사이버범죄의 방지를 위한 국제협력방안

정 완*

국문요약

인터넷의 발달은 각종 범죄의 모의와 실행을 쉽게 할 뿐 아니라, 과거에는 예상치 못한 국제적 범죄의 발생을 수월케 하고 있지만, 이러한 사이버범죄에 대한 수사 및 법집행에 있어서 각국의 대응조치는 그 인력과 법적, 제도적, 기술적 제약으로 인하여 여러 가지 한계에 부딪치고 있고 특히 국경을 넘는 사이버범죄에 대하여는 수사에 어려움이 많기 때문에, 사이버범죄의 보다 효율적인 수사를 위해서는 각국이 사이버공간상에서 국경을 넘나들며 신속하고도 효과적인 수사를 행할 수 있는 기술적·법제도적 환경을 갖추는 일이 시급하다.

그러나 이러한 문제는 어느 한 국가의 노력만으로 해결될 수 있는 것은 아니므로 국제적 협조를 통하여 조약이나 각국의 국내법과 정책 등에 사이버범죄에 대한 종합적 대책을 입안하여 시행함으로써만이 해결될 수 있다.

종래에는 사이버범죄의 특성상 국제조약 체결에 의한 해결이 어렵다고 생각하는 견해가 많았으나, 유럽이사회에서 2004년 7월 사이버범죄조약이 발효되었고 2007년 6월 현재 미국을 포함하여 국회의 인준을 얻은 국가가 20여개 국가로 늘어 이 조약의 중요성이 커져가고 있을 뿐 아니라, 그 가입대상을 지역적으로 한정하고 있지 않기 때문에 우리나라도 가입을 신중히 검토하지 않을 수 없는 상황에 있다. 본고에서는 이러한 문제의식을 가지고 사이버범죄분야에서의 국제형사사법공조방안에 대하여 고찰해 보고자 한다.

* 경희대학교 법과대학 교수, 국제법무대학원 인터넷법무학과 주임교수, 법학박사

Ⅰ. 서 언

컴퓨터와 인터넷의 발달은 각종 범죄의 모의와 실행을 쉽게 할 뿐 아니라, 과거에는 예상치 못한 국제적 범죄의 발생을 수월케 하고 있다. 예컨대, 인터넷을 통하여 국경 밖에서 해킹을 하거나 바이러스를 유포하는 경우, 외국서버에 한글 음란사이트를 개설하여 국내인에게 전시 및 배포하는 경우, 외국서버에 개설된 도박사이트에 국내인이 접속하여 도박을 하는 경우, 불법복제 소프트웨어 등 타인의 저작물을 불법적으로 사이버공간에 유통시키는 경우 등이 그것이다.

그런데 이러한 다양한 사이버범죄에 대한 수사 및 법집행에 있어서 각국의 형사사법기관들의 대응조치는 그 인력과 법적, 제도적, 기술적 제약으로 인하여 여러 가지 한계에 부딪치고 있고 특히 국경을 넘는 사이버범죄에 대하여는 수사에 어려움이 많은 상황에 있다.[1]

이러한 현상은 형사사법기관들에게는 과거에는 생각지 못하였던 새로운 도전이며 사이버범죄수사에 국제적 협조가 긴요한 이유이기도 하다. 사이버범죄 수사를 행하는 각국 형사사법기관들은 사이버공간에서 국경을 넘나들며 네트워크상에서 신속하고도 효과적인 수사를 할 수 있는 기술적, 법제도적 환경을 갖추는 일이 시급한 상황이다.[2]

---

1) 그러나 사이버범죄자들은 이와 같이 형사사법기관의 사법권이 자신들처럼 쉽게 국경을 넘나들 수 없다는 사실을 이용하여 더욱더 국경이 없는 사이버공간에서 활개를 치고 있는 것이다. 한봉조, "사이버범죄수사에 대한 국제적 협력문제", 한국형사정책연구원 제25회 형사정책세미나(2000.5.19) 자료 48쪽 참조.

2) 순전히 수사목적이나 법집행의 목적 달성을 위한 것이라면 현재의 정보통신기술로도 얼마든지 원격지에서의 자료의 무제한적인 접근이나 자료입수, 보관, 처리가 가능할 것이지만, 정보사회에서 디지털화한 자료들은 개인의 프라이버시와 인권보호, 전자민주주의, 국가주권과 국제법적인 관할권 문제 등 여러 가지 복잡한 법적, 제도적 문제들을 내포하고 있기 때문에 이러한 문제들을 종합적으로 고려하여 대처하여야 한다. 한봉조,

이와 같은 문제들은 어느 한 국가의 노력만으로는 해결될 수 있는 것이 아니므로 국제적인 협조를 통하여 조약이나 각국의 국내법과 정책 등에 사이버범죄에 대한 종합적인 대책을 반영하여 시행함으로써만이 해결될 수 있는 문제이다. 종래에는 사이버범죄의 특성상 국제조약의 체결에 의한 해결이 현실적으로는 어렵다고 생각하는 견해가 많았으니 유럽이사회에서 2004년 7월 사이버범죄협약이 발효됨으로써 생각을 달리하지 않을 수 없게 만들었다. 또한 발효 이후에 속도가 늦긴 하지만 2007년 6월 현재 미국을 포함하여 국회의 인준을 얻은 국가가 20여개 국가로 늘어가고 있으므로 이 사이버범죄조약의 중요성이 점차 커져가고 있을 뿐 아니라 가입대상을 유럽지역에 한정하지 않고 있기 때문에 우리나라와 같은 외부지역의 국가도 이 조약에의 가입을 신중히 검토하지 않을 수 없는 환경이 되고 있다.

이하에서는 이러한 문제의식을 가지고 사이버범죄분야에서의 국제형사사법공조방안에 대하여 고찰해 보고자 한다.

Ⅱ. 사이버범죄의 특성과 국제공조의 필요성

1. 국제범죄로서의 사이버범죄

사이버범죄는 기본적으로 국제범죄로서의 특성이 강하다고 할 수 있다.[3] 인터넷공간이라는 것이 금을 그어놓고 그 안에서만 이용하도록 되어

앞의 글, 48-49쪽 참조.

3) 특히 한 국가의 네티즌들이 정치적 목적 등으로 합세하여 타국 정부의 서버 등 타겟에 DOS 공격 등을 집중하는 이른바 Cyber War의 경우에는 그 국제범죄성이 뚜렷하다고 하겠다. 국제범죄는 여러 가지 방법에 의하여 분류가 시도되고 있지만, 이를 국제보통

있는 것이 아니기 때문이다.

특히 사이버범죄의 종류와 내용은 각국에서 이를 범죄로 다루는 내용과 질 및 형량에 있어서 크게 차이가 있기 때문에 이를 일률적으로 처벌할 수 없다는 문제점과도 상통한다.

