韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-3-5

# 국가간 사이버범죄 대응체제 구축에 관한 연구
## - 글로벌 거버넌스적 측면에서 -

오 태 곤*

# A Study on the Countermeasures of Cyber Crimes Among Nations
## - Focusing on the Global Governance -

Tae-Kon Oh*

## 요 약

사이버범죄는 가상공간에서 해킹, 바이러스 등과 같은 수단으로 목적물에 영향을 주어 예측 불가능의 피해를 초래한다. 특히 익명성을 담보로 시간과 공간을 초월하며 관련자의 처벌도 어렵다. 이러한 사이버범죄에 대처하기 위해서는 개별 국가 간의 법 제도의 상이성을 초월한 국제적인 형태의 공조체제가 필요하게 되는데 이에 대한 합리적인 대안이 '글로벌 거버넌스'이다. 이는 오늘날 전세계적으로 거버넌스가 사회체제나 정부의 역할 변화를 설명하는 중요개념으로 등장하여, 단순히 일개 국가의 전통적 통치행위를 대체하기 위한 개념이 아니라 인간의 사회적 행위 전반에 걸친 새로운 문제해결을 위한 인식체계로 자리 잡은 것처럼 사이버범죄에 대해 개인과 제도, 공공부문과 민간부문의 전범위적인 협조와 지속적 노력을 통해 합리적 해결책을 도출해 갈 수 있기 때문이다. 글로벌 거버넌스 측면의 사이버범죄 대응은 개별 국가 내의 민관 협조의 종합적 수사체제의 마련과 전문인력을 확보할 수 있으며, 국가간에 국제적인 공조체제를 구축할 수 있는 기반을 제공해 주는 것이다.

## Abstract

Cyber crimes caused unpredictable damages by influencing targets with means such as hacking and virus in virtual space. In specific, they transcend time and space because of their anonymity and it is difficult to punish the people who are involved in crimes. To manage such cyber crimes, we need an international cooperative systems beyond difference in legal systems between countries and 'Global Governance' was prepared as a reasonable alternative. These days, governance has been presented as an important concept to explain changed social systems or changed roles of government. Itwas not just a concept to replace traditional government of a single nation, but to overcome new problems on social actions of humans. So it is expected that it can help prepare reasonable measures through cooperation both in individuals and systems, and public and civil sectors. To countermeasure cyber crimes in terms of global governance, we can prepare general investigation systems and professional human resources through civil and public assistance, and provide a base on which international cooperation systems can be established.

▸ Keyword : 사이버범죄(Cyber Crime), 글로벌 거버넌스(Global Governance), 가상공간(Virtual Space) 수사체제(Investigation Systemx), 국제공조체제(International Cooperation System)

• 제1저자 : 오태곤
• 접수일 : 2005.05.25, 심사완료일 : 2005.07.14
* 전남도립남도대학 경찰행정경호과

# Ⅰ. 서 론

사이버범죄의 양태와 수법은 컴퓨터 관련 기술의 발달과 맞물려 새로운 모습들로 속속 나타나고 있다. 이로 인하여 사이버범죄의 대응은 기존 법체계 내의 추상적 구성요건의 조문 해석만으로는 구체적 법 집행과정에서 어려운 문제가 많이 발생하여, 관련 전문가의 입장에서도 위법행위와 적법행위의 한계를 구별하기가 매우 어렵게 된다. 즉 현대 형사법의 마그나카르타인 '죄형법정주의의 원칙'에 따라서 개별 행위에 대한 구체적인 규정이 필요하게 되는데, 일례로 미국 캘리포니아 주의 "Toll Fraud Law"에서는 전화사기의 행위태양을 다른 사람의 전화를 무단사용하거나, 루프를 이용하여 전화요금을 면제받는 행위, 전화카드를 위조, 변조하여 사용하는 행위, 제3자 부담전화를 함부로 사용하는 행위, 전화교환시설에 함부로 로긴(login)하여 전화통신 프로그램을 교란하는 행위, 이로 인하여 취득한 정보를 이용하는 행위 등을 구체적으로 열거하고 있고, 나아가 이러한 행위를 할 수 있는 기구나 장치를 제작, 소지, 매매, 양도, 배포하는 행위, 제3자 부담 전화번호, 전화카드의 번호체계, 발견된 루프의 전화번호 등 전화요금을 면제받을 수 있는 방법에 관한 책자나 전자적 기록을 제작, 배포하는 행위, 전화카드의 개인 식별번호를 알아내어 배포하는 행위 등 광범위하고 현대적인 프리킹(Phreaking) 행위태양까지 구체적으로 규정하고 있으며,[1] 법적대응이 미처 범죄의 발전속도를 제어하지 못하게 되어 사회 일반인들의 법감정으로는 응당 처벌되어야 함에도 불구하고, 법률의 불비로 이를 행사치 못하게 되는 것이다.

또한 사이버범죄는 초고속 네트워크망과의 결합을 통하여 국가를 초월한 가상공간에서 해킹, 바이러스 등과 같은 수단으로 목적물에 영향을 주어 예측 불가능의 피해를 초래한다. 특히 익명성을 담보로 시간과 공간을 초월하며 관련자의 처벌도 어렵다. 이러한 사이버범죄에 대처하기 위해서는 국가별 관련 법제의 정비는 물론이려니와 국가간 법 제도의 상이성을 초월한 국제적인 형태의 공조체제가 필요하게 되는데 이에 대한 합리적 대안 중 하나가 '글로벌 거버넌스'이다. 이에 본 논문에서는 먼저 오늘날 국가간, 개별 국가 내의 합리적 조정수단으로서 대두되고 있는 거버넌스에 대해 살펴보고 그 중 글로벌 거버넌스를 활용한 사이버범죄의 국가간 대응체제에 대해 연구한다.

# Ⅱ. Government to Governance

## 2.1 이론적 배경

1990년대 들어서면서 세계적으로 거버넌스(Governance)라는 개념이 사회체제나 정부의 역할 변화를 설명하는 중요한 개념으로 등장하고 있다. 거버넌스라는 개념은 다양한 시각에서 다양하게 정의되고 있으며, 학자들의 지속적인 관심과 노력에도 불구하고 거버넌스에 대한 일반화 작업은 아직 그 논의의 통일을 이루지 못하고 있다.[2] 거버넌스는 단순히 일개 국가의 전통적 통치행위를 대체하기 위한 개념이 아니라 인간의 사회적 행위 전반에 걸친 새로운 문제해결을 위한 인식체계로서 자리잡아가고 있다. 즉, 인간행위의 범위와 수준에 따라 거버넌스의 유형을 달리하는 것이다.

지금까지 거버넌스는 다양한 번역에서도 알 수 있듯이 개념상의 심한 혼란에 빠져 있었다. 그럼에도 불구하고, 일반적으로 거버넌스라는 개념은 정부의 역할, 정부운영의 체제, 그리고 사회문제의 해결방식에 있어서 새로운 변화를 의미한다. 거버넌스는 그 개념적 논의의 수준에 따라 다음의 세가지 형태로 정의되는데, 먼저 최광의로는 공통문제 해결기제로서의 역할이 강조되며, 광의로는 정부 관련 공통문제 해결 기제로서의 역할이 강조 된다. 그리고 협의로는 이른바 뉴거버넌스(New Governance)로서 그 개념의 다양성을 제기하고 있다.[3] 또한 사회적 공통문제인가, 혹은 정부 관련 공통문제인가에 따라서 최광의의 정의와 광의의 정의로 구분될 수 있을 것이다. 최광의의 정의는 국가 이외의 기업, 국제관계 등 다양한 단위·수준에서의 사회적 조정을 포함하는 반면에, 광의의 정의는 국가를 단위로 하는 공공문제와 관련한 사회적 조정을 범위로 한다는 차이가 있다. 그러나 공통의 문제를 해결하기 위한 다양한 사회적 조정방법을 포괄한다는 점에서는 거버넌스를 "공통의 문제를 해결하기 위한 사회적 조정기제"라고 정의할 수 있다.

