2008년 추계 학술회의

사이버 문화의 확산에 따른 역기능 증가와 대응방안

일 자 : 2008년 11월 1일(토) 09:00~18:00

장 소 : 연세대학교 광복관 B102호

한국형사정책연구원
한국형사정책학회
연세대학교 법학연구소

학술회의 진행일정

09:00 - 09:30 등록

09:30 - 09:40 개회사 : 박 상 기 한국형사정책연구원장 ····· 5

09:40 - 09:50 축 사 : 손 동 권 한국형사정책학회장 ····· 7

09:50 - 10:00 휴 식

사 회 : 장 준 오 (한국형사정책연구원 선임연구위원)

□ 사이버 문화와 범죄의 사회적 충돌 □

10:00 - 11:10 **제1주제 : 정보화시대의 유비쿼터스 범죄: 사이버 범죄의 이해와 규제** ····· 11

Ubiquitous Crime in the Information Age: Understanding and regulating Cybercrimes ····· 23

발표 : David Wall (영국 리즈대 교수)

토론 : 남 형 두 (연세대학교 교수)
연 성 진 (한국형사정책연구원 연구위원)

11:10 - 12:20 **제2주제 : 사이버 공간에서의 사회적 엔지니어링과 범죄예방** ····· 35

Social Engineering and Crime Prevention in Cyberspace ····· 65

발표 : Roderic Broadhurst (호주 그리피스대 교수)

Nicholas Chantler (호주 퀸즈랜드 공과대 교수)

토론 : Rajiv Narayan (연세대학교 교수)
최 진 혁 (NHN 법무그룹)

12:20 - 14:00 점심식사

□ 사이버범죄의 법적규제 및 대응전략 □

16:20 - 16:30 휴식

17:40 - 18:00 **종합토론**

개 회 사

오늘 한국형사정책연구원과 한국형사정책학회가 공동으로 주최하는 2008년도 추계학술회의에 참석해주신 손동권 한국형사정책학회장님, 발표와 토론을 맡아주실 각계의 전문가 여러분, 그리고 이 자리에 함께해 주신 참가자 여러분께 진심으로 감사드립니다.

모건 스탠리의 조사에 의하면 2007년 전 세계 인터넷 사용인구는 13억 4,300만에 달합니다. 또 국내 인터넷 이용 인구는 세계에서 6번째에 해당하는 3,500만 명에 이르며 이는 전체 인구의 76%를 넘는 수치입니다. 인터넷의 발달은 사이버 공간이라는 새로운 가상의 생활공간을 만들었고 사이버 문화라는 새로운 사회현상을 낳았습니다. 인터넷의 다양한 편리함은 우리 삶의 질을 높이는 한편, 우리의 생활을 더욱 편리한 유비쿼터스 사회로 이끌 것으로 기대됩니다. 하지만 사이버 문화의 발달 속도에 상응하여 법적 보호 장치가 따라가지 못한 결과, 사이버 문화는 적지 않은 문제점을 안고 있는 것도 현실입니다.

사이버도박, 인터넷사기, 사이버 폭력이 범람하는 등 신종 사이버범죄가 등장하고 있습니다. 사이버공간에서 발생하는 인격권 침해의 수준은 이미 극에 달했고, 한번 누설된 개인의 신상정보는 다시 주워 담을 수 없는 심각한 결과를 초래하고 있습니다. 이처럼 사이버범죄는 사이버 공간에서 벌어지지만 그 부작용은 사이버 공간을 벗어나 현실세계에까지 미친다는 점에서 심각한 사회문제를 야기하고 있는 것입니다.

한국형사정책연구원에서는 이미 사이버범죄에 대한 효과적인 형사정책적 대안을 연구해 왔으며 현재 유엔과 사이버범죄 방지를 위한 온라인 교육 프로그램 구축사업을 추진 중에 있습니다. 이번 학술회의는 사이버 문화현상을 고찰하고, 사이버범죄에 대한 대응방안을 논의할 수 있는 자리로서 사이

버범죄의 예방과 통제를 위한 우리 연구원의 지속적 노력을 반영하고 있습니다.

사이버 모욕죄 도입여부에 대한 논란 등이 초미의 관심사인 현 시점에서 오늘 학술회의는 관련 학계와 실무계 전문가들의 소중한 연구결과와 미래전망을 공유할 수 있는 자리가 될 것입니다. 아무쪼록 이 자리가 건전한 사이버 문화의 확립에 이정표가 될 수 있기를 기대합니다.

끝으로, 바쁜 일정 중에도 이번 학술회의의 개최를 위해 힘써주신 손동권 한국형사정책학회 회장님, 훌륭한 발표와 토론을 해주실 전문가 여러분, 자리를 함께 해주신 참가자 여러분, 그리고 행사준비에 수고해 주신 형정원 직원 여러분께 다시 한 번 감사의 말씀을 드립니다.

2008. 11. 1.

한국형사정책연구원장 박 상 기

축 사

오늘, 한국형사정책연구원이 한국형사정책학회와 공동으로 해외의 저명한 전문가를 모시고서, 사이버 문화의 확산에 따른 역기능적 현상에 대해, 바람직한 대응방안을 모색하려는 국제학술대회를 개최하는 것에 대해서, 우선 진심으로 축하드립니다.

초대장에 쓰인 바와 같이, 인터넷의 발달과 가상공간의 확대 등으로 사이버 범죄가 날이 갈수록 증가하고, 그 형태도 더욱 지능화 고도화되고 있습니다. 이러한 사이버 범죄에 효율적으로 대응하기 위해서는 전문 기술 내지 지식의 습득과 국제적 공조가 특별히 요구되고 있습니다.

이러한 시점에 개최되는 오늘의 국제학술대회는 매우 뜻 깊고 시의적절한 논의의 장이라고 하겠습니다. 이러한 뜻 깊은 자리에 한국형사정책학회 회원들이 사회자, 발표자, 토론자로서 많이 참여할 수 있게 된 것은, 박상기 한국형사정책연구원 원장님의 배려와 이 학술대회를 기획하신 장준오 국제이사님의 노고에 힘입은 바가 큽니다. 두 분께 학회의 대표자로서 깊이 감사드립니다.

아무쪼록 오늘의 학술대회가 성공적으로 마무리되어, 전 세계적 문제로서의 사이버범죄에 대한 효과적인 대응책이 구체적으로 제시되기를 기대합니다.

끝으로 이러한 뜻 깊은 학술대회를 개최할 수 있도록 훌륭한 장소를 제공해 주신 연세대학교 법학연구소에게도 깊이 감사드림과 동시에 무궁한 발전이 있기를 기원하면서, 이만 축사를 마칠까 합니다. 감사합니다.

2008. 11. 1.

한국형사정책학회장 손 동 권

[10:00 – 11:10]

사이버 문화와 범죄의 사회적 충돌

제1주제 : 정보화시대의 유비쿼터스 범죄: 사이버범죄의 이해와 규제

발표 : David Wall (영국 리즈대 교수)

토론 : 남 형 두 (연세대학교 교수)
연 성 진 (한국형사정책연구원 연구위원)

정보화시대의 유비쿼터스 범죄: 사이버범죄의 이해와 규제

David Wall*

[초록]

사이버범죄는 컴퓨터 네트워크 기술을 매개로 하는 점에서 종전의 범죄와 다르다. 진정한 사이버범죄의 징표는 네트워크 기술이 없어지면 함께 사라진다는 것이다. 사이버범죄는 몇 세대를 거쳐 기술의 발전에 따라 진화해 왔으며, 세 가지 주요 범죄 행동 영역으로 구성된다. 즉, 시스템 통합성에 대한 범죄, 범죄를 위한 컴퓨터의 사용, 컴퓨터 콘텐츠와 관련된 범죄가 그것이다. 사이버범죄는 정보적, 세계화적, 네트워크적 특성, 특히 편재성으로 인해 수사 및 형사사법절차에 있어 많은 어려움을 제기한다. 그러나 사이버범죄를 창출한 그 동일한 기술은 그 범죄를 규제하는 데에도 사용될 수 있으며, 우리에게 유용한 법집행 도구를 제공한다. 하지만 그 도구가 함부로 사용되면 우리의 핵심적 가치를 손상시킬 수도 있으며, 따라서 개인의 안전과 프라이버시의 보호가 균형을 이루어야 한다는 점에서 새로운 법적, 정치적 어려움을 가져온다.

인터넷에 의해 만들어지는 새로운 범죄 용어의 목록은, 새로운 디지털 환경이 확립되어 범죄자에게 이용됨에 따라, 매년 늘어가고 있다. 개인정보 절취(phishing), 사이버 테러리즘, 정보 전쟁, 스팸, 서비스 거부 공격, 해킹, 크래킹, 핵티비즘, 이메일 사기, 옥션 사기, 클릭 사기, 신용 사기, 증오 범죄, 사이버 협박, 불법 온라인 게임, 극단적 포르노, 바이러스 웜과 트로이얀, 해커와 크래커 등은 현재 '사이버범죄'로 불리는 몇몇 새로운 용어들이다. '사이버범죄'라는 용어는 원래 1980년대 사이버펑크 소설에서 처음 나타났는데, 이는 사이버공간과 범죄를 조합한 개념으로, 여전히 많은 사람들이 '사이버범죄'를 '컴퓨터'나 '전자적' 범죄의 다른 이름 정도로 생각하고 있지만, 그 용어는 이제 공통적 용어가 되었고, 정책 형성에 대해 알리기 위한 분석적 개념으로 사용하려면 그 용어에 대한 이해가 필수적이다.

[사이버범죄의 본질에 대한 서로 다른 견해]

뉴스보도와 문헌을 대충 봐도 사이버범죄에 대한 다양한 견해가 있다는 사실을 알 수 있다. 예컨대, 컴퓨터 보안 전문가들은 사회에 대한 잠재적이

* David S. Wall, Ph.D., 영국, Leeds 대학교, 로스쿨, 형사사법 연구센터, 형사사법 및 정보사회 교수

고 실제적 위험에 대해 말하고, 다양한 전략적, 전술적 해법을 제시한다. 물론 그들 자신의 제품이나 서비스를 판매하는 경우가 적지 않다. 반면에 법적/행정적 계통에서는 수용될 수 있는 행위와 그렇지 않은 행위의 경계를 설정하는 규칙을 밝혀 이를 확립함으로써 발생할 수 있는 일과 그렇지 않은 일을 규정한다. 범죄학계와 일반적 학계에서는 이미 발생한 사실과 그 이유에 대한 분석을 제공하려 노력한다. 동일한 주제에 대한 이러한 서로 다른 취급은 일반인의 생각을 반영하는 사이버범죄에 대한 과학 소설이나 영화 등과 뒤섞여 있다.

따라서 사이버범죄에 대한 관심은 다양한 목소리로 표현되지만 이에는 공통적 이해가 결여되어 있다. 사실 컴퓨터와 관련된 단순한 법 위반도 '사이버범죄'로 간주되는 경향이 있고, 또한 일반적으로 인터넷을 사용하는 범죄와 인터넷에 의해 만들어진 범죄를 구분하지 못하기도 한다. 이러한 경향은 높은 수준의 사이버범죄 문제를 보도하는 혼란스러운 미디어 보도들이 해결해 주지 못하는 것이다. 예를 들어, Symantec의 2008년 4월 위험 보고는 매년 50만 건까지의 사이버범죄가 발생하지만 그에 대한 기소는 매우 낮은 수준이라고 평가했다. 예컨대 영국에서 1990년 컴퓨터 남용법이 제정된 후 150건 정도의 성공적 기소만이 있었다고 한다. 이러한 경향은 다른 국가에서도 마찬가지이다.

[사이버범죄의 세대 구분]

사이버범죄는 사이버공간을 창조하고 사이버공간에 정보적, 네트워크적, 세계화적이라는 특징을 부여한 네트워크 기술과 함께 진화해 왔다. 그러므로 사이버범죄가 네트워크 기술에 의해 매개되거나 형성되는 해로운 행동으로 인식된다면, 사이버범죄 분석을 위해서는 그러한 기술들에 의해 매개되는 수준을 기준으로 사이버범죄를 유형화할 수 있을 것이다. '변형시험'을 적용함으로써 이는 단순하게 인터넷이 없는 상황을 가정할 때 그 범죄가 어떻

게 될 것인가를 생각해 보는 것이다. 3가지 세대로 사이버범죄를 구별할 수 있다. 각각의 세대는 기술적 매개에 있어 서로 다른 정보적, 네트워크적, 세계화적 수준의 조합으로 구성된다.

첫째, 세대의 사이버범죄는 컴퓨터를 사용하는 전통적 혹은 일반적 범죄이다. 처음에 이러한 사이버범죄는 별개의(보통 대형 컴퓨터) 연산 시스템 내에서 발생했다. 오늘날은 컴퓨터를 통신수단으로 사용하거나 혹은 범죄 사주와 범죄 조직을 위한 사전 정보를 수집하기 위해 사용하는 범죄도 이에 포함된다(뒷부분 참조). 요점은 비록 그러한 범죄들이 심각한 충격을 주지만, 인터넷이 없어지더라도 그러한 범죄들은 지속될 것이기 때문에 제일 낮은 수준의 사이버범죄라는 것이다. 인터넷이 없어져도 범죄자들은 그저 다른 통신 혹은 정보 수단을 사용할 뿐일 것이다.

둘째, 세대의 사이버범죄는 하이브리드 사이버범죄로, 이는 네트워크 기술이 전적으로 새로운 세계적 기회를 제공하게 된 '전통적' 혹은 법제화된 범죄이다. 이러한 범죄들은 네트워크를 통해서 이루어진다는 점(예컨대, 옥션 사기)에서 첫째 세대의 범죄와는 다르다. 인터넷이 없어도 이러한 범죄는 다른 형태로 지속될 것이지만, 이 경우 그 규모가 세계적이지 못하기 때문에 여러 국가나 문화에 걸치는 일은 없다.

셋째, 세대의 사이버범죄는 진정한 사이버범죄이다. 이는 전적으로 인터넷의 산물로서 인터넷이 사라지면 함께 사라질 최고 수준의 사이버범죄이다. 이에는 '스팸', '피싱(ID절취)' 및 '파밍(브라우저의 탈취)' 그리고 여러 가지 온라인 지적재산권 침해가 포함된다.

기존의 범죄가 이미 첫째와 둘째 세대의 사이버범죄에 적용되고 기존의 법집행 경험이 활용될 가능성이 높기 때문에(비록 법체계 내에서의 지위는 만족스럽지 못할지라도), 주요한 법률문제는 실체법이 아닌 법적 절차와 관련되기 쉽다. 그러나 셋째 세대의 진정한 사이버범죄가 발전하여 고유한 하

나의 유형이 되면서, 유럽연합, 미국 등의 지역에서의 스팸 관련 입법과 같은 새로운 입법이 요구되고 있다.

[사이버범죄의 유형]

사이버범죄의 세대적 구분과 함께, 실체적 범죄 행동을 기준으로 사이버범죄를 유형화할 수 있다. 이러한 유형은 3가지로 기존의 법률 및 법 집행 실무에 각각 연결될 수 있다.

컴퓨터 통합성에 대한 범죄, 예컨대 해킹과 크래킹, 사이버 폭력, spying, DDOS(서비스 거부) 공격, 바이러스 등은 각각 컴퓨터 네트워크 액세스 메커니즘의 통합성을 공격한다. 컴퓨터 통합성에 대한 범죄는 종종 좀 더 심각한 범죄를 위한 초석이 된다(아래 '피싱' 참조).

예를 들어 크래커들은 트로얀, 즉 나중에 다른 범죄에 이용(botnet로서)할 수 있는 '백 도어'를 설치하는 바이러스를 사용한다. 그 다른 범죄는 감염된 주소 목록을 구입한 스팸 발송자들에 의한 것일 수 있다. 대부분의 국가는 현재 이에 관한 입법을 갖추고 있다. 예를 들어, 2가지만 든다면, 영국의 컴퓨터 남용법(1990)이나 미국의 컴퓨터 사기 및 남용법(1986, 18 U.S.C. 1030) 등이 그러한 입법이다. 그러한 법률들은 유럽회의(Council of Europe) 사이버범죄조약(ETS No. 185)에 의해 국제적으로 조화를 이루고 있다. 이를 통해 컴퓨터 자료에 대한 비권한 접근, 추가적 범죄를 위한 비권한 접근, 컴퓨터 자료의 비권한 수정으로부터 컴퓨터 사용자들을 보호하고 있다. 비록 컴퓨터 남용 법률들의 실효성에 대한 의문이 없는 것은 아니지만, 그것은 분명 법적 기타 예방적 조치를 위한 중요한 출발점을 제공하고 있다. 현재까지 54개 국가 중 대략 절반이 서명하고 비준한 사이버범죄 조약에 있어서도 마찬가지이다.

컴퓨터 활용(관련) 범죄, 예컨대 '피싱'이나 진보된 수수료 사기 등은 컴퓨터 네트워크 시스템을 이용해(종종 합법적으로) 현금, 상품 또는 서비스를

부정하게 획득하는 것이다. 대부분의 국가들은 절취 및 사기 관련 법률과 손실된 자산의 회복을 위한 법적 절차를 마련하고 있다. 이와 함께 불법한 지적재산권 침해를 방지하는 지적재산권 관련 법률을 갖추고 있다.

컴퓨터 콘텐츠 범죄들은 컴퓨터 네트워크 시스템의 불법적 내용과 관련되며, 포르노의 거래 및 배포, 증오 범죄적 자료, 사기적 내용의 자료 등을 포함한다. 대부분의 국가들은 외설 관련 법률과 증오 유발을 금지하는 법률에 있어 편차를 보이고 있으며, 그러한 법률도 언론과 표현의 자유를 보장하는 법률로 인해 그 규제 수준의 강약을 보이고 있다.

기술적 매개 수준과 범죄 행위 유형을 기준으로 한 위의 구분들은 정책 형성에 있어 중요한 분석적 기준점을 제시한다. 위의 유형들을 다양하게 조합한 범죄 '매트릭스'를 통해 여러 유형의 사이버범죄 간에 존재하는 차이를 볼 수 있으며, 이는 예컨대 금전적 혹은 인적 자원을 어떻게 활용해야 할지를 결정함에 있어 사용될 수 있다.

범죄 매트릭스	컴퓨터 통합성에 대한 범죄	컴퓨터 활용 범죄	컴퓨터 콘텐츠 범죄
1세대: 일반 범죄	시스템 내의 해킹	시스템 내의 사기	극단적 포르노의 저장
2세대: 하이브리드 사이버범죄	시스템 간의 해킹	시스템 간의 사기	포르노/증오 범죄 자료의 유포
3세대: 진정한 사이버범죄	피싱/DDOSA/바이러스 스팸/다운로드에 의한 드라이브	마이크로 사기(long tail 범죄)	포르노/증오 범죄 자료의 전송

[온라인 범죄 조직]

사이버범죄가 진화하면서 연쇄적 효과로서 범죄 조직에 변화가 일어나고 있는데, 특히 범죄의 온라인 자동화가 특징인 2세대 및 3세대 범죄에 있어 그러하다. 개인 컴퓨터의 출현은 전체 범죄 과정의 장악을 1명 혹은 2명의 전문가의 수중에 놓이게 했는데, 그 예로 한때 세상을 공포에 떨게 했던 '해킹'이 있다. 그러나 더 최근에는 '플러그 앤 플레이' 및 '클라우드' 컴퓨터 시

스템의 출현으로, 운용 시스템에 대한 특별한 지식의 필요성이 극적으로 감소했다. 이러한 기술은 온라인을 통한 범죄 이익의 잠재성 증가와 조합하여, 은신 가능성과 수익(범죄 경영 윤리에 있어) 극대화의 욕구가 윤리적 유행과 윤리적 해커들의 기술적 허세를 대체하게 만들었다.

이러한 강력한 조합은 또한 새로운 형태의 평등하고 비계층적 범죄 조직을 요구해 왔다. 범죄자는 이제 냉정하게(전문가적으로 계약에 기초하여) 스패머, 즉 자신을 위해 스팸과 해킹을 할 수준 높은 소프트웨어를 만드는 바이러스 전문가를 고용한다. 예컨대 스팸 등을 통해 사기를 위한 사전 정보로서 개인정보를 절취하는 것이다. 그들이 만드는 악성 소프트웨어는 개인적으로는 작지만 전체적으로는 큰 희생을 만들어 낸다. 사이버범죄의 최신 세대는 적은 범죄자가 비율에 맞지 않는 양의 범죄를 저지르는 비대칭적 희생 창출의 새로운 세상을 만들고 있다. 결국 투자에 대비한 높은 수익 및 낮은 위험을 통해, 높은 위험의 5천만 달러 한 건을 저지르는 것보다, 기술적으로 50만 명에게 1달러씩을 벌어들이는 것을 선택할 수 있게 되었다.

[사이버범죄 및 형사사법 절차]

적용 가능한 국내 및 국제 법률의 존재에도 불구하고, 사이버범죄의 독특한 특성은 전통적 수사 절차를 어렵게 한다. 이러한 정보적, 네트워크적, 세계화적 범죄는 개인에게는 사소하고 전체적으론 엄청난 피해를 입히는 특성이 있다. 이러한 성질로 인해, 사이버범죄는 각국의 법 집행 및 형사사법 절차 시스템이 그러한 범죄에 반응하기 곤란하게 만드는 '사소한' 문제만을 만든다. 수사를 하기에는 개인적 피해가 너무 적은 것이다. 나아가 사이버범죄가 야기하는 위험 - 관념적이 아닌 실질적 위험은 잠재적 혹은 실재적 희생자에게 항상 직접적으로 명확한 것만은 아니다. 개인적으로 심각하게 여겨지지 않거나 실제로 심각하지 않은 것이다. 그러나 그러한 범죄들은 총계를 기준으로 볼 때, 혹은 보다 중대한 범죄의 사전 조치로서 기능한다는 점에서

볼 때, 잠재적 위험성을 가지고 있는 것이다. 초기에 대두된 각 범죄행위들은 바로 이러한 잠재성을 잘 설명해 준다. 예컨대 컴퓨터 통합성에 대한 사이버범죄들은 종종 다른 형태의 좀 더 심각한 범죄를 위한 문을 여는 것이었다. 컴퓨터의 개인정보 절취는 그 정보가 그 당사자에 대해 사용될 때에만 심각성을 가지게 된다. 마찬가지로 원거리에서 제어할 수 있는 트로얀에 감염된 '좀비' 컴퓨터의 로봇 네트워크(또는 botnets)는 다른 범죄를 위해 사용될 수 있다. 컴퓨터 활용 범죄, 예컨대 사기꾼에 의해 저질러진 인터넷 스캠은 스패머와 공모하여, (앞서 언급한 바와 같이) 개인적 차원에서는 비교적 사소하지만 총계를 기준으로 하면 본질적으로 중대한 성격을 가진다. 컴퓨터 콘텐츠 범죄들은 비록 주로 정보와 관련되어 있고 항상 불법인 것은 아니지만, 그럼에도 불구하고 사기적이고 매우 공격적일 수 있고, 심지어 타인에 대한 공격을 유발하거나 편견적 행동을 유발할 수도 있다.

형사사법 기관이 직면한 또 다른 문제는 특히 전통적으로 범죄로부터 사회를 보호하는 공공 경찰에 대해 사이버 범죄에 대응하도록 하는 지역적, 국가적, 국제적인 정치적 요구이다. 그러한 요구는, 비교적 적은 체포 및 기소가 이루어지는 상황에서, 뉴스 매체(그리고 사이버 보안 부문)에 의해 그려진 '사이버범죄'의 물결에 대한 법 집행의 명백한 불균형에 의해 일반적으로 촉발된다. 이러한 불균형에 대한 한 가지 이유는 대부분의 국가에서 지역 경찰이 그들의 일상적 활동을 기준으로 엄격하게 한정된 예산 내에서 활동해야 하고, 따라서 세계화된 전자적 네트워크로부터 발생하는 범죄를 조사하도록 하는 요구에 대처하기 어렵기 때문이다. 그러나 이러한 이유가 나름대로 중요성을 가지지만, 이는 분명 사이버범죄를 다룰 수 있는 능력을 개발하기 위해 경찰 기관들이 (종종) 들이는 실제적 노력을 무시하는 경향이 있음을 부인할 수 없다. 더 그럴듯한 설명은 불균형이 기대와 실재 사이의 간극으로 초래된다고 하는 것이다. 왜냐하면 공공 경찰은 사이버공간의 전체적 경찰활동에 있어 매우 작은 역할만을 하기 때문이다. 비록 지금이 21세기이

지만, 영국 공공 경찰과 다른 국가들의 경찰들은 여전히 100년이 넘는 과거에 주어진 원칙에 따라 업무를 하고 있다. 따라서 소아성애자, 아동 포르노 제작자, 사기꾼, 사회기반을 위협하는 테러리스트들, 그리고 좀 더 심각한 해커들과 같은 위험인물들에 대해 사회적 자원의 초점이 합리적으로 맞추어져야 한다. 그러나 이러한 비판이 사이버공간을 방치하자는 것을 주장하거나, 경찰활동이 비효율적, 비효과적이라는 것을 주장하는 것은 아니다. 오히려 공공 경찰의 역할은 좀 더 광범하고 널리 정보화가 된 인터넷 경찰활동의 네트워크 및 노드 구조 내에서 이해되어야 한다. 이러한 구조는 인터넷 사용자들과 사용자 그룹들, 디지털 환경의 조정자들 및 게이트키퍼들, 네트워크 기반 제공자들, 회사 보안 조직, 비정부, 비경찰 조직, 정부의 비경찰 조직, 공공 경찰 조직으로 이루어져 있다.

이러한 각 그룹들은 온라인 질서를 유지하기 위해 서로 다른 도덕적, 계약적(경제적), 기술적 혹은 법적 제재를 조합하여 사용한다. 이것은 사인의 경제적 이익을 보호할 책임이 있는 자들에 의해 공공의 이익이 보호될 수 있을 것인가에 대한 중요한 의문을 제기한다. 이러한 네트워크에의 참가는 그들의 규율 기능을 좀 더 효과적으로 만들기 위한 출발점이 된다. 이러한 네트워크에는 조직의 국제적 제휴, 복합 기능 기관, 초부문적 파트너쉽 및 제휴 그리고 국제적 정책 협력 등이 포함된다. 장래에 예상되는 어려움은 경찰이 사적 부문 내에서 좀 더 효율적으로 활동할 수 있도록 하면서 보안을 강화하기 위해 소프트웨어 기술을 일상적으로 무분별하게 사용하게 되는 거의 전 세계적인 흐름을 어떻게 조절할까 하는 것이다.

[사이버범죄에 대한 경찰활동]

소프트웨어 기술은 디지털의 규제자로서 법률보다 훨씬 더 강력하다. 왜냐하면 그것은 구조를 통제할 수 있을 뿐만 아니라 그 구조 안에서 벌어지는 행동을 형성할 수도 있기 때문이다. 사이버범죄에 적용되는 경우, 이 '디지털'

현실주의는 더 많은 범죄가 새로운 기술에 의해 억제될 수 있고, 동일한 기술에 의해 경찰활동이 더 효과적으로 이루어질 수 있다는 것을 의미한다.

그러나 기술적 개입은 일련의 새로운 윤리적 및 법적 문제를 제기하기 때문에, 예컨대 그것이 합법적인가 혹은 윤리적인가? - 그러한 개입이 성공하려면 승인될 수 있는 법적, 사회적, 경제적 및 기술적 틀 내에서 이루어져야 할 것이다. 편재적인 기술적 경찰활동이 통제되지 않으면, 이 활동은 현재 많은 자유사회에서 옹호되는 민주주의적 가치를 잠식할 수 있다. 그러나 좀 더 낙관적으로 볼 때, 사이버범죄를 통제하기 위한 기술의 사용이 승인될 수 있는 사회적, 법적 맥락 내에서 이루어진다면 그 기술은 경찰활동 과정에 도움을 줄 수 있을 것이다. 나아가 네트워크 기술을 강력한 경찰 도구로 만드는 동일한 감시적 특성이 경찰 혁신 과정에도 도움을 줄 수 있을 것이다. 왜냐하면 그러한 기술이 경찰에게 좀 더 광범위한 조직적, 공적 책임을 부여할 뿐만 아니라, 경찰과 경찰활동을 감시하는 데에도 사용될 수 있기 때문이다.

현재 매우 중요한 관심사는, 경찰관의 활동의 틀이 원칙적으로 국가의 법률에 의해 정해지고 그에 더하여 여러 가지 지역적 법령의 규제를 받지만, 경찰의 다른 많은 파트너들(위에 기재한)은 인터넷에서 경찰 활동을 하면서도 전체적인 국법의 틀 내에 구속되지 않는다는 것이다. 나아가 사이버범죄에 대한 경찰활동을 위해 소프트웨어 사용이 급증함에 있어(주로 사이버 보안 산업의 영향에 의한 급증) 견제와 균형이 결여되어 있다는 것은 염려가 되는 부분이다. 스팸 필터는 사이버범죄 문제에 대한 성공적인 기술적 해결의 예이다. 그러나 아무도 스팸을 원하지 않는 것은 사실일지라도, 현재까지 스팸 필터를 전송 메커니즘에 적용하는 것에 대해 비판적인 논의는 거의 이루어지지 않았다. 결과적으로 많은 부작용이 발생했다. 스팸 필터가 정당한 의사소통을 제한하거나(예컨대 중국, 한국, 일본 등으로부터의 정당한 이메일), 오래 지속되어 온(물론 변화는 있을 수 있지만) 원칙, 즉 최종사용자에서 최종사용자의 원칙에 저촉될 수 있는 것이다. 그 원칙은 누구든 네트워

크를 넘나들 수 있으며 수취에 대한 최종 결정은 최종 사용자에게 남겨둔다는 원칙이다. 그러나 기술적 솔루션이 명확하게 작동하기 때문에, 즉 어떤 이미지 또는 특정 단어, 혹은 단어들의 조합에 필터를 적용할지 혹은 원하지 않고 개인의 이익에 반한다고 생각되는 모든 것을 걸러낼지에 대한 작동이 명확하기 때문에, 스팸 필터에 대한 반대는 별로 없을 것이다. 더 실질적인 관심은 범죄를 덫으로 잡아내기 위한 소프트웨어 기술, 예컨대 'honeypots(꿀단지)' 및 'honeynets(꿀 그물)'와 같은 것에 놓여 있다. 그러한 기술들이 자신의 역할을 성공적으로 수행할 수 있는 반면, 그것들은 또한 일련의 도덕적, 윤리적 및 법적 문제를 창출한다. 특히 법원에 제출되는 증거의 유효성 및 증거력과 관련하여 그리고 함정수사에 대한 주장과 관련하여, 즉, 이러한 형태의 경찰활동이 실제로 범죄자를 잡기 위한 것인지, 아니면 모든 것을 들여다보는 '기율'을 기술적으로 행사함으로써, 그리고 행위에 대한 '위축효과'를 통해, 단순히 범죄를 단념시킨 것인지가 문제되는 것이다. 어느 쪽이든 간에, 이것은 논의가 필요한 문제이고, 필요하면 국제적인 법적 규율에 의해 규제되고 조화되어야 하는 문제이다.

[결론: 사이버범죄에 있어 새로운 것은 무엇인가?]

몇몇 종류의 사이버범죄는 단지 컴퓨터를 사용하여 예전의 범죄를 저지른 것이기 때문에 우리에게 친숙하다. 그러나 전혀 새로운 것도 있다. 하지만 그 모든 유형들은 기술의 매개 정도를 기준으로 하여 이해될 수 있고, 그러한 서로 다른 유형들은 전통적인 형사사법 절차에 있어서도 다르게 취급되어야 한다. 최신의 사이버범죄들을 이해하기 위해서는 상당한 학습을 필요로 한다. 이미 말한 바이지만, 최근 범죄 행동에 대한 네트워크 기술의 영향에 대한 기초지식 및 경험 수준의 일반적 증가는, 사이버범죄를 다루기 위한 더 효과적이고 승인 가능한 방법들을 가능하게 하고 있다. 국내 및 국제적 경찰 조직들은 그 분야에서의 경험을 축적하고 있고, 경찰/보안과 관련된 사

적 부문에 있어서도 이는 마찬가지이다. 또한 법률들은, 여러 국가의 법적 절차에 상응하여 다양한 방법으로, 그리고 국내 및 국제적 사이버범죄 논쟁에 의해 제기된 지역적, 공공적 및 정치적 관심에 대응하여, 계속 개정되고 서로 조화를 이루어 가고 있다.

사이버범죄는 바로 지금 여기에 존재하고 있으며 미래에도 계속 진화할 것이다. 지금 그러하듯이 미래에도 더 큰 어려움을 만들어 낼 것이다. 예컨대 아직 알려지지 않은 범죄(아마도 복잡한 사기나 속임수일 가능성이 크다)를 어떻게 다룰지에 대한 문제는 영원히 계속될 문제인 것이다. 이러한 범죄들은 새로운 유형의 주변 기술 및 클라우드 컴퓨팅 전략으로 가능하게 될 것이다. 이러한 기술들은 결국 우리의 가정, 직업 및 실제적 환경의 모든 측면을 통제할 수 있는 것들이다. 그러나 앞서 강조한 바와 같이, 우리는 사이버범죄에 대처함에 있어 기술적 부족이 발생하지 않도록 매우 주의해야 한다. 그렇다. 기술적 솔루션은 모든 범죄를 예방하거나 해결할 수 있다. 그것이 아무리 사소한 범죄일지라도 말이다. 그러나 그것에 아무런 구속이 없으면, 법이 과학 규칙으로 전락함으로써 우리는 사실상 입증책임이 전환되는 엄격한 책임의 세계로 끌려갈 뿐만 아니라, 종종 부당하게 많은 사람들이 범죄자가 되어버리는 세계에 이를 수도 있다. 결국 우리는 경고가 필요한 사람과, 도움이 필요한 사람 그리고 감옥이 필요한 사람을 구별해야 하며, 형벌이 범죄에 따라 상응하게 되도록 해야 한다. 따라서 질서를 유지할 필요와 법 집행의 필요를 모두 존중하는 섬세한 균형이 이루어져야 하며, 또한 법의 의도와, 범죄자를 잡는 법 집행자의 욕망을 제어하는 절차적인 보호가 균형을 이루어야 한다.

이 글은 Wall, D.S. (2007) 사이버범죄: 정보화 시대에 있어 범죄의 변형, 캠브리지: Polity에서 제기된 논의를 기초로 한 것이다.

Ubiquitous Crime in the Information Age: Understanding and regulating Cybercrimes

David S. Wall, Ph.D., Professor of Criminal Justice and the Information Society, Centre for Criminal Justice Studies, School of Law, University of Leeds, UK.
<d.s.wall@leeds.ac.uk>

Paper to be delivered at the *International Cybercrime Seminar*, Korean Institute of Criminology and The Korean Association of Criminology, Yonsei University, Seoul, Korea, 1st November.

Abstract

Cybercrimes are different to more conventional crimes because of their mediation by networked computer technology. The mark of a true cybercrime is that it disappears once networked technology is removed from the equation. Cybercrimes have evolved generationally alongside advances in technology and are constituted by three main areas of criminal behaviour – crimes against system integrity, using computers to commit crimes and crimes relating to the computer content. Their informational, globalized and networked characteristics pose many challenges for investigative and criminal justice processes, not least their ubiquity. But the same technologies that create cybercrimes can also be used to regulate them, which gives us a useful enforcement tool. However, it is a tool that can also infringe core values when used bluntly, and the need to balance personal security with privacy needs creates new legal and political challenges.

The list of new terms for crimes spawned by the internet expands each year as new digital environments are established and then exploited by criminals. Identity thefts (phishing), cyber-terrorism, information warfare, spams, denial of service attacks, hacking, cracking, hacktivism, e-frauds, auction fraud, click fraud, scams, hate crime, cyber-bullying, illegal online gambling, extreme pornography, viruses worms and Trojans, hackers and crackers are some of the new terms that are now called 'cybercrime'. The

term ‘cybercrime’ originally evolved from 1980s cyberpunk fiction which linked together the concepts of cyberspace and crime and, while there are many who would still argue that ‘cybercrime’ is just ‘computer’ or ‘electronic’ crime by another name, the term has now entered the common language and has to be made sense of if it is to be of use as an analytical concept that informs policy formation.

Differing views on the nature of cybercrime

A quick tour of news reports and literature reveals a range of divergent views on cybercrime. *The computer security experts*, for example, tell us about potential and actual risks to society and suggest a range of strategic and tactical solutions - often their own products and services. The *legal/ administrative* community, on the other hand, define what is, and what is not, supposed to happen by establishing and clarifying the rules that identify boundaries of acceptable and unacceptable behaviour. The *criminological and general academic* community endeavour to provide an informed analysis about what has happened and why. These different takes on the same subject mix with science fiction media presentations of cybercrime to feed into the *popular or lay* view, which reflects what the person on the street thinks is happening.

So, concerns about cybercrime are expressed through a range of voices that do not articulate a common understanding. In fact, just about any offence that involves a computer seems to be regarded as a ‘cybercrime’ and there is also a broad tendency to confuse crimes that use the Internet with those created by the Internet. None of this is helped by confusing media reports of high cybercrime threat levels – for example, Symantec’s April 2008 threat report estimates up to half a million cybercrimes per year – contrasted with the low levels of prosecutions, for example, the 150 or so successful prosecutions in the UK since the introduction of the Computer Misuse Act 1990. This trend is also found in other jurisdictions.

Generations of cybercrime

Cybercrimes have evolved alongside the networked technologies that create cyberspace

and bear the hallmarks of cyberspace in that they are informational, networked and globalized. Therefore, if cybercrimes are understood to be harmful behaviours that have been mediated or shaped by networked technology, then they can be typologized for analytical purposes by the level of their level of mediation by those technologies. By applying a 'transformation test' – simply thinking about what happens if the Internet is removed from the activity, three generational levels of cybercrime can be identified that each display different combinations of informational, networked and global mediation by technology.

At the first level, cybercrimes are *traditional* or *ordinary crimes* that use computers. Initially they were crimes that took place within discrete (usually mainframe) computing systems – today they might also include those crimes that involve the use of computers as a method of communication or to gather precursor information to assist in the commission or organisation of a crime (see later). The point is that, although they can be quite serious in their impact, they are nevertheless low end cybercrimes because the behaviour will persist if the Internet is removed from them. Offenders will simply revert to other forms of dishonesty or using other forms of available communication or information sources.

At the second level are the *hybrid cybercrimes,* 'traditional' or legislated crimes for which network technology has created entirely new global opportunities. They are distinguished from the first level by the fact that they are committed across networks (e.g., auction frauds). Take away the Internet and the behaviour will continue by other means, but not on such a global scale or across such a wide span of jurisdictions and cultures.

At the third level are the *true cybercrimes.* Solely the product of the Internet, they are high-end cybercrimes that vanish if you take away the Internet. They include 'spamming', 'phishing' (id theft) and 'pharming' (hijacking browsers) and variations of online intellectual property piracy.

Because the first and second levels tend already to be the subject of existing laws and existing law enforcement experience (though its allocation within the system may not be

as desired), any legal problems arising therefore tend to relate more to legal procedures than substantive law. However, as the third level of true cybercrime develops, then they will be of their own kind (*sui generis*) often requiring new legislation, as has been the case with spamming in the EU, US and elsewhere.

Types of cybercrime

In addition to generational levels of cybercrime are the different types of substantive criminal behaviours that fall under the cybercrime rubric. This behaviour falls into three basic categories that can also be linked to existing bodies of law and associated professional experience.

Computer integrity crimes such as hacking and cracking, cyber-vandalism, spying, DDOS (distributed denial of service) attacks, viruses etc., each assault the integrity of computer network access mechanisms. Computer integrity crimes often pave the way for more serious forms of offending (see 'phishing' below).

Crackers, for example, may use Trojans or viruses to install 'back doors' that are later used (as botnets) to facilitate other crimes, possibly by spammers who have bought lists of the infected addresses. Most jurisdictions now have legislation, such as the (UK) Computer Misuse Act 1990 or the (US) Computer Fraud and Abuse Act 1986 (18 U.S.C. 1030) - to name two. They are internationally harmonized by the Council of Europe's Convention on Cybercrime (ETS No. 185) to protect computer users against unauthorised access to computer material; unauthorised access with intent to commit further offences; and unauthorized modification of computer material. Although there has been some debate about the effectiveness of the computer misuse legislation, it does provide an important starting point for legal and other preventative action. It is similarly the case with the cybercrime convention which has to date been signed and ratified by about half of the 54 contributing states.

Computer assisted (or related) crimes, such as 'phishing' (identity theft), advanced fee frauds etc, use networked computer systems (often legitimately) to engage with victims with the intention of dishonestly acquiring cash, goods or services. Most jurisdictions

have theft and fraud legislation and legal procedures for the recovery of lost assets, along with intellectual property laws to protect citizens against the illicit acquisition of the expression of ideas.

Computer content crimes relate to the illegal content of networked computer systems and include the trade and distribution of pornographic, hate crime materials or materials that intend to deceive. Most jurisdictions have variants of obscenity laws and laws which prohibit incitement through hatred, although their legislative strength can vary where Internet content is also protected by legislation that guarantees freedoms of speech and expression.

The distinctions made here between the level of technological mediation and type of criminal behaviour provide important analytical reference points for policy formation. When they are cross-tabulated against each other the resulting mental map or 'matrix' usefully demonstrates the differences between the different types of cybercrime which can be used, for example for organisational purposes, say, in the allocation of financial or human resources.

The Crime Matrix	*Computer Integrity Crimes*	*Computer Assisted Crimes*	*Computer Content Crimes*
Level 1: Ordinary crimes	Hacking within systems	Fraud within systems	Storing extreme pornography
Level 2: Hybrid cybercrimes	Hacking across systems	Fraud across systems	Distributing e. pornography / hate crime/
Level 3: True cybercrimes	Phishing/ DDOSA/ Spammed Viruses/ Drive by downloads	Micro frauds (Long tail crime)	Networked content delivery of e. pornography / hate crime

The organisation of crime online

A knock-on effect of the evolutional development of cybercrimes has been a change in their organisation, especially with regard to the second and third generational levels that are characterised by the increasing automation of crime online. The advent of the personal computer changed radically placed control of a whole criminal process in the hands of one or two specialist individuals, as with, for example, the once feared act of ‘hacking’. More recently, however, with ‘plug and play’ and ‘cloud’ computing systems there has been a dramatic reduction in the need for specialist knowledge of operating

systems. This, when combined with the increased potential for criminal gain online, has meant that stealth and the desire to maximise returns (the criminal business ethics) have displaced the ethical chic and technological bravado of the ethical hacker.

This potent combination has also demanded new forms of criminal organisation that are flat and nonhierarchical. Offenders now coldly (professionally and contractually) employ spammers, who employ virus writers to write sophisticated software to do the spamming and hacking for them – as, for example, with identity theft as a precursor to fraud. The malicious software they produce is automating the process of small-impact victimisation on a massive scale. The latest generation of cybercrime is a new world of asymmetrical victimization in which a handful of offenders can commit a disproportionate amount of crime. After all, with such high returns on investment and such low risk to yourself, why commit a high-risk $50 million robbery when the technology enables you alone to scam 50 million people for $1 each!

Cybercrimes and the criminal justice processes

Despite the existence of applicable bodies of national and international law, the unique characteristics of cybercrimes conspire to impede the traditional investigative process. These informational, networked and globalized low-impact multiple victimisations tend to be individually minor, but serious in their aggregate. This quality creates *de minimis* problems for localised law enforcement and criminal justice systems not geared towards responding to such offences – the individual impacts of the offending are perceived to be too minor to warrant investigation. Furthermore, the actual, rather than perceived, dangers posed by cybercrime are not always immediately evident to potential or actual victims. Either they are not individually regarded as serious, or they are genuinely not serious. Yet, they possess a latent danger in their global aggregation or in being precursors to more serious crimes and each of the substantive criminal behaviours highlighted earlier illustrate this latency. Computer integrity cybercrimes, for example, often open the door for other forms of more serious offending - identity theft from computers only becomes serious when the information is used against the owner. Similarly, robot networks (or botnets) of 'zombie' computers that have been infected by remote administration trojan may be used to facilitate other crimes. Computer assisted cybercrimes, such as Internet

scams perpetrated by fraudsters in collusion with spammers, tend (as stated earlier) to be relatively minor in individual outcome, but serious by nature of their aggregate volume. Computer content crimes, although primarily informational and not always illegal, may nevertheless deceive or be extremely offensive or may even contribute to the incitement of violence or prejudicial actions against others.

A further problem for criminal justice agencies are the local, national and international political demands placed upon them to respond to cybercrime, especially the public police, who are traditionally expected to protect society from criminals. Such demands are regularly inflamed by the apparent disparity between the 'cybercrime' waves portrayed by the news media (and cyber-security sector) with the relatively few arrests and prosecutions of so-called cybercriminals. One explanation for this disparity is the fact that local police forces in most jurisdictions tend to work within tightly prescribed budgetary parameters defined by their routine activities and therefore find it difficult to cope with demands to investigate the crimes arising from globalised electronic networks. However, whilst carrying some weight, such explanations do tend to ignore the (often) substantial efforts made by policing agencies to develop capacities to combat cybercrime. A more likely explanation is that the disparity Is caused by a shortfall between expectations and actuality because the public police only play a very small part in the overall policing of cyberspace. Although we are now in the twenty first century, the UK public police and those in other jurisdictions still continue to work on principles laid down over a century or more ago. Hence, the understandable focus of resources on dangerous people such as paedophiles, child pornographers, fraudsters, those who threaten the infrastructure such as terrorists, and the more serious hackers. However, this critique is not to say that cyberspace goes unpoliced, nor is it the case that the police activity is inefficient or ineffective. Rather the public police role has to be understood within the broader and largely informal networked and nodal architecture of Internet policing comprised of: Internet users and user groups; Moderators and gatekeepers of digital environments; Network infrastructure providers; Corporate security organisations; Non-governmental, non-police organisations; Governmental non-police organisations; Public police organisations.

Each of these groups uses different combinations of moral, contractual (economic),

technological or legal, sanctions to maintain order online, which raises important questions about whether public interests are being protected by those charged with protecting the private commercial interests. Joining up these networks is a range of initiatives designed to make their governance function more effective. They include: international coalitions of organisations; multi-agency, cross-sectoral partnerships and coalitions and also international coordination policies. A challenge for the future is to enable the police to work effectively with the private sector and also temper the almost universal unreflective drift towards the routine use of software technology to strengthen security.

Policing cybercrimes

Software technology is far more potent than law as a regulator of digital, and for that matter physical, environments, because it not only controls their architecture, but it can also shape any behaviour that takes place within them. When applied to cybercrimes, this 'digital' realism means that the more a criminal behaviour is mediated by a new technology, then the more it can be policed by that same technology.

However, since technological interventions raise a range of new ethical and legal issues – for example, are they legal or ethical – then any successful interventions will have to be set within acceptable legal, social, economic and technological frameworks. Unless checked, the ubiquitous technological policing that arises could erode the democratic values that currently bind many liberal societies. Yet, more optimistically, if the use of technology to control cybercrimes were to be contained within a supportive socio-legal context, then those same technologies could assist with the policing process. Furthermore, the same surveillance characteristics that make network technology a powerful policing tool could also assist the process of police reform because they could be used to oversee police and regulatory practice as well as for creating broader organisational and public accountability.

Of considerable current concern is that while the actions of public police officers are in principle already framed by national legislation and are also subject of various local codes of policing practice, many of the other partners (listed earlier) who also police the

Internet, are not - other than within the broader confines of national laws. Furthermore, the lack of checks and balances on the noticeable drift towards using of software solutions to police cybercrime (largely been driven by the influence of the cyber-security industry) is rather worrying. Spam filters are a good example of a successful technological solution to a cybercrime problem, but whilst no one wants spam there has to-date been little critical discussion about the application of spam filters into the delivery mechanisms. Consequently, there have been a number of adverse side effects. Not only can Spam filters restrict some legitimate communications (e.g., legitimate emails from, say, China, Korea, Japan), but they also can contravene the longstanding (though changing) end-to-end principle of the Internet which is freedom of movement across the network to its nodes while leaving choice and mode of receipt to the end users. There is understandably little objection to spam filters, but since technological solutions clearly work, then what is to stop the application of filtering software to images or to certain words or combinations of words and filter out everything that is deemed undesirable and against private interests. Of more practical concern are the software techniques designed to entrap criminals, such as 'honeypots' and 'honeynets'. While they may be successful in their mission, they do generate a range of moral, ethical and legal concerns. Not least in terms of the validity and strength of the evidence presented to the court and allegations of entrapment – that is if this form of policing is in fact designed to capture offenders or simply to deter offending through the technological imposition of panoptic 'discipline' and its 'chilling effect' on behaviour. Either way, it is something that should be debated and then, where necessary, regulated and harmonized by international legal rules.