이와 관련하여 어느 나라에서는 범죄가 되지 않는 것이 다른 나라에서는 범죄로 다루어질 수가 있기 때문에 범죄자들이 이를 회피하기 위하여 그들의 죄를 묻지 않는 국가에 설치된 서버를 이용하여 사이버범죄를 저지르는 경우가 요즘의 대세라고 할 수 있다.

우리나라에서 벌어지는 수많은 사이버범죄에 대하여는 경찰과 검찰의 노력에 의하여 상당부분 단속의 손길이 뻗치고 있으나, 위와 같이 외국의 서버를 이용하는 경우에는 우리 형사법의 적용이 사실상 불가능한 상황이다.

2. 국제공조의 필요성

오늘날 전세계적으로 인터넷환경이 구축되고 그에 따라 인터넷 사용인구가 급증하면서, 인터넷공간에는 음란 · 도박사이트 등 불법유해정보가 만연하게 되었다. 이러한 현상은 특히 우리나라와 같이 음란정보유통이 법적으로 금지되어 있는 국가에 큰 피해를 주고 있어 그 신속하고도 종합적인 대책 마련이 시급하다.

이들 음란 · 도박사이트의 서버가 국내에 있거나 한국인이 운영하고 있다면 전기통신사업법, 정보통신망이용촉진법, 청소년보호법 등 관련법규에 의하여 형사처벌할 수 있지만, 국외에 서버를 둔 사이트로서 정보제공자 등을 알 수 없는 한글서비스를 제공하는 음란 · 도박사이트인 경우 국내법상

범죄와 국제형사범죄로 이분하여 고찰하는 견해가 유력하다. 상세는 문규석, "국제범죄 개념의 이원론적 분류에 관한 연구" 외법논집 제7집(1999.12) 537쪽 이하 참조.

불법정보임이 명백함에도 불구하고 이를 규제하기 위한 집행력을 갖지 못한다는 현실적인 한계가 있어 이에 대한 대책마련이 시급한 상황이다.

정보사회에서는 정보의 흐름이 국경 없이 넘나들고 있으며 해마다 엄청난 양의 정보가 등장하고 사라진다. 인터넷의 등장으로 정보통신기술분야 정책입안자들이 인터넷 공간에서 무차별적으로 늘어나고 있는 유해·불법정보를 근절하기 위해 엄청난 노력을 추진하고 있음은 이미 잘 알려진 사실이다. 최근 미국의 N2H2 리서치 회사의 조사에 의하면 포르노 사이트의 수가 1998년에 비해 2003년 현재 18배로 증가하였다고 한다. 더욱 심각한 것은 아동포르노인데 영국에서 아동포르노가 5년 전인 1998년에 비하여 2003년 15배 이상 증가하였다고 보도되기도 하였다.[4)]

이러한 양상을 볼 때 해외 유관기관과의 공조체제 강화는 절대적으로 필요한 과제이다. 국제공조는 단편적이거나 일회성 수준이 아닌 통합적이고 지속적인 차원에서 조성되어야 한다.

Ⅲ. 사이버범죄 방지를 위한 국제협력동향

사이버범죄에 대한 관할권을 다루는 국제조약이나 일반 국제법상의 원칙이 없는 상황 하에서, 사이버공간에서는 이미 수많은 행위가 국경을 초월하여 이루어지고 있고, 그에 따라 각종 사이버범죄도 급증하고 있으며 그로 인한 피해가 속출하고 있을 뿐 아니라 나아가 기업, 국가의 발전에 걸림돌로 작용하면서 사이버공간에 대한 관여와 규율이 각국의 주요한 현안으로 되어 있다.[5)]

---

4) 정보통신윤리위원회, 정보통신윤리백서(2003), 247쪽 참조.

국제화의 부정적 단면이라고 할 수 있는 국경을 넘나드는 사이버범죄의 급증에 대한 심각성을 환기하고 이에 대한 대책을 세우는 시발점으로 G8 차원에서 국제조직범죄 上級專門家회의[6]가 개최되었다. 즉, 1997년 1월 리용그룹[7] 전체회의에서 사이버공간에서 발생하는 각종 범죄에 대한 대응은 한 국가만으로는 한계가 있으며, 각국의 상호연대가 필요하다는 인식 하에 국제하이테크범죄대책을 검토하는 하위그룹이 설치되었다.[8] 동 하위그룹에서는 주요논점으로 법집행기관이 타국의 컴퓨터에 엑세스할 경우에 발생하는 문제, 하이테크범죄에 있어서의 범인의 장소 및 인물을 특정하는 기술이나 산업계와의 협력 등의 문제[9] 등이 다루어졌다.

또한 리용그룹이라는 사무차원에서의 검토결과를 토대로 국제조직범죄 대책에 대한 정치적 연구를 강화하자는 취지에서 G8 법무 · 내무장관회의(Meeting of Justice and Interior Ministers of The Eight)[10]가 1997년 이래 2년마다 개최되고 있다. 1997년 12월 워싱턴 DC에서 개최된 제1차 G8 법무 · 내무장관회의[11]에서 각국은 컴퓨터 등 하이테크범죄에 대한 국제사

---

5) 특히, 국가안보적 시각에서 사이버범죄의 대비책을 역설한 글로 정 완, "국가안보 위해요인으로서의 사이버범죄", 양지 162호(국가정보원, 2000년 1월호) 17쪽 이하 참조.

6) Senior Experts' Group of The Eight on Transnational Organized Crime.

7) G8에서는 1995년 캐나다의 할리팍스 정상회담에서 조직범죄대책 上級전문가회의의 설치가 합의되어 이듬해 1996년까지 수차례의 회의를 거쳐 국제조직범죄에 관한 40개 권고안을 정리하여 동년 리용정상회담에 제출하여 승인되었다. 이후 이 전문가회의는 통칭 '리용그룹'으로 불리우고 있다. 리용그룹의 주요기능과 내용에 대한 상세는 정완, "G8 국제조직범죄대책" 형사정책연구 제12권 제2호(2001년 여름호), 254-258쪽 참조.

8) 리용그룹의 하위그룹은 1999년 3월 시점에서 하이테크범죄, 사람의 밀매, 국제연합조약, 총기, 사법협력 등 5개 분야에 설치되었다. 정 완, "하이테크범죄대책에 관한 국제동향" 형사정책연구 제10권 제4호(1999년 겨울호), 341쪽 참조.

9) 이에 대한 상세하게는 정 완, 앞의 글("하이테크범죄대책에 관한 국제동향"), 346-351쪽 참조.

10) 이 회의에 대한 상세는 http://www.g7.utoronto.ca/justice/index.html 참조.

11) 이 회의에 대하여는 정 완, 앞의 글("하이테크범죄대책에 관한 국제동향"), 355쪽 이하 참조.