이러한 거버넌스의 유형을 보면 대표적으로는 Rhodes가 제시한 여섯 가지의 거버넌스 형태로 기업관리방식, 신공공관리 방식, 좋은 거버넌스적, 국제적 상호의존적, 사회와 연

결된 사이버 체계, 신정치경제적, 네트워크로 분류되고 있다.[4] 이러한 논거 하에 최근에는 '정부 없는 거버넌스(Governance without Government)' 또는 '정부에서 거버넌스로(from Government to Governance)'로 표현하기도 한다. 그리고 김석준 등은 거버넌스의 이론적 접근방식에 따라서 전통적 정부통치의 형태와 유사한 국가가 주도적으로 시장과 시민사회를 관리하는 국가 중심의 거버넌스와 자본주의와 시장주의가 통치의 중심을 가지는 시장중심의 거버넌스, 그리고 민주주의의 핵심적 요소인 주민이 중심이 되는 시민사회 중심의 거버넌스, 이웃한 국가들이 범국가적으로 지역공동체를 형성하여 지역의 문제를 다루고 해결하는 리저널 거버넌스, 가상공간에서 공동체를 형성하여 운영하는 사이버 거버넌스로 거버넌스의 유형을 제시하고 있다. 이 외에도 거버넌스를 통치행위에 참여하는 주체들의 활동영역의 범위와 수준을 통한 네트워크에 의해서 분류하고 있는데, 이는 국가들 사이의 수준 및 지방정부와 자발적 조직들간의 정책 네트워크를 형성하는 글로벌 거버넌스(Global Governance), 단일 국가 내에서 전국적 수준으로 국정운영과 문제해결 방안들을 위한 네트워크를 가지는 내셔날 거버넌스(National Governance) 그리고 국가 내 지역수준에서 이루어지는 공동체를 중심으로 지방정부와 민간부문과의 협력체제와 네크워크에 중심을 두는 로컬 거버넌스(Local Governance)로 구분하고 있다.[5]

따라서 거버넌스는 세계화의 물결과 함께 국가간 협력과 문제해결을 지향하는 글로벌 거버넌스(Global Governance); 인접국가간 지역공동체를 중심으로, 또는 그러한 지정학적 한계를 초월하여 현안문제들을 해결하고자 하는 리저널 거버넌스(Regional Governance); 개별국가 내부에서 새로운 국정운영 방안을 찾기 위한 내셔널 거버넌스(National Governance); 지역공동체에서 시민참여와 지역발전을 모색하는 로컬 거버너스(Local Governance); 그리고 Cyberspace라는 가상공간을 통해 형성되고 운영되는 사이버 거버넌스(Cyber Governance) 등으로 나누어 살펴볼 수 있다. 본 논문에서는 이러한 각 거버넌스 유형 중 사이버범죄 대응을 위한 국가간 대응체제 구축과 관련하여 특히 글로벌 거버넌스적 측면에서 거버넌스의 개념을 정의하고자 한다.

## 2.2 글로벌 거버넌스

글로벌 거버넌스에 대해서는 계속적인 논의가 진행되고는 있지만 Young(1994)은 "독립적 행위자로 구성된 국제사회에서 갈등을 해결하고 상호협조를 목적으로 하는 게임의 규칙을 정할 수 있는 사회적 제도를 수립하고 운영하는 것"이라고 규정하였다. 한편, 글로벌 거버넌스 위원회(Commission on Global Governance)는 "개인과 제도, 공공부문과 민간부문에 걸쳐 공동 관심사를 다루는 다양한 방법의 총화로서, 상호 대립하는 다양한 이해관계를 해결하기 위한 협조적이고 지속적인 과정"이라고 정의한 바 있다.[6] 이와 같이 글로벌 거버넌스는 주권국가들 간의 협상과 계약이라고 보는 시각이 지배적인 것 같다. 여기서 협상이란 당사자들 간에 비용과 혜택을 각자의 능력과 의사에 따라 분담하는 것을 말하며, 계약이란 협상내용의 강제라는 의미를 포함하고 있다.[7] 즉, 거버넌스 활동으로서의 계약에는 합의의 내용 그 자체보다는 합의의 준수와 이행이 더 중요한 요소가 된다. 그러나 이들 개별 주권국가들은 공동문제의 해결을 위해 자발적으로 공식적, 비공식적 거버넌스 행위에 참여하는 것이며, 계약의 성립에도 불구하고 모든 통제권을 보유한다고 보는 것이 일반적이다.

## 2.3 글로벌 거버넌스와 국가간 관계

이러한 글로벌 거버넌스의 개념은 국제관계에서 몇 가지를 암시한다. 첫째, 일반적 거버넌스의 개념과 같이 글로벌 거버넌스도 일체의 공식적 제도나 기구를 전제로 하지 않는다. 그러므로 모든 국가간의 공식적, 비공식적 계약은 글로벌 거버넌스이다. 둘째, 글로벌 거버넌스는 참여한 개별 당사자에게 포괄적인 권한을 유보하는 무정부적인 것에서부터 개별 참여자의 권리가 극도로 제한된 계서제적인 것에 이르기까지 얼마든지 다양한 형태를 띨 수 있다. 양극단의 연속선상에서 글로벌 거버넌스는 ① 각국이 모든 주권을 보유하고 있는 무정부적 동맹관계(Anarchic Alliance) ② 종속적 위치에 있는 국가가 지배적 국가에게 독자적인 동맹권을 포기하는 영향력에 따른 계서제(Spheres of Influence) ③ 종속적인 국가가 일체의 외교권을 포기하는 섭정체제(Protectorates) ④ 광범위한 권한이 지배적 국가에게 이양되는 비공식적 제국(Informal Empires), 마지막으로 거의 모든 권한이 지배적 국가에게 귀속되는 제국체제(Empire) 등 어디에서도 발생할 수 있다고 보는 것이다.[8] 셋째, 글로벌 거버넌스는 반드시 국가간의 관계에서만 성립하는 것이 아니라는 것이다. 특히 NGOs 등 비정부조직의 위상이 나날이 커지고 있는 최근의 상황에서 국제 비정부조직이나 다국적기업들은 정부에 갈음하는 권한과 발언권을 가지고 구체적인 문제에 대한 영향력을 행사하고 있다. 그러므로 이러한 다양한 비정부조직과 행하는 일체의 국제적 협력과 협상, 그리고 계약도 글로벌 거버넌스 활동에 포함된다고 하겠다.

자발적 협력과 경쟁을 통한 협조형태인 거버넌스 체제는 모든 참여자가 독자적 주권을 가지고 공동의 관심사를 위해 노력하는 분권화된 행동의 장인 국제무대에서도 유용하게 적용될 수 있는 것이다.

### 2.4 글로벌 거버넌스 측면의 국가간 협력의 필요성

사이버범죄는 과거에는 전혀 문제시 되지 않던 새로운 형태의 범죄현상이다. 즉 과학기술의 발전에 따른 역기능으로서 새로운 형태의 범죄로 처음에는 한 국가 내에서 일어나는 문제라고 치부되기도 하였으나, 작금의 현실은 초고속 네트워크망을 통하여 국가간의 경계를 무시하고 있고, 또한 불특정 다수에 대한 대규모 피해를 야기한다는 점에서 거버넌스 관점에서의 사이버범죄 방지를 위한 협력체계가 필수적이 되었다고 할 수 있다. 이는 최근의 새로운 패러다임으로 논의되고 있는 파트너십, 네트워크 등의 거버넌스적 접근법에 의한 위기관리시스템의 구축 방안을 모색할 필요가 있다는 것을 의미한다. 파트너십의 핵심적 내용은 공동 책임성(Joint Responsibility)과 협력(Co-operation)이다. 파트너십은 파트너관계의 대상에 따라 크게 두 가지로 구분해 볼 수 있다. 하나는 공공부문과 공공부문간에, 다른 하나는 공공부문과 민간부문간에 파트너관계를 맺을 수 있다. 전자는 정부간 협력이고 후자는 민관협력으로 불린다. 물론 이 둘 사이에도 좀 더 세분화될 수 있는데, 즉 중앙정부와 중앙정부간; 중앙정부와 지방정부간; 지방정부와 지방정부간; 중앙정부와 민간부문간 등으로 나눌 수 있다. 파트너십이 중요한 관리 전략으로써 각광을 받고 있는 것은 사회의 속성이 변화하여 네트워크 사회가 도래하였기 때문이다. 네트워크 사회에서는 복잡한 사회작용과 관계가 특징이며, 이러한 복잡한 관계를 유지하는 최선의 대안적 전략은 파트너십이다. 네트워크 사회에서는 전통적으로 구분해 온 중앙과 지방, 시장과 계층제 또는 공공부문과 민간부문간의 구분은 더 이상 설득력이 없어졌으며, 현대 사회에서 공공과 민간 영역의 행위 주체들간의 상호의존성은 더욱 확대되고 있다. 이에 따라 공공과 민간영역으로 명명되어온 전통적인 조직 체계가 변모하고 있다. 이러한 네트워크 사회의 특성을 요약하면 크게 상호의존성과 복잡성이라고 할 수 있다. 즉 네트워크 사회에서는 공사영역간의 경계가 불분명해질 뿐만 아니라 여러 조직들 간에 상호의존성이 증가한다. 따라서 어떤 정책이나 사업이 목표를 달성하기 위해서는 여러 관련 행위자들로부터 협력이 요구되며, 이러한 조직 간의 상호의존성은 또한 복잡성을 낳는다. 그리고 복잡성은 공동의 목표달성을 위해 필수불가결한 자원을 가지고 있는 여러 행위주체간의 상호작용과 협상 과정의 결과인 것이다.[9]

