http://dx.doi.org/10.5392/JKCA.2013.13.03.141

# 민간경비를 활용한 사이버범죄 예방 방안

## Prevention Methods of Cyber-crimes using the Private Security

김상운*, 조현빈**
대구가톨릭대학교 경찰행정학과*, 순천향대학교 경찰행정학과**

Sang-Woon Kim(ksw48@naver.com)*, Hyun-Bin Jo(johyunbin@korea.com)**

**요약**

2000년대 이후 폭발적으로 증가한 사이버 공간에 대한 활용으로 인해 인간의 삶은 과거와 다르게 큰 발전에 발전을 거듭함과 동시에 사이버 범죄라는 신종 범죄가 증가하게 되는 원인이 되었다. 이러한 사이버 범죄는 과거의 물리적 형태의 범죄와 달리 사이버 공간이라는 특징을 바탕으로 일어나는 범죄로서, 비대면성·익명성·전문성·기술성·반복성·계속성 등을 가지는 특징이 있다. 사이버 범죄 발생추이를 살펴보면, 2003년에 비해 2010년에는 거의 두 배에 가까운 범죄가 발생하고 있다. 주로 일반 피싱·음란물 유포 등과 같은 일반 사이버 범죄가 대부분이었으며, 사이버 범죄를 저지르는 범죄자들의 연령대가 다른 범죄들에 비해 낮은 모습을 보여주었다. 최근 사이버 범죄에 대해서 경찰에서는 '사이버테러 대응 센터'를 설치하여 대응하고 있으나, 예방 및 수사조직의 분산, 수사상의 문제점, 제도상의 문제점 등으로 인해 효과적으로 대처하지 못하고 있다. 따라서 경찰의 문제점을 보완하기 위하여 이 연구에서는 민간경비를 통해 사이버 범죄를 예방하기 위한 방안으로 물리적 경비를 통해 서버룸과 같은 주요시설에 접근을 통제하며 우수한 사이버 전문요원을 육성하는 기본적인 형태의 범죄예방을 비롯하여, 사이버 범죄 컨설팅 및 관련 법령 개정에 관하여 살펴보았다.

■ 중심어 : | 사이버범죄 | 해킹 | 사이버폭력 | 기계경비 | 민간경비 |

**Abstract**

With the spread of Personal Computers(PC) in the 1980's, many people started to deal businesses with PC. From late 1990's, the Internet age with PC have started and many people have showed keen interest in cyber-space and now they are utilizing it. Since 2000's the use of cyber-space have skyrocketed and it caused significant changes to humans' life. There was a huge prosperity to us but the new kind of crime, cyber-crime, was raised. Unlike past physical type of crimes, those cyber-crimes take place in the cyber-space and they have special features of non-facing, anonymity, specialty, technologic, repetition, continuation. Those cyber-crimes are continually growing since 2003 and in 2010 it almost doubled compared to 2003. General cyber-crimes like phishing-scam · pornography circulation was most of them and notably perpetrators of them are younger generation. Recently cyber-crimes are showing the trend of advancing more and more and cyber-bullying, fraud like phishing scam are on the rise. The police are responding by making 'Cyber Terror Response Center', but it does not work effectively with the problems of breakup of prevention and investigation unit, procedure of investigation and the system itself. So, I suggest practical use of private security to remedy our police's weakness and to prevent cyber-crimes. Preventing solutions of cyber-crime with private security are physical defense of large-scale servers and vital computers, building of Back-up system to prevent vital data loss, and building of cyber-crime preventing system combining software and hardware.

■ keyword : | Cyber-crime | Hacking | Cyber-Bulling | Electronic Security | Private Security |

* 이 논문은 2012년도 대구가톨릭대학교 교내연구비(정착)에 의해 연구되었음.

접수번호 : #121113-002
접수일자 : 2012년 11월 13일
심사완료일 : 2012년 12월 18일
교신저자 : 조현빈, e-mail : johyunbin@korea.com

## I. 서 론

1991년에 전 세계에 개봉되었던 영화 “터미네이터 2”에서는 MID와 같은 소형기기를 이용하여 현금자동인출기(Automated Teller Machine : ATM)에서 돈을 훔치는 장면이 그려졌다. 이러한 모습은 최근 우리 사회에서 빈번하게 발생하여 심각한 문제로 지적되고 있다. 특히, 1990년대부터 첨단과학의 발달로 인해 본격적으로 등장한 인터넷 기술과 사이버 공간의 발전은 현대사회를 새로운 정보통신혁명의 시대로 변화시킴과 동시에 사이버범죄라는 신종범죄를 발생시켜 심각한 사회문제가 되고 있다.

최근 사이버범죄는 기존의 은행전산망과 같은 대형컴퓨터에 의해 처리되던 데이터의 조작이나 퍼스널 컴퓨터에 저장되어 있던 정보를 훼손하는 등의 초기 컴퓨터범죄 유형을 벗어나 인터넷 공간에 유통되는 모든 정보에 대한 침해와 네트워크에 대한 무권한 접속, 사이버 공간에서 발생하는 사기, 폭력, 저작권 침해, 포르노그래피 유포, 사이버 테러 등 새로운 범죄현상이 지속적으로 나타나고 확대되고 있다[1]. 특히, 휴대전화・MID(Mobile Internet Device)・스마트폰 등의 발달은 사이버 공간의 활용도를 높여줌과 동시에 사이버범죄에 상시로 노출되게 되는 문제점을 가지게 되었다. 이러한 사이버범죄에 대해서 2000년대 이후부터 정부에서는 사이버범죄를 예방하기 위한 다양한 시도를 실시하였으나, 진화속도가 빠른 사이버범죄의 특성으로 인해 효과적으로 대처하고 있지 못하다.

따라서 사이버범죄에 대응하기 위한 경찰의 노력 이외에 민간경비 및 민간자원을 활용하여 사이버범죄를 예방하는 방안에 대해서 살펴보기로 한다.

## II. 사이버범죄의 의의와 특성

### 1. 사이버범죄의 정의

오늘날 사이버범죄는 네트워크 테크놀로지에 의해 이루어지는 범죄로 널리 기술되고 있다. 사이버범죄의 기원은 공상과학소설과 영화에 기원을 두고 있다[2].

이러한 사이버범죄에 대해서 아직 학문적으로 명확하게 정의된 바는 없지만, 일반적으로 사이버 공간에서의 범죄현상을 의미한다고 할 수 있다. 과거 컴퓨터 범죄, 정보통신 범죄, 하이테크 범죄 등의 용어가 사용되었으나 현재는 사이버범죄라는 용어가 널리 사용되고 있다[3].

