Korean Review of Crisis & Emergency Management 10(3) Mar. 2014 73-93
Available online at www.cemtp.re.kr

사이버 국제범죄에 대한 동북아 사이버 범죄센터 설립 방안
Establishment Way of Northeast Asian Cyber Crime Center for International Cyber Crime

Jae Hun Shin**, Sang Woon Kim***
Police Administration, Catholic University of Daegu, 13-13 Hayang-ro, Hayang-eub, Kyungsan-si, Kyungbuk, Korea

Abstract

From the late 20th century, the human race create Cyber Space for more wider ideas and activities out of the existing physical space, endless imagination and thoughts to create a place where you can get action with the spread of globalization was widespread. Cyberspace has typical characteristics that is temporal, physical and spatial unconstraint, Because of this, it has a number of advantages in daily life such as real-time processing tasks to do. But recently, Illegal practices that take advantage of cyberspace is creasing and has become a serious social problem. In particular, today's cyber crime across borders without the physical movement of criminals and to be able to commit a crime and it takes on the nature of international crime. As a result, cyber criminals can not be processed in the country. Because of the international criminalization of cybercrime, beginning with the Council of Europe Criminal matters in 1985, through a lot of international conference to aware about cybercrime and the severity. Until now, the world are trying to resolve the problem through Interpol and Europol, through each of the related institutions. Among them, the Europol Cybercrime center opened in 2013 and taking action against international form of cybercrime which is raised in Europe. In this study, we suggest Northeast Cyber Crime Center recognizing the problem of increasing international cybercrime, to solve Cyber international cybercrimes occurring around the world and in China and Taiwan, and Korea. Especially, rather than such agency as Interpol for simply sharing information, we suggest Northeast Cyber Crime Center that has expertise and real-time information sharing, investigations of the grant, which can be substantial international cooperation.

Key words: cybercrime, europol, international cybercimre, cyberterrorism, cyber crime center.

* Tel. +82-10-9152-5868. E-mail. enfant21@naver.com
** corresponding author. Tel. +82-53-850-3340. E-mail. ksw481@naver.com

Submission & Publication Process
Received: Jan. 7, 2014 / Revised: Feb. 28, 2014 / Accepted: Mar. 15, 2014

국문초록

20세기 후반부터 인류는 기존의 물리적인 공간에서 벗어나, 보다 넓은 생각과 활동을 위한 사이버공간(Cyber Space)을 창조하여, 무궁무진한 상상과 생각을 실행에 옮길 수 있는 장소를 만들어 세계화의 확산과 함께 널리 퍼지게 되었다. 사이버 공간은 시간적・물리적・공간적 무제약성을 대표적인 특징으로 가지고 있는데, 이로 인하여 실시간으로 업무를 처리하는 등 일상생활에 많은 장점을 주기도 하였으나, 최근에는 사이버 공간을 불법적으로 활용하는 사례가 증가하고 있어 심각한 사회문제가 되고 있다. 특히, 오늘날 사이버범죄는 범죄인의 물리적 이동 없이 국경을 초월하여 범죄를 저지를 수 있게 되어 국제범죄의 성격을 띠게 되었다. 그 결과 사이버범죄는 한 국가에서 처리할 수 없는 상황이 되었다. 사이버범죄의 국제범죄화로 인하여, 1985년을 형사문제 유럽회의를 시작으로 많은 국제회의를 통해 사이버범죄에 대한 심각성을 인식하고, 해결방안을 찾고자 전 세계는 지금까지도 인터폴 및 유로폴, 각 관련기관 등을 통하여 문제해결을 위하여 노력하고 있다. 이 중에서도 유로폴에서는 사이버 범죄센터를 2013년에 개소하여 유럽지역에서 발생하는 국제적인 형태의 사이버범죄에 대하여 대응하고 있다. 이 연구에서는 급증하고 있는 사이버 국제범죄에 대한 문제점을 인식하고 전 세계적으로 사이버 국제범죄를 발생시키고 있는 중국・대만・우리나라의 사이버 범죄를 해결하기 위하여, 동북아 사이버 범죄센터 설립을 제안해 보았다. 특히, 인터폴의 사례에서처럼 단순히 정보공유를 위한 기관이 되기보다는, 유로폴의 사이버 범죄센터와 같이 전문성을 가지고, 실시간 관련정보 공유, 수사권의 부여, 실질적 국제공조 등을 할 수 있는 동북아 지역 사이버 범죄센터를 제안해 보았다.

주제어: 사이버범죄, 유로폴, 사이버 국제범죄, 사이버테러리즘, 사이버범죄센터

Ⅰ. 서론

20세기 후반부터 인류는 기존의 물리적인 공간에서 벗어나 보다 넓은 생각과 활동을 위한 사이버공간(Cyber Space)을 창조하였다. 사이버공간은 시간적・공간적 제약이 많았던 물리적 공간에서 벗어나 무궁무진한 상상과 생각을 실행에 옮길 수 있는 장소로서, 20세기 후반부터 정보기술의 발달과 세계화의 흐름으로 인하여 널리 퍼지게 되었다.

사이버공간은 다양한 가능성이 많은 가상의 공간으로서 시간적・물리적・공간적인 제약이 없는 것이 특징이다. 그로 인하여 다양한 일들을 실시간으로 처리할 수 있어, 인터넷 및 모바일을 활용한 금융활동, 인터넷 및 관련 서버를 활용한 사무활동, 기타 사이버 공간을 활용한 일상생활 등 다양한 영역에서 이용되고 있다.

사이버 공간의 활용도가 높아짐에 따라, 사이버 공간을 불법적으로 활용하는 사례가 증가하고 있다. 특히, 오늘날 사이버범죄는 사이버 공간을 이용하여 컴퓨터나 정보시스템을 침해하기 때문에 범죄인의 이동 없이 물리적 경계라고 할 수 있는 국경을 얼마든지 초월하여 범죄가 발생될 수 있게 됨으로써, 특정 국가의 노력과 법 제정만으로는 효과적인 방지와 제재가 이루어지기 어려운 지경에 이르렀다[1].

그로 인하여, 사이버범죄로 인하여 발생하는 범죄경제적 비용은 점점 증가하고 있는 추세에 있다. 사이버범죄로 인하여 부당하게 벌어들이는 수익이 마약범죄로 인하여 얻는 수익을 초과하고 있다고 한다. 1980년대 초반만 해도 사이버범죄는 다른 전통적인 범죄와 다른 형식의 유형으로 분류되었으나, 현재 바이러스 유포, 해킹, 사이버 포르노, 사이버 테러, 스팸 메일과 같은

유형들은 이미 전통적인 범죄유형에 포함시켜야 될 정도로 사이버범죄는 급격한 변화를 거치고 있다[2]. 그리고, 국가 간 범죄행위가 유리하다는 기술적 특성으로 인하여 사이버범죄는 인터넷을 이용하여 초국가적 국제범죄화 현상이 가속화되고 있다. 특히, 정보통신망의 발달로 물리적으로 발생하는 고비용을 획기적으로 절감시키게 되어 사이버 범죄는 한 국가나 지역에서 국한된 형태의 범죄가 아닌 국제적인 형태범죄로 발전되어 국제사회는 초국가적인 문제라는 공통적인 인식을 가지게 되어 사이버 국제범죄에 대한 국제공조의 필요성을 인식하였다.

초국가적이 형태의 사이버범죄를 해결하기 위한 국제공조는 많은 어려움을 가지고 있는데, 그 중에서 가장 큰 문제는 각국의 수사상의 형사소송법과 관련된 문제이다. 국제공조수사란 각 국가의 수사기관 간에 수사 활동을 위하여 상호 협력하는 것으로서, 일반적으로 국내에 국한되는 수사 활동이 다른 나라에 영역의 영역에까지 미쳐야 하기 때문에 범죄인의 소재파악 및 추적수사에서부터 체포・송환・증거 수집 등 많은 부분에서 외국과의 협조가 필요하다. 그러나 실제로는 사이버 국제범죄의 경우 각국의 무체정보에 대한 증거능력을 인정하는 기준이 상이하고, 이에 대한 입법적인 문제해결과 함께 '초국가성'을 띠고 있는 사이버범죄의 특성을 고려해야 하기 때문에 국제공조가 효과적으로 이뤄지지 않고 있다.

따라서, 이 연구에서는 효과적인 국제적인 형태의 사이버범죄를 해결하기 위한 방안으로서 사이버 국제범죄에 대한 심각성을 인식하고, 사이버 국제범죄의 특성과 현황, 외국의 사례를 바탕으로 동북아지역의 사이버 국제범죄를 예방 및 수사할 수 있는 국제적인 형태의 사이버 범죄센터 설립을 제안한다. 이 연구는 위에서 언급한 목적을 달성하기 위하여, 선행연구로 사용되었던 각종 관련 논문과 인터넷 자료를 활용하였다.

II. 사이버 국제범죄의 의의

1. 사이버 국제범죄의 정의

사이버 국제범죄는 사이버범죄와 국제범죄가 합쳐진 형태이기 때문에 사이버범죄와 국제범죄에 대하여 먼저 이해해야 한다. 기존의 국제범죄는 전통적인 형태의 범죄였으나, 사이버공간에서 무분별하게 발생하는 특성을 반영하기 때문에 사이버 국제범죄를 논하기에 앞서 사이버범죄를 먼저 이해해야 한다.