세계화, 분권화의 진전과 더불어 고전적 개념의 국가를 중심으로 한 기존의 단층적인 거버넌스 만으로는 사회문제 또는 정책을 효과적으로 해결하기 어렵게 되었으며, 이제는 초국가적 국제기구, 국민국가, 지방 및 지역을 단위로 하는 다층적 네트워크 체제 또는 다층적 거버넌스(Multi-level Governance)를 구축할 필요가 있다. 특히 사이버범죄의 경우 더욱 한 국가 또는 한 지역에 국한되지 않고 발생하고, 또한 국가간의 경계가 중요한 의미를 가지지 못하기 때문에 이러한 다층적 거버넌스의 구축이 더욱 필요하다고 할 수 있다.

우선적으로 국가를 초월하는 지구적 문제를 해결하기 위해서는 국가간 협력체계인 글로벌 거버넌스를 구축할 필요가 있다. 사이버범죄의 경우 세계화가 더욱 심화됨에 따라 기존의 개별국가 단위의 정책결정 체제나 방지시스템으로는 효율적으로 대응할 수 없기 때문에 전 세계적 차원의 협력적 해결 방안이 필요하게 된다. 이러한 글로벌 거버넌스는 국가가 대외적으로 다양한 국제기구, 다른 국가와 국제적인 비정부조직 등과 관계를 맺으면서 국제사회의 변화와 도전에 대응하는 측면이라고 할 수 있다.[10] 그리고 중앙정부의 권한과 책임이 지방정부에 이양되는 수직적 분권화에 대응하기 위해서는 정부간 거버넌스를 구축할 필요가 있다. 일반적으로 지방정부의 권한과 책임이 이양되면 정부간 정책조정의 필요성이 증대되는 바, 정부간 거버넌스는 이러한 요구에 대응하기 위한 제도적 장치라고 할 수 있다. 특히 사이버범죄와 같은 위기발생의 경우 1차적 발생지의 대응과 복구가 가장 중요하다는 것을 감안할 때 중앙정부와 지방정부, 그리고 각 지방정부간의 협력체계가 아주 중요하다고 할 수 있으며, 이를 위해서는 무엇보다도 정부간 글로벌 거버넌스의 구축이 필요하다는 것을 알 수 있다.[11]

## III. 사이버 범죄

### 3.1 개념

컴퓨터의 발달과 보급에 따라 등장하게 된 신종범죄의 유형 중에서 근래 들어 가장 문제가 되고 있는 것이 바로

사이버범죄이다. 정보화 사회, 가상세계 내지는 사이버스페이스라는 말이 더 이상 어색한 것이 아닐 정도로 인터넷, PC통신과 같은 정보통신망이 일상생활 깊숙이 침투해있는 상황에서 인터넷을 필두로 한 사이버세계는 이미 현실의 세계에 버금가는 생활공간의 하나로 자리 잡게 되었다. 이런 상황 아래 범죄 역시 새로이 형성된 가상사회, 사이버스페이스를 기반으로 한 새로운 형태의 범죄들이 등장하고 있고, 이러한 범죄들은 기존의 컴퓨터범죄의 성질에 더해서 사이버스페이스 특유의 네트워크에 의한 전세계적인 연결이라는 특성에 따른 특유의 효과로 이미 상당한 사회적 문제가 되고 있으며 이러한 경향은 앞으로 더욱더 심화될 것으로 여겨진다.

이러한 상황아래에서 새롭게 등장하고 있는 인터넷 관련 범죄들을 유형화하고 정의하려는 시도들이 있으며, 이러한 견해들에서는 이들 정보통신망과 네트워크와 관련된 범죄를 사이버범죄 또는 정보범죄 등의 용어로 정의하고 있다. 사이버범죄란 사이버공간(Cyberspace)에서 발생하는 범죄를 총칭하는 용어로 사이버공간은 우리말로는 '가상세계' 혹은 '가상공간'으로 번역되어 인터넷과 통신망을 인프라로 한 또 하나의 생활공간이라고 할 수 있다. 따라서 사이버범죄는 무수히 많은 인터넷 사이트들과 그것들을 서로 연계시키는 컴퓨터연결망(인터넷)을 범행의 수단, 표적 혹은 무대로 삼는 범법사례를 총칭하는 개념이라고 말할 수 있다.[12]

또한 이러한 일체 유형의 컴퓨터 및 정보통신망과 관련한 범죄들을 정보범죄라 칭하기도 하며, 정보범죄란 좁은 의미의 사이버범죄 혹은 보다 더욱 넓은 의미로서 컴퓨터범죄와 컴퓨터관련 범죄현상을 포함하는 새로운 유형의 범죄행태 즉, '정보처리장치 또는 정보를 이용한 범죄, 그리고 정보처리장치 또는 정보에 대한 범죄를 총칭하는 의미'로 사용하는 견해도 있다.[13] 또, 주로 정보통신의 시스템의 보호에 중점을 두어 전산망 등으로 운영되고 있는 타인의 컴퓨터시스템 또는 컴퓨터프로그램이 정상적으로 작동하지 못하도록 하는 프로그램을 유포하거나, 컴퓨터의 부정조작을 통하여 타인의 컴퓨터 운영체계에 손상을 주는 행위, 컴퓨터의 부정조작, 컴퓨터 정보에의 부정침투 등을 통칭하는 것'으로서 컴퓨터시스템 운영방해 행위라는 개념을 사용하는 경우도 있다.[14] 이처럼 정보통신망을 기반으로 하는 사이버스페이스에서 발생하는 범죄의 개념에 대하여는 여러 가지 견해들이 있으며, 특히 사이버범죄와 같은 개념이 기존의 컴퓨터 관련범죄라는 개념과 어떠한 관계를 가지는 가에 대하여는 명확하지 않다. 따라서 기존의 컴퓨터 관련범죄와 구분되는 사이버스페이스를 기반으로 한 범죄들만의 개념적 성질들을 밝히는 것이 필요하며, 이를 위해 필요한 것은 다음과 같다.

먼저, 이러한 범죄들이 가지는 특징을 살펴봄으로써 그 유형상의 대상이 되는 범죄들을 정하는 것이 중요하다. 사이버범죄의 개념이 기존의 컴퓨터 관련범죄의 개념과 구별이 되는 특징으로는 기존의 컴퓨터 관련범죄의 유형 속에는 포함되기 힘든 소위 음란정보 등 불건전정보의 유통행위, 불법자금세탁, 명예훼손, 불법도박 등과 같은 전통적인 범죄에 의해서도 가능한 범죄에 의해서도 가능한 범죄들이 컴퓨터와 인터넷, 즉 사이버스페이스를 기반으로 범해지는 경우가 그 주된 범죄유형의 하나로 등장하게 된다는 것이며, 따라서 사이버범죄이건 혹은 정보범죄이건 그 용어사용의 문제에 앞서서 컴퓨터나 정보통신망 자체의 특성과 함께 기존의 범죄에 컴퓨터와 정보통신망(특히 인터넷)이 사용되는 경우 나타나게 되는 새로운 양상과 파급효과를 이러한 범죄의 개념 속에 어느 정도의 비중을 가지고 포함시킬 것인가가 먼저 논의되어야 한다. 이러한 관점에서, 전통적인 범죄에 컴퓨터와 인터넷이 이용되는 경우 매체의 특성에 따른 파급효과의 상이성을 인정하면서도 별개의 유형으로 구분하지 않는 견해도 있지만,[15] 이 경우에도 전통적인 범죄에 대하여 컴퓨터 및 인터넷과 결합한 새로운 양상이 가지는 특성에 대한 고찰이 이루어져야 할 것이며, 어떤 경우이든 이러한 정보화 사회라는 특수성을 외면할 수는 없는 것이 현실이다.