또한 사이버범죄란 컴퓨터 관련 범죄의 또 다른 명칭으로서 컴퓨터 범죄와 사이버 테러를 포함하는 개념이라고 할 수 있다. 범죄행위의 주요무대가 사이버 공간이며 컴퓨터를 도구로 한 범죄행위, 사이버공간에서 네티즌을 대상으로 행해지는 범죄행위, 사이버 공간에서 일반인을 대상으로 행해지는 범죄행위 모두를 포함하는 포괄적인 개념이다[4].

또 다른 정의를 살펴보면 사이버범죄의 정의를 “일반적으로 인터넷과 같은 정보통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로 형성되는 사이버 공간(Cyber space)을 중심으로 발생하는 범죄행위를 총칭하는 표현으로 사용된다”고 하였다[5].

사이버범죄란 개념이 아직 불확정의 신조어로서 학교폭력・가정폭력・지하철범죄 등과 같은 범죄가 행해지는 장소를 부각시킬 목적으로 가상의 사이버 공간을 장소화 하여 호칭하는 것으로 볼 수 있다. 나아가 컴퓨터나 네트워크가 사용되지 않는 범죄라도 특정범죄에 디지털 증거(digital evidence)가 관련되어 있을 때 이를 광의의 사이버범죄에 포함시키는 견해도 있다[6]. 이러한 사이버 범죄는 전통적인 범죄와 수사방법이나 증거수집 및 조사 등에서 달리 취급해야 할 필요성과 이들을 둘러싼 환경이 급속히 변화되기 때문에 법적 안정성을 중시하는 사법제도의 경직성과 괴리를 막기 위해서라도 새롭게 등장하는 범죄현상을 신속하게 포착하여 개념화시키는 작업이 필요하다[7].

따라서 사이버범죄에 대한 학자별 정의를 종합하면, 사이버범죄는 인터넷을 비롯한 사이버 공간과 같은 정보 통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로 한 사이버 공간을 이용하여 공공복리를 저해하고, 건전한 사이버 문화에 해를 끼치는 행위로서 사이버범죄는 빠른 시간 안에 불특정 다수에게 많은 악영향을 미치는 범죄행위라고 정의할 수 있다.

## 2. 사이버범죄의 분류

사이버범죄의 유형은 학자에 따라 다양하게 제시되고 있다. 사이버 범죄의 유형을 사이버 공간을 이용한 전통적인 범죄와 사이버 공간의 등장으로 새롭게 발생하는 범죄로 나누는 입장으로 범죄의 불법 내용이 사이버 공간 자체의 등장에 의존하고 있느냐에 따라 나누기도 한다. 그리고 사이버 공간을 합법적으로 이용한 범죄군과 보호되는 사이버 공간을 불법적으로 침입하여 이루어진 범죄로 구분하고, 전자를 다시 사이버 공간을 이용한 전통적 범죄와 사이버 공간에서만 존재하는 재물의 침해나 캐릭터의 인격권 침해로 나누는 입장으로 분류하기도 하였다[8].

그 밖에 David Wall은 사이버범죄를 범죄 유형과 독자성・강도에 따라 분류하기도 하였다. 경찰에서는 사이버 범죄의 심각성과 유형에 따라 구분하기도 하였다.

### 2.1 David Wall에 의한 분류

사이버범죄에 대해 학자별로 유형을 달리하고 있다. [표 1]에서와 같이 사이버범죄에 대한 분류에 있어서 대표적인 학자인 David Wall은 3단계로 분류하였다.

1단계에서는 컴퓨터 해킹, 컴퓨터 이용사기와 같은 형태의 비교적 가벼운 형태의 사이버범죄를 실시하는 유형이며, 2단계에서는 1단계보다는 높으면서 좀 더 복잡하고 지능적인 형태의 사이버범죄 유형으로, 네트워크를 통한 해킹 및 인터넷 사기, 포르노・증오범죄 자료를 유포하는 형태의 사이버 범죄 유형이다.

마지막으로 3단계에서의 사이버범죄는 좀 더 심각한 형태의 사이버범죄로서 신분절취・서비스 거부・스팸 바이러스 살포를 비롯하여 장기적 형태의 컴퓨터 이용사기, 네트워크를 통한 포르노・증오자료 전송과 같은 고도의 기술이 필요한 형태의 사이버범죄로 분류하였다.

### 2.2 경찰에 의한 분류

[표 2]에서처럼 사이버 범죄에 대한 분류를 경찰의 기준으로 나누어보면, 그 범행 목적에 따라 사이버범죄는 크게 사이버 테러형 범죄와 일반 사이버범죄로 나뉜다.

**표 1. David Wall에 의한 사이버범죄의 유형[9]**

| 범죄 매트릭스 | 컴퓨터 무결성 범죄 | 컴퓨터 이용 범죄 | 컴퓨터 콘텐츠 범죄 |
|---|---|---|---|
| 1단계: 일반 범죄 | 컴퓨터 해킹 | 컴퓨터 이용 사기 | 강성포르노 저장 |
| 2단계: 하이브리드 사이버범죄 | 네트워크를 통한 해킹 | 인터넷 사기 | 포르노・증오 범죄자료 유포 |
| 3단계: 진정한 사이버범죄 | 신분절취・서비스거부공격・다운로드를 통한 스팸 바이러스 | 장기적 형태의 컴퓨터 이용사기 | 네트워크를 통한 포르노・증오범죄 자료 등을 전송 |

첫 번째, 사이버 테러형 범죄는 해킹에 포함된 단순 침입, 사용자도용, 파일삭제변경, 자료유출, 폭탄메일, DDos 공격, 컴퓨터 바이러스와 같은 유형의 범죄가 사이버 테러형 범죄이다. 사이버 테러형 범죄는 단순히 범죄에서 그치는 것이 아니고, 그 파급효과가 테러와 같이 광범위하고 영향력이 큰 특징을 가지고 있다.