사이버범죄는 그 현상을 표현하기 위해 만들어진 신조어로 완전한 내포(connotation)를 포함하는 개념 정의가 어려우나, 네트워크의 발달로 인하여 단순 컴퓨터범죄와 사이버범죄와의 구분실익이 없으며, 최근 발생하는 모든 컴퓨터범죄가 사이버공간에서 이루어지고 있기 때문에, 컴퓨터 및 모바일 등과 같은 기기를 활용한 사이버공간에서 이루어지는 모든 유형의 범죄라고 정의할 수 있다.

따라서, 사이버 국제범죄는 개인수준에서 발생하였던 전통적인 형태의 사이버범죄와 국제범죄적인 성격이 강조되고 있다. 사이버 국제범죄는 기존의 사이버범죄와 달리 '초국가성'이 중요시 되기 때문에 사이버 국제범죄를 논함에 있어 반드시 고려되어야 한다.

앞에서 언급한 바와 같이 사이버범죄에 대한 정의는 학자별로 정의를 달리하고 있으나, 사이버공간에서 발생하는 범죄라는 것으로 의견을 일치할 수 있었다.

이러한 사이버 국제범죄에 대하여 박성훈(2012)은 사이버 국제범죄에 대하여 사이버공간에서 발생하는 범죄로서 범죄동기를 지닌 행위주체가 개인이 아닌 집단이며, 범죄의 양상이 일국수준을 넘어 발생하는 것을 의미한다고 하였다[3].

최근에 발생하는 사이버 국제범죄는 국제적으로 발생하는 경향이 강하기 때문에 범죄자를 효율적으로 검거하고 그 불법이익을 환수하기 위하여 수사단계에서의 국제사법공조・범죄인인도・몰수추징과 같은 국제공조가 긴밀하게 이루어져야 한다.

사이버범죄 역시도 공간적인 무제약성을 가지고 있으며, 사이버 국제범죄도 공간적인 무제역성을 가지고 있다. 따라서, 이 둘을 명확하게 비교하기는 어려우나 사이버 범죄를 가하는 대상이 일국에 그치지 않고 2개국 이상의 범죄지를 가지는 것으로서 구분할 수 있으며, 바라보는 관점에 따라서는 조직성을 포함하기는 하지만, 기본적으로 사이버 국제범죄는 2개국 이상의 범죄지를 가지는 유형의 사이버범죄라고 정의할 수 있다.

2. 사이버 국제범죄의 유형

이 연구에서 주로 살펴볼 사이버 국제범죄의 유형은 일반적으로 발생하는 사이버범죄의 유형과 크게 차이를 보이고 있지 않지만, 사이버 국제범죄는 범죄동기를 지닌 행위주체가 개인이 아닌 조직적인 특성을 가지고 있으며, 범죄가 초국가적인 국제범죄의 특성을 가지고 있기 때문에 이러한 특성을 바탕으로 사이버 국제범죄를 분류하였다.

박성훈(2012)에서는 사이버 국제범죄를 사이버테러리즘(Cyber Terrorism)・핵티비즘(Hacktivism)・사이버경제범죄(Cybercrime Economy)로 분류하였다. 첫 번째, 사이버테러리즘(Cyber Terrorism)은 사이버범죄에서 언급하였던 유형의 범죄로서 사이버테러리즘은 이전보다 덜 위험한 상황에서 자신들이 활동할 수 있으며, 사이버공간에서 발생하기 때문에, 현실공간에서의 테러에 비해 유리하면서도 공격에 성공할 경우 파괴력과 사회적 혼란은 현실 공간의 테러 못지않다는 점에서 갈수록 활용도가 높아지는 사이버 국제범죄 유형이다[3].

두 번째, 핵티비즘(Hacktivism)은 정치・사회적 목적을 위하여 자신과 다른 정치적 노선과 이념을 가진 기업・정부・개인・단체 등을 해킹하는 유형의 사이버 국제범죄로서, 해커(hacker)와 행동주의(activism)의 합성어이다.

인터넷이 일반화되면서 나타난 새로운 유형의 정치적・사회적 행동주의를 말한다. 기존의 정치・사회 운동가들이 사이버 공간으로 활동영역을 넓히면서 그들을 추종하거나, 혹은 그들 중에서 해킹기술로 자신과 다른 정치적 노선・이념을 가진 상대의 웹사이트를 해킹하여 조롱하거나 무력화하는 사이버범죄의 유형이다. 이들은 기존의 해커(Hacker)와는 달리 허술한 컴퓨터 보안장치를 해킹함으로써 자신의 실력을 과시하거나 자기만족에 그치는 것이 아니라, 자신의 정치적·사회적 목적을 이루기 위해 적극적이면서도 다양한 활동을 벌인다. 2000년 이후 급속히 늘어나 전 세계에서 광범위하게 활동하고 있는데, 웹 사이트를 침범해 해당 사이트에 자신들의 정치 구호를 내거는 단순한 경우에서부터 아예 상대방의 컴퓨터 서버를 무력화시키는 경우까지

다양하다[1].

세 번째는, 사이버경제범죄(Cybercrime Economy)는 사이버 상의 범죄활동으로 경제적 이익을 얻는 유형으로서, 전자상거래를 통한 사기・기망, 인터넷을 통한 불법밀수, 불법자금에 대한 금융세탁, 이메일을 통한 피싱(Phishing), 사이버 스파이 행위 등이 있다[3].

사이버경제범죄는 경제적 이윤을 목적으로 하고 있기 때문에, 사이버 공간을 도구적으로 이용하는 전통적인 범죄의 형태와 크게 다르지 않다. 다만 사이버 공간의 무제약성, 과학기술의 발달로 인하여 그 진화속도가 빠른 것이 특징이다.

<Table 1> The Type of International Cyber Crime

	사이버테러리즘	핵티비즘	사이버경제범죄
행위주체	국가 혹은 조직	조직 혹은 집단	조직 혹은 집단
범죄목적	기간시설 파괴, 사회혼란	반세계화, 정치적 자유	경제적 이윤
범죄피해	국민전체(불특정 다수) 매우 높음	정부, 기업, 해당기관 높은편	개인(집단)피해자 낮은편
사이버공간의 인식 및 활용	목적 혹은 수단	사이버공간 자체가 목적	도구적 수단
법적처벌 가능성	수사 및 법적처벌의 어려움	수사 및 법적처벌의 모호함	수사 및 법적처벌 가능
범죄발생이론	탈냉전과 세계화	갈등이론, 학습이론	아노미이론, 범죄기회이론

※ Source: [3].

3. 사이버 국제범죄의 특성

사이버 국제범죄는 사이버범죄의 특성과 함께 사이버 국제범죄가 가지는 몇 가지 특성을 추가로 가지고 있다. 첫 번째, 범죄자・피해자・범죄수단・범죄수익・증거자료의 국가 간 분산을 특성을 가지고 있다. 사이버 국제범죄의 경우 2개국 이상을 거쳐 범죄가 이루어지기 때문에, 하나의 범죄가 발생하더라도 2개국 이상의 국가에 증거자료가 분산되는 특성을 가지고 있다.

두 번째, 범죄의 조직화・분업화・국가 간 기술 간격의 이용하는 특성을 가지고 있다. 최근 발생하는 사이버범죄는 복잡한 보안체계를 뚫어야하기 때문에 전문성이 더욱 요구되고 있으며, 단독으로 이뤄지기 어렵기 때문에 조직적인 활동을 하고 있다. 실제로 사이버 국제범죄집단은 국제적으로 전문화 조직화 되어 있는 경우가 대부분이다. 최근에는 추적을 피하기 위하여 그들의 근거지를 기술적인 간격(Digital Divide)이 있는 곳을 이용하기도 한다.

세 번째, 유비쿼터스(Ubiquitous) 환경에서 발생하는 특성을 가지고 있다. 사이버공간에서 이루어지는 모든 활동들은 시간과 공간을 초월하는 특성을 가지고 있다. 사이버공간에서 발생하는 범죄 역시 사이버공간에서 가지는 특성을 그대로 가지고 있다. 이러한 특성은 전통적인 범죄와 달리 시간과 공간을 초월하기 때문에 범죄를 저지르는데 있어 시간과 공간의 벽을 훌쩍 뛰어넘는 획기적인 유비쿼터스(Ubiquitous)의 특징을 가진다[4].

1) 네이버검색, 2013년 10월 7일 검색, http://terms.naver.com/entry.nhn?docId=1222109&cid=200000000&categoryId=200000169.

네 번째, 관할권의 복잡성이라는 특성을 가지고 있다. 사이버범죄의 초국가성은 속지주의를 기본으로 하는 각국의 사법관할권의 표준을 무너뜨린다. 관할권이란 기초적으로 영토를 기본으로 하기 때문에 범죄 발생지가 불분명한 사이버 공간에서의 관할권 설정이 더욱 곤란하게 만들며, 사이버범죄는 행위자와 행위자가 다른 격리범인 경우가 많고, 그 행위 결과도 많은 나라에 동시적으로 발생하기 때문에 속지주의를 규정한 많은 나라들의 관할권 충돌이 야기되므로 행위지와 결과지에 대한 합리적 결정 기준도 요구된다[4]. 이렇듯 사이버 국제범죄는 일반적인 사이버범죄와 달리 2개국 이상을 거치기 때문에 기술적으로 진화하였으며, 초국가적인 공간을 활용하기 때문에, 기존의 사이버범죄에 비해 더욱 복잡하고 처리하기 곤란한 형태를 가지고 있다.

