현행법상 사이버 테러의 규제 가능성에 대한 검토

조현비
[illegible]

현실세계가 아닌 사이버 공간에서도 현실과 똑같은 불법행위 유형들이 나타나고 있고, 그 폐해가 확산되면서 가상공간에서의 제재 가능성에 대한 검토 필요성이 증대되고 있다. 그러나 우리 사회에서 일반적으로 사용하고 있는 '사이버 테러' 라는 용어는 사이버 공간에서의 각종 불법행위를 지칭하는 '사이버 범죄'라는 용어와 혼용되고 있고, 또한 전통적 테러리즘과도 다른 의미를 포함하고 있다. 따라서 본 연구에서는 우리나라에서 통제하고 있는 사이버 테러의 각종 유형을 검토하면서 사이버 범죄와 전통적 테러리즘과의 차이를 살펴보고 이를 바탕으로 사이버 공간에서의 불법행위 유형을 규제하는 관련 법규정으로 국제법상의 사이버범죄방지조약과 국내법상의 실제 적용가능 법률들을 살펴보았다. 관련 현행법으로는 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률, 화물유통촉진법, 형법 등이 실제 적용되고 있었다. 그러나 이러한 현행법들은 정보통신망을 보호를 주된 보호법익으로 하고 있고, 벌칙규정으로 정보통신망 침해 등의 한정된 행위만을 규율하고 있었다. 개별적 불법행위에 대하여는 형법의 적용 가능성만 열려 있었다. 그리고 사이버 공간에서의 불법행위 유형의 특성상 재판관할에 대한 부분도 문제가 되고 있었다. 현행법상 사이버테러를 규제하기에는 많은 부족한 점이 있고, 사이버세계도 현실세계와 마찬가지로 많은 불법행위 유형들이 나타나고 있기 때문에 불법행위들을 규율하기 위한 새로운 입법의 필요성이 제시되었다.

주제어: 사이버 테러, 사이버 범죄, 컴퓨터 범죄, 법적 규제

Ⅰ. 서론

우리 사회에서 소위 "정보화"는 급속도로 사회를 변화시키고 있으며 많은 유무형의 이익들을 가져오게 한 문명의 이기이다. 그러나 어느 사회든 그 사회의 질서를 유지시키기 위한 최소한의 테두리를 가지고 있으며 그러한 기준에 의하여 문명의 이기를 적절하게 이용하고자 하는 노력을 계속하고 있다. 그러나 "정보화"가 급속하게 진행되면서 기존의 2차원적 현실공간이 아닌 소위 사이버 공간에서도 현실세계와 똑같이 적법한 행위와 불법행위 유형이 나타나고 있다.

시간과 공간의 제약이 적은 사이버 공간을 이용한 첨단 신종 수법의 범죄가 계속 발생하고 있고, 그 피해나 파급효과도 대형화, 다양화 되고 있다. 문서위조, 신용카드 도용 등과 같은 컴퓨터를 이용한 단순한 형태의 범죄는 물론 국가기간전산망, 산업전산망 등에서 관리되고 있는 압축 집약된 정보에 대한 전문 범죄집단의 사이버 테러리즘 등 위협적 공격의 위험성이 다양하게 나타나고 있다(최진태, 2006: 163). 실제로 사이버 공간의 불법행위와 그로 인한 피해사례가 급격히 늘면서 사이버 공간의 법질서를 유지하는 문제가 법집행기관의 중요한 현안으로 부각되고 있으며, 법질서를 유지하기 위한 구체적인 매개체인 규제법률의 타당성에 대한 검토도 매우 필요하다.

사이버 공간에서의 다양한 불법행위 유형들을 규제하고 통제하는데 있어서 소위 사이버 범죄와 사이버 테러라는 용어가 우리 사회에서 쉽게 혼용되고 있다. 물론, 범죄와 테러라는 각각의 용어가 함축하는 의미는 매우 다

르지만, 사이버 공간에서의 불법행위에 대하여 구체적인 법률을 적용하는 데에는 과연 어떤 행위유형에 대하여 어떤 법률을 적용하는 것이 가능할 것인지에 대한 논의는 쉽게 찾아보기가 어렵다. 사이버 공간에서의 불법행위들을 현실공간에서의 법률에 의하여 규제하여야 하기 때문이다. 실제로 사이버 공간에서의 다양한 불법행위들이 존재하지만, 이에 대한 심도 있는 관심은 과거의 컴퓨터 범죄, 컴퓨터 관련 범죄, 하이테크 범죄, 사이버 범죄 등의 행위 양태에 대한 논의 및 연구가 붐을 이루다가 최근에는 약간 시들해 진 듯하다. 최근에는 사이버 범죄 전반에 대한 논의보다는 사이버 공간에서의 불법행위 중에서도 명예훼손, 개인정보침해, 인터넷 사기 등 개별적인 불법행위 유형으로 그 관심이 좁혀지고 있고, 본 연구에서 검토하고자 하는 사이버 테러에 대한 관심도 그 경향의 하나이다. 사이버 공간에서의 각각의 불법행위 유형들을 효율적으로 통제하기 위한 방법 중의 하나가 그에 대한 규제법규를 잘 정비하는 것이다.

그러나 사이버 공간에서의 불법행위들은 기존의 불법행위의 구성요건에 컴퓨터 또는 컴퓨터망을 이용한다는 부분을 추가하면 어느 정도 커버가 가능하지만 사이버테러 라고 하는 부분은 그 효율적 통제가 법률상으로는 약간 애매한 듯하다. 사이버 테러라고 하는 행위양태가 명확하게 구분되는 것이 어렵기 때문이다.

따라서 다음에서는 현행법상 사이버 테러의 규제가능성을 검토하는데 있어서 과연 사이버 테러라는 행위유형이 구체적으로 어떻게 구분되어야 하고 또 실제로 우리가 가지고 있는 규제법규가 적용가능한 가에 대하여 하나씩 살펴보도록 하겠다.

II. 사이버테러와 사이버범죄

1. 테러리즘 개념의 확장

테러 또는 테러리즘 이라는 표현은 일반 대중들의 흥미와 관심을 쉽게 이끌어 낼 수 있는 매우 매혹적인 용어로서 우리의 일상생활에서 어렵지 않게 찾아 볼 수 있다. 테러는 공포 또는 공포를 야기하는 행위 자체를 뜻하며, 테러리즘은 행위 자체와 함께 이념적 측면도 포함되는 말이다(신의기, 2002: 27). 테러리즘은 원래 정부 또는 혁명단체에 의하여 조직적, 집단적으로 행해지는 공포수단을 의미하는 것이었으나 오늘날에는 개인이나 단체가 정치, 종교 기타 목적을 달성하기 위하여 행하는 폭력행위로까지 그 정의의 범위가 확대되고 있다.

이처럼 테러리즘의 정확한 실체 내지 범위에 대하여는 학자들 및 관련 실무자들, 그리고 대중매체를 포함한 일반인들에게 있어서까지 매우 다양한 범위의 어떤 행동양태로서 받아들여지고 있으나, 공통적으로 지적되고 있는 요소는 정치적, 종교적, 사회적 주장 등의 일정한 목적을 위한 암살, 살해, 납치, 폭발 등 생명이나 신체의 안전을 위협하는 폭력의 행사로서, 충동적이거나 우발적이기보다는 조직적, 집단적, 계획적으로 행하여지며, 그 결과 직접적인 범죄피해자 뿐만 아니라 사회 전반에 대하여 공포 및 불안심리를 야기하는 일련의 범죄행위를 의미하기도 한다(이건종 · 조현지, 1995).

