韓國 컴퓨터情報學會 論文誌
第13卷 第3號, 2008. 5.

2008-13-3-5-1

경찰의 사이버범죄에 대한 효율적 대응방안에 관한 연구

박 창 욱*

A Study on Effective Response of Police Officer against Cybercrime

Park, Chang Wook *

요 약

현대사회 범죄의 주된 경향으로써 사이버범죄의 발생 빈도가 증가하고 있다. 사이버공간을 통해 단순범죄에서부터 범죄기술에 있어서 고도의 전문화된 범죄에 이르기까지 다양하게 나타나고 있다. 인터넷 보급률이 확대되면서 일반인들이 정보매체에 접근할 수 있는 기회가 많아지고 범죄와 무의식적으로 연관될 수 있는 가능성이 높아지고 있다는 점에서 그 심각성이 매우 크다고 할 수 있다.

본 논문에서는 사이버범죄의 여러 가지 유형과 특징들을 통해서 나타나는 사이버범죄의 현황과 사이버범죄에 대한 경찰 대응상의 문제점에 대해서 검토하고, 경찰의 효율적 대응방안을 제안하였다.

Abstract

In this modern society, a main tendency of crime is to increase in the incidence frequency of cyber crime. Varied criminal techniques from simple crimes to highly specialized crimes appear through cyber space. With the expansion of Internet spread, ordinary people increasingly have an opportunity to have access to information media and their possibilities to be involuntary associated with crimes get higher. In this sense, its seriousness is great.

This study examined the present state of cyber crimes that appear through their several types and characteristics and the problems of police response to cyber crimes. and suggest effective response of police officer

▸ Keyword : 사이버범죄(Cyber Crime), 하이테크범죄(Hi-Tech Crime), 익명성(Anonymity), 암수범죄(Hidden Crime), 사이버스토킹(Cyber Stocking)

• 제1저자 : 박창욱
• 접수일 : 2008. 2. 19, 심사일 : 2008. 3. 31, 심사완료일 : 2008. 5. 24.
* 원광대학교 대학원 경찰행정학과 박사과정
* 본 논문은 한국컴퓨터정보학회 제37차 동계학술대회에서 발표한 내용을 토대로 수정·보완하여 재구성한 것임.

Ⅰ. 서 론

현대사회 범죄경향의 주된 양상으로써 사이버범죄의 증가를 들 수가 있다. 사이버공간이 정보와 지식교환의 주요수단이 되고, 일반인들의 정보매체에 접근 및 활용가능성이 높아짐에 따라 무의식적으로 범죄와 연관될 가능성이 높아지고 있다.

사이버범죄의 양상은 단순범죄에서부터 고도의 전문화된 지능범죄에 이르기까지 다양하게 나타나게 되는데, 사이버공간이 가지고 있는 특징적인 면들과 매우 관련성이 높다.

다시 말해서 사이버공간에서 일어나는 범죄는 행위자의 신분이 노출되지 않기 때문에 범죄행위가 더욱 대담하게 나타나게 낸다. 이러한 특징은 사이버윤리의식이 완성되지 않고, 상대적으로 인터넷사용빈도가 높은 청소년들에 의해 '악성댓글'과 '사이버명예훼손'과 같은 사생활 침해의 범죄와, 고도로 전문화된 범죄 형태로써 '바이러스·해킹'과 같은 기관전산망 침투범죄 등의 범죄 형태로 나타나게 된다.

또한 사이버공간에서 발생하는 범죄는 행위지와 발생지가 일치하지 않고 범죄행위가 신속하고 폭넓게 파급됨으로써, 지상에서 일어나는 범죄에 비해 그 피해의 정도가 더욱 심각하다고 할 수 있다.

이러한 사이버범죄에 대하여 형사사법의 제 부문 중에서, 경찰 중심의 효율적 대응의 필요성이 높아지고 있는데, 그것은 오늘날 현대 형사사법체계의 마그나카르타라고 불리는 "죄형법정주의"의 원칙에서 기인된 것일 것이라 추정된다. 즉 과거 '복수'와 '죄형전단주의' 시대의 폐해를 타파하기 위해 법에 정함이 없으면 아무리 그 행위가 비도덕적이며 몰가치적이고 막대한 경제적 피해를 입혔다고 하더라도 처벌할 수 없게 되는데, 사이버범죄의 경우는 명백히 비도덕적이고 몰가치적이면서 막대한 경제적 피해를 입힘에도 불구하고 법 규정의 부재로 처벌할 수 없게 되는 폐단이 나타나고 있다. 다시 말해 과학기술의 발전을 법규와 정책이 뒷받침 되지 못하는 괴리현상이 발생하게 될 것이다.