4. 사이버범죄 현황

1) 국내 사이버범죄 발생현황

사이버범죄 발생건수는 2007년 88,847건 이었으나, 2009년 164,536건으로 불과 2년 사이 두 배 이상 증가하는 모습을 보였다. 2009년을 기점으로 서서히 줄어들어 2012년에는 108,223건으로 점점 줄어드는 추세에 있다. 반면 사이버범죄에 대한 검거건수는 사이버범죄의 발생과 같이 2009년까지 증가하는 모습을 보였으며, 2008년에는 전년 대비 사이버범죄 검거건수가 55%나 증가하는 모습을 보였다. 이후, 사이버범죄의 감소와 모습을 같이하여 2012년에는 84,932건으로 줄어드는 것으로 나타났다.

<Table 2> 2007~2012 Status of Cyber Crime and Arrest

	2007	2008	2009	2010	2011	2012
발 생	88,847	136,819	164,536	122,902	116,961	108,223
사이버테러형범죄	17.671	20,077	16,601	18,287	13,396	9,607
일반사이버범죄	71,176	116,742	147,935	104,615	103,565	98,616
검 거	78,890	122,227	147,069	103,809	91,496	84,932
사이버테러형범죄	14,037	16,953	13,152	14,874	10,299	6,371
일반사이버범죄	64,853	105,274	133,917	88,935	81,197	78,561
검거율(%)	88.8	89.3	89.3	84.5	78.2	78.5

※ Source: [5].

2007년 이전의 사이버범죄에 대한 대응은 미숙하였다. 사이버범죄에 대한 인식의 부족, 그로 인한 개념의 미정립, 대응방안의 부족 등으로 인하여 정확한 피해를 산출하는 것조차 쉽지 않았다. 그러나 2007년 상반기부터 경찰청과 민간업체, 한국소비자보호원 등 관련기관과의 협력을 통하여, 경찰청 홈페이지를 비롯한 포털사이트, 카페 등에 '사기피해 방지를 위한 10계명'을 제작하여 배포하는 등 대국민 사기피해 예방에 주력한 결과 사기피해 발생건수가 현저하게 감소하게 되었고, 타인의 주민등록번호 사용에 대하여 처벌토록 '주민등록법'을 개정하여 타인의 주민등록번호를 부정하게 사용한 자를 처벌할 수 있게 되었으며, 경찰청에서는 포털사이트 등과 협의하여 법률개정에 대한 홍보안내문 및 경고문구 등을 게재하여 개인정보침해사범 발생건수가 감소하게 되었다.

2009년도 대비 2010년도 발생대비 검거건수가 감소한 원인으로는 '사행행위 집중단속'과 '저작권법 침해사범 검거'가 큰 원인이 된 것으로 분석된다. 2008년부터 바다이야기 등 성인게임장 및 인터넷 불법 도박이 급속하게 증가하여 2009년에는 심각한 사회문제로 대두되자, 경찰은 '서민경제 침해사범 집중단속'을 실시하여 2010년 이후 도박사범이 현저하게 줄어들었다.

2011년에 전년대비 감소한 것은 사이버 테러형 범죄 중 일반 인터넷 계정 및 게임계정 탈취 등의 사용자 도용건수에 대한 피해자 신고가 대폭 감소한 것에 기인하며, 최근 보안의식 강화 등으로 개인상대 계정 탈취는 감소한 반면, 기업을 상대로 한 대형 해킹사건이 발생하였기 때문에 개인 신고가 감소한 것으로 추정된다.

최근 발생하는 사이버범죄는 발생건수는 과거에 비해 감소하였으나, 적발 및 검거비율이 점점 줄어드는 것으로 보아 범죄수법, 추적회피기법 등으로 날로 범인검거가 어려워지고 있으며, 특히 다양한 매체의 발달과 함께 전 세계가 네트워크로 연결되어 있어 국경 개념이 무색, 음란·도박사이트 등 불법사이트를 외국 서버에서 운영하는 등의 원인으로 인하여 사이버범죄 예방 및 수사에 어려움이 점점 증가하고 있다.

2) 동북아시아의 사이버범죄 현황

현재 사이버 국제범죄는 주로 중국과 대만에서 빈번하게 공격이 되고 있으며, 우리나라역시 악성코드 유포지로 악명이 높다. 이중에서 중국에서 발생하는 사이버범죄는 국외에 피해를 주로 입히고 있다. 중국에서 발생하는 사이버범죄의 특성은 지능적이며, 청소년의 범죄화, 공동범죄의 증가, 범죄수단의 특수성, 범죄행위의 익명성, 탈지역·탈국가화의 가속, 심각한 사회 위험성을 내포하고 있다.

중국에서 발생하고 있는 사이버국제범죄에 대하여 중국당국도 정확하게 파악하지는 못하고 있으나, 2006년에 중국 국가인터넷 긴급기술처리 협조센터(CNCERT/CC)[2]에서 발표한《2006년 인터넷안전업무보고》에 따르면, 2006년에 접수된 인터넷 안전사고는 26,476건으로 2005년의 9,112건에 비해 약 3배 증가하였으며, 인터넷 안전사고의 대부분은 인터넷 사이트의 수정·삭제 24,477건으로 전체 안전사고의 92.4%를 차지하고 있고, 스팸메일 587건, 가짜 사이트를 통한 피싱 563건의 순으로 나타났다[6].

그리고, 2006년에 처리한 건수는 613건이고, 인터넷을 통해 파악한 취약점공격형 악성코드는 모두 96건이고, 악성코드가 사이트에서 포착되는 건수는 매일 평균 3,069건에 이른다[6].

위 보고서에서 눈길을 끄는 것은 2006년 가장 전형적인 사건중 하나로 한국의 인터넷침해사고대응지원센터(KrCERT/CC)로부터 한국 국민의 주민등록번호 등 인적사항이 수 만개의 중국 사이트에 게시되어 계속 유포되고 있고, 중국에서 이들 인적사항을 도용하여 한국 온라인게임 등의 사이트에 접속함으로 인해 개인정보유출, 프라이버시 침해 등이 한국에서 최대 사회문제가 되고 있다는 연락을 받고, 확인한 결과 중국 쪽의 여러 사이트에 한국을 공격한 흔적이 남아 있는 것을 발견하고 적절한 통제조치를 하여 한국의 이해를 얻고 이 문제가 외교 분쟁으로 확대되지 않도록 할 수 있었다는 내용이 기록되어 있다[9].

위 보고서에 언급된 사항 중 외국에서 해킹프로그램으로 중국 사이트를 공격한 순위를 보면

2) 한국의 인터넷침해사고대응지원센터(KrCERT/CC)에 대응하는 기관(www.cert.org.cn).

트로이 목마형 해킹공격으로 미국(25%), 한국(12%), 대만(9%) 순이고, 스파이웨어 해킹공격으로도 미국(33%), 한국(10%), 대만(9%) 순으로 나타나 한국이 미국 다음으로 중국 사이트에 위협적인 나라로 인식되고 있음을 알 수 있다[10].

2013년 8월 발표된 중국공안의 사이버범죄 관련 자료에 의하면 현재까지 210명의 사이버범죄 관련 범죄조직을 적발하였으며, 8,700여명의 사이버범죄자를 체포하였다. 이들이 국제 인터넷 사기 등을 통하여 벌어들인 금액은 245억 달러에 달하는 것으로 나타나 중국의 사이버범죄가 빈번하게 발생하는 것을 증명하고 있다.[3] 중국에서는 1980년대 중후반이후, 사이버 범죄는 수천 건이 넘게 발생하였고, 그 범죄 분야 또한 사이버 절도, 사기, 공금횡령, 파괴, 간첩 등 모든 분야에 걸쳐 있다. 그중에서 가장 심각하게 발생하는 사이버 범죄는 사이버 재산범죄이며, 그 다음이 사회질서를 위협하는 사이버 범죄로 사이버도박・사이버 음란물 유포 순으로 발생하고 있다[11].

일본에서도 사이버범죄는 심각한 사회문제가 되고 있다. 사이버범죄로 인하여 체포되는 범죄자는 매년 증가하고 있으며, 2010년에는 6,933명이 체포되었다. 게다가 사이버범죄로 인하여 경찰에게 신고 혹은 상담을 받은 사례는 2010년 기준 총 75,810건으로 전년대비 7,929(9.5%)건이 감소하였으나 여전히 높은 발생빈도를 보여주고 있다.

발생건수별 내용을 살펴보면 네트워킹 관련 사이버범죄가 5,199건으로 가장 높은 비율을 차지하였으며, 전년대비 1,283(31.8%)건이 증가한 것으로 나타났다. 비인가 접속 위반사례는 총 1,601건으로 전년대비 933(36.8%)건이 감소하였나, 비인가 접속으로 체포된 범죄자는 전년에 11명에 불과하였으나 2010년에는 125명으로 증가하여 여전히 심각한 상황임을 증명하였다[11].

<Table 3> 2006~2010 Cyber Crime of Japan

년도	2006	2007	2008	2009	2010
합계	61,467	73,193	81,994	83,739	75,810
온라인사기	21,020	32,824	37,794	40,315	31,333
경매사기	14,905	12,707	8,990	7,859	6,905
명예훼손・비방	8,037	8,871	11,516	11,557	10,212
비인가접속・바이러스 유포	3,323	3,005	4,522	4,183	3,668
스팸메일발송	2,930	4,645	6,038	6,538	9,836
유해・불법정보	4,335	3,497	4,039	3,785	3,847
기타	6,917	7,644	9,095	9,502	10,009

※ Source: [8].