실무상으로는 미국 중앙정보국(CIA)에서 "테러리즘이란 정치적 상징효과를 얻기 위한 폭력의 사용 또는 그 위협으로서 직접적인 피해자보다는 다수 대중에게 심리적인 충격을 가하려는 목적을 가진 것이며, 여기에는 국가 내에서의 전복활동 또는 반란적 군사활동까지 포함한다"고 정의하고 있으며, 국제형사경찰기구(ICPO)는 "테러리즘이란 공포 또는 불안을 확산시켜 정치적인 목적을 달성하기 위해 계획된 조직집단에 의한 폭력적 범죄활동"이라고 규정하고 있다. 우리의 경우도 대통령 훈령 제47호인 '국가대테러활동지침' 제2조에서 "국가이익과 국민에 대하여 국제테러분자 등이 각종의 목적을 위하여 국내외에서 불법적으로 자행하는 각종 범죄행위"를 국제테러로 규정하고 있다(신의기, 2002: 29-30).

그러나 최근에는 전통적으로 테러리즘에 포함되는 요소인 정치적인 목적이 필요한 것 같지는 않다. 정치적 목적보다는 경제적 이익을 목적으로 하는 마약테러(Narco-Terrorism), 환경파괴를 수단으로 하는 환경테러(Environmental Terrorism), 컴퓨터 등을 이용한 정보, 통신관련 테러 등 새로운 형태의 행위유형들이 테러 또는 테러리즘의 범주로 들어오고 있다. 경우에 따라서는 단순 범죄로서 인식될 것을 테러로 분류하는 등 테러리즘 개념이 확장되는 경향을 볼 수 있다[1].

1) 2007년 7월 21일 한나라당 정형근 의원이 한나라당의 새 대북(對北)정책을 설명하러 재향군인회에 갔다가 달걀 세례를 받은 폭력행위를 달걀테러라는 표현으로 각종 매스컴에서 보도되기도 하였으며, 1999년 6월 3일에는 김영삼 전 대통령이

또한 테러행위 주체의 조직성 또는 집단성에 대한 요소도 문제가 될 수 있다. 과거에는 국제테러조직의 지휘하에 조직성을 가지고 테러리즘이 자행되는 경우가 대부분이었으나, 최근에는 사이버테러 등의 행위양태로서 제시되고 있는 해킹, 바이러스 유포 등을 통한 시스템의 무력화 등은 반드시 전통적인 테러리즘에서의 조직성을 요구하지는 않는 등 정치적 목적, 공포유발 등의 목적을 수반하지 않고 침해 또는 피해를 목적으로 하는 행위 또한 테러리즘의 한 유형으로 포함시키는 등 그 개념의 확장 경향을 볼 수 있다.

2. 사이버테러와 사이버범죄

1) 사이버테러와 사이버범죄의 개념

브리태니커 사전에 의하면 사이버테러란 인터넷을 이용해 시스템에 침입하여 데이터를 파괴하는 등 해당 국가의 네트워크 기능을 마비시키는 신종 테러 행위라고 정의하고 있다. 이러한 사이버테러라는 용어는 새로운 테러의 형태로서 일반적으로 이해되고 있다. 테러리즘이 사이버 공간을 통해 사이버 수단을 이용해 테러 목적을 달성하려고 하는 행위를 사이버테러라고 이해하고 있으며, 용어에 대한 공식적인 정의나 통일된 의견은 아직 결정되고 있지 않다. 그러나 이러한 사이버테러가 개인으로부터 집단, 국가에 이르기까지 다양한 주체로부터 행해질 수가 있고 그 결과가 국가기반시설에 초점이 맞추어질 경우 엄청난 피해를 야기한다는 사실에는 모두 공감하고 있고 그에 따른 준비의 필요성도 절감하고 있다. 이러한 사이버테러는 정보전(Information War)이라는 용어와 함께 유사한 의미로 불려지기도 하며 선진국 위주로 국가기반시설 보호를 위해 널리 연구되고 있는 분야이다. 우리나라의 경우 아직 사이버테러라는 용어가 법령에 사용된 예는 찾아보기 어려우나, "국가대테러활동지침(대통령훈령 제4호)" 제2조 제1호 마항 에는 '컴퓨터 통신망을 이용한 정보조작 및 전산망 파괴'를 테러 유형의 하나로 규정하고 있다(남길현, 2002: 163에서 재인용).

사이버 범죄는 사이버 공간을 대상으로 하거나 그것을 매개로 하여 나타나는 다양한 일탈적 행위 중에서도 공식적인 법규범을 어기는 행위이다. 이러한 사이버 범죄는 인터넷을 도구로 이루어지거나 대상으로 하여 발생하는 범죄로서 공식적 법규범을 어기고 사이버공간의 안전과 질서에 직접적으로 피해를 끼치는 각종 범죄를 포함하는 것으로 볼 수 있다(조동기, 2006: 84). 그러나 이러한 사이버 범죄라는 용어는 법률용어나 학술용어가 아닌 실무용어이다. 또한 용어 자체가 불확정적 성격을 지니기 때문에 사이버 범죄의 발생건수를 별도로 집계한 자료는 존재하지 않는다. 더구나 사이버 범죄는 암수율이 매우 높기 때문에, 통계가 있더라도 신뢰성을 인정하기 어려운 경우가 많다. 또한 수사기관마다 사이버 범죄 또는 컴퓨터 관련 범죄의 유형을 각자의 기준에 의하여 임의로 구분하고 있어 사이버 범죄의 유형별 현황을 파악하는 것은 매우 어렵다. 실제로 검찰은 적용법조를 기준으로 분류를 하고 경찰은 범행수법을 기준으로 사이버 범죄의 유형을 분류하고 있다.

경찰청은 사이버 테러로서 해킹과 바이러스를 그 행위 유형으로 제시하고 있고, 기타 사이버 공간에서의 범죄를 일반사이버범죄로서 구분하고 있다. 대검찰청에서는 첨단범죄수사과를 운영하고 있는데, 그 담당 직무로서 ⅰ) 산업기술 유출범죄 수사, ⅱ) 컴퓨터 및 인터넷관련 범죄 수사, ⅲ) 기업비리 및 회계부정 분석, ⅳ) 범죄수익 환수, ⅴ) 불법자금 추적, ⅵ) FIU이첩정보 분석, ⅶ) 첨단범죄 수사 전문 아카데미 운영 등에 관한 일을 하고 있다. 이 중에서 본 연구와 관련된 ⅱ) 컴퓨터 및 인터넷 범죄 수사와 관련하여서는 공용전자기록손상등, 전자문서관련죄, 전산업무방해, 전자기록비밀침해, 컴퓨터 사용사기, 전자기록손괴, 정보통신망법위반행위, 개인정보보호법 위반행위, 기타 특별법 위반행위 등으로 적용법조를 기준으로 하여 사이버 공간에서의 불법행위 유형을 구분하고 있다. 또한 국가정보원은 국가사이버 안전센터를 운영하면서, 국가 사이버 안전정책 총괄업무, 사이버안전 예방활동, 국가 사이버위협정보 종합수집, 분석, 전파 업무, 침해사고 긴급 대응 조사 및 복구 활동, 국내외 사이버 위협정보 공유 및 공조 업무 등을 하고 있다. 경찰, 검찰, 국가 정보원 등 직접적인 사이버 공간에서의

해외출장을 위해 김포공항에 도착하여 달걀세례를 받은 사건 역시 '테러'로서 표현되기도 하였다. 그러나 이러한 사례들에서의 가해자의 행위책임은 일반적으로 형법에서의 폭행죄에 해당된다. 형법에서는 폭행죄의 폭행에 대하여 타인에게 유·무형의 폭력을 행사하는 것을 그 객관적 구성요건으로 하고 있다.