하지만 현실적으로 실효적 처벌은 할 수 없을지라도, 관련 법규나 정책의 제정 등의 대응방안을 강구하면서 이와 동시에 동일한 사안에 대한 재발을 방지하는 예방적 기능의 위해를 가할 필요성이 존재하게 되고, 이에 대한 가장 효율적인 방책은 경찰력의 행사일 것이기 때문이다.

따라서 본 연구에서는 사이버범죄의 기존 이론의 검토를 통해서 사이버범죄 유형과 특징들을 살펴보고, 사이버범죄의 현황과 범죄에 대한 경찰대응상의 문제점에 대하여 검토하였다. 경찰의 효율적인 대응방안으로써 기존의 대응방법으로 범죄에 대한 전문성확보와 유관기관 및 국가간 협조체제 구축 등을 제시하였다.

Ⅱ. 이론적 논의

2.1 사이버범죄의 정의

사이버범죄와 유사한 개념으로써, 컴퓨터자료와 관련한 컴퓨터범죄, 고도의 전문기술과 관련 있는 하이테크범죄 등의 용어가 사용되고 있으나, 일반적으로 사이버범죄는 크게 두 가지로 나누어 볼 수 있는데, 첫째, 사이버공간을 이용하여 전통적인 범죄행위를 저지르는 경우로 사이버도박, 사이버스토킹과 성폭력, 사이버명예훼손과 협박, 인터넷을 통한 사기·매매춘 · 음화판매 · 마약밀매 등이 있고, 둘째, 사이버공간을 구성하는 컴퓨터시스템이나 정보통신기반에 대한 공격으로 사이버공간의 안전을 위협하는 해킹, 바이러스 유포행위 등으로 보고 있다[1].

따라서 사이버범죄의 정확한 의미에 대해서 일반적인 정의가 형성되어 있는 것은 아니지만, 여기에서 말하는 사이버범죄는 컴퓨터범죄를 포함해서 사이버공간에서 일어나는 모든 범죄행위를 가리키는 것으로 컴퓨터를 통한 전 세계적 연결망인 인터넷을 통해 형성된 사이버공간에서 발생하는 범죄를 통칭하는 것으로 이해한다[2].

2.2 사이버범죄의 유형

경찰청에서는 사이버범죄의 유형을 크게 사이버테러형범죄와 일반사이버범죄로 구분하고 있다. 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 정보통신망 자체에 대한 공격행위를 통해 이루어지는 것은 사이버테러형범죄로, 전자상거래, 사기, 프로그램 불법복제, 불법사이트운영, 개인정보침해 등과 같이 사이버공간이 범죄의 수단으로 사용된 유형은 일반사이버범죄로 분류하고 있다[3].

2.2.1 사이버테러형 범죄

1) 해킹

해킹(Hacking)은 일반적으로 다른 사람의 컴퓨터 시스템에 무단 침입하여 정보를 빼내거나 프로그램을 파괴하는 전자적 침해행위를 의미한다. 해킹은 사용하는 기술과 방법 및 침해의 정도에 따라서 단순침입, 사용자도용, 파일 등 삭제변경, 자료유출, 폭탄스팸메일, 서비스거부공격 등이 있다.

2) 바이러스

바이러스(악성프로그램)란 일반적으로 컴퓨터 바이러스

또는 인터넷 웜을 의미하며 정보시스템의 정상적인 작동을 방해하기 위하여 고의로 제작 유포되는 모든 실행 가능한 컴퓨터 프로그램이다. 보통 자기복제능력 등 각자의 특징에 따라 컴퓨터 바이러스, 인터넷게임, 트로이목마 등으로 구분하고 있으며, 법에서 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·위조 또는 그 운영을 방해할 수 있는 프로그램을 악성프로그램으로 규정하고 이를 유포하는 행위를 처벌하고 있다.

2.2.2 일반사이버범죄

1) 전자상거래 사기

전자상거래 사기는 인터넷을 통하여 물건을 사고파는 과정에서 발생하는 것으로 인터넷의 보급이 확대됨에 따라 그 규모는 날로 팽창하고 있다.

예를 들어, 인터넷 화면을 보며 마우스 클릭만으로 주문에서 결제, 배송가지 확인할 수 있다는 편리성 때문에 온라인쇼핑몰 이용자들이 급증하는 추세지만, 통상 '선결제'라는 인터넷 거래의 특성을 악용하여 인터넷 쇼핑사이트를 그럴듯하게 만들어 놓고 유명한 상품을 시중 가격에 비해 싸게 판매하는 것처럼 광고 한 후, 고객으로부터 선불금을 받은 뒤 잠적해버리거나, 상대방이 확인하기가 힘들다는 점을 악용하여 물건을 가지고 있지 않거나 팔 생각이 없으면서도 거래를 하기로 한 후 돈만 받고 연락을 끊어버리는 등의 수법을 이용한 사기사건이 급증하고 있다.