Conclusions: what is new about cybercrime?

Whilst some types of cybercrimes are familiar to us because they are simply old crimes that use computers, others are entirely new. But all can be understood in terms of their level of mediation by technology as types of crime that are set apart from the traditional diet of the criminal justice processes. Keeping up-to-date with developments in cybercrimes will require all involved to undertake a steep learning curve. Having said this, in recent years a general increase in levels of base knowledge and experience about

the impact of networked technologies on criminal behaviour is now allowing for more effective and acceptable ways of dealing with cybercrimes. National and international policing organisations are amassing a corpus of experience in the field, as are sections of the private sector with a policing/ security interest. Plus, laws are continually being revised and harmonised and in many different ways according to different jurisdictional legislative procedures and in response to local public and political concerns raised by national and international cybercrime debates.

Cybercrime is here to stay and it will continue to evolve in the future. As it does so it will generate even more challenges. On the horizon, for example, is the question of how we deal with the as yet unknown criminal opportunities (most likely complex frauds and deceptions) that will be created by new types of ambient technologies and cloud computing strategies. These are technologies that could eventually control most aspects of our domestic, occupational and physical environments. However, as emphasised earlier, we have to be very careful not to make technological short cuts in the process of policing cybercrime. Yes, technological solutions can prevent or solve all crimes, no matter how small and petty. But unfettered the process of reducing law to scientific rules not only draws us further into a world of *de facto* strict liability to reverse the burden of proof, but it could also end up criminalising, often unfairly, large sections of the population. At the end of the day we need to make sure that the punishments fit the crimes so that we can discern between those who need a warning, those who need help, and those who need incarceration. So a delicate balance has to drawn which respects the need to maintain order and the enforce laws, whilst also balancing the desires of law and the procedural protections it affords with the desires of law enforcement to catch offenders.

This paper is based upon arguments raised in Wall, D.S. (2007) *Cybercrime: The transformation of crime in the information age*, Cambridge: Polity.

[11:10 – 12:20]

사이버 문화와 범죄의 사회적 충돌

제2주제 : 사이버 공간에서의 사회적 엔지니어링과 범죄방지

발표 : Roderic Broadhurst (호주 그리피스대 교수)
Nicholas Chantler (호주 퀸즈랜드 공과대 교수)

토론 : Rajiv Narayan (연세대 교수)
최 진 혁 (NHN 법무그룹)

사이버 공간에서의 사회적 엔지니어링과 범죄방지

Dr. A. N Chantler*
Professor R.G. Broadhurst**

[초록]

본 논문은 현재 사이버 커뮤니티에서 흔한 구문적(syntactic) 그리고 의미적(semantic) 사회적 엔지니어링 공격 방법을 다루고 있다. 또한 새로운 추세와 사회적 엔지니어링에 대하여 사이버 범죄가 자행되는 추후 예상 방향에 대해서도 논의한다. 온라인 환경에서 사기의 위험은 점차 늘어나고 있으며, 인터넷 접속자의 급증으로, 많은 사람들이 속임수에 노출되기 쉽다. 온라인 사기나 사회적 엔지니어링 형태의 법적 대응은 분산되어 있고 적절하지 않아서 조직화된 범죄 활동의 증가 가능성을 파악하지 못하고 있다.[1)]

[서론]

유럽회의(Council of Europe) 벤치마크인 *사이버범죄조약(Cybercrime Convention)*을 사용하여 14개 아시아 태평양 국가[2)]의 사이버 보안법을 검토한 마이크로소프트 (2007)[3)]는 각기 범위가 다른 법률적 대응을 지적하였다. 특히 이 검토는 완화적 가치관[4)]을 따르는 4개국(호주, 홍콩, 일본, 뉴질랜드)에만 기초한 OECD 지침에 따라 개인정보보호법률(privacy laws)의 낮은 준수를 지적하고 있다. 스팸방지법(Anti spam laws)은 더욱 완화적인 '옵트-아웃(opt-out)' 스팸방지제도 벤치마크를 따르는 한 지역(홍콩)에서 악화되고

* 호주, 브리즈번, 퀸즈랜드 공과대학, 법대 교수
** ANU, 그리피스 대학 아시아 태평양 연구 분과, 윤리, 법률, 법률 및 정부 키 센터

1) 2007년 1월 호주 범죄학회의 기술 보고서인, '미래의 하이테크 범죄(Futures of High Tech Crime)'에서 작성한 원본 초안
2) 호주, 홍콩, 뉴질랜드, 인도, 대만, 중국, 일본, 베트남, 말레이시아, 한국, 필리핀, 인도네시아, 태국, 싱가포르.
3) 보고서 사본을 제공해준 마이크로소프트 싱가포르 지사의 제프 불윈켈에 감사한다.
4) 그러나 마이크로소프트의 검토는 중국, 인도, 인도네시아, 말레이시아, 한국, 태국이 2005년 APEC 개인정보보호법률 프레임워크의 일환으로 데이터보호법률을 마련중이라는 점에 주목하고 있다.

있으며 네 개 국가는 현재 금지조치가 부족한 상황이다.[5] 컴퓨터나 시스템, 프로그램, 데이터 등에 인가되지 않은 접근과 같은 중요 범죄에 대해서 조차, 일부 국가(인도네시아[6])에서는 여전히 법 제정이 필요한 실정이며 민사 구제[7]를 제공하지 못하고 있다. 대대적인 대중 경고에도 한 지역(호주)만이 온라인 아동 보호에 대한 이 모형법을 충족하였으며, 6개 국가(인도, 인도네시아, 필리핀, 싱가포르, 베트남[8])는 관련 법률을 갖지 못하고 있으나, 이 보고서는 일부 지역이 법률이 계류 중이라는 사실도 주목하고 있다. *요컨대, 일반적인 사이버범죄 행위에 대한 법적 대응의 범위는 국경을 초월한 법적 허점을 악용하려는 범죄자에게도 매우 포괄적인 조치를 제공한다.* '사회적 엔지니어링'에 대한 논의의 환경에서, 사이버 범죄자에 대한 위험은 크게 위험하지는 않지만 철저한 주의를 하지 않는다면 개인 '피해자'는 더 취약할 수 있다.

아시아는 세계인구의 56%를 점유하고 있으나, 아시아 인구의 13.7%만이 인터넷을 이용하고 있다(약 5억 1천만 명). 그러나 이는 현재 세계 인구의 1/3이 인터넷을 이용하고 있으며 그에 따라 매우 중요한 시장이라는 점을 말해준다. 아시아의 연간 성장률은 약 337%로 세계 다른 지역의 266%에 비해 월등히 높은 편이다. 북미 (인구의 71%) 오세아니아/호주(57%/75%) 및 유럽(43%)은 일인당 접속 수준이 가장 높은 반면 아프리카는 인구의 4.7%만이 인터넷을 사용하고 있다.[9]

---

5) 그러나 이 보고서는 대부분 지역은 스팸방지조치를 강화하거나 법률제정 과정에 있다.
6) 그러나 전자전보와 거래에 대한 법안은 계류 중이고 정부기관에 대한 공격에 관심을 두고 있기 때문에 CoE 조약보다 완화적으로 결정되고 있다.
7) 인도의 2006년 IT(개정) 법안은 이 규약에 따라 중요 범죄로 인정되나 "부정하거나 기만적인" 행위를 법률로 금지하도록 IT법안을 개정할 목적을 가진다.
8) 이 보고서는 다음과 같이 기술하고 있다: "대부분 국가가 아동의 포르노그래피에 대한 온라인 거래에 적용하는 외설 부분에 포괄적인 법안을 마련하고 있으나, 14개 대상 국가 중 5개 국가(호주, 홍콩, 일본, 한국, 대만)만 아동 포르노그래피를 구체적으로 다루는 법안을 마련하였고 14개 대상 국가 중 3개국(호주, 홍콩, 대만)은 컴퓨터를 이용한 아동 포르노그래피 범죄를 포함하는 법안을 마련하였다.
9) 추정 온라인 인구의 30%인 12억 6200만명(2007년 11월 기준)이 영어를 사용하며, 그 뒤로 중국어(15%), 스페인어(9%), 일본어(7%), 독일어(5%), 불어(5%), 한국어와 이탈리아어(약 2.6%), 포르투

사이버 범죄 피해에 대한 관심은 2004년 미국 국가 가정범죄피해조사 기관(US CVS)의 발표에 인터넷 범죄문제가 처음 포함되면서 인식되었다. 그 범위는 (가정, 학교, 직장 등에서) 컴퓨터 개인 소유나 홈 비즈니스의 사용 등으로 제한되며 금전적 손실 발생 여부나 그 사실을 경찰이나 기타 기관에 신고하였는지 등을 확인하고 있다. 시간이 흐르면서, 범죄피해조사(CVS)는 일반 사용자의 사이버 범죄 경험에 대한 중요 데이터를 제공하게 될 것이며 정책 대응[10]을 평가하는데 도움이 되는 데이터 추적을 제공할 것이다. 미국 CVS에서 고안한 이 문제들은 홍콩[11]에서도 그대로 사용하였다. 2,291명의 HK UNICVS 응답자의 결과는 58.3%가 컴퓨터에 접속하고 있으며 컴퓨터 사용자의 98%가 인터넷에 접속하고 있다고 보고하였다. 가정에서 컴퓨터를 사용하는 응답자중, 67%(891)는 적어도 과거 1년 동안 사이버범죄 형태를 경험하였으며 회사에서는 약 61% 이상이 경험하였다. 약 12%는 방화벽이나 백신 프로그램(4.7%)을 설치하지 않고 있었으며 설치여부를 모르는 사람도 있었다(7%). 기업 응답자의 8.3%는 방화벽이나 백신 프로그램이 없었으며, 5.4%는 알지 못한다고 응답했다. 가정이나 기업 응답자가 보고한 사이버 범죄의 중요 유형에는 외설 컨텐츠와 '말웨어(malware)' 등이 있었다. 약 13%의 가정 응답자는 사이버 범죄로 인해 자금 손실이 있었으며 약 26%는 1,001 홍콩 달러 이상의 손실을 봤다고 응답하였다. 기업에서 보고한 자금 손실은 14.5%로 더 높았고, 이 중 40%는 1,001 홍콩달러의 손실을, 12.5%는 10,001 홍콩달러의 손실을 보고하였다.

개정된 CVS는 신분위장절도(identity theft)의 문제에 관심을 두었으나 컴

갈어(4%), 아랍어(3.7%) 등이 많이 사용되고 있다. 세부 정보는 Thirty per cent of the estimated on line population of 1,262 million (as at November 2007) used English, followed by Chinese (15%), Spanish (9%), Japanese (7%), German (5%), French (5%), Korean, and Italian (about 2.6%), Portuguese (4%) and Arabic (3.7%) See for further details http://www.Internetworldstats.com/stats.htm, 참조. accessed April 9, 2008년 4월 9일 기준

10) 중국어 번역은 2006 2007년 중국에서 수행된 UN ICVS에서 하였다. .

11) 신분위장절도(Identity theft) 문제는 2004년 7월 US CVS에 추가되었다. 분석에는 6개월 데이터만 사용할 수 있었다.

퓨터의 오용을 구체적으로 다루지는 않았다.[12] 전체 미국 가정 사용자의 3%는 2004년 하반기 동안 최소 한 가지 이상의 신분위장절도에 피해를 당했다. 이들 피해자 중 48%는 타인의 신용카드의 무단사용을 경험하였고, 25%는 은행계좌와 같은 타 계좌의 무단 사용을 경험하였으며, 15%는 개인정보의 오용을 경험하였고, 12%는 여러 가지 유형을 동시에 경험했다고 응답했다.[13] 젊은 가구(18-24세), 도시와 교외지역 사용자 및 수입이 7만 5천 달러 이상인 사용자는 대부분 신분위장절도를 경험할 가능성이 가장 컸다. 피해는 민족이나 인종에 따라 다르지 않았다. 신분위장절도를 경험한 가구의 약 1/3은 자금분실이나 알지 못하는 청구 등으로 피해를 확인하였으며 약 1/4는 신용평가기관(Credit Bureau)을 통해 확인하였다. 이 6개월 동안 추정된 손실은 약 32억 달러에 이른다. 이들 가구의 약 2/3은 평균 1,290미화 달러를 잃어버렸으며 전체 피해가구의 1/4는 오용이 멈추지 않고 있다고 보고하고 있다.[14]

정부와 소비자는 민간 기업이 보유한 소비자정보에 대한 압력을 가하고 있다. 최소한 신원정보와 위반에 대한 고지 의무를 지키도록 하는 효과적인 절차를 마련하도록 하고 있다. 하지만 고지 의무 부분조차 보호제도가 존재하는 지역 이외에서는 보유가 가능하다는 점으로 인해 방해를 받고 있다.

[사회적 엔지니어링(Social Engineering)이란 무엇인가?]

본 논문 논의의 범위에서 '사회적 엔지니어링'은 범죄를 저지르기 위해 사이버 범죄자들이 일반 사용자의 '접속 정보'를 알아내어 심리적 속임수나 사기에 의한 행위 조작의 사용을 기술하면서 사용하는 용어이다. 사이버 범죄자들은 흔히 '해커'나 '콘맨(conmen)'이라 부르는 사람들로 복잡한 기술적 수단을 피해 컴퓨터에 접속하도록 사회적 엔지니어링을 이용한다.

---

12) 집필 당시 저자는 조사결과를 보고한 CVS의 미국 데이터를 확인할 수 없었다.
13) http://www.ojp.usdoj.gov/bjs/pub/press/it04pr.htm 4월 2일 발표 - 2006년 6월 20일 접속.
14) http://www.ojp.usdoj.gov/bjs/pub/press/it04pr 4월 2일 발표 - 2006년 6월 20일 접속.

사용자들은 조직의 컴퓨터 시스템과 같은 이들 사이버범죄자들의 이차 목표와 관련된 일차 목표가 되고 있으며 이는 다시 시스템 제어 프로그램, 데이터베이스, 금융 또는 통신시스템 등이 3차 또는 최종(중요) 목표로 이어진다. 사이버 범죄자들은 관련된 '접속 정보'를 이용하여 보안을 통과한다. 여기에는 사용자 이름과 비밀번호, 핀(개인확인번호), 토큰 및 신용카드 정보(연방통신위원회 2002) 등을 포함한다. 일단 시스템 접근을 하게 되면, 이들은 공격 요구에 따라 정보를 삭제하거나 수정 또는 복사한다(Guenther 2001).

사회적 엔지니어링은 개인의 본질적 욕구(예: 우정, 애정, 욕구 등)를 활용하여 목표 대상과 관계를 맺고 이 관계에 따라 대상을 속인다. 그리고 그 관계를 악용하여 원하는 정보를 얻는다. 사회적 엔지니어링과 관련된 이 과정은 ID 도난도 포함한다. 과거에는 주로 해커가 네트워크나 시스템 접속 중 최종 목표에 도달하도록 하는 수단을 제공했었다. 하지만 현재는 ID 절도만으로도 큰 우려를 낳고 있다(연방 거래 위원회, Smith, 2006).

정보통신기술은 계속 발전하고 있기 때문에 우리는 e커머스 활동과 개발, 특히 금융거래 보안을 위해 인터넷 사용이 증가하는 모습을 확인하고 있다. 이 개발은 암호화, 전문가 시스템, 개선된 어플리케이션 소프트웨어, 토큰, 방화벽 등의 수단을 활용하는 정보통신기술 보안의 정교함도 증가하게 된다. 문제는 컴퓨터 사용자가 더욱 기술적으로 능력이 증가하고 컴퓨터 보안 능력도 향상되고 있는 반면 사회적 엔지니어링과 관련된 보안의 중요성에 대한 인식의 증가나 학습이 이루어지지 않고 있다는데 있다. 이는 기업이나 가정환경 모두에 적용되는 것이다. 기업 신분위장절도(Fite B.K. 2006), 개인 신분 절도 및 '온라인 옥션 범죄'(AIC 2006)도 사회적 엔지니어링의 사용에 이용되고 있다.

이 신분 절도는 새로운 인구 증가가 또 다른 가치를 보유하는 형태가 되므로 미래에는 정보통신기술 보안에서 더 큰 문제가 될 수 있다. 예를 들어, "베이비붐 세대"는 현재 은퇴세대가 되고 있으며 흔히 'x' 세대나 'y' 세대로

불리는 세대와 비교할 때 다른 태도를 가지고 있다.

'베이비붐 세대' 특성은 '정부에 대한 믿음', '열악한 컴퓨터 사용 능력', '충성적이며 보수적', '신뢰' 등으로 인식되며 대부분은 '자신의 행동에 대한 결과에 대하여 직관적이다.' 한편 'x' 세대는 '기술적으로 능력이 뛰어나고', '직관적 능력이 부족', '현 상황에 대한 이전 세대 비난' 등으로 요약된다. 'y' 세대는 '기술적으로 가장 우월', '좋은 역할 모델의 부족', '자기 중심적', '타인에 대한 배려 부족', '현재를 중시'하는 것으로 요약된다. 이들의 사회적 태도를 기초로 한 가치의 인식 붕괴는 성공 가능성이 큰 유형의 사기 행위 변화의 발전으로 인해 미래의 보안에 영향을 줄 수 있다(Chantler 2006). 다시 말해서, 사이버 범죄자들은 '신뢰'와 '냉정'의 문화적 특징에서 변화에 적응할 것이다.

[해커의 동기]

효과적인 사회적 엔지니어링에 관련된 사기 행위의 인간 행동에는 다양한 동기가 존재한다:

ㅇ 기술적 회피(Technical Avoidance): 사회적 엔지니어링은 복잡하고 번거로운 기술적 경로를 깨기 위한 노력보다 손쉬운 금융이득 경로로 인식되고 있다.

ㅇ 자기 교육(Self Education): 흔하지는 않지만 단순히 '지식을 얻고' '시스템을 파괴하는' 행위의 스릴에 동기를 얻는 해커들도 있다.

ㅇ 재정 이득: 재정 이득 정보 수입에 대한 동기는 다양한 이유로 촉발되고 있다. 습관을 만들어낸다(중독). 그리고 쉽게 돈을 버는 방법으로 나타나며, 범죄를 조직화하며, 블랙메일 등과 관련된다.

ㅇ 복수: 불만을 품은 직원은 정보통신기술 프레임워크의 허점(약점)을 사용

하여 기업에 복수를 하거나 조직 내의 한 개인을 목표로 하기도 한다.

ㅇ 외부 압력: 블랙메일, 랜덤, 가족 압력, 조직범죄, 도덕적 딜레마, 극단적 믿음(지시) 등은 개인이 사이버 범죄를 저지르도록 압력을 가할 수 있다. 심리학적 측면에서, 사회적 엔지니어는 목표 대상자의 가치를 조작하여 자신이 타인에게 해를 주지 않는 것으로 믿게 하고 결국 불가능한 것을 가능하게 한다.

ㅇ 테러리스트, 정치 및 문제 동기부여 집단: 이들은 그 원인에 대하여 매우 광적이고 금융과 중요 정보 인프라의 허점을 파고들어 목표 집단을 충격에 빠뜨린다.

ㅇ 워너비(몽상가; 월터미티): 종종 자신이 남과 다르다고 생각하거나 “제임스 본드”가 되려는 사람들처럼 정신적 문제가 있는 사람들은 ‘존경하는 행동’으로 인식하거나 스파이가 되는 등 범죄행위의 동기를 얻게 되어 왜곡된 심리적 요구를 충족시킨다.

[사회적 엔지니어링 공격의 단계]

사회적 엔지니어링 공격에는 한 가지 공통된 패턴이 있다(Allan, Ant, Noakes-Fry, Kristen, Mogull, Rich 2005). Allen(2006, 5)은 ‘모든 범죄 행동은 한 가지 공통된 패턴을 가지며 이 패턴은 사회적 엔지니어링의 증거가 되고 있으며 인식 가능하고 예방이 가능하다’라고 기술하였다. Allen(2005, 5)는 이 패턴은 Cateledge(2005)가 제안한 단계와 유사한 네 가지 단계로 구성된 하나의 사이클로 인식할 수 있다고 말했다.

사회적 엔지니어링 공격에는 주로 네 가지 단계가 있다(Catledge, 2005, 8-9):

ㅇ 정보 수집: 이 단계는 사회적 엔지니어링이 목표로 하는 사람에 대한 정보나 기타 목표로 하는 개인이 필요한 정보를 누설하도록 하는 조직이나 인력에 대한 정보의 수집과 관련된다. 목표 대상에 대한 정보 수집을 위해 다양한 기법이 사용된다. 이 정보는 목표대상이나 공격의 성공에 중요하거나 영향을 가지는 타인과의 관계 수립에 사용될 수도 있다. 일반적으로 수집할 수 있는 정보는 내부 전화번호목록이나 생년월일, 조직도, 인사기록, 사회적 활동, 관계 등이다.

ㅇ 관계의 수립(개발): 목표대상과 접촉은 다음 단계에서 정보를 쉽게 수집하도록 한다. 사회적 엔지니어는 신뢰라는 심리적인 면을 사용한다. 이들은 목표 대상의 의지를 자유롭게 활용하여 이들로부터 신뢰라는 요소를 전개하며 종종 신뢰를 더 강화하도록 목표 대상자와 신뢰가 두터운 기관의 상사(연장자)를 제시하기도 한다.

ㅇ 관계의 활용(악용): 이는 사회적 엔지니어가 사용자이름, 패스워드 등의 정보를 얻거나 계정을 생성하는 등 일반적으로 가능하지 않은 행동을 수행하도록 목표 대상을 조작(활용)하는 것을 의미한다.

ㅇ 목표 달성을 위한 실행: 필요한 정보를 얻게 되면, 사회적 엔지니어는 이를 활용하여 시스템에 접근하며 나머지 단계를 완료한다.

이 사례는 단순하게 단계를 정리하고 있지만, 각각의 사회적 엔지니어 공격이 매우 다르다는 점을 인식해야 하며 많은 단계나 사이클을 사용하여, 해킹이나 패스워크 크래킹 등 전통적인 공격 방법도 포함할 수 있다는 점을 기억한다.

[사회적 엔지니어링의 심리적 유인]

Gragg(2002)는 사회적 엔지니어링이 사회적 심리적 행동(활동)이므로, 이

에 대한 방어시스템 개발을 고려하기에 앞서 사회적 엔지니어링의 이면에 있는 심리를 이해하는 일이 중요하다고 제시하고 있다.

이를 위해서는 사회적 엔지니어링 공격 중에 수반되는 심리적 '유인'을 인식해야 한다. 이 '유인'은 이들이 다른 행동을 하는데 영향을 주고 설득하며 전환시키는 힘의 형태를 보여주는 심리적 원리이다. 사회적 엔지니어링 이면에 있는 이런 심리적 유인을 이해함으로써 위협에 대처하거나 보안을 강화하는데 사용하는 다양한 측면도 이해할 수 있게 된다. Gragg(2002)는 특히 다음과 같은 유인에 대하여 말하고 있다.

ㅇ 강한 영향(Strong Affect) - 이는 해커가 합당하지 않은 형태로 소유하고자 하는 강조되는 정서적 상태를 사용하는 유인이다. 만일 피해자가 놀람이나 예상 또는 분노의 감정을 가지게 되면, 피해자는 현재 나타난 사실에 대한 생각을 제대로 하지 못하게 된다. 강한 영향(Strong affect)은 사회적 엔지니어가 강한 감정을 유인하도록 하는 상호작용의 초기에 언급을 하게 될 때 발생한다. 여기에는 기본적으로 두려움, 흥분 또는 혼란 등을 포함한다. 이는 수십만 달러 상당의 부상이나 직원의 직무가 한 사람의 의견에 좌우되는 혼란 등이 전제가 될 수도 있다. 그리고 이처럼 강한 감정이 격앙되면서 더 큰 혼란이 작용하고 분명한 사실에 대하여 평가하거나 논리적으로 사고하거나 반대적 주장을 펼치는 능력을 방해하게 된다(Rusch, 1999 p.4). 반 사실적(counter-factual) 사고는 강한 영향을 만들어내는 것과 직접 관련된 현상이다. Landman 등은(2000 p.299) 반 사실적 사고는 한 개인의 합리적인 사고과정을 중단시키는 예상과 스릴의 가능성에 의지한다고 설명한다. 일반적인 사례로는 '믿기지 않는 상(보상)의 수상자 중 한 명으로 선정되는 것이 있다. 그 사람은 수상 가능성이 실제로는 가능하지 않지만 자기만의 생각을 통해 혼란을 겪게 되어 상(부상) 가능성을 이해 정보나 접속 세부내용을 폭로

하는 위험을 감수하게 된다. 이는 그 사람이 주문에 걸린 상태와 같거나 현실과 다른 감각을 지니게 되어 다른 감정이 몰려오면서 놀람과 흥분으로 발생하게 된다.

ㅇ 오버로딩(Overloading) - 이는 자신이 빠르게 듣고 가능하지 않은 잘못된 약속을 제시하면서 이루어지는 상태이다. 이는 진부한 이치를 확신하는 상태로 제시되기 때문일 수 있다. 이를 오버로딩의 심리적 유인이라고 한다. 상당한 정보를 빠르게 다루게 되면 논리적 기능에 영향을 주게 되고 '감각적 과부하(sensory overload)를 겪게 된다. 너무 많은 정보를 처리하면서 사람들은 '정신적으로 수동적인 상태가 된다' - 즉 정보를 평가하기 보다는 흡수하는 상태가 된다(Burtner, 1991 p. 2). 예상치 못한 견해로부터 주장내용은 오버로딩을 유인할 수 있다. 목표대상은 새로운 견해에 대한 처리 시간을 필요로 하지만 시간은 충분하지 않다. 이는 목표대상자들에게 과도한 정보를 떠넘기게 되며 사고를 할 수 있는 시간도 충분하지 않게 하여 이들이 그 내용을 처리하거나 면밀하게 살펴보는 능력을 축소시킨다. 이들은 자신들이 처리해야 할 내용을 그대로 받아들이는 경향이 생기게 된다(Petty, et al. 2001 p.2).

ㅇ 보답(Reciprocation) - 이는 원하는 행동을 유인하는데 사용하는 심리적 유인이다. 사회적 상호작용에서 누군가가 우리에게 무엇을 제공하거나 약속하게 되면, 호의로 보답하려 한다는 전제를 가지고 있다. 그리고 이는 최초에 선물을 요구 받지 않았거나 요구 받은 선물이 최초에 받은 것보다 더 가치 있는 것으로 돌려주게 되는 경우와도 관련이 있다. 이를 보답이라고 한다(Rusch, 1999 p.6).

해커인, Kevin Mitnick는 "기업 환경에서, 사람들은 요청에 대하여 철저하게 평가하지 않으려 하므로 정신적으로 손쉬운 방법을 선택하게 된다"고 말

한다. 그에 대한 근거로는 만일 누군가가 호출하여 한 문제를 돕고 있다면, 그 사람은 '우리 중 한 명'이라는 생각을 하게 되고 위협에 대한 생각을 갖지 않게 된다(Farber, 2002 p.1). 이는 '역' 사회적 엔지니어링으로 보답 유인을 사용하도록 한다. 해커는 준비된 도움 제공자가 되어 목표 대상자의 문제를 해결할 능력을 갖추고 있다. 문제를 해결하기 이전에도, 대상자는 해커에게 빚을 진 느낌을 가지게 된다. 이는 해커의 이상적인 상황이기도 하다(Nelson, 2001 p.3).

사회적 엔지니어링에서 보상이 사용되는 또 다른 방법은 행동적 실험을 통해서도 입증된다. 이 실험은 두 사람이 합의하지 못하는 상황에서, 한 명이 일부 양보를 하게 되면, 아무리 사소한 일일지라도 상대방도 양보를 해야 할 것 같은 느낌을 받게 된다는 것이다. 해커에게 이는 매우 쉬운 일이다. 그는 하나 이상의 요청을 하고 세 개 중 한 개를 양보하게 되며 목표 대상은 나머지에 대해서 양보해야 하는 상황에 처하게 된다(Cialdini, et al 1992 p.38). 보답은 종종 목격되며 많은 기업 문화에서 장려되기도 한다. 이는 묵언의 '바터링 시스템(bartering system)'으로 누군가 성공을 원할 때 중요한 것으로 여겨진다. 한 직원은 누군가의 기대를 위해 돕게 되며 결국 호의를 돌려받게 될 것이다.

사기적 관계(Deceptive Relationship) - 이는 타인을 활용하도록 만들어진다. 이를 이행하는 한 가지 방법은 한 명의 공적에 대하여 정보나 간략한 설명 또는 인식을 공유하거나 논의하는 것으로(Farber, 2002, p.1) 상이한 상황에서 의심스러운 사람이 되는 한 직원을 속이는 상황을 기술한다. 이 때 Mitnick는 의사소통 수단으로서 이메일을 통해 직원들과 연락을 통해 관계를 수립하였고 보답을 요구하지 않은 상태에서 어떤 정보나 기술을 공유하게 되었다. 또한 이메일을 쓰지 못하게 한 "Kevin Mitnick"에 대한 험담을 주고받으며 관계를 강화한다. 관계가 수립된 후, Kevin은 목표대상의 시스템에 대

한 모든 종류의 정보를 얻을 수 있었다. 이처럼 빠른 관계를 수립하는 또 다른 방법은 자신과 매우 유사한 사람인척 하는 것이다. 이 개념은 피해자가 그 상대방을 자신과 같도록 느끼게 하고 요청자가 동일하게 생각하도록 하며 동일한 흥미와 동일한 인생의 목표를 원하는 것으로 느끼게 한다. 누군가 자신과 동일하거나 유사한 성격을 가진 것으로 믿게 되면 합법적인 기준을 따르지 않고 그 사람을 신뢰하는 범위에서 호의적으로 인센티브를 주게 된다 - 이는 상냥하거나 긍정적 행동의 증거 등이 있다(Rusch, 1999, p.6).

책임의 혼란(Diffusion of Responsibility) - 책임의 혼란은 목표대상이 어떤 행동에 대하여 자신만이 책임이 있는 것은 아니라고 생각할 때이다. 아이러니하게도 이 유인은 설득의 동기로서 도덕적 책임(moral duty)을 쉽게 사용할 수 있도록 한다. 도덕적 책임은 목표 대상자가 공동업무수행자로서 업무를 수행하는 느낌을 받게 될 때 생기며 그로 인해 조직을 돕고 죄의식은 갖지 않게 된다(Nelson, 2001 p.4). 대상자는 자신들이 기업 또는 요청한 '다른 직원'의 성공을 위해 중요한 영향을 가지는 결정을 하고 있다는 생각을 하게 되어 자신의 결정에 따라 직업을 잃을 수도 있다는 의미도 전달하게 된다. 이는 사람들이 결정하기에는 매우 어려운 문제일 수 있으며 목표 대상자는 발생한 결과에 대하여 책임이 없다고 믿게 될 때 더 쉽게 이를 따르게 된다.

권한(Authority) - 대부분의 사람들은 권위에 복종하도록 되어 있다. Rusch(1999, p.6)는 권한을 가진 것으로 생각하는 사람을 위해 일을 하게 된다고 말하였다. 가짜 CEO가 준비되지 않은 직원에게 미치는 영향을 생각해 보자. 이 유인은 요청자가 권위의 정당성을 가지고 있는지에 대해 확인해주도록 하는 것 자체가 위험이 될 수 있다는 사실 때문에 매우 강력한 영향을 가진다. 이와 같은 두려움은 이 유인이 권위를 가진 사람에게 스스로를 부각시키려는 보통 사람들을 활용하는데 동원되기 쉽다.

완전성과 일치성(Integrity and Consistency) - 사람들은 자신이 하는 일이 애초부터 무의미할 수 있다 하더라도 직장에서 업무를 수행하려는 경향을 가진다. 일부는 완전성의 문제를 비록 요청이 '매우 합당한' 것이 아닐 지라도 '자신이 하기로 한 일을 하는 것'의 문제로 볼 수 있다. 종종 이런 경향은 직원들이 그런 요청이 실제 자신의 동료 직원이 한 것이라고 믿게 하는 방법을 통해 정당화시키게 되면 수행하게 된다. '완전성과 일치성'의 유인이 가진 또 다른 특성은 발언을 할 때 다른 사람들이 진실한 느낌을 말한다고 믿는 경향이 있다는 점이다. 이에 상반되는 증거가 없다면, 사람들은 자신이 말하고 있는 상대방이 자신이 느끼거나 필요로 하는 진실을 말하고 있는 것으로 믿게 된다. 타인을 믿는 경향은 주로 감정을 표현하는 진실성을 기초로 한다(Rusch, 1999, p.7).

[공통 특성]

어떤 동기나 기법이 사용되더라도, 목표대상이 요청을 받아들이도록 하는 공통된 특성이 있다. Allen (2005)은 이런 특성을 다음과 같이 요약하고 있다.

- 목표 대상으로부터 책임을 풀어주어 특정 행동에 대하여 자신의 단독적인 책임이 아니도록 여기게 한다.
- 요청을 들어줌으로써 목표대상이 흔히 "상사와 함께 하고 있다"는 느낌으로 미래의 보상을 받게 될 사람의 '편'에 있다는 인식을 갖게 한다.
- 목표대상이 타인을 돕는다는 도덕적 행위에 대한 본능으로 죄의식을 갖지 않도록 한다.
- 어떠한 압력을 받지 않고 요청에 대하여 목표대상이 자발적으로 하게 하는 개인적 의사소통.

○ 목표대상은 최소한의 시간과 노력만으로 타당한 의사결정을 하고 있다고 믿는다.

목표대상의 준수 가능성은 다음의 경우에 증가한다.

○ 침입자(침략자)가 공격적 방법 대신 친화적 방법을 사용하여 갈등을 회피할 수 있는 경우 - 호감 대 괴롭힘.

○ 침입자(침략자)가 사전 거래를 통해 관계를 맺을 수 있는 경우. 목표대상은 이전에 더 작은 일에서 수행한 경험이 있어서 더 큰 요청에도 기꺼이 돕게 된다.

○ 침입자(침략자)가 시각과 청각 등 목표대상의 감각(감정)에 호소할 수 있는 경우. 이러한 감정에 호소하게 되면, 목소리나 이메일 보다 더 인간적으로 보이게 됨으로써 더 가까운 관계를 수립할 수 있다.

○ 침입자(침략자)가 두뇌회전이 빠르고 협상력이 있는 경우.

[사회적 엔지니어링 방법]

사회적 엔지니어링은 두 가지 유형으로 분류된다. 구문적(Syntactic)과 의미적, 그리고 아래와 같이 그 차이점을 요약할 수 있다.

구문적(SYNTACTIC) 사회적 엔지니어링

구문적 사회적 엔지니어링은 네트워크 공격의 '세컨드 웨이브(second wave)'라고도 부른다. 이는 네트워크 운영 논리나 소프트웨어의 루프홀(loop-holes), 서비스 거절, 암호화 알고리즘의 어려움 등과 관련되기 때문이다 (Schneier, 2001). 구문적 사회적 엔지니어링 공격은 내재적인 보안 실패로

인해 발생할 수 있다(Barrett, 1997, 43). 두 가지 잘 알려진 구문적 공격은 말웨어와 스머핑이 있다.

말웨어(Malware) - 바이러스를 유포할 목적을 가진 악성 소프트웨어 코드(악성 코드는 다른 사용자가 첨부파일이나 프로그램의 사용 시에 컴퓨터에 다운로드 된다)나 웜(컴퓨터에 감염되면 스스로 복제하여 다른 시스템으로 옮기는 악성 코드), 트로이 목마(해커가 개인정보 접속을 위해 나중에 사용하도록 감염된 컴퓨터에 잠복할 목적) 등을 말한다.

스머핑(Smurfing) - '핑'을 사용하여 인터넷 호스트 응답을 시험하는 서비스 거절로 이는 네트워크의 플러딩(flooding)을 유도하여 정당한 활동의 접근도 거절시킨다(AIC 2005, 1).

의미적(SEMANTIC) 사회적 엔지니어링

의미적 사회적 엔지니어링(또는 HUMINT, Human Intelligence)는 네트워크 공격의 3차 또는 커밍 웨이브로 고려된다. 이는 기계 자체보다는 컴퓨터를 사용하는 사람의 보안 허점을 목표로 사용되며 인적 또는 컴퓨터 기반의 방법을 사용하여 이루어지기도 한다(Schneier 2001). 이처럼 의미적 사회적 엔지니어링 공격은 외부적 보안 실패(비효과적으로 이행되는 보안 방법)나 비기술적 침투나 데이터 수집의 낮은 인식으로 발생하기도 한다(Barrett 1997, 43). 따라서 사회적 엔지니어는 다양한 조작 방법을 사용할 수 있다.

직접적 접근방법 : 목표 대상자는 조직 내부의 다른 사람에게 전화를 하거나, 패스워드나 사용자이름을 물어보도록 하는 등 사회적 엔지니어를 대신하여 업무를 수행하도록 요구 받을 수 있다 .

1. 중요 사용자: 중요한 마감(업무처리)이 있는 관리자인척 하는 사람. 사회적 엔지니어는 안내데스크에서 연락하여 원격 접속 서버의 번호나 사용

또는 구성에 대한 원격 접속 소프트웨어의 유형 또는 서버로의 기록에 필요한 내용 등 중요 정보를 말해주도록 급박하게 요청한다.

2. 무능한 사용자: 사회적 엔지니어는 능력이 없는 사람처럼 가장하여 비서와 같은 사람에게 자신을 돕도록 한다.

3. 기술 지원 인력: 정당한 사용자로부터 유용한 정보를 얻도록 사회적 엔지니어는 기술지원 팀의 일원인척 한다. 이처럼 가장함으로써 사용자 패스워드를 '바꿔야 한다'는 식으로 행세한다.

4. 역 사회적 엔지니어: 이 기법은 정당한 사용자가 정보를 얻고자 하는 사회적 엔지니어의 질문에 응답하도록 유인되는 것이다. 이 역 엔지니어링 공격은 다음의 세 가지와 관련된다:

- 사보타지(sabotage): 사회적 엔지니어가 워크스테이션 '붕괴'를 위한 접근을 획득하여 장애를 유발한다. 시스템 사용자는 문제를 확인하고 도움을 요청하게 된다(그리고 사회적 엔지니어가 도움을 제공하도록 나타난다)

- 마케팅(marketing): 이는 사용자가 사회적 엔지니어에게 연락하도록 하는 것으로 사회적 엔지니어는 자신의 명함을 미리 주변 사무실에 배치하거나 오류메시지에 대한 컨텐츠 번호를 두게 된다.

- 지원(support): 마지막으로 사회적 엔지니어는 문제해결에 도움을 제공하면서 사용자가 인식하거나 의심하지 못하도록 하며 필요한 정보를 얻는다(Allen 2006).

[방법]

다음은 인적 또는 컴퓨터를 이용한 의미적(semantic) 사회적 엔지니어링

방법 중 공통된 몇 가지 방법을 열거하고 있다.

전화 - 사회적 엔지니어/해커가 목표대상에 전화하여 권한이 있는 사람인 것으로 행세하여 필요한 정보를 빼낸다(Granger, 2001).

도청 - 사회적 엔지니어가 특정 기업의 직원으로 가장하여 점심시간 중 '업무 잡담'을 엿듣기도 한다.

라이브(Live) - 개인은 목표대상인 컴퓨터 시스템 건물에 접근하여 나중에 시스템 접근에 사용할 정보를 얻는다. 덤스터다이빙(Dumpster Diving)과 숄더 서핑(Shoulder Surfing)은 이 기법의 한 형태이다(Guenther 2001).

덤스더다이빙(Dumpster Diving) - 이는 직원기록, 조직도 등 사회적 엔지니어링 공격을 도울 수 있는 문서를 검색하는 시도에서 기업의 쓰레기통을 통해 확인하는 것을 말한다(Granger 2001). 덤스터다이빙은 오래된 컴퓨터에서 과거의 하드드라이브나 CD, 메모리스틱 등으로부터 중요 분석에 사용할 수 있다.

숄더서핑(Shoulder Surfing) - 말 그대로 직원이 컴퓨터에 입력하는 패스워드를 어깨너머로 보는 것을 가리킨다.

보거스 서베이(Bogus Surveys) - 광고(주로 현금 행사 등)가 있는 우편/메일을 통하여 민감한 문제를 물어, 개인이 해커가 나중에 사용하게 될 중요 정보를 노출하도록 한다(FCC, 2002).

팝업윈도우(Pop up Windows) - 인터넷 접속 중에 잘못된 윈도우 창이 나타나면서 사용자 정보를 재입력하도록 한다(사용자 이름과 패스워드). 이 정보는 해커에게 재전송된다(Guenther, 2001).

스파이웨어(Spyware) - 신용카드 정보, 사용자 이름, 패스워드와 기타 개

인신상 정보를 기록하도록 사용된다(주로 키로거의 사용을 통해 활용).

피싱(Phishing) - 해커는 합법적인 기관(예: 은행)으로부터 제공하는 식의 이메일을 전송한다. 스푸프 웹사이트의 URL이 제공되며 목표대상자는 자신의 신상정보를 확인하도록 요구받는다(사용자 이름과 패스워드). 이는 이후 개인 계좌에서 불법적으로 사용될 수 있다. 피싱 사용은 이름에서 알 수 있듯이 낚시처럼 투기적 행위(스페큘러티브 벤처)이다. 피싱 제공자는 순진한 사람들에게 미끼를 던지고 미끼를 물기만을 기다린다. 이들이 속임수로 사용하는 웹사이트는 PayPal, eBay, MSN, Yahoo, BestBuy, America Online 등이 있다. 은행도 주로 목표가 된다. 피싱 제공자는 수 많은 다른 사회적 엔지니어링을 사용하고 이메일 스푸핑을 사용하여 피해자를 현혹한다. 연방거래위원회(FTC)가 밝힌 전형적인 사례로, 17세 남성이 아메리카 온라인으로부터 온 것으로 꾸민 메시지를 발송하였고 수신자의 AOL 계정으로 요금 납부를 요청한 사례가 있다. 가해자의 이메일은 AOL 로고를 사용하였고 합법적인 링크를 포함하고 있었다. 만일 수신자가 “AOL 빌링센터(AOL Billing Center)” 링크를 누르면 개인 신상을 요구하는 허위 AOL 웹페이지로 연결되어 신용카드번호, 개인 확인번호, 사회보장번호, 은행계좌, 비밀번호 등을 입력하도록 요구받게 된다. 이 정보는 신분위조범죄에 사용되었다.[15]

[비싱(Vishing) - 피싱의 전화형태]

파밍(Pharming) - 개인 정보(사용자 이름과 패스워드)를 합법적인 사이트에 입력한다는 점에서 피싱과 유사하며 허위 또는 조작된 사이트를 사용하여 이메일이 사용자에게 발송되며 해커에게 신상 정보를 보내도록 한다. 그러나 파밍은 DNS서버를 마비시켜 URL에서 IP주소로 대화를 방해한다. 따라서 사이트의 URL에서 개별 형태에 따라 조작 사이트로 재발송 되도록

15) http://whatis.techtarget.com/definition/0,,sid9_gci916037,00.html

한다(De La Cuarda 2005).

[사회적 엔지니어에 대한 방어]

대부분 사람들은 일상생활에서 자기 자신이나 자신의 조직에 대해 얼마나 많은 정보를 노출하고 있는지 깨닫지 못한다. 보안 인식 프로그램은 잡담(loose talk)의 영향(결과)도 포함하고 있다. Gragg(2002)는 무엇이 취약성과 위협이 되며 그 위험에 대한 방어를 결정하도록 전통적인 방법을 기초로 멀티 레이어 방어를 제안하고 있다. 그는 방어는 다양한 레이어를 보유하여 해커가 한 레이어를 뚫더라도 다른 단계를 통해서 무력화해야 한다고 제안하고 있다. 이를 레이어로 칭하거나 레벨로 칭하든 지에 관계없이 사회적 조작 위험에 대한 충분한 인식이 방어의 기초가 되어야 한다.

[사회적 엔지니어링을 다루는 보안 정책]

정보 보안의 기초는 정책이다. 보안 정책은 네트워크, 시스템, 환경 등에 적용할 수 있는 기준과 보안 수준을 설정한다. 사회적 엔지니어링은 요청에 대응하는 요령을 알아야 하는 사람들을 대상으로 한다. 수립된 정책은 최종 사용자가 자신도 해커의 요청에 저항해야 한다는 느낌을 갖도록 지원해야 한다. 그리고 특정 정보가 노출되어도 되는 지에 대하여 문제를 제기하는 위치에 있지 않아야 한다. 이는 조직의 보안 정책을 수립하는 사람들이 사전에 마련해야 한다. 보안 정책은 정보통신기술의 기존 요소들(즉, 정보접근 제어, 계정 설정, 접근 승인 및 패스워드 변경)을 다뤄야 한다. 이는 문서나 기타 매체, 잠금, 아이디, 폐기 정책, 방문자 에스코트 등의 모든 분류를 다뤄야 한다. 그리고 이를 모두 강화해야 한다(Granger, 2002a, p. 2). 사회적 엔지니어링을 다루는 보안 정책은 직원이 상기에 제시했던 심리적 유인에 대하여 보호할 수 있도록 도움을 제공해야 한다. 정책은 권위에 대한 '균형

있는 효과'도 가지도록 하여 자신이 언제 전화호출을 받게 되는지를 추측하도록 한다. 정책은 어떤 정보가 노출되거나 접근이 있을 때 책임을 명시하여 직원들이 정보나 접근의 노출 시에 스스로 지는 위험에 이견이 없도록 해야 한다.

[모든 사용자에 대한 보안 인식 훈련]

유능한 사회적 엔지니어는 우선 신뢰관계를 형성하려고 시도한다. 모든 직원은 어떤 종류의 정보를 사회적 엔지니어가 사용할 수 있고 어떤 대화가 의심스러운 것인지에 대해서 알아야 한다. 이들은 기밀 정보와 그를 보호할 책임에 대해서 인식해야 한다. 그리고 요청을 거절할 때 경영진의 후원이 있다는 점도 알아야 한다. 이는 특히 거절로 인한 피해가 있을 때 중요하다. 직원은 사회적 엔지니어링 공격에 존재하는 기본적인 현상에 대해서도 알아야 한다. 이 중 일부는 연락처를 알려달라는 요청에 대한 거절, 러쉉, 친한 명칭을 부르는 일, 친밀감, 잘못된 스펠링, 이상한 질문, 기밀 정보의 요청 등이 있다. 직원들은 요청자에게 문제를 제기하고 부적절한 응답의 문제가 있을 때 정보를 거절해야 한다(Granger, 2002a "Combat Strategies", p. 3). 보안인식 훈련은 보안 정책을 따라야 하지만 사용자가 사회적 엔지니어링과 관련하여 반드시 인식해야 할 핵심적인 내용도 있다.

1. 가치 결정: 대부분 사람들은 해킹을 당하거나 시스템에 문제가 생기기 전에 데이터나 접근에 대하여 가치를 부여하지 않는다. 갑자기 컴퓨터 접속이 되지 않는다면 무엇을 해야 할지를 우선 생각해야 한다.

2. 친구와 적: 전화로 친밀함이 생긴 친구나 어떤 이유에서 든 중요 정보에 대한 질문을 하는 사람은 적일 수 있으며 결국 친구가 아닐 수 있다. 사회적 엔지니어는 요청을 하기 전에 피해자와 오랫동안 친구관계를 유지한다.

모든 사용자는 친구라는 이유로 중요 데이터나 접근에 대하여 신뢰하지 않아야 한다는 점을 인식해야 한다.