질서유지 활동을 하는 부서들의 업무를 보면 경찰을 제외하고는 직접적으로 사이버 테러라는 용어를 사용하고 있지는 않다. 다만 국가정보원 홈페이지에 신고 관련 메뉴를 보면, 사이버테러 유형으로 경유지악용, 자료훼손 및 유출, 단순침입 시도, 윔바이러스 피해, 홈페이지 변조, 홈페이지 접속불가, 악성코드 채증 등으로 구분하고 있을 뿐이다. 사이버 공간에서의 불법행위에 대하여 각 국가기관들이 이에 대한 대응의 필요성은 모두 인식하고 있으나 그 행위 유형에 대한 의견은 일치하고 있지 않은 것으로 보인다.

그러나 사이버 테러와 사이버 범죄의 개념에는 상당히 공통적인 부분들이 존재한다. 일반적으로 사이버 범죄는 사이버 공간상에서 발생할 수 있는 불법행위 유형을 포괄적으로 지칭하는 표현이다. 또한 사이버 테러의 개념도 사이버 공간을 이용하여 이루어지는 불법행위 유형을 표현하는 개념이다. 실제 사이버 공간에서 발생한 불법행위에 대한 규제는 법규를 중심으로 이루어지기 때문에 실무상이나 학계에서 논의하고 있는 행위유형에는 차이가 있을 수 밖에 없고 여기에서 사이버 테러와 사이버 범죄와의 구별의 혼란이 생기게 되는 원인이 될 수도 있다. 따라서 다음에서는 사이버테러라는 표현을 직접적으로 사용하여 부서를 운영하고 있는 경찰청의 구분에 따라 사이버 공간에서의 불법행위를 검토하여 사이버테러의 범주에 대한 부분을 다시 한 번 검토해 보도록 한다.

2) 사이버테러와 사이버범죄의 유형

경찰청에서 운영하는 사이버테러대응센타에서는 가상공간에서의 불법행위 유형 즉, 사이버범죄를 크게 사이버테러형과 일반형으로 구분하고 있다. 사이버테러형은 해킹과 바이러스를 이용한 다양한 침해 유형으로 구분하고 있으며, 일반형은 사기, 불법복제, 불법·유해사이트, 사이버명예훼손, 개인정보침해, 사이버스토킹 등으로 구분하고 있다. 이러한 구분은 전통적인 불법행위 유형이 사이버 공간을 매개로 하는 것과 그렇지 않은 것을 기준으로 구분한 것으로 보인다. 사이버 테러형은 전통적인 불법행위 유형을 바탕으로 한 것이 아니라 컴퓨터 관련 기술 자체를 오용하여 사이버 공간을 매개로 한 전통적인 행위유형보다는 좀 더 큰 침해가능성이 많은 유형을 사이버테러형으로 구분하고 있는 듯하다. 여하튼 사이버 공간에서의 불법행위에 대한 현행법상 규제가능성을 검토하기 위하여는 사이버테러이든 사이버범죄이든 간에 각각의 행위유형의 한계를 명확하게 검토하는 것이 필요하기 때문에 간단히 각각의 행위유형을 살펴보도록 한다.

(1) 사이버테러형 사이버범죄

① 해킹(Hacking)

해킹은 일반적으로 다른 사람의 컴퓨터 시스템에 무단 침입하여 정보를 빼내거나 프로그램을 파괴하는 전자적 침해행위를 의미한다. 해킹은 사용하는 기술과 방법 및 침해의 정도에 따라서 다양하게 구분된다. 경찰청 사이버테러대응센터에서는 해킹에 사용된 기술과 방법, 침해의 정도에 따라서 단순침입, 사용자도용, 파일 등 삭제 변경, 자료유출, 폭탄스팸메일, 서비스거부공격 등으로 구분하고 있다.

가. 단순침입

단순침입은 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입 하는 것을 의미하는 것으로 행위자가 해당 정보통신망의 자원을 사용하기 위해서 거쳐야 하는 인증절차를 거치지 않거나 비정상적인 방법을 사용해 해당 정보통신망의 접근권한을 획득하는 것을 말한다. 즉 정보통신망의 자원을 임의대로 사용할 수 있는 상태가 되었을 때 침입이 이루어진 것이라고 할 수 있다.

나. 사용자 도용

사용자 도용은 정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의 없이 사용하는 유형을 말한다. 개념상으로만 보면 단순침입의 한 가지 유형에 해당하지만 사용자 도용이 차지하는 부분이 많아 별도로 구분하고 있다.

다. 파일 등의 삭제와 자료유출

파일 등의 삭제와 자료유출은 정보통신망에 침입한 자가 행한 2차적 행위의 결과로, 일반적으로 정보통신망에 대한 침입행위가 이루어진 뒤에야 가능한 행위유형이

다.

라. 폭탄메일

폭탄메일은 메일서버가 감당할 수 있는 한계를 넘는 많은 양의 메일을 일시에 보내 장애가 발생하게 하거나 메일내부에 메일 수신자의 컴퓨터에 과부하를 일으킬 수 있는 실행코드 등을 넣어 보내는 행위유형을 의미한다. 정보통신망에 일정한 시간 동안 대량의 데이터를 전송시키거나 처리하게 하여 과부하를 야기시켜 정상적인 서비스가 불가능한 상태를 만드는 일체의 행위인 서비스거부공격(DOS)의 한 유형이다.

마. 스팸메일

상업적인 내용의 메일을 불특정 다수에게 보내는 것. 이메일이 광고의 주요한 수단으로 부상하면서 이메일을 이용한 상업적인 목적의 광고가 많이 늘어나고 있으며 특히 기업광고, 특정인 비방, 음란물 및 성인사이트 광고, 컴퓨터 바이러스 등을 담은 이메일을 대량으로 발송하여 사회적인 문제를 일으키고 있다.

② 바이러스

바이러스(악성프로그램)는 일반적으로 컴퓨터 바이러스 또는 인터넷 웜을 의미하며 '정보시스템의 정상적인 작동을 방해하기 위하여 고의로 제작 유포되는 모든 실행 가능한 컴퓨터 프로그램'이다. 보통 자기복제능력 등 각자의 특징에 따라 컴퓨터 바이러스, 인터넷웜, 트로이목마 등으로 구분하고 있으며 법에서 '정보통신시스템, 데이터 또는 프로그램 등을 훼손, 멸실, 변경, 위조 또는 그 운용을 방해할 수 있는 프로그램'을 악성프로그램으로 규정하고 이를 유포하는 행위 처벌하고 있다.