2) 불법복제

불법복제는 저작권법 및 컴퓨터프로그램보호법상의 창작물에 대한 저작권을 침해하는 행위이다 .인터넷의 발달로 불법복제가 쉬워지면서 과거 불법 복제되어 오프라인에서 거래되던 컴퓨터프로그램, 영화, 음반CD 등이 최근에는 인터넷을 통해 파일 형태로 유포되거나 인터넷을 매개로 판매되는 등, 불법복제물의 유포 및 판매가 사이버범죄의 한 형태로 나타나고 있다.

3) 사이버명예훼손

사이버명예훼손이란 인터넷 게시판에 타인의 명예를 훼손하는 글, 사진 등을 게시하거나 전자우편 등을 통해 유포하는 것을 말한다. 불특정 다수인의 무제한 접근이 가능한 인터넷의 특성상 인터넷 게시판 등에 해당 내용이 일단 게재되면 시간이나 공간의 제한 없이 단시간 내에 급속도로 유포될 수 있기 때문에 그로 인한 피해가 심각하다 .이러한 이유로 정보통신망이용촉진 및 정보보호 등에 관한 법률에서는 사이버명예훼손죄를 일반 명예훼손죄보다 더 무겁게 처벌하도록 규정하고 있다

4) 개인정보침해

쇼핑, 오락, 교육, 금융업무 등 생활 전반이 온라인을 통해 이루어짐에 따라 온라인에서 개인의 성명, 주민등록번호, 주소 및 전화번호 등과 같은 개인정보의 중요성은 점점 커지고 있다 . 개인정보침해 범죄의 심각성은 단순히 개인정보가 유출된 것으로 끝나는 것이 아니라, 유출된 개인정보가 다른 범죄에 사용될 수 있다는 점에 있으며, 이러한 개인정보는 범죄의 표적이 되고 있다. 개인정보는 재화로서의 가치를 갖고 유통되기도 하기 때문에 법에서는 정보통신서비스제공자가 이용자의 동의 없이 개인정보를 수집하는 경우나 개인정보를 취급하거나 취급하였던 자가 개인정보를 타인에게 누설하거나 제공하는 경우 등과 같은 조직적인 개인정보침해행위도 규제하고 있다.

5) 사이버스토킹

사이버스토킹이란 인터넷게시판, E-mail 등 정보통신망을 통하여 상대방이 원하지 않는 접속을 지속적으로 시도하거나 욕설, 협박 등의 내용을 담고 있는 메일 송신 행위를 지속하는 것을 말한다. 우리나라에서는 현재까지 사이버스토킹을 구체적으로 범죄로 규정하지 않고 사이버 성폭력의 한 사례로 분류하고 있으나, 외국에서는 사이버스토킹을 독립된 하나의 범죄로 중요하게 취급하고 있으며, 우리나라도 스토킹에 대한 입법이 요구되고 있는 실정이다.

2.3 사이버범죄의 특징

사이버범죄는 사이버공간이 가지고 있는 고유의 성격과 깊은 연관성을 가지고 있다. 다시 말해, 사이버공간의 익명성과 비대면성은 사람들이 서로 만나지 않고, 서로의 신분을 밝히지 않으면서도 각종 정보와 지식 그리고 각종 교류를 가능하게 한다. 또한 시·공간의 초월성과 정보의 신속성은 언제 어디서든 세상의 누구와도 신속하게 정보교류 및 접촉이 가능하게 된다.

이러한 사이버공간의 성격에서 사이버범죄현상의 특징적인 면들이 나타나게 되는데 그 내용을 살펴보면 다음과 같다.

2.3.1 비대면성과 익명성

지상범죄가 가해자와 피해자가 직·간접적인 대면을 통해서 이루어지는 반면에, 사이버 범죄는 당사자가 대면을 하지 않고 가상의 인물을 통해서 발생하기 때문에 죄책감이 없고 행동에 있어서도 훨씬 대담하게 범행을 저지르게 된다. 또한 사이버공간은 행위자가 실재적으로 나타나지 않기 때문에 자신의 감정을 직선적으로 표출하게 되는데, 예를 들어, '악성댓글'과 무책임한 허위사실의 유포는 네트즌 간에 순식간에 유포됨으로써, 본인이 범죄행위를 인식하지 못한 순간에 이미 범죄행위를 저지르게 된다. 최근에는 사이버공간에서 익명성을 차

단하고자 하는 시스템이 개발되고 있지만, 고도의 전문적 기술을 가진 범죄자에 의해 자신의 신분을 교묘히 속이고 범죄를 하는 경우가 많다[4].