법 공조체제의 강화를 목표로 국제협력 관계의 기본원칙과 이를 이행하기 위한 실천방안을 결의하였다. 이는 하이테크 첨단범죄에 관하여는 새로운 컴퓨터와 네트워크 통신기술의 발달로 전 세계적인 통신이 용이하게 되었고 이로 인한 피해는 전세계적인 경제 사회적 시스템 전반에 걸쳐 심각한 영향을 미칠 수 있다는 상황을 정확히 인식하고 이에 대한 국제적 협력관계가 어느 때 보다도 긴급하다는 현실적인 필요성을 바탕으로 출발한 것이다.[12] 본 회의에서 채택된 10가지 기본원칙과 10가지 행동지침[13]은 사이버범죄를 공동규제하기 위해 각국이 취해야 하는 사항을 열거한 것이다. 1999년 10월 모스크바에서 열린 제2차 G8 법무·내무장관회의[14]에서는 G8 워싱턴회의에서 합의된 구체적인 내용들의 실천을 위하여 보다 세부적인 사항들에 대하여, 특히 법집행기관이 형사사건을 수사할 때와 각국의 전산자료에 대한 엑세스 또는 복사, 압수수색을 할 때 지켜져야 할 원칙들에 대하여 합의하고 이들 원칙들은 조약이나 각국의 국내법으로 반영되어야 한다는데 합의를 하였다. 2001년 밀라노에서 열린 제3차 G8 법무·내무장관회의[15]에서도 하이테크범죄대책을 위한 국제협력의 강화, 정부·산업계의 연대 등에 대하여 결의하였다. 2002년 5월 캐나다의 퀘벡주 몬트렐브랜에서 열린 제4차 G8 법무·내무장관회의에서도 두 번째 의제인 "공공의 안전을 확보하기 위한 적절한 기술의 사용"과 관련하여, 정부와 하이테크산업 간의 협력촉진 및 인터넷상에서의 아동보호 등에 대하여 결의하였

12) 정완, "G8의 국제조직범죄대책" 형사정책연구 제12권 2호(2001년 여름호), 249-250쪽 참조.
13) 이 회의에서 채택된 10가지 원칙과 10가지 행동지침에 대하여는 정 완, 앞의 글("하이테크범죄대책에 관한 국제동향"), 359-361쪽 참조.
14) 모스크바 법무·내무장관회의에 대하여는 정 완, "국제조직범죄 및 하이테크범죄 대책을 위한 G8 장관회의" 형사정책연구소식 통권 제57호(2000년 1/2월호) 30쪽 이하 참조.
15) 이 회의의 상세한 내용에 대하여는 정 완, "밀라노 G8 법무·내무장관회의" 형사정책연구소식 통권 제66호(2001년 7/8월호) 40쪽 이하 참조.

으며, 2003년 5월 파리에서 개최된 제5차 G8 법무 · 내무장관회의에서는 테러와의 전쟁, 리용 그룹의 추후 작업, 주요 인프라 보호회의의 개요와 전망, 아동포르노대책 등의 논의와 함께, 국제형사사법협력으로서 첫째 범죄관련자산의 추적가능성, 동결, 압류 및 몰수, 둘째 특별한 수사기술, 셋째 DNA 정보의 국가간 공유 등에 대하여 논의하였다.

이들 회의들을 살펴보면, 국제적 관점에서는 특히 G8 및 유럽평의회(Council of Europe)의 활동이 활발하며,[16] 기타 실무적 측면을 담당하는 ICPO,[17] 그리고 보다 학구적인 관점에서 법학의 국제적 표준을 책정하는 입장에 있는 IOCE[18]가 각각 중요한 역할을 맡고 있다.

사이버공간의 관할권문제는 사이버공간의 범죄에 대하여 국제적인 동의를 얻어 이를 국제범죄로 규율하는 조약을 만들어 국제형법에 포함시키고, 국제형사재판소와 같은 메커니즘으로 다루자는 견해가 있고,[19] 이에 대하여 형법은 각국의 사회적 기준에 따라 내용과 적용의 기준이 다르므로 통합적인 형태의 국제조약은 불가능하다는 비판이 있으며,[20] 설혹 기존의

16) 유럽평의회의 컴퓨터범죄관련 활동에 대하여는 정 완, 앞의 글("하이테크범죄대책에 관한 국제동향"), 343 - 345쪽 참조.

17) ICPO(International Criminal Police Organization, 국제형사경찰기구)는 통칭 '인터폴'로 불리우는 국제기구이며, 하이테크범죄에 대한 실효적 대책을 강구하기 위하여 1995년부터 컴퓨터관련 범죄에 관한 국제회의(International Conference on Computer-related Crime)를 개최하고 있다. 좀더 자세한 내용은 정완, 앞의 글("하이테크범죄대책에 관한 국제동향"), 345-346쪽 참조.

18) IOCE(International Organization on computer Evidence, 컴퓨터상의 증거에 관한 국제기구)는 각국의 법집행기관으로 구성되는 국제포럼으로, 하이테크범죄 수사에 관한 법학상의 제문제에 대한 논의 및 정보교환을 목적으로 한다. 정완, 앞의 글("하이테크범죄대책에 관한 국제동향"), 345쪽.

19) 예컨대, John Goldring, Netting the Cybershark: Consumer Protection, Cyberspace, the Nation-Statem and Democracy, in Borders IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFRASTRUCTURE (Brian Kahin and Charles Nesson, Eds., 1997), 322-354쪽.; 홍성필, "관할권의 문제", 정보법학 제3호(1999.12), 457쪽 참조.

국제형법에 포함시킨다고 하더라도 국제범죄로 인정되는 범위가 협소하므로 사이버공간의 범죄를 추가할 수 있을지 의문이며 이러한 방법이 옳은지의 여부에 대하여도 회의적인 견해가 있다.[21] 이외에도 특정행위의 범죄성립여부가 국가들 사이에 차이가 있을 수 있다는 점, 동일하게 범죄로 인정된다고 하더라도 처벌에 있어서 그 범위와 정도의 차이가 있을 수 있다는 점, 그리고 근본적으로 각국의 정치, 경제, 사회, 문화적 차이에 기인한 범죄의 성립과 처벌의 다양성이라는 난제가 존재한다.[22]

그럼에도 불구하고 2001년 6월 사이버범죄에 관한 조약(Convention on Cybercrime)[23]이 유럽이사회에서 채택되어 2001년 11월 23일 헝가리 부다페스트에서 가입절차가 개시되었다. 이 조약은 기존의 정보기술개발에 있어서 개발도상국 등과 비교하여 상대적으로 우수한 지위를 차지하고 있거나 정보기술의 보편적 이용과 부정적 사용에 따른 피해 등을 경험한 일부 선진국 등에서 국내법으로만 입법하여 처벌하던 사이버범죄에 대하여 초국가적 범죄 또는 국제범죄로서 최초로 범국가적 차원에서 이를 방지·처벌해야 한다는 국제적 합의가 형성된 것이다. 이 조약은 불법접속, 불법감청, 데이터손괴, 시스템 손괴, 장치의 오용, 컴퓨터를 이용한 위조 및 사기, 저작권과 저작인접권 침해 등 사이버범죄의 실체적 구성요건을 명확히 규정하고 있을 뿐 아니라 범죄행위의 미수, 방조, 교사행위와 법인의 형사상

---

20) Joel P. Trachtman, "Cyberspace, Sovereignty, Jurisdiction and Modernism", Indian Journal of Global Legal Studies, 5 Ind. J. Global S. Stud. 561 (Spring, 1998), 569-572쪽.; 홍성필, 앞의 글, 457-458쪽 참조.