가. 트로이목마

프로그램에 미리 입력된 기능을 능동적으로 수행하여 시스템 외부의 해커에게 정보를 유출하거나 원격제어 기능 수행. 트로이목마처럼 유용한 유틸리티로 위장하여 확산되기 때문에 감염사실 알아채기 어려운 경우가 많다.

나. 인터넷웜

시스템 과부하를 목적으로 이메일의 첨부파일 등 인터넷 이용하여 확산됨. 확산시 정상적인 파일이 이메일에 첨부되기도 하기 때문에 개인정보 유출의 위험이 내포되어 있다.

다. 스파이웨어

공개프로그램, 쉐어웨어, 평가판 등의 무료 프로그램에 탑재되어 정보를 유출시키는 기능이 있는 모든 종류의 프로그램을 의미하고, 최근에는 스파이웨어를 이용한 사기범죄 유형도 나타나고 있다.

(2) 일반형 사이버범죄

① 전자상거래 사기

전자상거래 사기는 인터넷을 통하여 물건을 사고 파는 과정에서 발생하는 것으로 인터넷의 보급이 확대됨에 따라 그 규모는 날로 팽창하고 있다. 인터넷 화면을 보며 마우스 클릭만으로 주문에서 결제, 배송까지 확인 할 수 있다는 편리성 때문에 온라인쇼핑몰 이용자들이 급증하는 추세지만, 통상 '先결제'라는 인터넷 거래의 특성을 악용하여 인터넷 쇼핑 사이트를 그럴듯하게 만들어 놓고 유명한 상품을 시중 가격에 비해 싸게 판매하는 것처럼 광고 한 후 고객으로부터 선불금을 받은 뒤 잠적해버리거나, 상대방이 확인하기가 힘들다는 점을 악용하여 물건을 가지고 있지 않거나 팔 생각이 없으면서도 거래를 하기로 한 후 돈만 받고 연락을 끊어버리는 등의 수법을 이용한 사기 사건이 급증하고 있다.

② 게임사기

게임사기는 인터넷 게임인구가 늘어나고 게임시장이 점점 확대됨에 따라 게임사이트에서 실제 돈으로 게임머니를 충전해 주거나 사이버 상에서 통용되는 게임머니나 게임아이템 등이 게임매니아 사이에서 실물처럼 거래되고 있는 실정으로, 게임머니나 아이템을 거래하기로 하는 과정에서 사기피해가 발생하고 있다

③ 불법복제

불법복제는 저작권법 및 컴퓨터프로그램보호법상의 창작물에 대한 저작권을 침해하는 행위이다. 인터넷의

발달로 불법복제가 쉬워지면서 과거 불법복제되어 오프라인에서 거래되던 컴퓨터프로그램·영화·음반CD들이 최근에는 인터넷을 통해 파일 형태로 유포되거나 인터넷을 매개로 판매되는 등, 불법복제물의 유포 및 판매가 사이버범죄의 한 형태로 나타나고 있다. 특히 최근에는 자신의 컴퓨터에 관련 프로그램만 설치하면 동일한 프로그램을 사용하는 다른 사람의 컴퓨터에 보관되어 있는 자료를 공유할 수 있는 P2P(peer to peer) 방식의 인터넷 자료공유 서비스가 확산되면서 자료공유를 원하는 네티즌들 사이에 범죄의식 없이 불법복제된 컴퓨터 프로그램이나 영화 및 음반들이 유포되고 있다.

④ 불법·유해사이트

불법·유해사이트는 공공의 안녕·질서 또는 미풍양속을 해하는 등 반사회적 내용을 담고 있는 사이트로 개설 목적 자체가 법률에 위반되거나 범죄수단으로 사용되는 위법사이트를 포함한다. 접근의 제한이나 이용의 제약이 없는 인터넷을 이용하여 각종 불법행위에 대한 정보교환 등이 이루어지고 있으며 특히 자살사이트나 마약거래를 위한 사이트는 물론이고 최근에는 청부살인이나 폭력을 의뢰하는 심부름센터 사이트까지 생겨나 인터넷으로 정보를 주고받음으로써 오프라인 범죄의 모태가 되기도 한다.

⑤ 사이버 명예훼손

사이버 명예훼손이란 인터넷 게시판에 타인의 명예를 훼손하는 글·사진 등을 게시하거나 전자우편 등을 통해 유포하는 것을 말한다. 불특정 다수인의 무제한 접근이 가능한 인터넷의 특성상 인터넷 게시판 등에 해당 내용이 일단 게재되면 시간이나 공간의 제한 없이 단시간내에 급속도로 유포될 수 있기 때문에 그로 인한 피해가 심각하다. 이러한 이유로 정보통신망이용촉진및정보보호등에관한법률에서는 사이버 명예훼손죄를 일반 명예훼손죄보다 더 무겁게 처벌하도록 규정하고 있다.

⑥ 개인정보침해

쇼핑, 오락, 교육, 행정, 금융업무 등 생활 전반이 온라인을 통해 이루어짐에 따라 온라인에서 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 다른 범죄에 사용될 수 있다는 것에 있으며 이러한 개인정보는 범죄의 표적이 되고 있다. 개인정보는 재화로서의 가치를 갖고 유통되기도 하기 때문에 법에서는 정보통신서비스제공자가 이용자의 동의없이 개인정보를 수집하는 경우나 개인정보를 취급하거나 취급하였던 자가 개인정보를 타인에게 누설하거나 제공하는 경우 등과 같은 조직적인 개인정보침해행위도 규제하고 있다.

⑦ 사이버스토킹

사이버스토킹이란 인터넷 게시판, 대화방, E-mail 등 정보통신망을 통하여 상대방이 원하지 않는 접속을 지속적으로 시도하거나 욕설, 협박 내용을 담고 있는 메일 송신 행위를 지속하는 것을 말한다. 우리나라에서는 현재까지 사이버스토킹을 구체적으로 범죄로 규정하지 않고 사이버 성폭력의 한 사례로 분류하고 있으나 외국에서는 사이버 스토킹을 독립된 하나의 범죄로 중요하게 취급하고 있으며 우리나라도 스토킹에 대한 입법이 요구되고 있다.

III. 사이버테러 규제 동향

1. 국제법상 사이버테러 규제 동향

사이버 범죄는 대체로 각국의 국내법상 처벌이 가능한 국내범죄이지만, 해킹, 바이러스 유포 등의 경우에는 그 법률의 적용에 한계를 가질 수 밖에 없기 때문에 그 불법행위 유형은 '국제성'을 띨 수 밖에 없게 된다. 따라서 사이버 공간에서의 불법행위의 효과적 해결과 형사처벌을 위해서는 각국의 합의에 의한 공동대처가 필수적이다. 그럼에도 불구하고 현재까지 사이버 공간에서의 불법행위에 대한 효과적 대응이 제대로 이루어지고 있지 않는 이유는 각국이 사이버범죄를 국내법상의 실체적 범죄 또는 불법행위로 규율하고 있을 뿐, 이에 대한 효과적 수사, 압수, 수색, 기소, 판결 등의 형사절차를 위한 국제조약이나 메카니즘을 형성하고 있지 않기 때문이다.

