e-테러리즘의 효율적 통제방안

Efficient countermeasures against e-terrorism

이 윤 호* · 김 대 권**

〈목 차〉

Ⅰ. 서론
Ⅱ. e-테러리즘의 정의
Ⅲ. e-테러리즘의 실태 및 문제점
Ⅳ. e-테러리즘의 효율적 통제방안
Ⅴ. 결론

〈요 약〉

e-테러리즘은 테러리스트들의 국가적인 목적달성의 수단으로 인터넷 등의 사이버공간을 활용하여 테러에 이용하는 것이다. 최근에 일어나고 있는 테러사건들도 사이버라는 공간이 전략적 도구로 이용되었다는 사실을 확인할 수 있었다.

이 연구에서는 e-테러리즘의 주체자인 테러리스트의 다양한 공격형태 그리고 사이버상의 네트워킹 등에 대한 테러의 효율적 통제방안을 모색함으로써 현대적 의미에서의 테러 방지에 대하여 논의하였다.

사이버공간이라는 특수성으로 인해 개별국가에 적용되어지는 문제가 아니라는 점을 감안한다 하더라도 현재 나타나고 있는 국내의 해킹사고 급증, 특히 외국 해커의 경유지로서의 한국이 이용된다는점 그리고 이러한 상황임에도 불구하고, 외국에 비해 전문 보안인력이나 기반시설이 선진외국에 비해 부족하다는 점을 문제점으로 제시 할 수 있었다. 이에대한 대안으로 e-테러리즘에 대응할 수 있는 사이버 정보군 등의 인력양성과 예산확보, e-테러리즘에 대응체계를 종합화·체계화하기위한 네트워크 관리, 사이버 공격현황의 정보수집 및 분석 강화를 제시하였다.

주제어 : e-테러리즘, 사이버 테러리즘, 사이버테러, 사이버네트워킹, Netwar

* 동국대학교 경찰행정학과 교수(제1저자).
** 동국대학교 경찰행정학과 강사(교신저자).

I. 서 론

인터넷과 컴퓨터의 발달로 사회전반의 활동이 사이버상에서의 활동과 연계되어 이루어지고 있는것이 오늘날의 사회현상이다. 이러한 사이버세계에의 중요성이 확대되어감에 따라 사이버테러는 초기의 호기심과 자기과시의 개인적인 부분을 넘어서 특정한 목적을 이루고자 하는 국가적인 목적달성의 수단으로 확대되어지고 있다. 이러한 수단으로써의 사이버활동은 전 세계적인 테러의 확산에도 커다란 영향력을 형성함으로써 최근에는 전쟁의 도구로 이용되는 상황에 놓이게 되었다.

특히 정보화 사회에서 사이버해커는 테러리스트(Computer Terrorists)라고 얘기할 정도로 그 범죄적인 성향이 강화되고 있다. 현재는 단순해커(Recreational Hacker)와 범죄적 해커로 구분하고 있는데, 범죄적 해커의 경우 기업정보, 군사정보, 국가 기밀 정보를 수집하는 등 매우 위험하게 발전되고 있다(백광훈, 2001: 32).

국내·외적으로 중요정보와 의사소통을 컴퓨터와 인터넷에 의존하는 현상이 보편화 됨에 따라 테러리스트나 정보기관, 산업보안 등의 위협이 증대되고 있는 현실에서 고도의 기술로 무장한 해커나 사이버테러리스트 들은 중요 정보기반구조에 대한 공격을 꾸준히 시도하고 있다.

흔히 e-테러리즘으로 볼 수 있는 사이버테러리즘은 첨단 정보통신기술을 이용해 물리적 세계가 가상의 세계로 전환되어 있는 공간을 무차별적으로 공격하는 행위를 지칭한다. 즉 현실에서 자행되는 테러리즘을 사이버 공간으로 옮겨놓은 형태이다(이진수, 2000: 6-7).