21) 홍성필, 앞의 글, 458쪽 참조.

22) John T. Soma, Tomas F. Muther, Heidi M. L. Brissette, "Transnational Extradition for Computer Crime: Are New Treaties and Laws Needed ?", Harvard Jouranl on Legislation, Vol.34, No.1, 1997, 333-358쪽.; 권재원, "국제법상 국가관할권에 관한 연구-사이버스페이스상의 관할권을 중심으로-" 연세대 석사논문(2002.6), 92쪽 참조.

23) Council of Europe, Convention on Cybercrime, ETS. no.185., Budapest, 23. XI. 2001. 조약의 내용 전문은 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm 참조.

및 행정상 책임까지도 상세히 규정하고 있다. 또한 사이버범죄의 수사와 기소 및 관할권에 관한 절차법을 규정함으로써 사이버범죄의 효과적 처벌을 위한 체계를 갖추고, 사이버범죄자의 범죄인인도에 관한 사항과 효과적 수사를 위한 국제사법공조에 관한 사항을 하나의 조약에 수용함으로써 사이버범죄의 수사와 처벌을 용이하게 하였다.

이 조약은 당초 2002년 발효예정이었으나 조약당사국들의 비준이 늦어져 2004년 7월 1일에나 발효되었다.[24] 이 조약은 사이버범죄에 관한 최초의 국제조약으로 사이버공간을 규율하기 위한 국제적인 노력의 첫 결실로 볼 수 있으며, 사이버범죄방지를 위한 국제협력 및 조약체결의 가능성을 보여주었다는 점에서 그 의의가 크다고 할 것이다.[25]

2007년 6월 13일 현재 43개 가입국 중 21개 회원국이 국회 인준을 얻은 상태이며, 특히 비회원국가로서 상당한 영향력을 끼쳐온 미국에서도 2006년 9월 인준을 얻어 2007년 1월 1일부터 발효된 상태이다.[26]

한편 사이버범죄방지조약의 초안을 작성할 당시에 컴퓨터네트워크를 통한 인종차별적이고 외국인 적대적인 활동의 범죄화에 관한 합의를 이루지 못했었는데, 이는 일부 회원국이 이러한 규정이 자유로운 의사표현의 권리와 일치하는지에 대하여 의문을 가지고 있었기 때문이다.

그리하여 유럽이사회 집행위원회는 유럽범죄문제위원회에 대하여 구체적으로 컴퓨터시스템을 통하여 범해지는 인종차별적 외국인 적대적 행위

---

24) 이 조약은 가입국 5개국(3 회원국 포함)이 인준하면 그로부터 3개월 후에 발효되도록 되어 있는바, 2004년 3월 18일 5번째 회원국이 인준을 하여 7월 1일 발효되었다.

25) 사이버범죄방지조약에 관한 글로, 이영준, "유럽의회(Council of Europe)의 사이버범죄방지를 위한 국제협력(안) 소고" 형사정책연구 제12권 제2호(2001년 여름호), 5-30쪽; 정 완, "유럽 사이버범죄방지조약 발표에 즈음하여" 정보보호21c 2001년 9월호; 정 완 外, 사이버범죄방지조약에 관한 연구, 형사정책연구원 보고서 2001.12 등 참조.

26) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=6/13/2007&CL=ENG 도표참조.

의 범죄화를 위한 전문가위원회에 추가의정서[27]의 제정을 위임하였다.

이에 따라 동 추가의정서는 2003년 1월 28일 서명을 시작으로 2007년 6월 13일 현재 31개국이 서명하였고 그 중 11개국이 인준한 상태이다. 추가의정서는 5개국이 인준한 2006년 3월 1일부터 발효되었다.[28]

Ⅳ. 사이버범죄의 국제관할권과 형사사법공조

1. 사이버범죄의 형사재판관할권

인터넷은 전통적인 개념의 국가주권을 초월하고 있어서 장소에 기반을 둔 국가주권의 실현, 즉 법집행이나 재판관할의 행사에 대해 근본적 변화를 요구하고 있다. 실제로 최근에는 인터넷을 이용한 범죄행위로 자국내의 인터넷서버를 이용하여 이루어지는 경우뿐 아니라 자국의 법망을 피하기 위하여 외국의 인터넷서버를 이용하는 경우가 증가하고 있다. 또한 외국의 통신회사에 의해 제공되는 인터넷서비스를 이용하는 경우가 증가함에 따라 다수국가를 경유하는 범죄의 형태가 증가하고 있다. 여기서 사이버범죄에 이용된 서비스제공회사가 국내에 위치하는가 아니면 외국에 위치하는가에 따라, 행위자가 자국민인가 혹은 외국인인가에 따라 자국의 형사법을 적용할 수 있는가의 문제가 발생하게 된다. 그러나 현재로서는 새로운 국

27) 사이버범죄협약 추가의정서의 정식명칭은 "Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems"이다. 내용 전문은 http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm 참조.

28) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=7&DF=6/13/2007&CL=ENG 도표참조.

제적 질서를 형성하는 것이 불가능하고 문제되는 사항에 대하여 각국의 법에 의존하여 나름대로 일치된 질서를 형성하도록 노력할 수밖에 없는 상황이다.[29] 이에 형사재판관할도 각국의 전통적인 관할이론을 기본으로 하여 관련국간에 국제재판권을 확정하거나 국제형사사법공조의 확립에 의하여 해결해야 한다.[30]

장소적 제한을 받지 않는 사이버범죄의 재판에서 가장 중요한 사항은 형사재판관할권이 어느 나라에 있는가의 문제이다. 국제재판관할권은 한 나라의 입장에서 보면 자국이 재판권을 행사하는 전제로서 그 재판권을 갖고 있는가의 여부가 문제로 되는 경우와, 외국의 재판을 자국에서 승인 · 집행할 요건으로서 타국이 그 재판권을 갖고 있었는가의 여부가 문제된다. 그러나 국제형사재판관할권을 정하는 기준에 관하여는 아직 조약 등의 국제법에 의한 통일적 원칙이 마련되어 있지 않기 때문에 오늘날 각국은 독자적으로 그 국내법에 따라 특정사건에 대하여 재판관할권을 갖는가의 여부를 결정하고 있다. 다만 예외적으로 외국판결을 승인함에 있어서 타국의 재판관할권의 존부를 심사할 수 있을 뿐이다.[31] 기본적으로 각 국가의 주권이 미치는 영토범위 내에서 자국은 형사재판관할권을 갖게 되는데, 자국법이 적용될 수 있는 원칙은 주지하는 바와 같이 속지주의, 속인주의, 보호주의 및 세계주의(보편주의) 등으로 나눌 수 있다.[32]