그러나 사이버 공간에서의 국제적 불법행위문제를 해결하기 위하여 마련된 사이버범죄방지조약은 2001년 6

월 22일 유럽이사회 제50차 형사문제위원회에서 최종안을 작성하고 2001년 11월 8일 각료위원회의 승인을 받아 2001년 11월 23일 헝가리 부다페스트에서 가입절차가 개시되었는데, 이 조약은 사이버 공간에서의 불법행위를 처벌할 수 있는 최초의 국제조약으로서 다양한 국제공조절차를 명시하고 있다.

사이버범죄방지조약은 사이버 공간에서의 불법행위 유형을 첫째, 컴퓨터데이터와 시스템의 기밀성, 무결성 및 유용성에 대한 범죄(Offences against the confidentiality, itegrity and availability of computer data and systems), 둘째, 컴퓨터 관련 범죄(Computer-related offences), 셋째, 컨텐츠관련 범죄(Content-related offences), 넷째 저작권 및 저작인접권 침해에 관한 범죄(Offences related to infringements of Copyright and related rights) 등 네 가지로 구분하고 동 범죄에 가담한 종범의 책임과 처벌에 대하여 규정하고 있다.

1) 주요내용

(1) 컴퓨터 데이터와 시스템의 기밀성, 무결성 및 유용성에 대한 불법행위

사이버범죄방지조약은 컴퓨터 데이터와 시스템의 기밀성, 무결성 및 오용성에 대한 불법행위를 불법접속, 불법감청, 데이터손괴, 시스템손괴, 장치의 오용 등 다섯 가지 유형으로 분류하고, 이를 국내법상의 형사법에 규정하여 범죄로서 처벌하고 이에 수반되는 조치를 취하도록 요구하고 있다. 이 부분은 본 연구에서 논의하고 있는 사이버테러의 규제 가능성과 관련하여 사이버테러라는 내용과 가장 일치하는 부분으로서 우리나라에서는 이와 관련된 규제 규정을 다음 항에서 후술할 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률, 화물유통촉진법 등에서 찾아볼 수 있다.

(2) 컴퓨터 관련 범죄

사이버범죄방지조약은 컴퓨터와 관련된 범죄를 컴퓨터 데이터의 위조와 컴퓨터 데이터 및 시스템상의 불법행위를 통한 사기 등 두 종류로 구분하고 있다. 컴퓨터 데이터의 진정성에 흠결이 있는 데이터를 마치 진정한 것처럼 합법적으로 인식되도록 하거나 행사할 목적으로 권한 없이 고의적으로 컴퓨터데이터를 입력, 변경, 삭제 또는 은폐하는 행위를 '컴퓨터 관련 위조' 범죄로서 국내법으로 규율할 것을 요구하고 있다.

(3) 컨텐츠 관련 범죄

사이버범죄방지조약은 컨텐츠 관련 범죄를 아동포르노 범죄에 한정하고 있다. 컴퓨터 시스템을 통하여 아동포르노를 배포할 목적으로 제작하는 행위, 컴퓨터 시스템을 통하여 아동포르노를 전송 또는 배포하는 행위, 본인 또는 타인의 컴퓨터 시스템을 통하여 아동포르노를 획득하는 행위 등을 규율하는 것을 내용으로 하고 있다.

(4) 저작권 및 저작인접권 침해에 관한 범죄

사이버범죄방지조약은 컴퓨터 시스템을 이용하여 저작권 및 저작인접권을 침해하는 것을 범죄로 하고 있다. 저작권과 관련된 각종 국제조약에 따라 악의로 상업적 목적으로 컴퓨터 시스템을 이용하여 저작권을 침해하는 행위를 국내법상의 범죄로 규정하여 처벌할 의무로 부과하고 있다.

2) 절차규정

국제법상 사이버 공간에서의 각종 범죄행위를 규율하기 위하여 당사국들은 다음과 같은 내용을 따를 것을 의무화하고 있다.

첫째, 저장된 컴퓨터 데이터의 신속한 보존을 위하여 컴퓨터 데이터가 손괴 또는 변경될 수 있다고 믿을만한 근거가 있는 경우 각 당사국은 전송데이터를 포함하여 컴퓨터 시스템 내에 저장된 컴퓨터 데이터의 신속한 보존을 법집행기관이 명령 또는 요청할 수 있도록 하는 절차적 규정을 입법하도록 요구하고 있다.

둘째, 저장된 컴퓨터 데이터의 수색과 압수에 관하여 동 조약은 자국의 영역내에 있는 컴퓨터 시스템 및 컴퓨터 내에 저장되어 있는 컴퓨터 데이터와 컴퓨터 데이터가 저장되어 있는 저장매체를 법집행기관이 수색 또는 접속할 수 있도록 필요한 입법을 할 것을 요구하고 있다.

셋째, 자국의 법집행기관이 당사국의 영역내에서 전송되는 특정 통신과 관련되는 전송데이터를 실시간으로 기록 또는 수집하고, 현존하는 기술력 내에서 서비스 제공자가 전송데이터를 실시간으로 기록, 수집하는 것을

지원 및 협조할 수 있는 필요한 입법을 요구하고 있다.

넷째, 사이버범죄와 관련된 관할권과 관련하여 해당 범죄가 당사국 영토, 자국기를 게양한 선박 위, 당사국의 법에 따라 등록한 항공기내에서 발생한 경우 당사국이 관할권을 행사하도록 하고 있다. 또한 범죄행위지의 형법에 따라 처벌이 가능하거나 어떤 국가의 영토 관할권 밖에서 동 범죄가 행해진 경우라 할지라도 자국민이 범죄를 저지른 때에는 해당 범죄의 관할권을 행사하는데 필요한 입법조치를 할 것을 의무화 하고 있다. 즉, 사이버범죄방지조약은 속지주의에 관한 상세한 관할권 규정을 명시하고 보충적으로 속인주의를 적용할 수 있도록 하고 있다.

2. 국내법상 사이버테러 규제 동향

1) 해킹행위의 규제

국내법상 해킹행위를 규제하는 법적 근거로는 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한 법률, 화물유통촉진법 등을 들 수 있다.

정보통신기반보호법 제28조(벌칙)에서는 제12조(주요정보통신기반시설 침해행위 등의 금지)에서 금지하고 있는 행위 즉, 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위를 하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 하고 있으며, 미수범 처벌규정 또한 마련하고 있다.

정보통신망이용촉진및정보보호등에관한법률 제63조(벌칙)에서는 제48조(정보통신망 침해행위 금지) 제1항의 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 아니된다는 규정에 위반하여 정보통신망에 침입한 자에 대하여는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 하고 있다.

또한 화물유통촉진법 제54조의4(벌칙)에서는 제48조의7(전자문서 및 물류정보의 보안)제5항의 누구든지 불법 또는 부당한 방법으로 제4항의 규정에 의한 보호조치를 침해하거나 훼손하여서는 아니된다는 규정에 위반하여 물류전산망의 보호조치를 침해하거나 훼손한 자는 3년 이하의 징역 또는 3천만원이하의 벌금에 처하도록 하고 있다.