**표 2. 사이버범죄의 형태**

| 구 분 | 행위유형 | 내 용 |
|---|---|---|
| 사이버 테러형 범 죄 | 해 킹 (Hacking) | 일반적으로 다른 사람의 컴퓨터 시스템에 무단으로 침입하여 정보를 빼내거나, 바이러스를 심거나, 프로그램을 파괴하는 행위를 의미함 |
| | 바이러스 (Virus) | 컴퓨터 바이러스 또는 인터넷 웜을 의미하는 것으로서 정상적인 컴퓨터 시스템을 방해하기 위하여 고의로 제작 유포되는 모든 프로그램을 의미함 |
| 일 반 사이버 범 죄 | 전 자 상 거 래 사 기 | 편리한 인터넷 쇼핑의 단점을 이용하여 저질러지는 범죄로서, 상대방이 확인하는 힘들다는 점을 악용하여, 잘못된 물건을 전달하거나, 돈만 받고 연락을 끊어 버리는 등 전자 상거래를 활용한 사기를 의미함 |
| | 불법복제 | 가장 많은 형태의 사이버 범죄로서, 「저작권법」 및 「컴퓨터프로그램보호법」상의 개인의 창작물에 대한 침해행위로서, 과거 CD나 플로피디스크를 활용한 물리적 형태의 불법복제에서 네트워크 방식을 활용한 불법복제 유통으로 형태가 변화하고 있는 것이 특징임 |
| | 사 이 버 폭 력 | 사이버 공간에서 행해지는 모욕적인 언사나 욕설, 타인에 대한 명예훼손, 음란한 대화 및 성적 수치심을 주는 사이버 성희롱, 인터넷을 통해 성매매를 유도하는 사이버 성매매 등과 같이 물리적인 폭력형태보다는 사이버 공간을 이용하여 정신적 형태의 폭력을 구사하는 유형 |
| | 개인정보 침 해 | 쇼핑・오락・교육・금융업무 등 일상생활을 하는데 있어서 사용되는 개인정보를 훔쳐서 불법으로 사용하는 유형임 |

일반 사이버범죄는 통신・게임을 활용한 사기, 음란물・프로그램에 대한 불법복제, 음란・도박・폭발물 제조・동반자살과 같은 자료를 공유하는 형태의 불법・유해사이트, 명예훼손, 개인정보침해, 사이버 스토킹, 사이버 성폭력, 사이버 공갈・협박이 여기에 해당한다. 일반 사이버범죄는 사이버범죄 중에서 비교적 흔하게 발생하고 있는 특징을 가지고 있다.

## 3. 사이버범죄의 특성

사이버범죄는 기존의 범죄와 달리 비대면성・익명성・전문성과 기술성・시간과 공간의 무제약성・상당한 재산피해와 빠른 전파성・발각과 원인규명이 어려움・범죄의 암수성이 높은 특징을 가지고 있다[3].

### 3.1 비대면성

사이버 공간에서는 사람들이 사회생활을 영위하면서 서로 일일이 굳이 만날 필요성이 없다는 특징이 있다. 또한 사이버 공간은 인터넷을 매개로 하여 형성되는 생활공간으로서 불가시적이므로 현실세계와는 달리 행위자들이 자신의 얼굴을 드러내지 않고 행동한다. 따라서 그곳에서의 모든 범죄행위도 행위자가 전혀 모습을 드러내지 않는 상태에서 행해진다[10].

사이버범죄의 이러한 비대면성으로 인하여 범죄자들은 보다 과격하고 대담하게 행동하게 되며, 실제 대면했을 때와 달리 더욱 잔인하고 과감한 범죄를 저지르게 된다. 그리고 이러한 비대면성은 책임의식의 결여로 이어져 인터넷 사기를 유발하는 계기가 되곤 한다. 비대면성으로 인해 피해자는 행위자를 거의 알 수 없어 범인파악이 어렵고, 피해의식이나 공포감이 더욱 커지게 되는 특성을 가지고 있다.

### 3.2 익명성

사이버 공간에서는 자신의 신분을 노출시키지 않은 채 활동하는 것이 가능하다. 인터넷을 이용하고자 할 때 인적 사항을 적도록 하고 일정한 인증절차를 거쳐 사용자를 확인하기도 하지만, 정확한 인적 사항을 요구하지 않는 경우가 많으며 타인의 인적사항이나 ID를 도용하면 완벽하게 자신의 익명성을 보장받을 수 있다. 이로 인해, 사이버 폭력과 같은 형태의 범죄발생이 용이하게 된다. 사이버 폭력의 경우 익명성을 보장받기 때문에 더욱 과격하고, 과감한 형태의 언어폭력이 난무하게 되며, 성희롱과 같은 유형의 범죄로 발전하게 되는 큰 요인으로 작용한다.

### 3.3 전문성 · 기술성

최근 들어 발생하는 사이버범죄의 경우 전문성을 띠는 경우가 많았다. 사이버범죄의 특성 상 컴퓨터나 전문기기를 사용하는 것이 대부분이기 때문에, 이러한 기기를 잘 활용하고 전문적인 지식이 있는 자가 범죄를 저지르기 때문에 전문성을 가지고 있다.

최근에는 사이버범죄를 실행함에 있어 전문적인 기술의 필요성이 점점 퇴색되어 가고 있다. 과거에는 사이버범죄 중에 하나인 해킹을 비롯한 바이러스 제작・유포와 같은 행위에 대해 전문적인 지식과 기술이 필요하였으나, 최근에는 관련 프로그램의 발달로 인해, 보다 쉽게 해킹과 바이러스 제작・유포가 이뤄지고 있어 사이버범죄의 특성인 전문성과 기술성이 점점 퇴색되고 있다.

### 3.4 시간과 공간의 무제약성

사이버 공간에서는 시간과 공간의 제한이 없는 특징을 가지고 있다. 누구든지 마음만 먹으면 인터넷을 24시간 내내 이용할 수 있으며, 별다른 어려움 없이 세계 어느 곳에 있는 인터넷 사이트에 접속할 수 있다. 사이버 공간의 이러한 시간적・공간적 무제약성은 사이버범죄자들에게 많은 범죄의 기회를 제공하고 있으며, 사이버범죄 수사에 있어서 실질적・법률적으로 많은 어려움을 주고 있다.

시간적・공간적 무제약성은 광역성과 초(超) 국가성을 띠는 형태로 발전하고 있다. 사이버 공간의 특성 상 현실 공간과 같이 행위자의 행위지와 범죄 발생지가 실질적으로 존재하지 않기 때문에, 사이버범죄에 대한 광역적인 형태의 특성과 아울러 수사상에 발생하는 초국가적인 특성을 띠고 있다.

### 3.5 반복성 · 계속성

일반범죄의 경우 범죄의 반복성과 계속성을 가지기

위해서는 적발되지 않거나 체포되지 않아야 하는데, 사이버범죄의 경우 적발될 가능성과 체포될 가능성이 낮음과 동시에, 사이버 상의 프로그램을 활용하여 행위의 반복과 지속이 가능하기 때문에 반복성과 계속성을 가지고 있다.