결국, 사이버범죄의 개념에서 보다 중요하게 생각해야 할 문제는 사이버스페이스라는 가상사회가 이미 현실사회와 분리할 수 없는 밀접한 관련을 가지며, 일상생활에서 빼놓을 수 없는 것으로 자리 잡고 있다는 점이다. 컴퓨터범죄, 사이버범죄, 정보범죄 등의 용어가 현재까지 매우 다양한 의미로 사용되면서 그에 포섭되는 범죄들 역시 매우 다양하고 비통일적이라는 점에서 볼 때, 이러한 범죄현상들을 어떻게 정의할 것인가에 있어서 중심이 되는 것은 개개 용어의 정의라는 면보다는 사이버스페이스라는 환경변화에 따라 발생하는 범죄들의 양상을 일정한 기준 아래에 하나의 범죄형태로서 포섭하는 것이 되어야 하는 것이다. 이런 점에서 볼 때, 사이버범죄의 개념을 정의하는 두 개의 축은 사이버스페이스라는 가상사회에서 컴퓨터의 특수한 기술적 특성들을 이용하는 기존의 컴퓨터 관련범죄들이 인터넷과 같은 네트워크와의 결합으로 어떠한 새로운 형태로 변모되고 있는가의 문제와, 현실사회의 전통적 범죄들이 가상과 익명의 공간이자 새로운 생활공간인 사이버스페이스 특유의 특성과 결합하여 어떠한 양상으로 일어나고 있는지에 대한 문제가 될 것이다.

이러한 맥락에서 사이버 범죄는 기존의 컴퓨터범죄의 특성을 모두 가지면서 그에 더해 정보통신망이라는 네트워크적 특성을 가지고 있으므로, 본 논문에서는 사이버범죄의 개념을 “정보통신망을 그 배경, 수단, 대상으로 하는 범죄들로서 컴퓨터 관련범죄의 한 유형임과 동시에 전통적 범죄의 정보통신망이라는 배경 아래에서의 특수한 발생형태를 포함하는 개념”이라고 정의한다.

### 3.2 특 징

사이버범죄는 보이지 않는 사이버 공간에서 해킹과 바이러스와 같은 수단으로 목적하는 대상의 정보시스템에 영향을 주어 목적하는 결과를 기대한다는 점에서 다음과 같은 여러 가지 새로운 특징을 갖고 있는데,[16] 첫째 전문성과 우발성을 띈다. 이는 컴퓨터가 지식인의 두뇌를 이용한 게임의 도구로 등장함에 따라 단순히 유희의 동기에서 범행이 자행되기도 하고, 컴퓨터를 다룰 수 있는 정도의 지식인이면 대부분 고등학교 이상의 고학력자들이고 두뇌도 명석한 편에 속하므로 생활의 곤궁을 겪는 경우가 많지 않아 빈곤을 해결하기보다는 개인적인 호기심의 충족과 향락의 추구 또는 영웅심의 발로, 기술능력에 과신과 우월감, 완전범죄를 꿈꾸는 범죄 심리에서 비롯되는 범행이 많으며, 그 동기 또한 사회나 자기 소속기관에 대한 불평불만 또는 상사에 대한 원한에 의한 범행이 많으며, 정치적인 동기의 범행도 자행된다. 최근에는 경제적인 경쟁이 국가간에 격심해지자 각종산업정보와 기술정보를 부정으로 빼내거나 중요자료를 지워버리는 행위를 국가의 한 정치 타켓으로 삼는 확신적인 동기도 늘고 있다고 한다.[17] 그리고 핵커(Hacker)라고 부르는 모험군은 다른 범죄동기와는 달리 자기 자신이나 제3자의 재산적 이익 없이 오직 자신의 모험심을 충족시키려는 동기로 범행하는 경우가 많다. 또한 컴퓨터를 가장 많이 접하게 되는 층이 젊은 층이라는 점에서 컴퓨터범죄자 역시 다른 재산범죄에 비해 연령이 비교적 낮고 초범인 경우가 많으며 행위자는 고도의 기술과 지능을 이용한 결과라는 점에서 파렴치범적인 죄의식보다는 자신의 능력에 대한 만족감을 얻는 다는 특색을 들 수 있다. 최근 미국에서 개봉된 ‘스타워즈3’의 경우에도 극장에 개봉되기도 이전에 영화사 서버를 해킹한 해커들에 의해 동 상영물의 불법복제물이 인터넷을 통하여 전세계에 유포됨으로써 사이버범죄에 대한 이슈가 다시 한번 세계민들의 이목을 집중적인 사건이 있었고,[18] 국내에서는 중국의 해커가 우리의 포털사이트를 경유하여 엔씨소프트의 리니지 서버를 해킹하는 사건이 발생하기도 하였다.[19] 둘째 광범위성과 동시성을 띈다. 전세계를 연결하는 초고속 네트워크 망은 의사소통을 매우 빠르게, 때로는 실시간(real time)으로 이루어지게 한다. 이러한 동시성으로 인해 사이버공간에서는 기존의 물리적 공간과 시간에 의한 구속을 받지 않게 되었다. 이에 따라 사용자는 자신의 메시지를 동시에 전세계 이용자들에게 전달할 수 있게 된 순기능이 있으나 다른 이용자 개인의 사생활을 침해하는 정보, 음란정보, 위험정보 등도 전세계 이용자들에게 전파시킬 수 있게 되었으며, 인터넷이 연결된 곳이면 어느 나라의 컴퓨터에도 바이러스를 유포시킬 수 있고 해킹도 가능하게 되는 등의 역기능이 있다. 셋째, 실행이 용이하다. 사이버공간의 기본적인 커뮤니케이션 수단인 인터넷은 단지 한번의 클릭만으로 상대방과의 의사소통을 가능하게 하므로 이용자는 별다른 고려 없이 즉흥적으로 특정 또는 불특정의 상대방에게 직접 정보를 발송할 수 있게 되었다. 이는 사이버공간의 구성원이 현실세계보다 용이하게 상대방과 접촉할 수 있으며, 메시지 전달의 공적 성격이 상대적으로 약하다는 것을 의미한다. 이러한 특성으로 인해 사이버공간에서의 반론 행위나 범죄행위가 현실세계에서보다 더욱 쉽게 발생할 수 있다.[20] 넷째, 자동성을 갖는다. 이는 프로그램에 부정한 데이터를 한번 삽입하면 결과를 원할 때는 항시 자동적으로 의도한 부정한 결과를 얻을 수 있으므로 매번 동일한 프로그램 조작행위를 할 필요가 없다. 정보처리과정에서 취약점을 발견하거나 어떠한 방법으로든 데이터 조작, 오용의 방법을 한 번 알아낸 이상 그러한 방법은 언제든 임의로 사용할 수 있다.[21] 즉 어떤 행위는 1회 행위를 명령하고 나면 그것을 다시 정지시키지 않은 한 그 행위는 자동적이며 영속적으로 전개된다는 것이다. 이는 일반범죄가 어떤 행위를 1회 실행하면 1회로 끝나는데 비해 사이버범죄는 1회 명령 또는 작동을 하여 두면 자동으로 행위가 이루어지며 또한 경우에 따라서는 그 작업이나 명령을 중지시키거나 지워버리지 않은 한 영구히 계속되는 것이 특징이다. 가장 대표적인 예로 1973년 미국 로스엔젤레스에서 발생한 최대의 컴퓨터범죄인 이퀴티 펀팅(Equity Funding) 보험사기 사건 경우 무려 64,000회 반복조작 범행이 이루어졌으며, 그 피해액은 20억불에 달하였다.[22] 다섯째 입증이 대단히 곤란하다. 사이버범죄는 적발과 증명은 대단히 어려운데 이는, 컴퓨터조작은 단시간에 처리되는 양이 대단히 많기 때문에 부정조작의 경우, 이를 사후에 자세히 검토하여 잘못을 가려낸다는 것은 사실상 어렵거나, 경제적으로 막대한 비용이 드는 경우가 많다. 이는 가상공간에서의 자료들은 국경도 없이 또한 이동식 저장장치 등의 좁은 공간에도 축소 저장시킬 수 있고, 또한 그 자료는 폐쇄성, 은닉성, 불가