그러나 요즘은 사이버 테러리즘이란 말이 인터넷상에서 특정인에 대한 유언비어 날조나 동영상 등을 이용한 허위 사실 유포 또는 개인의 사생활 침해로 인한 모독 등에도 쓰이고 있다. 이러한 사적인 침해 부분은 사이버 윤리를 어기는 사이버 범죄에 해당 될 뿐 명확히 말해서 어떠한 단체나 국가를 공격하고 시위하는 사이버 테러리즘에 해당되지는 않는다고 본다.

따라서 이 논문에서는 사이버테러리즘을 다수의 단체나 국가를 공격하는 행위, 그것이 물리적 공간에서 가상공간으로 전환되는 부분 또는 전환되어있는 부분에서 이루어진 범위에서 다루고자 하며, 또한 이러한 사이버테러리즘을 포함한 e-테러리즘의 개념을 보다 명확히 정의 내리고 e-테러리즘의 주체자인 테러리스트의 다양한 공격형태 그리고 사이버상의 네트워킹 등을 통한 현실에서의 피해 등에 대한 효율적인 통제방안을 모색하고자 한다.

Ⅱ. e-테러리즘의 정의

1. e-테러리즘의 개념과 전략

인터넷은 사이버상의 공간이라는 특이성으로 인하여, 테러집단의 이상적인 활동무대가 되어오고 있다. 이러한 인터넷과 테러리즘의 긴밀한 관계는 'e-terroorism'이란 용어를 만들어 냈다. 그리고 인터넷은 현실세계에서의 테러와 연관되어 테러리스트들의 목적 달성을 용이하게 하는 도구로 사용되고 있다.

주수기(2006)의 연구에 따르면 e-테러리즘을 인터넷을 이용한 모든 테러리즘의 개념으로 기존의 사이버테러리즘이나 사이버 네트워킹 등을 포함한 포괄적인 의미에서의 인터넷 테러리즘으로 정의하였고, 이러한 테러리스트들의 인터넷 사용 전략을 심리전, 선전·홍보, 테러요원 충원, 재정조달, 정보수집과 교환, 의사소통과 테러 네트워크 관리 등의 여섯가지 측면으로 나누어 정의하고 있다.

먼저 심리전은 테러리즘에 있어서 심리적인 교전상태를 전개하는 선택된 도구로 활용된다는 것이다. 이러한 심리전은 테러리스트들의 이미지를 확대하고 대치세력을 위축시키는 등의 심리적인 압박으로 테러의 공포를 제공하나 이를 제지하기가 쉽지 않은것이 문제이다.

둘째, 테러에 있어서 인터넷을 선전과 홍보에 이용한다. 특히 테러리스트들은 자신의 행위를 변명하고 정당화하는 수단으로 인터넷의 가상공간을 이용하고 있다.

셋째, 인터넷을 통한 지지세력의 규합과 테러요원을 충원하고 교육한다. 이외에도 인터넷을 이용하여 재정적인 후원과 정보를 수집하고 교환하는 등의 총체적인 테러활동이 현재는 모두 인터넷을 통하여 이루어지고 있다고해도 과언이 아닐것이며, 이를 e-테러리즘이라고 개념 지을 수 있을 것이다.

2. 사이버 테러리즘과의 비교

테러리즘의 본질에는 변화가 없으나 테러리즘의 유형은 시대에 따라 끊임없이 변화하고 있다. 테러를 자행하는 동기가 변하고 있는것처럼, 테러리즘의 수단이나 수법도 과거에는 없었던 새로운 형태가 인류를 위협하고 있다. 그러나 과거의 정보체계, 전술, 보안절차 등은 새로운 위협에는 거의 무용지물이다. 뿐만 아니라, 과거의 테러리즘에 대항하여 인류의 평화와 인권을 보호하던 대 테러리스트 특공대도 이 새로운 유형의 테러리즘에는 아무런 효과를 거두지 못한다(이윤호, 2008: 344).

사이버 테러리즘은 "국가대테러활동지침(대통령훈령 제47호) 제2조제1항 마항에 '컴퓨터

통신망을 이용한 정보조작 및 전산망 파괴'를 테러리즘 유형의 하나로 규정하고 있다. 이는 정보화사회 도래와 함께 국가·사회의 주요기반시설이 정보통신기반에 의한 의존도가 심화되면서 사이버공간에서 행해지는 전산망 파괴가 물리적인 테러리즘 못지않게 우리사회를 혼란에 빠뜨릴 수 있기 때문이다. 근래에 와서는 사이버테러리즘은 국가안보 및 국가경제 보호 차원에서 새롭고 중요한 분야로 인식되고 있다(이진수, 2000: 7).