3. 패스워드: 일부 해커는 결코 패스워드를 묻지 않는다. 그러나 어떤 이들은 전혀 모르는 사람에게 직원들이 패스워드를 말해 주는 것에 대하여 사회적 조작(social manipulation)을 사용하는 확신적인 이유가 있게 된다. 보안 인식이 없는 사람들은 별 생각 없이 자신의 패스워드를 말하기도 하며 특히 '조사'를 위한 정보제공 요청에 속거나 호화 유람선 사진이나 기타 별 이상이 없어 보이는 사이트에 패스워드를 입력하도록 유도한다. 사용자는 다른 시스템에도 종종 동일한 패스워드를 이용하기 때문에 해커는 메신저나 채팅룸 같은 다른 소스를 통해서 피해자의 도메인 접근을 얻기도 한다.

4. 유니폼과 배지: 가짜 배지나 유니폼을 이용하여 침입자가 현장에서 합당하게 존재할 근거로 믿게 하는 일은 매우 쉽다.

5. 핵심 인력 저항: 핵심 인력에는 IT 헬프데스크 인력, 고객 서비스, 비즈니스 보조자, 비서 및 리셉션니스트, 시스템 관리자와 엔지니어 등이 있고, 저항 훈련을 통해 직원들이 해커가 요청하는 정보요청에 설득 당하지 않도록 한다. 일부 저항 교육 기법은 사회심리학 분야에서 사용되는 것으로 직원들이 사회적 엔지니어의 설득기법에 저항할 수 있도록 돕는다.

주입 방법(Innoculation) - 직원들은 사회적 엔지니어가 사용하는 설득적인 말을 듣게 한다. 이는 예방주사를 통해 질병유포를 방지하는 것과 동일한 역할을 한다. 직원들은 사회적 엔지니어가 직원이 사용할 수 있는 논리적 주장에 따라 사용하는 형태에 노출된다. 연구에 따르면 이는 효과적이고 오래 지속되는 예방책이 된다. 문제는 훈련자가 사회적 엔지니어의 모든 진술에 대하여 예측할 수 있어야 한다는 점이다.

사전경고 - 이는 유입되는 메시지의 내용이나 유입되는 메시지의 설득 의도와 관련된다. 메시지 내용의 사전경고는 설득력 있는 의도의 사전 경고보다 더 강력한 사회적 엔지니어 공격 저항이 된다. 이 훈련은 실제로 사회적 엔지니어가 목표대상을 설득하려는 시도 뿐만 아니라 이들의 주장이 조작적이고 기만적이며 거짓이라는 점도 강조한다. 직원들은 해커의 의도가 범죄이며 훔쳐내려는 의도를 가지고 있다는 내용을 전달 받는다. 이 '블랙 앤 화이트' 정의는 사전 경고가 효과적일 경우에 필수적이다(Sagarin et al; 2002, 527).

현실 직시 - 직원들이 스스로 공격에 취약하다는 점을 깨닫도록 한다. 종종 사람들은 아무도 자신을 바보로 취급하지 않을 것이라는 생각으로 취약성에 대하여 비현실적이 되기 쉽다. 이 인식은 많은 사람들이 실제 위험을 무시하도록 하며 위험에 대처하는 방안을 취하지 못하도록 한다. 그러나 일단 직원들이 이를 직시하고 자신이 취약하단 점을 알게 되면 훈련 결과는 더욱 효과적이다(Sagarin et al; 2002, 536).

위험 취약성 인식에는 세 가지 단계가 있다.

1. 인식 - 위험이 존재하는 것을 인식한다.
2. 일반적 취약성 - 타인에 대한 위험 가능성에 대한 생각(믿음)
3. 개인적 취약성 - 자신의 개인적 취약성에 대한 인식

보안인식과 저항 훈련은 인식으로만 제한되는 경우 제한된 가치를 가진다(Sagarin et al; 2002, 540).

메모리 조깅(Memory Jogging) - 사회적 엔지니어링에서 보안 안식 훈련 노출은 단기적으로 효과가 있다. 정기적인 메모리 조거나 리마인드를 통

해 위험 접근을 항상 인식하도록 한다. 이는 사고에 대한 정기보고나 사고가 없더라도 보고를 통해 달성된다. 아마도 주간 비즈니스 보고나 정기적인 보안 전용 뉴스레터가 좋을 듯하다.

사회적 엔지니어링 트랩 - 실제 위험에 노출되어 이를 저지하는 시스템에서 설정된다. 트랩은 잠재적 피해자와 피해가 진행중인 보안에 대하여 경고를 한다. 실제로 종종 시뮬레이션 위험으로 직원들이 일반적인 사회적 엔지니어링 조작에 대응하도록 한다. Gragg(2005)는 사회적 엔지니어링을 벗어나는 몇 가지 제안을 하고 있다.

정당화된 노우잇올(know-it-all) - 대범한 사회적 엔지니어는 주저 없이 조직으로 걸어 들어가서 탐색을 시작한다. 모든 직원들은 사회적 엔지니어의 실제 존재에 따른 보안 위험에 대해 충분히 인식해야 하고 에스코트가 없는 방문자에 대하여 대응할 수 있는 권한을 가지고 있어야 한다. 이 트랩은 배지를 착용하는 경우에도 유용할 수 있는데 종종 해커들은 가짜 배지를 차고 나타날 수 있기 때문이다. 큰 조직에서는 직원을 배치하여 '목양견'이나 '라운드업' 침입자 형태를 복도에서 탐문하도록 하고 있다.

집중된 보안 기록 - 이는 정보보안인력이 효과적인 공격을 방어하도록 감시되도록 한다. 단순한 시스템이나 네트워크 접근 기록이 아니며 안내데스크나 고객서비스요청도 포함하고 있다. 실제로 모든 직원이 민감한 정보를 요청하거나 의심스러운 경우마다 기록을 유지하는 커뮤니케이션 채널이 있어야 한다. 집중식 기록이 효과적이 되려면, 기록을 정기적으로 확인해야 한다.

폰백(Phone Back) 정책 - 종종 잊기 쉬운 단순한 절차로 효과적인 트랩이 패스워드 리셋을 통한 사회적 엔지니어의 접근을 방어하도록 한다. 콜

백은 2차 및 3차 확인 정보가 있는 개인 아이디로 지원되어야 하며 기업과 실제 당사자만 알고 있어야 한다. 다시 말해서 보안 로그의 처음에 생성되어야 한다(Farber; 2001, 1). 세 가지 다른 강화도 폰백 정책을 강화하도록 사용될 수 있으며 '단독' 모드도 사용된다.

- 세 가지 질문(The Three Questions) - 질문과 답변 식으로 제공되며 안내데스크 직원이 아이디 확인을 위해 사용한다. 세 가지 질문은 직원과 미리 조율되고 타인과 구별이 명확하도록 한다.

- 콜 홀드(Call Hold) - 의심스러운 전화나 패스워드 리셋이나 중요 정보를 요청하는 전화는 홀드시킨다. 사람들은 압력이 있거나 놀라거나 업무 부담이 있을 때 잘 모르는 것을 수행하도록 쉽게 설득 당한다. 중요한 점은 기록을 하고 그 내용이 정당하며 추가적인 검증이 필요하거나 거절을 해야 하는지를 판단하여 정보를 다루어야 한다.

- 허위 질문: 이는 잘못된 정보를 제공하여 호출자가 바로 잡거나 잘못된 정보를 수립하도록 하는 질문이다. 이런 질문 유형은 '새로 산 차는 어때?'라고 물으면 호출자가 '저는 새 차가 없습니다'라고 응답하여 단일 질문을 통과하도록 한다. 이 때 직원은 자신이 실수했음을 사과하고 설명해야 한다. 하지만 호출자가 새 차에 대하여 말을 하게 되거나 목표 대상자가 새 차에 대하여 말하도록 하면 해커가 걸려들게 된다. 이 때 전화 목표가 되는 사람은 즉시 보안을 인식해야 한다.

사고 대응: 이는 보안 네트워크가 사회적 엔지니어가 보안을 잘 모르거나 관심이 없는 조직의 일원을 찾도록 하지 못하게 한다. 이 과정을 수립하여 지원들이 가능한 의심스러운 상황 발생 직후 사고를 보고하도록 할 수 있고 이 과정은 적극적으로 해커에 대응하여 선제적으로 다른 가능한 피해자에게 고지하도록 한다.

[현재의 추세]

지난 해에만도 보트넷(botnet; 좀비)의 사용이 급증한다는 보고가 있었다. 지멘텍은 2005년 상반기에 매일 평균적으로 1만여 보트(좀비)가 확인된 것으로 발표하였다. 이 수치는 2004년 동기 대비 두 배에 해당한다. 사회적 엔지니어 형태의 피싱 사용(10억 4천만 건 확인)도 2004년 상반기에 비해 2005년 상반기에 거의 두 배로 증가하였다. 그러나 2005, 2006년 중, 보고된 피싱 사고 건수는 동일한 수준으로 유지되고 있다. 이는 컴퓨터 사용자의 사이버 범죄에 대한 인식 증가와 파밍이라는 새로운 기법의 개발로 인한 것이다(CCRC 2006).

비싱(피싱의 전화 형태)도 피싱 활동을 대체하고 있다. 비싱은 목표 대상자에게 확인 요청을 통해 세부정보를 기재하도록 하는 '안내전화'를 통해 신용카드계좌 등에 허위 활동을 한 것으로 알려주어 필수적인 신용카드 정보(예: 카드번호, 만기일, 보안코드) 등을 요청하게 된다(CCRC 2006). 이 데이터는 뉘상스 해커 공격에서 수익 동기적 공격(CCRC 2006)으로 변형된 것으로 보인다. 공격은 보다 집중적인 목표로 소규모의 성격을 띄고 있다. 키로거(사용자의 타이핑 내용을 알아내는 프로그램)가 2004, 2005년 기간 중 3%나 증가(12%-15%)하고 있는 중요 스파이웨어가 되고 있다(CCRC 2006).

[미래의 추세]

보트(bot)의 사용은 가까운 미래에 증가할 것으로 예상되고 있다(CCRC 2006). 보트 컴퓨터 커뮤니티는 "훨씬 정교하고 집중적인 공격"이 될 것으로 예상된다(CCRC 2006). 이는 모든 해커 공격 분야에서 더욱 집중적인 추세를 반영한다. 웜이나 바이러스 같은 구문적(syntactic) 공격이 과거에 유포되

어 파괴나 불편을 유발하였다면, 보트(bot)나 파밍(pharming) 등 의미적(semantic) 사회적 엔지니어링 방법은 은행계좌 접근에 사용할 수 있는 개인 정보를 탈취한다. 따라서 조직범죄가 이런 유형의 범죄 활동을 할 것으로 예상되며 미래의 하이테크 범죄에서 중요한 역할을 할 것으로 예상된다. 또한 사용자가 은행 비밀번호 등을 데스크톱 컴퓨터에서 전화기, 블루베리나 기타 인터넷 연결 기기 등 스마트 장치로 저장하는 경향으로 인해 목표가 이동할 것으로 예상된다. 이는 의미적(semantic) 공격의 다음 중요 목표 대상이 될 것이다.

인터넷에 연결되는 상용 장치(예, 자판기, 가스펌프, ATM)의 도입과 결재에 사용되는 전화기 사용의 증가는 바이러스의 미래에 중요 대상 영역이 될 것이라는 점을 말해준다(CCRC 2006). PC 이외의 다른 장치도 목표가 될 것이다. 그 중에는 라우터, 스위치, 백업장치 등이 있다(CCRC 2006). 그리고 IM(인터넷 메신저)와 같은 실시간 프로그램도 점차 목표대상으로 확대되고 있으며 연 간 1,700%나 급증하였다(CCRC 2006). 이전에 사용하던 구문적(syntactic) 수단 보다 의미적(semantic)/인간의 지적 방법으로 추세가 나타나고 있다. 이는 의미적(semantic) 방법이 바이러스와 고장 형태의 공격과 같은 구문적(syntactic)에 비해 구체적인 정보(예, 신용카드정보)를 목표로 하고 있기 때문이다. 인적 기준의 사회적 엔지니어링은 기술적 방법으로 할 수 없었던 많은 정보를 취득할 수 있도록 악용되고 있다. 이는 추후 수익 동기적 공격으로의 변화추이를 보여주고 있다.

참고문헌

Allan A., Noakes‐Fry K. and Mogull R. (2005) 'Management Update: How Businesses Can Defend against Social Engineering Attacks'; March 16, 2005; Gartner.

Allen M. (2006) 'Social Engineering‐A Means to Violate a Computer System'; June 2006; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006

Australian Institute of Criminology (AIC) (2007) 'Online Auction Crime'. AIC High Tech Crime Brief, AHTCC; Canberra.

Australian Institute of Criminology (AIC) (2005a) 'Concepts & Terms'‐High Tech Crime Brief (http://www.aic.gov.au/publications/htcb/htcb001.html) accessed 20 Dec 2006

Australian Institute of Criminology (AIC) (2005b) 'Phishing'‐High Tech Crime Brief (http://www.aic.gov.au/publications/htcb/htcb009.html) accessed 20 Dec 2006

Barrett N. (1997) *Digital Crime: Policing the Cybernation.* Dover, NH, London: Kogan Page, UK.

Burtner W. K. (1991) "Hidden Pressures." Notre Dame Magazine, Winter 1991‐92 p.29‐32.

Cateledge B. (2005) 'Social Engineering Overview'; University of South Carolina, Colombia, USA.
(http://www.chem.sc.edu/support/publicSocialEngineering.pdf) accessed 20 Dec 2006

Chantler A.N. (2006) 'Intelligence Futures: Brace Yourself, Be Prepared to Accept the Unacceptable'; Presentation at the Annual Conference of AIPIO (Australian Institute of Professional Intelligence Officers) October 2006; Brisbane, Australia.

Choo, R.,and R.Smith, 2008, 'Criminal exploitation of online systems by organised crime groups', Asian Journal of Criminology, 3:in press.

Cialdini R. B., Green B. L. and Rusch, A. J. (1992) "When Tactical Pronouncements of Change Become Real Change: The Case of Reciprocal Persuasion" Journal of Personality and Social Psychology: Vol. 62(1), 1992, 30 – 40.

Computer Crime Research Centre (CCRC) (2006a) 'Hackers Replaced by Phish Con Artists'; Date: January 03, 2006 (http://www.crime – research.org/ analytics/ pure – hackers – replaced – by – phish – con – artists/) – accessed 20 Dec 2006

Computer Crime Research Centre (CCRC) (2006b) 'Telephone Version of Phishing'; Date: July 13, 2006 (http://www.crime – research.org/news/13.07.2006/2116/) accessed 20 Dec 2006

Computer Crime Research Centre (CCRC) (2006c) 'Hackers Shift Targets in 2006'; Date: March 06, 2006 (http://www.crime – research.org/analytics/1862/) accessed 20 Dec 2006

De La Cuarda, F. (2005) 'Pharming – a new technique for Internet fraud' Computer Crime Research Centre. (www.crime – research.org/news/07.03. 2005/1015) accessed 1 Dec 2006

Farber, D. (2002) "Mitnick on Mitnick: 'Why I'm going legit' (Part Two) Interview with Dan Farber." ZDNet. October 8, 2002. http://www.silicon.com/public/door?6004REQEVENT=&REQINT=55863&REQSTRI1

Federal Communications Commission (2002) 'Computer Security Notice: Social Engineering'; Computer Security Week; Federal Communications Commission, USA.(http://csrc.nist.gov/fasp/FASPDocs/securityate/December – 2002 – 2.pdf) accessed 18 Dec 2006

Federal Trade Commission (2005) 'Take Charge: Fighting back against Identity Theft'; Federal Trade Commission, Washington D.C. USA. (http://www.ftc.

gov/bcp/conline/pubs/credit/idtheft.pdf) accessed 20 Dec 2006

Fite B.K. (2006) 'Corporate Identity Theft'; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006

Gragg D. (2002) 'A multi‐Level Defense Against Social Engineering'; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/)accessed 20 Dec 2006

Granger S. (2002a) "Social Engineering Fundamental, Part I: Hacker Tactics."

Security Focus Online. (http://online.securityfocus.com/infocus/1527) accessed 20 Dec 2006

Granger S. (2002b) "Social Engineering Fundamental, Part II: Combat Strategies."

Security Focus Online. (http://online.securityfocus.com/infocus/1533) accessed 20 Dec 2006

Guenther M. (2001) 'Social Engineering ‐ Security Awareness Series'; Information Warfare Site U.K. (http://www.iwar.org.uk/comsec/ resources/sa‐tools/Social‐Engineering.pdf) accessed 20 Dec 2006

Landman, J. and Petty, R. (2000) "It Could Have Been You: How States Exploit Counterfactual Thought to Market Lotteries," Psychology & Marketing Special

Issue: Counterfactual thinking. Vol. 17(4), April 2000, 299‐321

MicroSoft 2007, Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws. A Study by Microsoft, November 2007, online

Nelson, R. (2001) "Methods of Hacking: Social Engineering." Institute for Systems research, University of Maryland, (http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html) accessed 30 Feb 2006

Petty R. E., Fleming M A., Priester J. R. and Feinstein A. H. (2001) "Individual versus group interest violation: Surprise as a determinant of argument

scrutiny and persuasion." Social Cognition: Vol. 19(4), Aug 2001, 418 – 442.

Rusch J. (1999) 'The Social Engineering of Internet Fraud'; United States Justice Department – Proceedings of the 1999 Internet Society Conference, USA. (http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm) accessed 20 Dec 2006

Sagarin, Brad J.; Cialdini, Robert B.; Rice, William E.; Serna, Sherman B. (2002)"Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion." The Journal of Personality & Social Psychology: Vol.83(3), Sept 2002, 526 – 541.

Schneier B. (2000) 'Semantic Attacks: The Third Wave of Network Attacks' (http://www.schneier.com/crypto – gram – 0010.html#1) accessed 20 Dec 2006.

Smith R.G. (2006) 'Preventing Identity – related Crime: 100 points, biometrics or identity cards'; AIC Trends & Issues No 324, August 2006; Canberra.

Social Engineering and Crime Prevention in Cyberspace

Dr. A. N Chantler, School of Justice, Queensland University of Technology, Brisbane, Australia
Professor R.G. Broadhurst, Key Centre for Ethics, Law, Justice and Governance, Griffith University and Visiting Fellow Research School of Asian and Pacific Studies, ANU.

Draft October 2008[1)]

Abstract

This paper highlights methods of syntactic and semantic social engineering attacks (human-based and computer-based) that are currently prevalent in the cyber community. It will also discuss emerging trends and, the likely future direction cyber-crime will take with respect to social engineering. The risks of deception in the on-line environment appear to be increasing and with the rapid growth of internet access a large pool of people are likely to be exposed to manipulation. The legal response to on-line forms of deception or social engineering remains fragmented and inadequate failing to recognise the increased potential of organized criminal activity.

Introduction

Microsoft (2007[2)]) in an extensive review of cyber security laws among 14 Asia Pacific nations[3)] using the Council of Europe bench mark *Cybercrime*

1) Original draft paper prepared as a technical report for the Australian Institute of Criminology 'Futures of High Tech Crime', ,January 2007.
2) I am grateful to Mr Jeff Bullwinkel of Microsoft's Singapore office for providing a copy of the report.

Convention noted the diverse range of legislative responses. In particular the review noted the poor compliance with model privacy laws based on OECD guidelines with only four countries (Australia, Hong Kong, Japan and New Zealand) achieving moderate alignment[4]. Anti-spam laws fared worse with only one jurisdiction (Hong Kong) meeting the rather modest 'opt-out' anti spam regime benchmark applied and four countries currently lacked any prohibitions (India, Indonesia, Malaysia and Taiwan[5]). Even for core offences such as the criminalization of unauthorized access to computers, systems, programs and data some countries have yet to enact laws (Indonesia[6]) or provide for civil remedy (India[7]). Despite widespread public alarm only one jurisdiction (Australia) met the model laws for on-line child safety and six countries were without relevant laws (India, Indonesia, Malaysia, Philippines, Singapore and Vietnam)[8], however the report noted that several jurisdictions had legislation pending. *In short the scope of legal countermeasures to common cybercrime offences provide ample manoeuvre for offenders wishing to exploit cross-border legal loopholes.* In the context of our discussion of 'social engineering' the risks to cyber-criminals are consequently less hazardous and individual 'victims' more vulnerable unless robust precautions are taken.

---

3) Australia, Hong Kong, New Zealand, India, Taiwan, China, Japan, Vietnam, Malaysia, South Korea, Philippines, Indonesia, Thailand and Singapore.

4) The Microsoft review noted, however, that China, India, Indonesia, Malaysia, South Korea, Taiwan and Thailand are preparing data protection laws in part because of the 2005 APEC Privacy Framework.

5) The report, however, notes that most jurisdictions are in the process of enacting or strengthening anti-spam measures.

6) Although the Electronic Information and Transaction Bill is pending and is adjudged moderate to weakly aligned to the CoE Convention as it focus on offences against government agencies.

7) India's Information Technology (Amendment) Bill 2006 proposes to amend the IT Act to criminalise many of the acts that constitute core offences under the Convention but only where they are done "dishonestly or fraudulently."

8) The report states: "Although most countries have enacted broad obscenity regimes that have some application to online dealing in child pornography, only five of the fourteen jurisdictions – Australia, Hong Kong, Japan, South Korea and Taiwan – have enacted legislation that specifically addresses child pornography, and three of the fourteen jurisdictions – Australia, Hong Kong and Taiwan – have enacted legislation that contains computer facilitated childpornography offences.

Although Asia represents about 56% of the world population only about 13.7% of its population has access to the Internet (about 510 million users). However, this represents over a third of the world's current population with access to the Internet and thus a highly significant market. Asia's growth rate remains higher than the rest of the world at around 337% per annum compared to 266%. North America (71% of the population have access) Oceania/Australia (57%/75%) and Europe (43%) have the highest levels of access per head while Africa a mere 4.7% of the population have Internet access.[9)]

Interest in cyber crime victimization has been recognized when for the first time questions about Internet crimes were included in the 2004 US National Institute of Justice household Crime-Victim Survey (US CVS). The scope is restricted to the *personal use* of computers (at home, school or work), or for operating a home business and also asks if any monetary loss occurred and if the matter was reported to police or other agencies. Over time CVS will yield valuable data about the cyber-crime experience of ordinary users and provide tracking data helpful in evaluating policy responses[10)]. The questions devised for the US CVS were duplicated in the Hong Kong UNICVS.[11)] Results for the 2291 HK UNICVS respondents found that 58.3% had access to computer and 98% of these computer users had access to the Internet (n=1332). Of the household respondents with access to a computer 67% (891) experienced at least one form of cyber crime in the past year somewhat more than the 61% of businesses. Nearly 12% did not have a firewall or anti-virus software installed (4.7%) or did not know if they did (7%). Among business respondents 8.3% reported not having a firewall or anti-virus programme and 5.4% did not know. The main types of cyber crime reported by household and

9) Thirty per cent of the estimated on line population of 1,262 million (as at November 2007) used English, followed by Chinese (15%), Spanish (9%), Japanese (7%), German (5%), French (5%), Korean, and Italian (about 2.6%), Portuguese (4%) and Arabic (3.7%) See for further details http://www.Internetworldstats.com/stats.htm, accessed April 9, 2008

10) A Chinese translation was implemented in the UN ICVS conducted in China in 2006-2007.

11) Identity theft questions were added to the US CVS in July 2004. Only 6 months of data were available for analysis.

business respondents were obscene content and ‘malware’. About 13% of household respondents claimed that the cybercrime event incurred monetary loss and of these approximately 26% estimated the loss to be greater than $HKD1,001. Among businesses the losses were significantly higher with 14.5% reporting monetary losses and of these 40% had losses greater than $HKD1,001 and 12.5% losses exceeding $HKD10,001.

A revised US CVS focused on problems of identity theft i but did not specifically address the misuse of computers[12]. About 3 percent of all US households had been the victims of at least one type of identity theft during the last six-months of 2004. Forty-eight percent of these victims had experienced an unauthorized use of credit cards; 25 percent had other accounts, such as banking accounts, used without permission; 15 percent experienced the misuse of personal information and 12 percent experienced multiple types of theft at the same tim e[13]. Households headed by young people (18-24 years old), those in urban or suburban areas and those with incomes over $75,000 were the most likely to experience identity theft. Victimization did not differ by race or ethnicity. About one-third of households that were identity theft victims discovered the loss by noticing missing money or unfamiliar charges on an account, and about one-quarter were contacted by a credit bureau. The estimated loss during the 6-month period was about $3.2 billion. About two thirds of the households said they lost money at an average of $USD1,290 and one-quarter of all victimized households said the misuse had not stopped[14].

Increasing government and consumer pressure is now exerted on the security of consumer information held by private companies. At the least this involves effective procedures to safeguard identity information and a notification obligation of any breach. Even this latter measure may be hampered by the fact that such information may also be held outside the jurisidiction where the protections exist.

---

12) At the time of writing the authors have not been able to find any US data from the CVS that reports survey results.

13) http://www.ojp.usdoj.gov/bjs/pub/press/it04pr.htm released on April 2 – accessed June 20, 2006.

14) http://www.ojp.usdoj.gov/bjs/pub/press/it04pr.htm released on April 2 – accessed June 20, 2006.

What is Social Engineering?

In this context 'social engineering' is the term used to describe the use of psychological tricks and the manipulation of behaviour often by means of deception, by cyber-criminals on unsuspecting users to gain 'access information' in order to commit crime. Cyber-criminals are those people that we already 'label' as hackers and conmen who use social engineering to avoid complex technical means to access computers.

The users become the *primary* target associated with the cyber-criminals' *secondary* target, such as the organisation's computer system; which in turn may lead to a *tertiary* or main target such as a system control program, database, financial or telecommunication system. Cyber-criminals will try to gain the relevant 'access information' enabling them to bypass security. This can include usernames and passwords, PIN's (personal identification numbers), tokens and credit card information (Federal Communications Commission 2002). Once they have gained access to the system they are then able to erase, modify or copy the information to suit the needs of their attack (Guenther 2001).

Social engineering manipulates any individual's innate desires (e.g. friendship, romance, greed) by building a trustworthy relationship with the target usually by deceiving the target about the bona fides of the relationship; and, then exploiting that relationship to obtain the information required. Part of the process involved in social engineering includes ID theft. In the past, this provided a means for a hacker to reach their final goal in accessing a network or system; today, ID theft alone, is becoming a major concern (Federal Trade Commission, 2005; Smith, 2006).

As ICT (information communications technologies) continue to evolve, we see an increasing use of the internet for the conduct and development of e-commerce, particularly for secure financial transactions. Tied to this development, we also see a parallel with an increase in the sophistication of

ICT security utilising encryption, specialist hardware, improved application software, tokens, firewalls and other means. The problem is that whilst computer users are becoming more technically competent and computer-security literate, there has not been a comparable ‘learning’ or development of ‘awareness’ of the security implications associated with social engineering. This applies to both corporate and home environments.
Corporate identity theft (Fite B. K. 2006), the theft of an individual’s identity, and, ‘Online Auction Crime’ (AIC 2006) can all be capitalised upon using social engineering.

This theft of identity may become an even greater issue for ICT security in the future, as the attributes of successive generations of the population are seen to hold different values. For example, the ‘baby-boomers’ are now heading towards retirement age and hold different attitides when compared-with the current ‘x’ and ‘y’ generations of today.

‘Baby-boomers’ attributes are perceived as having a ‘belief in the government’; ‘not being very computer literate’; are ‘loyal and conservative’; ‘reliable’ and, for the most part are ‘intuitive about the consequences of their actions’. The ‘x’ generation are seen as being ‘technically competent’; ‘somewhat lacking in intuitive ability’; discontent; and ‘they blame the previous generation for their current situation’. The ‘y’ generation are considered ‘highly technically competent’; ‘lacking good role-models’; are ‘self-centred’; ‘lack consideration for others’; and, ‘are only concerned with the present’. This perceptive erosion of values, based on these social attributes, may impact on security in the future through an evolution of changes in the kinds of deceptions likely to succeed (Chantler 2006). In other words cyber-criminals will adapt to the changes in cultural markers of ‘trust’ and ‘cool’.

Motivation for Hackers

There are a variety of motivations that exist in human behaviour for the deceptions involved in effective social engineering:

- **Technical Avoidance.** Social engineering is perceived as a much easier path to financial gain rather than become involved in trying to breach a complex and cumbersome technical pathway.

- **Self-Education.** Whilst it seems to be much more infrequent, there are still those hackers who are motivated simply by the thrill of 'gaining knowledge'; and 'beating the system'.

- **Financial Gain.** Motivation for financial gain information gathering can be triggered by many reasons: feeding a habit (an addiction); seen as an easy way to get money; organised crime; blackmail; etc.

- **Revenge.** Disgruntled employees use weaknesses within the ICT frameworks to 'get back' at the corporate entity; or, they may even target an individual within the organisation.

- **External Pressure.** Blackmail, ransom, family pressure, organized crime, moral dilemmas and extremist beliefs (orders) can be used to apply pressure to an individual to commit a cybercrime. From a psychological aspect, the social engineer will manipulate the target person's values so that they are led to believe that they are not hurting anyone, 'after all you are only dealing with zeroes and ones'.

- **Terrorist, Political and Issue Motivated Groups.** These groups can be fanatical about their cause and will try and capitalise on weaknesses inherent in the financial and critical information infrastructure to cause shock to a target population.

- **The Wannabe ('Walter Mitty').** Often people who have psychological issues in believing that they are someone who they are not; people who want to be a 'James Bond' are only motivated to commit a criminal act, to do 'something daring', to become 'a spy' thereby

satisfying their own distorted psychological needs.

The Stages in a Social Engineering Attack

There is a common pattern associated with a social engineering attack (Allan, Ant, Noakes-Fry, Kristen, Mogull, Rich 2005). Allen (2006, 5) states that 'any criminal act has a common pattern. Such a pattern is evident with social engineering, and it is both recognizable and preventable.' Allen (2005, 5) suggests that this pattern can be considered as a Cycle consisting of four stages, similar to the steps proposed by Cateledge (2005).

There are generally *four* steps in a social engineering attack (Catledge 2005, 8-9):

1. **Information Gathering** - this involves gathering information about the person that the social engineer is targeting, or other information about the organisation or personnel that will convince the target individual to divulge the required information. A variety of techniques can be used to gather information about the targets; this information can then be used to build a relationship with either the target or someone of influence or important to the success of the attack. Typical information that may be gathered could be an internal phone directory; birth dates; organisational charts; personnel records, social activities, relationships etc.

2. **Development of Relationship** - developing a rapport with the target makes it easier to obtain the information in the next step. The social engineer will capitalise on the psychological aspect of trust. They may feely exploit the willingness of a target in order to develop an element of trust from them; often by presenting themselves as a more senior member of the organisation who will share a confidence with the target to further strengthen the element of trust.

3. **Exploitation of Relationship** - this refers to the manipulation of the

target resulting in the social engineer obtaining the information e.g. username and password; or, perform an action which they may not normally do e.g. creating an account.

4. **Execution to Achieve the Objective** – having obtained the required information, the social engineer is able to use this to access the system; and the steps or stages are complete.

Whilst this example is a simplistic presentation of the stages, it must be remembered that each social engineering attack is unique; and, that it is highly likely that many phases or cycles may be involved that also incorporate traditional attack methods e.g hacking, password cracking etc.

Psychological Triggers Behind Social Engineering

Gragg (2002) suggests that since social engineering is a social and psychological activity, it is reasonable to try and comprehend the psychology behind social engineering before considering the development of a defence system against it.

To be able to do this, it is necessary to recognise the psychological 'triggers' that are invoked during a social engineering attack. These 'triggers' are psychological principles that demonstrate a form of the power to influence, persuade or distract people in to behaving differently. Understanding these the sorts of psychological triggers behind social engineering also helps to appreciate different aspects that may be used to combat the threat and enhance security. Gragg (2002, 6-9) makes particular mention of the following triggers.

Strong Affect - is a trigger that uses a heightened emotional state to enable a hacker to get away with more than what would be reasonable. If the victim is feeling a strong sense of surprise, anticipation or anger, then the victim will be less likely to think through the arguments that are being presented. *Strong*

affect is introduced when the social engineer makes some statement at the outset of the interaction that triggers strong emotions. The *strong affect* includes, but is not limited to fear, excitement or panic. This could be the promise of a substantial prize worth hundreds or thousands of dollars, or the panic of having an employee's job dependent on one decision. This surge of strong emotions works as a powerful distraction and interferes with the victim's ability to evaluate, think logically or develop a counter-factual argument based on tangible facts (Rusch, 1999 p. 4). Counter-factual thinking is a phenomenon that is related directly to producing a *strong affect*. Landman et al. (2000 p. 299) explains how counter-factual thinking relies on the possibilities of anticipation and thrill that will short-circuit a person's reasonable thinking process. A typical example is to have been selected as 'one of a few to win a fabulous prize'. The person ignores the fact that the likelihood of winning is actually very remote, but gets distracted by their own thoughts, often leading themselves to risk giving away information or access details for the possibility of a prize. It is as if the person is 'under a spell'; or, placed into a different sense of reality which has been brought on by the sudden surprise and excitement, with a rush of other emotions.

Overloading - is a condition that is achieved by presenting mistaken premises that are unchallenged when they are heard rapidly; this is because they are presented interlaced with convincing truisms. This is a psychological trigger of *overloading*. Having to deal with a lot of information quickly affects logical functioning and can produce a 'sensory overload.' With too much information to process, people become 'mentally passive – they absorb information rather than evaluate it' (Burtner, 1991 p. 2). Arguing from an unexpected perspective can also trigger overloading. The target needs time to process the new perspective but that time is not available. This leaves the target with too much information and not enough time to think it through, reducing the target's ability to process or scrutinize the argument. The target is then more willing to accept arguments that should have been challenged (Petty, et al. 2001 p. 2).

Reciprocation - is a psychological trigger that is often used to induce desirable

behaviour. It is based on the premise that in social interactions if someone gives us something or promises us something, we should return the favour. This is often the case even when the original gift was not requested or even if what is requested in return is far more valuable than what was originally given. This truth is known as reciprocation (Rusch, 1999 p. 6).

The hacker, Kevin Mitnick, suggests that "In the corporate environment, people are unlikely to evaluate a request thoroughly, so they take a mental shortcut". The reasoning that follows is that if someone calls and is helping with a problem, then that person is 'one of us' and is no threat (Farber, 2002 p. 1). It is this 'reverse' social engineering that makes use of the reciprocation trigger. The hacker presents as a helper who is ready, willing and able to fix the target's problems. Even before the problem is resolved, the target feels indebted to the hacker. This is an ideal situation for the hacker (Nelson, 2001 p. 3).

Another way that reciprocation can be used in social engineering is demonstrated by behavioural experiments. These experiments show that when two people are in disagreement, if one will yield on some point – no matter how small – the other will feel compelled to yield as well. For a hacker this is fairly easy. He or she needs only to make more than one request, then yield on one of these request and then the target will feel pressure to yield on the other (Cialdini, et al 1992 p. 38). Reciprocation is often seen and indeed encouraged in many corporate cultures. It is an unwritten 'bartering system' that is considered invaluable if one wants to be successful. One employee will help out another with the expectation that, eventually, the favour will be returned.

Deceptive Relationships - are built in order to exploit the other person. One way to do this is sharing information, a belief, or a perception and discussing it as a common enemy. Mitnick (Farber, 2002 p.1) describes when he was conning an employee who had already become suspicious of him in a different context. This time Mitnick was establishing a relationship with the employee

through email as an alias, by sharing information and technology without asking for anything in return. He also helped strengthen the relationship by talking negatively about "Kevin Mitnick" whom the employee did not realize was authoring the emails. After the relationship was established, Kevin was able to obtain all kinds of information about the target's system. Another way one can build a quick relationship is by appearing to the target as if they are both very much alike. The idea is for the victim to feel like he and the caller think alike, have the same interests or want the same things out of life. Believing that someone has characteristics identical or similar to our own provides a strong incentive to deal with that person favorably even to the extent of trusting that person without a legitimate basis – such as evidence of benign or positive conduct (Rusch, 1999 p. 6).

Diffusion of Responsibility - Diffusion of responsibility is when the target is made to feel that they will not be held solely responsible for his or her actions. Ironically, this trigger can work very well with the use of *moral duty* as a motivation for the persuasion. Moral duty is actioned when the target feels like they are doing something to save a co-worker, to help the organisation, or, at least, to avoid feeling guilt (Nelson, 2001 p. 4). The target is made to feel that they are making major decisions that will have a crucial impact for the success or failure of the company, or of the "employee" who is calling, implying that the caller may lose their job based on their decision. This can often be a very difficult decision for people to make and the target will comply more easily if they believe that they will not be held responsible for what happens.

Authority - the majority of people are conditioned to respond to authority. Rusch (1999, p6) suggests that people will do a great deal for someone they think is in authority. Consider the impact that a bogus director CEO may have on an employee who has not been prepared. This trigger is made even more powerful by the reality that it is considered a risk to challenge the caller to even verify the legitimacy of the authority. Such fear leaves this trigger wide

open for exploitation by anyone willing to represent him or herself as an authoritarian figure.

Integrity and Consistency - People tend to follow through commitments in the workplace, even though those commitments may appear to be unsound in the first place. For some it is a matter of integrity to “do what you say you are going to do”, even if you are suspicious that the request may not have been ‘quite legitimate’. Often this inclination is so strong that staff will even carry out their commitments so long as they can justify it to themselves in some way so that they believe the requests were genuinely made by their fellow employees. Another feature of the ‘Integrity and Consistency’ trigger is that people tend to believe that others express their true feelings when they make a statement. Unless there is strong evidence to the opposite, people will believe that the person with whom they are talking is telling the truth about what they feel or need. The tendency to believe others is based primarily on their own honesty in expressing feelings (Rusch, 1999 p. 7).

Common Traits

Whatever the motivation or technique used, there are certain common traits that usually entice the target to comply with the request(s). Allen (2005) suggests that these traits include:

- The movement of responsibility away from the target, so that the target is not considered solely responsible for his/her actions.
- The perception by the target that, by conforming with the request, the target will get on the 'right side' of somebody who could award them future benefits, more commonly known as "getting in with the boss".
- The target's instinct to act morally in helping someone out, thus avoiding the feeling of guilt.
- Communication on a personal level, resulting in the target voluntarily complying with the request without realizing the pressure being applied.
- The target believes he/she is making a reasoned decision in exchange for a

small loss of time and energy.

The likelihood of the target's compliance is further increased if:

- The aggressor is able to avoid conflict by using a consultative approach rather than an aggressive approach – charm vs bullying.
- The aggressor is able to develop and build a relationship through previous dealings. The target will probably comply with a large request having previously complied with smaller one.
- The aggressor is able to appeal to the target's senses, such as sight and sound. By appealing to such senses, the aggressor will be able build a better relationship with the target by appearing 'human' rather than just a voice or email message.
- The aggressor has a quick mind and is able to compromise.

Methods of Social Engineering

Social engineering is categorised into two types: *Syntactic* and *Semantic* and we briefly outline the difference below.

SYNTACTIC

Syntactic social engineering has often been referred to as the ‘second wave’ of network attacks. This is because it relates to the network’s operating logic and vulnerabilities such as loop-holes in software, denial-of-service and difficulties with cryptographic algorithms (Schneier 2001). A syntactic social engineering attack is possible due to intrinsic security failings (Barrett 1997, 43). Two popular forms of syntactic attacks include the use of *malware* and *smurfing*.

Malware - refers to the group of malicious software code which is responsible for the distribution of viruses (malicious code that is downloaded onto a computer system through the use of attachments or programs, when activated by another user), worms (malicious code that once infected on a computer

requires no human assistance to replicate and transmit itself to other systems) and trojan horses (responsible for creating backdoors in the infected computer system which can later be used by the hacker to access personal information).

Smurfing - a Denial of Service attack which uses 'pings' to test an internet host's response. This can result in a flooding of the network therefore denying access to legitimate activity. (AIC 2005, 1)

SEMANTIC

Semantic social engineering (or HUMINT, Human Intelligence) is considered to be the third and coming-wave of network attacks. It is used to target the security flaws in the people operating the computer rather than the machine itself and can be done using human-based or computer-based methods (Schneier 2001). As such, semantic social engineering attacks are also possible due to extrinsic security failures (security measures that have been implemented ineffectively) and low awareness of non-technical forms of intrusion and data gathering (Barrett 1997, 43). The social engineer may adopt different methods of manipulation accordingly.

Direct approach. A targeted individual may be asked to complete the task on behalf of the social engineer, such as making a phone call someone inside the organization asking for their password and username.

1. **Important User** by pretending to be a senior manager with an important deadline. The social engineer could pressure the help desk operates into disclosing useful information such as: telephone numbers to remote access server, type of remote access software that's used and how to configure it and what is needed to log in to the server.
2. **Helpless User.** Social engineer pretends to be somebody who is helpless, who will capitalize on somebody's helpfulness such as secretary that takes pity on them.
3. **Technical Support Personnel** by pretending to be technical support team

member social engineer could extract useful information from an unsuspecting user. Perhaps by pretending to be system engineer needing the users password to be able to 'fix something'.

4. **Reverse Social Engineer** this technique is when the legitimate user is enticed to ask the social engineer questions to obtain information. This reverse engineering attack involves *three* parts:

   sabotage in order to gain access our social engineer 'corrupts' the workstation so it appears to be faulty or corrupted. The user of the system discovers the problem and tries to seek help (and the social engineer positions themselves to help).

   marketing in order to make sure the user calls the social engineer. The social engineer must advertise, he a can do this by leaving his business cards around target's office or by placing his content number on the error message itself.

   support finally, social engineer assist resolving the problem, making sure that the user remains completely unaware and unsuspicious whilst he obtains the required information (Allen 2006).

Methods

The following is a list of some of the more common methods of human based and computer based semantic social engineering methods:

Phone - a social engineer/hacker calls up the target and presents themselves as a person of authority and uses techniques to extract the required information (Granger 2001)

Eavesdropping - a social engineer may place themselves at a known 'haunt' for employees of a particular company, to be able to overhear 'work chat' over lunch.

Live - individuals gain access to the building of the targeted computer system in order to obtain information that may later be used to access the system. Dumpster Diving and Shoulder Surfing often form a part of this technique (Guenther 2001).

Dumpster Diving - this refers to individuals sorting through a company's trash in an attempt to retrieve helpful documents i.e. employee records, organisational charts that may assist a social engineering attack (Granger 2001). Dumpster diving may also provide old computer equipment for 'forensic analysis' such as old hard drives, CDs, memory sticks etc.

Shoulder Surfing - literally looking over one's shoulder to see what password an employee is typing into the computer

Bogus Surveys - surveys that are left in the mail (usually advertising a cash prize) asking subtle questions that causes the individual to unknowingly divulge personal information that may later be used by the hacker (FCC 2002)

Pop-up Windows - false windows notifying the individual that their internet connection has dropped out and are required to re-enter their user details (username and password). This information is then redirected to the hacker (Guenther 2001)

Spyware - used to record credit card information, usernames, passwords and other forms of personal information (usually through the use of a keylogger)

Phishing - hackers distribute emails presenting themselves to be from a legitimate organisation (e.g Bank). A URL is supplied (directing them to a spoof website) and the target is informed that they are required to confirm their personal information (such as username and password). This can later be used to illegally access that person's account (AIC 2005, 09) A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online. Banks have also become regular targets. Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims. In one fairly typical case before the Federal Trade Commission (FTC), a-17-year old male sent out messages purporting to be from America Online that said there had been a billing problem with recipients' AOL accounts. The perpetrator's e-mail used AOL logos and contained legitimate links. If recipients clicked on the "AOL Billing Center" link, however, they were taken to a spoofed AOL Web page

that asked for personal information, including credit card number, personal identification numbers (PINs), social security numbers, banking numbers, and passwords. This information was used for identity theft.[15)]

Vishing - the phone version of phishing

Pharming - similar to phishing in the sense that while the user believes they are entering their personal details (username, password) into a legitimate site, they are actually using a spoofed or mimicked site which emails the user's details to the hacker for future use. Pharming however interferes with the conversion from URL to IP address by poisoning the DNS server. Therefore when an individual types in the URL of a site they are redirected to a spoof site. (De La Cuarda 2005)

Defence against Social Engineering

Most people do not realize just how much information they reveal about themselves, or the organisations that they work for, in the course of their daily discussions. Security awareness programs should include the consequences of 'loose talk'. Gragg (2002) proposes a multi-layered defence against social engineering based on a conventional approach to determine what the vulnerabilities and threats are and then defend against those risks. He suggests that 'the defence must have several layers of protection so that even if a hacker were able to penetrate one level, there would be other levels at which he or she would be stopped.' Regardless whether these are considered as layers or levels adequate awareness of the risks of social manipulation must be a basic line of defence.

Security Policy to Address Social Engineering

The foundation of information security is its policy. The security policy sets the standards and levels of security that can be applied to any network, system or environment. As social engineering targets people who need to know how to respond to requests. Any established policy must support end users to feel as

15) http://whatis.techtarget.com/definition/0,,sid9_gci916037,00.html

if they have no choice but to resist the hacker's requests. They should not be in a position where they have to question whether or not certain information can be given out. It should be well-defined beforehand by those who construct the security policy for the organisation. A security policy should address the conventional components in ICT: information access controls; setting-up accounts; access approvals; and, password changes. It should also deal with classification of documents and other media, locks, ID's, shredding policy, and the escorting of visitors; and, above all, it must be enforced (Granger, 2002a, p. 2) A Security Policy that addresses social engineering helps staff defend against the psychological triggers presented above. Policies also have a 'balancing effect' on the authority that a person may assume when they address a call on the phone. A policy defines the responsibility for information or access that when and if given out, so that there is no question as to the employee's own risk when giving away privileged information or access.

Security Awareness Training for all users

A good social engineer will first try to set up a trusted relationship. All staff must know what kind of information a social engineer can use and the kinds of conversations that could be suspicious. They should recognize confidential information and their responsibility to protect it. They also need to know that when they refuse requests they have the backing of management; this is especially important on the occasions where refusals may offend. Staff should be aware of the basic indicators present in a social engineering attack. Some of these include a refusal by the caller to give contact information, rushing, name-dropping, intimidation, misspellings, odd questions, and requesting confidential information. Employees must be willing to question the inquirer and withhold information when their challenges are met with inappropriate responses (Granger, 2002a "Combat Strategies", p.3). Security awareness training should follow the security policies, but there are some key points that all users should be aware of in social engineering:

1. **Determine Value** – Most people undervalue their data and access before

being hacked or having hardware fail. They need to consider what they would do if they suddenly had no access to their computer.

2. **Friends and Enemies** – Friends that are made through familiarity over the phone or who, for any reason, are asking questions concerning privileged information may be enemies and not friends at all. Social engineers make friends with their victims long before they request anything. All users should be aware that just because someone seems to be a friend does not mean that they can be trusted with privileged data or access.
3. **Passwords** – Some hackers will never ask for a password. However, others will come up with very convincing reasons using social manipulations as to why an employee should give their password to a complete stranger. People without security awareness often give their password away without much thought, especially when conned into providing information for a 'survey', entering into a site where they provide their password to be entered into the draw for a luxury cruise, or some other seemingly valid reason. Users will often use the same password on different systems, so a hacker that may also have obtained the victim's domain access may also gain information through other sources such as Instant Messenger and chat rooms.
4. **Uniforms and Badges** – It is easy to make fake badges and get uniforms to pretend that an intruder has a legitimate reason to be on site.
5. **Key Personnel Resistance** Key personnel include IT help desk personnel, customer service, business assistants, secretaries and receptionists and system administrators and engineers. Good resistance training will help prevent employees from being persuaded to give information that the hacker might need. Several resistance training techniques can be used from the field of social psychology to help adequately prepare employees to resist the persuasion techniques of a social engineer.