시성을 갖기 때문에 그 적발과 증명이 곤난한 것이다.[23] 또한 네티즌들은 현실세계의 모습과는 전혀 다른 모습으로 사이버공간에 나타난다. 즉, 익명성으로 인한 취약점을 이용하여 다른 사람에 대한 명예훼손이나 모욕, 물품판매를 가장한 사기행위, 경쟁사의 소프트웨어에 하자를 발생하게 하는 등 지능적인 업무방해행위가 증가하고 있는 것 이다.[24] 마지막으로 쌍방향성을 그 특징으로 한다. 인터넷, 특히 월드와이드웹(www) 서비스를 이용할 경우에 나타나는 가장 두드러진 특징은 상호대화식 쌍방향 서비스가 가능하다는 것이다. 대화실, 전자우편, 그리고 뉴스그룹 등이 이용자에게 말하고 듣는 기회 모두를 제공하는 커뮤니케이션의 쌍방향적인 형태라고 할 수 있다. 이러한 쌍방향성으로 인해 인터넷 사용자들은 일반적으로 정보를 제공받는 것이 아니라 정보를 제공하기도 하고 대화할 수도 있게 되었으며, 이러한 특성은 음란물사이트 혹은 위험사이트의 개설을 가능하게 하고, 특히 익명의 사람들이 자살싸이트에 접속하여 독극물을 마시고 동반자살을 하는 사례가 있으며,[25] 특히 미성년자들의 인터넷 챗팅을 통한 성매매행위 등은 이미 우리 사회에 큰 문제가 된 바 있다.[26]

### 3.3 유형

국내 정보통신의 발전과 인터넷 이용의 폭발적 증가로 인하여 21세기 디지털시대로의 편승으로 인한 국가 경쟁력 확보라는 긍정적인 측면 외에 정보화 역기능, 즉 사이버범죄에 대한 심각성과 피해는 사회적 문제로 야기되고 있다. 이 같은 사이버범죄의 유형 구분에는 다음과 같은 견해가 있다.

첫째, 전통적인 기존 범죄 영역에서 발생하는 것과 신종 범죄영역으로 구분하는 방법이다.

둘째, 불법의 유형별로 행위에 의한 남용과 내용에 의한 남용의 두가지 유형으로 구분하는 방법이다.[27]

셋째, 사이버 세계 불법침입인 해킹을 중심으로 한 범죄유형과 기타의 범죄유형으로 분류하는 방법이다.[28]

넷째, 사이버 공간에서의 전통적 범죄유형, 사이버공간에서의 새로운 불법유형, 사이버공간에서만 특유한 불법유형의 3가지로 분류하는 방법이다.[29]

다섯째, ① 전상망 범죄로서 해킹범죄, 바이러스 범죄, 개인정보범죄, 전자상거래범죄를 들고, ② 불건전 정보범죄로서 음란물범죄, 소프트웨어 저작권 침해 범죄, 사이버폭력, 사이버 公害 범죄를 들고, ③ 영상미디어 범죄로서 채팅범죄, 온라인 게임범죄, 사이버 도박 범죄, 인터넷 방송국범죄 등을 들며, ④ 기타 범죄로서 반사회적 정보제작 및 유포, 반사회적 사이트 등을 드는 방법이다.[30]

우리 경찰청은 사이버범죄를 사이버테러형 범죄와 일반 사이버범죄로 분류하고 있는데, 먼저 사이버테러형 범죄는 정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스유포, 메일폭탄, DOS공격 등 전자기적 침해장비를 이용한 컴퓨터시스템과 정보통신망을 공격하는 행위라 하고, 일반사이버범죄는 사이버 공간을 이용한 일반적인 불법행위로서 사이버도박, 사이버 스토킹과 성폭력, 사이버명예훼손과 협박, 전자상거래 사기, 개인정보유출 등의 행위를 의미한다고 한다.

이와 같이 사이버범죄의 유형은 기술 발전의 단계 만큼이나 복잡하고 다양하며 범죄의 개별 태양 또한 다양하다. 그중 가장 대표적인 형태인 '해킹'과 '컴퓨터 바이러스'의 경우만을 보더라도,[31] 해킹은 ① 사용자 도용(일반적인 해킹형태로 다른 일반 사용자의 ID 및 패스워드를 도용하는 방법) ② S/W보안오류(컴퓨터내의 시스템 S/W나 응용 소프트웨어의 버그 등을 이용한 공격방법) ③ 버퍼오버플로우 취약점(소프트웨어 변수관리상의 문제인 오버플로우 버그를 이용하여 불법으로 명령어를 실행하거나 권한을 가지는 방법) ④ 구성설정 오류(시스템 S/W의 설치나 운영상에 오류를 이용한 공격방법) ⑤ 프로토콜 취약점(인터넷의 통신프로토콜인 TCP/IP의 설계취약점을 이용한 구조적인 공격기법) ⑥ 서비스 거부공격(시스템이나 네트워크의 정상적인 동작과 서비스를 방해하거나 정지시키는 공격) ⑦ 취약점 정보수집(특정의 시스템을 공격하기 전에 시스템의 취약점을 알아내고자 하는 스캔 공격) ⑧ 사회공학(관리자를 속여 패스워드를 알아내거나 권한을 얻어내는 공격) 등의 다양한 범죄 태양을 보이고 있으며, 또한 컴퓨터 바이러스의 경우도 ① 부트형(디스크드라이브를 인식하기 위해 처음 읽혀지는 부분을 부트영역이라고 하는데, 이 영역에 있는 운영체계를 공격하는 형태) ② 파일형(프로그램을 실행하기 위해 가장 필요한 실행 프로그램 파일을 공격하는 형태) ③ 부트/파일형(프로그램을 실행하기 위해 가장 필요한 실행 프로그램 파일을 공격하는 형태) ④ 매크로형(매크로 기능을 사용하는 마이크로소프트사의 워드나 엑셀 등의 자료파일을 매개체로 하여 컴퓨터 시스템을 공격하는 형태) ⑤ 트로이목마형(유용한 프로그램으로 위장하여 특정일자나 특정 조건이 되면 컴퓨터 시스템이나 파일을 공격하고, 개인정보를

불법적으로 취득하는 악의적인 해킹을 주 목적으로 하는 형태) ⑥ 웜형(다른 사람에게 보내는 E-mail에 자신을 첨부하여 빠른 전파력으로 인터넷 시스템, 하디디스크, 프로그램을 공격하는 형태) ⑦ 스크립트형(프로그래밍 언어가 아닌 언어로 작성한 짧은 프로그램이나 명령문들의 집합체를 이용하여 컴퓨터 시스템을 공격하는 형태) ⑧ 복합형(일반적인 바리어스형태에 해빙기법이 첨가되어 두가지 공격을 같이 하는 형태) 등의 다양한 태양으로 나타나며 이러한 유형들은 향후 더욱더 정교해지고 복잡다단해질 것 이다.

### 3.4 관련법규 및 현황

이와 같은 사이버범죄에 대한 현행 대응법제를 일별해 보면 다음 표와 같다.[32]