이렇듯 우리나라와 인접해 있는 일본과 중국에서는 사이버범죄가 빈번하게 발생하고 있으며, 발생빈도도 점점 증가하고 있다. 현재 사이버국제범죄에 대하여 국가 간의 공조부족, 사이버국제범죄 인식부족 등의 원인으로 인하여 정확하게 파악하지 못하고 있지만, 사이버국제범죄가 상당하게 발생하고 있다고 추정되며, 피해금액 및 발생건수는 매우 많을 것으로 판단된다.

3) First Post World. 2013. 8. 14. China arrests 8,700 people for cyber crimes.

Ⅲ. 사이버 국제범죄에 대한 국제기관의 대응

1. 인터폴의 사이버 국제범죄에 대한 대응

인터폴은 가맹 각국의 경찰이 상호 간에 주권을 존중하면서 국제범죄의 방지, 진압에 협력하기 위해 설립한 조직으로서, 정식명칭은 '국제형사경찰기구(ICPO: International Criminal Police Organization)'이다. 인터폴은 각국의 현행 법률의 범위에서, 그리고 세계인권선언의 정신에 입각해 모든 형사경찰당국 간 최대한 협조를 보장·증진하는 것(헌장 제2조)에 그 설립 목적을 두고 있다. 사무총국은 프랑스 리옹(Lyon)시에 있고, 각 회원국은 사무총국 또는 회원국 간의 연락 및 협조요청에 주요한 창구가 되는 국가 중앙사무국을 설치·운영하고 있다.[4)]

1914년 모나코에서 열린 국제경찰회의가 효시이며, 1923년 유럽 24개국으로 국제형사경찰위원회(ICPC)가 발족, 1956년에 현재와 같은 형태가 되었다. 원래 비정구간기구로 출범한 인터폴은 1971년 유엔 경제사회이사회로부터 정부 간 기구로 공인되었으며, 1996년 10월 유엔총회에서 유엔의 옵서버 자격을 인정받았다.

인터폴의 업무에 대해서는 국제법상의 협정이 아니기 때문에, 자체 수사 인력이 없으므로 회원국이 24시간 운영하는 'X400'이라는 통신망을 운영하여 인터폴 가맹국의 중앙사무국과 연결하여 광범위한 분야에 대한 국제경찰공조가 가능하게 하는 유일한 창이다. 인터폴을 통한 국제공조는 외교경로를 거칠 필요가 없고 인터폴 가맹국의 국제통신망을 이용하기 때문에 정보공유에 대하여 신속한 공조가 가능할 뿐 수사 인력이 없어 실제 사이버 국제범죄에 대응하는데 한계를 가지고 있다[12].

인터폴의 국제공조의 범위는 「국제형사사법 공조법」 제38조 제1항에 명시된 바와 같이 국제범죄의 정보 및 자료교환, 국제범죄의 동일증명 및 전과조회, 국제범죄의 동일증명 및 전과조회, 국제범죄에 관한 시실 확인 및 그 조사로 규정하고 있다. 그리고 실무상 공조내용으로는 국외도피사범의 강제송환, 사건수사」 수사자료 교환, 사실확인, 국외 출장수사, 국제형사사법 공조법」, 「범죄인 인도법」에 의한 공사사항 협력 등의 업무를 공조한다[12].

이러한 규정이 있음에도 불구하고, 인터폴을 통한 국가 간 국제공조가 활발하지 못한 것은 하다. 실질적인 국가 간의 공조는 상대국의 충분한 협조가 있어야 하며, 강제성을 가지는 국제공조의 경우 국내법에 내용이 있어야 하며, 상대국가의 문화와 관습의 차이로 인하여 관련법이 없는 경우도 많아 국제공조가 원활하지 못하게 되는 원인이라고 지적된다.

특히, 기술적인 진화속도가 빠르고, 국제적으로 발생하는 빈도가 높으며, 사이버국제범죄 사사를 위한 절차와 방식도 국내법이 정하는 한도 내에서 이루어지기 때문에, 사이버국제범죄의 경우 인터폴을 중심으로 실제 수사상의 국제공조가 필요함에도 불구하고 앞에서 언급하였던 바와 같이 정보교환정도의 형식적인 국제공조 밖에 이뤄지지 않고 있다.

2. 유로폴 사이버범죄센터(European Cyber-crime centre)의 대응

4) 네이버. http://terms.naver.com/entry.nhn?docId=71406&cid=446&categoryId=446. 2013. 10. 7.

EU의 사이버보안 담당기구인 유럽 네트워크 정보보호원(European Network and Information Security Agency: ENISA)은 최근 사이버범죄 동향과 관련한 「Threat Landscape(사이버범죄 전망 보고서)」를 통해 사이버공간에서는 공격자와 방어자 간에 끊임없는 경주가 벌어져 왔으며, 현재는 공격자가 한 걸음 앞서 있는 상황임을 지적하면서, 국가와 기업・이해 당사자들이 사이버범죄에 효과적으로 대응할 수 있도록 최신 기술 내에서 발생하는 사이버범죄의 동향을 분석하였다.

EU집행위원회(Commission of the European Communities)를 통하여, 사이버범죄로 인한 피해액을 연간 2,900억 유로로 추산, 특히 영국의 연간 피해액은 매년 300억 유로에 달하며 독일의 피싱(Phishing)사기 피해는 지난 2008년 2,000건에서 2010년 5,000건으로 크게 증가했다고 발표하였다.[5)]

그 동안 유럽 내의 사이버범죄가 국가 간의 심각한 국제범죄로 발전한 원인은 유럽연합(European Union)의 특성 상 역사적・사회문화적 유사성이 높고, 지리적으로 가까우며, 동일한 화폐를 사용하고 있기 때문에 사이버 범죄가 빈번하게 발생하였다.

그럼에도 불구하고 사이버범죄에 대한 대응은 소극적 이었다. 그 원인은 유럽연합으로 경제적・사회적인 통합을 실시하였으나, 법체계는 통일되지 못해 관할의 문제가 발생하였고, 국가 간의 정보공유의 어려움, 인접한 지형적 특성으로 인하여 범죄자의 이동이 자유로움, 새로운 기술과 융합하여 점점 진화하는 특성 등으로 인하여 사이버범죄가 사이버 국제범죄로 성장함에도 소극적으로 대처할 수 밖에 없었다.

유럽연합(European Union: EU) 회원국 간의 이러한 문제점을 인식하여, 사이버 범죄에 대하여 효과적으로 대응하기 위하여 유럽연합은 사이버범죄에 보다 대응하기 위하여 유로폴(Europol) 산하에 '사이버범죄센터(European Cyber Crime Centre; EC3)'를 2013년 1월에 개소하였다. 유럽의 사이버범죄센터는 유로폴 소속의 기관으로서 유럽연합 내에 발생하는 사이버범죄 수사지원, 정보와 첩보의 저장 및 공유, 사이버 범죄예방지원업무를 수행하는 기관으로서, 기존의 유로폴에서 시행하였던 사이버범죄 수사를 비롯하여 디지털 범죄과학수사 및 교육프로그램 등을 실시하는 기관으로서 주요 사이버범죄를 다루고 감시하는 업무를 하는 기관이다.

이 기관은 유로폴로부터 예산을 지원받는데 2013년에는 700만유로(약930만 달러)를 지원받으며, 전문 상주인력은 30명으로 2013년 말까지는 60명까지 충원하는 것으로 계획하고 있다. 주로 다뤄지는 사이버범죄 유형은 온라인사기와 같은 조직화된 범죄활동, 온라인 아동성추행과 같은 심각한 피해를 유발하는 범죄, EU 주요 인프라 및 정보시스템을 목표로 하는 범죄를 대상으로 하고 있다.

사이버범죄센터 출범으로 사법권 관할 문제 해결 및 법제 일원화가 가능해질 것으로 기대된다. 그 간 사이버범죄에서 국가 간의 장애물로 지적된 사법권 관할 문제 해결의 단초를 마련할 것이라고 하였다. 또한 사이버범죄센터를 통해 회원국 간의 정보 공유가 체계적으로 이루어져 법체계의 일원화가 가능해질 것으로 전망하였다.

1) 유로폴 사이버 범죄센터의 업무적 시사점

5) 한정연. 2013. EU, 사이버범죄 예방을 위해 강화된 대응체계 구축.

① 유로폴의 사이버 범죄센터 업무특성에 관한 시사점

사이버 국제범죄에 효과적으로 대응하기 위해서는 문화적・지정학적 유사한 관계에 있는 유로폴의 사이버 범죄센터를 참고할 필요가 있다. 유로폴의 사이버 범죄센터는 기본적으로 급증하고 있는 국가 간의 온라인 범죄에 적극적으로 대응하기 위한 목적으로 설립되었다.

급증하는 국제적 사이버 범죄에 대응하기 위하여 이들이 가지는 목적을 달성하기 위하여 사이버 범죄센터에서는 사이버범죄 및 사이버 국제범죄에 대하여 수사 및 국제공조활동, 분석, 사전 대응준비 활동을 실시한다.

사이버 범죄센터에서는 여러 사이버 범죄 중에서도 온라인 사기와 같이 큰 피해를 발생시키는 조직화된 범죄, 심각한 피해를 줄 수 있는 범죄 및 아동 성폭력물 유포 행위, 유럽연합의 정보시스템과 사회에 부정적인 영향을 줄 수 있는 행위에 대하여 중점적으로 수사와 분석, 국제공조를 실시한다.