### 3.6 높은 암수율

사이버범죄는 현실공간에서 벌어지는 범죄와 달리 피해자나 수사기관이 인지하기가 상당히 곤란하고 그것의 원인을 규명하기가 쉽지 않아 증가거가 인멸될 가능성이 높다[11].

특히, 범행주체가 고도의 전문지식을 갖추었거나 조직의 내부자인 경우는 단속기관의 접근이 곤란하여 은폐될 소지가 많다. 금융기관이나 유명기업, 국가기관 등은 범죄를 발견하더라도 신용도의 훼손이나 중요한 기밀누설, 또는 취약점의 노출 등으로 인한 역 공략을 당할 가능성을 고려하여 수사기관에 고발을 기피하기 때문에 암수율이 높은 특성을 가지고 있다[4].

### 3.7 빠른 전파성과 큰 피해

기존의 범죄유형과 달리 사이버범죄는 인터넷을 활용한 초국가적인 특성으로 인해, 전파성이 매우 빠르며, 광범위하게 전파되는 특성으로 인해, 피해가 커지는 특징을 가지고 있다.

사이버 공간에서의 명예 훼손적 표현이나 음란물 또는 바이러스는 순식간에 전 세계에 널리 유포될 수 있으며 그에 따라 범죄로 인한 피해가 광범위하게 미치게 된다. 특히 바이러스와 해킹에 의한 시스템 작동불능은 경우에 따라서 시스템에 연결된 모든 컴퓨터의 작동을 멈추게 함으로써 업무 전반을 마비시키는 심각한 결과를 초래하여 천문학적인 재산피해를 야기하게 되며, 불특정 다수를 상대로 하는 인터넷사기도 광범위한 피해를 야기한다.

**표 4. 실제 범죄와 사이버범죄의 비교**

| | 실제 범죄 | 사이버범죄 |
|---|---|---|
| 거 리 | 근접성 | 초국가적 |
| 범죄자와<br>피해자와의 관계 | 일대일의 피해자화 | 일대 다수의<br>피해자화 |
| 물리적 영향 | 물리적 제약 | 물리적 무제한 |

## Ⅲ. 사이버범죄 발생 실태와 문제점

### 1. 사이버범죄 실태

사이버범죄는 다른 범죄보다 2000년대 이후 급격한 성장세를 보이고 있다. 1980년대 개인용 PC시대부터 1990년대 중반까지, 사이버범죄에 대한 개념이 생겨나지 않을 만큼 그 범죄 발생은 미미하였다. 그러나 1990년대 후반 이후부터 인터넷의 발달과 정보통신 시스템의 발달로 인해 사이버 공간이 발달하게 됨에 따라 급격한 성장세를 보이고 있다.

2003년부터 2010년까지 발생한 사이버범죄의 실태를 살펴보면, 2003년에는 6만8천 여 건에 불과하던 사이버범죄가 2006년을 제외하고 급격한 성장세를 보이며, 2010년에는 2003년에 비해 거의 두 배 가까운 성장을 하였다.

사이버 테러형 범죄의 경우 2003년 14,241건 발생하였다. 이후 2005년과 2006년에 20,000건이 넘었으나, 2009년에는 16,000여건 정도 발생하는 등 20,000건 전후로 발생하고 있다. 반면 검거비율은 지속적으로 상승하고 있어, 경찰의 범죄수사 기술이 증가하였음을 나타내고 있다.

반면, 일반 사이버범죄의 경우 2003년에는 54,000여 건에 불과하던 일반 사이버범죄의 발생이 2010년에는 104,615건으로 두 배 가까운 증가세를 보이고 있었으나, 검거율은 그에 미치지 못하고 있어 문제의 심각성으로 대두되고 있다. 특히, 사이버 테러형 범죄에 비해 통신·게임을 활용한 사기, 음란물·프로그램에 대한 불법복제, 음란·도박·폭발물 제조·동반자살과 같은 자료를 공유하는 형태의 불법·유해사이트, 명예훼손, 개인정보침해, 사이버스토킹, 사이버성폭력, 사이버 공갈·협박과 같은 형태의 일반 사이버범죄가 급격한 성장세를 보이고 있었다.

최근 들어 급증하고 있는 일반 사이버범죄의 경우 사이버 상의 불법도박, 피싱(phishing)사이트의 증가, 불법·유해사이트의 증가 등으로 인해, 증가세를 보이고 있으며, 이러한 범죄 들은 주로 금전적인 목적을 위해 저질러지는 경우가 많기 때문에 향후, 지속적인 양적·질적 증가가 예상이 된다.

**표 5. 2003~2010 사이버범죄 발생 및 검거 현황[15]**

| | 총계 | | 사이버 테러형 범죄 | | 일반사이버 범죄 | |
|---|---|---|---|---|---|---|
| | 발생 | 검거 | 발생 | 검거 | 발생 | 검거 |
| 2003 | 68,445 | 51,722 | 14,241 | 8,891 | 54,204 | 42,831 |
| 2004 | 77,099 | 63,384 | 15,390 | 10,339 | 61,709 | 52,391 |
| 2005 | 88,731 | 72,421 | 21,389 | 15,874 | 67,342 | 56,547 |
| 2006 | 82,186 | 70,545 | 20,186 | 15,979 | 62,000 | 54,566 |
| 2007 | 88,847 | 78,890 | 17,671 | 14,037 | 71,176 | 64,853 |
| 2008 | 136,819 | 122,227 | 20,077 | 16,953 | 116,742 | 105,274 |
| 2009 | 164,536 | 147,069 | 16,601 | 13,152 | 147,935 | 133,917 |
| 2010 | 122,902 | 103,809 | 18,287 | 14,874 | 104,615 | 88,935 |

2010년 발생한 사이버범죄 현황을 살펴보면, 사이버 테러형 범죄 중에서는 사용자 도용에 의한 범죄가 가장 많이 차지하였다. 이중에서도 게임계정이 8,827건으로 약 9천 건에 육박하였으며, 그 다음으로 일반계정을 도용한 사건이 5,292건으로 다음을 차지하였다. 그리고 사회에 심각한 영향을 줄 수 있는 자료유출・서비스거부공격・바이러스 유포와 같은 범죄도 각각 105건・40건・124건이 발생하였다.