2.3.2 고도의 전문성

사이버공간에서 벌어지는 각종범죄는 간단한 기술로도 범할 수 있는 단순범죄에서 고도의 전문성과 기술로 무장한 전문범죄가 날로 증가하고 있는 추세를 보이고 있다. 예를 들어, 바이러스프로그램을 제작·유포하는 기술, 해킹이나 영업비밀을 몰래 절취하는 인터넷스파이, 컴퓨터사기, 그리고 타인의 컴퓨터방호기술을 무력화시키는 행위들은 일정수준이상의 전문가적 기술을 보유해야만 가능한 범죄들이다.

따라서 수사기관의 입장에서 보면 컴퓨터에 관한 전문지식을 요하는 범죄가 날로 증가하고 있어 증거확보와 범인검거를 더욱 어렵게 하고 있다[5].

2.3.3 시·공간 초월성

사이버공간은 시간과 공간의 제약을 받지 않고 24시간 내내 어디서든 사용할 수 있다. 이러한 시·공간적 무제한성은 사이버범죄자들에게 범죄의 기회를 제공하게 되는데, 국가간의 바이러스 유포 와 주요기술 해킹과 같은 범죄현상이 나타나게 된다. 이로 인한 심각한 문제는 범죄행위장소와 범죄발생장소의 불일치, 또는 국가간에 발생하게 되는 범죄는 범죄수사의 한계를 나타내게 된다. 이처럼 사이버범죄의 시·공간 초월성은 사이버범죄수사에 현실적 어려움을 안겨주고 있을 뿐만 아니라, 국제적 공조의 필요성을 시사하고 있다[6].

2.3.4 범죄의 암수성

사이버범죄는 현실공간에서 벌어지는 범죄와 달리 피해자나 수사기관이 인지하기가 상당히 곤란하고 그것의 원인을 규명하기가 쉽지 않아 증거가 인멸된 가능성이 많은 범죄이다[7]. 사이버공간에서 벌어지는 범죄는 현실공간에서 일어나는 범죄보다 평균적으로 높은 암수범죄(hidden crime)가 존재하고 있다. 이처럼 사이버범죄의 암수율이 높은 이유는 사이버범죄의 전문성으로 피해사실을 확인하기가 어렵고 피해사실의 인지시점의 지연으로 인하여 증거확보가 곤란하다는 측면도 있으나, 개인컴퓨터사용자는 그 피해규모가 소규모로 범죄피해신고를 꺼리고, 기업에서는 피해사실을 공개함으로써 기업이미지에 타격을 줄 가능성과 모방 및 반복피해의 우려 때문에 신고를 기피하는 경향이 높다. 이와 같이 사이버범죄의 암수성은 증거확보의 곤란과 범죄대책을 강구하는데 많은 어려움을 가지고 있다[8].

III. 경찰의 사이버범죄 대응 실태

3.1. 사이버범죄의 현황

3.1.1 범죄발생현황

〈표1〉에서와 같이 고도의 전문기술을 보유한 해커나, 대량메일 발송을 통해 유포되는 웜과 정보유출을 목적으로 제작된 트로이목마나 스파이웨어와 같은 심각한 피해를 입히는 사이버테러형 범죄가 증가하고 있다. 또한 컴퓨터 인터넷에 기본적인 활용방법으로 사이버범죄를 저지를 수 있는 일반사이버범죄 증가는 인터넷사용자들이 본인들에 의해 사이버공간에서 이루어지는 행위들을 범죄로 인식하지 못하는 순간에 범죄로 연결되고 있다.

표 1. 유형별범죄현황
Table 1. Crime present state by pattern

구분	계	사이버테러형범죄	일반사이버범죄
2006	82,186	20,186	62,000
2005	88,731	21,389	67,342
2004	77,099	15,390	61,709
2003	68,445	14,241	54,204
2002	60,068	14,159	45,909
2001	33,289	10,638	22,651

〈단위:건〉
자료 : 경찰청 사이버테러대응센터

〈표2〉에서 연령별 사이버범죄 발생현황은 20대와 30대 그리고 40대의한 범죄가 증가하고 있는 추세에 있다. 이것은 청소년기를 갓 지난 20대가 인터넷을 이용하는 시간이 많아지고 접근성이 용이해짐에 따라 범죄와 연관될 수 있는 확률이 높아지고 있다고 할 수 있다. 또한, 책임의식과 윤리의식이 성숙하지 못한 상태에 있기 때문에 본인이 알지 못하는 순간에 범죄화 되는 경우가 나타난다. 30대와 40대의 범죄의 증가는 컴퓨터관련 직종이나 전문기술을 보유한 사람들에 의해서 해킹이나 바이러스 또는 사이버공간의 불법운영을 통한 영리를 목적으로 하는 범죄와 연관되며, 성인들에 의해 저질러진다는 측면에서 위험성이 크다고 할 수 있다.