Innoculation – employees are given weakened arguments that will be used by the social engineer. It works on the same principle as preventing the spread of a disease by giving an innoculation. Employees would be exposed to the arguments that a social engineer might use along with strong refutation

argument that could be used by the employee. Studies indicate that this is an effective and long-lasting resistance technique. The concern is that the trainer must be able to anticipate the all the arguments of the social engineer (Sagarin 2002; Cialdini 1992; Serna; 2002:527**).**

Forewarning - relates to the content of an incoming message and the persuasive intent of an incoming message. Forewarning of the content of a message causes greater resistance to a social engineering attack than the forewarning of persuasive intent. The practical aspect of this training is to warn that not only will the social engineer attempt to persuade the target, but more importantly, that the arguments they use will be manipulative, deceptive, and insincere. Staff must be told that the hacker's intent is criminal and that they are intent on stealing from them. This 'black and white' definition of terminology is necessary if forewarning is to be effective (Sagarin et al; 2002, 527).

Reality check - It is important to let staff realize that they are vulnerable. Often people tend to be unrealistic about their own vulnerability believing that nobody could ever fool them. This perception leads many of them to ignore legitimate risks and fail to take measures to address those risks. However, once they have this aspect demonstrated to them, that they are vulnerable, the training outcome is much more effective (Sagarin et al; 2002, 536).

There are *three* stages of perceived susceptibility to risk:

1. Awareness
   : knowing a risk exists;
2. General Vulnerability
   : a belief in the likelihood of the risk for others; and
3. Personal Vulnerability
   : acknowledgement of one's own personal susceptibility.

Security awareness and resistance training has limited value if it is limited to only *awareness* (Sagarin et al; 2002, 540).

Memory Jogging - one exposure to security awareness training in social engineering will only be effective for a short period. Regular memory joggers or reminders are necessary to keep people aware of the dangers that may be approaching. This can be done through the use of regular reports of incidents and even no incidents; perhaps as an adjunct to a weekly business report, or a regular dedicated security newsletter.

Social Engineering Traps - are set up in the system to actually expose and stop an attack. A trap will alert the potential victim and security that an attack is in progress. Indeed from time time simulated attacks help prepare staff for common social engineering manipulations. Gragg (2005) presents several suggestions for trapping the social engineer as follows:

The Justified Know-it-all - A bold social engineer will not hesitate to walk right into an organisation and start exploring. It is imperative that all personnel be briefed on the security risks of the physical presence of a social engineer; and, they should have the power to do something quickly to deal with this un-escorted visitor. This trap is useful even if badges are used, as hackers will often make a fake badge and not expect to be confronted. In large organisations a nominated staff member can be assigned to act as a the 'designated sheep dog' to 'round-up' intruders found wandering on their floor.

Centralized Security Logs - must be monitored by information security personnel to prevent an effective attack. These are not just the access logs onto a network or system; they also include Help Desk and Customer Service requests. In fact, there should be a communications channel where a record is kept each time staff are asked to provide sensitive information; or if they are suspicious. For the central log to be an effective the log must be examined on a regular basis.

Phone-Back Policy - a simple procedure that seems to be often forgotten, makes an effective trap to block the approach from a social engineer in having a password reset. Calling back must be supported by a persons ID with

secondary and even tertiary confirmation information, only known by the company and the true identity. Again an entry in the security log should also be generated. (Farber; 2001, 1) Three other enhancements can be used to enhance the phone-back policy, or used in 'stand-alone' mode:

- The Three Questions - provides a list of questions and answers that the Help Desk personnel can use to verify identity. These questions would have been arranged earlier with the employee. The questions should be obvious for the employee but not for others.
- Call Hold - any suspicious call or any call asking for a password reset or privileged information should be put on hold. People are more easily persuaded to do something questionable when there is pressure, surprise, or overloading. The key is to take a minute and process the information that is being given, to determine if it is legitimate, needs further verification or should be denied.
- Bogus Questions - are questions that imply false information and give the caller a chance to correct or build upon the false information. An example of this type of question would be to ask 'How is your new car?' If the caller says, 'I don't have a new car' then the caller has passed a single test. At this point the employee would apologize and explain that they must be mistaken. However, if the caller starts talking about the new car, or lets the target talk about the new car, then the hacker has been hooked. The person receiving the call target should immediately notify security.

Incident Response - is critical so that the security network is not just waiting for the social engineer to find someone in the organisation that does not know or care about security. A well-defined process must exist so that any employee can immediately report an incident as soon as they suspect something is wrong. This process should actively follow the hacker and proactively inform other potential victims.

Current Trends

There has been a reported massive increase in the use of bot-nets (zombies) within the last year. Symantec reported that on average in excess of 10,000 bots were discovered every day in the first six months of 2005. This figure is double the number identified during the same period in 2004. The use of phishing as a form of social engineering (1.04 billion detected incidences) has also been reported to have nearly doubled from the first half of 2004 to the first half of 2005 (CCRC 2006). However between 2005-2006 the number of reported phishing incidences has remained relatively the same. This may be due to computer user's increased awareness of cyber crime and also the development of the new technique called pharming (CCRC 2006).

Vishing (the phone version of phishing) may also replace some phishing activity. Vishing is used to extract essential credit card information (e.g. account number, expiry date, security code) by informing the target that there has been fraudulent activity on their credit account and instructing them to call a "help line" where they are further instructed to enter their details for confirmation (CCRC 2006). These data seem to support the view that there has been a shift from nuisance hacker assaults, to profit-motivated attacks (CCRC 2006). Attacks are becoming smaller with a more focused objective. Keyloggers (programs designed to capture a computer user's keystrokes) are also becoming a more prevalent form of spyware with a 3 percent increase during the period of 2004-2005 (12%-15%) (CCRC 2006).

Future Trends

The use of bots is expected to increase in the near future (CCRC 2006). The community of Bot computers are expected to become involved in "more sophisticated, targeted attacks" (CCRC 2006). This reflects a general trend toward more focused attacks in all areas of hacker assaults. While syntactic attacks such as worms and viruses were previously spread to cause disruption and inconvenience, the use semantic social engineering methods such as bots and pharming are used to steal personal information that may be used to

access bank accounts. Therefore organised crime is expected to utilise this form of criminal activity and take a more active role in future high tech crime. Furthermore, there is expected to be a target shift from desktop computers to smart devices i.e. cellular phones, Blackberry's and other such internet linked organisers, due to user's inclination to store confidential information such as bank pins on such devices. These are expected to become the next prime target for largely semantic attacks.

The introduction of commercial appliances being linked to the internet (e.g. vending machines, gas pumps, ATM's) and the increased usage of mobiles to pay for such products suggests that this will be the target area of virus's in the future (CCRC 2006). Other non-PC devices will also be targeted. This includes routers, switches and backup devices (CCRC 2006). Furthermore, real-time programs such as IM (Instant Messaging) are likely to be increasingly targeted in the near future with a 1,700% year over year increase (CCRC 2006). There appears to be a trend towards a greater emphasis on the development of semantic/human intelligence methods rather than the previously used syntactic measures. This is due to semantic methods placing value on particular information (i.e credit card information) rather than the use of syntactic methods to release viruses and denial-of-service attacks. Human based social engineering is able to obtain information in many cases that technological methods are unable to. This further illustrates the changing trend towards profit-motivated attacks.

REFERENCES

Allan A., Noakes-Fry K. and Mogull R. (2005) 'Management Update: How Businesses Can Defend against Social Engineering Attacks'; March 16, 2005; Gartner.

Allen M. (2006) 'Social Engineering - A Means to Violate a Computer System'; June 2006; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20

Dec 2006

Australian Institute of Criminology (AIC) (2007) 'Online Auction Crime'. AIC High Tech Crime Brief, AHTCC; Canberra.

Australian Institute of Criminology (AIC) (2005a) 'Concepts & Terms' - High Tech Crime Brief (http://www.aic.gov.au/publications/htcb/htcb001.html) accessed 20 Dec 2006

Australian Institute of Criminology (AIC) (2005b) 'Phishing' - High Tech Crime Brief (http://www.aic.gov.au/publications/htcb/htcb009.html) accessed 20 Dec 2006

Barrett N. (1997) *Digital Crime: Policing the Cybernation.* Dover, NH, London: Kogan Page, UK.

Burtner W. K. (1991) "Hidden Pressures." Notre Dame Magazine, Winter 1991-92 p29-32.

Cateledge B. (2005) 'Social Engineering Overview'; University of South Carolina, Colombia, USA. (http://www.chem.sc.edu/support/publicSocial Engineering.pdf) accessed 20 Dec 2006

Chantler A.N. (2006) 'Intelligence Futures: Brace Yourself, Be Prepared to Accept the Unacceptable'; Presentation at the Annual Conference of AIPIO (Australian Institute of Professional Intelligence Officers) October 2006; Brisbane, Australia.

Choo, R.,and R.Smith, 2008, 'Criminal exploitation of online systems by organised crime groups', Asian Journal of Criminology, 3:in press.

Cialdini R. B., Green B. L. and Rusch, A. J. (1992) "When Tactical Pronouncements of Change Become Real Change: The Case of Reciprocal Persuasion" Journal of Personality and Social Psychology: Vol. 62(1), 1992, 30-40.

Computer Crime Research Centre (CCRC) (2006a) 'Hackers Replaced by Phish Con Artists'; Date: January 03, 2006 (http://www.crime-research.org/ analytics/pure-hackers-replaced-by-phish-con-artists/) – accessed 20 Dec 2006

Computer Crime Research Centre (CCRC) (2006b) 'Telephone Version of Phishing'; Date: July 13, 2006 (http://www.crime-research.org/news/13. 07.2006/2116/) accessed 20 Dec 2006

Computer Crime Research Centre (CCRC) (2006c) 'Hackers Shift Targets in

2006'; Date: March 06, 2006 (http://www.crime-research.org/analytics/1862/) accessed 20 Dec 2006

De La Cuarda, F. (2005) 'Pharming – a new technique for Internet fraud' Computer Crime Research Centre. (www.crime-research.org/news/07.03.2005/1015) accessed 1 Dec 2006

Farber, D. (2002) "Mitnick on Mitnick: 'Why I'm going legit' (Part Two) Interview with Dan Farber." ZDNet. October 8, 2002. http://www.silicon.com/public/door?6004REQEVENT=&REQINT=55863&REQSTRI1

Federal Communications Commission(2002) 'Computer Security Notice: Social Engineering'; Computer Security Week; Federal Communications Commission, USA. (http://csrc.nist.gov/fasp/FASPDocs/security-ate/De-cember-2002-2.pdf) accessed 18 Dec 2006

Federal Trade Commission (2005) 'Take Charge: Fighting back against Identity Theft'; Federal Trade Commission, Washington D.C. USA. (http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf) accessed 20 Dec 2006

Fite B.K. (2006) 'Corporate Identity Theft'; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006

Gragg D. (2002) 'A multi-Level Defense Against Social Engineering'; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006

Granger S. (2002a) "Social Engineering Fundamental, Part I: Hacker Tactics."

Security Focus Online. (http://online.securityfocus.com/infocus/1527) accessed 20 Dec 2006

Granger S. (2002b) "Social Engineering Fundamental, Part II: Combat Strategies."

Security Focus Online. (http://online.securityfocus.com/infocus/1533) accessed 20 Dec 2006

Guenther M. (2001) 'Social Engineering - Security Awareness Series'; Information Warfare Site U.K. (http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering.pdf) accessed 20 Dec 2006

Landman, J. and Petty, R. (2000) “It Could Have Been You: How States Exploit Counterfactual Thought to Market Lotteries,” Psychology & Marketing Special Issue: Counterfactual thinking. Vol. 17(4), April 2000, 299-321

MicroSoft 2007, Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws. A Study by Microsoft, November 2007, online

Nelson, R. (2001) “Methods of Hacking: Social Engineering.” Institute for Systems research, University of Maryland,

http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html) accessed 30 Feb 2006

Petty R. E., Fleming M A., Priester J. R. and Feinstein A. H. (2001) “Individual versus group interest violation: Surprise as a determinant of argument scrutiny and persuasion.” Social Cognition: Vol. 19(4), Aug 2001, 418-442.

Rusch J. (1999) ‘The Social Engineering of Internet Fraud’; United States Justice Department – Proceedings of the 1999 Internet Society Conference, USA(http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm) accessed 20 Dec 2006

Sagarin, Brad J.; Cialdini, Robert B.; Rice, William E.; Serna, Sherman B. (2002) “Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion.” The Journal of Personality & Social Psychology: Vol.83(3), Sept 2002, 526-541.

Schneier B. (2000) ‘Semantic Attacks: The Third Wave of Network Attacks’ (http://www.schneier.com/crypto-gram-0010.html#1) accessed 20 Dec 2006.

Smith R.G. (2006) ‘Preventing Identity-related Crime: 100 points, biometrics or identity cards’; AIC Trends & Issues No 324, August 2006; Canberra.

[14:00 – 15:10]

사이버범죄의 법적규제 및 대응전략

제3주제 : 사이버범죄의 최근 동향, 원인 및 대책

발표 : 정　　완 (경희대 교수)
토론 : 하 태 훈 (고려대 교수)
　　홍 승 희 (원광대 교수)

사이버범죄의 최근 동향, 원인 및 대책

정 완*

Ⅰ. 서 설

최근 사이버모욕죄의 입법을 둘러싼 찬반양론으로 사이버공간이 뜨겁게 달구어지고 있지만, 사이버공간에서 사이버모욕, 명예훼손 등 사이버폭력이 문제된 것은 이미 오래전부터였다. 필자는 이미 2005년에 정보통신부의 용역을 받아 사이버폭력 대응방안에 관한 보고서를 제출한 바 있는데,[1] 당시 사이버모욕죄의 입법이 필요하다는 의견을 제시하였으나 정부에서는 야당의 의견 등 여러 요소를 고려하여 입법을 유예하였으나 지금에 와서는 여야간 입장이 바뀐 것 같다.

사이버범죄의 최근동향을 살펴봄에 있어서 사이버범죄의 유형간 중요도에 차이가 있는 것은 아니다. 현재까지 알려진 사이버범죄 중 어느 하나라도 없어진 유형은 없으며 다만 그때그때 상황에 따라 적절한 유형의 사이버범죄가 매스컴을 타고 이슈화할 뿐이다.

최근 주목되는 사이버범죄로는 연예인의 자살사건을 둘러싸고 새삼 사이버모욕죄가 주목을 받고 있고, 새로운 인터넷사기수법으로 등장한 피싱, 특히 보이스피싱이 자주 매스컴에 언급되고 있는 상황이며, 이와 아울러 지속적으로 사이버음란물, 사이버성매매, 소프트웨어불법복제, 사이버도박 등이 문제되고 있다.

---

* 경희대학교 법과대학 교수

1) 정 완, 사이버폭력에 대한 법제도적 대응방안 연구, 정보통신부 정보통신윤리위원회 2005 참조.

본 논문에서는 사이버범죄의 개념과 원인 및 실태에 대하여 간단히 살펴보고, 최근동향으로 몇 가지 현재 이슈화된 사이버범죄 유형을 소개한 후, 그 정책적·법제도적 대응책에 대하여 살펴봄으로써 결론을 맺기로 한다.

Ⅱ. 사이버범죄의 개념과 실태

1. 사이버범죄의 개념

사이버범죄의 개념은 아직 학문적으로 정립된 것은 아니지만 일반적으로 사이버공간에서의 범죄현상을 의미한다고 할 수 있다. 과거 컴퓨터범죄, 정보통신범죄, 하이테크범죄 등의 용어가 사용되었으나 현재는 사이버범죄라는 용어가 널리 사용되고 있다.

컴퓨터와 정보통신기술의 결합으로 등장한 인터넷이라는 새로운 생활공간을 일반적으로 '사이버공간'이라고 부르는데, 그러한 새로운 생활공간에서 행하여지는 범죄적 현상에 대하여 형사법적 검토를 함에 있어서는 이론적 관점보다는 현상적 맥락에서 파악하는 용어가 타당할 것이므로 사이버공간에서의 범죄현상을 아우를 수 있는 용어로 '사이버범죄'라는 용어는 매우 적절하다. 결국, 사이버범죄란 "컴퓨터범죄를 포함하여 사이버공간에서 행하여지는 모든 범죄적 현상"을 의미한다고 하겠다.

사이버범죄의 유형은 매우 다양하지만, 사이버도박, 인터넷사기, 사이버음란물, 사이버명예훼손, 사이버성희롱 등과 같이 대체로 종래의 현실공간에서의 범죄가 무대를 사이버공간으로 옮겨 행해지는 경우가 많으며, 나머지는 해킹과 바이러스 유포, 캐릭터 및 도메인주소 침탈행위 등과 같이 사이버공간이라는 새로운 생활공간이 등장하면서 나타나게 된 새로운 범죄유형이 이에 해당한다.

2. 사이버범죄의 실태

전 세계 인터넷사용인구는 현재 10억을 돌파하였고, 국내에서도 지난 2007년말 현재 3천5백만 명을 넘어섰다. 이렇게 많은 사람들이 이용하는 인터넷 공간은 전자상거래의 발달을 포함한 많은 유익한 발전을 가져왔지만, 그 역기능으로 사이버음란물의 범람, 사이버폭력의 확산, 인터넷사기의 증가, 사이버도박의 증가 등 다양한 사이버범죄를 초래하였다. 사이버범죄의 실태를 살펴보면 다음과 같다.[2)]

사이버범죄의 최근 5년간 발생건수는 2003년도에 6만8천여 건, 2004년도에 7만7천여 건, 2005년도에 8만8천여 건, 2006년도에 8만2천여 건, 그리고 지난해인 2007년도에는 8만9천여 건으로 꾸준한 증가추세를 보이고 있다. 아래 표에서 '사이버테러형범죄'란 "정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스유포, 메일폭탄, DOS공격 등 전자기적 침해장비를 이용한 컴퓨터시스템과 정보통신망을 공격하는 행위"를 말하고, '일반사이버범죄'란 "사이버 공간을 이용한 일반적인 불법행위로서 사이버도박, 사이버 스토킹과 성폭력, 사이버명예훼손과 협박, 전자상거래 사기, 개인정보유출 등의 행위"를 말한다.[3)]

사이버범죄의 최근 5년간 발생현황 (단위 : 건)

구 분	총 계			사이버테러형 범죄			일반사이버 범죄		
	발 생	검 거		발 생	검 거		발 생	검 거	
		건 수	인 원		건 수	인 원		건 수	인 원
2003	68,445	51,722	56,724	14,241	8,891	10,047	54,204	42,831	46,677
2004	77,099	63,384	70,143	15,390	10,993	11,892	61,709	52,391	58,251
2005	88,731	72,421	81,338	21,389	15,874	17,371	67,342	56,547	63,967
2006	82,186	70,545	89,248	20,186	15,979	17,498	62,000	54,566	71,750
2007	88,847	78,890	88,549	17,671	14,037	15,302	71,176	64,853	73,247

2) 경찰청 사이버테러대응센터 2007년 12월 31일까지의 통계자료.
3) 사이버테러대응센터 홈페이지 http://www.ctrc.go.kr 참조.

사이버범죄의 발생에 따른 유형별 검거인원 역시 2003년도에 5만2천여 명, 2004년도에 6만3천여 명, 2005년도에 7만2천여 명, 2006년도에 7만여 명, 2007년도에 7만9천여 명 등으로 꾸준한 증가추세를 보이고 있다.

사이버범죄의 유형별 발생현황 (단위 : 명)

구분	총계	해킹 바이러스	인터넷 사기	사이버 폭력	불법 사이트운영	불법복제 판매	기 타
2003	51,722	8,891	26,875	4,991	1,719	677	8,569
2004	63,384	10,993	30,288	5,816	2,410	1,244	12,633
2005	72,421	15,874	33,112	9,227	1,850	1,233	11,125
2006	70,545	15,979	26,711	9,436	7,322	2,284	8,813
2007	78,890	14,037	28,081	12,905	5,505	8,167	10,195

한편, 경찰청과 별도로 검찰청에서 처리하고 있는 사이버범죄의 단속실태는 인터넷범죄수사센터가 공개한 컴퓨터범죄의 유형별 처리현황에 제시되어 있다. 1997년부터 2005년까지의 기간 동안 제시된 사이버범죄의 단속건수를 보면 공용전자기록손상등, 전자문서관련죄, 전산업무방해죄, 전자기록비밀침해죄, 컴퓨터사용사기죄, 전자기록손괴죄, 정보통신망법위반죄, 개인정보보호법 위반죄, 기타 특별법 위반죄 등으로 유형을 분류하여 통계가 제시되어 있는데, 1997년도에 132건 232(71)명, 1998년도에 195건 354(82)명, 1999년도에 326건 500(64)명, 2000년도에 802건 1,074(122)명, 2001년도에 2,353건 3,143(331)명, 2002년도에 5,722건 7,198(990)명, 2003년도에 12,501건 15,575(1,745)명, 2004년도에 11,685건 15,814(1,104)명, 2005년도에 12,672건 19,234(1,766)명 등으로 꾸준한 증가추세를 보이고 있으며, 9년간 총 46,388건에 63,124명 입건, 6,275명 구속으로 나타나고 있다. 특히 사이버범죄의 기본법률이라고 할 수 있는 정보통신망 이용촉진 및 정보보호에 관한 법률 위반사범의 숫자는 크게 높아 9년간 총 25,568건에 32,601명 입건, 1,422명 구속으로 나타났다.

컴퓨터범죄의 구성요건별 처리현황(1997년~2005년)

범죄유형	처리현황		
	기간	건수	인원수(구속자수)
공용전자기록손상등	1997~2005	5	10(1)
전자문서관련죄	1997~2005	4,194	8,360(1,705)
전산업무방해	1997~2005	215	290(35)
전자기록비밀침해	1997~2005	45	67(4)
컴퓨터사용사기	1997~2005	7,653	9,345(2,407)
전자기록손괴	1997~2005	71	89(5)
정보통신망법	1997~2005	25,568	32,601(1,422)
개인정보보호법	1997~2005	563	1,078(64)
기타 특별법	2003~2005	8,074	11,284(632)

컴퓨터범죄의 연도별 발생현황(1997년~2005년)

연도별 컴퓨터범죄 발생현황	1997	132	232(71)
	1998	195	354(82)
	1999	326	500(64)
	2000	802	1,074(122)
	2001	2,353	3,143(331)
	2002	5,722	7,198(990)
	2003	12,501	15,575(1,745)
	2004	11,685	15,814(1,104)
	2005	12,672	19,234(1,766)
	계	46,388	63,124(6,275)

Ⅲ. 사이버범죄의 특징과 원인

사이버범죄는 주로 다음과 같은 특징에 기인하여 발생한다.

첫째, '비대면성'이다. 사이버공간은 컴퓨터를 이용하여 인터넷을 매개로 하여 형성되는 생활공간으로서 불가시적이므로 현실세계와는 달리 행위자들이 자신의 얼굴을 드러내지 않고 행동한다는 특징을 갖고 있다. 따라서 그곳에서의 모든 범죄행위도 행위자가 전혀 모습을 드러내지 않는 상태에서 행하여진다. 사이버범죄의 이러한 비대면성으로 인하여 범죄자들은 보다 과격하고 대담하게 행동하게 되어, 얼굴을 맞대고 있으면 하기 어려운 행동을 하는 경우가 많다. 예컨대 자신이 노출된 상태에서 상대방과 얼굴을 맞대고 있는 경우에는 할 수 없는 성적 표현이나 명예훼손적 발언을 하게 되어 사이버성폭력이나 명예훼손 또는 협박 등을 하기가 용이해진다. 또한 이러한 비대면성은 책임의식의 결여로 이어져 인터넷사기를 유발하는 계기가 될 수 있다. 비대면성으로 인하여 피해자는 행위자를 거의 알 수 없어 범인파악이 어렵게 되고 피해의식이나 공포감이 훨씬 커지게 된다.

둘째, '익명성'이다. 사이버공간에서는 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 인적 사항이나 ID를 도용하면 완벽하게 자신의 익명성을 보장받을 수 있다. 이러한 이유로 사이버공간을 '익명의 바다'라고 부르기도 한다. 이와 같이 자신을 숨길 수 있는 익명성이 보장되면 범죄의 유혹에 쉽게 빠져들 수 있다. 컴퓨터바이러스의 제작·유포, 해킹, 음란물의 유포·전시 판매, 인터넷사기 등은 바로 이러한 익명성으로 인하여 행위자들이 쉽게 빠져들 수 있는 범죄들이다. 이러한 익명성은 수사기관이 범죄자를 발견하는데 많은 어려움을 주고 있다.

셋째, '전문성과 기술성'이다. 사이버범죄 중에는 컴퓨터와 인터넷에 대하여 약간의 지식과 기술만 습득하면 범할 수 있는 것도 있지만, 프로그램조작을 통한 재산취득, 바이러스의 제작·유포, 해킹과 같은 사이버범죄는 고도의 전문적인 지식과 기술을 갖추고 있어야만 가능하다. 물론 최근에는 바이러스를 제작할 수 있는 프로그램을 이용하여 쉽게 만들어진 바이러스가 유포되기도 하지만 여전히 이들 범죄는 상당한 실력을 갖춘 네티즌들만이 범할 수 있다. 사이버범죄의 이러한 전문성과 기술성으로 인하여 수사기관은 고도의 전문적 기술을 가진 전문수사관을 반드시 필요로 하게 된다.

넷째, '시간적·공간적 무제약성'이다. 사이버공간에서의 생활은 시간과 공간의 제약을 거의 받지 않는다. 누구든지 마음만 먹으면 인터넷을 24시간 내내 이용할 수 있으며, 별다른 어려움 없이 세계 어느 곳에 있는 인터넷사이트에도 접속할 수 있다. 사이버공간의 이러한 시간적·공간적 무제약성은 사이버범죄자들에게 엄청나게 많은 범죄의 기회를 제공하고 있다. 즉, 범죄자는 인터넷이 연결된 곳이면 지구 반대편에 있는 나라의 컴퓨터에도 바이러스를 유포할 수 있고 해킹도 할 수 있다. 실제로 우리나라에서 발생한 해킹사건의 대부분이 해외에서 국내로 침입한 것이며, 외국 해커들의 상당수가 우리나라를 경유지로 활용하고 있다고 한다. 사이버범죄의 이러한 특징은 사이버범죄 수사에 사실상·법률상의 많은 어려움을 안겨 주고 있을 뿐만 아니라 국제형사사법공조의 필요성을 던져 주고 있다.

다섯째, '빠른 전파성과 엄청난 재산피해'이다. 수많은 컴퓨터가 네트워크화되고 인터넷을 통해 시공을 초월하는 사이버공간을 형성함에 따라 사이버공간에서는 시간과 장소의 제약을 뛰어 넘어 모든 정보가 매우 빠르게 전파된다. 즉 사이버공간에서의 명예훼손적 표현이나 음란물 또는 바이러스는 순식간에 전세계에 널리 유포될 수 있으며 그에 따라 범죄로 인한 피해가 매우 광범위하게 미치게 된다. 특히 바이러스와 해킹에 의한 시스템 작동불

능은 경우에 따라서는 시스템에 연결된 모든 컴퓨터의 작동을 멈추게 함으로써 업무 전반을 마비시키는 심각한 결과를 초래하여 천문학적 재산피해를 야기하게 되며, 불특정다수를 상대로 하는 인터넷사기도 광범위한 피해를 야기한다.

Ⅳ. 사이버범죄의 최근동향

1. 사이버모욕 등 사이버폭력

최근 인터넷을 통한 정보전달 등 유통이 매우 활발해지고 있어 인터넷의 발달전망을 밝게 하고 있지만, 이와 함께 각종 뉴스에 등장하는 개별 사건마다 인터넷이용자들의 활발한 개인적 의견이 댓글 등의 형태로 제시됨에 따라 욕설이나 모함 등 근거 없는 각종의 모욕 또는 명예훼손행위가 크게 늘고 있어 크게 사회문제화하고 있다.[4)]

최근 자살하여 연예인을 대상으로 한 악성댓글의 피해를 크게 부각시키는 계기가 된 최진실 자살사건이 우리의 주목을 끌고 있고, 과거 야당 당수나 대통령 등 유명정치인을 대상으로 한 사진합성물에 의한 명예훼손 행위가 우리를 놀라게 하였을 뿐 아니라 연예인 X파일 공개 및 유포에 의한 명예훼손사건, 간호사들의 신생아 학대사진 유통 사건, 개똥녀 사건, 된장녀 사건, 군삼녀 사건 등 하루가 멀다 하고 우리의 관심을 끄는 사이버폭력 사례가 인터넷 등 사이버공간을 장식하고 있는 상황이다.

악성댓글 등에 의한 최근의 주요 피해사례를 도표로 정리하면 다음과 같다.[5)]

---

4) 사이버폭력의 실태와 법제도적 문제점에 대한 상세한 내용은 정 완, 사이버폭력에 대한 법제도적 대응방안 연구(정보통신윤리위원회, 2005) 참조.

5) 박종현, “사이버폭력 피해구제제도 현황 및 문제점” 2005.7.21 정보통신윤리위원회 세미나 발표자료에 일부 첨삭함.

<게시물, 댓글 등에 의한 최근 피해사례>

사건명	일 시	내 용
최진실 사건	2008	톱 탤런트 최진실이 자살을 하였는데 그녀에 대한 인터넷상의 악성댓글이 그 주요원인의 하나로 언급되었음. 특히 가수 유니, 탤런트 정다빈도 악성댓글을 못 견뎌 자살한 것으로 알려진 터라 더욱 주목을 받았고, 이른바 '최진실법' 제정논란을 야기하였음.
군삼녀 사건	2007	남성들의 군복무기간에 관한 한 여학생의 인터뷰 내용이 실명과 동영상으로 알려지면서 이 여학생에 대한 무차별적 폭언이 댓글로 행해져 이 여학생의 정신적 피해가 큰 것으로 보도됨.
된장녀 사건	2006	사치스런 생활을 하는 여성들에 대한 비난성 댓글에 의한 사이버폭력이 도를 지나치고 있음
MBC 음악캠프 나체 시위 장면	2005.8	MBC 음악캠프라는 프로그램에서 출연가수 일부가 나체로 시위를 한 내용의 비디오물이 인터넷을 통하여 확산되고 있어 추가 피해가 우려되고 있음
개똥녀 사건	2005.6	지하철에서 애완견의 배설물을 치우지 않은 여성 사진 및 동영상 유포
체별여교사 자살 사건	2005.4	체벌 혐의를 받은 여교사가 자살하자 체벌 사실을 알렸던 학생들이 가출한 사건
신생아 학대사건	2005.4	간호사들이 자신의 홈페이지에 올린 신생아 학대사진이 유포되어 문제됨
트위스트김 사건	2005.4	연예인 트위스트킴이 음란사이트의 운영자로 몰려 피해
연예인 X파일 사건	2005.1	유명연예인 99명의 신상정보를 담은 미확인 사실이 유포됨
왕따 동영상 사건	2004.2	왕따동영상이 촬영된 중학교의 교장이 자살

사이버모욕이나 사이버명예훼손 등 타인의 정신적 공황을 가져오는 범죄를 이른바 '사이버폭력' 범죄로 부르는 경우가 많다. '사이버폭력'이란 아직 확정된 개념은 아니며 다의적이고 논쟁적인 개념이다. 대체로 사이버공간에서 행해지는 온갖 형태의 폭력적 표현행위를 포함하는 개념이라 하겠다.

사이버폭력의 일반적 사례로는 특정인에 대하여 모욕적인 언사나 욕설 등을 게시판에 올리거나 메모 또는 채팅 상에서 행하는 '사이버모욕', 특정인에

대한 허위의 글이나 명예에 관한 사실을 인터넷게시판 등에 올려 불특정 다수인에게 공개하는 '사이버명예훼손', 인터넷상에서 음란한 대화를 강요하거나 성적 수치심을 주는 대화로 상대방에게 정신적 피해를 주는 '사이버성희롱', E-mail로 특정인 또는 불특정 다수인에게 음란·폭력적인 내용의 글 또는 영상물을 발송하는 '음란스팸메일', 인터넷 또는 PC통신상의 대화방, E-mail 등 정보통신망을 이용하여 특정인에게 원하지 않는 접근을 지속적으로 시도하거나 성적 괴롭힘을 행사하는 '사이버스토킹', 인터넷이나 PC통신망의 대화방을 이용하여 원조교제를 유도하거나 알선·중개하여 10대 매매춘을 확산시키는 '사이버성매매', 유명연예인의 몰래카메라 등 현실세계에서 만들어진 내용을 유통시키는 '사이버음란물' 등을 들 수 있다.

■ 사이버 폭력 피해 상담내용 분석(2001 - 2007. 3)

(단위 : 건)

구 분	계	피 해 내 용			
		명예훼손(모욕)	성폭력	스토킹	기타
2001	1,054	278(33)	204	22	550
2002	3,616	1,248(115)	224	53	2,091
2003	4,217	1,916(894)	557	95	1,649
2004	3,913	2,285(979)	322	81	1,225
2005	8,406	5,735(1,802)	889	193	1,589
2006	7,050	4,751(1,641)	968	184	1,147
2007. 3	1,361	923(422)	125	36	277
합계	29,617	17,136(5,886)	3,289	664	8,528

사이버공간은 빠른 전파력이 특징인데다 익명성이 상당부분 보장돼 정치인이나 연예인 등 유명인뿐 아니라 누구나 폭력의 희생양이 될 수 있다는 점에서 이 같은 사이버폭력에 관한 문제의 심각성이 더해지고 있다. 아래에

예시한 방송통신심의위원회(구 정보통신윤리위원회) 통계자료에 따르면 사이버폭력 피해상담 건수가 해마다 늘고 있고 그 주요내용은 명예훼손 또는 모욕에 관한 것으로 나타나고 있다.[6]

2. 피싱사기

인터넷사용이 보편화되면서 각 개인의 인터넷상 금융거래정보를 노리는 범죄자들이 늘어나게 되었다. 금융정보 등 타인의 개인정보를 절취하는 방법에는 종래 '해킹'이 유력하였고 기타 여러 가지 방법이 있겠으나, 최근에는 피해자의 방심을 이용하여 직접 피해자로부터 금융정보를 얻는 이른바 '피싱'(Phishing)이라는 수법이 사용되고 있다. 피싱이란 "피싱공격자가 위장된 금융기관 등의 웹사이트나 전자메일로 고객을 현혹하여 이들로부터 인증번호나 신용카드번호, 계좌번호 등 금융정보를 취득한 후, 이를 불법적으로 이용하여 고객에게 재산상의 손해를 입히는 신종 인터넷사기"이다.[7]

그런데 인터넷을 이용한 피싱 수법에서 한 걸음 더 나아가 아예 피해자에게 전화를 걸어 금융기관, 수사기관 등을 사칭한 뒤 직접 개인정보를 물어보거나 송금을 하게 하는 이른바 보이스피싱(Voice Phishing)이 많아져 크게 사회문제화되고 있다.[8] 보이스피싱은 무작위로 전화를 걸기보다는 인터넷사이트 등에서 입수한 개인정보를 기초로 범행이 이루어지고, 이러한 보이스피싱에 의하여 많은 사람들이 피해를 입게 되는바, 중요한 문제는 보이스피싱을 통해 '고액의 현금'을 인출당하는 피해자가 속출하고 있다는 점이다. 그리

---

6) 정보통신윤리위원회 홈페이지 http://www.kiscom.or.kr 통계자료 참조.

7) 한국의 피싱피해는 외국에 비해 크지 않은데 그 이유는 전자금융거래에 공인인증서를 사용할뿐더러 비밀번호와 보안카드 사용 등 여러장치가 복합적으로 사용되어 다른 나라보다 안전하기 때문이다. 정 완, "인터넷사기의 최근동향" 형사정책연구소식 95호(2006.6), 36쪽 참조. 참고로 독일의 인터넷뱅킹의 경우에는 계좌번호, 비밀번호, 송금번호만 알면 계좌이체에 아무 문제가 없다고 한다.

8) 2007년 10월 국정감사 자료에 의하면 2006년 6월 ~ 2007년 7월 전화사기 피해는 4천235건이고 피해액은 399억원에 이른 것으로 조사됐으나, 일선 경찰서에서 보이스피싱 발생보고가 제대로 된다면, 이보다 훨씬 큰 규모임을 짐작할 수 있다.

고 피해자의 상당부분은 세상 물정에 어두운 서민층이며, 따라서 피해자가 사기를 당한 후 이를 비관하여 자살하거나 신체적으로 환청에 시달리는 등의 부작용도 발생하고 있다.

최근에는 가족이 납치당한 것처럼 가장하는 수법 또는 국민연금관리공단, 법원, 금융기관, 경찰서 등을 사칭하여 세금 환급, 신용카드 대금 연체, 출석 요구, 연금 환급 등을 빌미로 송금을 요구하거나 개인정보와 금융정보를 수집하는 경우가 많다. 또한 이들은 상당한 조직을 갖추어 범행에 임하고 있는바, 예컨대 콜센터 운영은 중국에서, 현금송금과 대포통장 개설은 한국에서 하는 등 그 역할이 분담되어 있어 단순 국내범죄가 아닌 국제범죄의 성격을 띠고 있어 더 큰 문제가 되고 있다.[9]

3. 사이버음란물 유통

요즘 인터넷에는 유명연예인들의 성관계장면이 녹화된 동영상이나 국내외에서 제작된 몰래카메라 동영상을 비롯한 수많은 음란 화상 및 동영상들로 가득 차 있고 이를 손에 넣기 위하여 많은 청소년 및 성인들이 시간을 헛되이 보내는 등 중독증세를 보이고 있어 우리 사회를 크게 병들게 하고 있다.[10]

또한 청소년들 사이에서 많이 이용되고 있는 화상채팅에 있어서도 음란화상과 동영상을 주고받는 행태가 계속 늘어나고 있으며, 또한 이메일의 역기능으로 크게 사회문제가 되고 있는 스팸메일의 증가에 있어서도 음란메일이 크게 한 몫을 하고 있는 점들을 언급하지 않을 수 없는 상황이다.

최근에는 UCC의 범람추세와 함께 대형 포털사이트에마저 음란동영상이

9) 보이스피싱의 문제점과 대응방안에 대하여는 정 완, “보이스피싱 대응체제의 문제점과 대책” 수사연구 298권, 2008.8 33쪽 이하 참조.

10) 사이버음란물의 유통과 규제에 관한 다양한 내용에 대하여는 정 완, “사이버공간상 음란물 유통의 심각성과 법적 규제”, 경희법학 2007.6; 정 완, “사이버음란물의 유통과 규제” 형사정책연구 2000.3 등 참조.

장시간 게재되는 사건이 잇따라 발생되어[11] 정부, 포털사이트 사업자, UCC 사업자 등이 대책회의를 통하여 사이버음란물 차단대책을 발표하고 있는 상황이다.[12]

이와 같이 사이버공간에 넘쳐나는 음란물에 대한 보다 효과적인 대응책이 매우 절실한 상황이지만, 최근 미국 연방법원이 인터넷포르노금지법에 대하여 표현의 자유를 규정한 헌법을 위반하였다는 판결을 내린 바에서도 알 수 있는 바와 같이 사이버공간상의 음란물에 대한 정부차원의 대응은 매우 힘든 것이 사실이다.[13]

4. 사이버성매매의 증가

최근 집창촌 등에 대한 성매매 단속을 강화하자 각종 변종 성매매가 오히려 늘어나고 있다.[14] 경찰청 자료 '성매매 집결지 현황(2005년~2008년 9월)'에 따르면, 집결지 업소 수는 2006년 1097개에서 지난해 995개, 올해 9월 현재 935개로 줄었으며, 종업원 수는 2006년 2663명에서 지난해 2508명, 올해 9월 현재 2282명으로 감소했지만, 성매매 사범은 매년 크게 늘어난 것으로 나타났다.[15]

이와 같이 전통적 형태의 집창촌이 쇠락하자 '변종 성매매업소'와 '사이버

11) 경향신문 "유명 포털에 포르노동영상 6시간 노출, 물의" 2007.3.19자 기사 및 머니투데이 "네이버, 다음에서도 음란물 노출사고" 2007.3.21자 기사 등 참조.

12) 첫째, 정부와 민간업체의 모니터링 및 대응 체계 강화, 둘째, 해외사이트에 대한 기술적 차단 강화, 관리 소홀 사업자에 법적 제재 강화, 넷째, 이용자·사업자의 자율적 책임의식 강화, 다섯째, 대국민 캠페인 등 인터넷 윤리의식 확산 등이 그것이다. 정보통신부 2007.3.26자 보도자료 "정부, 민간인터넷업체와 함께 음란물 차단에 적극 나서기로" 내용 참조.

13) 미국 연방법원은 2007년 3월 미성년자의 사이버음란물 접근을 허용한 음란사이트 운영자를 처벌하는 내용의 아동온라인보호법(Child Online Protection Act, 1998)이 헌법상 표현의 자유를 침해한다고 판결하였다. 뉴시스, "미법원, 아동온라인법에 위헌판결" 2007.3.23자 기사 및 한국일보, "포르노규제보다는 표현의 자유가 우선" 2007.3.23자 기사 등 참조.

14) 이하 자료내용은 뉴시스 2008.9.30자 "성매매 사범 검거는 매년 증가…구속은 떨어져" 기사 참조.

15) 경찰청 자료 '성매매사범 단속현황(2005~2008년 6월)'을 보면, 검거인원은 2005년 18,508명, 2006년 34,795명, 2007년 39,236명, 2008년 상반기 20,407명으로, 성매매업주(알선자), 성매수자, 성매매 여성이 모두 증가하였다.

성매매'가 최근 급증하고 있는 것으로 나타났다. 경찰청 자료에 따르면, 풍속영업소는 2005년 132,553개소에서 올해 8월 현재 169,104개소로 증가했다. 이 중 변종 풍속영업소 등은 2005년 5,841개소에서 2006년 8,714개소, 2007년 31,601개소, 올해 8월 현재 32,950개소로 최근 급격히 증가하고 있는 것으로 나타났다.

사이버 성매매 문제는 더욱 심각한 수준인 것으로 조사됐다. 방송통신심의위원회의 '불건전만남 유도신고센터 신고접수 현황'에 따르면, 지난해 접수된 신고건수는 총 1만2264건으로 전년도에(2648건)에 비해 4.6배나 급증했다.[16]

정책당국은 성매매 사범단속의 성과를 크게 홍보하고 있지만, 실제 성매매 사범은 매년 증가하는 반면 구속률은 오히려 줄어들고 있고 특히 청소년 및 노인 성매매가 급증하고 있음에도 정부의 예방정책은 전무한 실정이고, 사후 단속처벌 중심의 대응으로 일관하고 있는 점은 큰 문제라고 할 수 있다.

여성부, 법무부, 교육과학기술부, 보건복지가족부 등 관련부처 모두가 성매매 방지 및 단속을 위한 긴밀한 협조체계를 구축해야 하며 무엇보다 건전한 성문화의식을 우리사회에 정착시키고 신체의 존엄성을 알리는 생명교육을 강화하는 노력이 중요하다고 하겠다.

5. 사이버도박

인터넷을 이용한 도박장 개설과 도박행위는 수사기관의 꾸준한 단속활동에도 불구하고 지속적으로 늘고 있다. 이들 도박업체들은 대체로 태국, 중국, 홍콩 등 외국에 서버를 설치하고 국내인들을 대상으로 도박사이트를 운영하여 수익을 올리는 형태를 취하고 있다.

---

16) 이를 연령대별로 살펴보면, 30대가 9605건(52.5%)으로 가장 높았고, 20대 4063건(22.2%), 40대 2428건(13.3%), 50대 이상 1346건(7.4%)의 순이었다. 변종 성매매 '불건전만남 사이트'에 대한 심의 결과(1만7759건)에 따르면, 시정요구는 8164건, 청소년유해정보 결정은 121건으로 나타났으며, 2007년도에는 전년 대비 심의건수가 4.3배, 시정요구건수가 25.4배나 증가했다.

최근에도 도박사이트 운영자, 장애인 바지사장 알선책, 도박사이트 개발관리업체 대표, 관련 조직폭력배 등이 한꺼번에 구속된 사건이 발생하였는데, 이들은 태국(파타야)과 중국 연길에 설치한 콜센터(가맹 PC방에 대한 사이버머니 충전 및 자금 정산)를 이용, 불법으로 인터넷 도박사이트인 엠비게임 등을 운영하면서 경기지역에 수백개의 PC방을 모집, 도박사이트의 사이버머니를 환전하게 해 주면서 손님의 배팅 금액당 일정액을 수수료로 공제, 가맹 PC방 및 총판과 배분하는 방법으로 도박을 개장해 수억 원의 이익을 챙겼다고 한다.[17] 이번 사건에서는 장애인 바지사장 알선책과 바지사장 공급책, 전 다단계판매원 등과 함께 공모해 단속시 관대한 처벌을 받는다는 점을 이용하여, 가맹 PC방 업주로 장애인 등 바지사장 수십명을 내세워 허위조사를 받게 한 뒤 수익금을 나눠 가진 것으로 밝혀져 도박사이트 운영자체도 매우 지능화되고 있음을 알 수 있다. 특히 도박사이트 운영과정에서 주변 폭력조직으로부터 보호비 명목으로 상당금액을 갈취당한 것으로 드러나, 추후에는 사이버도박의 수사를 함에 있어서도 조직폭력배들에 대한 수사를 함께 행해야 하는 상황이 되었다.[18]

한편 2년 전 게임장을 중심으로 도박을 유행시켜 전국적으로 물의를 일으켰던 '바다이야기'가 현재 인터넷상에서 크게 이용되고 있어 다시 사회문제로 되고 있다. 과거의 바다이야기 게임장은 지정된 장소에서 이뤄져 피해자는 대부분 성인남성이었지만, 인터넷 도박의 피해대상은 남녀노소를 가리지 않고 있어 문제가 더욱 심각하다. 경찰청은 지난해 정보통신정책연구소가 파악한 1,600여개 도박사이트 중 현재까지 141개만을 파악·단속하고 있는 실정이라 무분별하게 늘어나는 사이트를 단속하기에는 턱없이 부족한 현실이다.[19] 경찰청 사이버 수사팀이 2004년 679명에서 2008년 900명으로 전담인

17) 뉴시스 2008.10.13자 "검찰, 인터넷도박 조직 143명 적발" 기사 참조.
18) 사이버도박에 관한 사례와 실태 및 대응방안 등에 대하여는 정 완, "사이버도박의 사례와 대응", 형사정책연구소식 2001.6; 정 완, "인터넷도박의 실태와 대응" 경희법학 41권 2호 2006.12 등 참조.
19) 경찰청 국정감사 자료에 의하면 '온라인도박 검거건수'는 2004년 64건, 2005년 277건이었던 것이 2006년 5,874건, 2007년 2,714건, 2008년 8월 현재 2,406건으로 폭발적으로 증가하고 있다. 아이뉴

력을 늘리기는 하였으나 우후죽순 늘어나는 인터넷 도박을 인력충원 만으로는 감당하기 어려우므로, 현재의 도박사이트 발견에서 검거까지 함께 하는 수사방식을 탈피해 네티즌들에게 제보를 받고 현장을 검거하는 방식 등 보다 효율적인 방법을 제도적으로 도입하여 사이버도박을 시급히 근절할 필요가 있는 상황이다.

6. 소프트웨어 불법복제

BSA(Business Software Alliance, 사무용소프트웨어연합회) 2007년도 보고서[20]에 따르면 전 세계의 소프트웨어 불법복제율은 35%로 3년 연속 동일한 수준이며, 중간 불법복제율은 62%이다. 이는 조사대상국의 절반 이상의 불법복제율이 62%이상이라는 의미이다.

구 분	불법복제율(%)	손실액 (백만달러)
2003년	36 %	28,803
2004년	35 %	32,711
2005년	35 %	34,297
2006년	35 %	39,576

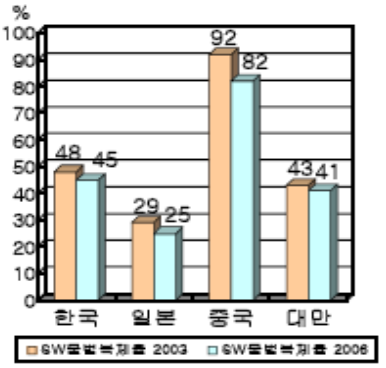
전세계의 2006년도 소프트웨어 불법복제율은 전년도에 대비하여 아시아태평양, 중동/아프리카 지역에서 증가하였으며, 중/동부유럽, 라틴 아메리카, 서부 유럽 지역에서는 감소하였고, 북미지역은 동일하다. 아태지역은 15개국 중 11개국에서 불법복제율이 하락했으나, 2006년 중국과 인도의 아시아시장 점유율이 늘어나 아태지역 전체의 불법복제율[21]은 증가하였다.