**표 6. 2010년 사이버범죄 발생 현황[12]**

| | | | | 발생 건수 | 검거 건수 | 검거 인원 |
|---|---|---|---|---|---|---|
| 총 계 | | | | 122,902 | 103,809 | 111,772 |
| 사이버테러형범죄 | | 소 계 | | 18,287 | 14,874 | 16,777 |
| | 해킹 | 단순침입 | | 2,944 | 2,160 | 2,546 |
| | | 사용자 도용 | 일반계정 | 5,292 | 4,506 | 4,934 |
| | | | 게임계정 | 8,827 | 7,169 | 8,112 |
| | | 파일 등 삭제·변경 | | 356 | 328 | 359 |
| | | 자료유출 | | 105 | 75 | 103 |
| | | 폭탄·스팸메일 | | 139 | 138 | 144 |
| | | 서비스거부공격 | | 40 | 35 | 36 |
| | | 바이러스유포 | | 124 | 114 | 121 |
| | | 기 타 | | 460 | 349 | 422 |
| 일반사이버범죄 | | 소 계 | | 104,615 | 88,935 | 94,995 |
| | | 사기 | 통신 | 35,305 | 26,290 | 26,826 |
| | | | 게임 | 11,800 | 8,814 | 9,586 |
| | | 불법복제 | 음란물 | 8,659 | 8,765 | 9,015 |
| | | | 프로그램 | 10,159 | 9,120 | 9,272 |
| | | 불법유해 사이트 | 음란 | 2,364 | 2,672 | 2,796 |
| | | | 도박 | 5,767 | 5,847 | 7,312 |
| | | | 폭발물·자살 등 | 175 | 92 | 171 |
| | | 명예훼손 | | 5,344 | 4,773 | 5,075 |
| | | 개인정보침해 | | 4,529 | 3,770 | 4,253 |
| | | 성폭력 | | 1,021 | 978 | 1,079 |
| | | 사이버스토킹 | | 1,474 | 1,273 | 1,360 |
| | | 협박·공갈 | | 1,908 | 1,614 | 1,730 |
| | | 기 타 | | 16,110 | 14,927 | 16,520 |

일반 사이버범죄는 사이버 테러형의 범죄에 비해 약 10배 정도 더 일어나고 있다. 특히, 일반 사이버범죄에서는 사기범죄가 전체 사이버 테러형 범죄의 세 배나 더 많이 발생하였다. 일반 사이버범죄 중 가장 높은 비율을 차지하는 범죄유형은 컴퓨터를 이용한 사기 범죄로서 통신사기와 게임사기를 합해 총 47,105건의 범죄가 발생하였다.

그 다음으로 불법복제로서 음란물, 프로그램 복제행위 18,818건의 범죄가 발생하였다. 그 밖에 불법 유해사이트가 다음을 따르고 있다.

사이버범죄의 경우 다른 범죄와 달리 연령대가 비교적 낮은 것이 특징이다. 2003년 기준 연령대 비율을 살펴보면, 10대에서 30대까지의 연령대에서 발생한 사이버 범죄가 전체의 90%에 육박하였다. 이러한 추세는 2011년 현재까지 이어져 오고 있다.

과거에 비해 연령대가 높아지기는 하였으나, 여전히 주된 범죄 연령대가 10대에서 30대 사이에서 가장 높은 비율을 차지하고 있다.

**표 7. 사이버범죄 연령별 현황[15]**

| 구분 | 10대 | 20대 | 30대 | 40대 이상 | 기타 |
|---|---|---|---|---|---|
| 2003 | 33.8% | 37.1% | 18.0% | 10.0% | 1.1% |
| 2004 | 26.0% | 36.8% | 22.6% | 12.8% | 1.8% |
| 2005 | 22.8% | 36.9% | 23.9% | 14.8% | 1.6% |
| 2006 | 13.4% | 33.6% | 29.5% | 22.1% | 1.4% |
| 2007 | 15.1% | 39.2% | 26.3% | 17.7% | 1.7% |
| 2008 | 26.6% | 39.0% | 21.8% | 11.8% | 0.8% |
| 2009 | 19.4% | 34.0% | 29.6% | 16.5% | 0.5% |
| 2010 | 19.5% | 39.5% | 25.4% | 14.4% | 1.2% |
| 2011 | 17.6% | 40.2% | 27.2% | 14.7% | 0.3% |

## 2. 사이버범죄의 최근 동향

최근 발생하는 사이버범죄는 초기의 사이버범죄에 비해 진화하는 형태를 보이고 있다. 특히, 사이버범죄는 기존의 범죄와 달리 진화속도가 빠르기 때문에 다양한 형태로 발전하고 있다.

첫 번째로 최근 사이버범죄는 사이버 모욕 등 사이버 폭력이 증가하고 있다. 스마트 폰의 보급과 무선인터넷의 일반화로 인해, 정보에 대한 공유가 활발해진 반면에, 이러한 긍정적인 작용의 문제점으로 인터넷뉴스의 댓글을 통해 근거 없는 각종 모욕 및 명예훼손 행위가 증가

하고 있다. 이러한 사이버 폭력은 아직 확정된 개념은 아니지만 대체로 사이버 공간에서 행해지는 모욕적인 언사나 욕설, 타인에 대한 명예훼손, 음란한 대화 및 성적 수치심을 주는 사이버 성희롱, 인터넷을 통해 성매매를 유도하는 사이버 성매매 등과 같이 물리적인 폭력형태보다는 사이버 공간을 이용하여 정신적 형태의 폭력을 구사하는 유형으로서, 사이버 공간의 활용도가 증가함에 따라 사이버 폭력이 증가하고 있는 실정이다.

두 번째, 인터넷을 활용한 피싱(phishing)사기가 증가하고 있다. 피싱은 공격자가 위장된 금융기관 등의 웹사이트(web site)나 전자메일로 고객을 현혹하여 이들로부터 인증번호나 신용카드번호, 계좌번호 등 금융정보를 취득한 후 이를 불법적으로 이용하여 고객에게 재산상의 손해를 입히는 신종 인터넷사기이다[3].

피싱 사기의 경우 금전을 목적으로 하기 때문에, 지속적으로 발생하고 있으며, 초기의 피싱 범죄에 비해 진화하는 형태를 보이고 있는 특징이 있다.

그 외에도 사이버 사설 도박, 소프트웨어 불법배포 등과 같이 사이버 공간에서 다양한 형태의 사이버범죄가 발생하고 있다. 특히, 최근 발생하고 있는 사이버범죄의 경우 과거 해킹과 같은 전문적인 기술을 가진 형태의 범죄에서 일반인도 쉽게 저지를 수 있는 형태의 범죄로 변화하고 있는 것이 특징이다.