| | | |
|---|---|---|
| 전산망범죄 | 해킹범죄 | ·해킹자체<br>- 정보통신망 무단침입죄(정보통신망법 제48조)<br>·해킹에 의한 비밀침해<br>- 정보통신망비밀침해죄<br>(정보통신망법 제49조, 62조)<br>·해킹에 의한 재산취득<br>- 컴퓨터사용사기죄(형법 제347조의 2)<br>·해킹에 의한 자료삭제<br>- 정보통신망정보훼손죄<br>(정보통신망법 제49조, 62조) |
| | 바이러스범죄 | ·바이러스 전달·유포<br>- 악성프로그램 전달·유포죄<br>(정보통신망법 제48조 제2항,제62조 제4호)<br>·바이러스 제조<br>- 처벌규정 없음 |
| 전산망범죄 | 개인정보침해범죄 | ·개인정보 유출<br>- 개인정보무단이용죄(정보통신망법 제24조 1항,공공기관의 개인 정보보호법 제23조 1항)<br>·사이버 스파이<br>- 영업비밀무단사용죄(부정경쟁방지법 제18조) |
| | 전자상거래범죄 | ·전자상거래에 있어서의 기망행위로 인한 재산취득<br>- 사기죄(형법 제347조) |
| 영상미디어범죄 | ID도용 | ·ID도용<br>* 정보통신망법 개정안의 정보통신서비스이용 명의도용죄가 입법과정에서 삭제됨<br>- 정보통신망 무단침입죄<br>(정보통신망법 제48조, 제63조)에 해당하는 경우를 제외하고는 입법적 필요성은 존재하지 않음<br>* 주민등록법에 의하여 타인의 주민등록 번호를 무단사용하는행위의 가벌성 인정 |
| 영상미디어범죄 | 온라인게임범죄 | ·자살사이트, 자살교사, 방조죄<br>(형법 제252조 2항)<br>·폭탄제조 사이트, 무허가 약품거래 사이트 등<br>- 불법성 여부 검토 |
| | 사이버도박 | ·사이버 도박<br>- 도박죄·상습도박죄(형법 제246조)<br>- 도박개장죄(형법 제247조)<br>- 미등록 외환거래죄<br>(외국환거래법 제3조, 제27조 제1항 제5호) 등 |
| | 디지털콘텐츠무단복제범죄 | ·디지털 산업발전법(2002년 7월 15일 시행) |
| 불건전정보범죄 | 음란물범죄 | ·사이버성매매<br>- 성매매알선등행위의처벌에관한법률<br>(제21조 1항)<br>- 음행매개죄<br>(형법 제242조)<br>- 아동음행매개죄<br>(아동복지법 제18조 제5호,제34조 제1호)<br>- 청소년 보호법에서는 19세 미만의 자로 규정<br>·성매매·음란행위 관련 광고 행위(제20조 1항)<br>* 정보통신망법 개정안의 정보통신망이용윤락 알선죄는입법과정에서 삭제됨<br>*온라인사업자의 책임문제에 관하여도 명시적 입법은 없음<br>* 성매매알선등행위의처벌에관한법률이2004. 9. 23.자로 시행되면서윤락행위방지법은 폐기 |
| 불건전정보범죄 | 소프트웨어저작권침해범죄 | ·사이버 음란물<br>- 정보통신망 음란부호등 배포죄개정(정보통신망법 제65조 제2호)[33]<br>* 위 규정으로 전기통신기본법상 전기통신역무이용음란물반포죄는 정보통신망법 부칙 제5조 제1항은 삭제됨.<br>- 청소년유해매체물표시위반죄공죄<br>(정보통신망법 제42조, 제64조) |
| | 사이버폭력 | ·사이버 스토킹<br>(사이버 성폭력 포함)[34]<br>- 정보통신방이용 공포심 조성죄<br>(정보통신망법 제65조 제1항 제3호)<br>- 통신매체이용 성적 수치심 유발죄<br>(성폭력특별법 제14조)<br>* 스토커처벌특례법안의 입법이 현재 논의중임 |
| | 사이버공해범죄 | ·사이버 명예훼손<br>(정보통신망이용법 제61조)[35] |

* 출처: 경찰청 사이버테러대응센터에서 본인 재구성.

다음으로 우리 경찰청이 밝히고 있는 2001년부터 2004년까지 4개년간의 사이버범죄 관련 현황은 다음과 같다.[36]

사이버범죄의 발생현황 단위 : 건(명)

| 구 분 | 계 | 사이버테러형범죄 | | | 일반 사이버 범죄 |
|---|---|---|---|---|---|
| | | 소 계 | 해 킹 | 바이러스 | |
| 2001년 | 33325 | 10674 | 10562 | 112 | 22651 |
| 2002년 | 60068 | 14159 | 14065 | 94 | 45909 |
| 2003년 | 68445 | 14241 | 14159 | 82 | 54204 |
| 2004년 | 77099 | 15390 | 15348 | 42 | 61709 |

* 출처 : 경찰청 사이버테러대응센터(http://ctrc.go.kr)

사이버범죄의 검거현황단위 : 건(명)

| 구 분 | 계 | 사이버테러형범죄 | | | 일반 사이버 범죄 |
|---|---|---|---|---|---|
| | | 소 계 | 해 킹 | 바이러스 | |
| 2001년 | 22693 (24455) | 7595 (8099) | 7512 (8004) | 83 (95) | 15098 (16356) |
| 2002년 | 41900 (47252) | 9707 (10762) | 9650 (10689) | 57 (73) | 32193 (36490) |
| 2003년 | 51722 (56724) | 8891 (10047) | 8844 (9992) | 47 (55) | 42831 (46677) |
| 2004년 | 63384 (70143) | 10993 (11892) | 10955 (11846) | 38 (46) | 52391 (58251) |

* 출처 : 경찰청 사이버테러대응센터(http://ctrc.go.kr)

사이버범죄자의 연령별 현황 단위 : 명

| 구 분 | 계 | 10대 | 20대 | 30대 | 40대 | 50대 | 기타 |
|---|---|---|---|---|---|---|---|
| 2001년 | 5052 | 2193 | 1661 | 777 | 242 | 87 | 92 |
| 2002년 | 21817 | 8205 | 6876 | 3743 | 181 | 563 | 549 |
| 2003년 | 30150 | 10187 | 11185 | 5437 | 2277 | 725 | 339 |
| 2004년 | 36148 | 9391 | 13296 | 8176 | 3337 | 1289 | 659 |

* 출처 : 경찰청 사이버테러대응센터(http://ctrc.go.kr)

사이버범죄자의 직업별 현황단 위 : 명

| 구 분 | 계 | 무 직 | 학 생 | 회사원 | IT 전문직 | 자영업 | 전문직 (의사등 | 기 타 |
|---|---|---|---|---|---|---|---|---|
| 2001년 | 5052 | 1398 | 2039 | 735 | 76 | 404 | 47 | 353 |
| 2002년 | 21817 | 6763 | 6598 | 2876 | 283 | 2129 | 415 | 2753 |
| 2003년 | 30150 | 11620 | 8228 | 3237 | 202 | 2558 | 346 | 3959 |
| 2004년 | 36148 | 12533 | 8294 | 5251 | 449 | 3870 | 552 | 5199 |

* 출처 : 경찰청 사이버테러대응센터(http://ctrc.go.kr)

# Ⅳ. 글로벌거버넌스 측면의 사이버범죄 대응

## 4.1 사이버범죄의 전망

향후 사이버범죄는 기존의 운영체제 및 범용프로그램의 신규 취약점을 공략하기 위한 해킹프로그램이나 웜·바이러스가 출현하여 시스템 관리자들을 괴롭힐 것으로 예상된다. 또한, 기존 수법을 뛰어넘어 새로운 차원의 공격기법의 등장이 가속화 될 것으로 전망된다.[37] 이를 좀더 구체적으로 살펴보면, 향후에는 웜·바이러스 등의 전파속도가 가속화 될 것 이다. 인터넷 등 정보통신망의 발달은 신속한 정보수집, 전송 등 지식기반 정보화 사회촉진에 기여하고 있으나 각종 신규 출현한 웜 또한 이를 기반으로 전파속도가 급격히 증가하면서 동시다발적인 대량의 피해를 야기하고 있다. 특히, 2003년 1월 25일 사상 초유의 인터넷 마비사태를 초래했던 슬래머웜은 376바이트 크기의 웜으로 출현 당시 단기간에 전세계 수많은 호스트를 감염시킨 바이러스로 악명을 떨쳤으며 손실액만 10억 달러에 이르는 것으로 나타났다. 이는 2001년도에 맹위를 떨쳤던 코드레드웜 보다 두배 가량 전파속도가 빠른 것이다. 전파속도가 빨랐던 가장 큰 이유는 기존의 웜이 사전 접속단계가 비교적 복잡한 TCP 프로토콜을 이용했던데 비해 슬래머웜은 사전 접속 과정이 필요 없는 UDP 프로토콜을 이용했고 MS사의 취약한 범용시스템을 공격대상으로 삼았기 때문이다. 이처럼 웜·바이러스가 증가하면서 파괴력이 강력해진 이유는 전자우편 및 프로그램 불법복제를 이용해 유포되던 기존 바이러스와 달리 자동으로 시스템의 취약점을 공격하여 유포되는 해킹

기법을 적용하고 있으며 개인이 즐겨 사용하는 MS메신저 eDonkey와 같은 P2P 프로그램을 통해 확산되는 등 유포 경로가 다양해졌고 네트워크의 발달로 감염 후 순식간에 확산되어 대규모 피해를 유발함에 따라 해커들이 즐겨 찾는 수단이기 때문이다.[38]