온라인사기와 같이 큰 피해를 주는 조직화된 범죄에 대하여 전문분석을 실시함과 동시에 효과적인 수사를 실시하기 위하여 사이버 범죄센터 수사관들의 유로폴 데이터베이스에 접속할 수 있도록 허가하고 있다. 현장에서 즉각적인 수사가 가능할 수 있도록 스마트폰, PDA, 테플릿PC와 같은 모바일 기기를 통하여 범죄정보를 조회할 수 있도록 휴대용 분석장치(Universal Forensic Extraction Device kit: UFED)의 제공, 중요한 자료를 암호화하여 보유할 수 있는 전문 데이터 저장장치를 제공하여 즉각적인 수사가 가능하도록 지원하고 있다.[6)]

이렇듯 유로폴 사이버 범죄센터는 신속한 수사가 가능하도록 유로폴의 데이터베이스 활용을 비롯한 수사의 효과적인 국제공조가 가능하도록 가입국가 간의 조약을 통하여 수사권을 보장하고 있다. 특히, 중국・한국・대만 등 동북아 국가에서 빈번하게 발생하고 있는 피싱・금융사기・사이버 공격・사이버 공간상의 침해 등과 같은 초국가적 범죄에 대하여 즉각적인 국제공조가 가능하도록 휴대용 정보공유장치 및 암호화된 저장장치의 적극 활용, 국가기관과의 실질적인 공조, 활발한 범죄정보의 공유 등을 시사하고 있다.

② 국가 기관과의 협조 및 관련기관 협조의 시사점

사이버 국제범죄 및 사이버범죄에 대항하기 위하여 사이버 범죄센터에서는 EU회원국의 국제공조를 이끌어 낼 뿐만 아니라, 유럽 내 비 EU국가와의 국제공조, 비유럽 국가와의 국제공조, 시민사회 단체・인터넷 거버넌스 기구와의 협력, 인터넷 서비스 업체・사이버보안관련 업체 등과의 협력・지원, 국가 컴퓨터 긴급 대응팀(National Computer Emergency Response Teams: CERT)와의 공조를 실시하고 있다.

그리고, 유럽연합 사이버범죄 태스크포스(European Union Cybercrime Taskforce: EUCTF), 유럽 네트워터정보보안센터(European Network and Information Security Agency: ENISA), 유럽 사이버범죄 훈련교육그룹(European Cybercrime Training and Education Group: ECTEG), 유럽경찰학교(European Police College: CEPOL), 유럽연합 형사연합기구(European Union's Judicial Cooperation Unit: EUROJUST), 인터폴(International Criminal Police Organization) 등과도 상호협력 프로그램을 설치하여 수시로 교육지원 및 수사업무 지원을 받

6) European Cyber Crime Center, https://www.europol.europa.eu/ec3

고 있다.[7)]

특히, 사이버 범죄센터는 외부 사이버관련 기업 및 금융전문회사를 통하여 전문기술의 지원 및 업무적인 조언을 받고 있다.

사이버 범죄와 관련하여 사이버 보안업체인 CISCO, McAFEE, Microsoft, Kaspersky를 비롯하여, 모바일 관련 전문업체인 BlackBerry, Verizon 와 같은 민간기업과의 협조 뿐 만 아니라, 각 국가별로 사이버범죄를 전문으로 다루고 있는 기관 중에서 업무능력이 우수한 프랑스의 French National Cybercrime Unit, 아일랜드의 IRISSCERT와 협조를 실시하고 있다. 그리고 컴퓨터 전문 기업인 Microsoft사의 Cybercrime Division등으로부터 사이버 보안에 관한 업무협조 및 지원을 받고 있으며, 온라인 금융과 관련하여, Citi Group, VISA, Western Union, Cartes Bancaries와 같은 일반 금융기관의 협조 및 지원을 통하여 사이버상의 업무를 수행하고 있다.

유로폴의 사이버 범죄센터는 사이버 공간에서의 범죄 예방 및 증거물 확보를 위하여, 자신들의 부족한 점을 인식하고, 국가 간의 국제공조 뿐만 아니라, 다른 외부 국가 및 외부기관과의 긴밀한 협조체제를 갖추어 사이버 범죄에 대응하고 있다.

특히, 유로폴의 사이버 범죄센터에서는 국가 간에 발생하는 사이버 국제범죄에 대하여 수사권을 가지고 협력할 수 있도록 제도화하여 범죄해결을 위한 직접적인 활동을 가능케하고 있다는 점과 수사를 위한 정보공유가 단순히 국가 간의 업무협조를 위한 수준이 아닌 전문가의 조언을 받을 수 있도록 외부기관과의 업무협조가 가능케 한다는 점은 향후 동북아 사이버 범죄센터 설립에 큰 시사점을 남긴다.

3. 사이버국제범죄 대응의 문제점

1) 국제공조수사의 시스템의 미완비

형사사법에서 성공의 성패 중에 하나는 바로 빠른 수사이다. 그러나 사이버국제범죄의 경우 발생하여 피해를 입는 속도가 공간적 제약이 없기 때문에, 전통적인 형태의 형사사법체계를 적용할 경우 실패할 것이 자명하다. 특히, 사이버범죄는 정보기술이 발달해감에 따라 초국가적인 성격이 더욱 강화되었고, 범죄의 성공을 위하여 더욱 조직화・분업화되고 있기 때문에 수사상의 긴밀한 국제공조가 필수적이다. 이러한 국제공조는 과거와 같이 정보 수집을 위한 국제공조가 아닌, 정보 수집 단계에서부터 수사개시, 증거자료 수집, 피의자 검거, 범행 수익추적・몰수 등 모든 단계에서 국제공조가 필요하다.

사이버국제범죄는 여러 나라에 걸쳐 발생되는 특성을 가지고 있는데 반해, 각국의 실체법과 절차법의 구체적 내용은 국가별로 다양하므로 컴퓨터 네트워크 범죄에 대하여 공통적인 관할권과 준거법을 인정할 것인가의 문제는 한계가 있을 수 밖에 없고, 현실적인 대처방안은 양국 간의 합의 또는 국제적 협약에 의하여 이루어질 수 밖에 없는 문제일 것이다[12].

현재의 국제공조수사 시스템은 관할의 문제, 국가 간의 정치적・법적・제도적・기술적 차이와 한계로 인하여 미완성 상태에 머무르고 있어 그 심각성을 더하고 있다[13].

---

7) European Cyber Crime Center, https://www.europol.europa.eu/ec3

2) 증거확보의 곤란성

기본적으로 사이버범죄는 빠른 전파성・진화속도를 특성으로 하고 있다. 이는 사이버국제범죄에도 똑 같이 적용된다. 따라서, 사이버국제범죄를 수사하기 위해서는 증거의 확보가 중요하다. 그러나 실제로는 상대적으로 느린 증거확보 과정・다양한 국가 간의 관계・형사사법의 차이로 인하여 증거확보가 용이하지 않다.

특히, 기존의 공조수사 절차가 지나치게 형식적인 면에 치우쳐 절차가 지연됨으로 인하여, 필요한 증거를 시간 내에 확보하기가 어렵다. 그리고 사이버범죄에 있어서 대부분의 증거는 영구적으로 보존되지 않는 데이터로 구성되어 있고, 범죄자들은 손쉽게 사이버 공간 상에서 자신들의 위치를 바꾸어 나가기 때문에 이들을 검거하기 위해서는 '신속성'이 수사의 생명이라고 할 수 있다. 그럼에도 불구하고, 전통적 의미에서의 형사사법 공조절차는 그 요청 당시부터 상대방이 요청을 수행할 때까지 보통 여러 외교채널을 거치면서 상당한 시간이 소요되기 때문에 사이버범죄 국제공조수사에 있어서는 전혀 그 효용성을 발휘하지 못하고 있다[13].

3) 각국의 범죄구성요건의 상이성

사이버범죄에 대하여 각 국가별로 심각성을 인식하고 예방・수사를 위하여 공조해야 한다는 원칙에는 모두 공감하고 있다. 그러나, 기본적으로 국가별로 상이한 법체계와 문화적・사회적 입장차이로로 인하여 효과적인 국제공조가 이루어지지 않고 있다.

인터넷 상의 음란사이트, 위험정보 사이트 혹은 도박 사이트를 처벌하는 경우에 있어서와 같이 국가마다 사이버공간의 행위에 대한 법적 구성요건이 서로 다른 경우가 많기 때문이다[14]. 특히, 동양권 국가들에 비해 서양권 국가에서 인식하는 문화적 개방성은 음란물 사이트 단속과 같은 문제에 있어서 서로 상이한 시각차를 가지고 있어, 범죄의 구성요건을 판단하는 데 기준의 차이를 보이고 있다.

따라서 이러한 문제는 기본권에 대한 인식 차이 혹은 문화적・역사적 인식차이에서 비롯되는 국가 간 구성요건의 적용의 차이를 발생시켜 국제공조를 어렵게 만드는 중요한 요인이 되고 있다[15].

4) 국가주권 우선성의 문제

국제형사사법조약이 체결된 상태라도 국가 간의 공조가 효과적으로 이루어지지 않는 것은 국가주권 우선성의 문제 때문이다. 국가주권 우선성의 문제는 국제공조를 저해하는 원인이라고 볼 수 있다. 사이버 국제범죄가 발생하는 것이 반드시 국가의 이익을 침해하는 것이 아니며, 오히려 국가의 이익을 줄 수도 있는 경우가 많기 때문에, 국가의 주권을 우선적으로 판단하는 경우 오히려 국제공조가 이뤄지지 않을 수 있다.