2) 바이러스 유포행위의 규제

국내법상 사이버테러의 한 유형으로 볼 수 있는 바이러스 유포행위를 규제하고 있는 법적근거로는 정보통신기반보호법을 들 수 있다.

정보통신기반보호법 제28조(벌칙)에서는 제12조(주요정보통신기반시설 침해행위 등의 금지)의 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위를 하여서는 아니된다는 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 하고 있으며 미수범 처벌규정도 마련하고 있다.

3) 인터넷 사기

사이버 공간에서의 사기행위를 규제하고 있는 국내법상 근거로는 일반적으로 형법을 적용하고 있다.

형법 제347조(사기)에서는 사람을 기망하거나 제3자로 하여금 재물의 교부를 받거나 재산상의 이익을 취득한 경우에는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 규정하고 있다. 또한 형법 제347조의2(컴퓨터등 사용사기)에서는 컴퓨터 등 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 처하도록 하고 있으며 미수범 처벌규정도 마련하고 있다.

4) 불법복제

사이버 공간에서의 불법복제 행위를 규제하고 있는 국내법상 근거로는 저작권법, 컴퓨터프로그램보호법, 온라인디지털콘텐츠산업발전법 등을 들 수 있다.

저작권법에서는 제97조의5, 제98조 등에서 불법복제 행위를 규제하고 있으며, 컴퓨터프로그램보호법 제46조(벌칙)에서는 제29조(프로그램저작권 침해행위 등), 제30조 (기술적 보호조치의 침해 등의 금지)에서 규제하고 있는 행위를 위반하였을 경우에 각각 처벌규정을 두고

있다. 또한 온라인디지털콘텐츠산업발전법 제22조(온라인콘텐츠의 복제 등의 죄)에서는 제18조(금지행위 등)에서 규정하고 있는 디지털콘텐츠에 적용한 기술보호조치의 회피・제거 또는 변경하는 행위 등을 규제하고 있다.

5) 명예훼손

사이버 공간에서의 명예훼손 행위를 규제하고 있는 국내법상의 근거로는 정보통신망이용촉진및정보보호등에관한법률을 들 수 있다. 동 법 제61조(벌칙)에서는 형법상의 명예훼손 행위를 정보통신망을 통하여 하였을 경우에 규제하는 내용을 명시하고 있다.

6) 개인정보유출

사이버 공간에서의 개인정보유출과 관련된 행위를 규제하고 있는 내용 역시 정보통신망이용촉진및정보보호등에관한법률에서 찾아볼 수 있다. 동 법에서는 개인정보침해행위 관련 규제유형을 다음과 같은 것들을 제시하고 있다. 이용자의 동의 없이 개인정보 수집, 개인정보 수집시 기본사항 미고지 및 이용약관 등에 명시하지 않은 경우, 서비스 제공에 불필요한 개인정보 요구, 제공받은 목적 이외로 개인정보 사용, 이용자의 동의 없이 제3자에게 개인정보 제공, 개인정보 관리책임자 미지정, 개인정보 취급자가 개인정보 유출, 이용자의 개인정보 열람요구에 불응, 오류정정・삭제요구에 불응, 오류정정 요구 접수한 후에도 정정되지 않은 정보 이용, 타인의 개인정보를 훼손하거나 비밀을 침해・도용・누설, 수신자가 원하지 않는 영리목적의 광고성 정보 전송(스팸메일 발송 포함) 등을 그 내용으로 하고 있다.

3. 사이버공간과 재판관할권

전술한 바와 같이, 사이버 테러리즘과 사이버 범죄행위의 각각의 행위태양이 아직은 명확하게 구분되어 있지 못하다. 해킹, 바이러스 유포 등의 행위를 통한 불법적 행위가 단순한 일반 범죄보다는 좀 더 큰 유무형의 결과를 가져온 경우 등에야 사이버 범죄라기보다는 좀 더 불법적인 내용이 큰 사이버 테러리즘이라고 부를 수 있을 것이다. 그러나 사이버 범죄이든, 사이버테러리즘이든 정치적 목적 등을 달성하기 위한 전통적인 의미에서의 테러리즘이 반드시 아니라 하더라도 사회를 충분히 혼란에 빠트릴 수 있는 사이버 공간에서의 불법행위에 대하여는 최소한의 법률적 통제는 필요하다. 그러나 이러한 사이버 공간에서의 테러리즘은 전통적인 테러리즘과는 달리 시간적, 공간적 제약이 매우 적은 초국경적 특성을 가지고 있고, 또한 특정인 또는 불특정 다수에 대하여도 실시간으로 접속할 수 있는 동시성 등의 특성을 가지고 있기 때문에 법적인 규제에 대하여는 각국이 그 나라의 통치권에 기초하여 가지고 있는 법률적 통제권의 행사에 충돌이 발생할 수 밖에 없다.

이와 같은 문제가 발생하는 이유는 사이버 공간의 특수성으로 인하여 사이버공간에 정보를 제공하는 자는 그 정보가 가는 경로, 지역, 대상 등을 의도대로 한정할 수 없는데 반하여, 대다수의 국가들은 외국에서 인터넷을 통하여 들어오는 정보서비스와 서비스내용을 점검하여 자국에 유해성을 가질 때에는 규제하려 하고 있기 때문이다. 다시 말하면, 전통 국제법상 성립하고 인정되었던 주권, 관할권의 전제가 되는 지역, 사람, 행위간의 관계가 사이버 공간에서는 잘 들어맞지 않을 수밖에 없기 때문이다. 그러나 본 연구에서 논의하고 있는 테러리즘, 특히 사이버 테러리즘에 대하여는 그러한 행위를 규율할 필요성은 분명히 존재한다는 데에는 이견이 있을 수 없다. 문제는 그러한 행위를 '누가' 규율할 것인가 하는 점이다.

사이버 공간에서의 다양한 행위양태를 규제 또는 통제하고자 하는 국가의 의도는 외국으로부터 아무런 장애없이 유입되는 일정한 정보나 활동으로부터 자국민과 법익을 보호하고자 하는 것이지만, 결과적으로 적법하게 수행되고 있는 정보교류 등의 활동을 억압할 수도 있다. 그렇기 때문에 사이버 공간에서의 특정 행위 등을 규제하고자 하는 것을 반대하는 이들은 다음과 같은 반대이유를 들고 있다. 첫째, 국경을 초월하는 활동에 대한 국가적 규제 자체가 국제법상 특정 통치권의 범위를 넘어서는 위법한 것이며, 둘째, 국경을 초월하는 인터넷 정보제공자에 대한 법 적용을 위한 사전통지가 현실적으로 어려우며, 셋째, 타국의 통치권 등 법 적용을 위한 관할권에 대하여 부당한 간섭효과를 발생할 수 있기 때문이라고 한다.