사이버 폭력의 경우 불법적인 사이트가 아닌 합법적인 형태의 뉴스사이트에서 빈번하게 발생하고 있으며, 피싱의 경우 사이버 공간 이외에 일반 휴대 전화기, 스마트폰 등 다양한 루트를 통해 범죄가 이루어지고 있다.

## 3. 경찰대응의 문제점

사이버범죄에 대해서 경찰에서는 1997년 8월 컴퓨터범죄수사대 창설하여, 1999년 사이버 범죄수사대를 거쳐 2000년 현재의 사이버테러대응센터로 발전시켰다. 최초 컴퓨터 범죄수사대는 사이버범죄의 개념보다는 컴퓨터와 관련된 모든 범죄에 대한 수사를 하는 기관에 불과하였으나 1999년 사이버 범죄수사대로 개편, 2000년부터 현재까지 사이버테러대응센터로 영역을 확장하여 현재에 이르고 있다.

### 3.1 예방 및 수사조직의 분산

사이버범죄에 대해 국내의 대응조직은 경찰・검찰・국가정보원・정보통신부 등 다양하게 산재되어 있다. 특히, 각 기관별 업무가 명확하게 분장되어 있는 상황이 아닌 조금씩 중복되어 있으며, 사이버 수사에 있어서 정보 확보를 통해 수사의 진행이 연계되어야 하는 상황임에도 불구하고, 범죄 수사는 경찰과 검찰에게 정보의 확보는 국가정보원과 방송통신위원회에 흩어져 있기 때문에, 효과적인 대응 및 예방을 하기 어려운 문제점이 있다.

특히, 국내의 사이버범죄에 대응하기 위한 기관의 수가 너무 많으며, 중복되어 있는 문제로 인해 수사조직이 분산되어 있는 문제가 있다. 일반적으로 사이버범죄에 대한 단속과 수사기능은 경찰과 검찰에서 실시하고 있으며, 국가정보원에서는 사이버테러와 같은 국가에 심각한 영향을 미치는 국제 사이버범죄 및 심각한 수준의 사이버 범죄에 대해 단속을 실시하고 있으며, 방송통신위원회에서는 사이버범죄 예방을 위한 활동을 실시하고 있다.

그 밖에 사이버범죄 상담・신고 기관으로는 국가사이버 안전센터를 비롯하여 인터넷 침해 대응센터 등 총 16개의 상담・신고 기관이 존재하고 있다. 이중에서 공정거래위원회, 한국소비자원, 한국저작위원회 등과 같이 큰 관련성이 없는 기관까지 사이버범죄 상담・신고 기관으로 등록 되어 있어 전문성 결여와 아울러 예방・수사 조직의 중복으로 인한 문제가 발생하고 있다.

### 3.2 수사상의 문제점

사이버범죄는 현실공간에서 일어나는 범죄와 달리 가상공간에서 이루어지는 범죄이기 때문에 피해사실의 적발이 어려워 암수율을 높이는 원인으로 작용하고 있으며, 타인의 아이디나 비밀번호를 도용하여 불특정 다수를 대상으로 사기행각이나 바이러스를 유포한 경우에는 구체적 피해사실을 파악하기 힘들며, 피해자가 피해범위와 피해실태를 파악하기 어렵게 한다[11].

그리고 경찰내부의 사이버범죄를 전문적으로 수사하는 전문 수사관의 수가 매우 부족하기 때문에, 효과적인 수사가 어려운 문제점이 있다. 현재 경찰에서는 “사

이버테러대응센터"를 통해 사이버범죄에 대한 예방과 수사를 동시에 진행하고 있는데, 과거에 비해 많은 전문 인력이 증원되기는 하였으나, 국내에서 발생하는 사이버 범죄에 대한 수사 및 단속을 하기에는 여전히 인력 및 장비가 부족한 실정이다.

### 3.3 제도적 한계

사이버 공간에서 벌어지는 범죄는 비교적 진화속도가 빠르기 때문에, 이에 적절한 대응이 어려운 것이 사실이다. 범죄의 진화속도에 비해 대응하기 위한 제도적 변화 속도는 이를 따라가는데 어려운 것이 현실이다. 또한 결과범만 처벌을 할 수 있고 미수범에 대한 처벌규정이 없는 문제점을 가지고 있으며, 법적근거는 있지만 단속기준에 관한 해석이 시대적 상황이나 법관에 따라 달라짐으로서 단속상의 혼동을 초래하는 경우가 있다[11].

또한, 사이버 공간의 특성상 디지털 증거의 확보가 어려운 문제점이 있다. 전자적 증거가 갖는 제반 특성으로 무체 정보성, 변조 용이성, 원본과 구별 불가능성, 대량성, 전문성이라는 특성을 고려하여 수사를 진행해야 함에도 불구하고, 법적・제도적인 어려움이 있는 실정이다[13].

### 3.4 업무의 과다

사이버범죄의 특성 상 불법적인 명령어를 가진 파일의 복제 및 자가 증식과 함께, 사이버범죄를 실행하는 기술의 발달에 비해 늦은 대응기법의 도출과 같은 기술적인 특성으로 인해, 많은 범죄가 발생하는 것에 비해 관련 업무를 수행할 수 있는 인원이 턱없이 모자라는 것이 사실이다. 특히, 사이버범죄를 예방하고 수사하기 위한 전문요원은 경찰을 비롯한 국가정보원 등에서 근무하고 있는데, 이들의 수는 제한적인 반면에 사이버범죄의 실태에서 나타난 바와 같이 지속적으로 급증하고 있는 추세에 있다.

그리고 사이버범죄를 저지르는 기술이 새롭게 개발되고 진화되고 있는 반면에 경찰을 비롯한 국가기관의 사이버 예방 기술은 대응속도가 더딘 문제점을 지니고 있다. 따라서 일반 범죄에 대한 예방을 민간경비업체와 함께 나누어 진행하는 것을 바탕으로 사이버범죄 역시 전문 민간업체와 함께 업무를 나눌 필요성이 증대되고 있다.

## Ⅳ. 민간경비를 활용한 사이버범죄 예방 방안

나날이 증가하고 있는 사이버범죄에 대한 예방방안을 살펴보면, 우선 사이버범죄의 특성을 바탕으로 접근해야 한다. 사이버범죄에 대해 일반 민간차원에서의 시민적 대응은 국가의 공식적인 대응능력을 보충할 수 있다고 한다[9]. 따라서 사이버범죄는 국가기관에서 관리한다는 기존의 개념을 바꾸어 민간경비를 활용한 사이버 범죄 예방 및 수사법에 대하여 제시해 본다.