형사재판관할권을 확정함에 있어서는 범죄행위지, 범죄행위결과지 그리고 범죄자의 거주지 및 국적 그리고 범죄행위의 유형 등이 종합적으로 고

29) 현대호, 인터넷상의 정보보호에 관한 법제연구(한국법제연구원, 2000), 108쪽 참조.
30) 원혜욱, 인터넷범죄의 증거와 재판관할에 관한 연구(형사정책연구원 연구보고서, 2001. 12), 91쪽 참조.
31) 강병섭, "국제재판관할", 재판자료 34집 섭외사건의 제문제(하) (법원행정처, 1986), 32쪽 이하.
32) 국제법상 국가관할권에 관한 기본이론 및 사이버공간에의 적용에 대하여는 권재원, "국제법상 국가관할권에 관한 연구 - 사이버스페이스상의 관할권을 중심으로 -" 참조.

려되어 결정되어야 할 것이다. 따라서 각각의 사안에 따라 속지주의나 속인주의 등 국가보호주의와 세계주의 등 국가연대주의의 양 측면을 고려하여[33] 재판관할권을 확정하는 것이 타당할 것이다.

실제로 인터넷범죄에서 자국의 형사재판관할권 적용이 문제되는 경우는 두 가지가 있을 수 있다. 하나는 국내에 거주하는 자가 국내의 인터넷서비스를 이용하여 범죄를 행한 경우이고, 다른 하나는 외국에 거주하는 자가 외국의 인터넷서비스를 이용하여 자국 혹은 자국민에 일정한 침해의 결과를 발생시킨 경우이다.[34] 전자의 경우에는 속지주의에 의하여 자국 형법을 적용하는 것에 특별한 문제가 발생하지 않는다. 그러나 후자의 경우에는 행위자의 거주지와 범죄의 결과발생지가 다르기 때문에 관할권의 문제가 발생하며, 더욱이 행위자가 제3국의 인터넷서비스를 이용하는 경우에는 행위자의 거주지, 범죄행위의 결과발생지 및 인터넷서비스를 제공한 나라가 모두 범죄관련국이 될 수 있으므로 이에 대한 형사재판관할권의 확정이 문제된다. 또한 외국에 거주하는 자가 외국의 인터넷서비스를 이용하여 유포한 유해정보에 자국민이 접속할 경우 자국의 형법을 적용할 수 있는가의 문제가 발생한다.

이에 대하여 독일은 형법 제3조(속지주의)와 제9조(범죄지)를 적용하여 재판관할권을 행사하고 있다. 예컨대, 미국 뉴욕에 있는 독일의 'Deutsche Bank'의 온라인시스템이 해커의 침입을 받았다면 은행이 소재하는 미국법의 적용을 받아 미국의 재판관할권이 인정되나, 반면에 은행의 중앙시스템

33) Lehle, Thomas, Der Erfolgsbegriff und die deutsche Strafrechtszustandigkeit im Internet (Hartung - Gorre Verlag Konstanz, 1999), 38쪽 이하. 원혜욱, 앞의 글, 97쪽 참조.

34) 특히 후자의 경우에는 인터넷을 이용하여 자국의 사이버공간에 유해정보를 유포하는 것과 같이 자국의 형법이 보호하는 법익이 직접적으로 침해되는 경우와 자국민이 인터넷망을 통하여 외국에서 제공되는 위험정보에 접속하는 경우가 포함된다.

이 미국인에 의하여 침입되는 경우에는 은행본부가 독일에 소재하므로 독일법의 적용을 받아 독일의 재판관할권을 인정해야 한다고 한다. 즉 속지주의의 적용을 받는 범죄지는 독일형법 제9조 제1항에 근거하여 범죄행위지가 아닌 범죄행위의 결과발생지가 된다고 한다. 즉 인터넷상에서의 범죄행위결과지는 위험정보에 의하여 직접적인 침해의 결과가 발생한 경우뿐 아니라 위험정보에 접근할 수 있는 개연성이 인정되면 충분하다고 해석한다.[35] 따라서 전 세계적인 웹사이트를 이용한 범죄 역시 독일에서 범죄행위의 결과가 발생하면 독일형법 제3조와 제9조에 의하여 독일이 형사재판관할권을 갖게 된다고 한다. 뿐만 아니라 사이버범죄의 심각성을 인정하여 형법 제6조에 규정된 세계주의를 적용하여 재판관할권을 확정할 수 있다는 데에도 이견이 없는 상황이다.[36]

우리나라에는 아직 사이버범죄의 국제적 분쟁과 관련하여 판례가 형성되어 있지 않으나 현행법에 근거하여 국제형사재판관할권을 확정할 수 있다. 즉, 형법은 형법의 장소적, 인적 적용범위에 대하여 제2조, 제4조에 따라 속지주의를 원칙으로 하면서 속인주의(제3조)와 보호주의(제5조, 제6조)를 가미하고 있다. 그러나 세계주의는 채택하고 있지 않다. 따라서 국내에 거주하는 행위자가 국내 인터넷서비스를 이용하여 범죄행위를 하는 경우뿐 아니라 외국에 거주하는 자가 외국의 인터넷서비스를 이용하여 우리나라에서 범죄행위의 결과를 발생시킨 경우에도 속지주의를 적용하여[37] 우

35) Sieber, Ulich, Internationales Strafrecht im Internet, NJW 1999, 2072쪽. 원혜욱, 앞의 글, 100-101쪽 참조.

36) 원혜욱, 앞의 글, 101쪽.

37) 통설에 의하면 '범죄지'란 행위자가 범죄를 실행한 장소는 물론, 구성요건에 해당하는 결과가 발생하였거나 행위자의 표상에 따라 발생하였으리라고 추측되는 장소, 공범의 경우에는 정범의 실행행위 및 공범의 가공행위의 장소가 대한민국 영역내에 있으면 족한 것으로 보고 있다. 서보학, "인터넷상의 정보유포와 형사책임", 형사정책연구 제12권 제3호(2001년 가을호), 36쪽 이하 참조.