게다가, 국가 간의 보이지 않는 힘겨루기로 인하여, 자국민이 다른 나라의 법정에서 심판받게 될 것을 알면서도 범죄에 관련된 증거나 용의자를 넘겨준다는 것은 주권의 나약성을 인정하는 것이나 다름없기 때문에, '상호주의원칙'도 실상은 상대국이 협조하는 만큼 협조해 준다는 것이므로, 불필요한 협조는 응하지 않겠다는 의지에 근거하는 것이다. 이러한 입장은 사이버범죄의 단속에도 그대로 적용되기 때문에 국제공조를 어렵게 하는 요인으로 지적된다[15].

5) 국제사회의 복잡성

국제사회는 빈부격차・기술격차・지정학적 관계・역사적 배경에 따라 복잡하게 뒤얽힌 국제사회의 복잡한 이해관계가 국가 간의 공조를 어렵게 한다. 과거 냉전시대와 달리, 이념보다는 들어 국가의 이익을 최우선으로 하는 국제적인 경향으로 인하여, 비록 범죄자 일지라도 자국의 이익에 부합이 된다면 국제공조를 거부하거나, 소극적인 자세로 협조하지 않고 있는 경우가 있다.

특히, 돈세탁(Money Laundering), 산업스파이(Industrial Spy)와 같은 전통적인 형태의 국제범죄 뿐만이 아니라, 기밀을 훔쳐내는 스파이형 해커(Hacker), 사이버 테러리스트(Cyber Terrorist), 위협적인 프로그램 개발자 등에 대하여 대승적인 차원에서 국제공조를 실시하지 않고, 오히려 국제사회에서의 힘의 원리에 따라 사이버 국제범죄에 대하여 소극적인 형태의 국제공조가 이뤄지고 있다.

Ⅳ. 동북아 사이버 국제범죄 공조기관 설립을 통한 대응

사이버 국제범죄는 국경 없는 사이버 공간에서의 위험에 대한 사이버 보안은 일국의 노력만으로 해결하기 어려운 상황이다[15]. 특히, 사이버 국제범죄로 분류하고 있는 사이버 테러범죄의 경우 해외에서 공격하는 해킹이나 DDoS공격에 대한 용의자를 추적하기 위해서는 관련 당사국과 긴밀한 협력체제가 필요하게 되었다[16].

이러한 문제를 해결하기 위하여 이미 몇몇 국가들끼리 단체를 결성하여 사이버국제범죄에 대응하고 있는데, 국제적 단위의 G8의 사이버범죄 하위그룹, OECD 정보보호대응, 아시아 지역 CERT(Computer Emergency Response Team) 연대와 같은 국제적 공조 연대를 통하여 사이버 국제범죄를 해결하기 위하여 노력하고 있으나, 아직 초국가적인 차원에서 수사권을 행사하고, 즉각적인 정보를 공유할 수 있는 조약과 기관이 없기 때문에 앞에서 언급하였던 바와 같이 그 효과는 아직 미미한 실정이다.

따라서, 사이버 국제범죄가 빈번하게 발생하고 있는 동북아 지역의 국가를 대상으로 유로폴과 유사한 형태의 형사사법기관을 조직하여 운용할 필요가 있다. 유로폴은 1992년 체결된 EU 조약에 의거하여 테러리즘과 불법적인 마약거래, 국제조직범죄 등을 예방하고, 각 국가별 형사사법기관의 충돌을 조율하여 범죄수사 및 진압에 효율성과 협력을 증진시키는 기관으로서, 문화적・지정학적 특성이 유사한 동북아 지역의 상황을 고려하여, 사이버 국제범죄를 해결하기 위한 국제형사사법기관으로서 좋은 선례가 될 수 있다.

1. 동북아 사이버 국제범죄 공조기관 설립을 위한 선행조건

사이버 국제범죄에 대응하기 위하여 실질적인 수사와 강제력을 행사할 수 있는 국제적인 기구의 설립이 필요성에 의해 2010년 7월 'UN 사이버안전에 관한 정부 전문가그룹(U. N. Group of Governmental Expert)'이 제출한 보고서에서는 다음의 원칙을 포함해야 한다고 하였다.

첫째, 사이버공간에 대한 국가책임으로서, 국가는 자국 영토 내의 해커(Hacker)나 인터넷서비스제공자(Internet Service Provider) 등의 불법행위 방지 및 처벌의 책임이 있다. 둘째, 민간핵심기간시설에 대한 선제적 사이버공격의 금지로서, 전시가 아닌 평시에 동 시설에 대한 함정문(Trap Door), 논리폭탄(Logical Bomb)의 설치는 금지되어야 한다. 셋째, 사이버공격의 제한을 위한 합의 준수를 검증하기 위하여, 컴퓨터 포렌식(Computer Forensic)의 활용이 가능해야 한다. 넷째, 지원의무로서, 서버 등의 보전, 국제조사관에 대한 편의의 제공 등이 사이버공격에 대한 국제조사의 협력과 지원의무가 있다[28].

이러한 내용을 기본으로, 2010년 UN 사이버안전에 관한 정부 전문가그룹의 보고서에서 제안한 사이버 안전 국제기구의 운영원칙 뿐만이 아니라, 동북아지역의 특성을 고려하여 몇 가지 형사사법의 기본적인 요건을 추가적으로 포함해야 한다.

첫 번째, 동북아 사이버 국제범죄 기구는 사이버 범죄를 수사하기 위하여, 수사상 강제성을 가질 수 있는 국가 간 조약형태로서 국제법상의 법인격을 향유할 수 있어야 한다. 국가 간 조약은 국제법상의 권리의무가 부가되기 때문에 초국가적 범죄를 수사할 수 있는 활동이 부과되고 협력의무가 부가되어 실질적인 협력이 가능해지기 때문에 사이버 국제범죄를 수사하기 위해서는 수사상 강제성을 가질 수 있는 조약형태의 합의가 필요하다[29].

그리고 이러한 조약형태의 합의에서는 반드시 기본적인 협력사항에 대한 각 회원국의 국내법적 근거가 마련되어야 한다. 구체적인 협력의 항목과 범위・내용 등에 대하여 세부적으로 규정하기는 어렵더라도, 기본적으로 이행해야 할 의무에 관한 사항을 국내법적 근거를 바탕으로 명문화하여 실질적인 협력이 가능하도록 해야 한다.

두 번째, 사이버 국제범죄의 특성을 고려하여 관련기관과의 직접적인 협력을 할 수 있도록 운영되어야 한다. 국제적인 문제를 다루고 있기 때문에 외교채널을 이용할 수도 있으나, 이 경우 시간적으로 늦어질 뿐만 아니라 국가 간의 보이지 않는 힘겨루기로 인하여 업무의 효용성이 떨어질 가능성이 높기 때문에 관련기관의 직접적인 협력을 이루어지도록 명문화시켜야 한다. 다만, 공조대상자의 인권보호를 위한 제도적 장치는 별도로 마련되어야 할 것이다[30].

세 번째, 사이버 국제범죄에 효과적인 대응이 가능하도록 정보공유 시스템이 구축되어야 한다. 인터폴(Interpol)의 권한은 국제법상 협정이 아니므로 강제수사권이나 체포권이 없어 자체 수사인력이 없기 때문에 단순 통신프로토콜인 X400을 사용하고 있다.

X400을 이용한 인터폴의 소극적인 정보공유 보다는 수사자료 및 사이버 상의 증거확보를 위하여 사이버 국제범죄에 대한 공유를 강화된 적극적인 형태의 정보공유시스템을 구축해야 한다. 강화된 정보공유시스템은 피싱과 같이 국제적으로 금전이 오가는 사이버 범죄에 대하여 효과적으로 대응을 기대할 수 있다.

네 번째, 사무국과 일정규모의 조직을 갖춘 상시적인 협력체로 운영되어야 한다. 사무국과 하부조직은 각 회원국에서 파견 받은 경찰관 또는 사법기관원으로 구성하여 최소한의 조직이라도 상시적으로 운영되어야 지속적이고 실질적인 협력이 이루어 질 수 있기 때문이다[31].

EU 사이버 범죄센터에서는 사이버 국제범죄에 능동적으로 대처하기 위하여 EU 회원국과 EC(European Community), 유로폴(EUROPOL) 등에서 차출한 30명으로 시작하여 2013년 말까지 60여명 수준으로 증원하여 운영할 것이라고 하였다.[8)]

이렇듯 동북아 사이버 국제범죄 공조기관 설립을 통하여 사이버 국제범죄를 해결하기 위하여 선행되어야 하는 조건을 충족해야 사이버 국제범죄를 해결할 수 있는 기본적인 기틀이 마련된다.

2. 동북아 사이버 범죄센터 설립을 위한 구체적 방안

기본적으로 유로폴은 유럽지역 내의 국가를 대상으로 가입토록 하여 초국가적인 범죄를 해결하기 위하여 만들어진 기관으로서 정보공유는 물론이고 범죄에 대한 수사권을 부여하고 있다는 점에서 국제공조기관 설립을 제안하는데 많은 시사점을 주고 있다.

