학원 박사학위논문.

이종상(2000).「컴퓨터 데이터 압수·수색에 관한 연구」. 서울대학교 대학원 석사학위논문.

이주성(2003).「사이버범죄의 수사절차상 문제점」. 호남대학교 석사학위논문.

이 철(1995).「컴퓨터범죄와 소프트웨어보호」. 서울: 박영사.

이황우·조병인·최응렬(2003).「경찰학개론」. 서울: 한국형사정책연구원.

조병인(2000). 사이버경찰에 관한 연구 (연구보고서 00-1). 서울: 한국형사정책연구원.

최응렬(1990).「컴퓨터 조작범죄의 유형과 그 대책에 관한 연구」. 동국대학교 대학원 연구논집. 20, 87-107.

하태훈・강동범(1998). 정보사회에 대비한 일반법 연구(Ⅱ). 서울: 정보통신정책연구원.

Bennett, Wayne W. and Hess, Karen M.(2001). Criminal Investigation. 6th ed. Belmont, CA: Wadsworth/Thomson Learning.

Parker, Donn B.(1983). Fighting Computer Crime. New York: Charles Scribner's Sons.

Sullivan, Scott. "Policing the Internet.." FBI Law Enforcement Bulletin, Vol. 68, No. 6, June. 18-21.

廣田耕一(2000). ハイテク犯罪捜査における技術支援の現狀と課題について. 警察學論集. 53(8), 61-72.

貴志浩平(1998). ハイテク犯罪の捜査に關する諸問題. 警察學論集. 51(7), 99-119.

渡邊敏晃(2002). ハイテク犯罪と關う技術職員の育成. 警察學論集. 55(7), 145-155.

英太郎(1999). ハイテク犯罪捜査における技術的留意事項. 警察學論集. 52(3), 132-150.

後藤啓(2000). ハイテク犯罪の現況と對策. 警察學論集. 53(8), 1-21.

砂田務(1998). ハイテク犯罪に對處するための技術的支援體制の整備. 警察學論集. 51(7), 54-66.

디지털타임즈(2003). 정부 정보화사업 주관부처 다툼‥ "우리가 적임"…주도권 확보 경쟁.「디지털타임즈」. 8. 11.

한겨레(2001). "사이버범죄 급증, 검거율 낮아".「인터넷 한겨레」. 8. 31.

Abstract

The Limited Investigation of the Cyber-police and the Reinforcement of its Investigative Ability

Choi, Eung Ryul · Hwang, Young Gu

The cyber-crime is one of the results occurring from the increased dependency toward information-telecommunication devices. Currently, the Korean National Police Agency and many other related law enforcement agencies have made efforts to respond against the cyber-crimes. However, the number of cyber-crime is increasing steadily.

The worse problem is that the arresting rate for the cyber-crime has been decreased than before. The reasons of decreasing arresting rate come from many different kinds of cyber-crime methods with the developed computer and network technology. Also, the easy concealment of the cyber-crime by the violater and the difficulty of specification against the data objected to search and seizure make the crackdown difficult. The other difficulties come from the lack of professionally trained investigators, the lack of high-technological investigation devices, and the failure of the technology development for the search and seizure of evidences because of the budget deficit. That is to say, these phenomenon show the comprehensive problem of the cyber-police system.

Accordingly, to respond against newly changed cyber-crime activities and to investigate effectively, the cyber-police has to take consideration into the professional reorganization of the cyber-police, the development of the investigation technology, and the adjustment of current cyber-crime laws. Most importantly, the cyber-police needs the high-technological investigation devices, the development of the investigation methods, and the training for the professional human resources with the enough budget support.J

Key Word : cyber-crime, cyber-police, reinforcement of investigative ability