리 형법을 적용할 수 있을 것이다. 다만, 독일의 사례에서와 같이 외국인이 외국의 인터넷사이트를 이용하여 유포한 유해정보에 한국인이 접속한 경우에, 외국에서는 표현의 자유로 인정되어 범죄로 처벌할 수 없는 행위에 대하여 우리나라의 형법을 적용하여 사이트를 폐쇄하는 등의 처분을 할 수 있는가에 대하여는 형법 제5조의 보호주의에 저촉되는 경우에는 우리 형법을 적용할 수 있을 것이나 음란물 등과 같이 형법 제5조에 포함되지 않는 범죄에 대하여는 형법을 적용할 수 없게 된다.[38] 또한 우리나라는 세계주의도 채택하고 있지 않으므로 독일의 경우와 같이 이 경우에 우리 형법을 적용할 수 없다. 결국 사이버범죄에 현실적으로 대처하기 위해서는 외국인의 국외범에 대하여 행위지를 근거로 하는 행위지법을 우선적으로 적용하되, 관련국간의 국제적인 협력을 필요로 하는 것이다.

2. 수사와 재판에서의 국제형사사법공조

형사사법에 있어서 국제협력의 문제는 크게 두 가지 측면에서 고찰될 수 있다. 첫 번째 실체법적 접근방법으로서, 국제사회가 공통적으로 해악이라고 인식하는 행위를 방지·진압하기 위하여 각국이 조약에 의하여 특정의 행위를 범죄로 규정·처벌할 의무를 부담하고 그 조약의 시행을 위한 각각의 국내법으로 그와 같은 행위를 범죄로 처벌함으로써 국제협력의 실현을 도모하려는 분야에 관한 문제이다. 두 번째 절차법적 접근방법으로서, 소위 형사사법공조에 의한 개별적인 사건에 대한 각국의 형사사법절차에 관한 협력의 諸問題를 논의하는 측면이다. 그러나 실체법분야를 통한 국제협력은 그 기초에 조약의 체결 등 국제적인 행위가 있다고 해도 직접

38) 원혜욱, 앞의 글, 102쪽 참조.

적으로는 내국적인 범죄문제로 된다. 따라서 형사사법공조는 절차법 분야에서의 국제간의 문제로 파악할 수 있다.[39]

이러한 형사사법공조가 일면 타국의 형사사법절차에 대한 협력이라는 점에서 보면 사법공조의 실시에 있어서는 일반적으로 형사사법절차에서 요청되는 엄격성 및 진실발견의 확보가 필요할 뿐 아니라 국내법상의 관계자의 권리보호 및 국내법체계와의 조화를 고려할 필요가 있다. 따라서 사법공조의 절차는 원칙적으로 피요청국의 법률과 형사정책에 합치되도록 행사되어야 하며 개인이 향유하는 권리를 침해하는 형태로 행사되어서도 안 될 것이다.[40]

또한 국가는 형사사건에 관한 사법공조를 제공하여야 할 관습법상의 의무를 지고 있지 않기 때문에 조약상의 근거가 없는 한 청구된 사법공조는 항상 거부될 수 있다. 사법공조에 관한 일반적 합의가 존재하고 국내법상의 근거를 가진 경우라 할지라도 사법공조의 요청의 대상이 된 범죄행위에 관하여 요청국과 피요청국의 형법이 동시에 적용되어 형사사법권의 행사가 경합되는 경우에는 양자의 조정이 필요하게 되는데, 기본적으로 피청구국의 법일반원칙에 저촉되거나, 형사정책에 반하거나, 형사사법의 이익에 반하는 사법공조는 언제나 거부될 수 있다. 그러나 사법공조의 거부사유는 나름대로의 불가피성을 인정할 수 있으나 이로 인하여 꼭 필요한 증거수집이 좌절되고 재판문서의 전달이 방해된다면 당해 사건에 관한 소송은 계속 지연되거나 진행이 불가능해지는 상황에 이르게 될 것이다. 따라서 형사사법공조를 통한 국제협력을 증대시키기 위하여는 공조거부사유는

39) 이규홍, "형사사법에 있어서의 국제협력", 재판자료 제34집 섭외사건의 제문제(하) (법원행정처, 1986), 714쪽 참조.

40) 이규홍, 앞의 글, 717쪽 이하; 백충현, "형사사건에 관한 국제사법공조" 이한기박사 화갑기념논문집(박영사, 1978), 197쪽 참조.

최소한에 그쳐야 할 것이다.[41]

3. 현행 국제형사사법공조법상 공조절차

사이버범죄의 수사는 그 특성상 신속하고 효과적인 국제협력관계가 필요한데, 현행 국제형사사법공조법상 통상범죄에 있어서의 공조절차는 너무 복잡하여 사건해결에 지장을 초래할 가능성이 높다.[42] 우리나라의 형사사법공조법에 따른 통상적인 경우의 형사사법 공조절차를 살펴보면 다음과 같다.[43]

먼저 외국의 요청에 의한 수사공조에 관하여 공조요청의 접수와 요청국에 대한 공조자료의 송부는 외무부장관이 행하는 것이 원칙이고, 공조요청은 공조요청 사건의 요지와 공조요청의 목적 및 내용을 기재한 서면으로 하여야 한다. 이러한 절차에 있어서도 공조는 대한민국 법률이 정하는 방식에 의하여 실시하되, 다만 대한민국 법률에 저촉되지 않는 경우에는 요청국이 요청한 공조방식에 의할 수도 있다.

요청국으로부터 형사사건 수사에 관한 공조요청을 받은 외무부장관은 이를 법무부장관에게 송부하며, 법무부장관은 공조요청에 응하는 것이 상당하다고 인정할 경우 관할 지방검찰청 검사장에게 공조에 필요한 조치를 취하도록 명할 수 있고, 검사장은 소속검사에게 공조에 필요한 자료를 수집하거나 기타 필요한 조치를 취하도록 명하여야 한다.

검사는 공조에 필요한 자료를 수집하기 위하여 관계인의 출석을 요구하여 진술을 들을 수 있고, 감정·통역 또는 번역을 촉탁할 수 있으며, 서류

41) 백충현, 앞의 글, 216쪽; 이규홍, 앞의 글, 730쪽 참조.
42) 경찰의 통상적인 국제범죄수사에서의 공조체계 및 절차에 대하여는 조규철, "한국경찰의 국제범죄 대응능력 제고방안에 관한 연구" 경기대 박사논문(2001), 57-61쪽 참조.
43) 한봉조, 앞의 글, 49-51쪽 참조.

기타 물건의 소유자 · 소지자 또는 보관자에게 그 제출을 요구하거나 공무소 기타 공 · 사 단체에 그 사실을 조회하거나 필요한 사항의 보고를 요구할 수 있다. 검사는 공조에 필요할 경우 영장에 의하여 압수 · 수색 또는 검증을 할 수 있다. 검사는 사법경찰관리를 지휘하여 이러한 수사를 하게 할 수 있고, 사법경찰관은 검사에게 신청하여 검사의 청구로 판사가 발부한 영장에 의하여 압수 · 수색 또는 검증을 할 수 있다.