일반적으로 국가들은 자국영역 내에 거주하는 사람들에게 관할권을 갖고, 자국 영역 내에서 발생한 사건이나 행위에 관하여 관할권을 행사한다. 이러한 관할권 행사

는 당연히 관련 국가간에 충돌의 여지를 갖게 한다. 현실적으로 영토주권을 갖고 있는 2개 이상의 국가가 서로 국적, 주소, 행위지 등을 이유로 관할권을 행사하는 것을 막을 수는 없다. 이러한 관할권의 충돌이 발행할 경우, 대부분의 경우에는 상호주의에 기초한 외교교섭, 일방적 자제 등으로 문제를 해결한다. 그 외 사전합의를 통하여 일방이 전속적 관할권 혹은 우선적 관할권을 갖는 것으로 정하기도 하고, 아니면 제3의 재판기관이 관할권을 갖도록 결정하기도 하나 이러한 부분은 물리적 공간으로 이루어진 사회를 전제로 하고 있다는 점에서, 사이버 공간상에서의 실질적 적용 가능성에 대에서는 회의적일 수 밖에 없다. 그리고 이러한 재판관할권에 대한 관심은 주로 사이버 공간에서의 전자상거래 등의 민사적인 분쟁을 다투는 내용이 주된 것들이고 본 연구에서 논의하는 사이버 공간에서의 테러리즘에 대하여는 민간차원의 분쟁해결 차원이 아니라 각국의 형벌권 행사라는 형사사법적인 측면 즉, 국가의 통제권을 어떻게 인정할 수 있는가라는 다른 차원의 것이기 때문에 위에서 살펴본 유럽의 사이버범죄방지조약과 같은 국제법상 법인인 다중 국가간의 불법적 인식을 통한 적극적 논의 또한 매우 필요할 것이다.

IV. 사이버테러 규제 가능성 논의의 한계 및 결론

이상에서 사이버 테러리즘과 관련하여 우리의 현행법상 규제가능성을 간단히 살펴보았다. 그러나 사이버 테러리즘이라는 것은 용어상으로는 테러리즘이라는 표현을 사용하고 있지만, 전통적인 테러리즘과는 그 양상 및 수법 등이 매우 다르고 그에 따른 대응방안도 다를 수 밖에 없다. 또한 사이버 공간에서 일어나게 되는 불법행위를 다루고 있지만, 사이버 범죄와 사이버 테러리즘과의 구분 또한 명확하지 않다. 외국의 해커들이 우리의 시설에 침입해 그에 따른 침해사고가 발생했을 경우, 우리의 법익이 침해되었지만, 우리의 법규정을 적용하여 그들을 의율할 수 있을지도 현실적으로 의문시 된다. 즉, 본 연구에서 논의하고 있는 사이버 테러리즘의 법률적 규제 가능성은 현실적으로 여러 가지 한계를 가지고 있을 수 밖에 없다. 이러한 한계를 구체적으로 검토하면 다음과 같다.

사이버 테러리즘의 법률적 규제 가능성의 첫 번째 한계는 전통적 테러리즘과 사이버테러리즘의 실체가 너무 다르기 때문에 그 법률적 대응에 있어서 차이가 존재할 수 밖에 없다는 것이다. 전통적 테러리즘의 규제에 있어서는 테러관련 특별법을 규정하지 않고 각각의 구체적인 행위에 대해서 형법이나 특별형법에서 규정하고 있다. 형법에서는 외국원수나 사절에 대한 폭행(제107조), 범죄단체 조직(제114조), 폭발물사용(제119조), 공무집행방해(제136조), 공용물의 파괴(제141조), 공용건조물 등에의 방화(제165조), 폭발성물건과열(제172조), 가스·전기 등 방류(제172조의2), 가스·전기 등 공급방해(제173조), 일반건조물 등에의 일수(179조), 일반교통방해(185조), 기차, 선박 등의 교통방해(186조), 음용수의 사용방해(192조), 수도음용수의 사용방해(193조), 살인(제250조), 상해(제257조), 중상해(제258조), 상해치사(제259조), 특수폭행(제261조), 폭행치사상(제262조), 체포·감금(제267조), 특수체포·특수감금(제278조), 체포·감금 등의 치사상(제281조), 특수협박(제284조), 국외이송을 위한 약취, 유인, 매매(제289조), 해상강도(제340조), 재물 또는 문서의 손괴(제366조), 공익건조물파괴(제367조), 중손괴(제368조), 특수손괴(제369조) 등의 죄를 규정하고 있는데 이러한 규정들이 전통적인 테러리즘에 적용될 수 있는 것들이다. 이러한 범죄들은 그 자체가 바로 테러리즘을 규율하기 위한 것은 아니나 테러리즘을 수행하는 과정에서 발생되는 개개의 불법행위들을 규제할 수 있는 현행법상 근거들이다.

그러나 사이버 테러에 대하여는 우선, 법률 적용을 위한 행위유형이 명확하게 규정되어 있지 않고, 행위유형이 나름대로 정형화 되어 있다 하더라도 전술한 바와 같이 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률, 화물유통촉진법 등에 의하여 규율이 가능하다는 것이 전부이다. 위에서 열거한 형법상의 불법행위들도 마찬가지이긴 하지만 개개 조문들이나 형법의 자체의 목적은 불법행위를 규율하기 위한 것들이다. 그러나 정보통신망기반보호법, 정보통신망이용촉진및정보보호등에관한법률, 화물유통촉진법 등 사이버 테러리즘에 적용가능한 법률들의 본래 제정취지는 불법행위에 대한 규율보다는 정보통신망 등을 보호하기 위한 것이 본래

취지이기 때문에 그 제적목적에 있어서 차이가 있다. 사이버 테러리즘의 수단이 되는 해킹, 바이러스 유포 등을 그 자체로 불법행위화 하여 규제하고자 하는 취지가 아니기 때문이다. 또한 정보통신망 등을 보호하기 위한 여러 법률들은 해킹, 바이러스 유포 등의 행위 자체만을 처벌하고 있다. 이는 사이버 테러리즘의 위험성에 대하여 인식하고 그에 대한 해결책을 논의하는 부분에서 그 위험한 결과를 충분히 인식하고 이에 대한 규제를 하고자 규정된 부분은 분명히 아닐 것이다. 분명히 전통적 테러리즘과 사이버 테러리즘의 성격이 다른 부분이 존재한다 하더라도 특정 행위유형 등을 불법행위로 인식하고 이에 대응하기 위한 필요성은 누구도 부인할 수 없다. 하지만 현행법상 이러한 사이버 테러리즘을 규제 또는 규율하기 위하여는 현실세계와 사이버 공간상에서 발생되는 불법행위에 대한 차이점을 인정하고, 좀 더 포괄적인 사이버 공간에서 발생가능한 불법행위를 규제할 수 있는 법률 등의 제정이 필요할 것이다.