스24 2008.10.4자 “인터넷도박사이트 1,600개 달해” 기사 참조.

20) 2007년 발표 BSA/IDC SW불법복제율보고서 참조.

21) 54%에서 55%로 증가하였다.

한국의 2006년도 불법복제율은 45%로 매년 꾸준히 감소해오고 있다. 이는 미국(21%), 영국(27%), 일본(25%) 등 선진국과는 상당한 격차가 있는 반면, 같은 아시아지역 내의 중국(82%)보다는 월씬 낮은 수치이다. 참고로 한국, 일본, 대만, 중국 등 아시아지역 주요국가의 소프트웨어 불법복제율을 2003년과 2006년을 비교하여 살펴보면 다음 도표와 같다.



국내의 불법복제율은 50%보다 약간 더 높게 나타나고 있으며 이는 기업과 기관의 불법복제율만을 계산하였을 때의 수치이고, 개인의 불법복제율(75%)을 반영하면 전체 불법복제율은 60%에 이르는 것으로 나타났다. 개인의 경우 4명중 3명은 불법복제 소프트웨어를 이용하고 있다는 뜻이 된다. 이처럼 많이 이용되고 있는 불법복제소프트웨어는 친구나 동료로부터 얻는 경우가 50%를 넘고, 컴퓨터를 구입할 때 미리 설치하는 경우가 20%, 인터넷을 이용하여 얻는 경우가 10% 정도로 나타나고 있지만, 최근에는 접근이 손쉬운 인터넷을 통한 불법복제(다운로드)가 급격히 늘고 있는 추세여서 그 심각성을 더해가고 있다. 인터넷을 통한 불법복제경로는 이른바 와레즈(Warez) 사이트에서 다운로드하는 경우(30%)와 소리바다 등 P2P 방식의 다운로드(30%)가 중심을 이루고 있고, 기타 팝폴더, 웹하드, PD박스 등 개인정보 저장공간을 이용하거나 FTP에 의한 전송 등에 의해서도 불법복제가

많이 행해지고 있다.[22]

최근 연구조사[23]에 의하면 일일 평균 조회 수 및 다운로드 수를 근거로 불법소프트웨어 유통에 따른 손실액을 산정한 결과 3개의 웹 하드에서만 연간 11,736백만원에서 최대 16,756백만원 규모의 소프트웨어가 공유되고 있는 것으로 나타났다. 이를 근거로 소프트웨어 공유가 이루어지고 있는 35개 국내 주요 웹 하드 업체에서 발생하는 전체 손실액을 추정한 결과 연간 700억원에서 985억원 규모에 달했다. IDC에서 보고한 2006년 우리나라의 소프트웨어 불법복제에 따른 연간 손실액 440백만달러(약 4천8십억원)와 비교하면 전체 소프트웨어 불법복제 손실액의 약 20%에 해당하는 것으로 파악됐다.[24] 이러한 연구결과는 광랜 보급확대 및 웹하드 등 인터넷을 통한 불법복제가 광범위하게 확산되고 있음을 알 수 있다.

Ⅴ. 사이버공간 규제와 '표현의 자유'

1. 사이버범죄의 특수성

사이버공간을 통하여 발생하는 각종 사이버범죄는 현실공간에서 행해지는 범죄행위와는 여러 가지 면에서 그 차별성이 인정된다. 예컨대 현실공간에서의 모욕이나 명예훼손은 한정된 공간에서 행해지고 그 피해의 확산도 그다지 심각하지 않다고 할 수 있고, 따라서 가해자와 피해자간의 해결에 의하여 사건이 마무리되는 것이 보통이다.

---

22) 소프트웨어 불법복제에 대한 실태와 문제점 및 대응방안에 대한 상세한 내용은 정 완, 소프트웨어 불법복제실태와 법제도적 개선방안, 한국형사정책연구원 보고서 2003 참조.

23) 정보통신정책학회, 온라인상의 콘텐츠 공유에 따른 소프트웨어 저작권 침해 실태 및 경제적 손실액 추정에 관한 연구, 2007.12 참조.

24) 차태원, "온라인상의 소프트웨어 불법복제 피해현황 및 신고센터운영", Enter 145권 2007.12, 9쪽 참조.

그러나, 사이버공간에서 행해지는 각종 유형의 사이버범죄는 그것이 일단 발생하면 순식간에 인터넷을 이용하는 모든 사람들에게 무제한적으로 퍼지게 되어 피해자가 입은 인격적 침해나 명예훼손의 피해는 이루 말할 수 없이 크고 회복불가능한 상태에 빠지게 된다.

또한 사이버공간의 특성인 익명성에 의하여 사이버범죄는 실명으로 나타나지 않기 때문에 사이버범죄자가 누구인지 특정하기가 매우 어렵고 퍼나르기에 의한 무수한 공범자들이 존재하므로 범죄피해에 대한 신고나 고소, 고발이 매우 어려운 특징을 가지고 있다.

아울러 이러한 사건들을 지켜보는 수많은 네티즌들은 보고 싶지 않고 알고 싶지도 않는 사건들에 대하여 수많은 사람들이 피해자를 공격하는 폭력적 언사를 두 눈 뜨고 지켜볼 수밖에 없으며 관련 사진이나 각종 증거물이 인터넷을 뒤덮어 인터넷은 그야말로 쓰레기 공간으로 변해버리기 일쑤인 것이다.

이러한 사이버공간 및 사이버범죄의 특수성은 형법상의 종래의 범죄구성요건으로는 처벌하기 어려운 '특별하고 새로운 범죄'임을 보여주고 있으나 우리의 법적 규제 현실은 이를 따라가고 있지 못하며 막연한 '표현의 자유' 침해가 우려된다는 주장에 막혀 건전한 사이버문화 조성에 어려움을 겪고 있는 것이 현실이다.

2. 사이버공간상 표현의 자유의 한계

인터넷은 뚜렷한 중심이 없고 누구나 참여와 이용이 가능하며 외부의 통제나 규제가 어렵고 시간과 공간의 제약으로부터도 자유롭다는 특성을 가진다. 또한 익명성이 보장되어 상호간에 사회적 지위나 성별, 연령, 인종 등의 선행조건을 전제하지 않은 상태에서 대화와 토론이 가능한 수평적 커뮤니케이션이 가능하다. 이러한 자신의 신원을 드러내지 않는 익명성이라는 특성

때문에 실생활에서 적용되는 법규라든가 윤리·도덕과 같은 일련의 사회적 구속으로부터 벗어난 일탈행위들이 자행되는 결과를 초래하기 쉽다.

인터넷의 등장으로 인하여 포르노와 같은 음란물이 만연하고 청소년유해물에 대한 청소년의 접근이 더욱 용이해졌으며, 보이지 않는 자에 의한 통제가 가능해져 종전보다 개인정보 등 프라이버시가 침해될 위험성이 높아졌을 뿐 아니라, 사회적 연대보다는 개인의 고립화를 초래하고 있다는 비판이 있다. 또한 전자우편이라는 편리한 통신수단이 스팸메일의 형태로 악용됨으로써 개인이 정신적·물질적 피해를 입게 되는 역기능이 발생하고 있다. 또한 기존 매체와 달리 무한복제가 가능하고 신속한 전파가 그 특징인 인터넷은 저작권침해라거나 개인의 사생활침해 또는 명예훼손 행위 등이 더욱 빈번해지고 있고 사이버공간을 통하여 순식간에 확산되는 개인의 피해는 상상하기 힘들만큼 매우 심각한 상황이다.

헌법 제21조 제1항은 언론출판의 자유를 보장하고 있고, 그 중요한 내용 중 하나가 이른바 '표현의 자유'이다. 사이버공간상 표현의 자유는 어느 정도의 수준에서 인정되고 보호되어야 할 것인가?

헌법재판소는 "헌법 제21조에서 보장하고 있는 언론·출판의 자유, 즉 표현의 자유는 전통적으로는 사상 또는 의견의 자유로운 표명(발표의 자유)과 그것을 전파할 자유(전달의 자유)를 의미하고, 개인이 인간으로서의 존엄과 가치를 유지하고 행복을 추구하며 국민주권을 실현하는데 필수불가결한 것"으로 파악하고 있다.[25]

그러나 어떠한 표현을 사용하든 인터넷상의 표현의 자유도 헌법 제21조 제4항의 "타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해해서는 안된다"는 한계를 분명히 가지고 있다. 이 한계내에서 표현의 자유는 분명히 제약을 받는 것이다. 아울러, 헌법 제13조는 "모든 국민은 법률에 의하지 아니하고는 언론, 출판, 집회, 결사의 자유를 제한받지 아니한다"고 규정하고

25) 헌법재판소 1992.2.25 89헌가104, 2002.4.25 2001헌가27 등 참조.

있으므로, 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하는 행위에 대한 사이버공간의 규제는 '입법'을 통해서 가능한 것이라고 하겠다.

3. 사이버공간 규제와 '표현의 자유'의 조화

사이버범죄의 규제는 개인의 법익보호를 위하여 반드시 필요하지만 그러나 사이버공간에 대한 지나친 규제는 자칫 표현의 자유를 침해하는 결과로 이어지기 쉽다.

반대로 사이버공간에 대한 규제의 완화는 곧 자유로운 의사소통의 가능을 의미하며 이는 표현의 자유의 확장을 의미하는 것이다.[26] 그러나 만일 사이버공간의 규제가 적절히 행해지지 않는다면 사이버범죄의 피해가 발생할 경우 합리적으로 대응할 수 없게 되므로 개인의 중요한 보호법익을 지켜주지 못하는 결과를 초래할 수 있고 또한 무책임한 유언비어의 남발이나 명예훼손성 표현으로 인해 큰 사회적 혼란을 야기할 수도 있는 것이다. 결국 사이버공간 규제에 관한 논의는 이 두 가지 중요한 법익, 즉 인격권으로서의 명예와 자유권으로서의 표현의 자유를 어떻게 효과적으로 조화시킬 수 있을 것인가의 문제로 발전되어 온 것이라 하겠다.

사이버공간은 자유로운 의사표현을 위한 무한한 가능성을 지닌 공간이라는 점에서 '표현의 자유'를 가장 중요시하지 않을 수 없다. 이와 관련하여 헌법재판소는 사이버공간에서의 표현의 자유에 대하여 인터넷을 '가장 참여적인 시장, 표현촉진적인 매체'라고 하면서 "인터넷상의 표현에 대하여 질서위주의 사고만으로 규제하려고 할 경우 표현의 자유 발전에 큰 장애를 초래할 수 있다"고 하여 사이버공간에서의 표현의 자유의 중요성을 명시적으로 선언한 바 있다.[27]

---

26) 인터넷상 표현의 자유에 대하여는 鈴木秀美, "インタネットと表現の自由-ドイツ·マルチメディア法制の現狀と課題-" ジュリスト1153, 1999.4.1 참조.

27) 헌법재판소의 구 전기통신사업법 제53조의 위헌결정문에 표현된 구절이다. 헌법재판소 2002.6.27

사이버공간을 규제함에 있어서는 헌법상 표현의 자유를 침해하지 않도록 그 합리성과 적절성이 보장되는 전제하에 개인의 법익침해행위에 대한 보호적 차원의 규제가 될 수 있도록 조화가 이루어져야 할 것이다.

Ⅵ. 사이버범죄에 대한 대응방안

1. 사이버윤리교육 강화 등 예방대책

사이버범죄의 예방대책으로는 첫째로 사이버공간에 대한 올바른 이해와 활용방안에 대한 청소년, 교사, 학부모, 사업자 등 대상별 정보윤리교육의 확대실시가 매우 중요하다. 이에 따라 각종 학교와 정보통신서비스사업체에서의 사이버윤리교육 확대, 온라인 원격교육 실시, 다양한 사이버윤리교재의 개발 및 보급이 행해져야 한다. 아울러 학부모와 청소년이 동시에 참여하는 사이버윤리교육 방안도 모색해야 한다. 일회성 이벤트 행사로 끝날 것이 아니라 학부모와 청소년 등 다양한 계층이 동시에 참여할 수 있는 지속적인 교육과정의 개설이 중요하다.

많은 사회 공동체 중에서 윤리교육이 가장 효과적으로 행해질 수 있는 곳은 바로 “종교공동체”라고 할 수 있다. 따라서 사이버윤리교육도 국민의 상당수를 구성하고 있는 종교인을 중심으로 종교운동의 일환으로 행해진다면 가장 효율적 교육이 가능할 것이다.

둘째, 유관기관 간 협력체제의 구축이 필요하다. 불법·유해정보와 관련하여 유관기관 간 신고처리지연, 공조체계 미흡 등 문제점이 발생하고 있다. 정보통신윤리위원회, 검찰, 경찰 등 관련기관간 적극적 협력이 무엇보다 중요하다. 이러한 협력방안으로 인터넷 이용자, 인터넷 사업자, 검찰·경찰, 정

결정 참조.

부유관기관을 포함하는 실무자급 협의체 구성 및 사이버범죄 신고사항 처리기관별 분류·이관 및 처리결과 안내 등에 관한 종합시스템 구축 등도 검토되어야 할 것이다. 또한 불법·유해정보의 생산·유통자 및 불법스팸발송자에 대한 신속하고 종합적인 대응을 위한 민·관 핫라인 구성·운영의 활성화도 필요하다.

셋째, 인터넷사업자, 민간단체 등의 자율규제를 강화해야 한다. 해외 한글 불법사이트에 대한 인터넷 사업자의 모니터링과 국제관문에서의 자율차단 확대실시뿐만 아니라 포털사업자, 인터넷정보센터(KRNIC), 인터넷서비스제공자(ISP) 등 사업자가 상시협력체제를 구축하여 스팸발송자 유동IP 차단 등에 대한 효과적 대책이 마련되어야 한다. 또한 성인정보에 대한 청소년 접근을 방지하기 위해 포털사이트 검색서비스에 성인인증제도의 철저한 시행을 유도하고 포털업체의 성인사이트 등록기준 마련 및 관리 강화가 필요하다. 또한 최근 대형화되고 있는 커뮤니티 및 채팅사이트 등에 대하여 개설자의 실명확인 및 운영자와 회원 준수 사항에 대한 사업자 공동 가이드라인 제정 및 해당 사이트 신고센터 간 핫라인 운영을 통한 불량회원 관리 강화를 위한 사업자의 자율규제를 적극 지원해야 할 것이다.

한편, 청소년유해환경감시단, 안전한 온라인을 위한 민간네트워크, 한국사이버감시단, 한국여성단체협의회, 한국 ISP협회, 한국인터넷콘텐츠산업협회, 게임비디오물 민간 합동자율지도위원회, 이메일환경개선협의체 등 수많은 민간단체와의 협조도 효율적인 규제를 위하여 필수적이다. 그러나 이러한 자율규제가 사이버범죄의 범람을 적절히 차단하기에는 여전히 역부족인 상황이며, 앞으로 무선인터넷이 활성화될 경우에는 문제가 더욱 확대될 것으로 예상된다. 민간단체에 의한 자율규제가 효과를 발휘하려면 기업이나 민간단체가 정부와 효율적인 협조체제를 구축하고, 자율규제를 법제도와 연계되도록 방안을 강구해야 할 것이다.

넷째, 인터넷이용기관의 자체 지침서를 마련해야 한다. 학교, 직장 등 인터

넷 이용기관에서도 자체적인 대책 마련을 강구할 필요가 있다. 많은 기업체와 회사에서 인터넷의 이용을 생활화하고 있는데, 소속 직장인들은 직장 내에서 발생하는 불만을 직장 홈페이지 게시판이나 직원의 이메일을 이용하여 제기하고 있다. 학교에서도 홈페이지 게시판이 교사나 동료 학생을 비방하거나 조롱하는 곳으로 이용되는 일이 증가하고 있다. 그러므로 학교, 직장 등에서는 인터넷 이용에 관한 지침을 마련하고 문제발생시 이를 신속히 해결할 수 있도록 하여야 할 것이다. 예컨대 직장 내에서 사이버 성폭력, 음란물 전송 등과 같은 행위를 할 경우 징계할 수 있는 근거규정을 만들고 아울러 사이버 성폭력 방지를 위한 교육이나 캠페인을 실시하여야 한다. 그리고 학교 홈페이지 운영자는 학생들에게 학교 홈페이지 이용에 대한 안내서를 제공한다. 안내서의 내용은 주로 인터넷상에서 자기 표현하는 기술 가르치기, 불량 행위에 대한 제재조항 설명, 경고성 메일을 받은 횟수에 따라 게시판의 이용 금지 그리고 실생활에 가해지는 제재조치 등을 포함할 수 있을 것이다.

2. 법제도적 대응방안

(1) 수사기관의 단속・처벌 활동 강화

모든 범죄에 대하여 마찬가지의 말을 할 수 있지만, 사이버범죄에 대하여도 사법기관을 통한 사건해결은 가장 강력하고 최종적인 피해해결방안이라고 말할 수 있다. 경찰청 사이버테러대응센터나 검찰청 첨단범죄수사부 등이 사이버범죄에 적절한 대응을 하려고 노력하고 있지만, 아직 사이버범죄에 대하여 '적극적인' 대처를 하고 있다고 보기 어렵다.

사이버범죄의 피해자들은 경찰의 적극적 수사를 기대하고 있지만, 사안이 경미하여 수사인력을 투입하기 어려운 경우가 적지 않고, 피해자가 충분한 증거자료를 확보하고 있지 못한 경우가 많다. 또한 경찰이 사이버범죄를 조

사하는데 필요한 컴퓨터 기술이 부족하고, 범죄자 ID의 진정한 사용자를 제대로 파악하기가 어려우며, 사이버사건의 수사에는 장기간의 수사기간을 요하고, 사이버범죄자를 수사할만한 수사력이 충분히 확보되어 있지 않은 등의 이유로 사이버범죄 수사는 현실적으로 많이 미흡한 상황이다.

이 결과 사이버범죄에 대해 수사기관에 신고한 피해자는 곧 좌절하게 되며 경찰의 대응이 소극적인 것으로 여겨지게 된다. 따라서 경찰 등 수사기관은 사이버범죄에 대한 전문 수사인력과 수사역량을 확보하여 다수의 인터넷 이용자들의 범죄피해에 보다 적극적으로 대응하여야 할 것이다.

(2) 사이버모욕죄 입법의 필요성

최근 법무부에서 사이버모욕죄 신설 방침을 발표한데 대하여 의견이 분분하다.[28]

주지하는 바와 같이, 사이버공간은 우리에게 순기능뿐 아니라 많은 역기능을 제공하고 있다. 역기능 해소에 우선순위를 부여할 수는 없겠지만 의사소통을 인터넷의 중요기능이라고 볼 때, 의견제시가 아닌 욕설 등 모욕행위로 일관하거나 타인의 명예를 훼손하여 치명적 피해를 입히는 악플 등 이른바 '사이버폭력' 행위의 해결은 매우 시급하다. 사이버모욕행위가 '일부'에서 행해지고 무분별한 동조행위가 덩달아 이루어져 '전체'의 의사소통을 방해하는 결과를 초래하게 되는 저질 '사이버폭력'의 방지는 현대판 마녀사냥식 인권침해행위를 허용하자는 의견이 아니라면 정말로 시급한 정책이라고 하겠다.

'모욕'행위는 범죄인가? 형법에는 1953년 입법당초부터 모욕죄를 범죄로 규정하였고, 그 제311조에서 '공연히 사람을 모욕한 자'를 처벌하도록 규정하고 있는바, 이 모욕죄의 부당성이나 불필요성을 말하는 사람은 없다. 사이버공간

28) 이하의 내용은 동아일보에 발표한 시론의 내용이다. 정 완, "사이버모욕죄 입법 적극 검토를" 2008.8.2자 동아일보 29쪽 기고문 참조.

에서의 모욕행위는 어떠한가? 현실공간에서 소수 사람들 앞에서의 모욕행위가 범죄인 마당에 절대 다수의 사람들, 아니 인터넷 이용자 전체에 공개되는 모욕행위인 사이버모욕행위가 범죄라는 점을 부정할 수는 없을 것이다. 사이버모욕행위를 기존 사이버명예훼손죄로 처벌할 수 있는가? 양자는 구성요건이 다르다. 사이버모욕죄를 형법상의 모욕죄로 의율하면 되는가? 현실공간에서의 범죄와 사이버공간에서의 범죄는 그 무대가 다르다. 많은 사람들이 사이버공간을 범죄수단의 하나에 불과한 것으로 생각하지만 '죄형법정주의'라는 형법사상을 대전제로 할 때 아무규정이나 두루뭉실 적용하기보다는 좀 더 적절하고 세밀한 별도의 규정이 필요하다. 사이버공간에서의 게임아이템 등 절도행위를 형법상 절도죄로 의율할 수 없는 이유와 비슷하다.[29]

사이버모욕죄 신설은 헌법상 '표현의 자유'를 침해하는가? 많은 사람들의 입에 회자되는 표현의 자유는 헌법 제21조 제1항에 규정된 언론출판의 자유의 한 내용이다. 그런데 헌법 제21조 제4항에는 사람들이 잘 인용하지 않는 언론출판의 자유에 대한 '중대한 제한'이 규정되어 있다. 즉, 언론출판의 자유는 "타인의 명예나 권리 또는 공중도덕이나 사회윤리"를 침해하여서는 아니 된다고 헌법상 규정되어 있는 것이다. 표현의 자유는 반드시 수호되어야 하지만, 그를 이유로 사회윤리를 침해하여서는 아니 된다는 또 하나의 '헌법상 의무'를 저버려서는 안 되는 것이다. 따라서 사이버공간상 타인에게 이유없이 또는 감정적으로 심하게 욕설을 가하는 등의 이른바 '악플' 등 모욕행위는 심한 경우 피해자에게 자살을 생각게 하고 실행에 옮기게 하는 등 치명적 상태에 빠지게 하므로 반드시 근절되어야 하며, 이러한 상황을 인터넷 이용자의 도덕에 맡겨 자율적으로 개선되기를 바라기에는 이미 때늦은 상황이 아닌가 생각된다.

---

29) 마찬가지의 취지로 필자는 '사이버도박'에 대하여도 형법상 도박죄를 그대로 적용하기보다 사이버도박의 특성을 고려한 별도의 사이버도박죄의 신설 필요성을 제기한 바 있다. 정 완, "사이버도박의 사례와 대응", 형사정책연구소식 2001.6; 정 완, "인터넷도박의 실태와 대응" 경희법학 41권 2호 2006.12 등 참조.

필자는 사이버모욕죄 신설을 강력한 해결책의 하나로 생각한다. 사이버모욕죄의 입법은 여러 가지로 가능할 것이다. 형법상 모욕죄나 정보통신망법상 사이버명예훼손죄의 구성요건을 추가하여 개정할 수도 있고 아예 규정을 신설할 수도 있을 것이다.[30] 다만, 입법의도에 오해를 야기하지 않도록 기존 형법상 모욕죄의 추상성을 불식할 수 있는 보다 구체적인 구성요건을 마련해야 할 것이며, 아울러 친고죄의 적용여부, 가중처벌 여부 등에 대한 충분한 연구와 검토가 행해져야 할 것이다.

(3) 인터넷 루어링 금지

현재 미국에서는 주마다 약간 다르지만 대체로 인터넷을 이용하여 성행위를 하려는 목적으로 아동에게 채팅 또는 이메일로 접근하는 행위를 인터넷 루어링(Internet Luring)으로 처벌하고 있다. 인터넷 루어링은 그루밍(Grooming) 행위 중의 하나로서 아동에게 성매매 또는 성폭력을 행사하기 전에 인터넷상으로 그루밍 행위(믿음과 신뢰를 쌓는 것)를 하는 것을 의미한다. 가령 어떤 아동이 부모님으로부터 꾸중을 듣거나 한 경우 고민상담 등을 통하여 친분관계를 형성하고 그것을 이용하여 성적 행위를 자연스레 언급하는 등 아동의 경계심을 없애는 것을 포함하는 경우가 종종 있기 때문에 아동이 피의자에 대한 친분관계로 인하여 피해사례를 부모님에게 말하지 않게 되는데, 바로 이러한 점은 인터넷루어링의 심각성을 보여주는 단적인 예이다.[31] 물론 인터넷 루어링은 굳이 친분관계를 포함하지 않아도 호기심 많은 미성년자에게 단순한 성행위 주제의 이야기나 포르노를 보여주겠다는 유인 등을 한 경우 범죄 요건이 성립했다고 보는 것이다.

---

30) 현행 정보통신망법상 사이버명예훼손죄의 구성요건에 사이버모욕행위가 빠져 있는 것은 결함이며, 따라서 그 보완입법이 필요하다는 지적이 있다. 박상기, 형법각론 제7판(박영사, 2008), 199쪽 참조.

31) Electronic Luring Statue Under Fire, Danica Szarvas-Kidd, American Prosecutors Research Institute, Volume 3, Nov.1, 2006, at Part I of II.

참고로 아동을 대상으로 한 사이버범죄가 지속적으로 증가하는 것을 막기 위해 플로리다주는 2007년 6월 아동을 대상으로 한 사이버범죄 관련법(The Cybercrimes Against Children Act of 2007(SB 1004))을 제정하였다. 이 법은 인터넷을 이용하여 아동을 성적으로 유인하는 범죄에 대하여 강경조치를 취할 수 있게 하였다. 예컨대 2007년 6월부터 그루밍, 특히 인터넷루어링(인터넷상 피의자가 범죄아동피해자의 경계심을 없애기 위해 자신의 나이를 속이는 것)까지 처벌할 수 있도록 하였으며, 이 점에서 미국의 유일한 주이다. 그뿐만 아니라 인터넷을 통해 온라인 피해자에게 그루밍 행위(믿음을 형성함)를 하고 그 해당 아동을 상대로 성범죄를 저지를 목적으로 이동하는 것에 대하여 따로 처벌할 수 있도록 입법하였다. 플로리다는 현재 아동 포르노와 아동 성범죄에 대하여 가장 엄중하게 대처하는 주의 하나이다.[32] 또한 조지아주법에 의하면 의도적으로 아동을(심지어 성인 포함) 성적으로 유혹하거나 권유하거나 유인하려는 등의 목적으로 컴퓨터 온라인 서비스, 인터넷서비스, 또는 지역게시판 등을 이용하는 것은 법률위반이다. 기타 알라바마주, 아리조나주 등 30여 개 주에서 인터넷루어링을 주법으로 금지하고 있다.[33]

이러한 미국의 법제도를 참고하여 우리나라도 사이버성매매의 강력한 단속을 위하여 인터넷 루어링을 엄격히 금지하는 입법의 필요성이 신중히 검토되어야 할 것으로 생각한다.[34]

---

32) 미국 미아 및 아동착취 국립센터(National Center for Missing and Exploited Children)의 보고서에 따르면 7천7백만 명의 아동이 매일 인터넷을 사용하고 있고, 10세부터 17세까지의 인터넷 사용 아동 중 7명 중 한 명이 성적인 유혹을 받는다. 플로리다주는 아동을 성적으로 유인하기 위하여 사용되는 컴퓨터상(웹카메라, 채팅룸과 비디오 포함) 아동포르노의 규모가 미국 전체의 4위이다. McCollum 검찰총장은 인터넷을 이용한 아동대상 성범죄가 더욱 중요하게 다뤄져야 하며, 연방법에서 '그루밍'을 구체적으로 대처하는 연방법이 없기 때문에 연방적인 차원에서 국회가 더욱 엄중하게 처벌하는 법안을 만들 것을 촉구하는 편지를 국회에 보내기도 하였다.

33) 상세한 주의 명칭과 법률조문 근거는 박병식・김경제・임규철・이혜리, 온라인상 청소년 성보호 관련 법적 규제 도입을 위한 연구(서울: 국가청소년위원회, 2007), 44~46쪽 참조.

34) 이에 관한 상세한 내용은 정 완, "영미의 청소년인권침해 관련법제" 한국청소년정책연구원 워크숍 자료집 08-S04, 2008.8 53쪽 이하 참조.

(4) 사이버도박죄의 도입 필요성

현재 사이버도박은 형법상 도박죄와 도박개장죄로 의율, 처벌되고 있고 많은 사례와 판례도 형성되고 있다. 그러나 형법상 도박죄의 구성요건은 인터넷이 없던 시대에 만들어진 것이며 현재 유행하고 있는 사이버도박의 특성을 전혀 고려하고 있지 못하므로 이는 죄형법정주의의 원칙과도 합치된다고 장담할 수 없다. 따라서 인터넷도박을 보다 효율적으로 단속하고 예방할 수 있는 별도의 사이버도박죄에 관한 입법의 추진이 필요하다고 생각한다.

이와 관련하여, 최근 바다이야기 등 온라인도박이 기승을 부리며 심각한 사회문제로 대두되자 정치권에서도 이를 근절하기 위한 관련법 제정이 추진되고 있는바, 한나라당 이정현 의원이 관계 전문가, 시민단체 등과 함께 가칭 '온라인도박금지법' 제정을 추진 중인 것으로 알려졌다. 이 의원의 입법추진 취지는 미국의 경우 2006년에 온라인도박금지법이 제정되었고, 그 계기는 달러 유출문제였는바 우리나라도 대부분의 불법 온라인도박사이트들이 외국에 서버를 두고 있거나 외국 회사이기 때문에 온라인도박으로 인한 손실금은 곧바로 국부유출로 이어지고 있어 이에 대한 감독, 처벌 강화가 시급하다는 것이다.[35] 가칭 '온라인도박금지법'은 온라인 도박에 대하여 미국 등에서 실시하고 있는 방식과 마찬가지로 은행 등의 금융거래기관에서 도박자금의 신용결재를 차단하도록 하고, 국내 접근 도박 사이트에 대한 접근 차단 및 국제공조를 통해 불법도박 사이트 운영 영업자에 대한 감시 및 처벌을 강화하며, 이를 위한 관리 체계와 감독을 강화토록 하는 것이 주요 골자로 되어 있다.

(5) 인터넷실명제 확대실시

사이버명예훼손 범죄를 막기 위한 방안으로 '인터넷 실명제'를 확대실시

35) 경향신문 2008.9.30자 "한나라당 이정현 의원, 온라인도박금지법 제정추진" 기사 참조.

해야 한다는 여론이 높아지고 있고 정부에서도 그러한 쪽으로 적극 검토하고 있다. 세계 제일의 초고속 인프라를 바탕으로 한 우리의 인터넷 문화는 선진국조차 부러워할 정도로 만개된 상태다. 그러나 양날의 칼과도 같이 긍정적인 면 못지않게 해악을 주는 악영향도 심각하다. 인권침해와 명예훼손, 욕설과 같은 인신공격이 가장 문제다. 인터넷에 의한 개인의 인격권 침해는 본인에게는 회복불능의 치명적 타격이 된다. 네티즌과 메카시즘의 합성어인 '네카시즘'이란 말이 생겨날 정도로 현대판 마녀사냥이 사이버 공간에서 공공연하게 자행되고 있는 것이 현실이다.

매년 발생되는 사이버범죄 건수는 급증하고 있다. 사이버명예훼손을 당하더라도 당사자가 고발을 꺼린다는 점을 감안하면 실제 인터넷공간의 개인명예 훼손 사례는 비일비재할 것으로 짐작된다. 인터넷실명제의 확대실시 필요성은 계속 제기되고 있다. 반대하는 사람들은 인터넷 실명제가 표현의 자유를 억제하고 설사 실명제를 하더라도 시간이 지나면 별 효과가 없을 것이라는 등을 주장하고 있다. 일리 없는 것은 아니지만 부작용 실태가 너무 심각하다는 점을 고려할 때 인터넷 환경을 모종의 정화조치 없이 이대로 방치해서는 안 된다.

인터넷실명제는 우리 헌법이 보호하고 있는 문화국가의 실현을 위한 제도이다. 그 동안 인터넷을 통한 국어훼손은 그야말로 커다란 충격이었다. 욕설 등 무례한 언어사용뿐만 아니라 표준어를 파괴하고 의사소통에 있어 다른 상대방의 의견을 무시하는 발언 등은 문화국가 실현에 중대한 걸림돌이 된다고 생각한다. 토론문화의 올바른 형성과 국어보호를 위해 인터넷실명제는 긍정적 기능을 한다고 볼 수 있다.[36]

우리는 새로이 등장한 효율적 매체인 사이버공간의 특성과 문제점을 제대로 파악하지 못하고 이에 대응하는 방법을 갖지 못한 것이 사실이다. 이제는 헌법 제21조 제4항이 요구하는 역기능에 대한 대책을 세우고 강력하게

36) 명재진, "공공기관 인터넷게시판 실명제실시에 관한 소고" CLIS Monthly, 2003.5/6 참조.

실천해 나가려는 노력이 필요한 때이다. 인터넷 게시판을 이용함에 있어서 실명을 사용하게 하는 것이 국민의 기본권을 제한하는 것인지에 대하여는 의견이 갈리고 있지만, 어느 쪽의 의견을 택하건 적절한 규제를 위해서는 적정한 입법에 의한 제도의 실천이 요구되는 바이다.

현재 정보통신망법상 일정수 이상의 하루이용자를 가진 포털사이트 게시판에 대하여 '본인확인조치'를 의무화되어 있어 부분적이나마 인터넷실명제를 실시하고 있다. 하지만 이러한 제한적 인터넷실명제 실시는 명목상의 시행에 그칠 수 있어 제도의 본래의 취지와 효과를 살리지 못할 가능성이 있다. 이에 따라 최근 그 시행범위를 하루이용자 30만명 이상의 포털사이트에서 10만명 이상의 포털사이트 게시판으로 확대하겠다는 정부의 방침이 거의 매일 보도되다시피 하고 있다. 생각건대 인터넷실명제는 일부공간으로의 확대실시가 아니라 아예 전체 사이버공간으로 확대, 시행하는 방안을 적극적으로 검토할 필요가 있다.[37]

(6) 인터넷서비스제공자(ISP)의 책임 강화

최근 인터넷 포털사이트나 대형 ISP 게시판, 각종 경매사이트를 이용한 사이버범죄가 증가하고 있으나, 업체들의 무관심으로 사이버범죄행위가 무방비 상태로 방치되고 있는 실정이다. 이러한 사이트에 접근하여 보면, 다양한 유형의 사이버범죄가 행해지고 있음을 알 수 있다(예컨대 각종 음란물 판매광고나 성매매를 부추기는 내용 등). 업체 관계자들은 이러한 불법 게시물에 대해 인력부족 등의 이유를 들어 삭제가 불가능하다고 변명하고 있으나, 이는 변명에 불과하고 도덕적 불감증과 상업적 이기주의에 의해 이러한 불법 게시물을 방치하는 것으로 보인다. 따라서 이들 업체에 대하여 보다 강화된

37) 인터넷실명제의 도입에 관한 상세는 정 완, "사이버폭력방지책으로서의 인터넷실명제 실시", 경희법학 2005.12 참조.

법적 책임을 물을 수 있도록 하여야 할 것이다.

타인이 제공한 정보에 대하여도 정보통신서비스제공자는 책임을 면하기 어렵다. 다만 정보통신서비스제공자가 구체적으로 어떠한 형태의 책임을 져야 하는지는 매우 어려운 문제이다. 예컨대 인터넷 경매 사이트에서 이용자가 음란물을 판매한 경우 또는 누구나 이용할 수 있는 인터넷게시판에서 타인을 비방하는 명예훼손성 글을 게재한 경우 사이트 운영자를 형법상의 방조범으로 처벌할 수 있는지는 용이한 문제가 아니기 때문이다.

따라서 법·제도의 개선을 통하여 불법·유해정보 유통 관련 사업자 책임 규정 명문화를 할 수 있는 방안을 적극 고려해야 한다. 당해 정보가 불법정보임을 알 수 있었거나 불법정보 제공 또는 유통을 방지하는 것이 기술적으로 가능할 경우 이에 대한 정보통신서비스제공사업자의 책임규정 명문화는 반드시 필요하다.

사이버공간상의 불법정보에 대하여 ISP의 형사책임을 인정할 수 있는가에 대하여는 논란이 있다. 관련법령의 직접위반자와 함께 게시판관리자 또는 온라인서비스제공자에게도 최소한 방조범으로서의 형사책임을 물을 수 있어야만 그 자율규제를 초래하여 사이버공간의 건전한 문화를 조성할 수 있다는 필요성은 제기되고 있으나 민사책임과 달리 형사책임의 경우에는 직접 위반의 고의를 전제로 하기 때문에 이론적으로 그 적용이 쉽지 않은 상황이다.

음란사이트를 링크한 인터넷서비스제공자에 대하여 그 형사책임을 인정한 대법원의 판결이 주목된 바 있다.[38] 그러나 이 판결에 대하여 학자들은 방조범으로서의 책임이라면 몰라도 정범으로서의 책임은 인정하기 곤란하다는 의견을 제시하거나,[39] 입법을 통하지 않은 이러한 해석은 지나치고 무리한 해석이므로 반드시 입법을 통하여 해결해야 한다는 의견을 제시하고 있다.[40]

---

38) 대법원 2003.7.8 선고2001도1335 판결 참조.

39) 예컨대 서보학, "유해정보사이트에 링크해 놓은 경우의 형사책임", 법률신문 제3205호 판례평석 참조.

40) 오영근, "인터넷상 음란정보 전시의 개념" 법률신문 제3213호(2003.10.23) 판례평석, 13쪽 참조.

이와 같이 ISP의 형사책임 인정에 비판적인 견해도 보이지만, 현재의 상황은 어떠한 형태로든 그 책임을 인정하는 추세로 가고 있음을 확인할 수 있다고 하겠다.[41]

가장 효과적인 사이버공간 규제는 당해 사이버공간을 관리하고 있는 ISP라고 할 수 있으므로 ISP에 대하여 해당 관리공간에 대한 사이버게시물에의 감시의무를 부여하고 그러한 의무를 게을리할 경우 행정벌 또는 형사벌에 처할 수 있도록 입법함으로써 보다 적극적인 사이버공간 정화에 나설 수 있을 것이다.

우리도 정보통신망법에 ISP의 행정적 또는 형사적 책임을 물을 수 있는 조항을 엄격한 요건 하에 추가, 신설한다면 보다 효과적이고 실제적인 사이버공간 정화가 가능하다고 하겠다. 참고로, 불법복제에 대한 사법부의 동향으로, 그 동안 P2P 서버운영자의 형사책임 인정에 법원은 소극적 태도를 견지해 왔었으나, 2007년말 대법원은 '소리바다' 측에 대하여 운영자의 미필적 고의에 의한 방조범으로서의 형사책임을 인정하는 판결을 내려 우리의 주목을 끌었다.[42]

(7) 디지털증거의 형사절차법상 사용근거 마련

사이버공간상 디지털증거의 수집과 사용의 중요성은 매우 크다. 디지털증거는 삭제하더라도 복구가 가능하고 네트워크상의 정보는 당사자의 의사에 관계없이 서버에 존재하므로 증거수집이 유체물증거보다 오히려 용이할 수도 있다. 따라서 디지털 증거가 형사재판에서 증거로 사용되기 위해서는 이미 증거를 수집하고 분석하는 단계에서 원본 증거의 멸실이나 훼손을 막고 증거의 진정성이 훼손되는 것을 방지할 수 있는 적절한 조치를 취할 필

41) 사이버범죄에 대한 ISP의 형사책임에 관하여는 백광훈, 사이버범죄에 대한 ISP의 형사책임에 관한 연구, 한국형사정책연구원 2003 참조.
42) 대법원 2007.12.14 선고 2005도872 판결 참조.

요가 있다.[43]

현행 형사소송법에는 디지털 정보나 증거의 압수, 수색과 관련하여 직접적인 근거규정이 없다. 다만 일반 유체물인 증거에 대해서만 증거수집 절차만을 가지고 있을 뿐이다.

따라서 형사소송법에 디지털 증거의 수집과 분석, 증거사용에 대한 일반적인 규정을 마련해야 하며, 그러한 후에는 아울러 디지털 증거를 수집하고 분석하는 구체적인 표준지침이나 가이드라인 등 디지털포렌식 표준도 마련되어야 한다. 그러한 내용으로는 수사관과 분석가의 이원화, 디지털 증거수집시의 준수사항, 원본증거의 수집, 보관 및 복사 증거의 제작방법, 증거분석의뢰시 준수사항, 분석의뢰서 접수시 준수사항, 분석의뢰서 접수후 준수사항, 기타 분석의뢰서 및 결과보고서 양식 등을 생각해볼 수 있다.[44]

(8) 국제사법공조 강화

아동포르노의 심각성, 해외한글 음란사이트 문제 등을 해결하기 위해서는 국제 간 공조체제구축을 위하여 국제기구나 단체에 적극 참여해야 한다.

정보통신윤리위원회는 인터넷상의 아동포르노 등 불법유해정보에 대한 국제적인 공조체제를 구축하기 위하여 2003년 인터넷핫라인협회(INHOPE)[45]에 가입한 바 있다. 그 동안 불법·유해정보가 한국의 서버로부터 세계 각국으로 유통되어 국가적 이미지를 손상시켜도 각 국의 핫라인 간 협력체제

43) 디지털증거의 증거조사와 증거능력에 대한 상세는 정 완, “컴퓨터관련증거의 증거조사와 증거능력” 수사연구 247권 2004.5 17쪽 이하 참조.

44) 안경옥, “정보화사회에서의 형법의 중요 문제와 과제”, 인터넷법학회 세미나 자료, 2007.6 151쪽~154쪽 참조.

45) INHOPE는 유럽연합의 지원을 받는 기관으로서 1999년 11월에 설립되었으며 유럽 국가들 가운데 핫라인을 운영하는 사업자들이 주축이 되어 만들어진 단체이다. 주요 목적은 인터넷의 불법 유해정보로부터 이용자를 보호하는 것이고, 아동포르노, 상업사이트, 음란영상, 대화방, 인종차별 사이트 등을 주요 검토 대상으로 활동하고 있다. 현재 한국을 포함하여 16개국 18개 단체가 가입되어 있다. 김기봉, “인터넷상에서 청소년보호정책의 방향과 과제”, 한국형사정책연구원 제32회 형사정책세미나 2003.11.13, 129쪽 참조.

미흡으로 적절한 조치를 취하기 위한 수단이 적었다. 따라서 불법·청소년 유해정보에 대한 신고처리를 신속히 하고 국제적인 이미지와 신뢰도 향상에 기여하기 위해서는 INTERPOL 등 국제기관 및 INHOPE, Cyber Tipline(미국의 민관협력 감시망) 등 해외민간감시기구와의 유기적 공조체제 구축이 적극 요망된다.

한편, 사이버범죄는 국가마다 그 규제방식과 내용이 달라 국제조약으로 법규범화하기에는 어려움이 있고 그 불가능을 주장하는 견해도 있어 왔다. 그러나 이러한 예상과는 달리 유럽에서 최초로 사이버범죄방지조약이 체결되었다.[46]

5개 가입국의 국회인준이라는 요건을 충족한 3개월 후인 2004년 7월 1일 발효한 이 사이버범죄방지조약에는 회원국뿐 아니라 비회원국인 미국, 캐나다, 일본, 남아프리카공화국 등도 가입되어 있고 2007년 6월 현재 미국을 포함하여 20여개 국가가 인준한 상태이므로 추후 세계 사이버범죄방지정책의 흐름을 주도하게 될 것으로 예상된다. 따라서 비회원국의 가입절차에 따라 우리나라도 가입을 검토하여 사이버범죄의 방지를 위한 국제협력에 적극적으로 동참해야 할 것이다.[47]

Ⅶ. 결 어

최근 사이버공간에서 주로 유통되는 불법유해정보는 상당부분 포털사업자가 운영하는 포털사이트의 게시판이나 뉴스댓글 등을 통하여 주로 발생하고 있다. 앞에서 ISP의 법적 책임 강화 필요성을 서술하였지만, 다수의 네티즌

46) 유럽의 사이버범죄방지조약에 관한 상세한 내용에 대하여는 정 완 外, 사이버범죄방지조약에 관한 연구, 형사정책연구원 보고서(2001)를 참조 바람.

47) 사이버범죄방지를 위한 국제형사사법공조에 관한 상세한 내용은 정 완, 사이버범죄 방지를 위한 국제공조방안, 한국형사정책연구원 연구총서 04-22 2004 참조.

이 이용하는 사이트의 관리자가 불법게시물에 대하여 가장 효율적인 관리를 할 수 있으므로 포털사업자에게 사이버윤리척도 등 평가기준을 마련하여 이를 적용하여 평가를 하고 그 결과에 따라 관련 사업에 대하여 인센티브를 부여하거나 오히려 규제를 하는 등의 방법을 통하여 포털사이트의 합리적 규제가 가능할 것이다.

사이버공간은 전파성이 강하여 불법유해정보가 게시되면 순식간에 전국적으로 확대되기 때문에 그 폐해는 이루 말할 수 없이 커진다. 사이버공간이 이제 우리 생활의 상당부분을 차지하는 오늘날 건전한 사이버문화를 조성하기 위해서는 규제를 강화해야 할 것이며, 특히 피해자의 심각한 정신적 공황을 가져오는 사이버범죄에 대해서는 새로운 입법을 통해서라도 이를 적극 규제함으로써 관련 범죄의 발생을 최소화할 필요가 있을 것이다.

참고문헌

[단행본]

박상기, 형법각론 제7판, 박영사, 2008

박병식・김경제・임규철・이혜리, 온라인상 청소년 성보호 관련 법적 규제 도입을 위한 연구, 국가청소년위원회 2007

백광훈, 사이버범죄에 대한 ISP의 형사책임에 관한 연구, 한국형사정책연구원 2003

이영준・정 완・금봉수, 사이버범죄방지조약에 관한 연구, 한국형사정책연구원 2001

정 완, 인터넷과 법, 한국형사정책연구원 2007

_____, 사이버폭력에 대한 법제도적 대응방안 연구, 정보통신윤리위원회 2005

_____, 사이버범죄 방지를 위한 국제공조방안, 한국형사정책연구원 2004

_____, 소프트웨어 불법복제실태와 법제도적 개선방안, 한국형사정책연구원 2003

정보통신정책학회, 온라인상의 콘텐츠 공유에 따른 소프트웨어 저작권 침해 실태 및 경제적 손실액 추정에 관한 연구, 2007.12

[논 문]

김기봉, “인터넷상에서 청소년보호정책의 방향과 과제”, 한국형사정책연구원 제32회 형사정책세미나 2003.11.13

명재진, “공공기관의 인터넷게시판 실명제실시에 관한 소고” 정보통신부 자료실

박종현, “사이버폭력 피해구제제도 현황 및 문제점” 2005.7.21 정보통신윤리위원회 세미나 발표자료

서보학, “유해정보사이트에 링크해 놓은 경우의 형사책임”, 법률신문 제3205호 판례평석

안경옥, “정보화사회에서의 형법의 중요 문제와 과제”, 인터넷법학회 세미나 자료, 2007.6

오영근, “인터넷상 음란정보 전시의 개념” 법률신문 제3213호(2003.10.23) 판례평석

정 완, “보이스피싱 대응체제의 문제점과 대책” 수사연구 298권 2008.8

_____, “영미의 청소년인권침해 관련법제” 한국청소년정책연구원 워크숍자료집 08-S04, 2008.8

_____, “사이버범죄의 현상”, 형사정책 2007.12

_____, “사이버범죄의 방지를 위한 국제협력방안”, 형사정책연구 2007.6

_____, “사이버공간상 음란물 유통의 심각성과 법적 규제”, 경희법학 2007.6

_____, “인터넷도박의 실태와 대응” 경희법학 41권 2호 2006.12

_____, “사이버폭력방지책으로서의 인터넷실명제 실시”, 경희법학 2005.12

_____, “사이버공간상 불법정보 유통실태와 법적 대응방안”, 형사정책연구 2005.9

_____, “인터넷사기의 신종유형과 법제도적 대응방안”, 경희법학 2005.9

_____, “컴퓨터관련증거의 증거조사와 증거능력” 수사연구 247권 2004.5

_____, “사이버음란물의 유통과 규제” 형사정책연구 2000.3

_____, “사이버도박의 사례와 대응”, 형사정책연구소식 2001.6

_____, “인터넷사기의 최근동향” 형사정책연구소식 95호(2006.6)

차태원, “온라인상의 소프트웨어 불법복제 피해현황 및 신고센터운영”, Enter 145권 2007.12

鈴木秀美, “インタネットと表現の自由-ドイツ·マルチメディア法制の現狀と課題-” ジュリスト 1153, 1999.4.1

Danica Szarvas-Kidd, Electronic Luring Statue Under Fire, American Prosecutors Research Institute, Volume 3, Nov.1, 2006

[홈페이지 기타]

사이버경찰청 http://www.police.go.kr

사이버테러대응센터 http://www.ctrc.go.kr

정보보호진흥원 http://www.kisa.or.kr

방송통신심의위원회 http://www.kocsc.or.kr

(구 정보통신윤리위원회 http://www.kiscom.or.kr)

컴퓨터프로그램보호위원회 http://www.socop.or.kr

정 완, “사이버모욕죄 입법 적극 검토를” 동아일보 2008.8.2

[15:10 – 16:20]

사이버범죄의 법적규제 및 대응전략

제4주제 : 사이버범죄 법규 및 한계 – 사이버범죄와 관련된 현행 법규의 문제점 고찰

발표 : 최 정 호 (경찰대 교수)
토론 : 조　　국 (서울대 교수)
　　김 윤 희 (서울중앙지검 형사3부 검사)

사이버범죄 법규 및 한계
- 사이버범죄와 관련된 현행 법규의 문제점 고찰

최 정 호*

Ⅰ. 들어가며

우리가 살고 있는 사회환경의 상당 부분은 이미 사이버공간과 아주 밀접한 관계를 맺고 있을 뿐만 아니라, 전반적인 사이버공간과의 융합화 현상은 관련 기술의 발달과 더불어 더욱 가속화되어 가고 있다. 컴퓨터, 정보처리기기 및 정보처리망에 대한 의존도는 이미 그것들이 없으면 업무가 마비될 정도를 넘어서서, 그것들이 없어서 업무를 할 수 없는 필수불가결의 지위를 차지하고 있으며, 이런 변화된 환경에 맞추어 각종 사회문제에 대한 법과 제도들이 보조를 맞추어 변화하는 것은 당연한 일이라고 할 수 있다.