동북아지역의 사이버 범죄센터를 설립하기 위해서는 앞에서 언급하였던 선행조건을 바탕으로 수사를 할 수 있도록 하는 기능과 정보공유를 할 수 있도록 하는 기능을 반드시 포함시켜 범죄를 예방하고 수사하는 데 실질적인 영향을 미칠 수 있도록 하는 것이 가장 큰 목표이다.

특히, 사이버 범죄를 효과적으로 해결하기 위하여 국제적인 사이버 범죄자를 대상으로 강제성이 있는 수사기능과 정보의 공유를 할 수 있는 전문기관의 설립이 필요한데, 중요설립기관의 업무는 동북아 국제 사이버범죄의 특성을 고려한 해결방안을 제시해 본다.

1) 국제공조수사의 시스템의 설립

사이버국제범죄는 여러 나라에 걸쳐 발생되는 특성을 가지고 있기 때문에, 효과적으로 대응하기 위해서는 국제공조수사를 위한 전문적인 시스템의 설립이 필요하다. 국제적인 형태의 사이버범죄 대응을 위한 국제공조수사 시스템이란 사이버범죄를 확인할 수 있는 조기경보시스템(Early Alarm System), 즉각적인 대응을 위한 사이버 대응시스템, 사이버범죄를 수사・체포할 수 있는 수사시스템, 피해 입은 내용을 회복할 수 있는 피해복구 시스템, 국제적인 공소 및 범죄인인도를 위한 범죄인인도 시스템을 포함하는 것으로서, 동북아시아의 경우 이러한 시스템이 미비되어 있는 것은 물론이고, 통제할 만한 기관조차 없기 때문에 위에서 언급한 국제공조수사를 위한 시스템을 확립하는 것이 우선된 업무라고 볼 수 있다.

우선 조기경보시스템의 경우 각 국가별로 운영되고 있는 인터넷 정보센터의 위협에 대한 경보영역을 확장하여 주변국에 전파하도록 시스템을 확장해야 하고, 사이버 대응 시스템의 경우 각 국가별・영역별 전문가를 채용하여 피해를 최소화 할 수 있도록 시스템을 구축해야 하며, 수사시스템 확보를 위하여 각 국가별로 형사종합시스템을 통한 국제공조강화와 함께 동북아지역 발생 시 범죄자 인도 및 국제공조를 위한 내용을 강화시켜야 한다.

그리고 피해내용에 대한 회복시스템은 범죄수사 이후 즉각적인 피해회복을 위한 금융시스템과의 연계 및 협조를 통하여 시스템이 구축되어야 한다. EU의 사이버범죄센터의 경우 유로폴을 통한 국제공조가 기본적으로 형성되어 있기 때문에, 실질적인 범죄인 수사 및 체포,・범죄인인도가 어렵지 않게 시스템화 되어 있다. 반면, 이 연구에서 제안하는 동북아 사이버범죄센터의 경우 유로폴과 같은 범죄수사기관이 없기 때문에 사이버범죄에 대응하기 위하여 반드시 실효성을 가진 내용을 포함한 시스템구축이 필수적이다.

---

8) 한정연. 2013. EU, 사이버범죄 예방을 위해 강화된 대응체계 구축.

2) 사이버범죄에 대한 각국의 범죄구성요건의 통일

사이버범죄에 대하여 각 국가별로 심각성을 인식하고 예방・수사를 위하여 공조해야 한다는 원칙에는 모두 공감하고 있다. 그러나, 기본적으로 국가별로 상이한 법체계와 문화적・사회적 입장차이로로 인하여 효과적인 국제공조가 이루어지지 않고 있다.

앞에서 언급한 바와 같이 인터넷 상의 음란사이트, 위험정보 사이트 혹은 도박 사이트에 대한 기준이 서로 다르기 때문에, 동북아시아에서 자주 발생하는 사이버범죄인 음란사이트운영 및 음란물 유포, 금융관련 사이버범죄 등에 대한 통일이 필요하다.

사이버범죄와 관련하여 범죄구성요건의 통일을 위하여 각 사이버 범죄군 별 유형을 분류하여 기준을 마련하는 방법이 효과적이다. 유럽연합의 경우 유럽의회는 1999년 '국제적 네트워크상의 불법·유해 콘텐츠와의 싸움을 통해 인터넷의 안전을 증진시키기 위한 다개년 계획'을 통하여 사이버범죄에 대한 기준을 다음과 같이 규정하였다.

<Table 4> Standards of Harmful cyber information

보호법익	위법 또는 유해한 정보의 내용
국가안전보장	폭탄제조, 위법의 약품제조, 테러
미성년자의 보호	부정판매행위, 폭력, 아동포르노
개인존엄성의 확보	인종차별
경제의 안전・신뢰성	사기, 신용카드의 도용
정보의 안전・신뢰성	악의적인 해킹
Privacy의 보호	비합법적인 개인정보의 유통, 전자적 통신피해
명예, 신용의 보호	불법의 비교광고
지적소유권	소프트웨어, 음악 등 저작물의 무단배포

※ Source: [32].

위 내용을 바탕으로 2007년 발효된 '유럽사이버범죄 방지협약'에서는 사이버범죄에 대하여 제2장에서는 '사이버범죄와 구성요건', '사이버범죄에 대한 형사제재'에 관하여 기술하였으며, 제3장에서는 '사이버범죄 대응을 위한 절차적 권한의 적용요건', '절차적권한의 제한'을 규정하였다. 그리고 제4장에서는 '일반적 상호사법공조', '사이버범죄관련 상호사법공조', '상시네트워크'에 관한 내용을 규정하였다.

따라서, 유럽의 범죄구성요건 통일사례에서와 같이 사이버범죄에 대한 기준을 정하여 통일할 필요가 있다. 위 사례를 바탕으로 음란사이트 운영, 음란물 제조 및 유포, 인터넷 사기, 온라인 도박, 불법적인 콘텐트 유포, 악성 코드 및 바이러스 유포 등과 같이 동북아지역에서 빈번하게 발생하고 있는 사이버범죄에 대한 범죄구성요건의 통일을 통하여 대응할 수 있다.

3) 국가주권 우선성의 문제

국제형사사법조약이 체결된 상태라도 국가 간의 공조가 효과적으로 이루어지지 않는 것은 국가주권 우선성의 문제 때문이다. 특히, 사이버 국제범죄 중에서 주요정보에 대한 해킹 및 산업보안에 대한 정보획득과 같이 반드시 국가의 이익을 침해하는 것이 아니라, 국가의 이익을 줄 수도 있는 경우가 빈번하기 때문에 국가의 주권을 우선적으로 판단하는 경우 오히려 국제공조

가 이뤄지지 않을 수 있다.

그리고, 자국민이 다른 나라의 법정에서 처벌받도록 하지 않는 국가 간의 보이지 않는 자존심 문제 등으로 인하여 국제공조가 효과적으로 이뤄지지 않고 있다. 특히, 범죄자와 관련하여 가장 문제가 되는 것은 범죄인 인도와 국제공조의 문제이다.

2007년 발효된 '유럽사이버범죄 방지협약'에서 사이버범죄를 저지른 범죄자에 대한 범죄인도는 제24조에 의하여 '당사국 법에 따라 최소 1년 이상 구금형 또는 그 이상의 중범죄로 하고 있다'고 규정하였으며, 국제공조와 관련하여 효율적인 국제공조체제 구축을 위하여 필요한 입법 및 그에 부수되는 조치를 취하도록 의무화하고 있다. 국제공조 요청 시에는 당사국간에 공조협약이나 피요청국의 법적요건을 준수하도록하고 있으며, 당사국이 공조요청을 받지 않았다 하더라도 당사국의 수사기관이 획득한 정보를 다른 당사국에게 제공할 수 있다고 하였다[33].

따라서, 동북아 사이버 범죄센터를 개설하기 위해서는 실제적인 영향력 행사를 위해하여 EU의 사례에서와 같이 명확한 조약을 제정하여 효과적인 활동이 가능하도록 해야 할 것이다.

Ⅴ. 결론

이 연구는 최근 급증하고 있는 국제적인 사이버범죄 해결을 위하여 동북아지역의 사이버범죄 수사기관 설립을 제안하는 연구로서, 국제적인 형태의 사이버범죄의 정의와 특성, 유형을 분류하였고, 현재 국제적인 사이버범죄의 실태와 관련 국제협약・기관에 대하여 살펴보고, 해결방안으로서 유로폴의 사이버범죄센터 사례를 바탕으로 동북아지역의 사이버범죄수사기관의 설립에 필요한 시사점을 제안한 연구이다.

사이버범죄는 사이버공간에서 발생하기 때문에 사이버범죄를 정의하기 위해서는 사이버공간의 특성을 먼저 이해해야 한다. 사이버 공간은 인터넷과 컴퓨터를 바탕으로 만들어내는 가상의 공간으로서 물리적・시간적・공간적 제약이 없는 것을 특징으로 하고 있다.

특히, 공간상의 제약이 없기 때문에 우리국민이 외국의 사이버공간에서 범죄를 저지를 수 있게 됨과 동시에 외국인이 우리의 사이버공간에서 범죄를 저지를 수 있게 되었다. 문제는 국제적인 형태의 사이버범죄가 발생함에 따라 국제적인 수사를 실시해야 함에도 불구하고 국제공조가 원활하지 않은 탓에 효과적인 수사가 이뤄지지 않고 있다.