표 2. 연령별범죄현황
Table 2. Crime present state by age

구분	계	10대	20대	30대	40대	50대	기타
2006	45,877	6,158	15,400	13,543	7,967	2,149	660
%	100%	13.42%	33.56%	29.52%	17.36%	4.68%	1.43%
2005	37,828	8,630	13,982	9,026	4,135	1,461	594
%	100%	22.81%	36.96%	23.86%	10.93%	3.86%	1.57%
2004	36,148	9,391	13,296	8,176	3,337	1,289	659
%	100%	25.98%	36.78%	22.62%	9.23%	3.57%	1.82%
2003	30,150	10,187	11,185	5,437	2,277	725	339
%	100%	33.79%	37.1%	18.03%	7.55%	2.4%	1.12%
2002	21,817	8,205	6,876	3,743	1,881	563	549
%	100%	37.61%	31.52%	17.16%	8.62%	2.58%	2.52%
2001	5,052	2,198	1,661	777	242	87	92
%	100%	43.41%	32.88%	15.38%	4.79%	1.72%	1.82%

〈단위:명〉
자료 : 경찰청 사이버테러대응센터

〈표3〉에서 직업별 범죄현황은 무직자, 학생, 회사원 그리고 자영업자에 걸쳐 모든 직업군에서 범죄발생률이 증가하고 있다는 것을 알 수 있다. 이것은 인터넷 보급률이 확대됨에 따라 전 직업군에 고르게 정보화 능력을 습득하게 되고 인터넷이 집 또는 직장을 비롯한 사회어디에서나 주요 생활 수단이 됨에 따라 모든 직군에서 인터넷을 접할 수 있는 기회가 증가함으로써 사이버범죄와 접촉할 수 있는 기회가 많아지고 있다는 것을 나타내고 있다.

표 3. 직업별범죄현황
Table 3. Crime present state by job

구분	계	무직	학생	회사원	IT 전문직	자영업	전문직(의사등)	기타
2006	45,877	13,690	6,101	7,556	427	8,227	682	9,194
%	100%	29.84%	13.29%	16.47%	0.93%	17.93%	1.48%	20.04%
2005	37,828	14,147	7,580	6,186	410	3,793	905	4,807
%	100%	37.4%	20.04%	16.35%	1.08%	10.03%	2.39%	12.71%
2004	36,148	12,533	8,294	5,251	449	3,870	552	5,199
%	100%	34.67%	22.94%	14.53%	1.24%	10.71%	1.53%	14.38%
2003	30,150	11,620	8,228	3,237	202	2,558	346	3,959
%	100%	38.54%	27.29%	10.74%	0.67%	8.48%	1.15%	13.13%
2002	21,817	6,763	6,598	2,876	283	2,129	425	2,753
%	100%	31%	30.24%	13.18%	1.3%	9.76%	1.9%	12.62%
2001	5,052	1,398	2,039	735	76	404	47	353
%	100%	27.67%	40.36%	14.55%	1.5%	8%	0.93%	6.99%

〈단위 : 명〉
자료 : 경찰청 사이버테러대응센터

3.1.2 미신고범죄

사이버범죄의 실제규모는 나타나는 수치보다 더 많다고 추정되고 있다. 2005국가정보보호백서에 따르면, 사이버침해사고를 신고하지 않는 기관이 전체의 11%로 나타났기 때문이다. 신고하지 않은 기관들의 신고기피 이유는 우선 자체적인 해결이 가능하다고 판단하기 때문(44%)인 것으로 파악되었다. 그 외에'보고 및 신고절차의 미비(11%)', '문책 등 신분상의 불이익(11%)', '공개 시 기관의 이미지 훼손(6%)'등도 신고를 기피하는 이유로 나타났다. 이와 같은 조사결과는 아직까지도 상당수의 인터넷 사용자들이 사이버범죄의 심각성을 고려하지 않고 있음을 짐작할 수 있다[9].

3.2 검거현황

경찰청에서는 컴퓨터범죄수사대를 설치하여 컴퓨터관련 범죄를 수사해 오다가 1999년 12월 23일에 사이버범죄수사대라는 명칭으로 확대 개편하였다. 그리고 2000년에는 사이버테러대응센터를 발족하여 사이버범죄에 대하여 대비하고 있다. 현재 경찰청의 사이버범죄수사대에서는 해킹, 바이러스 유포범죄 등 고도의 전문기술이 필요한 부분을 직접수사하고 일반적인 범죄는 일선 전담수사요원들에 수사지시 하거나 수사기술을 지원함으로 전국적인 공조체제를 이루고 있다[10].