다음으로 윈도우시스템 피해 증가세가 지속될 것이다. 최근에 해킹대응 분야의 특징 중 하나로 미 MS사가 개발한 NT 및 Windows 2000 운영체제를 탑재한 전산 시스템에서 피해가 지속적으로 증가하고 있다는 것이다. 2000년도까지는 윈도우시스템이 리눅스 등 유닉스계열의 시스템보다 사고발생이 없어 상대적으로 안전한 시스템으로 인식되어 왔으나 2001년 초반부터 해커들의 반미 반MS 분위기 확산을 MS사 관련시스템에 대한 공격기법 연구 및 공개가 늘어나면서 피해도 급증하고 있다. 또한 웹 해킹사고가 증가할 것 이다. 침입차단시스템 등 정보보호시스템 설치가 각급기관에 보편화되면서 외부에 공개할 필요가 없는 서비스 포트는 외부에서 접속하지 못하도록 아예 막아버리기 때문에 더 이상 해킹툴만을 이용한 과거의 손쉬운 해킹기법은 불가능해지고 있다. 따라서 해커들은 이러한 문제를 타개하기 위해 각 기관마다 외부에 개방하여 상시 서비스하고 있는 웹 서비스 포트 80번에 대한 공격기법을 연구하고 있으며 이에 대한 피해도 급증하고 있는 실정이다. 이러한 기법의 특징은 다른 해킹도구나 스캐닝도구가 전혀 필요없고 단지 인터넷에 접속할 수 있는 웹브라우저 하나만 있으면 된다는 것이다. 또한 웹프로그램은 보통 소규모 업체에서 제작하다 보니 기능과 디자인에만 치중한 나머지 보안을 고려한 코딩에 대해서는 관심을 갖지 못하는 것이 현실이며 주기적으로 갱신이 이루어지지 못하므로 취약점이 항시 내재되어 있는 것이 특징이다. 따라서 스크립트 카드로 알려진 초보자들보다는 전문해커에 의해 악용되고 있는 실정이다.

### 4.2 글로벌 거버넌스 측면의 대응체제 구축

이와 같이 사이버범죄는 과거 각 컴퓨터가 서로 연결되지 않은 상태로 각각의 개인 컴퓨터에 대하여 컴퓨터파괴, 해당 컴퓨터의 직접적인 불정조작, 바이러스 감염된 디스켓의 삽입 등으로 범죄행위가 이루어졌으나 오늘날 인터넷의 탄생과 네트워크의 발달로 거의 대부분의 범죄가 유선 통신망을 따라 이루어지는 범죄행위로 양상을 바꿔 발전되고 있음을 알 수 있다. 이제는 네트워크라는 하나의 가상공간 속에서 쫓고 쫓기는 상황이 발생하였으며 각국에서는 위 가상공간의 세계의 질서유지를 위하여 투자와 노력을 아끼지 않고 있는 것이다. 이러한 맥락에서 국가와 국가, 국가와 민간단체, 민간단체간의 유기적이고 종합적인 글로벌 거버넌스 측면의 대응은 필수 불가결한 것이다.

국가간 사이버범죄 대응체제를 구축하기 위한 글로벌 거버너스 측면의 과제는 다음과 같다. 먼저, 사이버범죄에 대한 종합적 대응체제를 구축해야 한다. 이는 한 국가 내에서의 대응체제의 확립은 물론이려니와, 사이버범죄 수사는 범죄 발생시 신속한 압수·수색과 이와 관련된 광범위한 전산증거자료들을 효과적으로 수집하지 않으면 안 된다. 따라서 신속한 증거수집과 원거리 또는 국제간 수사협력체제가 필수적이다. 또한 민간기관과의 협조 또한 필요불가결하다. 사이버범죄 수사는 다른 어떠한 유형의 범죄보다도 종합적인 수사체제의 확립이 중요하기 때문이다. 현재 우리 검찰에서는 서울에 정보범죄수사센터를 설치하여 사이버범죄 뿐 아니라 각종 유형의 첨단 정보시스템 범죄에 대한 종합대책을 강구하고 있으며 각 지방검찰청에 전담검사를 두어 각종 압수물과 증거자료 및 정보들을 계속 수집하고 각종 대규모 경제범죄 수사 등에서 컴퓨터로 처리된 각종 증거물들에 대한 분석업무를 지원하고 있으며, 경찰에서는 사이버범죄 수사대를 창설하여 금융관련범죄, 해킹관련범죄, 컴퓨터통신일반범죄, 바이러스관련범죄를 담당하는 수사관, 협력관과 연구관을 두고 있다. 사이버범죄 수사대는 국내외 컴퓨터 통신망에 대한 24시간 검색·분석 및 수사체제를 구축하여 해킹이나 바이러스 범죄 등 전문적, 기술적 범죄사건은 직접 수사하고, 일반 사건은 각 지방청에 하명하여 수사를 하고 있다. 국가정보원에서도 행정전산망 등 국가기간전산망의 보안에 각별한 관심과 노력을 기울이고 있고 주로 전산망 암호체제의 규제에 관한 외국의 동향을 예의 주시하고 이에 대한 국내의 문제점 등을 찾아내고 이의 개선방안이나 외국의 해킹 등에 대비한 대응방안 등을 강구하고 있다. 또한 정보보호의 주관부처인 정보통신부는 정보화기획실 아래에 있는 정보보호과에서 정보화 역기능 방지 업무를 담당하고 있고, 정통부산하기관인 한국정보보호센타와 정보통신윤리위원회가 정보화 역기능 방지를 위한 지원업무를 담당하고 있는 실정이다. 그러나 앞서 살펴본 바와 같이 처벌 법규조차도 통일적이지 못하고 개별법에서 산별적으로 규율하고 있는 것과 같이, 대응체제 또한 그 영역이 불분명한 체 여러 기관에 산발적으로 분포되어있으며 이 또한 유기적인 관계를 형성하지 못하고 있다. 둘째, 전문인력이 확충되어야 한다. 현재 사이버범죄 수사요원들도 상당한 수준의 컴퓨터 정보분석 능력을 갖추어야 첨단 테크놀로지를 이용한 범죄에 효과적으로 대처할 수 있는 바, 수사요원들을 이에 대처할 수 있는 수준으로 끌어올리거나 장기간의 꾸준한 전문적

인 교육훈련과 경험의 습득이 필요하다. 경찰에서는 금융관련범죄담당, 해킹관련범죄담당, 컴퓨터통신 일반범죄 담당, 바이러스 관련범죄 담당 등 4개 영역으로 분류되어 있어 범죄수사 및 단속의 방향이 주로 국내 문제로 좁혀서 접근하는 경향이 있다고 볼 수 있으며 실제 수사기관의 단속 또한 인터넷상의 단순한 검색 등으로 인한 원조교제나 불법컴퓨터프로그램의 무단 사용 그리고 음란물 등의 판매 등에 관한 단속 등에 그치고 있는 상황으로 전문적인 분야의 수사가 이루어지고 있다고 보기는 어렵다. 따라서 현행조직에 타 부처 조직과 수사 및 단속에 관하여 공조체제를 구축할 수 있는 요원, 국제적인 사이버범죄행위에 대처할 수 있는 전담요원, 연구기관과의 연계시스템을 관리하는 전담요원, 그리고 민간기구와의 글로벌 거버넌스 측면의 공조 시스템이 구축되어야 하는 것이다. 셋째, 컴퓨터보안기구와의 상호협조체제 구축이 필요하다. 사이버범죄 수사는 고도의 전문적이고 과학적인 첨단 기술이 필요한 수사로서 일반적으로 수사요원들은 이러한 전문적인 과학기술을 갖춘다는 것은 쉽지 않은 일이다. 따라서 전문적 과학기술분야의 실력을 갖춘 전문수사관들을 채용하여 양성도 하면서 그와 함께 전산망 보안기술에 관한 전문가조직, 예를 들어 전산망보안센터(Certcc)나 인터넷 침해사고 대응센터(CERT-Korea) 등으로부터의 전문적인 기술지원협력도 중요하다. 민간 분야의 역동적인 기술발전과 전문지식을 충분히 활용함으로써 사이버문화의 역기능을 최소화하고 사회방위 책임을 완수할 수 있다. 따라서, 수사기관은 외부 자문위원을 위촉하여 적극적으로 활용하고, 한국정보보호센터 등 유관기관과 업무협조체제를 상호 잘 유지하고, 또한, 사이버 공간에서 활동중인 연구기관, 민간단체 또는 자원봉사자를 적절히 활용하여야 할 것이다. 마지막으로, 국제적 수사기관 간의 정보교류 및 수사공조에 대한 협조체제 구축이다. 사이버범죄의 특징은 국제적인 통신망을 통하여 국경을 초월한 범죄가 벌어진다는 점이다. 통상 국가간의 형사사법공조관계는 외무부를 경유하여 상대방 국가의 법집행기관의 형사사법업무의 공조를 요구하는 것이나 이런 경우 통상 1개월 이상의 상당한 기간이 소요되어 통상의 국제형사사법공조절차는 현실적으로 소기의 목적을 달성하기 어려운 것이 대부분이다. 사이버범죄 수사에 있어서는 보다 국제적으로 신속한 수사협력체제의 구축이 필요하기 때문에 이러한 국제적 환경 하에서는 각국 형사사법집행기관간의 국제적 공감대 형성과 구체적인 협력방안 협의가 시급한 과제인 것이다.