이러한 과정을 거쳐 공조에 필요한 조치를 완료한 검사장은 지체 없이 수집한 공조자료 등을 법무부장관에게 송부하고, 법무부장관은 이를 외무부장관에게 송부한다. 또한 법무부장관이 검사장 또는 검사에게 하는 명령 · 서류송부와 검사장 또는 검사가 법무부장관에게 하는 보고 · 서류송부는 검찰총장을 거쳐야 한다. 다만 공조요청이 법원 또는 검사가 보관하는 소송서류의 제공에 관한 것일 때에는 법무부장관은 그 서류를 보관하고 있는 법원 또는 검사에게 공조요청서를 송부한다.

한편, 법무부장관은 국제형사사법공조법이나 관계국과의 공조조약에 의하여 공조할 수 없거나 공조하지 않는 것이 상당하다고 인정할 경우 또는 공조를 연기하고자 할 경우에는 외무부장관과 협의하여야 한다.

외국의 공조요청에 소요되는 비용은 특별한 약정이 없는 한 요청국이 부담한다. 다만, 대한민국 영역 안에서 발생하는 비용은 대한민국이 부담할 수 있고, 국내법 또는 공조조약에 의하여 요청국이 공조실시를 위하여 필요한 비용을 부담하도록 되어 있는 경우에는 요청국으로부터 그 비용지급에 대한 보증을 받아야 한다.

이와 같이 통상적인 국제형사사법공조관계에 있어서는 실제로 수사공조가 이루어지기까지 상당한 시간이 소요될 뿐 아니라, 그 절차와 방식도 국내법이 정하는 한도 내에서 이루어지지 때문에 신속하고도 긴밀한 증거의

수집과 범인의 추적이 요구되는 사이버공간에서 발생되는 하이테크 범죄의 경우에는 이를 적용하기가 용이하지 않다.

그러나 법제도의 변화가 없는 현 상황에서 국가간 형사사법공조의 원칙적 틀은 기본적으로 국제형사사법공조법에 의하여야 할 것이므로, 사이버범죄의 국제적 협력관계에서는 이러한 현재의 각국 형사사법공조법의 한계를 보완하는 기술적, 제도적 장치들의 개발이 중요한 과제가 될 것이다.

Ⅴ. 국제형사사법공조의 한계

수사와 재판에 있어 국제형사사법공조는 기본적으로 다음과 같은 몇 가지 한계를 가지고 있다.[44]

첫째, 각국의 범죄구성요건의 차이이다. 사이버범죄를 철저히 단속해야 한다는 원칙에 대해서는 각국의 견해가 일치하지만, 현실적으로는 구체적인 방법론에 대하여는 입장과 기준 등의 차이로 모든 국가가 공감할 수 있는 단속기준을 정하기가 어렵다. 이는 인터넷상의 음란사이트, 위험정보사이트 혹은 도박사이트를 처벌하는 경우에 있어서와 같이 국가마다 사이버공간의 행위들에 대한 법적 구성요건이 서로 다른 경우가 많기 때문이다. 예컨대 음란물사이트와 관련하여 동양권 국가에서는 '표현의 자유'를 중시하면서도 음란사이트를 운영하거나 음란물을 제공하는 행위는 허용되지 않으나, 서양에서는 표현의 자유를 훨씬 더 중요하게 여기기 때문에 성인들을 대상으로 음란사이트를 운영하는 것은 허용하고 있다. 도박사이트를 운영하는 경우도 양상이 비슷하다. 기본권에 대한 인식 차이 혹은 문화

44) 조병인, 사이버경찰에 관한 연구, 형사정책연구원 보고서(2000), 143쪽 이하 참조.

적 · 역사적 인식 차이에서 비롯되는 국가간 구성요건의 차이는 공조를 어렵게 만드는 중요한 요인이다.

둘째, 국가주권의 우선성이다. 국제형사사법조약이 체결된 상태라도 국가간 공조가 용이하게 이루어지지는 않는다. 이는 비록 범죄자일지라도 자국민의 범죄에 관한 증거물 등을 순순히 다른 나라에 넘겨줄 국가는 드물기 때문이다. 자국민이 다른 나라의 법정에서 심판받게 될 것을 알면서 범죄에 관련된 증거나 용의자를 넘겨준다는 것은 주권의 나약성을 노출하는 것이나 다름이 없기 때문이다. '상호주의원칙'도 실상은 상대국이 협조하는 것만큼만 협조해 준다는 것이므로, 불필요한 협조는 하지 않겠다는 의지에 근거하는 것이다. 각국의 이러한 기본입장은 사이버범죄의 단속에서도 그대로 적용되어 국제공조가 제한되는 원인으로 작용한다.

셋째, 국제사회의 복잡성이다. 빈부격차, 기술격차, 지정학적 관계, 역사적 배경 등에 따라 복잡하게 뒤얽힌 국제사회의 복잡한 이해관계가 국가간 공조를 어렵게 하기도 한다. 국제사회의 복잡성이 형사사법공조를 어렵게 만드는 이유는 첫째, 세계 곳곳에는 자국의 이익을 최우선으로 고려하는 국가들이 산재해 있기 때문이다. 유엔은 국가마다 돈세탁행위를 범죄로 규정해 철저히 단속할 것을 권고하고 있지만, 이를 실제로 이행하는 국가는 좀처럼 증가하고 있지 않다. 국제사회의 평판을 의식해 국내법의 개정 혹은 새로운 입법을 천명하고서도 산업자본의 이탈 등을 우려해 돈세탁단속을 미루는 국가가 많은 것이다. 둘째, 국가차원에서 '산업스파이'를 묵인 혹은 지원하는 경우가 많기 때문이다. 기술력과 자본력이 국제질서를 좌우하는 현실 속에서 국가가 경쟁력을 가지려면 첨단기술을 개발해 국가산업을 일으키는 노력이 절대적으로 필요하다. 개발도상국이나 저개발국가들은 말할 것도 없고, 선진국가 사이에도 첨단기술의 개발경쟁이 치열하다. 그

런데 경쟁국가를 능가할 수 있는 새로운 기술을 개발하기란 쉬운 일이 아니므로, 세계 모든 국가가 다른 국가의 신기술을 파악하기 위해 투자를 아끼지 않는다. 예를 들면 해커들을 동원하여 컴퓨터에 저장된 기계도면이나 공정설계도 등을 복사해 가기도 한다. 이러한 활동을 산업스파이라고 부르는데, 이들의 정보탐지 및 정보유출을 배후에서 조정하는 정부들이 이들의 범죄를 추적하고 적발하는 데 적극적으로 협력할 것을 기대할 수는 없다.