표 4. 유형별검거현황
Table 4. Arrest present state by pattern

구분	계	사이버테러형 범죄	일반사이버범죄
2006	70,545(89,248)	15,979(17,498)	54,566(71,750)
2005	72,421(81,338)	15,874(17,371)	56,547(63,967)
2004	63,384(70,143)	10,993(11,892)	52,391(58,251)
2003	51,722(56,724)	8,891(10,047)	42,831(46,677)
2002	41,900(47,252)	9,707(10,762)	32,193(36,490)
2001	22,693(24,455)	7,595(8,099)	15,098(16,356)

〈단위 : 건(명)〉

3.3 경찰대응의 문제점

3.3.1 조직의 분산

사이버범죄 대응조직은 각 기관 곧, 경찰청, 검찰청, 국가정보원, 정보통신부에 다양하게 분산되어 있다. 또한 경찰과

검찰은 사이버 범죄의 단속과 수사기능을 담당하고 있고, 국가정보원은 사이버테러와 같은 국가기간망 침투방지와 국제범죄 단속을 담당하며, 정통부의 정보보호과는 정보화 역기능 방지정책 수립을 담당하고 있다. 이처럼 사이버범죄단속기관은 기능에 따라 분산되어있지만 광의의 관점에서 보면 모두 유사한 업무를 담당하고 있다. 그러나 유사한 업무를 통합 조정할 수 있는 기구가 형성되어 있지 않다[11].

3.3.2 수사상의 문제

사이버범죄는 현실공간에서 일어나는 범죄와 달리 가상공간에서 이루어지는 범죄이기 때문에 피해사실의 적발을 어렵게 하여 암수율을 높이는 원인으로 작용한다. 타인의 아이디나 비밀번호를 도용하여 불특정 다수를 대상으로 사기행각이나 바이러스를 유포한 경우에는 구체적 피해사실을 파악하기 힘들며, 피해자가 피해범위와 피해실태를 파악하기가 어렵게 한다[12].

또한 컴퓨터 환경의 특성상 사후적으로 범행을 입증하기가 매우 어렵고 피해신고율도 낮다. 컴퓨터는 단시간에 방대한 양의 정보를 처리하고 있으므로 간단히 컴퓨터조작에 의해 사후에 범죄혐의를 입증하기가 곤란하다. 특히 금융기관이나 전산시스템운영자가 자사의 담당업무나 전문지식을 활용하여 고객이나 기업에 피해를 입히거나 중요정보를 유출시키는 사례가 빈번하게 나타나는데 경찰수사력이 이를 따라가지 못하고 있는 실정이다.

3.3.3 제도적 장치부족

사이버공간에서 벌어지는 범죄행위 중에서 단속법규가 미흡하여 적절한 형사제재를 가하지 못하는 경우가 있다. 다시 말해서 범죄기술화 환경이 나날이 새롭게 변하는 사이버범죄에 대하여 정태적인 형법상의 조항들로 처벌규정을 법제화 하는 데는 무리가 따를 것이다[13]. 또한 결과범에만 처벌을 할 수 있고 미수범에 대한 처벌규정이 없는 문제점도 가지고 있는 허점을 지적할 수 있다. 법적근거는 있지만 단속주기에 관한 해석이 시대적 상황이나 법관에 따라 달라짐으로써 단속상의 혼동을 초래하는 경우가 있다[14].

3.3.4 조직의 미비와 전문성 결여

경찰수사조직은 경찰청에 사이버테러대응센터를 중심으로 16개 지방청 사이버범죄수사대와 전국 236개 경찰서에 사이버범죄수사팀을 두고 있지만, 사이버범죄에 있어서 중대한 범죄는 컴퓨터 업종에 종사하는 자나 그것에 대한 전문지식이나 전문적 컴퓨터기술을 보유한 사람들에 의해서 저질러지게 되는데, 이 같은 고도의 하이테크 범죄를 수사할 수 있는 사이버범죄 전문수사체제가 부족한 실정이다.

IV. 사이버범죄의 효율적 경찰 대응방안

4.1 유관기관과의 연대강화

앞의 문제점에서 언급하였듯이 사이버범죄에 대응하기 위한 전문조직의 육성을 위해서는 분산되어 있는 조직을 연계하여 적극적으로 대응할 수 있는 기구가 필요하다. 또한 사이버범죄는 고도의 첨단기술이 연루된 범죄이기 때문에 범죄의 기법이 나날이 발전하며, 경찰인력의 지식만으로는 새로운 범죄수법을 따라잡기가 어렵다. 따라서 첨단컴퓨터 기술력을 보유한 단체 및 연구기관과의 긴밀한 협력관계를 가질 수 있어야 한다[15].

4.2 사이버범죄 수사의 효율화 방안

4.2.1 사이버범죄 방범반 활성화

지금까지는 사용자가 아닌 단속자에 대한 전문적 교육만이 강조되었었다. 하지만 사이버범죄의 발생 형태를 보면, 단속자만의 문제를 초월하여 사용자 중심의 교육이 도입되어야 할 것이다.