우리의 생활이 정보처리기술과 함께 그들이 형성하는 사이버공간의 덕으로 자유로운 의사소통의 장을 더 넓힐 수 있었지만, 그 변화의 진행정도가 너무 급속도로 이루어져 이에 대한 법적 대응은 변화의 속도를 제대로 따라잡지 못하였고, 제대로 다듬어지지 않은 체제에서 필연적으로 나타날 수밖에 없는 반작용으로서의 사이버범죄는 어느덧 우리 주위에서 가장 흔하게 접할 수 있는 범죄유형 중의 하나가 되었다.

사이버범죄 혹은 사이버테러에 대한 명쾌한 해석도 없이, 사이버공간에서의 폭력과 위협에 불안과 공포를 느끼며 살게 되었고, 일련의 연예인 자살사

* 경찰대학 교수

건의 주요 원인으로 사이버공간 상에서 이루어지는 언어폭력이 막연히 지목되고 있는 상황에서, 현실세계와 사이버공간의 점증적 밀착관계를 생각해 볼 때, 사이버공간에서의 무분별한 일탈행위를 무작정 매도만 하기 보다는, 사이버범죄에 대한 정확한 이해와 대책마련의 고려가 필요하다는 것을 부인할 수 없게 되었고, 이는 우리생활에서 사이버공간이 아주 중요한 일부분을 차지하고 있다는 것을 반증하는 것이기도 하다.

그동안 우리나라는, 물론 IMF 이후의 국가 주도 경제성장정책에 공을 돌릴 수도 있겠지만, 세계가 주목할만한 정보통신 기술분야의 발전을 이룩하였고, 이런 외형적 발전과 신기술에 민감한 국민들의 호응이 상호적 상승작용을 불러 일으켜, 계속적인 신기술의 경연장 또는 그 시험무대가 되고 있는 상황이다. 그러다 보니, 전 세계적으로 공통된 사이버범죄의 유형은 말할 것도 없고, 새로운 기술에 따르는 새로운 형태의 사이버범죄가 다른 나라보다 먼저 나타날 수 있다든지, 혹은 이런 신기술이 우리나라 특유의 사회문화 현상과 결합하여 독특한 형태의 사이버 일탈행위로 표출될 수 있으리라는 것은 어렵지 않게 짐작할 수 있을 것이다. 자신의 표현에 인색하던 사회문화가 인터넷이라는 급작스런 표현의 자유 수단과 어우러져, 폭발적인 사용자 증가를 가져왔지만, 표현의 자유에만 너무 힘이 실린 나머지, 사용자들끼리 배려하는 문화가 부족하여 나타나는 인터넷 댓글의 폐해가 그 대표적인 예라고 할 수 있을 것이다.

이 글에서는 사이버공간에서 일어나는 부정적인 행위들에 대해, 기술적이거나 사회문화적 혹은 이용자의 행태적인 접근 보다는 이들에 대응하는 법률을 중심으로 연구하였다. 따라서 현재 우리나라의 사이버범죄 관련 법률들을 먼저 살펴보고, 이들 법률에서 나타나고 있는 몇 가지 문제점과 미비점에 대해 다루었으며, 현재보다는 앞으로 일어날 수 있는 부작용들에 더 초점을 맞추어 개선방향 등을 고찰해보고자 한다.

Ⅱ. 우리나라의 사이버범죄

1. 사이버범죄 정의

우리나라에서 정의하고 있는 사이버범죄란, “인터넷과 같은 정보통신망으로 연결된 컴퓨터시스템이나 이들을 매개로 형성되는 사이버공간을 중심으로 발생하는 범죄행위를 총칭하는 표현”,[1] 또는 “컴퓨터범죄를 포함하여 사이버공간에서 행하여지는 모든 범죄적 현상”[2]이라고 할 수 있다.

다른 한편으로, 인터넷을 매개로 하거나 대상으로 하는 범죄 및 일탈에 초점을 두어, 사이버범죄 또는 일탈을, “수많은 인터넷 사이트들과 그것들을 서로 연계시키는 컴퓨터 네트워크(즉, 인터넷)를 수단으로 하여 개인들, 사이트들, 또는 네트워크 그 자체를 대상으로 하는 범죄 및 일탈을 총칭하는 개념”[3]으로 설명하기도 한다.

사이버범죄의 처벌과 관련하여 최초의 국제조약이며 거의 유일한 법원이라고 할 수 있는 ‘유럽 사이버범죄방지조약’(Convention on Cybercrime)[4]을 살펴보면, 사이버범죄에 대한 명확한 정의는 내려져 있지 않지만, 그 서문에 나타난 의도들을 종합해볼 때, 사이버범죄란 “정보처리시스템, 인터넷망 그리고 컴퓨터 자료들의 기밀성, 완전성과 가동성에 해를 끼치는 행위, 그러한 시스템, 네트워크와 자료의 악의적인 사용 또는 정보통신망과 전자정보를 이용함으로써 사이버공간에서 벌어지는 형법적 침해행위”[5]라고 유추할 수 있

1) 양근원, “사이버범죄의 특징과 수사방향”
2) 강동범, “사이버범죄와 형사법적 대책”, 형사정책연구 2000년 제42호
3) 이민식, “사이버범죄 및 일탈의 개념 및 유형”, 사이버범죄연구회 제4회 세미나, 2000. 11. 4.
4) 2001년 6월 22일 유럽이사회 제50차 형사문제위원회에서 최종안을 작성하고 2001년 11월 8일 각료위원회의 승인을 받아 2001년 11월 23일 헝가리 부다페스트에서 가입절차가 개시됨.
5) 최정호, “인터넷 이용자들의 이용행태에 따른 사이버범죄의 변천 - 프랑스와 한국의 법률 비교 연구 (Les comportements des internautes et l'évolution de la cybercriminalité - Etude comparée entre la France et la Corée du Sud)”, 프랑스 몽뻴리에(Montpellier) 1대학, 박사학위 논문, 2007년 10월 18일. Ces quelques extraits nous paraissent pertinents pour tenter une définition : la cybercriminalité est constituée des « actes portant atteinte à la confidentialité, l'intégrité et la

을 것이다.

이를 종합해볼 때, 기존에 존재하지 않았던, 시스템이나 네트워크에 대한 공격행위를 지칭하는 고유한 의미의 사이버범죄를 넘어, 사이버공간과 연계된 다양한 형태의 범죄행위로 사이버범죄 정의의 외연을 점점 더 넓혀가고 있는 것을 알 수 있고, 사이버공간을 매개로 한 범죄행위와 관련 법률에 대한 문제점을 고려하는 입장에서 생각해 볼 때, 사이버공간을 수단으로 사용하면서 나타날 수 있는 범죄까지도 그 대상으로 정의하는 것이 더욱 타당하다고 생각된다.

2. 사이버범죄 분류

사이버범죄의 분류에 있어서는 여러 시각이 존재하고, 범죄의 특성상 아직도 현재 진행형인 듯하다. 그 중에서 대표적인 것들을 언급해 보면, 사이버공간의 등장으로 새롭게 발생하는 범죄와 사이버공간을 이용한 전통적인 범죄로 나누는 견해, 사이버공간을 합법적으로 이용한 범죄군과 보호되는 사이버공간을 불법적으로 침입하여 이루어진 범죄로 구분하는 견해, 사이버공간에서의 전통적 범죄 유형과 사이버공간에서의 새로운 범죄유형 그리고 사이버공간에 특유한 불법유형 등 세 가지로 구분하는 견해[6], 정보통신기술에 고유한 범죄와 정보통신기술에 관련된 범죄 그리고 정보통신기술로 촉진된 범죄와 같이 세 가지로 구분하는 견해[7]가 바로 그것이다.

'유럽 사이버범죄방지조약'은 사이버범죄의 유형을 첫째, 컴퓨터데이터와 시스템의 기밀성, 무결성 및 유용성에 대한 범죄(Offences against the confidentiality, integrity and availability of computer data and systems),

---

disponibilité des systèmes informatiques, des réseaux et des données ainsi que l'usage frauduleux de tels systèmes, réseaux et données, ou des infractions pénales dans le cyber-espace en utilisant les réseaux informatiques et l'information électronique ».

6) 강동범, 앞의 글.

7) 최정호, 앞의 글.

둘째, 컴퓨터 관련 범죄(Computer-related offences), 셋째, 컨텐츠 관련 범죄(Content-related offences), 넷째, 저작권 및 저작인접권 침해에 관한 범죄(Offences related to infringements of Copyright and related rights) 등 네 가지로 구분하였다.[8)]

이들 견해와는 다소 차이를 보이지만, 경찰청 '사이버테러대응센터'[9)]에서는 사이버범죄를 크게 '사이버테러형 범죄'와 '일반 사이버범죄'로 구분하고 있다. 비록 이와 같은 유형 구분방식의 문제점을 찾을 수 없는 것은 아니지만, 실무상 드러날 수 있는 법률적 문제점을 부각시키기 위해, 경찰청의 분류 방법에 따라 이 글을 구성하고자 한다.

3. 사이버범죄 관련 법률

가. 사이버테러형 범죄 관련 법률

실무상 사이버테러형 범죄라고 지칭하는 해킹, 컴퓨터바이러스와 관련된 법률로는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 '정보통신망법'이라고 약칭함), '정보통신기반 보호법' 및 '물류정책기본법'을 들 수 있고, 나타나는 범죄 형태는 <표 1>과 같다.

<표 1> 사이버테러형 범죄 관련 법률

유 형	범죄 형태	관련 법률
해 킹	정보통신망에 침입, 미수	정보통신망법 제72조 제1항 제1호, 제2항, 제48조 제1항
	정보통신망에 장애 발생	정보통신망법 제71조 제10호, 제48조 제3항
컴퓨터 바이러스	악성프로그램 전달, 유포	정보통신망법 제71조 제9호, 제48조 제2항

8) 이영준, 정 완, 금봉수, "사이버범죄방지조약에 관한 연구", 한국형사정책연구원 연구보고서 01-30, 2001년 12월.

9) 경찰청 사이버테러대응센터 (Cyber Terror Response Center), Cyber Cop NETAN, www.ctrc.go.kr.

(1) 해 킹

‘정보통신망법[10]’ 상에는 해킹과 관련하여 정보통신망에 침입과 장애발생 이렇게 두 가지 범죄 형태를 처벌하고 있다.

첫째, 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입한 자에게는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 하고 있고, 이에 대한 미수범을 처벌하고 있으며,[11] 둘째, 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 한 자에 대해서는 5년 이하의 징역 또는 5천만원 이하의 벌금으로 처벌한다.[12]

‘정보통신기반 보호법’[13]에서는, 첫째, 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위, 둘째, 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위, 셋째, 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위, 이와 같이 세 가지 유형의 행위 중 하나로 주요정보통신기반시설을 교란·마비 또는 파괴한 자에 대하여 10년 이하의 징역 또는

10) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (일부개정 2008.6.13 법률 제9119호, 시행일 2008.12.14.)

11) [제48조] (정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다. [제72조] (벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 1. 제48조 제1항을 위반하여 정보통신망에 침입한 자 ② 제1항 제1호의 미수범은 처벌한다.

12) [제48조] (정보통신망 침해행위 등의 금지) ③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다. [제71조] (벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 10. 제48조 제3항을 위반하여 정보통신망에 장애가 발생하게 한 자.

13) 정보통신기반 보호법 (일부개정 2008.2.29 법률 제8852호)

1억원 이하의 벌금으로 처벌하며, 이에 대한 미수범을 처벌하고 있다.[14]

'물류정책기본법[15]'에서는, 종합물류정보망 또는 국가물류통합데이터베이스에 의하여 처리·보관 또는 전송되는 물류정보를 훼손하거나 그 비밀을 침해·도용 또는 누설한 자에 대해 5년 이하의 징역 또는 1억원 이하의 벌금에, 보호조치를 침해하거나 훼손한 자는 3년 이하의 징역 또는 5천만원 이하의 벌금에 처하고 있다.[16]

(2) 컴퓨터바이러스

'정보통신기반 보호법' 제12조 내용 중에 '컴퓨터바이러스'라는 용어가 등장하긴 하지만, 이는 주요정보통신기반시설의 데이터를 파괴하거나 운영을 방해하기 위한 목적을 가진 위반행위의 하나로서 컴퓨터바이러스와 같은 프로그램을 투입하는 행위를 예시적으로 나타낸 것일 뿐으로, 컴퓨터바이러스와 관련된 불법행위에 대한 처벌조항이라고 볼 수 없다.

컴퓨터바이러스의 전달이나 유포에 대한 처벌조항은 '정보통신망법' 제71조 제9호, 제48조 제2항이며, 정당한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프

14) [제12조] (주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다. 1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위, 2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위, 3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위, [제28조] (벌칙) ① 제12조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. ② 제1항의 미수범은 처벌한다.

15) 물류정책기본법 (일부개정 2008. 2. 29. 법률 제8852호)

16) [제71조] (벌칙) ② 제33조제2항을 위반하여 종합물류정보망 또는 국가물류통합데이터베이스에 의하여 처리·보관 또는 전송되는 물류정보를 훼손하거나 그 비밀을 침해·도용 또는 누설한 자는 5년 이하의 징역 또는 1억원 이하의 벌금에 처한다. ③ 제33조 제5항을 위반하여 종합물류정보망 또는 국가물류통합데이터베이스의 보호조치를 침해하거나 훼손한 자는 3년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

로그램(“악성프로그램”)을 전달 또는 유포한 자에 대해서는 5년 이하의 징역 또는 5천만원 이하의 벌금으로 처벌하고 있다[17].

나. 일반 사이버범죄 관련 법률

사이버공간과 관련된 일반 사이버범죄 또는 사이버공간을 범죄의 수단으로 이용하는 범죄는 그 유형이 매우 다양하고, 분류하기에 따라서 지극히 확장될 수도 있으며, 새로운 기술의 발달에 따라 새로운 유형의 범죄가 출현할 수도 있으므로, 관련된 법률을 일괄적으로 정리하기에는 어려움이 있다. 여기서는 현재 경찰 실무상 일반적으로 다루어지고 있는 일반 사이버범죄에 대해서 그 유형과 관련된 법률을 살펴보고자 한다. 각 유형에 따른 범죄 형태는 <표 2>와 같다.

(1) 인터넷사기

일반 사이버범죄에서 수치상으로 가장 큰 비중을 차지하고 있는 것이 바로 인터넷사기 유형이다. 인터넷을 통한 전자상거래와 오픈마켓이 발달할수록 그 과정에서 발생하는 인터넷사기의 규모는 날로 팽창하고 있다. 날이 갈수록 각종 신종기법의 인터넷사기가 진화하고 있는 가운데, 인터넷 온라인 게임과 관련된 사기 사건의 피해도 무시할 수 없는 수준이다. 인터넷사기는 일반 사기사건과 마찬가지로 형법 제347조에 따라 10년 이하의 징역 또는 2천만원 이하의 벌금으로 처벌할 수 있다.[18]

---

17) [제48조] (정보통신망 침해행위 등의 금지) ② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다. [제71조] (벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 9. 제48조 제2항을 위반하여 악성프로그램을 전달 또는 유포한 자.

18) [제347조] (사기) ① 사람을 기망하여 재물의 교부를 받거나 재산상의 이익을 취득한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. ② 전항의 방법으로 제삼자로 하여금 재물의 교

<표 2> 일반 사이버범죄 관련 법률

유형	범죄 형태		관련 법률
인터넷사기	온라인 사기		형법 제347조, 제347조의2, 제348조
	인터넷 게임 관련 사기		
불법·유해 사이트	음란물		정보통신망법 제74조 제1항 제2호
	인터넷 도박		형법 제246조~제248조
	밀거래사이트	불법 무기류 매매	총포·도검·화약류등단속법 제70조 제1항 제1호/ 제71조 제1호
		마약류 밀거래	마약류관리에 관한 법률 제60조 제1항 제1호, 제3호
		위조 신분증 밀거래	형법 제225조, 제229조
		해외명품 불법복제 판매	상표법 제93조
		대포폰, 대포통장 거래	주민등록법 제37조 제9호, 형법347조
	자살사이트		형법 제282조
	해결사 사이트(청부살인, 폭력, 신용카드 연체해결, 카드깡, 채권·채무 해결)		형법, 폭력행위등 처벌에 관한 법률, 여신전문금융업법
사이버 명예훼손	인터넷 상 명예훼손		정보통신망법 제70조
사이버스토킹 및 성폭력	사이버스토킹		정보통신망법 제74조 제1항 제3호
	인터넷상 성폭력		성폭력범죄의 처벌 및 피해자 보호 등에 관한 법률 제14조
불법복제	영화, 음악 파일 복제		저작권법 제136조
	컴퓨터프로그램 복제		컴퓨터프로그램 보호법 제46조
개인정보침해	정보통신제공자 의무위반 등		정보통신망법
	비밀침해 등		형법, 정보통신망법, 통신비밀보호법, 주민등록법
스팸메일	규정에 위반한 광고메일 전송		정보통신망법 제74조
	청소년 대상 청소년유해매체물 광고		정보통신방법 제73조

부를 받게 하거나 재산상의 이익을 취득하게 한 때에도 전항의 형과 같다.

한편, 현행 형법 상 컴퓨터와 관련한 처벌조항으로는 제314조(업무방해)와 함께 거의 유일한 조항인 제347조의2(컴퓨터등 사용사기)에 따라, 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 권한없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.[19]

(2) 불법·유해사이트

불법·유해사이트란 공공의 안녕·질서 또는 미풍양속을 해하는 등 반사회적 내용을 담고 있는 사이트로 개설목적 자체가 법률에 위반되거나 범죄수단으로 사용되는 위법사이트를 포함한다. 사회의 여러 가지 현상에 따라 가장 민감하고 다양하게 분화할 수 있는 범죄유형이라고 할 수 있으며, 누구나 접근할 수 있는 사이버공간에 이러한 유해정보를 제공하는 것은 청소년이나 기타 일반 네티즌 등에게 범죄의 유혹을 제공함으로써 사회적으로도 큰 물의를 빚게 된다.

현행 법률에 문제가 되는 불법·유해사이트의 대상을 정리해보면, 첫 번째로 음란물과 관련된 사이트를 들 수 있는데, 정보통신망을 통하여 음란물을 배포·판매·임대하거나 공연히 전시한 자는 '정보통신망법' 제74조 제1항 제2호에 따라 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.[20]

인터넷 상에서 행하여지는 도박과 관련해서는 '형법'으로 처벌하는데, 인터넷 사이트에 개설된 도박에 참여한 자와 영리의 목적으로 도박 사이트를 운

19) [제347조의2] (컴퓨터등 사용사기) 컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

20) 정보통신망법 [제74조] (벌칙) ① 다음 각호의 1에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 2. 정보통신망을 통하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공연히 전시한 자

영한 자, 복표를 발매하거나 이를 중개한 자도 모두 처벌 대상이다.[21]

인터넷 상에서 불법 총기를 매매하였을 경우에는 '총포·도검·화약류등 단속법'으로 처벌하는데, 총포, 화약류 매매의 경우 같은 법 제70조 제1항 제2호, 제6조 제1, 2항, 제12조 제1항에 따라 10년 이하의 징역 또는 2천만원 이하의 벌금에, 도검, 분사기, 전기충격기, 석궁 매매의 경우 같은 법 제71조 제1호, 제6조 제1, 2항, 제12조 제1항에 따라 5년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

마약류 밀거래 사이트는 '마약류관리에 관한 법률'을 적용하여, 마약을 취급하거나 그 처방전을 교부한 자는 같은 법 제60조 제1항 1호, 제28조 제1항에 따라, 향정신성의약품을 매매, 매매의 알선, 수수, 소지, 소유, 사용, 관리, 조제, 투약, 교부한 자, 처방전을 발부한 자는 같은 법 제60조 제1항 3호, 제4조 제1항에 따라 10년 이하의 징역 또는 1억원 이하의 벌금으로 처벌한다.

위조신분증 밀거래 사이트는 공문서 등의 위조, 변조에 해당되어 형법 제225조, 제229조에 의해 10년 이하의 징역을, 해외명품 불법 복제품을 인터넷 상에서 판매하는 행위는 상표법 제93조(상표권 및 전용사용권 침해행위)에 따라 7년 이하의 징역 또는 1억원 이하의 벌금에 처해진다.

대포폰이나 대포통장을 거래하는 행위에 대해서는 '주민등록법' 제37조 제9호에 따라 3년 이하 징역 또는 1천만원 이하 벌금에 처해지지만, 이를 구입하여 사용하는 사람은 정상적인 목적이 아닌 사기 등 불법행위에 이용할 것이므로 그에 따른 법률 적용도 당연히 따르게 될 것이다.

자살을 조장하는 사이트에 대해서는 '형법' 제252조 제1, 2항에 따라 촉탁 또는 승낙에 의한 살인, 자살교사, 방조 등을 적용하여 1년 이상 10년 이하

21) 형법 [제246조] (도박, 상습도박) ① 재물로써 도박한 자는 500만원이하의 벌금 또는 과료에 처한다. 단, 일시오락정도에 불과한 때에는 예외로 한다. ② 상습으로 제1항의 죄를 범한 자는 3년이하의 징역 또는 2천만원이하의 벌금에 처한다. [제247조] (도박개장) 영리의 목적으로 도박을 개장한 자는 3년 이하의 징역 또는 2천만원이하의 벌금에 처한다. [제248조] (복표의 발매등) ① 법령에 의하지 아니한 복표를 발매한 자는 3년 이하의 징역 또는 2천만원이하의 벌금에 처한다. ② 전항의 복표발매를 중개한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

징역으로 처벌하며, 청부살인이나 폭력을 행하는 해결사 사이트의 경우에는 '형법'과 '폭력행위 등 처벌에 관한 법률'을, 신용카드 연체해결이나 카드깡, 채권·채무 해결을 위한 청부 해결사 사이트에 대해서는 '여신전문금융업법'을 적용하여 처벌한다.

(3) 사이버 명예훼손

요즘 인터넷 상에서 가장 민감한 토론의 소재로 등장한 것이 바로 사이버 명예훼손 유형이다. 이는 인터넷 게시판이나 메신저, 전자우편을 통해 타인의 명예를 훼손하는 글·사진 등을 게시하거나 유포하는 행위를 말하며, 불특정 다수인의 무제한 접근이 가능한 인터넷의 특성상 시간이나 공간의 제한 없이 단시간 내에 급속도로 유포될 수 있기 때문에 그로 인한 피해가 심각할 수밖에 없고, 이러한 이유로 '정보통신망법'에서는 일반 명예훼손죄보다도 더 무겁게 이를 처벌하고 있다.[22]

사람을 비방할 목적으로 공연히 사실을 적시하여 타인의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에, 허위의 사실을 적시하여 타인의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

(4) 사이버스토킹 및 성폭력

사이버스토킹이란 인터넷 게시판, 대화방, 전자우편 등 정보통신망을 통하여 상대방이 원하지 않는 접속을 지속적으로 시도하거나 욕설 또는 협박의

22) 정보통신망법 [제70조] ① 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처한다. ② 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다. ③ 제1항과 제2항의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다.

내용을 담고 있는 전자우편 송신 행위를 지속하는 것을 말한다. 우리나라에서는 현재까지 사이버스토킹이 구체적인 범죄로 규정되어 있지 않지만, '정보통신망법'에 따라, 정보통신망을 통하여 공포심이나 불안감을 유발하는 말, 음향, 글, 화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금으로 처벌하고 있다.[23]

아울러, 자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화·우편·컴퓨터 기타 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건을 상대방에게 도달하게 한 자는 '성폭력범죄의 처벌 및 피해자 보호 등에 관한 법률'에 따라, 2년 이하의 징역 또는 500만원 이하의 벌금에 처한다.[24]

(5) 불법복제

컴퓨터와 인터넷이 발달하고, P2P(peer to peer) 방식의 인터넷 자료공유 서비스가 확산되면서 자료공유의 자유를 원하는 네티즌들 사이에 범죄의식 없이 불법복제된 컴퓨터프로그램이나 컴퓨터 파일 형태의 영화 및 음악들이 유포되고 있다. 이는 엄연히 '저작권법' 및 '컴퓨터프로그램 보호법'으로 보호되는 창작물에 대한 저작권을 침해하는 행위로서, 관련 기관들의 단속이 수시로 행하여지고 있지만, 워낙 광범위하게 이루어지는 복제행위와 내려받기(다운로드)로 인해 단속과 수사에 있어 어려움을 겪고 있는 실정이고, 네티즌들의 올바른 이용의식에만 의존하기에는 한계가 있어 보인다.

불법적인 영화 및 음악 파일들에 대해서는 저작권법 제136조 제1항에 따

23) 정보통신망법 [제74조] ① 다음 각호의 1에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 3. 정보통신망을 통하여 공포심이나 불안감을 유발하는 말, 음향, 글, 화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자.

24) 성폭력범죄의 처벌 및 피해자 보호 등에 관한 법률 [제14조] (통신매체이용음란) 자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화·우편·컴퓨터 기타 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건을 상대방에게 도달하게 한 자는 2년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

라, 이를 복제・공연・공중송신・전시・배포・대여・2차적 저작물 작성의 방법으로 재산적 권리를 침해한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있고,[25] 컴퓨터프로그램에 대해서는, 정당한 권원없이 복제・개작・번역・배포・발행 및 전송의 방법으로 프로그램저작권 또는 배타적 발행권을 침해하거나 프로그램의 기술적 보호조치를 회피, 제거, 손괴 등의 방법으로 무력화한 행위에 대해 '컴퓨터프로그램 보호법' 제46조 제1항에 따라 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하고 있다.[26]

(6) 개인정보침해

쇼핑, 오락, 교육, 행정, 금융업무 등 생활 전반이 온라인을 통해 이루어짐에 따라 개인의 성명, 주민등록번호, 주소 및 전화번호 등과 같은 개인정보의 중요성은 점점 커지고 있다. 개인정보침해 범죄의 심각성은 단순히 개인정보가 유출된 것으로 끝나는 것이 아니라 유출된 개인정보가 2차적으로 다른 범죄에 사용될 수 있기 때문이며, 이런 개인정보는 재화로서의 가치를 갖고 유통되기도 하기 때문에 이를 법으로써 엄격히 규제하고 있다.

'정보통신망법'에서는 이용자의 동의 없는 개인정보 수집, 개인정보 수집시 기본사항 미고지 및 이용약관 등에 명시하지 않은 경우, 서비스 제공에 불필요한 개인정보 요구, 제공받은 목적 이외로 개인정보 사용, 이용자의 동의

25) 저작권법 [제136조] ① 저작재산권 그 밖의 이 법에 의하여 보호되는 재산적 권리(제93조의 규정에 따른 권리를 제외한다.)를 복제・공연・공중송신・전시・배포・대여・2차적 저작물 작성의 방법으로 침해한 자는 5년 이하의 징역 또는 5천만원이하의 벌금에 처하거나 이를 병과할 수 있다.

26) 컴퓨터프로그램보호법 [제46조] (벌칙) ① 다음 각호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있다. 1. 제29조 제1항의 규정을 위반한 자, 3. 제30조의 규정을 위반한 자 [제29조] (프로그램저작권 침해행위 등) ① 누구든지 정당한 권원없이 다른 사람의 프로그램저작권을 복제・개작・번역・배포・발행 및 전송의 방법으로 침해하거나 다른 사람의 프로그램배타적발행권 등을 복제・배포 및 전송의 방법으로 침해하여서는 아니된다. [제30조] (기술적 보호조치의 침해 등의 금지) ① 누구든지 정당한 권원없이 기술적 보호조치를 회피, 제거, 손괴 등의 방법으로 무력화 (이하 "기술적 보호조치 무력화"라 한다)하여서는 아니된다.

없이 제3자에게 개인정보 제공, 개인정보 관리책임자 미지정, 개인정보 취급자의 개인정보 유출, 이용자의 개인정보 열람요구에 불응, 오류정정·삭제요구에 불응, 오류정정 요구를 접수한 후에도 정정하지 않은 정보 이용, 타인의 개인정보를 훼손하거나 비밀을 침해·도용·누설, 수신자가 원하지 않는 영리목적의 광고성 정보 전송 등 세밀한 각 유형에 따른 위반행위에 대해 처벌하고 있다. 개인정보 뿐만 아니라, 정보통신망으로 처리되는 비밀의 침해행위에 대해서도 '형법', '정보통신망법', '통신비밀보호법', '주민등록법' 등 다양한 법률로 제재를 가하고 있다.

(7) 스팸메일

스팸메일의 경우, 일반 사이버범죄의 유형에도 해당하지만, 정보통신망의 안정적 운영을 방해할 목적을 지닌 공격의 한 형태로 쓰일 수 있어 사이버테러형 범죄에 해당할 수 있다는 점에 유의해야 한다. 여기서는 단순히 영리목적의 광고를 스팸메일을 통해서 보내는 행위만을 대상으로 한다.

'정보통신망법'에 의하면, 광고를 전송하는 자가 광고를 전송하는데 지켜야 할 사항들을 위반하여 기술적 조치를 하거나, 운영자 또는 관리자의 사전동의 없이 인터넷 홈페이지에서 자동으로 전자우편주소를 수집하는 프로그램 그 밖의 기술적 장치를 이용하여 전자우편주소를 수집하고 이를 판매·유통하거나 이를 정보전송에 이용한다면 1천만원 이하의 벌금으로 처벌할 수 있다.[27]

---

27) 정보통신망법 [제74조] (벌칙) 다음 각호의 어느 하나에 해당하는 자는 1천만원 이하의 벌금에 처한다. 1. 제50조제6항의 규정을 위반하여 기술적 조치를 한자 [제50조] (영리목적의 광고성 정보전송의 제한) ⑥영리를 목적으로 광고를 전송하는 자는 다음 각호의 1에 해당하는 기술적 조치를 하여서는 아니된다. 1. 광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 조치 2. 숫자·부호 또는 문자를 조합하여 전화번호·전자우편주소 등 수신자의 연락처를 자동으로 생성하는 조치 3. 영리목적의 광고성 정보 전송을 목적으로 전자우편주소를 자동으로 등록하는 조치 4. 광고성 정보 전송자의 신원 또는 광고 전송 출처를 은폐하기 위한 각종 조치 5. 제50조의2의 규정을 위반하여 전자우편주소를 수집·판매·유통 또는 정보전송에 이용한 자 [제50조의2] (전자우편주소의 무단 수집행위 등 금지) ① 누구든지 인터넷 홈페이지 운영자 또는 관리자의 사

또한, 전자메일을 통해 청소년에게 유해한 매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년 접근을 제한하는 조치없이 공개적으로 전시한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.[28]

Ⅲ. 사이버범죄 관련 법규의 문제점

1. 사이버테러형 범죄 관련 법규의 문제점

가. 법조문상 관련 용어들의 불명확한 정의

'정보통신망법' 제48조 제2항과 제71조 제9호에는 "정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램", 즉 '악성프로그램'이라는 용어를 사용하고 있는 반면에, '정보통신기반 보호법' 제12조 제2호에는 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 투입하는 프로그램의 예시로 '컴퓨터바이러스'와 '논리폭탄'이라는 용어를 사용하고 있다.

먼저 용어에 대한 정의를 살펴보면 '악성프로그램'(malicious program)[29]

전동의 없이 인터넷 홈페이지에서 자동으로 전자우편주소를 수집하는 프로그램 그 밖의 기술적 장치를 이용하여 전자우편주소를 수집하여서는 아니된다. ② 누구든지 제1항의 규정을 위반하여 수집된 전자우편주소를 판매·유통하여서는 아니된다. ③ 누구든지 제1항 및 제2항의 규정에 의하여 수집·판매 및 유통이 금지된 전자우편주소임을 알고 이를 정보전송에 이용하여서는 아니된다.

28) 정보통신망법 [제73조] (벌칙) 다음 각호의 1에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 2. 제42조의2의 규정을 위반하여 청소년유해매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년 접근을 제한하는 조치없이 공개적으로 전시한 자 [제42조의2] (청소년유해매체물의 광고금지) 누구든지 청소년보호법 제7조제4호의 규정에 의한 매체물로서 동법 제2조 제3호의 규정에 의한 청소년유해매체물을 광고하는 내용의 정보를 정보통신망을 이용하여 부호·문자·음성·음향·화상 또는 영상 등의 형태로 동법 제2조 제1호의 규정에 의한 청소년에게 전송하거나 청소년 접근을 제한하는 조치없이 공개적으로 전시하여서는 아니된다.

29) 악성 프로그램은 주로 웹페이지를 검색할 때, P2P 서비스를 이용할 때, 셰어웨어를 사용할 때, 불법복제 프로그램을 사용할 때, 내부자(해커)가 직접 설치할 때, 전자우편의 첨부파일 또는 메신저 파일을 열 때 침투한다. 주요 증상은 네트워크 트래픽 발생, 시스템 성능 저하, 파일 삭제, 이메일

은 악성코드(malicious code), 말웨어(malware, malicious software)라고도 불리며, 악의적인 목적을 위해 작성된 실행 가능한 프로그램의 통칭으로 자기 복제 능력과 감염 대상 유무에 따라 '컴퓨터바이러스', '웜'(worm),[30] '트로이목마'(trojan horse)[31] 등으로 분류된다. 즉, '악성프로그램'의 대표격이 바로 '컴퓨터바이러스'이며, 컴퓨터바이러스는 컴퓨터프로그램이나 실행 가능한 부분을 변형하여, 여기에 자기 자신 또는 자신의 변형을 복사하여 컴퓨터 작동에 피해를 주는 명령어들의 조합이라고 정의된다.

'논리폭탄'은 해커나 크래커가 프로그램 코드의 일부를 조작해 이것이 소프트웨어의 어떤 부위에 숨어 있다가 특정 조건에 달했을 경우 실행되도록 하는 것이다. 즉 논리폭탄이라는 용어 그대로 프로그램에 어떤 조건이 주어져 숨어 있던 논리에 만족되는 순간 폭탄처럼 자료나 소프트웨어를 파괴하여, 자동으로 잘못된 결과가 나타나게 한다.

이와 같이 자칫 혼란을 가져올 수 있는 기술적인 용어들이 사이버테러형 범죄와 관련된 법조문 내에서 명확한 개념정의 없이 개별적으로 나열되는 것은 문제를 불러일으킬만한 소지가 있다. 물론, 계속해서 발전하는 정보통신 관련 기술에 사용되는 용어들을 일일이 제 때에 설명해 내기가 어려울 수 있지만, 법령에 일반적으로 사용되고 있으면서도 해석상 문제를 불러일으킬 수 있는 용어인 '데이터'나 '악성프로그램', '해킹'에 대한 명쾌한 정의가 없고, 매일매일 새로운 변종들이 탄생과 소멸을 반복하는 '컴퓨터바이러스'나 기타 해킹 기법 중의 하나인 '메일폭탄', '논리폭탄', '서비스거부공격' 등을 아무런 설명 없이 버젓이 조문 안에 명시해 놓았는데, 이들 용어에 대한 일

자동발송, 개인 정보 유출, 원격 제어 등이다. (출처 : 두산백과사전 EnCyber & EnCyber.com)

30) 다른 프로그램의 감염없이 자신 혹은 변형된 자신을 복사하는 명령어들의 조합이라고 정의된다. 웜은 네트워크 어웨어 바이러스(Network Aware virus)라고 불리기도 한다. 웜은 기억장소에 코드 형태로 존재하거나 혹은 실행파일로 존재하며 실행되면 파일이나 코드 자체를 다른 시스템으로 복사한다. (출처 : 두산백과사전 EnCyber & EnCyber.com).

31) 컴퓨터의 프로그램 내에 사용자는 알 수 없도록 프로그래머가 고의로 포함시킨 자기 자신을 복사하지 않는 명령어들의 조합이라고 정의된다. 고의로 포함시켰다는 점에서 프로그램의 버그(bug)와 다르며, 자신을 복사하지 않는다는 점에서 바이러스나 웜과도 약간 다르다. (출처 : 두산백과사전 EnCyber & EnCyber.com).

반적이거나 구체적인 설명이 없다면 계속 진화하고 있는 새로운 형태의 사이버테러리즘 행위에 제대로 적용할 수 없을 뿐만 아니라, 요즘과 같이 여러 유형의 해킹 형태가 복합적으로 작용하는 경우, 정작 필요할 때에는 오히려 법률 적용에 혼란만을 가져올 것이다.

나. 처벌의 내용과 형량의 차이

‘정보통신망법’과 ‘정보통신기반 보호법’의 처벌 조항을 살펴보면, 일반적인 정보통신망에 대하여 상대적으로 그 중요도가 높은 주요정보통신시설을 지정하고 이를 침해한 행위에 대해 처벌을 강화한 것에는 어느 정도 수긍할 수 있으나, ‘물류정책기본법’에 따라 종합물류정보망 또는 국가물류통합데이터베이스의 침해행위에 대한 처벌을 상대적으로 강화한 것에는 쉽게 동의할 수가 없다.

처벌의 내용을 다시 한 번 살펴보면, ‘정보통신망법’에서 정보통신망 침입은 3년 이하의 징역 또는 3천만원 이하의 벌금에, 정보통신망에 장애발생은 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하고 있고, ‘정보통신기반보호법’에서는 주요정보통신기반시설의 교란·마비 또는 파괴행위에 대해 10년 이하의 징역 또는 1억원 이하의 벌금에, ‘물류정책기본법’에서는 물류정보훼손이나 비밀침해·도용 또는 누설 행위에 대해 5년 이하의 징역 또는 1억원 이하의 벌금에, 보호조치 침해·훼손 행위에 대해 3년 이하의 징역 또는 5천만원 이하의 벌금으로 처벌하고 있다. 즉, 산술적으로 따져볼 때, 주요정보통신기반시설에 대한 침해행위는 일반 정보통신망의 그것에 비해 정확히 2배의 처벌을, 물류정보망의 훼손행위에 대해서는 일반 정보통신망의 그것보다 2배의 벌금을, 보호조치 침해에 대해서는 1.7배의 벌금을 예견하고 있다.

물론 물류통신망의 사회적 중요성을 부인하는 것은 아니지만, 병원이나 교육기관, 대기업 등 다른 사회주요기간망에 비해 이를 특별히 더 중요하게

다룰 이유가 없고, 이를 통해 오히려 다른 정보통신망에 대한 배려가 상대적으로 부족해 보이기까지 한다.

아울러, 세 법률은 그들이 보호대상으로 하는 정보통신망만 다를 뿐, 비슷한 유형의 불법 침해행위를 처벌하고 있는데, 첫째, '정보통신기반 보호법'에서는 주요정보통신기반시설을 교란·마비 또는 파괴한 행위와 미수범만을 처벌하고 있어, 미수의 요건에까지는 이르지 않는 주요정보통신기반시설에의 단순침입 행위는 '정보통신기반 보호법'을 적용하지 못하고 오히려 논리적으로는 '정보통신망법'의 기수범으로 적용받게 되고, 둘째, '정보통신망법'이나 '정보통신기반 보호법'에서는 컴퓨터바이러스 또는 사이버공격 등과 같은 침해행위도 처벌하고 있는 반면, '물류정책기본법'에서는 물류정보를 훼손하거나 그 비밀을 침해·도용 또는 누설한 행위, 보호조치 침해·훼손한 행위만을 처벌의 대상으로 규정하고 있어, 같은 면을 바라보고 있는 세 법률의 일관성이 부족하다 할 것이다.

다. 사이버범죄의 조직화에 대비

사례 : 전문 해커단 고용 인터넷 게임 아이템 해킹 판매

피의자들은 2005년 3월경 중국 전문 해커단을 고용하여, 채팅으로 해킹프로그램을 유포하게 한 후 컴퓨터 150여대를 해킹하여 사이버머니를 절취하고 이를 판매하여 5천만 원 상당의 부당이득을, 4월경에는 국내 OOO 게임 사이트 서버를 해킹한 후 복제한 사이버머니를 중개상에게 판매하여 2억 5천만 원 상당의 부당이득을, 5월경에는 국내 컴퓨터 5만여 대에 악성프로그램을 감염시켜 이를 해킹한 후, 사이버머니를 절취하고 이를 판매하여 2억 원 상당 부당이득을, 인터넷 카페에서 해킹 프로그램을 유포하여 컴퓨터 2,000여대를 해킹 후, 절취한 사이버머니를 되팔아 3천여만 원의 부당이득을 취하였다.

경찰은 2005년 6월 20일에서 28일간 인천, 진주 지역 등 5개소에서 피의자들을 검거하여 9명을 구속하고, 13명은 불구속 수사하였으며, 중국인 해커 8명은 인터폴에 통보하여 사법처리 요청하였고, 상습적으로 해킹을 시도하는 IP주소에 대해서는 한국정보보호진흥원에 통보하였다.

과거 단순 호기심 차원이나 자기를 과시하는 욕구에서 비롯되어 이뤄졌던 '해킹'이 '검은 돈'과 결탁되면서 위 사례처럼 해킹 산업이 조직화, 분업화되고 있다. 악성코드 제작과 웹 사이트 해킹은 중국에서, 불법 아이템 거래와 현금 환전은 국내에서 각각 이루어지는 행태를 보이면서, 중국을 경유하면 수사기관들의 추적 자체가 어렵다는 허점을 악용해 국제 분업화된 형태로 암거래 시장이 진화되고 있는 것이다.

세계에서 그 유례를 찾아볼 수 없을 정도로 활성화된 우리나라의 인터넷 게임시장, 이 인터넷 게임을 이용하는 데 필요한 아이템 그리고 고가의 게임 아이템을 거래하는 중개 사이트. 우리나라는 인터넷 게임의 메카라는 긍정적 명성의 화려한 그림자 속에 인터넷 게임과 관련된 독특한 형태의 사이버범죄가 게임 내·외적으로 복잡하게 얽혀 부정적인 면모도 다수 보여주고 있다.

개인의 능력을 과시하기 위해 이루어지던 사이버테러형 범죄유형이 이제는 집단화하여 범죄조직을 구성하고, 점점 더 전문화, 분업화, 국제화되고 있는 추세이다. 사이버테러형 범죄의 경우 집단의 범죄는 개인의 범죄일 때보다 그 피해영역 범위가 넓어지고 파급효과도 훨씬 배가된다고 할 수 있기 때문에, 이런 조직화를 미연에 방지할 필요가 있다.

프랑스 형법 제323-4조는 정보통신망에 침입하거나 컴퓨터바이러스를 유포하는 행위 등을 준비하기 위한 목적으로 형성된 조직이나 공모에 참여하는 것을 처벌한다. 이는 해킹과 관련된 지식을 교류할 수 있는 비공식적인 조직에의 참여까지도 미리 예방하기 위한 목적을 띠는데, 입법자는 예비나 공모, 은닉까지 이어지지 않는 조직결성 자체만으로도 처벌을 하는 것을 예상하고 있고, 조직 참가자는 공범으로 간주되어 주범과 같은 형이나 또는 가장 중한 형으로 처벌 받도록 되어 있다 우리도 사이버테러형 범죄의 경우 범죄조직 결성시와 범죄시에 이들을 가중처벌하는 규정의 삽입을 적극 고려해야할 것이다.

라. 수사 및 처벌의 국제적 공조 필요

사례 : 중국 해커집단에 의한 주요 기관 해킹

피의자들은 2003년 12월 말경부터 보안이 취약한 국내 민간 시스템을 공격하여 이를 공격 거점으로 사용하기 위해, 악성 프로그램(변종 Peep과 변종 Revacc)을 전자우편 또는 인터넷 게시판에 정상 첨부파일인 것처럼 위장하여 발송하거나 게시한 후, 사용자가 의심 없이 파일을 실행시키도록 유도하였다.

이런 악성 프로그램은 역접속 기능 및 도메인주소를 사용해 방화벽 등 피해기관의 침입탐지시스템을 무력화하는 기능을 하였으며, 시스템을 장악한 후에는 악성프로그램의 감시 및 파일전송 기능을 이용해 시스템 내부의 정보를 획득하는 등의 불법행위를 저질렀다. 피의자들은 또한 공격거점으로 이용한 국내 민간시스템과 피해기관의 시스템에 체계적인 명칭을 부여해 관리하는 등 아주 치밀하게 사전 계획을 작성한 것으로 드러났다.

이런 방법으로 2004년 2월 초경 OO연구소 컴퓨터를 시작으로, 다수 민간시스템을 사전에 장악하여 주요기관 공격선 다변화 및 탐지·추적 방지를 위한 중간 경유지로 이용하였다. 해커들은 중국 소재 특정 네트워크를 이용하였으며 공격에 사용된 상당수의 프로그램에 중국어가 사용되었다.

이들 해커 집단에 의해 2004년 4월부터 6월까지 국내 10개 공공기관 222대의 컴퓨터와 민간시스템 79대가 해킹 피해로 자료 유출 등의 피해를 입었다. 또한 OO 공공기관 직원 122명의 전자메일 ID를 도용당했으며, 일부 언론사 기자들의 전자메일도 도용당한 것으로 드러났다.

경찰청은 외교통상부와 협조하여 외교채널 및 인터폴 공조를 통해 중국 공안부에 공격자에 대한 공조수사를 추진하였으나 중국 측의 수사불가 통보로 범인들을 검거하지 못한 채 수사를 종결하였다.

위 사례는 해외 특정 세력에 의한 국가 주요정보 시스템 해킹시도를 인지하여 일부 용의자와 공격 수법 및 경로 등 전모를 밝힌 최초의 사건으로, 그동안 드러나지 않은 상태에서의 추측만으로 존재하던 해킹 단체 및 국가간 공격을 사실로 밝혔다는 점에서 큰 의의를 찾을 수 있지만, 국가 간의 공조 미비로 더 이상 수사의 진전을 볼 수 없는 아쉬움을 남겼다.