### 1. 민간경비 업무영역의 확장

기존의 경비업법에서 민간경비원의 업무범위는 시설경비업무, 호송경비업무, 신변경비업무, 기계경비업무, 특수경비업무로 나뉘어져 있으며 사이버보안 업무는 민간경비원의 업무에 속해있지 않다. 그렇기 때문에 민간경비를 사이버범죄에 활용하기 위해서는 경비업법 개정을 통해 사이버보안 업무 또한 민간경비의 업무로 규정해야 한다.

미국의 사이버보안 정책을 살펴보면 오바마 대통령은 취임 후 기존의 사이버보안을 60일의 기한 내에 총체적으로 점검하도록 지시를 내렸고 그에 따라 검토보고서를 발표하는 등 이전과 차별된 사이버보안정책을 추진하고 있다. 이처럼 미국 또한 사이버범죄를 예방할 수 있는 사이버보안의 중요성을 일찌감치 깨닫고 그에 대한 대비를 하기 위한 법과 제도를 정비하고 있다. 우리나라 또한 미국과 같이 사이버범죄를 예방하기 위해 법과 제도의 정비가 필요하다.

특히, 사이버범죄의 특성 상 국가기관에서 사이버범죄를 예방하는 데에는 한계를 가지고 있다. 따라서 사이버범죄를 예방하기 위해서는 민간경비업의 영역을 확장할 필요성이 증대되고 있다.

민간경비업의 영역을 확장하기 위해서는 기본적으로 사이버범죄를 예방하는 업무의 개념을 바꾸어야 한다. 사이버범죄는 특별한 형태의 범죄이기 때문에 전문성을 가진 전문가에 의해 해결해야 하는 것이 특징이다.

따라서 사이버범죄를 예방하기 위하여 업무영역이 민간으로까지 확장될 수 있도록 경비업법을 개정하여 사이버범죄 예방을 위한 활동을 할 수 있도록 제도적 장치를 마련해야한다.

## 2. 민간 사이버보안요원 육성

사이버범죄를 예방하기 위해서는 우수한 사이버보안요원들이 육성되어야 한다. 일반적인 교육경로를 통해 양성된 컴퓨터 전문가들 또한 우수한 인적자원이지만 그와는 반대로 일반인들 중에서 일반적인 교육경로를 거치지 않은 자신만의 독자적인 방법으로 컴퓨터를 공부한 사람들 또한 필요하다. 그러나 그러한 컴퓨터 전문가들은 자신의 과거경험 등 여러 가지 이유로 경찰, 국정원 등 국가기관에 일정한 거부감이 있기 때문에 에스원, 캡스, KT 텔레캅 등 민간경비업체에서 나서서 이들을 육성하는 것이 바람직할 것이다.

이를 위해서는 컴퓨터 해킹 대회 등의 관련 대회 개최를 통해 컴퓨터 전문가들을 선발하고 사이버범죄를 통해 체포된 경력이 있는 전문가들을 회유하여 사이버보안요원으로 활용한다. 그리고 인터넷상의 유명한 해커들을 섭외하여 해킹을 막는 사이버보안 요원이 되도록 설득한다.

갈수록 해킹의 방법이 교묘해지고 다양해지므로 이러한 방법들에 대응하기 위해서는 다양한 배경을 가진 전문가들이 필요하다. 기존의 기성세대들의 방법으로는 점점 더 해킹을 막기가 어려워져가고 있다. 그래서 좀 더 창의적인 방법의 사이버범죄 대응이 필요하다.

그리고 화이트 해커와 같은 모의해킹이나 다른 취약점 점검 등의 기법에 전문적인 보안전문가들과 교류를 통해서 사이버보안 시스템에 대한 취약점을 점검하고 해킹을 직접적으로 막는 경험을 통해서 해킹에 대한 대응전략을 구상할 수 있다.

## 3. 경찰이 나서지 못하는 사이버범죄에 대응

사이버공간을 통한 범죄는 실체가 없기 때문에 피해를 당한다고 해도 쉽게 경찰서로 찾아갈 수 없으며 경찰에 신고하더라도 경찰이 해줄 수 있는 방법이 딱히 없는 실정이다. 특히 스토킹과 같은 범죄의 경우는 피해자를 보호할 장치나 피의자를 처벌할 법조차 마련되어 있지 않다. 이를 악용해서 스토커들은 스토킹 대상의 컴퓨터를 해킹하거나 블로그, 미니홈피, SNS 등을 해킹하여 상대의 일거수 일투족을 감시하는 등 그 수단이 교묘해지고 있다.

이러한 범죄에 대응하기 위해 민간경비업체는 여러 가지 서비스를 제공할 수 있다. 해킹과 같은 사이버범죄를 예방하는 것은 물론이고, 사이버범죄로 인한 피해의 증거 수집을 통해 경찰에 고발할 때 증거로 제출하는데 도움을 줄 수 있다. 사이버범죄는 지속적으로 발전하고 있지만 법과 제도는 그것에 따라가지 못하고 있는 실정이다. 그렇기 때문에 공적인 사법기관이 개인을 위해 나서지 못할 때 민간기업인 민간경비업체가 나서서 그 부족함을 보완할 수 있다.

## 4. 사이버범죄에 대한 컨설팅 업무

사이버범죄나 사이버보안에 대한 일반 사람들의 인식은 그리 높지 못하다. 컴퓨터와 스마트폰은 사람들이 가장 친근하게 어디에서든지 사용되고 있지만 거기에 범죄라는 것이 결부되면 자기와는 먼 느낌이드는 것이 사실이다. 하지만 최근에 문제가 되고 있는 기업체에서의 고객정보 유출사고에서 볼 수 있듯이 사이버범죄는 한 번에도 수백만 명의 피해자가 생길 수 있는 범죄이고 자신이 피해를 입고 있는지조차 확실하게 알 수가 없다.

이를 위해서는 사이버범죄에 대한 홍보를 통해 국민들에게 사이버범죄에 대한 경각심을 갖게 하는 것이 중요하다. 이를 위해 사이버범죄에 전문적인 지식을 가지고 있는 민간경비업체 전문가들이 일반시민들에게 사이버범죄의 유형과 사례 등을 소개하면서 어떠한 경우에 사이버범죄에 노출이 될 수 있는지를 숙지시키는 것이 좋다.

또한 일반시민들 뿐만 아니라 기업체에 구성원들 또한 기업이 가지고 있는 중요한 정보들과 주요 산업기술들을 빼내가기 위한 사이버범죄의 타겟이 될 가능성이 높다. 이를 예방하기 위해서 기업체의 임원과 직원들에게 사이버범죄를 예방할 수 있는 보안교육을 통해 범죄가 발생하는 것을 막아야 한다.