사이버범죄 방범반은 사이버범죄의 예방을 위한 순찰기능을 담당하며, 순찰 중에 포착된 범죄행위에 대해서는 관계수사관에게 수사요청을 하거나, 혹은 직접 수사에 임하는 기능을 담당한다. 방범반에 배치된 요원은 원칙적으로 사이버스페이스 순찰활동이 주요 임무이며, 사이버범죄 예방활동을 전담한다. 사이버범죄 방범반에는 3개 부문으로 나누어 수사요원을 배치한다. 첫째 네티즌이 자율방범활동을 할 수 있도록 조직하는 기능뿐만 아니라, 필요한 경우 자율방범에 대한 다양한 지원을 통한 사이버범죄행위의 예방을 하도록 하는 시민자율방범지원담당, 둘째, 사이버스페이스에서 상행위의 예방을 하도록 하는 전자상거래자율방법지원담당, 셋째, 사이버스페이스 범죄예방과 건전한 질서 확립을 위해 조직된 시민조직을 통하여 방범활동을 하고, 시민조직에 대한 지원을 통하여 사이버범죄예방활동을 하는 시민기구자율방범지원담당이 필요하다[16].

4.2.2 국제적 협력체제 구축

사이버범죄는 지리적인 공간에서의 범죄와 달리 국경을 초월하여 발생하며, 피해의 범위가 광범위하다는 특징을 가지고 있다. 따라서 외국의 수사기관과의 공조체제를 구축하여 사이버범죄에 공동 대응해야 할 것이다. 이를 위해서 국제공조를

위한 컴퓨터범죄 관련 국제회의나 세미나에 참석하고, 사이버테러대응센터 내에 국제협력반을 두어 해외로부터의 사이버범죄 자료를 지속적으로 수집할 수 있도록 해외수사기관과 지속적 연대를 구축할 필요가 있다[17].

4.2.3 사이버범죄 정보시스템 구축

우리나라는 명실상부한 IT강국임을 자처한다. 세계에서 가장 높은 컴퓨터 보급률과 빠른 속도와 넉넉한 IT 인프라가 이를 뒷받침해주는 증거일 것이다.

이는 인터넷게임의 영역에 있어서도 비슷하다.

이와 함께 우리 경찰의 사이버범죄 수사능력은 세계최고임을 인정받고 있다. 하지만 이러한 영예에 만족만 하고 있을 것이 아니라 앞날을 내다보는 정책을 제시해야 할 것이다.

예를 들어 인터폴의 "국제지명수배제도"와 비슷한 형태의 '사이버범죄 정보시스템'을 우리의 힘으로 구축해야 할 것이다.

우리의 차세대 성장동력으로 인정받고 있는 인터넷 게임이나 관련 콘텐츠들은 모두 안정된 사이버 공간의 존재에서만이 가능한 일이며, 동 시스템의 구축에 관련하여 당장 우리에게 얼마간의 투자가 발생되어야 겠지만, 이러한 투자는 후일 환가할 수 없는 경제적 이익으로 우리에게 귀속될 것이기 때문이다.

4.3 제도적 정비

익명성, 시공초월성, 피해확산성, 비대면성 등의 특징을 가진 사이버범죄에 대하여 현행법만으로는 법의 공백 또는 한계로 인하여 사이버범죄 대처에 많은 어려움이 있다. 현재 컴퓨터범죄에 대하여는 주로 형법이 규율하고 있고, 사이버범죄에 대하여는 산발적인 행정형법 내지 특별형법에 규제되고 있다. 따라서 새로이 발생하고 있는 사이버범죄에 대한규정들이 산재하고 있거나 때로는 미비하므로 이에 대하여 효과적으로 규율하기 위해 형법 규정을 보완하는 것 외에 사이버범죄특별법의 제정을 검토할 필요가 있다[18].

4.2.4 전문인력확보와 교육실시

사이버범죄는 사이버스페이스가 새로운 생활공간으로 자리 잡게 됨으로써 발생되는 범죄이기 때문에 범죄수사를 담당하는 수사관을 대상으로 나날이 발전하는 범죄기법과 수사방법에 대한 교육훈련이 무엇보다도 중요하다. 교육훈련은 다음 두 가지로 나누어 실시할 수 있다. 첫째, 수사요원의 지속적인 해킹학습과 교육훈련이 요구된다. 사이버범죄 수사관을 국내외 연구기관에 파견하여 첨단 해킹기술을 익힐 수 있도록 하는 교육훈련 프로그램 개발이 요구된다. 둘째, 정통부의 통계에 의하면, 해킹사고의 80%가 해외에서 침투한 경우라는 사실을 감안할 때 사이버범죄 수사관은 국제 해킹에 대해 민감하게 대처할 필요가 있으며, 사이버범죄의 수사에 관한 국제공조를 원활히 취할 수 있도록 하는 국제공조 교육훈련과 국제간 협약이 필요하다.