사이버 공간에서는 외국의 시스템을 자신의 점유물처럼 사용할 수 있는 이동성이 존재하지만, 현실에서는 여전히 국경이라는 장벽에 부딪쳐서, 국가간의 공조가 없다면 사이버테러와 관련된 범죄는 수사가 불가하다는 점을 여실히 보여주는 사례라고 할 수 있을 것이다. 사이버범죄 관련 법규의 문

제점을 언급할 때, 늘 거론되는 요소가 바로 수사와 처벌에 있어 국제적 공조의 미비일 것이다. 우리나라의 경우 주변국가와의 사이버공간상 교류가 무척 활발한 만큼 수사 및 처벌과 관련된 국제적 조약의 가입이 필수적이고, 특히 중국, 일본의 국가수사기관간의 협조도 매우 절실한 상황이다.

마. 사이버테러 피해신고와 고지의 의무화

사례 : 대형 상업사이트 대상 해킹, 협박

2007년 10월경 피의자는 국내 대형 포털 사이트 OO의 고객상담 외주업체 상담원의 ID와 비밀번호를 알아낸 뒤 이를 통해 약 7,000여 건의 고객 상담 내용을 열람하고, 이 사이트에 "고객상담 내용을 유출했으며, 이를 유포하겠다"고 협박하며 금품을 요구하다가 검거되었다[32].

한편, 2008년 3월 21일 신원 불상의 해커들이 트래픽(방문자 수)을 일시적으로 증가시켜 다른 방문자들의 접속에 장애를 일으키는 방법으로, OOOO증권 홈페이지를 해킹하여 마비시키고 이를 볼모로 5,000만원을 요구하였다[33].

위 사례는 '해킹'이 '돈'을 바라는 경제적인 목적의 사이버테러로의 변화를 극명하게 보여준다고 할 수 있을 것이다. 그동안 해커들의 표적은 피해를 당해도 신고하기를 꺼리는 화상채팅, 도박, 성인사이트, 게임 아이템거래 사이트에 주로 몰렸지만, 최근 들어 언론사를 비롯해 대형 포털, 중소 쇼핑몰, 게임업체 등으로 표적이 점점 넓어지고 있는 양상이다.

해커들의 공격이 갈수록 과감해지고 전 방위로 확산되는 까닭은 바로 이런 수법을 이용한 해킹이 '돈'이 되기 때문이다. 은행이나 증권사와 같이 신용과 보안이 최우선시 되고 돈거래와 직결된 금융권 웹 사이트가 해킹 표적으로 떠오르는 이유도 여기에 있다.

해킹을 당한 대형 상업사이트들은 해당 기업의 인지도 하락이나 신뢰성

32) 머니투데이, "OO 해킹 당했다", www.moneytoday.co.kr, 2008. 3. 26.
33) 머니투데이, "OOOO그룹 홈페이지 해킹 당해", www.moneytoday.co.kr, 2008. 3. 21.

실추를 우려하여 해킹 피해사실을 숨기기에 급급하였고, 결과적으로는 더 큰 피해와 손실을 가져왔다. 해당 기업이 해킹으로 인해 경제적인 손실을 입는 것도 큰 문제이겠지만, 더 큰 문제는 이들 기업 사이트를 이용하는 이용자들이 자신도 모르는 사이에 그들의 개인정보가 유출되어 또 다른 범죄에 이용될 수도 있다는 것이며, 해당 기업이 피해사실을 숨기는 사이, 이용자들은 스스로의 보호조치를 강구할 기회조차 박탈당한다는 데에 있다. 따라서 이용자들의 피해를 최소한으로 줄이기 위해, 사이트 운영자에 대해 해킹 피해사실에 대한 관련 기관에의 신고와 이용자에 대한 피해사실 고지를 법적으로 의무화해야할 필요가 있다. 이는 '정보통신망법'에서 개인정보와 관련하여 정보통신서비스 제공자에게 부과된 여러 가지 의무규정들과 논리적으로도 연결된다고 할 수 있을 것이다.

물론 지금과 같은 체제에서라면, 어떤 기업도 해킹피해에 대해 절대로 신고 및 고지 의무를 이행하지 않을 것이므로 그에 따른 합리적 기준의 제정도 필요할 것으로 보인다. 예를 들어, 해당 사이트가 국가공인기관에서 지정하는 기준 이상의 보안시설을 갖추고 이에 필요한 의무를 모두 이행하였다면, 해킹으로 피해를 당했다 할지라도 어느 정도의 형사상·민사상의 면책특권을 인정해 주어야만, 제대로 된 피해신고가 따를 것이고, 이용자에 대한 보호도 더 강화될 수 있을 것이다.

2. 일반 사이버범죄 관련 법규의 문제점

가. 사이버범죄의 과도한 특별형법화

'정보통신망법'은 사이버테러형 범죄뿐만 아니라 전반적인 사이버범죄에 대하여 일반법 또는 기본법적인 성격을 갖고 있다. 정보통신망에서 일어날 수 있는 거의 모든 유형의 불법행위를 다룬다고 생각할 수 있을 정도이지만,

이 법률은 형법에 대하여는 어디까지나 특별법일 뿐이다. 특별형법의 필요성과 유용성이 부정될 수는 없겠지만, 사이버공간이 현실의 세계와 밀접한 관련을 맺고 있고 또 그만큼 일체화·대중화되어가고 있는 현 상황에 비추어 볼 때, 위법행위에 대하여 형벌이라는 가장 엄중한 제재를 규정하는 형법구성요건은, 일반국민의 행위준칙으로서, 가능하다면 형식적 의미의 형법인 형법전에 두는 것이 바람직하다 할 것이다. 그래야만 수범자인 일반국민들이 무엇이 처벌되고 어떠한 행위는 처벌이 되지 않는지 쉽게 알 수 있어, 현실세계에서와 마찬가지로 사이버공간에서도 형법의 규범력을 담보할 수 있게 되고, 그에 따라 "형법의 보호적 기능과 사회보전적(예방적·진압적) 기능"을 제대로 수행할 수 있을 것이다[34].

물론 "구성요건이 당해 특별법의 관련규정과 유기적인 연관성을 가지거나 빠르게 변화하는 상황에 시의적절하게 대처할 필요가 있는 경우와 같이 구성요건의 성격상 특별형법의 형식을 취할 수밖에 없는 때"에는 형법전에 규정하기가 어렵겠지만, 그러한 특별한 합리적인 이유가 있는 경우를 제외하고는 특별형법을 지양하고 형법전에 규정하여야 한다. '정보통신망법'에 규정된 형벌규정 중 형법규정과 중복되어 굳이 특별형법에 두어야 할 이유가 없는 구성요건도 상당수 있기 때문에, 형법구성요건의 경고적 기능을 제대로 활성화하기 위해서라도 이들을 과감하게 형법전 안으로 정리할 필요가 있다. 현재 인터넷사기나 인터넷도박의 경우 인터넷과 관련된 특별한 규정이 없음에도 형법의 관련 조항만으로 충분히 처벌을 적용하고 있는 것만으로 시사하는 바가 크며, 필요하다면 사이버범죄와 관련된 형법 조문에 인터넷과 같은 정보통신매체를 수단으로서 보충하고, 파급효과나 필요에 따라서 가중처벌을 규정하는 것도 한 방법이 될 수 있을 것이다.

나. 지나친 주민등록번호에의 의존

34) 강동범, "정보통신망법상 사이버범죄처벌규정의 검토", 인터넷법률 통권 제39호, 2007. 7.

우리나라 사이버범죄의 많은 부분이 주민등록번호 도용과 같은 개인정보 침해와 관련된 범죄이며, 평생토록 변경이 불가능한 주민등록번호를 인터넷 상에서 너무 빈번하게 사용한다는 사실에 대해서는 그동안 여러 차례 중요한 문제점으로 지적되어 왔다. 하지만 대부분의 인터넷 사이트들은 비교적 간단하게 이용자의 신원을 확인할 수 있다는 편의성 때문에 아직까지도 신원확인 수단으로서의 주민등록번호에 대한 의존도는 줄어들지 않고 있고, 대체수단으로 고안된 제도들의 시행도 미진한 상태이다.

실제로 무료 전자우편 계정을 제공하는 우리나라의 사이트와 외국의 사이트의 가입신청 단계를 비교해보면, 우리나라 사이트의 경우, 제공하는 서비스와 직접적인 관련도 없이, 주민등록번호를 포함하여 지나치게 많은 개인정보를 요구하는 것을 알 수 있다. 따라서 우리나라는 인터넷 상에서 거의 만능키와도 같은 역할을 하고 있는 주민등록번호에 지나치게 의존하다보니, 주민등록번호를 향한 사이버범죄의 유혹이 계속되는 것은 당연한 귀결이라 할 수 있을 것이다. 특히, 사이버테러형 범죄 중 해킹 유형의 많은 부분이 인터넷 게임과 관련되었다는 것은 드러내놓고 얘기할 수 없는 안타까운 우리의 현실이고, 인터넷 게임 아이템을 해킹하기 위한 방편으로서의 주민등록번호의 도용·유출은 간과할 수 없는 수준이다.

따라서 일단 도용이 된다면 그 피해를 돌이킬 수 없는 주민등록번호의 사용은 최대한으로 제한을 하고, 이를 강력하게 법규화하는 것이 필요하다고 본다. 프랑스의 경우, 이미 '정보처리, 파일 그리고 자유에 관한 1978년 1월 6일 법'[35] 제정 당시부터, 우리나라의 주민등록번호와 유사한 역할을 하는 국민신원확인부의 등록번호 사용을 엄격히 제한하였고, 현재는 형법 제226-16-1조에, 1978년 1월 6일 법으로 지정된 경우를 제외하고는, 이와 같은 번호를 지니는 자료를 포함하는 개인정보의 처리 행위를 금지하고 있으며, 이를 위반했을 경우에는 5년 이하의 징역 또는 300,000 유로 이하의 벌금에

35) La loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés.

처하고 있다.

다. 1인 미디어와 범죄 관련 동영상 배포

미국산 쇠고기 수입과 관련된 촛불집회는 인터넷 강국으로서의 대한민국의 새로운 면모를, 그리고 신시대의 집회 문화 가능성을 유감없이 보여준 계기가 되었다. '유튜브'나 '다음 TV팟'에 게시되는 사용자창작물(UCC)들이 네티즌들의 주요한 정보원천이 되어 인기를 끌고, '아프리카'와 같은 1인 방송국은 기존 언론이 담당하던 역할을 어느 정도 대체하게까지 되었다[36].

1인 미디어가 표현의 자유에 무한한 날개를 달아주고, 새로운 시각에서 뉴스에 접근할 수 있는 통로를 제공해준다는 점에서, 그리고 기존의 틀에 얽매이지 않는 양방향성 소통방식으로 운영된다는 점에서 눈길을 끌긴 하지만, 보도의 내용이 전혀 여과없이 전달될 수 있고, 책임성 없는 보도 의식이 나타날 수 있으며, 네티즌들의 인기에 영합하기 위한 선정성이 가미될 수 있고. 자칫 피보도자의 사생활의 비밀이 제대로 지키지 못한 상태에서 폭력성이 무한정 노출될 수 있다는 문제점을 갖고 있기도 하다.

우리나라에서는 휴대폰에 장착된 카메라로 촬영된 부적절한 동영상이 사회적으로 큰 반향을 불러일으키는 등 일찍이 여러 각도에서 이런 종류의 문제점이 제기되어 왔음에도 아직까지 불법적인 동영상 유포 또는 1인 미디어의 문제점에 대한 인식이나 대책마련이 미흡한 실정이다. 반면, 프랑스에서는 2006년 4월, 선생님에 대한 고교생의 폭행 휴대폰 동영상 촬영과 배포가 문제된 이후, 2007년 3월 5일 '범죄예방에 관한 법'[37]을 제정하여, 직업상의 목적이 아닌 범죄에 대한 동영상 촬영과 배포를 심각하게 고려하였다.

---

36) 이에 대한 언론 보도를 잠시 살펴보면, * 디지털 생중계...'길거리 저널리즘'떴다. (한겨레신문 2008. 5. 28.), * 시민 '디지털 저널리즘'의 힘... '언론 사각'틈새급속 확산 (경향신문 2008. 5. 27.), * 한 손에 촛불 또 한 손엔 캠코더 (PD저널 2008. 5. 27.)

37) La loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance

이 법은 '형법'에 제222-3-3조를 삽입하면서, 인간의 존엄성에 해를 끼치는 범죄를 저지르는 것과 관계되는 영상의 녹화와 배포를 처벌하고 있는데, 녹화(촬영) 행위는 관련된 범죄 행위의 공범과 같은 무게로 이해되므로, 정범과 마찬가지로 무기징역에까지 이르는 형벌을 받을 수 있게 되며, 이 촬영 동영상을 전파(배포)하는 행위는 5년의 금고와 75,000유로의 벌금으로 처벌된다. 또한 같은 조 제3항에는 이런 동영상의 녹화와 배포가 공중에게 정보를 제공할 목적을 가진 직업을 가진 사람이 직무상 실행하거나 법정의 증거로 사용하기 위해서일 때는 예외로 하고 있다.

1인 미디어가 활성화되고 있는 상황에서, 과연 직업적인 활동에 기인한 정보를 개인적 활동에서 나온 정보와 어떻게 제대로 구별할 수 있을 것인가에는 상당부분 의문이 생기긴 하지만, 다른 사람에게 피해를 줄 수 있는 무분별한 불법 동영상 유포의 폐해를 막기 위한 시도만큼은 상당히 진보적인 것으로 평가할 수 있고, 우리나라도 이에 대한 관련 규정이 정비되어야 할 것이다.

라. 명예훼손 등 인터넷 상 불법게시물

인터넷 상의 명예훼손이 피해자에게 돌이킬 수 없는 큰 상처를 줄 수 있다는 것은 비단 어제 오늘의 일이 아님에도, 그 유형을 달리하고 강도를 강화하면서 명예훼손 관련 범죄는 계속 반복되고 있는 실정이다. 펌글의 형태로 계속 전달되는 엄청난 전파속도의 파급력 때문에 피해 당사자들은 제대로 된 해명이나 반론의 기회마저 박탈당하고 있다.

'정보통신망법' 제44조의2, 제44조의3에 의하면, 정보통신서비스 제공자는 타인의 명예훼손이나 허위사실 등의 불법게시물에 대해 삭제·임시조치 등 필요한 조치를 하여야 한다고 규정되어 있음에도 불구하고, 해당 업체들은 네티즌의 표현의 자유를 보호한다는 명목으로 또는 자체 점검 및 처리인력

이 부족하다는 등의 이유로 해당 게시물을 방치하고 있다. 네티즌들이 많이 이용하는 포털 사이트들은 게시물의 불법 여부 판단이 애매할 경우에는 방송통신위원회의 심의위원회 유권해석이 필요하다는 핑계로 비난 여론을 피하면서 시간을 끄는 등 포털의 사회적 책임을 회피하고 있다.

방송통신위원회[38]의 심의위원회에서는 사안에 따라 심의한 후 결정을 내리게 되는데, 밀려드는 심의요청과 7일 이내에 판단하도록 하는 기간적인 지연 때문에, 위원회의 결정이 내려졌을 때에는 이미 인터넷 상의 피해는 확산될만큼 다 되어 있어 회복불가능한 상태로까지 번진 이후이다.

<표 3> 방송통신위원회 연도별 심의 및 시정요구 실적

구 분	1995~2004	2005	2006	2007	2008. 1.	합 계
심 의	297,752	119,184	156,734	216,224	9,337	799,231
시정요구	141,533	42,643	44,289	112,220	6,808	347,493

(출처 : 방송통신위원회)

인터넷 방문 빈도수에 따른 우리나라의 상위 30개 사이트 중 포털 사이트는 1위부터 4위까지를 포함하여 모두 10~13개를 점유하고 있고, 총 방문객의 47.2%를 끌어들이고 있다. 이용시간으로만 본다면 우리나라 네티즌은 한 달에 19시간 49분을 포털에 머무르고 있는데, 이는 총 인터넷 사용시간 중 73.2%를 차지[39]할 정도여서, 포털은 우리나라 인터넷 시장에서 막강한 영향력을 행사하고 있고, 또 그에 따른 사회적 책임도 무시할 수 없는 수준이다. 하지만 포털에 게시된 이용자들의 게시물과 관련해서는 포털들도 이중적인 입장에 처할 수밖에 없다. 왜냐하면, 포털들은 관련 규정상 이용자의 게시물

38) 이전 '정보통신망법'에서는 방송통신윤리위원회임, KISCOM : Korea Internet Safety Commission, www.kiscom.or.kr
39) 최정호, 앞의 논문.

을 함부로 삭제할 수도 없고[40], 그렇다고 문제가 된 게시물의 민형사상의 책임을 게시물 작성자에게만 일방적으로 떠넘길 수도 없는 관리책임이 있기 때문이다.

최근 일련의 연예인 자살사건과 관련하여 부분별한 댓글문화의 폐해를 줄이기 위해 '사이버 모욕죄'의 신설 여부와 더불어 방송통신위원회의 심의기간을 단축하는 방법이 모색되고 있다. 포털에 특히 집중된 한국적 인터넷 문화를 생각해볼 때, 불필요한 심의기간을 길게 갖기 보다는, 포털과 방송통신위원회가 융합되어 관련 사안들을 즉석에서 신속하게 함께 심의하여 처리하는 전환적이며 전격적인 사고방식이 필요하다고 본다.

마. 허위사실의 유포의 처벌 법규

인터넷 게시판의 게시물들을 살펴보면, 네티즌들의 관심을 유발하기 위해 게시물 제목에 자극적인 문구를 사용하고, 그 유인효과로 '베스트 글'에 선정되어 초기화면 상단에 배치되는 등 여과장치 없는 게시판 운영이 문제점으로 지적되고 있다. 또한 사실 확인 없이 무분별한 '퍼나르기'로 허위사실이 급속히 전파되고, 인터넷 방송을 통해 여과 없이 보도됨으로써 기정사실화되는 경향이 나타나고 있다. 지난 미국산 쇠고기 수입반대 촛불시위와 관련하여, 명예훼손과는 전혀 차원이 다른, 대상없는 허위 사실의 유포가 문제 되었다. 예를 들자면, 광우병 시위와 관련하여, '5. 17 휴교시위, 등교거부' 등 허위의 휴대전화 문자메시지를 작성하여 중・고교생을 대상으로 유포한다든

40) (전략)... 공정거래위원회는 20일 NHN(네이버), 다음커뮤니케이션(다음), SK커뮤니케이션즈(네이트, 엠파스), KT하이텔(파란), 야후코리아(야후) 등 5개 대형 포털업체를 상대로 25가지 불공정약관 유형에 대해 9월 말까지 자진 시정토록 했다. 공정위에 따르면 네이버와 다음은 지금까지 회원의 게시글에 대해 "회사가 서비스 성격에 부합하지 않는다고 판단할 경우 사전 동의 없이 임시게시중단, 수정, 삭제, 이동, 등록거부 등의 조치를 취할 수 있다"는 내용의 약관을 운용해왔다. 공정위는 이 같은 약관에 대해 "관련법 등 구체적 사유나 근거 없이 포털 측이 자의적으로 게시글을 일방 삭제 또는 수정할 수 있도록 하는 것은 이용자에게 부당하게 불리한 조항"이라고 지적하고 시정을 요구했다. 머니투데이.

지, 진압전경이 연행여성을 기동대 차량에서 강간하고 신고를 못하게 휴대전화로 촬영한 뒤 그 사실을 알리면 동영상을 공개한다는 협박을 하였다고 허위의 사실을 포털 토론방에 게시한다든지, 시위진압을 맡은 기동대원을 가장하여 “시민진압 직무명령을 포기한다”는 내용의 허위 사실을 인터넷 라디오 방송 게시판에 게시하여 혼란을 불러일으킨 것이 바로 그것이다.

이와 같은 행위는 ‘전기통신기본법’[41]에 따라, 공익을 해할 목적으로 공연히 허위의 통신을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에(제47조 제1항), 자기 또는 타인에게 이익을 주거나 타인에게 손해를 가할 목적으로 전기통신설비에 의하여 공연히 허위의 통신을 한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다 (같은 조 제2항). 하지만 이 처벌조항에는 문제가 있다. 왜냐하면 동일한 위법행위일지라도 오프라인 상의 위법행위는 처벌하지 않으면서, 사이버공간에서의 위법행위만을 처벌하기 때문이다. 동일한 법익에 대한 침해행위의 경우 사이버공간에서의 행위가 현실공간에서의 행위보다 더 중대하거나 더 위험하다고는 볼 수 없으므로, 사이버공간에서의 위법행위만을 처벌하는 것은 그 근거가 빈약하고 법체계나 법감정상 맞지 않는다고 생각한다.

프랑스의 예를 들자면, 형법 제322-14조에, 사람에 대한 위험한 파괴, 손상, 훼손이 일어났다고 또는 일어날 거라고 믿게 할 목적으로 거짓 정보를 소통하거나 폭로하는 행위는 온라인, 오프라인 관계없이 2년의 금고와 30,000유로의 벌금으로 처벌한다. 공중을 위험하게 처할 수 있는 정보 중, 생물학적 또는 화학적 폭탄제조법을 전파하는 행위에 대해서는 1년의 금고와 15,000유로의 벌금으로 처벌하지만, 이 전달방법이 통신 통해 불특정 다수인

41) 전기통신기본법 [제47조] (벌칙) ① 공익을 해할 목적으로 전기통신설비에 의하여 공연히 허위의 통신을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. ② 자기 또는 타인에게 이익을 주거나 타인에게 손해를 가할 목적으로 전기통신설비에 의하여 공연히 허위의 통신을 한 자는 3년 이하의 징역 또는 3천만원이하의 벌금에 처한다. ③ 제2항의 경우에 그 허위의 통신이 전신환에 관한 것인 때에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. ④ 전기통신업무에 종사하는 자가 제1항 또는 제3항의 행위를 한 때에는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하고, 제2항의 행위를 한 때에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

을 대상으로 할 때에는 3년의 금고와 45,000유로의 벌금으로 가중처벌하고 있다(형법 제322-6-1조).

다른 사람에게 피해를 입힐 수 있는 거짓정보의 전달행위에 대해서, 인터넷의 파급효과로 그 처벌의 정도를 강화하는 태도에는 일응 수긍할 수 있지만, 현실세계에서는 처벌하지 않는 허위사실 유포행위가 사이버공간에서만 처벌되고 있는 현행 법규는 재검토의 필요가 있다 할 것이다.

Ⅳ. 나오며

우리 스스로도 기록적인 발전을 이룩한 정보통신 기술과 초고속 인터넷으로 대변되는 관련 기반 시설 그리고 세계 최상급의 인터넷 이용자수에 대해 자랑스러워하고 있긴 하지만, 그 화려함의 이면에 가려진, 개인정보 보호의 소홀이라든지 악성 댓글의 폐해 같은 사이버 부작용에 대한 법률적 고려가 부족하였고, 이를 해결하려는 사회적 공감대도 제대로 형성되지 않았던 것이 사실이다.

우리나라는 정보통신과 관련된 발전된 기술을 바탕으로, 이 기술을 어느 누구보다도 빨리 시험해보려는 관심이용자층의 열성 덕분에 다른 어떤 나라보다도 먼저 새로운 사이버 문화현상을 접할 수 있었고, 이런 현상을 이해하려는 노력과 함께 부작용에 대한 대비책을 마련하였더라면, 사이버 세계에 관한 한, 세계적인 주도권을 발휘할 수 있었음에도 불구하고, 사이버범죄를 본격적으로 논하기 시작한 지 십여 년이 지난 지금까지도, 신기술의 시험무대로만 이용되고 있을 뿐, 제대로 된 법률적 제도 마련의 열성도 없이 선진국의 법률만을 비교 답습하고 있는 듯하다.

본문에서는 날로 세분화되고 있는 전체 사이버범죄의 유형과 관련 법률에 대해 모두 언급하지 못하였지만, 좀 더 정교한 연구를 바탕으로 이에 대한

총체적인 정리가 필요하다고 생각된다. 아울러, 사이버테러형 범죄 및 일반 사이버범죄 관련 법규의 문제점과 함께 어설픈 개선방향도 제시하였는데, 개인적인 역량의 부족으로 내용도 불충분하고 논리적으로도 부족한 부분이 많아 계속적인 연구의 필요성을 느꼈다.

이미 살펴본 내용 이외에, 음란물의 유통이라든지, 아동포르노물에 대한 규제, 인터넷을 통한 성매매 등 우리 사회의 구조적 또는 문화적 요인으로 인해 도출될 수 있는 사이버범죄와 관련된 더 심화된 문제제기가 필요하며, 처음에 발표제의를 받을 때 법률적 비교대상을 프랑스로만 한정하였으나 여타 다른 선진국의 법률과의 비교를 통해 사이버범죄의 예방 연구가 계속되어야 함을 강조하는 바이다.

참고문헌

La loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés

La loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance

강동범, “정보통신망법상 사이버범죄처벌규정의 검토”, 인터넷법률 통권 제39호, 2007. 7.

강동범, “사이버범죄와 형사법적 대책”, 형사정책연구 2000년 제42호

양근원, “사이버범죄의 특징과 수사방향”

이민식, “사이버범죄 및 일탈의 개념 및 유형”, 사이버범죄연구회 제4회 세미나, 2000. 11. 4.

이영준, 정 완, 금봉수, “사이버범죄방지조약에 관한 연구”, 한국형사정책연구원 연구보고서 01-30, 2001년 12월.

최정호, “인터넷 이용자들의 이용행태에 따른 사이버범죄의 변천 - 프랑스

와 한국의 법률 비교 연구 (Les comportements des internautes et l'évolution de la cybercriminalité - Etude comparée entre la France et la Corée du Sud)", 프랑스 몽뻴리에(Montpellier) 1대학, 박사학위 논문, 2007년 10월 18일.

경찰청 사이버테러대응센터 (Cyber Terror Response Center), Cyber Cop NETAN, www.ctrc.go.kr

두산백과사전 EnCyber & EnCyber.com

방송통신위원회, KISCOM : Korea Internet Safety Commission, www.iscom.or.kr

머니투데이, "OO 해킹 당했다", www.moneytoday.co.kr, 2008. 3. 26.

머니투데이, "OOOO그룹 홈페이지 해킹 당해", www.moneytoday.co.kr, 2008. 3. 21.

한겨레신문, "디지털 생중계...'길거리 저널리즘'떴다", 2008. 5. 28.

경향신문, "시민 '디지털 저널리즘'의 힘... '언론 사각'틈새급속 확산", 2008. 5. 27.

PD저널, "한 손에 촛불 또 한 손엔 캠코더", 2008. 5. 27.

[16:30 – 17:40]

사이버범죄의 법적규제 및 대응전략

제5주제 : 현행 사이버 명예훼손죄 법리의 문제점 및 사이버 모욕죄 도입의 정당성 검토

발표 : 주 승 희 (덕성여대 교수)

토론 : 박 광 민 (성균관대 교수)
탁 희 성 (한국형사정책연구원 연구위원)

현행 사이버 명예훼손죄 법리의 문제점 및 사이버 모욕죄 도입의 정당성 검토

주 승 희*

Ⅰ. 들어가며

이제 인터넷이 무엇이며, 그 순기능과 역기능이 무엇인지를 소개할 필요가 없을 정도로 인터넷은 우리 사회 대중의 삶에 깊숙이 자리 잡았다. 법제 역시 마찬가지이다. 1990년대 중반 처음 인터넷의 대중화가 시작되었을 때, 자칫 법과 제도가 기술의 빠른 발전을 따라잡지 못할까 하는 우려가 나라를 불문하고 적지 않았다. 그러나 그 사이 각 국가마다 또 필요한 경우 국제적으로 연합하여 발 빠르게 대처함으로써 그와 같은 우려는 상당부분 해소된 것으로 보인다.

그런데 최근 들어 인터넷에 대한 정부의 관심이 뜨겁다. 새 정부 들어서 정부와 국민간의 의사소통 필요성이 더욱 강조되면서 한편으론 인터넷의 정보제공기능 및 의사소통적 기능을 십분 활용하기 위한 방안이,[1] 다른 한편으론 '쇠고기괴담'이나 '독도괴담'과 같은 각종 허위사실유포의 차단 필요성이 제기되고 있다. 지난 7월 법무부장관도 인터넷상 허위사실 유포와 명예

* 덕성여자대학교 법학과 교수, 법학박사(Dr. jur.)

1) 올 봄 미국쇠고기수입반대를 위한 촛불시위를 경험하면서 국민과의 의사소통이 부족했다는 자각하에 청와대의 홍보기능을 대폭 강화하면서 홍보기획관을 기용하고, 그 아래에 인터넷을 전담하는 국민소통비서관을 신설한 것을 그 예로 들 수 있다(http://www.heraldbiz.com/SITE/data/html_dir/2008/06/16/200806160231.asp).

훼손과 관련하여 사이버 모욕죄 신설을 검토하는 등 인터넷 유해사범에 대한 처벌 강화를 추진하겠다는 의사를 밝힌 바 있다.[2] 같은 취지에서 방송통신위원회는 '제한적 본인확인제'의 도입 및 인터넷댓글의 모닝터링강화, 사업자과태료 도입을 주요 골자로 하는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 함)의 개정안을 국회에 상정할 계획이고, 때마침 10월 초 발생했던 유명연예인의 자살사건의 주된 원인으로 인터넷상 악성댓글이 지목되면서 그에 대한 엄중한 대처의 요구가 더 커지고 있어 향후 인터넷이용자의 표현의 자유는 전방위적으로 제한될 가능성이 있다.

이미 여러 비교법적 연구를 통해 알려진 바와 같이 우리나라는 다른 나라에 비해 명예훼손행위를 엄격하게 규제하고 있다.[3] 그럼에도 현재의 명예훼손법규가 익명성을 이용한 악성댓글로부터 개인의 인격권을 보호하기 위해서는 역부족인지, 따라서 사이버모욕죄의 신설과 같은 더욱 강화된 처벌 방안이 필요한 것인지 면밀히 검토해보아야 할 시점으로 보인다. 본 발표문은 현행 (사이버)명예훼손죄 및 모욕죄의 법리를 통설과 판례를 중심으로 검토한 후 개선해야 할 점을 짚어본 후에, 정보통신망법에 대한 최근의 개정논의 중에서 반의사불벌조항 삭제 및 사이버모욕죄신설의 필요성 여부를 형법이론 및 형사정책적 측면에서 살펴보고자 한다.

Ⅱ. 인터넷상 명예훼손 및 모욕 행위의 발생 현황

인터넷상 명예훼손 사건이 매년 폭증하고 있음은 언론 보도 등을 통해 익히 알려진 사실이다. 인터넷이용자라면 누구나 쉽게 명예훼손 및 모욕의 범

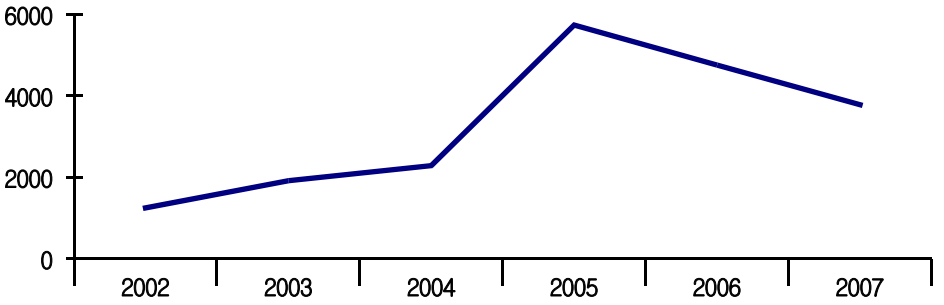
2) http://news.hankooki.com/lpage/politics/200807/h2008072303240621060; htm.http://www.donga.com/fbin/output?n=200807230166

3) 독일, 일본, 영국, 미국, 프랑스, 오스트리아 등의 명예훼손죄 입법례는 이천현・도중진・권수진・황만성, 형법각칙 개정연구[2] -개인적 법익에 관한 죄-, 한국형사정책연구원, 28쪽 이하를 참고할 것.

죄현장을 목격할 수 있을 정도로 매우 가까이 그리고 빈번하게 발생하는 범죄이다. 이를 뒷받침할 만한 공식적인 통계자료로서 먼저 정보통신윤리위원회[4]의 명예훼손분쟁조정을 위한 상담건수를 연도별로 정리하면 아래의 표와 같다.

구 분	2001	2002	2003	2004	2005	2006	2007
명예훼손(모욕)	278 (33)	1,248 (115)	1,916 (894)	2,285 (979)	5,735 (1,802)	4,751 (1,641)	3,780 (1,257)

<정보통신윤리위원회의 인터넷상 명예훼손・모욕 상담건수>[5]



위 그래프를 보면 명예훼손관련 상담건수가 2001년 278건에서 2007년 3780건으로 전체적으로 볼 때 증가 추세에 있음을 알 수 있다.[6] 다음으로 『검찰연감 2007』에 소개된 1987년부터 2006년까지 20년간의 범죄사건처리 현황에 관한 자료를 분석한 아래의 표를 보면 지난 20년간 명예훼손죄가 꾸

4) 정보통신부장관은 정보통신망에서의 명예훼손관련 정보에 관하여 정보통신윤리위원회 산하 명예훼손분쟁조정부의 심의를 거쳐 정보통신서비스제공자 또는 게시판 관리·운영자로 하여금 그 취급을 거부·정지 또는 제한하도록 명할 수 있다(정보통신망법 제44조의7 제2항, 제44조의9 제4호, 제44조의10).

5) 정보통신윤리위원회의 「2007년 사이버권리침해 사례집」, 265쪽의 사이버권리침해 관련 표, '연도별 상담내용(20001-2007)'의 내용 중 명예훼손(모욕)의 수치만 추출하여 작성함.

6) 2005년 명예훼손상담건수가 특히 많았던 이유에 대해서 위 자료집에는 아무런 언급이 없다. 2005년 당시 서울대 황우석교수 논문조작 사건의 전말이 드러나며 전국민을 공황에 빠뜨린 바 있고, 정부의 8・31 부동산대책, 헌법재판소의 호주제헌법불합치결정, 기생충알김치파동 등 사회적으로 큰 파장을 일으킨 사건들이 줄지어 언론에 보도되었는데, 이들 이슈가 직간접적으로 영향을 미친 것은 아닌지 추측해볼 뿐이다.

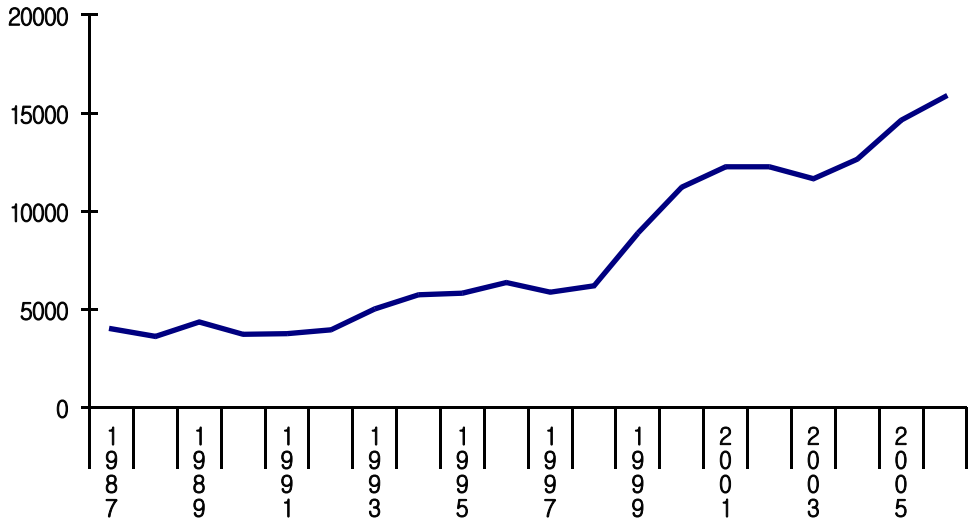
준히 증가하고 있음을 확인할 수 있다.

<검찰에 의한 지난 20년간 명예훼손죄처리 통계>[7)]

연도 \ 처리현황		처 리	기 소	불기소	기소율(1994년~타관·송치등)
1987		4003	647	3354	16.2
1988		3614	615	2994	17.0
1989		4349	813	3535	18.7
1990		3720	700	3020	18.8
1991		3756	765	2989	20.4
1992		3948	710	3233	18.0
1993		5015	915	3734	18.2
1994		5737	816	4108	333
1995		5820	781	4231	220
1996		6360	918	4829	160
1997		5867	992	4267	187
1998		6191	1111	4248	192
1999		8880	1719	5965	281
2000	명예훼손	7593	1399	5367	266
	출판물등명예훼손	1773	175	1170	171
	모욕	1858	532	1260	21
	계	11224	2106	7797	458
2001	명예훼손	8713	1709	6078	306
	출판물등명예훼손	1476	151	883	215
	모욕	2069	554	1408	41
	계	12258	2414	8369	562
2002	명예훼손	8192	1651	5537	424
	출판물등명예훼손	1990	163	1385	198
	모욕	2077	595	1377	41
	계	12259	2409	8299	663
2003	명예훼손	8479	1483	6055	313
	출판물등명예훼손	1226	147	812	73
	모욕	1948	534	1316	49
	계	11653	2164	8183	435
2004	명예훼손	9140	1714	6332	268
	출판물등명예훼손	1196	73	772	106
	모욕	2311	687	1529	9
	계	12647	2474	8633	383
2005	명예훼손	10933	1954	7644	289
	출판물등명예훼손	1184	104	785	65
	모욕	2516	802	1579	37
	계	14633	2860	10008	391
2006	명예훼손	11791	2226	8364	275
	출판물등명예훼손	1185	90	800	139
	모욕	2857	913	1826	40
	계	15833	3229	10990	454

위의 도표를 보면 아직 일반인에게 인터넷이 널리 보급되기 전인 1990년

7) 검찰연감 2007, 516쪽 이하 541쪽의 20년간의 '전체사건의 죄명별' 처리현황에 관한 표에서 명예에 관한 죄에 대한 통계를 추려내어 표를 작성하였음.



대 중반까지는 명예훼손죄의 증가율이 그리 높지 않다. 반면 1990년대 후반 이후 명예훼손처리사건수가 서너 배 가량 높아진 것을 볼 수 있는데, 이는 인터넷의 확산과 함께 일반인의 이용률이 높아지고 인터넷매체의 특성상 그 이용자들이 게시판이나 블로그 등 '공연성'이 확보된 장소에서 타인의 명예를 훼손할 만한 내용의 글을 쉽게 올리거나 다른 게시판에 옮길 수 있어 명예훼손죄의 성립이 그 전보다 용이해진 결과로 분석된다.[8)]

Ⅲ. 인터넷상 명예훼손 및 모욕행위의 법적규제

타인의 명예를 훼손할 만한 글을 인터넷게시판 등에 올리는 경우, 형법 제33장의 명예에 관한 죄 및 정보통신망법 제70조 사이버명예훼손죄에 의한 처벌이 가능하다.

8) 인터넷상 명예훼손 실태에 관한 풍부한 사례는 박균성, 인터넷상 명예훼손 실태 및 대응방안, 정보통신윤리위원회 보고서, 2005를 참고할 것.

1. 형법

현행 형법 제307조 제1항은 공연히 사실을 적시하여 사람의 명예를 훼손한 경우, 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처할 수 있도록 하고 있고, '허위의' 사실을 적시한 경우에는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금에 처할 수 있도록 하고 있다. 허위의 사실을 적시하여 사자(死者)의 명예를 훼손한 경우, 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다(동법 제308조). 신문, 잡지 또는 라디오 기타 출판물을 이용한 명예훼손(이하 '출판물등명예훼손죄'라 함)의 경우, 법익침해의 중대성을 고려하여 사실을 적시한 경우 3년 이하의 징역이나 금고 또는 700만원 이하의 벌금에(제309조 제1항), 허위의 사실을 적시한 경우 7년 이하의 징역, 10년 이하의 자격정지 또는 1천500만원 이하의 벌금에 처함으로써(동조 제2항) 일반 명예훼손죄보다 가중처벌규정을 두고 있다. 또한 일반 명예훼손죄와 달리 '비방할 목적'이라는 초주관적 요소가 추가적으로 충족되어야 한다. 욕설과 같은 사실의 적시 없는 비방의 경우 모욕죄에 의한 처벌(1년 이하의 징역이나 금고 또는 200만원 이하의 벌금)이 가능하다(동법 311조). 사자명예훼손죄와 모욕죄는 친고죄이며, 일반명예훼손죄와 출판물등명예훼손죄는 반의사불벌죄이다.(제312조). 타인의 명예를 훼손한 경우에도 진실한 사실로서 오로지 공공의 이익에 관한 경우, 위법성이 조각된다(제310조).

2. 정보통신망법

인터넷을 이용한 명예훼손의 경우, 출판물등에 의한 명예훼손죄와 동일한 혹은 더욱 심각한 법익침해의 우려가 있음에도 '신문, 잡지 또는 라디오 기타 출판물'에 TV나 인터넷을 포함시키는 것이 해석상 논란의 여지가 컸는

데,[9] 2001년 정보통신망법 제61조(현행법 제70조)를 신설함으로 해결하였다. 동법은 '정보통신망을 통하여' 사실을 적시하여 타인의 명예를 훼손한 경우, 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에, 허위의 사실을 적시하여 타인의 명예를 훼손한 경우, 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처하도록 하고 있다. 그 법정형을 볼 때 자유형의 상한은 출판물등명예훼손죄와 동일하지만, 벌금액의 상한이 더 높아 전체적으로 볼 때 인터넷상 명예훼손행위를 출판물등명예훼손의 경우보다 가중처벌하고 있음을 알 수 있다. 사이버명예훼손죄 역시 형법상 명예훼손죄(일반명예훼손죄, 출판물등명예훼손죄)와 마찬가지로 반의사불벌죄이다(정보통신망법 제70조 제3항).

3. 사이버명예훼손죄의 보호법익 및 성립 요건

가. 보호 법익 및 명예 개념

상술한 형법과 정보통신망법의 명예훼손죄 모두 사람의 '명예'를 보호하고 있으며, 그 내용이 서로 동일하다는 점에는 의견이 일치한다. 다만 명예의 구체적 내용과 모욕죄의 보호법익에 대해서는 견해가 나뉘고 있다. 우선 우리나라의 통설과 판례는 명예훼손죄와 모욕죄 모두 명예를 보호법익으로 삼고 있으며, 구체적으로 '사람의 인격적 가치와 그의 도덕적·사회적 행위에 대한 사회적 평가', 즉 '외적 명예(äußere Ehre)'만을 보호한다고 보고 있다.[10]

---

9) 본죄의 '기타 출판물'에 TV, 인터넷을 포함시키는 것이 목적론적 해석에 부합한다는 견해로는 김일수·서보학, 형법각론, 2004, 200쪽 이하; 이정원, 형법각론, 2003, 244쪽. 유추해석금지원칙에 반한다는 이유로 반대하는 견해로는 박광민, 인터넷 명예훼손의 기본법리와 위법성조각, 성균관법학 제15권 제2호, 155쪽; 오영근, 형법각론, 255쪽; 임웅, 형법각론, 2003, 209쪽.

10) 박광민, 앞의 논문, 153쪽; 박상기, 형법각론, 2008, 178쪽; 배종대, 형법각론, 2007, 265쪽; 이재상, 형법각론, 2007, 181쪽; 임웅, 형법각론, 2003, 192쪽; 대법원 1987.5.12, 87도739; 대법원 1985.10.22, 85도1629 외 다수.

나. 정보통신망

'정보통신망'이란 「전기통신기본법」 제2조 제2호의 규정에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 뜻한다(정보통신망법 제2조 제1항 제1호). 구체적으로 인터넷상 포털게시판이나 댓글, 블로그, 카페, 홈페이지, 메신저, 전자우편 등을 이용하는 경우를 뜻한다. 타인의 명예를 침해할만한 내용의 글을 게시하거나 사진 또는 동영상을 올리는 등 다양한 방법에 의해 행해지고 있다.

다. 비방 목적

판례에 따르면 '비방의 목적'이란 형법 제309조 제1항의 '사람을 비방할 목적'과 마찬가지로 '가해의 의사 내지 목적'을 뜻한다. 비방의 목적 유무의 판단에 있어서는 '적시한 사실이 공공의 이익에 관한 것'인지 여부가 주된 판단 기준이다. 즉 행위자의 주관적 의도의 방향에 있어 비방의 목적과 공공의 이익을 위한 것이 서로 상반된 관계에 있는 것으로 파악하여, 적시한 사실이 공공의 이익에 관한 것인 경우에는 특별한 사정이 없는 한 비방할 목적이 없는 것으로 판단하는 것이다. 여기에서 '적시한 사실이 공공의 이익에 관한 경우'란 적시된 사실이 객관적으로 볼 때 공공의 이익에 관한 것으로서 행위자도 주관적으로 공공의 이익을 위하여 그 사실을 적시한 것이어야 하며, '공공의 이익에 관한 것'에는 널리 국가·사회 기타 일반 다수인의 이익에 관한 것뿐만 아니라 특정한 사회집단이나 그 구성원 전체의 관심과 이익에 관한 것도 포함된다고 한다. 구체적으로 적시한 사실이 공공의 이익에 관한 것인지를 판단하기 위해서는 피해자가 공무원 내지 공적 인물과 같은 공인(公人)인지 아니면 사인(私人)에 불과한지 여부, 그 표현이 객관적으로

국민이 알아야 할 공공성·사회성을 갖춘 공적 관심 사안에 관한 것으로 사회의 여론형성 내지 공개토론에 기여하는 것인지 아니면 순수한 사적인 영역에 속하는 것인지 여부, 피해자가 그와 같은 명예훼손적 표현의 위험을 자초한 것인지 여부, 그리고 그 표현에 의하여 훼손되는 명예의 성격과 그 침해의 정도, 그 표현의 방법과 동기 등 제반 사정을 고려할 것으로 요구한다.[11] 다수설은 타인의 명예를 훼손할 만한 내용의 글을 인터넷상 게시한 경우에도 비방의 목적이 부인되는 경우에는 사이버명예훼손죄로 처벌할 수 없지만 형법 제307조의 명예훼손죄의 적용은 가능한 것으로 보고 있다.[12]

라. 공연성

형법상 명예훼손죄와 마찬가지로 사이버명예훼손죄가 성립하기 위해서는 '공연성'이 요구된다. 이는 '불특정 또는 다수인이 인식할 수 있는 상태'를 의미하며, 높은 전파성을 갖는 인터넷의 특성상 공연성의 요건은 쉽게 충족된다. 예컨대 1 대 다수의 채팅방이나 게시판 등에 비방의 글을 올린 경우 다수의 네티즌들이 그 글을 읽을 수 있으므로 공연성이 인정된다.