## Ⅴ. 결 어

최근 언론보도에서는 '인터넷 상의 명예훼손'과 인터넷을 통한 '여론몰이식의 마녀사냥'에 대한 이슈가 뜨거운 감자가 되고 있다.[39] 즉, 1960년대 영화 '맨발의 청춘'에서 트위스트 춤으로 사랑 받았던 노배우 트위스트 김(본명 김한섭)이 이러한 사이버범죄 때문에 자살기도까지 했다고 하며, 그의 아내는 우울증에, 그의 손녀 딸은 주변 친구들의 놀림에 등교를 거부하는 지경에까지 이르렀다고 한다. 또한, 친구의 물건을 훔쳤다는 누명을 뒤집어쓴 여고생은 자살을 감행하기까지 이르렀다. 이러한 사건들은 사이버범죄로 인하여 나타나는 피해상황의 빙산의 일각에 지나지 않는다. 나날이 발전되고 있는 기술만큼이나 앞으로 얼마나 더 새롭고 다양한 형태의 사이버범죄 들이 자행될지 모를 일인 것이다. 이에 대응하기 위해 본 논문에서는 글로벌 거버넌스 측면의 사이버범죄 대응체제의 구축에 대해 연구하였다. 즉 상술한 바와 같이 전국광역으로 뿐만 아니라 국경을 넘어서 일어나는 특성을 가지고 있기 때문에 관련 전문인력의 양성을 통한 국제적, 국내적 유관기관에서의 협조체제가 반드시 구축되어야 하며, 이와 같은 맥락에서 향후 수사력의 중복방지와 과잉경쟁 예방을 위해 중앙에 사이버범죄 대책본부를 두고 종합적인 교육훈련과 수사대책 수립 및 운영, 관련 기관간의 업무협조, 관련 전문요원을 육성, 확충해나가는 것도 좋은 방안이 될 것이다. 국제적으로는 현재 국가간의 협약으로 체결하여 운영되고 있는 인터폴 내에 각국이 사이버범죄만을 전문적으로 수사공조하여 처리할 수 있는 기구를 별도의 협약을 통하여 설치하고, 이를 운영하면서 서로의 정보교류 및 수사공조의 활성화를 모색할 수도 있을 것이다.

마지막으로 글로벌 거버넌스의 한가지 단점으로 지적되고 있는 개별 국가단위의 국정운영의 대안으로서 개발된 거버넌스 개념이 국제적 영역에서 적용될 때 발생할 수 있는 경쟁의 공정성과 협조의 생산성 및 공익성을 어떻게 확보할 것인가 라는 문제가 있는데, 이러한 문제는 단순한 주권국가간의 모임이라는 기능밖에는 수행하고 있지 못한 UN이나, 미국 등 선진국의 이해에 지배되고 있는 IMF 등의 국제기구를 대체할 수 있는 국제적 레짐의 탄생과 이를 통한 민주적이고 효율적인 국제적 이슈의 관리라는 방법을 통해서 해결될 수 있을 것이다.

## 참고문헌


[1] 한봉조, "정보시스템 범죄 대응체계 동향", 대검찰청, 2000.8., 19면.

[2] 김정렬. "정부의 미래와 거버넌스, 신공공관리와 네트워크." 「한국행정학보」, 34(1), 2000, 21-39면.

[3] 이명석. "거버넌스의 개념화: '사회적 조정'으로서의 거버넌스." 「한국행정학보」, 26(4), 2002, 322-326면.

[4] Rhodes, R.A.W. "The New Governance: governing without government." Political Studies. 44(4), 1996, pp.652-667.

[5] 전영평, "지방정부의 거버넌스 모형 구축." 「행정논총」, 41(1), 2002, 47-70면.

[6] Young, O. R. (1994). International Governance: Protecting the Environment in a Stateless Society. Ithaca, NY: Cornell University Press, p.2.

[7] Lake, D. A. (1999). Entangling Relations: American Foreign Policy in its Century. Princeton, NJ: Princeton University Press, p.33.

[8] Ibid.

[9] 박광국·주효진. "인위재난관리의 효과성 제고에 관한 연구: 상인동 가스폭발사고를 중심으로." 「정책분석평가학회보」, 9(1), 1999, 91-113면.

[10] 정무권. "정부와 NGO와의 관계." 「사회과학논평」, 제20호, 2001, 17면.

[11] 이창용. "한국의 위기관리시스템 구축방안: 테러리즘 방지를 중심으로." (행정학박사학위논문, 영남대학교, 2004). 67-69면.

[12] 조병인·정진수·정완·탁희성, "사이버범죄에 관한 연구", 한국형사정책연구원, 2000, 18-21면.

[13] 최영호, "정보범죄의 현황과 제도적 대처방안", 한국형사정책연구원, 1998, 20-21면.

[14] 정병두, "컴퓨터시스템운영방해행위에 대한 형사적 처벌", 「해외연수검사연구논문집」 제11집 1호, 1995.12.

[15] 강동범, "컴퓨터범죄와 개정형법", 「법조」 제146권 8호, 1997.8., 109면.

[16] 오태곤, "컴퓨터범죄에 대책에 관한 연구", 「사회과학연구」 제25권 1호, 2003, 8-9면.

[17] 노연후, "컴퓨터범죄의 특징과 사례", 「수사연구」, 1993.6. 18면.

[18] 디지털타임스, 2005.5.27.

[19] 동아일보, 2005.6.15.

[20] 황승흠, "사이버공간의 분쟁해결", 제1회 법학자대회 발표문, 1998, 1면.

[21] 성낙현, "컴퓨터범죄의 형법적 대응방법", 「영남법학」 제1권 2호, 영남대 법학연구소, 1994, 97면.

[22] Donn B. Parker, Crime by Computer, Charles Scribner's Sons. 1976, p.118; 이철, 「컴퓨터범죄와 소프트웨어 보호」, 박영사, 1995.6. 28면.

[23] 정진섭, "인터넷과 컴퓨터범죄의 신동향", 「저스티스」, 1996.10. 40면.

[24] 최영호, 전게논문, 57면.; 강동범, "사이버범죄와 형사법적 대응", 한국형사정책연구원 제25회 세미나자료집, 2000.5. 72면.

[25] 동아일보, 2003.8.14.

[26] 경향신문, 2005.6.14.

[27] Lilie·Hans, Cyber-Kiminalitat und Pravention, 연세대학교 강연원고, 2000.10.6, 2면.

[28] 유인모, 정보형법의 과제와 전망, 형사정책 제12권 1호, 2000, 71면.

[29] 강동범, 전게논문, 72면.

[30] 2002년 한국사이버 범죄백서, 전자신문사.

[31] 이강래, 사이버테러 현황과 대처방안 연구, 국정감사 정책자료집, 2000.에서 재구성.

[32] http://ctrc.go.kr/rule/index.html에서 재구성.

[33] 중앙일보, 2001.1.6.; 아동포르노사이트 개설 10대 긴급체포.

[34] 국민일보, 2001.1.9.; 내연관계 제자 변심하자 전 교수 인터넷에 비방글.

[35] 조선일보, 2001.11.8.; 사이버명예훼손 34명 적발.

[36] http://ctrc.go.kr/statistics/index.jsp에서 재구성.

[37] 권선필, 지식정보사회의 향후구도와 한국의 효율적 정보화 전략 수립 방안 연구, 2001.

[38] 국가정보원, 국가정보보호백서, 2004.

[39] 동아일보, 2005.6.17.; 서울신문, 2005.6.15.


## 저 자 소 개


**오 태 곤**

2005년 2월 조선대학교 법학과. 법학박사

2005.~현재 :전남도립남도대학 경찰행정경호과 초빙교수 조선대학교 법학연구소 전임연구원 조선대학교 외래교수

<관심분야> 컴퓨터범죄, 테러리즘