V. 결 론

앞으로 사이버 범죄가 더욱 기술적으로 교묘해지고 고도화되며, 그 수법이 다양해지고 은밀해질 것으로 보인다. 그 피해 또한 단순한 전산망 장애에 국한되지 않고, 기관, 기업의 중요자료 및 개인정보유출 등의 위험수위가 더욱 높아 질 것이다.

세계적인 수준에서 정보화가 진전되고 있는 가운데, 한국사회에서도 초고속 통신망이 구축되었고 인터넷인구 또한 급속도록 증가하였다. 이에 따라서 삶의 편익도 증가하지만, 사이버범죄에 노출될 위험성도 더욱 커지고 있다.

따라서 신속하게 변화하고 전문화 되어가는 사이버범죄에 대응하기 위한 대응책을 마련해야 될 것이다. 이를 위해서 먼저, 사이버범죄를 사전에 예방하고, 대응할 수 있는 제도적 기술적 장치가 마련되어져야 할 것이다. 두 번째로, 사이버범죄에 신속하게 대응할 수 있는 조직과 인력을 구축해 나가야 될 것이다. 세 번째로, 전 국민적 인터넷 보안의식과 교육을 통해서 해킹 또는 바이러스감염과 같은 치명적 범죄에 대하여 사전에 예방하여야 할 것이다. 마지막으로 시·공간을 초월해서 나타나는 사이버범죄에 효율적으로 대응하기 위해서 국가간의 원활한 협조관계가 필요하게 될 것이다.

결국, 사이버범죄에 대해서 인적· 제도적·, 기술적 그리고 국제적 협조관계를 통해 대응과 더불어서 전 국민적 사이버윤리의 교육과 홍보를 위한 방안들이 체계적으로 구성되어져야 할 것이다.

이러한 정책적 시사점에도 불구하고 본 논문은 이론적 논의에서 제시한 각각의 이슈들에 대하여 경찰의 대응실태에 대한 연관성이 연구자의 주관적 판단에 의하여 제시되었다는 점은 본 연구의 한계점이라 할 수 있다. 따라서 후속 연구에서는 경찰의 사이버범죄 대응에 대한 보다 객관적인 경험연구를 통하여 구체적인 방안들이 제시되기를 기대한다.

참고문헌

〔1〕 김종섭, 사이버범죄 현황과 대책, 한국형사정책학회, 2000.

〔2〕 강동범, 사이버 범죄와 형사법적 대책, 형사정책연구, 2006.

〔3〕 경찰청사이버테러대응센터 (http://www.netan.go.kr/index.jsp), 2007.

〔4〕 김상균, 사이버범죄에 대한 경찰의 수사력강화 방안, 한국법학회, 2001.

〔5〕 양문승, 전자상거래관련범죄와 대응방안, 한국공안행정학회, 1999.

〔6〕 우제태, 사이버공간과 사이버범죄, 전주대학교 사회과학연구원, 2000.

〔7〕 허만형, 사이버범죄에 대한 국가의 정책적 대응방안, 사이버커뮤티케이션학회, 2000.

〔8〕 허만형, 사이버범죄에 대한 국가의 정책적 대응방안, 사이버커뮤티케이션학회, 2000.

〔9〕 장종인, 사이버범죄에 대한 사회·문화적 논의, 정보통신정책연구원, 2006.

〔10〕 경찰청사이버테러대응센터. (http://www.netan.go.kr/index.jsp), 2007.

〔11〕 허만형, 사이버범죄에 대한 국가의 정책적 대응방안, 사이버커뮤티케이션학회, 2000.

〔12〕 한국형사정책연구원, 사이버경찰에 관한 연구, 한국형사정책연구원보고서, 2000.

〔13〕 유인모, 정보형법의 과제와 전망, 현국형사정책학회, 2000.

〔14〕 김상균, 사이버범죄에 대한 경찰의 수사력강화 방안, 한국법학회, 2001.

〔15〕 허만형, 사이버범죄에 대한 국가의 정책적 대응방안, 사이버커뮤티케이션학회, 2000.

〔16〕 허만형, 사이버범죄에 대한 국가의 정책적 대응방안, 사이버커뮤티케이션학회, 2000.

〔17〕 김종섭, 사이버범죄 현황과 대책, 한국형사저책학회, 2000.

〔18〕 박윤해, 컴퓨터범죄에 관한 연구, 숭실대학교법학연구소, 2006.

저 자 소 개

박 창 욱

2007~현재 : 원광대학교 대학원 경찰행정학과 박사과정