마. 사실의 적시

'사실의 적시'란 '사실관계에 관한 보고 내지 진술로서 가치판단이나 평가를 내용으로 하는 의견표현에 대치되는 개념으로 시간과 공간적으로 과거 또는 현재의 사실관계에 관한 보고 내지 진술'을 의미하며,[13] '사실의 적시'

---

11) 대법원 2006.8.25. 선고 2006도648 판결; 대법원 2006.9.28. 선고 2004도6371 판결; 대법원 2005. 10. 14. 선고 2005도5068 판결; 대법원 1998. 10. 9. 선고 97도158 판결; 2000. 2. 25. 선고 98도2188 판결; 2003. 12. 26. 선고 2003도6036 판결; 2005. 4. 29. 선고 2003도2137 판결

12) 박광민, 인터넷상의 명예훼손에 대한 형사법적 규제, 형사법연구 제24호, 2005/겨울, 106쪽; 정대관, 사이버 공간에서의 명예훼손죄, 성균관법학 제17권 제1호, 2005, 209쪽

13) 대법원 2006.9.28. 선고 2004도6371 판결

와 '단순한 의견 또는 논평의 표명'을 구별할 때에는 '당해 표현의 객관적인 내용과 아울러 일반의 독자가 보통의 주의로 표현을 접하는 방법을 전제로 표현에 사용된 어휘의 통상적인 의미, 표현의 전체적인 흐름, 문구의 연결 방법 등을 기준으로 판단'할 것을 요하고, 더불어 '당해 표현이 게재된 보다 넓은 문맥이나 배경이 되는 사회적 흐름 등도 함께 고려'하여야 한다.[14] 타인의 명예를 훼손할만한 내용의 것이라도 사실의 적시에 해당하지 않을 경우 모욕죄가 성립가능하다. 다만 정보통신망법상 모욕죄를 별도로 규율하고 있지 않으므로 형법 제311조의 모욕죄에 의한 처벌이 가능하다.[15]

바. 형법 제310조의 적용 가능성 여부

타인에 대한 명예훼손이 인정되는 경우에도 진실한 사실로서 오로지 공공의 이익에 관한 경우 위법성 조각되어 처벌받지 않는다. 여기서 공공의 이익이란 '국가·사회 또는 다수인의 일반의 이익'을 뜻한다. 그런데 만약 어떠한 행위가 출판물등명예훼손죄 또는 사이버명예훼손죄의 성립 요건을 충족하는 경우에는 형법 제310조에 의한 위법성 조각이 불가능해진다. 왜냐하면 공익을 위해 진실한 사실의 적시를 통해 신문이나 라디오, 인터넷을 수단으로 피해자의 명예를 훼손한 경우, 가해자의 행태가 비방목적이 있는 것으로 인정된다면, 그와 같은 행위는 '오로지' 공공의 이익을 위한 행위가 아닌 것이기 때문이다.[16] 그런 점에서 출판물등을 이용해 타인의 명예를 훼손한 경우라도 비방 목적이 부정되는 경우에는 적시한 사실의 진실성과 공익성이 인정되는 경우 형법 제310조에 따라 처벌을 면할 수 있기 때문에 가벌성유무를 좌우하는 중요한 요소이므로 그 판단 기준 역시 중요할 수밖에 없다. 법원은 사람

14) 대법원 2006.8.25. 선고 2006도648 판결; 대법원 2000. 2. 25. 선고 98도2188 판결, 2003. 6. 24. 선고 2003도1868 판결

15) 대법원 2004. 6. 25. 선고 2003도4934 판결.

16) 대법원 1995.6.30. 선고 95도1010 판결; 대법원 2003. 12. 26. 선고 2003도6036 판결; 정대관, 앞의 논문, 209쪽; 정완, 인터넷상 명예훼손의 합리적 대응방안, 한국형사정책연구원, 2007, 81쪽

을 비방할 목적이 있는지 여부를 “당해 적시 사실의 내용과 성질, 당해 사실의 공표가 이루어진 상대방의 범위, 그 표현의 방법 등 그 표현 자체에 관한 제반 사정을 감안함과 동시에 그 표현에 의하여 훼손되거나 훼손될 수 있는 명예의 침해 정도 등을 비교, 고려하여 결정”하도록 하고 있다.[17]

Ⅳ. 현행 사이버명예훼손죄 법리 및 관련 개정논의의 비판적 검토

1. 현행 사이버명예훼손죄 법리의 비판적 검토

가. 명예 개념

1) 통설・판례의 입장에 대한 기존의 비판과 재비판

앞서 소개한 바와 같이 우리나라 학계의 통설과 판례는 (사이버)명예훼손죄와 모욕죄 모두 사람의 인격적 가치에 대한 외부적 평가, 즉 ‘외적 명예’만을 보호법익으로 삼는다는 입장이다. 그러나 외적명예뿐만 아니라 ‘인간의 존엄성에 근거한 내면적인 인격가치’, 이른바 ‘내적 명예(innere Ehre)’도 보호대상이 된다는 ‘내적・외적 명예’ 개념이 있는데,[18] 이에 대해서는 내적 명예가 타인에 의해 훼손될 성질의 것이 아니라는 이유 및 현행법상 ‘공연성’ 요건을 근거로 수용하지 않는다.

다른 각도에서 통설의 외적 명예 개념을 비판하는 견해가 있다. 현행법상 진실한 사실의 적시에 의한 명예훼손죄의 성립을 인정하고 있는데, 피해자에

17) 대법원 2002. 8. 23. 선고 2000도329 판결.
18) 김일수・서보학, 앞의 책, 183쪽 이하.

게 당연한 사실을 적시하는 경우 명예의 침해가 없거나 불가능하며, 진실한 사실의 적시에 의한 명예훼손죄를 인정하기 위해서는 명예개념을 순수하게 규범적으로 이해해야 할 필요성을 제시한다. 즉 인간의 존엄성에 근거한 사회적 승인관계에서의 '중요한 가치' 내지 '존중 대우의 요구'가 명예훼손죄 및 모욕죄의 보호법익으로 보아야 한다는 '규범적 명예' 개념(normative Ehre)으로의 대체를 주장하는 것이다.[19] 이 역시 학계의 다수 견해에 의해 비판을 받고 있다. 형법상 모든 규정이 기본적으로 보호법익에 대한 존중요구를 내포하고 있기 때문에 명예에 관한 죄에서만 그러한 존중요구를 보호법익으로 파악하는 점에서 타당치 않다는 것이다.[20]

한편 모욕죄의 경우 외적 명예뿐 아니라 인격적 가치에 대한 자기 자신의 주관적인 평가 내지 감정으로서의 '명예감정(Ehrgefühl)'도 보호법익이 될 수 있다는 일부 견해[21]에 대해서는 그 가벌성이 피해자의 주관적인 감정에 의해 좌우될 수 있다는 점에서 모욕죄의 보호법익으로 부적절하다는 비판을 가한다.

2) 사 견

가) 내적 명예의 침해가능성

우선 내적 명예개념을 비판하는 통설의 논거가 부적절하다는 지적을 하고 싶다. 내적 명예가 외부로부터 침해될 것의 성질이 아니라는 이유로 명예훼손죄 및 모욕죄의 보호법익에서 배제시키는 통설의 논거는 내적 명예 역시 타인의 비방이나 욕설 등에 의해 훼손될 수 있으므로 타당치 않다. 즉 어느 개인이 갖는 인격적 가치로서의 내적 명예가 비방이나 욕설에 의해 양적으로 줄어드는 것은 아니지만(그 점에서 양적 변화를 가져오는 외적 명예와

19) 이정원, 98쪽
20) 김일수・서보학, 제6판, 183쪽; 이천현・도중진・권수진・황만성, 앞의 보고서, 55쪽.
21) 유기천, 형법학(각론강의 상), 138쪽.

구별된다), 그로 인하여 명예 자체가 손상될 수 있는 것이다. 예컨대 아직 사회적인 명성을 획득하지 못한 갓난아기나 연쇄살인범과 같은 악명 높은 범죄인, 사회적 접촉이 전혀 없는 중증장애인이라도 내적 명예를 갖고 있으며 이들에게 비방이나 욕설을 퍼붓는 경우 외적 명예의 침해는 없을지라도 내적 명예의 손상은 인정 가능하다. 그런 점에서 내적 명예를 보호법익의 범주에 포함시킬 것인가 여부는 '침해가능·불가능'의 차원에서 접근할 것이 아니라 명예에 관한 죄의 보호범위를 어디까지 인정할 것인가 하는 입법정책의 문제로 접근해야 할 것으로 보인다.[22]

나) 공연성 요건의 해석

또한 통설은 현행법상 '공연성'의 요건을 근거로 오로지 외적 명예만이 보호법익이라고 주장하는데, 이는 '내적 명예가 침해불가능하기 때문에 보호법익이 될 수 없다'는 다수 견해의 입장을 반박할 수 있는 근거가 될 수 있다. 만약 통설이 이해하는 바와 같이 내적 명예가 본질상 침해불가능한 것이라면 어차피 외적 명예가 침해되기 위해서는 불특정 또는 다수인이 인식할 수 있는 상태가 요구되어질 것이고 따라서 '공연성'이라는 요건이 전혀 불필요한 것이 되기 때문이다. 현행법상 '공연성'의 요건은 그 요건이 충족되지 않는 경우, 즉 불특정 또는 다수인이 인식할 수 있는 상태에서의 비방 또는 욕설행위의 경우, 그로 인한 명예 훼손의 정도가 비교적 경미하여 보호의 필요성이 적고 입증의 어려움도 크다는 점을 고려하여 보호 영역에서 배제하고자 하는 것으로 이해해야 할 것이다.

다) 규범적 명예 개념

또한 '규범적 명예' 개념에 대한 기존의 비판 역시 수긍하기 어렵다. 우선 용어 사용과 관련하여 독일 학계에서의 규범적 명예 개념은 국내에 소개·주

22) 주승희, 인터넷상 명예훼손죄에 대한 비범죄화 주장 검토, 형사법연구 제25호, 2006/여름, 290쪽 이하.

장된 '인격의 중요한 가치로부터 도출되는 존중의 요구'뿐만 아니라 '인간의 존엄성에 근거한 내면적인 인격적 가치', 즉 '내적 명예'를 포함하는 매우 폭넓은 개념이다.[23] 이 외에도 인격체로서의 개인의 독자성을 마련해준다는 의미에서의 '다른 인격체와의 승인관계(Anerkennungsverhältnis)'[24]나 일반적 인격권의 발현으로서의 '상호인격적 명예 개념(interpersonaler Ehrbegriff)'[25] 등 '인간의 존엄성'이라는 규범적 관점에서 도출되는 모든 개념을 규범적 명예 개념으로 포섭하여 이해하고 있다.[26]

위의 여러 가지 규범적 명예 개념 가운데 국내에 소개·주장된 '인격의 중요한 가치 내지 그로부터 도출되는 존중의 요구'를 명예로 이해하는 견해에 대해서 형법상 모든 규정이 기본적으로 보호법익에 대한 존중요구를 내포하고 있기 때문에 명예에 관한 죄에서만 그러한 존중요구를 보호법익으로 파악하는 점에서 타당치 않다는 비판이 있음은 앞서 소개한 바와 같다. 그러나 상기한 규범적 명예, 즉 '인격의 중요한 가치 내지 그로부터 도출되는

---

23) Hirsch, 주 3)의 글, 59면 이하; Schönke·Schröder-Lenckner, Strafgesetzbuch Kommentar, München, 2001, Vor §§185이하. Rd.1; Schmitt-Gläser, Meinungsfreiheit und Ehrenschutz, JZ 1983, 100면. 독일의 규범적 명예개념에 대한 상세한 소개로는 Ju, Seung-Hee, Strafrechtlicher Ehrenschutz im Internet, München, 2005.

24) Wolff, Ehre und Beleidigung, ZStW 1969, 887면. 따라서 승인이론으로 설명되고 있다(Ignor, Der Strafbestand der Beleidigung, Baden-Baden, 1995, 37면).

25) 개인이 사회공동체내에서 다른 사람들과 공존하기 위해서는 인격체로서 존중되어야 하고 자아를 실현할 수 있도록 보장되어야 함을 논거로 한다. Nomos Kommentar zum StGB-Zaczyk, Baden--Baden, 1995, Vor §185; Schönke·Schröder-Lenckner, 주 6)의 글, Vor §§185 이하, Rd.1. 특히 장애인과 비장애인의 관계에서 유의미하다는 평가는 Schramm, Über die Beleidigung von behinderten Menschen: Festschrift für Lenckner zum 70. Geburtstag, 1998, 545면 이하. 그러나 이러한 명예 개념은 너무 불명확하여 인격권 침해의 모든 형태를 모욕죄로 이해할 수도 있다는 비판을 받고 있다.Kubiciel/Winter, Globalisierungsfluten und Strafbarkeitsinseln - Ein Plädoyer für die Abschaffung des strafrechtlichen Ehrenschutzes, ZStW 2001, 310면; Leipziger Kommentar-Herdegen, Strafgesetzbuch, B/5, 10.Aufl., Berlin, 1988, Vor §185 Rd.11; Tenckhoff, Die Bedeutung des Ehrbegriffs für die Systematik der Beleidigungstatbestände, Berlin, 1974, 174면. 이러한 비판에 대한 재비판은 Schramm, 앞의 글, 546면.

26) 우리나라와 같이 명예를 형법적 보호대상으로 삼고 있는 독일의 경우 명예 개념을 둘러싼 논쟁이 매우 활발하다. '만인의 만인을 향한 투쟁(bellum omnium contra omnes)'으로 비유할 만큼 다양한 명예 개념이 등장하며, 법문헌에서만도 60여 가지의 명예 개념을 찾을 수 있다(Hirsch, Ehre und Beleidigung, Karlsruhe, 1967, 5면; Kaufmann, Zur Frage der Beleidigung von Kollektivpersönlichkeiten, ZStW 1972, 418면; Schößler, Anerkennung und Beleidigung, Frankfurt a.M., 1997, 21면, 각주 40).

존중의 요구'를 분석해보면, 앞의 '인격의 중요한 가치'는 기존의 '내적 명예'와 내용이 동일하며, 뒤의 '그로부터 도출되는 존중의 요구'는 명예라는 '보호법익에 대한 존중요구'가 아니라 그 자체가 보호법익이라는 점에서 위와 같은 비판이 타당치 않은 것으로 보인다. 내적 명예라는 것이 사실적으로 존재하는 가치가 아니다. 따라서 이를 보호한다는 것은 결국 '타인의 내면적 인격 가치를 존중하라'는 규범적 의무를 지운다는 점에서 동전의 양면과 같은 내용이며, 서로 분리하여 비판할 것은 아니다.[27]

라) 진실한 사실의 적시에 의한 사실적 명예의 침해 가능성

그렇다고 해서 필자가 국내 문헌에서 주장된 규범적 명예 개념을 지지하는 것은 아니다. 진실한 사실의 적시를 통해서 규범적 명예뿐 아니라 사실적 명예도 침해 가능하기 때문이다. 예컨대 어느 개인에 대한 외부적 명성이 그릇된 정보에 기초한 것일지라도 그가 현재 누리고 있는 명성은 사실적으로 존재하는 것이고, 진실한 사실의 적시를 통해 그동안 누렸던 명성에 금이 간다면 이는 사실적 명예의 침해가 인정될 수 있기 때문이다. 진실한 사실의 적시에 의한 명예훼손죄를 처벌함으로써 어느 개인이 누리는 부당한 명예를 국가가 보호한다는 사실에 대해서 입법론상 비판할 수는 있겠지만, 진실한 사실의 적시에 의한 사실적 명예의 침해가능성을 부정하고 오로지 규범적 명예의 보호만을 주장하는 논거로서는 부적절하다고 생각된다.

마) 소 결

지금까지의 필자의 견해를 정리하자면, 내적 명예(규범적 명예) 역시 본질상 명예에 관한 죄의 보호법익이 될 수 있으며, 이를 보호법익에 포함시킬지 여부는 입법정책상의 문제라는 것이다. 내적 명예를 보호법익으로 삼는 경우, 외적 명예 없이 오로지 내적 명예만 인정되는 사람에 대한 비방행위 또

27) 그런 점에서 한편으론 내적 명예를 보호법익으로 주장하면서 다른 한편으로 '규범적 명예' 개념을 비판하는 주장(김일수・서보학, 앞의 책, 183쪽)에 모순이 있어 보인다.

는 외적 명예의 침해 없이 오로지 내적 명예의 침해만 인정되는 사례의 가벌성을 인정함으로써 명예를 더욱 두텁게 보호한다는 측면이 있지만, 그와 반비례하여 행위자의 표현의 자유가 더욱 제한될 수 있다는 점에서 신중하게 접근할 필요가 있다. 구체적 설명은 아래의 '사이버모욕죄'의 신설의 정당성 검토에서 행하기로 한다.

나. '비방 목적' 요건의 검토

정보통신망법상 사이버명예훼손죄는 형법상 출판물등명예훼손죄와 마찬가지로 명예훼손의 고의 외에 초주관적 불법요소로서 '비방의 목적'을 요구하고 있다. 일반명예훼손죄에 비해 가중 처벌되는 이유가 신문이나 라디오, 인터넷 등을 이용하여 타인을 비방하는 경우 전파성이 더욱 높다는 점이고 또한 비방의 목적을 필요로 하는 목적범이라는 점에서 그 행위반가치가 더 높다는 고려에서라는 것이다.[28]

지금까지의 학설과 판례를 보면 비방 목적이라는 구성요건의 존재 자체에 대해서는 아무런 이의를 제기하고 있지 않지만, 필자는 동 구성요건이 현행법상 명예에 관한 죄의 체계 내에서 다음과 같은 이유 때문에 순기능적 요소보다는 역기능적 요소로 작용할 여지가 크다고 보면, 따라서 형법 제309조 및 정보통신망법 제70조의 비방목적 요건을 삭제할 것과 동시에 양자 모두 진실한 사실의 적시로서 공익성이 인정되는 경우 그 위법성이 조각될 수 있도록 관련 법조문을 정비할 것을 제안하는 바이다.

1) 비방 목적의 개념과 기능에 대한 다수설・판례의 태도

통설은 '비방 목적'을 '사람의 명예를 훼손시키기 위해 인격적 평가를 저하시키려는 의도'로 해석하고 있는데, 이는 명예훼손죄가 성립하기 위해 기본

28) 김일수・서보학, 앞의 책, 200쪽; 박상기, 앞의 책, 190쪽; 배종대, 앞의 책, 287쪽; 이재상, 앞의 책, 196쪽; 임웅, 앞의 책, 208쪽

적으로 요구되는 주관적 요소로서의 고의의 내용과 다르지 않아 보인다. 즉 타인의 명예를 훼손한다는 사실의 '인식'과 '의욕'이라는 내용 중 단지 '의욕'의 측면을 부각시킨 것이다. '비방 목적'에 대한 판례의 해석은 더욱 간단하다. '가해의 의사 내지 목적'이 그것인데,[29] '가해'의 의미가 타인의 명예에 '해'를 '가'하는 것으로 풀이하는 것이 옳다면 또한 '의사 내지 목적'이 '의욕'에 다름 아니라면 결국 명예훼손죄의 주관적 요소로서의 고의와 동일한 것이 된다. 만약 '비방 목적'을 고의와 구별되는 그 무엇으로 해석하고자 하는 경우에는 다음의 두 가지 해석이 가능할 것이다.

첫째, 고의 종류가 인식·의욕강도에 따라 여러 종류로 나뉜다는 점을 고려할 때, 출판물등명예훼손죄 및 사이버명예훼손죄에서 '비방 목적'의 요구가 의욕강도가 낮은 '미필적 고의'에 의한 동죄의 성립을 부정하는 요소로서 기능하는 것이다. 아래의 판례를 보면 법원은 '비방목적'과 '고의'를 별도의 구성요건요소로 구분하여 각각의 존재여부를 판단하는 것이 아니라 '범의'로 통칭하여 판단함을 알 수 있다.

"형법 제309조 제2항 소정의 출판물에 의한 명예훼손죄는 타인을 비방할 목적으로 신문, 잡지 또는 라디오 기타 출판물에 의하여 허위의 사실을 적시하여 타인의 명예를 훼손할 경우에 성립되는 범죄로서, 피고인이 범의를 부인하고 있는 경우에는 사물의 성질상 고의와 상당한 관련성이 있는 간접 사실을 증명하는 방법에 의하여 입증할 수밖에 없고, 무엇이 상당한 관련성이 있는 간접사실에 해당할 것인가는 정상적인 경험치에 바탕을 두고 치밀한 관찰력이나 분석력에 의하여 사실의 연결상태를 합리적으로 판단하는 방법에 의하여야 한다."[30]

---

29) 판례는 사이버명예훼손죄의 비방목적의 의미도 이와 동일하게 해석하고 있다. "정보통신망이용촉진 및 정보보호 등에 관한 법률상의 명예훼손죄에 있어서 '고의'는 타인의 사회적 평가를 저하시킬 사실의 인식과 그 의사를 말하고, '비방의 목적'은 가해의 의사 내지 목적을 요하며, '사실의 적시'는 사실관계에 관한 보고 내지 진술로서 가치판단이나 평가를 내용으로 하는 의견표현에 대치되는 개념으로 시간과 공간적으로 과거 또는 현재의 사실관계에 관한 보고 내지 진술을 의미한다"(대법원 2006.9.28. 선고 2004도6371 판결).

30) 대법원 2002. 12. 10. 선고 2001도7095 판결.

계속해서 법원은 '비방목적'이 '공공의 이익'과 상반관계에 있는 것으로 바라봄으로써 공익성과 적시사실의 진실성이 인정되는 언론매체의 통상적인 보도활동의 경우 '비방목적'이 부인되어 종국적으로 제310조에 의한 위법성 조각의 가능성을 열어 두고 있다. 공익성이 인정되는 경우 비방 목적이 부인됨으로써 그 속성상 공익을 위해 타인의 명예에 관련된 사실을 보도할 수밖에 없는 언론매체의 언론·출판의 자유를 보장해주는 것이다. 다수 견해도 판례의 이와 같은 해석을 지지한다.[31]

"형법 제309조 제1항 소정의 '사람을 비방할 목적'이란 가해의 의사 내지 목적을 요하는 것으로서 공공의 이익을 위한 것과는 행위자의 주관적 의도의 방향에 있어 서로 상반되는 관계에 있다고 할 것이므로, 형법 제310조의 공공의 이익에 관한 때에는 처벌하지 아니한다는 규정은 사람을 비방할 목적이 있어야 하는 형법 제309조 제1항 소정의 행위에 대하여는 적용되지 아니하고 그 목적을 필요로 하지 않는 형법 제307조 제1항의 행위에 한하여 적용되는 것이고, 반면에 적시한 사실이 공공의 이익에 관한 것인 경우에는 특별한 사정이 없는 한 비방 목적은 부인된다고 봄이 상당하므로 이와 같은 경우에는 형법 제307조 제1항 소정의 명예훼손죄의 성립 여부가 문제될 수 있고 이에 대하여는 다시 형법 제310조에 의한 위법성 조각 여부가 문제로 될 수 있다"(대법원 1998.10.9. 선고 97도158 판결).[32]

한편 판례는"행위자의 주요한 동기 내지 목적이 공공의 이익을 위한 것이라면 부수적으로 다른 사익적 목적이나 동기가 내포되어 있더라도 형법 제310조의 적용을 배제할 수 없는 것"[33]으로 판시함으로써, 법문과 달리 '오로지'의 의미를 '주로'의 의미로 해석함으로써 제310조의 적용범위를 넓히고 있다.

---

31) 박상기, 앞의 책, 193쪽 이하; 이재상, 앞의 책, '비방목적'과 명예훼손의 '고의'가 동어반복임을 지적하면서 '비방목적'의 의미를 주관적 의도의 강도 내지 방향성에 찾도록 해야 하고 따라서 '비방목적'과 제310조의 '공공의 이익'이 상호 배척적인 관계에 있는 것으로 보아야 한다는 견해로는 박광민, 앞의 논문, 154쪽.

32) 같은 취지의 판결로는 대법원 2000. 2. 25. 선고 98도2188 판결; 대법원 2003. 12. 26. 선고 2003도6036 판결

33) 대법원 2003. 11. 13. 선고 2003도3606 판결

둘째, '비방 목적'을 그 기능이 아닌 문자적 의미에서 찾는 것인데, 즉 타인의 명예를 훼손한다는 인식과 의욕과 구별되는 '타인을 비난하고자 하는 심정적 상태(비난의도)'로 이해하는 것이다. 다수설이 출판물등명예훼손죄와 사이버명예훼손죄의 가중처벌근거로서 매체의 큰 확산성 외에도 '비방 목적'이라는 행위 양태를 들고 있음을 볼 때, 비방 목적은 단순히 (언론출판자유의 보장을 위하여) 출판물등명예훼손죄와 사이버명예훼손죄의 성립을 제한하는 요소로서만 작동하는 것이 아니라, 그 자체가 불법가중요소로서 인식되고 있는 것으로 보인다. 또한 언론기관이 공익을 위하여 진실을 보도하더라도 비방목적에 의한 출판물등명예훼손죄가 성립되는 경우 제310조에 의한 위법성 조각을 부인하는 취지의 아래 판결은 '비방 목적'이 '공공의 이익'과 상호배척 관계에 있는 것이 아니라 병존할 수 있는 개념으로 파악하는 것으로 보인다.

형법 제307조 제1항의 명예훼손행위가 진실한 사실로서 오로지 공공의 이익에 관한 때에는 위법성은 조각되나 형법 제309조 소정의 출판물등에 의한 명예훼손행위는 그것이 오로지 공공의 이익을 위한 행위였더라도 위법성이 조각되지 않음은 형법 제310조의 규정에 비추어 명백하다(대법원 1986.10.14. 선고 86도1603 판결)[34]

2) 사 견

'비방 목적'에 대한 위의 두 가지 이해 가능성 모두 다음과 같은 이유에서 비판의 여지가 크다.

가) '비방 목적'과 '공공의 이익'의 병존가능성

우선 출판물등명예훼손죄와 사이버명예훼손죄에서의 '비방 목적'과 '공공의 이익'이 주관적 의도의 방향에서 서로 상반되는 것으로 파악하는 것은 법리

34) 같은 취지의 판결로는 대법원 1993. 4. 13. 선고 92도234 판결; 대법원 1995. 6. 30. 선고 95도1010 판결.

상 부적절하다고 본다. 비방 목적은 행위자의 내심의사로서 그 유무를 판단하기 위해서는 피해자가 자백하지 않는 한 간접사실에 의존할 수밖에 없고, 그 한 요소로 적시한 사실의 '공익성'이 고려될 수 있을 것이다. 그러나 공익성과 비방목적은 별개의 구성요건으로 사안에 따라 얼마든지 병존할 수 있으며, 더 나아가 공익성이 클수록 피해자에 대한 '가해의사' 내지 '사람의 명예를 훼손시키기 위해 인격적 평가를 저하시키려는 의도(비난의도)'가 더욱 커지는 것이 오히려 일반인의 본성에 부합하는 것으로 보이기 때문이다. 말하자면 공익성이 인정되는 명예훼손행위에서의 피해자는 공무원이나 어느 단체의 장 등 공적인 위치에 있는 사람이거나 어떤 형태로든 공적인 일과 관련된 사람일 것이고, 이들에 대해서는 일반 사인보다 더욱 높은 윤리가 요구되는 것이 일반적이라는 점에서 그의 비리를 누설하고자 하는 의욕이나 비난의 욕구 모두 클 것이라는 점이다.[35] 법리상 비방목적이 인정되는 경우에는 형법 제310조에 의한 위법성 조각이 부정될 것이므로 구태여 공익성 유무를 판단할 필요가 없는데, 법원은 거꾸로 '공익성'이 인정되는 경우 '비방목적'이 부인된다고 봄으로써 명예훼손죄 체계에 혼란을 초래하고 있다.[36]

나) 윤리형법적 성격

물론 피해자에 대한 아무런 비난의도(비방 또는 명예훼손의 의욕) 없이 오로지 공익을 위해 피해자의 비리를 누설하는 경우를 생각해볼 수 있다. 신문사 등 언론매체의 기자는 그 내심에 피해자에 대한 어떤 비난 또는 비방 의도 없이 업무상 오로지 공익을 위해 피해자의 비위사실을 밝힐 수 있기 때문이다. 그렇다면 결과불법이 동일함에도 비방의도가 있었던 사례를 그렇지 않은 경우보다 가중처벌해야 할 근거는 무엇인가? 만약 다수설과 같

35) 예컨대 국회의원의 성매매사실의 적시는 그가 공인이기에 일반 사인의 성매매사실의 적시와 달리 '공익성'이 인정됨과 동시에 그가 공인이기에 가해자의 내면에는 일반 사인의 성매매보다 더욱 큰 비난의도가 수반될 수 있는 것이다.

36) 같은 견해로는 윤종행, 사이버명예훼손죄에 있어서 비방의 목적과 공익관련성, 형사정책 제18권 제1호, 318쪽.

이 '비방 목적'을 불법의 가중요소로 이해하게 되면 이는 국가가 개인에게 '죄는 미워하되 사람은 미워하지 말라'와 같은 윤리의무, 즉 '타인의 비위사실을 공익을 위하여 적시하되 내심에 그를 비난하는 의도를 품지 말라'라는 윤리적 의무를 부과하고 이를 위반하는 것을 비윤리적인 행위로 보아 더욱 중하게 처벌하는 것이 되어 부당하다. 근대형법이 벗어나고자 하는 일종의 '윤리형법'의 성격을 갖게 되기 때문이다.

다) 언론기관과 일반 사인의 차별

이와 달리 출판물등명예훼손죄의 '비방 목적'이 언론기관이 갖는 사실공개적 성격과 공공성, 공익성을 감안하여 개인의 명예보호와 언론출판의 자유를 조율하는 기능을 가지고 있기 때문에 그런 성격을 갖지 않는 정보통신망 이용행위는 비방 목적이 없더라도 사이버명예훼손죄의 성립을 긍정해야 한다는 견해가 있다.[37] 행위주체면에서 언론기관과 사인을 구별하여, 언론기관은 비방목적이 없는 경우 사이버명예훼손죄의 성립을 부정하지만, 사인의 경우 정보통신망에 공익을 위해 진실한 사실을 적시하더라도 동죄의 성립을 인정하자는 것인데, 이와 같은 차별은 오늘날 인터넷상 정보교류현황을 보면 그다지 합리적으로 보이지 않는다. 언론사에게 공정하고 진실한 사실의 보도의무가 인정된다고 해서 현실적으로 각 언론사가 정치적·경제적 이익과 무관하게 공정하게 진실한 보도를 하여 독자들로부터 큰 신뢰를 얻는 것은 아니기 때문이다.[38] 오히려 '정보프로슈머(information prosumer)'라는 신조어가 있을 정도로 일반 사인도 때에 따라서는 자신의 전문성을 발휘하여 공공의 이익과 고도의 신뢰성을 확보할만한 정보를 제공할 수 있고, 실제로 언론매체가 게시한 기사에 대해 그 오류 및 부당성을 지적하는 댓글을 심심찮게 볼 수 있다. 과거 일반 사인은 대중매체가 제공하는 정보의 수용자에 불과했지만 인터넷의 등장으로 인해 얼마든지 정보제공자가 될 수 있는 오늘날

37) 박상기, 앞의 책, 199쪽; 정완, 앞의 보고서, 81쪽.
38) '안티조중동운동'이 그 대표적 예이다.

정보화시대에는 더 이상 일반 사인(네티즌)을 언론기관과 차별할 실익이 없고, 오히려 제공된 정보의 '진실성'과 '공익성'을 잣대로 그 불법성을 판단하는 것이 합리적으로 보인다.

라) 소 결

결론적으로 현행 출판물등명예훼손죄와 사이버명예훼손죄의 구성요건 가운데 '비방 목적' 요건은 삭제할 필요성이 있다고 판단된다. 동시에 제310조의 위법성조각사유에 제309조 제1항을 추가함으로써 출판물등명예훼손죄의 경우에도 진실한 사실의 적시로서 공공의 이익이 인정되는 경우 그 가벌성을 배제시켜야 할 것이며,[39] 같은 취지에서 정보통신망법에도 형법 제310조에 상응하는 위법성조각규정을 신설해야 할 것이다.[40] 앞에 지적한 바와 같이 '비방 목적' 요건이 출판물등명예훼손죄의 성립을 제한함으로써 언론출판의 자유를 보장하는 기능으로만 작동하는 것이 아니라 일부 판례와 같이 '비방 목적'이 인정되는 경우 형법 제310조에 의거한 위법성조각을 불가능하게 함으로써 그 가벌성을 확장하는 요소로서 기능할 수 있기 때문이다. 공익을 위하여 진실한 사실을 적시한 행위가 타인의 명예를 훼손했다는 이유로 처벌하게 된다면 개인의 명예보호에 치중한 나머지 국민의 알권리나 언론의 자유를 부당하게 침해할 수 있어 부당하며, 법원이 '비방목적'과 '공익성'을 '행위자의 주관적 의도의 방향에 있어 서로 상반되는 관계'로 파악하고자 하는 것은 바로 위와 같은 불합리함을 시정하기 위한 고육지책으로 보이기 때문이다. 비방목적이라는 요건을 삭제하더라도 출판물등명예훼손죄와 사이버

39) 형법제정 당시 정부가 제출한 형법초안에는 명예훼손죄의 위법성조각규정인 제333조(현행 제310조)의 적용대상에 제332조 제1항(현행 제309조 제1항)도 포함되었으나, 법제사법위원회는 현재의 다수설, 판례의 태도와 같이 '비방 목적'을 '오로지 공공의 이익에 관한 이유'라는 제333조 구성요건과 상반된 관계로 보아 목적범인 제332조 제1항에 대해서는 제333조가 적용될 여지가 없다는 이유로 이를 삭제할 것을 주장하였는데 이것이 받아들여져 오늘날에 이른 것이다(한국형사정책연구원, 형사법령제정자료집(1), 형법, 1990, 70쪽, 482쪽 이하),

40) 특별형법의 범람과 일반형법의 사문화를 고려할 때 종국적으로는 정보통신망법상의 명예훼손에 관한 규율 규정이 형법전 속으로 편입되어야 할 것이다.

명예훼손죄는 그 확산성으로 인해 가중처벌의 근거가 충분한데, 비방목적 요건이 존재하고 제310조의 적용 대상에 제309조 제1항이 제외됨으로써 '공익성'과 애매한 관계에 처하게 되고, 결과적으로 법관의 자의적 판단 가능성을 높이는 구실만 하고 있다. 참고로 명예훼손죄의 성립에 있어 고의 외에 '비방 목적'을 초주관적 요소로 요구하는 입법례는 우리나라가 유일하다. 현행 명예에 관한 죄는 다른 범죄들과 마찬가지로 연혁상 일본법과 독일법에 기초한 것인데, 양국의 법에 있지 않는 요소를 첨가했다는 점에서 독창성을 인정할 수 있겠지만, 언론출판의 자유보장이나 윤리형법의 탈피를 위해서 삭제하는 것이 바람직하다.

2. 관련 개정 논의의 검토

가. 반의사불벌조항의 삭제 필요 여부

현행법상 사이버명예훼손죄는 오프라인에서의 명예훼손죄와 마찬가지로 피해자의 명시한 의사에 반하여 기소할 수 없다(정보통신망법 제70조 제3항). 따라서 인터넷상 명예훼손의 내용을 담고 있는 사이트가 발견되더라도 피해자의 처벌의사부터 확인한 후에나 심의에 들어가거나 수사를 개시하는 것이 실무이다. 이와 관련하여 사이버명예훼손죄의 반의사불벌조항이 삭제되어야 한다는 주장이 제기되고 있다. 인터넷상 명예훼손죄가 발생하게 되면 다수의 네티즌들에 의한 무비판적 퍼나르기 등을 통해 순식간 사이버공간 전체로 그 피해가 확산되기 때문에 피해자의 피해가 사후구제조치만으로 회복하기에 너무 심각해지고, 원래의 가해자뿐 아니라 수많은 가해자들이 가담하게 됨으로 피해자의 의사만을 고려하여 사건을 해결하는 전통적인 수사방법이 부적절하다는 이유이다.[41]

41) 정완, 앞의 보고서, 113쪽.

필자 역시 사이버공간에서의 명예훼손행위가 법익침해 양태나 정도에 있어 현실공간에서의 명예훼손행위와 차이가 있다는 사실 인식에는 공감하지만, 다음의 두 가지 이유에서 반의사불벌조항의 존치를 주장하는 바이다.

첫째, 입법자가 명예훼손죄를 반의사불벌죄로 규정한 이유는 본 죄가 폭행죄나 협박죄 등의 다른 범죄와 마찬가지로 국가형벌권의 발동을 피해자의 의사에 종속시켜도 괜찮을 만큼 법익침해가 경미하다는 판단에 기초한 것인데,[42] 이와 같은 판단은 사이버명예훼손죄라고 해서 달라지지 않기 때문이다. 인터넷이 갖는 특성, 예컨대 무한복제가능성, 신속한 전파가능성, 익명성 등으로 인해 인터넷게시판 등에 타인에 대한 비방의 글을 올릴 경우 제3자에 의해 쉽게 확산될 가능성이 있다는 점에는 이론의 여지가 없지만, 그로부터 곧바로 사이버명예훼손죄의 법익침해의 정도가 크다는 결론을 내려서는 안될 것이다. 현실적으로 인터넷에 올려진 모든 비방정보가 복제·확산되는 것이 아니라, 일반적으로 사회적 관심을 끌만한 이슈들만이 네티즌들에 의해 확산되기 때문이다. 예컨대 정치인의 부적절한 언동이나 정책의 발표, 연예인의 사생활 등 공적 관심사가 대부분이며, 사인과 관련한 정보 역시 그 사인의 행동이 공적 관심을 충분히 끌 만한 언행인 경우에나 다수 복제·전파되고 있다.[43] 물론 타인에 대한 명예훼손적 정보가 다수의 네티즌들의 관심을 끌게 되어 일단 확산된 경우에는 법익침해의 정도가 오프라인에서보다 클 수 있다. 그러나 그와 같은 가중된 결과불법은 현행 정보통신망법상 사이버명예훼손죄의 법정형에 이미 반영되어 있는 것으로 보인다.

둘째, 사이버명예훼손죄에 대한 반의사불벌조항의 삭제는 형사정책적 측면에서 부정적 결과를 초래할 수 있다. 피해자가 미처 인식하지 못한 법익침해행위에 대해 발빠르게 대응할 수 있다는 점에서 명예라는 법익보호가 좀 더 강화될 수 있겠지만, 인터넷상 타인에 대한 비방내용이 곳곳에 넘쳐나

42) 배종대, 형법총론(제9판), 2008, 148쪽
43) 일명 개똥녀 사건을 예로 들 수 있다.

는 현실과 명예훼손죄보다 법익침해가 더욱 큰 중범죄에 대한 수사인력과 예산도 부족한 현실을 고려할 때, 오히려 사이버명예훼손죄에 대한 집행의 결손만이 더욱 부각될 우려가 있다. 더 나아가 부족한 인력과 예산으로 인한 집행의 결손은 자의적인 법집행의 우려와 함께 사법부에 대한 국민의 신뢰를 저하시킬 수 있다는 점을 간과해서는 안 될 것이다.[44] 현재 명예훼손의 피해자가 피해사실을 경찰에 적극적으로 알린 경우에도 사안의 경미성과 수사인력의 부족으로 경찰의 대응이 소극적이라고 한다.[45] 그런 점에서도 반의사불벌조항 삭제 주장은 이미 피해자로 부터 고소된 명예훼손사건에 대해서 수사기관이 적극적으로 대응할 수 있는 여건이 마련된 후 논의해도 늦지 않으리라는 판단이다.

나. 사이버모욕죄 신설의 필요성 여부

최근 연예인의 자살의 원인으로 인터넷상 '악플'[46]이 지목되면서 사이버모욕죄를 신설하자는 주장이 더욱 힘을 받고 있다. 현행 정보통신망법에는 모욕행위의 처벌에 관한 별도의 규정이 없어 형법상 모욕죄의 적용을 받게 되는데, 인터넷에 게시된 악플의 경우 오프라인에서의 욕설보다 순식간에 전체 사이버공간으로 확대되고 그에 따라 피해자가 받는 정신적 충격이 매우 크고 회복불가능하다는 점에서 오프라인에서의 모욕죄보다 가중처벌할 필요성이 있다는 것이다.[47] 사이버모욕죄의 가중처벌의 필요성은 사이버모욕죄의

---

44) 경찰청은 2008년 10월 6일부터 한달간 전국 사이버수사요원 900명을 동원해 인터넷상 허위사실 유포 및 악성댓글에 대해 집중단속을 벌인다고 밝힌 바 있다.(http://www.police.go.kr/announce/newspdsView.do?idx=92861&cPage=1) 그 자체만 보면 법익보호의 측면에서 바람직하지만, 그 시기면에서 볼 때 자칫 정부정책에 반대하는 네티즌들의 통제라는 정치적 목적이 개입된 것이라는 오해를 살 수 있다(http://www.mediatoday.co.kr/news/articleView.html?idxno=73239).

45) 정완, 앞의 보고서, 19쪽

46) 네티즌들이 인터넷 뉴스나 게시글 밑에 자신의 의견이나 소감 등을 적는 일이 많은데 이를 댓글이라 하며, 댓글 중에서 욕설 등과 같은 비난의 내용을 글을 '악플'이라고 하고, 반대로 칭찬의 내용을 담은 경우 '선플'로 표현하고 있다,

47) 정완, 앞의 보고서, 107쪽 이하.

불법이 오프라인에서의 불법보다 크다는 것을 전제로 해야 할 것인데, 사이버모욕죄의 가중처벌을 주장하는 견해는 사이버모욕죄로 인한 법익침해가 일반 모욕죄가 적용되는 사례보다 더욱 크다는 점을 그 이유로 삼고 있다.

그러나 사이버모욕죄가 일반 모욕죄와 마찬가지로 '외적 명예'라는 법익을 보호한다는 통설과 판례의 견해에 따르면, 위의 전제는 잘못된 것으로 보인다. 현재 우리나라의 댓글문화를 고려해 볼 때 인터넷게시판 등에 악플이 많이 달린다고 해서 악플대상자의 외적 명예가 그만큼 많이 침해되는 것으로 보기 어렵기 때문이다. 게시판에 악플이 달리는 경우를 가정해보면 크게 두 가지로 나눌 수 있다. 그 한 가지는 기사나 게시물의 내용상 악플대상자가 비난받을 만한 행동을 했을 경우이고, 나머지는 기사나 게시물의 내용이 악플이 아닌 선플의 대상이 됨이 마땅함에도 엉뚱하게 악플이 달린 경우이다.

우선 첫 번째 사례의 경우 네티즌의 악플달기로 인해 그 대상자의 외적 명예가 침해되었다고 보기 어렵다. 만약 악플대상자의 외적 명예가 침해되었다면, 이는 악플에 의한 것이 아니라 악플을 유발한 기사나 게시물의 게시자의 게시행위로 인해 비롯되었다고 보아야 할 것이고, 따라서 그 법적 책임은 게시자가 부담해야 할 것이다.(진실한 사실인 경우 정보통신망법 제70조 제1항이, 허위사실인 경우 동법 동조 제2항이 적용될 것이다.)

두 번째 사례의 경우에도 악플 자체로 인해 악플대상자의 외적 명예가 침해되었다고 보기 어려운 측면이 있다. A의 선행을 보도한 기사에 B가 악플을 다는 경우, B를 비난하는 악플이 무수히 달리는 것이 일반적인데, 이를 볼 때 그와 같은 행위로 인해 침해되는 외적 명예는 A가 아닌 B의 것이며, 그와 같은 행위를 규제할 경우 B를 비난하는 다수의 네티즌들이 오히려 법적 책임을 부담하는 부당한 결과를 초래할 수 있다.

그런 점에서 외적 명예를 보호법익으로 보는 한 사이버모욕죄의 불법이 일반 모욕죄보다 크다고 보기 어렵다. 반면 '명예감정'이나 '규범적 명예'를 보호법익으로 간주하는 견해를 취하는 경우에는 사이버모욕죄의 불법이 크

다고 볼 여지는 있다. 그러나 앞서 지적한 바와 같이 명예감정은 자신의 인격가치에 대한 주관적 평가로서 얼마든지 과소·과대평가될 수 있고, 정신병자나 유아처럼 주관적 명예감정이 없는 경우도 있어 보호법익으로 삼기 어렵다는 비판이 계속 제기되고 있다. 특히 사이버모욕죄는 그 특성상 악플 등 욕설을 담고 있는 정보가 인터넷 곳곳에 퍼져있을 수 있어 명예감정의 훼손정도가 피해자의 정보수집양에 좌우될 수 있다는 점을 간과해서는 안될 것이다. 구태여 자신에 대한 부정적 평가를 모두 서핑할 필요가 없음에도 부지런히 수집·확인하여 명예감정의 훼손을 자초한 피해자에 대해서 법익침해가 크다는 이유로 국가가 강력한 보호를 해줄 필요성이 없다는 점에서 명예감정을 법익으로 삼기 어렵다고 본다.

반면 규범적 명예는 '인격의 중요한 가치로부터 도출되는 존중의 요구' 또는 '인간의 존엄성에 근거한 내면적인 인격적 가치'를 보호한다. 따라서 인터넷게시판 등에 악플을 다는 행위는 곧바로 타인의 인격적 가치의 존중 위반으로서 명예훼손이라는 법익침해의 결과를 인정할 수 있으며, 일반 모욕죄에 비해 더욱 많은 수의 사람들이 이를 목격할 수 있다는 점에서 결과불법이 더욱 크다고 볼 여지가 있다. 즉 독일의 통설처럼 사실적·규범적 명예개념을 취하는 경우 사이버모욕죄의 가중처벌이 정당화될 수는 있겠지만, 이는 형법이론적 측면과 형사정책적 측면에서 모두 바람직하지 않다고 본다.[48] 타인과 더불어 사는 삶 속에서 타인을 자신과 동등한 인격체로 존중함이 마땅하고, 따라서 타인의 그릇된 행동을 보아도 다수의 사람들 앞에서 지적하고 모욕하여 상처를 주는 것은 비윤리적인 행위로서 지양되어야 할 것임에는 이론의 여지가 없다. 그러나 재산이나 생명, 외적 명예와 같은 구체적 법익의 침해가 수반되지 않는 단순한 인격존중윤리위반을 형벌로 처벌하는 것은 형법의 최후수단성원칙에 반하며, 장차 그와 유사하게 타인의 인격을 존

48) 현실세계에서의 모욕행위보다 사이버공간에서의 모욕행위의 불법성이 더 크다고 할 만한 뚜렷한 근거가 없으며 일반형법으로 충분히 대응할 수 있다는 이유로 사이버모욕죄의 신설을 반대하는 견해로는 이천현·도중진·권수진·황만성, 앞의 보고서, 115쪽.

중하지 않는 모든 행위를 처벌대상으로 수용하지 않는 한 평등원칙에도 반할 수 있다. 무엇보다 한정된 사법자원을 모욕행위보다 가벌성이 큰 중대범죄를 적발·처벌하는데 사용하는 것이 형사정책적으로 더욱 합리적이라고 사료된다.

Ⅴ. 나가며

헌법재판소는 인터넷이 '가장 참여적인 시장'으로 '표현촉진적인 매체'임을 인정하면서, "인터넷상의 표현에 대하여 질서위주의 사고만으로 규제하려고 할 경우 표현의 자유의 발전에 큰 장애를 초래할 수 있다"는 전제하에, "표현매체에 관한 기술의 발달은 표현의 자유의 장을 넓히고 질적 변화를 야기하고 있으므로 계속 변화하는 이 분야에서 규제의 수단 또한 헌법의 틀 내에서 다채롭고 새롭게 강구되어야 할 것"임을 밝힌 바 있다.[49] 그러나 개인의 명예 보호 역시 표현의 자유가 보장하고자 하는 민주주의 발전과 개인의 자아실현에 기여한다는 점에서 인터넷상 명예훼손죄의 형사처벌 역시 정당성을 갖는다.[50] 다만 인터넷상 개인의 명예 보호는 그와 상반관계에 있는 표현의 자유를 과도히 침해하지 않아야 할 것이며 행위자는 그 불법에 상응하는 한도내에서만 책임을 진다는 형법이론적 한계내에서 이루어져야 할 것이다. 한정된 사법자원의 효율적인 사용이나 집행의 결손이 초래할 사법에 대한 신뢰저하 등 형사정책적 요소도 함께 고려해야 할 요소이다. 그런 취지에서 필자는 현행 출판물등명예훼손죄와 사이버명예훼손죄의 '비방목적' 요건이 그 개념과 기능면에서 삭제될 필요성이 있음을 본문에서 제시하였고 최근 논의되고 있는 정보통신망법상 반의사불벌조항의 삭제나 사이버모욕죄

49) 헌법재판소 2002.6.27, 99헌마480.
50) 인터넷상 명예훼손죄에 대한 비범죄화 주장에 대한 비판으로는 주승희, 앞의 논문, 292쪽 이하.

의 신설 필요성에 대해서는 다소 비판적인 입장을 피력하였는데, 앞으로 이에 대해 더욱 활발한 논의가 진행되길 희망하는 바이다.

2008년 추계 학술회의 자료집

사이버 문화의 확산에 따른 역기능
증가와 대응방안

발행인 / **박 상 기**
발행처 / **한국형사정책연구원**
서울시 서초구 우면동 142
전화 (02) 575-5282~9
팩스 (02) 571-7488
발행일 / 2008년 10월 30일
등 록 / 1990.3.20. 제21-143호
인 쇄 / ㈜피알앤북스 (02) 467-4545

※ 본서 내용의 무단복제를 금함

[비매품]