그 다음으로, 사이버테러와 사이버범죄 행위유형 구분의 어려움이 현행법상 사이버 테러리즘을 규제하는데 있어서의 두 번째 한계이다. 전술한 바와 같이 사이버 공간에서의 불법행위에 대하여 어디까지가 테러로서 인정되어야 하고 어디까지가 일반적인 범죄행위로서 인식되어야 하는가이다. 경찰청은 해킹과 바이러스 유포 등의 행위를 사이버테러리즘으로서 분류하고 있지만 테러 또는 테러리즘이라는 표현을 사용할 수 있기 위하여는 그 행위유형 자체만이 아니라 결과적으로 중한 결과까지를 일반적으로 요구하고 있기 때문에 행위유형만으로 사이버 테러리즘이다 또는 사이버 범죄다 라고 분류하는 것은 무리한 것으로 보인다. 해킹이나 바이러스 유포 등을 통해 사이버 머니를 불법적으로 획득하거나 개인정보를 침해 또는 유출하고, 나아가 국가기관의 국가기밀까지 침해하는 등의 다양한 불법행위 유형들이 나타나고 있기 때문에 행위유형만으로 사이버 테러리즘으로 분류하는 것은 옳지 않은 것 같다. 어떤 면에서는 해킹 등을 통하여 국가기관의 국가기밀을 유출하였다 하더라도 그것 만으로는 전통적인 테러리즘과는 달리 소위 "테러 또는 테러리즘"이라 부르는 데에는 그 본래적 의미에서 차이가 있을 수 밖에 없는 한계를 인식하여야 한다. 유출한 국가기밀을 소위 정치적 목적에 사용하지 않고 금전적 이득을 위해 사용하는 경우도 쉽게 가정할 수 있기 때문이다. 우리가 언론매체 등을 통하여 쉽게 접하는 많은 사이버 공간에서의 불법행위들은 쉽게 사이버 범죄와 사이버 테러리즘으로 구분하기가 너무 애매하고 어려운 것이 대부분이다.

물론, 우리가 사이버 테러리즘이라 하여 그 행위들로 인한 침해의 중요성을 인식한다 하더라도 현행법상 사이버 공간에서의 불법행위를 규율하기 위하여는 다시 한 번 사이버 테러리즘이든 사이버 범죄이든 그 구체적인 행위와 결과 등에 관하여 좀 더 논의 할 필요가 있다. 이러한 노력 등을 통하여 사이버 공간에서의 불법행위를 정확하게 현행법에 의하여 규율하거나 다시 새로운 법률을 제정할 수 있을 것이기 때문이다.

마지막으로 사이버 공간에서의 테러리즘에 대한 재판관할권의 한계가 그 규제 가능성에 대한 한계이다. 가장 단순하게 우리 나라에서 우리 국적을 가진 해커나 외국 국적을 가진 해커라 하더라도 해킹 등 사이버 테러리즘을 자행했다 하는 경우면 우리의 법률을 적용하여 처벌하기 위한 재판관할권은 큰 문제가 아닐 것이다. 당연히 속지주의에 의하여 우리의 법률을 적용할 수 있기 때문이다. 그러나 사이버 테러리즘이라는 것은 전통적 테러리즘에 비하여 시간적, 공간적 제한을 받지 않기 때문에 속지주의를 적용하여 우리의 법률에 의하여 사이버 테러리즘을 규제할 수 있는 가능성은 매우 적다. 실무상으로 사이버 공간에서의 불법행위를 저지르는 경우들을 보면, 실력과시, 호기심 등에 의하여 해킹을 하는 경우가 거의 대부분이기 때문에 국내에서 발생하는 사이버 공간에서의 각종 침해문제는 소위 테러리즘의 성격을 가지고 있는 경우는 거의 없기 때문이다. 우리가 논의하고 있는 좀 더 무거운 성격의 사이버 테러리즘까지 가는 경우는 거의 찾아볼 수가 없다. 문제는 외국에서 외국인 해커가 우리의 시스템에 침해를 한 경우에 그 해커를 찾는다 하더라도 우리의 법률을 적용할 수 있을까의 문제이다. 이것은 비단 사이버 테러리즘과 관련되지 않는다 하더라도 전통적인 테러리즘이나 일반 국제성 범죄와 마찬가지로 범죄인인도조약, 범죄 관련 국제조약(형사사법공조조약 등), 외교 교섭 등을 통해 각종 형사문제를 해결하는 간접적인 방법에 의존할 수 밖에 없는 본질적 한계를 가지고 있으며 사이버 공간에서의 침해를 실시간으로 대응하

고 이에 따른 후속조치로서 우리의 법률을 적용할 수 있는 보다 적극적인 국제적인 공조 등이 필요하다.

<참고문헌>

▷ 곽병선. 2006. 사이버명예훼손에 관한 규제상의 문제점 및 대응방안. 법학연구. 23: 371-387.

▷ 남길현. 2002. 사이버테러와 국가안보. 국방연구. 45(1): 157-191.

▷ 신동준 외. 2006. 사이버폭력과 그 대책: 자율적 통제의 가능성을 중심으로. 사이버커뮤니케이션학보. 20: 149-195.

▷ 신의기. 2002. 테러리즘 관련법제 정비방안. 한국형사정책연구원. 연구보고서.

▷ 우제태. 2007. 사이버 범죄의 대응방안에 관한 연구. 경찰연구논집. 1: 169-193.

▷ 이건종·조현지. 1995. 각국의 테러범죄대응책에 관한 연구 - 법적규제를 중심으로. 한국형사정책연구원.

▷ 이미정 외. 2005. 사이버 공간에서의 국가안보 위협요인 및 대책방안. 국방연구. 48(2): 37-69.

▷ 이성식. 2004. 사이버공간에서의 피해자에 대한 피해인식과 사이버범죄행위. 피해자학연구. 12(2): 161-179.

▷ 이영준 외. 2001. 사이버범죄방지조약에 관한 연구. 한국형사정책연구원, 연구보고서.

▷ 이정훈. 2006. 사이버범죄에 관한 입법동향과 전망. 사이버커뮤니케이션학보. 20: 233-276.

▷ 장신. 2007. 사이버공간과 국제재판관할권. 부산대학교 법학연구 48(1): 429-453.

▷ 조동기. 2006. 사이버공간의 일탈 유형과 사회통제의 특성. 정보와 사회: 73-106.

▷ 조병인. 2000. 사이버경찰에 관한 연구 - 사이버범죄의 규제를 중심으로. 한국형사정책연구원, 연구보고서.

▷ 한국사회학회. 2004. 사이버범죄와 보안의식. 정보통신정책연구원.

▷ 허태회 외. 2005. 위기관리이론과 사이버안보 강화방안: 이론과 정책과제. 국방연구. 48(1): 29-62

趙賢彬: 동국대학교에서 경찰학 박사학위를 취득하고(논문: 청소년의 법의식이 비행에 미치는 영향에 관한 연구, 2004), 현재 극동대학교 법경찰학부 조교수로 재직 중이다. 주요 관심분야는 경찰활동 중 범죄예방, 범죄예측, 비교경찰, 경찰인권 등이며, 주요 논문으로는 "한국경찰활동의 다변화에 관한 연구(2007)", "외근경찰관의 인권보호에 관한 연구(2006)", "성폭력과 성폭력 피해자 심리의 이해(2006)", "주요국가의 공인탐정 현황과 정책적 시사점(2006)", "경찰수사과정의 인권보호에 관한 연구(2005)" 등이 있다. 주요 경력으로는 한국경찰학회 간사, 대불대학교 경찰학부 교수를 지냈고, 현재는 한국공안행정학회, 한국경찰학회, 한국민간경비학회, 한국범죄심리학회에서 상임이사 및 이사, 편집위원 등을 맡고 있다(johyunbin@korea.com).