최근에는 사람의 심리를 이용한 휴먼해킹이 기승을

부리고 있다 각 기업이나 기관의 내부기밀 혹은 개인정보를 노리는 해커들이 사람들이 방심하는 순간을 노리는 것이다. 무심결에 주운 USB를 컴퓨터에 사용한다면 보안시스템에 의해 메모리에 설치된 악성코드가 걸러지면 다행이지만 보안시스템이 없는 PC에 사용했다간 내부데이터가 유출되거나 해커에게 PC의 통제권을 넘겨 줄 수 있다[14].

그리고 직접적으로 정보나 기술을 다루는 사람들보다는 사이버 보안의식이 낮으면서 직접적으로 기술이나 정보를 다루지 않는 부서의 사람이나 하청업체, 그리고 가족과 같은 주변 사람들을 노리는 방식으로 이루어지고 있기 때문에 사이버범죄 예방교육을 통한 일반 국민과 기업구성원 모두의 사이버 보안의식을 높여야 한다.

## V. 결 론

첨단과학기술의 발달은 우리에게 많은 장점을 주었다. 특히, 범죄예방에 있어서 다양한 형태로 영향을 주었다. 그러나 반대적 형태로 범죄에 악용되고 있는 사례가 종종 발생하고 있다. 최근에는 사이버범죄 중에서 사이버 모욕 등과 같은 사이버 폭력이 증가하고 있으며, 피싱과 같은 형태의 사기 범죄가 증가함과 동시에 사이버 사설도박, 소프트웨어 불법배포 등과 같은 형태의 범죄가 급증하는 것으로 나타나고 있으나 경찰의 예방 및 수사조직의 분산, 사이버범죄의 특성으로 인한 수사상의 문제점, 빠른 진화속도를 따라가지 못하는 제도적 한계가 여러 선행연구에서 문제점으로 지적되고 있다.

따라서 이 연구에서는 사이버범죄의 예방에 대해서 기존의 경찰중심적인 형태의 예방에서 벗어나 전문성을 갖춘 민간경비 업체에서의 예방을 제안해 본다. 먼저 경비업법 개정을 통해 민간경비의 업무영역에 사이버보안이 포함되어야 한다. 그래야만 민간경비가 사이버범죄를 예방하는 업무를 수행할 법적인 근거가 된다. 그리고 서버룸과 같은 컴퓨터시설에 대한 물리적 경비를 통해 내부자나 타인의 접근을 통제한다. 다음으로 우수한 사이버보안요원 육성을 위해서 에스원, 캡스 등과 같은 민간경비업체에서 여러 가지 배경을 가진 다양한 컴퓨터 전문가들을 섭외하여 점점 더 다양하고 교묘해지는 사이버범죄에 대처해야 한다. 그리고 법령의 미비로 경찰이 나서지 못하는 사이버범죄 피해에 대해 민간경비가 나서서 그 피해를 예방해야 한다. 또한, 일반 시민들과 기업체 조직원들에 대한 사이버범죄 예방 교육을 통해 사이버 보안의식을 높여야 한다.

이제 사이버 범죄도 기존의 5대 범죄 못지않은 범죄로 양적·질적으로 성장하게 되었다. 그로 인해 많은 피해자가 양산되었고, 경찰과 검찰 등 국가기관에서 담당하고 있는 예방 · 단속 및 수사 활동이 실패하고 있다고 볼 수 있다. 따라서 국가기관의 범죄예방활동 실패를 보완하는 개념으로 민간경비를 활용한 방안을 제안해 본다.

## 참 고 문 헌


[1] 이정훈, "사이버범죄학의 동향과 전망", 경찰법연구, 제9권, 제2호, pp.194-220, 2011.

[2] 이병종, "테크놀로지 발전에 따른 사이버 범죄의 진화와 범죄현상의 조명 및 대응", 한국공안행정학회보, 제38권, pp.173-201, 2010.

[3] 정 완, "사이버 범죄의 실태와 동향 및 대응책", 홍익법학, 제10권, 제1호, pp.195-224, 2009.

[4] 허경미, *현대사회와 범죄*, 박영사, 2005.

[5] 양근원, "사이버 범죄의 특징과 수사방향", 수사연구, 2000(6).

[6] 양근원, 장윤식, 사이버범죄수사론, 경찰대학, 2008.

[7] 전지연, "사이버 범죄의 과거, 현재 그리고 미래", 형사법연구, 제19권, 제3호, pp.3-32, 2007.

[8] 강동범, "사이버 범죄 처벌규정의 문제점과 대책", 형사정책, 제19권, 제2호, pp.33-54, 2007.

[9] 권오걸, "사이버 범죄와 대응전략", 법학연구, 제36권, pp.191-216, 2009.

[10] 김대권, "사이버 마약에 대한 범죄심리학적 고찰

과 그 대책", 한국범죄심리연구, 제10권, pp.3-29, 2010.
[11] 박창욱, "사이버 범죄에 대한 효율적인 경찰대응 방안에 관한 연구", 한국컴퓨터정보학회 동계학술발표논문집, 제15권, 제2호, pp.139-146, 2007.
[12] 경찰청, 2010 경찰통계연보, 경찰청, 2011.
[13] 노명선, "사이버 범죄의 증거확보에 관한 몇 가지 입법적 제언", 성균관법학, 제19권, 제2호, pp.341-356, 2007.
[14] http://news.kukinews.com/article/view.asp?page=1&gCode=kmi&arcid=0005949826&cp=du
[15] http://www.netan.go.kr/

## 저 자 소 개

**김 상 운(Sang-Woon Kim)** 정회원

- 1996년 2월 : 동국대학교 경찰행정학과(행정학사)
- 2008년 8월 : 계명대학교 정책학과(행정석사)
- 2012년 2월 : 동국대학교 경찰행정학과(경찰학박사)

- 현재 : 대구가톨릭대학교 경찰행정학과 교수

<관심분야> : 경찰교육, 경찰인사, 조직관리

**조 현 빈(Hyun-Bin Jo)** 정회원

- 1999년 2월 : 동국대학교 경찰행정학과(행정학사)
- 2001년 8월 : 동국대학교 경찰행정학과(법학석사)
- 2004년 8월 : 동국대학교 경찰행정학과(경찰학박사)

- 현재 : 순천향대학교 경찰행정학과 교수

<관심분야> : 청소년범죄, 위기관리, 경찰조직, 경찰인사