이러한 사이버국제범죄에 대하여 초국가성과 심각성을 인식하고 대책을 세우기 위하여 1995년 G8(미국・일본・영국・프랑스・독일・이탈리아・캐나다・러시아)차원에서 국제조직범죄 상급전문가회의를 시작으로 1997년부터 실시된 G8 법무・내무장관회의를 통하여 사이버범죄에 대한 심각성을 인식한 이후부터 2년마다 실시된 G8 법무・내무장관회의를 시작으로, 지금까지 관련 협의 및 조약을 통하여 국제협력을 실시하고 있다.

주요 협의 내용으로는 사이버범죄에 대한 국가 간의 공조의 필요성을 강조하며, 각 세부 업무상의 문제점 인식・해결에 대한 협의를 통하여, 사이버범죄에서 사이버 국제범죄로 그 영역을 세분화 및 확장하여 문제를 해결하기 위하여 국가 간・협의국 간의 협력을 위한 회의를 지금까지 실시하고 있다. 그리고 인터폴과 유포폴 및 유럽연합 사이버범죄 태스크포스(European

Union Cybercrime Taskforce: EUCTF), 유럽 네트워터정보보안센터(European Network and Information Security Agency: ENISA), 유럽 사이버범죄 훈련교육그룹(European Cybercrime Training and Education Group: ECTEG), 유럽경찰학교(European Police College: CEPOL)등의 국제협력기관을 통하여 사이버 국제범죄를 예방하기 위한 노력을 실시하고 있다.

그러나 우리에게 위협적인 형태로 발생하는 사이버 국제범죄들은 상당수가 우리나라를 비롯하여, 중국・대만・일본 등지에서 집중적으로 발생하고 있으며, 이들 국가들도 상당한 피해를 입기 때문에 세계적으로 이들 국가의 사이버 보안에 대하여 심각한 우려를 낳고 있다.

이러한 문제를 해결하기 위하여 이 연구에서는 문화적・지정학적으로 유사점이 있는 유럽의 특성을 고려하여, 유럽 내의 형사사법 문제를 해결하기 위한 기관인 유로폴 내의 사이버 범죄센터와 같이 사이버 국제범죄에 대응하기 위한 동북아 사이버 범죄센터를 제안한다.

사이버 국제범죄 수사 및 해결을 위하여 가장 큰 걸림돌이 수사의 국제공조와 관련 데이터 공유문제에 대하여 유로폴의 사이버 범죄센터에서는 국가 간에 발생하는 사이버 국제범죄에 대하여 수사권을 가지고 협력할 수 있도록 제도화하여 범죄해결을 위한 직접적인 활동을 가능케 하고 있다는 점과 수사를 위한 정보공유가 단순히 국가 간의 업무협조를 위한 수준이 아닌 전문가의 조언을 받을 수 있도록 외부기관과의 업무협조를 포함하여 실시간으로 범죄정보를 공유할 수 있도록 시스템화 시키는 것은 향후 동북아 사이버 범죄센터 설립에 큰 시사점을 남긴다.

우리나라에서도 지속적으로 증가하고 있는 사이버범죄를 해결할 수 있도록, 2014년부터 경찰청 내 사이버수사국을 신설할 예정이라고 하여 국가차원에서 대처하기 위한 노력을 실시하고 있다. 그러나 사이버범죄의 특성상 이제 더 이상 사이버 범죄는 한 국가차원에서 해결할 수 있는 수준을 넘어서게 되었다. 특히, 중국・대만을 비롯한 동북아시아 지역의 사이버범죄 발생은 한 나라를 마비시킬 수 있는 수준에 까지 이르러 매우 심각한 실정이다.

따라서 이 연구에서는 급증하고 있는 사이버범죄에 대하여 효과적인 대응을 할 수 있도록 초국가적 차원의 동북아 사이버 범죄센터 설립을 제안해보고, 사이버 범죄센터 설립에 바탕이 되는 국제공조 및 정보공유, 수사권확보에 관하여 문화적・지정학적 유사성이 많은 유로폴의 사이버 범죄센터 사례를 살펴보았다.

References

[1] Jeong, Jeong Ile. 2005. A Study of International Confrontation on the Prevention of Cyber Crime. *Korean Security Science Review*. 10: 323-354.

[2] Shin, Dong Il. 2007. Global Reaction of Cyber Crime. *Forum of Crime Prevention*. 20: 44-48.

[3] Park, Seong Hoon. 2012. An Exploratory Study of Transnational Cybercrime in Age of globalization. *Korean Criminology Review*. 5(2): 43-80.

[4] Jeong, Jae Joon. 2013. A Correspondence Plan for International Cybercrime. *New Trend of Crimnal Justice*. 39: 110-141.

[5] Korean Police Cyber Terror Response Center www.ctrc.go.kr.

[6] Lee, Kwang Hyung. 2007. *Cybercrime Investigation of China.* Korean Prosecution Overseas Research Prosecutor Article.

[7] Nam, Jae Do. 2009. *Study on Cooperation Investigation of Cybercrime between Korea and China.* Seoul: Korean Police Agency.

[8] Japanese Police http://www.keishicho.metro.tokyo.jp.

[9] Kim, Jae Duk. 2011. A Study to Improve the International Mutual Assistance inCriminal Investigation via INTERPOL. *Wonkwang Law.* 27(3): 39-65.

[10] Han, Bong Jo. 2000. A Study on Issue of Cybercrime Investigation about International Cooperation. *Reserch of Criminal Justice.* 42: 27-38.

[11] Lee, Chang Soo. 2009. A Activation Plan for International Cybercrime about International Cooperation. *New Trend of Criminal Justice.* 21: 94-151.

[12] Choung, W. 2007. International Cooperation for the Prevention of Cybercrime. *Research of Criminal Justice.* 18(2): 113-140.

[13] Jeong, Jae Joon. 2013. A Correspondence Plan for International Cybercrime. *New Trend of Criminal Justice.* 39: 110-141.

[14] Park, No Hyoung. 201). Establishment of International Norms for Cyber Security. *Ahnahm Law.* 37: 795-822.

[15] Park, Ki Ryun. 2009. A Study on Plans for the Development of International Police Mutual: Assistance in the Northeast Asian Region. *Review of Police Science.* 11(4): 131-161.

[16] Kim, Han Kyun, Seong Eun Kim, and Seung Hyun Lee. 2009. *A Study on International Cooperation for Cybercrime Prevention.* Prosecution Research.

참고문헌 (References in Non-roman Script)

[1] 정정일. 2005. 사이버범죄에 대한 국제적 대응방안. 한국경호경비학회지. 10: 323-354.

[2] 신동일. 2007. 사이버범죄에 대한 글로벌 대응. 범죄방지포럼. 20: 44-48.

[3] 박성훈. 2012. 사이버 상에서 발생하고 있는 국제범죄의 유형과 대응방안의 모색. 한국범죄학. 5(2): 43-80.

[4] 정재준. 2013. 국제 사이버범죄에 대한 대응방안. 형사법의 신동향. 39: 110-141.

[5] 경찰청 사이버테러대응센터. www.ctrc.go.kr.

[6] 이광형. 2007. 중국의 사이버범죄 수사. 대검찰청 해외연구검사 논문.

[7] 남재도. 2009. 중국내 사이버범죄 실태 및 한중간 효과적인 공조방안연구. 서울: 사이버경찰청.

[8] 일본 경시청. http://www.keishicho.metro.tokyo.jp.

[9] 김재덕. 2011. 인터폴을 통한 국제공조수사의 개선방안. 원광법학. 27(3): 39-65.
[10] 한봉조. 2000. 사이버범죄수사에 대한 국제적 협력 문제. 형사정책연구. 42: 27-38.
[11] 이창수. 2009. 초국가적 사이버범죄에 대한 국제공조 활성화방안과 그 선결과제. 형사법의 신동향. 21: 94-151.
[12] 정 완. 2007. 사이버범죄의 방지를 위한 국제협력방안. 형사정책연구. 18(2): 113-140.
[13] 정재준. 2013. 국제 사이버범죄에 대한 대응방안. 형사법의 신동향. 39: 110-141.
[14] 박노형. 2012. 사이버안전 관련 국제규범의 정립을 위한 연구. 안암법학. 37: 795-822.
[15] 박기륜. 2009. 동북아지역 국제 경찰공조의 발전방안에 관한 연구. 한국경찰학회보. 11(4): 131-161.
[16] 김한균, 김성은, 이승현. 2009. 사이버범죄방지를 위한 국제공조방안 연구. 대검찰청 연구총서.

신재헌: 동국대학교에서 범죄박사학위를 받고(2013), 대구대학교 경찰행정학과, 영남이공대 경찰행정학과 등의 강사를 역임하였다. 주요 연구로는 “다문화사회의 자생적 테러리즘 예방을 위한 경찰활동(2013)”, “경찰관의 소셜 네트워크 서비스 사용이 경찰업무에 미치는 영향에 관한 연구(2013)” 등이 있다(enfant21@naver.com).

김상운: 동국대학교에서 경찰학 박사학위를 받고(2012), 대구가톨릭 경찰행정학과 교수로 재직 중이다. 민간경비, 경찰교육 등이 주요 관심분야이며, 주요 연구로는 “민간경비를 활용한 사이버범죄 예방 방안(2013)”, ”경찰공무원의 징계결과에 따른 소청제기에 관한 연구(2013)”, “경찰의 테이저 사용에 대한 영향요인 연구(2013)”, “학교폭력으로 인한 두려움이 청소년의 반응에 미치는 영향(2013)”등이 있다(ksw48@naver.com).