Ⅵ. 결 어

이상과 같은 한계를 정확히 인식하고 보다 현실적인 형사사법공조를 위해서는 현행 국제형사사법공조법을 사이버범죄에도 적용할 수 있도록 대폭 개정하고 이와 아울러 유럽과 미국에서 이미 발효하였고, 일본 등 기타 주요국가에도 적용을 앞두고 있는 사이버범죄방지조약에의 가입을 적극적으로 준비할 필요가 있다.

현행의 국제형사사법공조법은 사이버범죄에 적용하기에는 무리가 있다. 따라서 시간을 다투는 사이버범죄에 대응하기 위한 새로운 국제형사사법공조 모델이 만들어져야 한다. 유럽이사회 사이버범죄방지조약에서 제시하고 있는 것과 같이 저장된 컴퓨터 자료의 신속한 보존, 저장된 컴퓨터 자료의 접속에 관한 공조, 저장된 자료의 초국경적 접속, 전송자료의 실시간 수집에 관한 공조, 콘텐츠 자료의 감청에 관한 공조, 1주일 24시간 네트워크 구축 등의 조항은 전 세계가 사이버범죄라는 국경을 넘는 범죄에 공동으로 대응하기 위해 필수적인 국제공조 수단들이므로 이에 대한 규정은 우리 법제에도 반영되어야 할 것이다.

유럽 사이버범죄방지조약은 각국이 공동대처할 수 있는 사이버범죄의 유형을 해킹(및 바이러스유포), 컴퓨터사기, 아동포르노, 저작권(및 저작인접권) 침해 등 네 가지로 한정하고 있고, 최근 문제되고 있는 사이버도박, 사이버성폭력, 사이버스토킹, 사이버스쿼팅, 폭력유해사이트 등에 대하여는 규정하고 있지 않은바, 각국의 규제현황과 입장이 크게 달라 제외되었을 것으로 판단되지만, 추후 세계적 동향에 따라 사이버범죄의 새로운 유형이 추가될 수 있을 것으로 예상된다. 이 조약은 가입국의 찬반절차를 거쳐 비회원국 전체에 가입을 개방하도록 규정하고 있으므로 우리나라도 철저한 검토를 거쳐 가입을 준비해야 할 것이다.

한편, 현재 APEC 등에서도 위 사이버범죄방지 조약 수준의 법제정립을 추진하고 있으므로 조약 사항에 대한 국내 법제 작업을 검토해야 할 것이며, 보다 주도적으로 유럽 사이버범죄조약의 내용과 비슷하거나 더욱 다양한 내용의 사이버범죄조약 체결을 APEC 또는 한 · 중 · 일을 중심으로 추진해보는 것도 하나의 방안일 것이다.

참고문헌

강병섭, "국제재판관할", 재판자료 제34집 섭외사건의 제문제(하) (법원행정처, 1986)

권재원, "국제법상 국가관할권에 관한 연구 - 사이버스페이스상의 관할권을 중심으로 -" 연세대 석사논문(2002.6)

문규석, "국제범죄 개념의 이원론적 분류에 관한 연구" 외법논집 제7집 (1999.12)

백충현, "형사사건에 관한 국제사법공조" 이한기 박사 화갑기념논문집(박영사, 1978)

오기두, "형사절차상 컴퓨터관련증거의 수집 및 이용에 관한 연구", 서울대 박사논문(1997)

원혜욱, 인터넷범죄의 증거와 재판관할에 관한 연구(형사정책연구원 연구보고서, 2001.12)

이규홍, "형사사법에 있어서의 국제협력", 재판자료 제34집 섭외사건의 제문제(하) (법원행정처, 1986)

이영준, "유럽의회(Council of Europe)의 사이버범죄방지를 위한 국제협력(안) 소고" 형사정책연구 제12권 제2호(2001년 여름호)

정 완 外, 사이버범죄방지조약에 관한 연구, 형사정책연구원 보고서(2001.12)

정 완, "하이테크범죄대책에 관한 국제동향" 형사정책연구 제10권 제4호(1999년 겨울호)

정 완, "G8 국제조직범죄대책" 형사정책연구 제12권 제2호(2001년 여름호)

조규철, "한국경찰의 국제범죄 대응능력 제고방안에 관한 연구" 경기대 박사논문(2001)

조병인, 사이버경찰에 관한 연구, 형사정책연구원 보고서(2000)

탁희성, 형사절차상 digital evidence에 관한 연구, 형사정책연구원 보고서(2002.12)

하태훈·강동범, "정보사회에서의 범죄에 대한 수사와 재판", 정보사회에 대비한 일반법연구(II), 정보통신정책연구원(1998)

한봉조, "사이버범죄수사에 대한 국제적 협력문제", 한국형사정책연구원 제25회 형사정책세미나(2000.5.19) 자료

현대호, 인터넷상의 정보보호에 관한 법제연구(한국법제연구원, 2000)

홍성필, “관할권의 문제”, 정보법학 제3호(1999.12)

Michael L. Rustad, Cyrus Daftary, E-Business Legal Handbook 2002 Edition, (New York Gaithersburg, 2002)

Marcus Franda, Launching into Cyberspace - Internet Development and Politics in Five World Regions(LYNNE RIENNER Publishers, 2002)

John Seely Brown & Paul Duguid, The Social Life of Information(Harvard Business School Press, 2002)

Jan Samoriski, Issues in Cyberspace - Communication, Technology, Law, and Society on the Internet Frontier(Allyn and Bacon, 2002)

Ferrera etc, Cyber Law(West, 2001)

Jan Samoriski, Issues in Cyberspace - Communication, technology, Law and Society on the Internet Frontier (Allyn and Bacon, 2002).

Graham J H Smith, Internet Law and Regulation (3rd Ed.) (London: Sweet & Maxwell, 2002)

名和小太郎, 変わりゆく情報基盤 - 走る技術・追う制度(關西大學出版部, 2000)

田村善之, “デジタル時代の知的財産法制度” 現代の法 10. 情報と法(岩波書店, 1997)

西村總合法律事務所, IT法大全(日經BP社, 2002)

岡村久道, 新保史生, 電子ネットワークと個人情報保護(經濟産業調査會, 2002)

サイバーロ研究會 編, サイバースペース法(日本評論社, 2000)

International Cooperation for the Prevention of Cybercrime

Choung, Wan*

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the “cyber” prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the

* Professor, Law Department of Kyunghee University. Ph.D of Law

centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information

on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001.

The European Convention on Cybercrime was opened for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration, in Budapest, on 23 November 2001. and entered into force on 1 July 2004.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is the product of four years of work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the Organisation. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

주제어 : 사이버공간, 사이버범죄, 국제범죄, 사이버범죄조약, 국제협력, 국제공조, 형사사법공조

Keywords : Cyberspace, Cybercrime, International Crime, Convention of Cybercrime, International Cooperation, International Investigation, International Countermeasure