일반적인 사이버 테러리즘의 특징으로는 첫째, 전통적인 테러리스트들의 방식보다 익명성을 가지고 있다. 사이버공격의 신원을 확인하는 것은 매우 어려운 일이나 테러리스트들에게는 발각되거나 체포될 위험이 제한적이다(김정태·이현우, 2003: 783).

둘째, 기존의 테러리즘 방법에 비해 비용이 적게 든다(Adam Salvino, 2003). 일반적으로 풍부한 자금을 확보하기 어려운 테러리스트들에게 많은 비용이 드는 폭탄이나 생화학 무기 등 장비를 마련하지 않아도 되고, 공간 이동을 위한 비용, 교육 등에 소요되는 비용이 상대적으로 저렴하다고 할 수 있다.

셋째, 컴퓨터에 의해 제어되는 정보통신기반시설 모두를 대상으로 한다. 목표시스템이 다수 존재한다는 것이다. 국가의 주요 기반시설로 전력, 가스, 수도의 공급시설, 통신망, 육해공로의 교통시설 등이 있으며 이러한 모든 주요 시설이 사이버 테러리즘의 대상이 될 수 있다. 이러한 대상들은 국가 주요 기반시설에 피해가 발생할 시 국가기능 자체가 마비될 수도 있는 심각한 사태가 발생될 수도 있을 것이다.

넷째, 지역적·공간적 및 정치적인 경계가 존재하지 않고 시간과 공간을 초월하여 동시다발적으로 공격이 가능하다는 것이다. 현실 세계에서는 지리적, 공간적 차이로 인해 전세계 동시다발적인 공격이 사실상 불가능하나, 인터넷으로 연결된 사이버 공간에서는 시간적·공간적 제약없이 동시다발적인 공격이 가능하나 이러한 공격의 예측은 더 어렵다는 것이다(윤영성, 2005: 19).

2. e-테러리즘 공격형태

1) e-테러리즘의 위협요인

주요기반시설은 물리적으로나 사이버 상에서 위협을 받을 수 있다. 개인이나 조직이 사이버 공격을 할 수 있는데, 컴퓨터와 네트워크의 의존도가 높아지면서 사이버 공격으로 위해를 가할 수 있는 조직과 개인의 수가 늘어나고 있다(국가사이버안전센터 2004: 21).

e-테러리즘의 위협요인을 살펴보면 범죄집단, 해커, 핵티비스트, 내부자, 정보기관, 테러리스트, 바이러스 작성자등의 유형별로 위협내용이 다르게 나타날 수 있다. 그러나 이러한 다양한목적과 동기로인한 위험은 대상자에게 커다란 공포로 다가올 수 있을 것이다.

〈표 1〉 e-테러리즘의 위협요인

위협유형	위협내용
범죄집단	- 국제 산업 스파이, 범죄조직 - 산업체 기밀 약탈, 대규모 경제 범죄 등
해 커	- 중요 정보의 유출 또는 시스템 파괴
핵티비스트	- 정치적 동기를 가지고 공격 - 중요 기반시설의 파괴보다는 선전활동에 치중
내부자 위협	- 조직 내부 불만자에 의한 컴퓨터 범죄 일차적 발생 원인 - 대상 시스템에 대한 지식을 이용 시스템 파괴
정부 및 외국 정보기관	- 평시, 전쟁수행시 적 시스템의 파괴, 교란 - 군사력을 지지하는 통신, 경제기반시설 파괴
테러리스트	- 특정 목적 달성을 위해 인명 손상 및 시설물의 파괴 - 전통적인 테러리즘에서 사이버 테러리즘으로 이동중
바이러스 작성자	- 바이러스 작성자는 지속적인 심각한 위협이 될 수 있음 - 파일과 하드 드라이브 등에 상당한 손상을 입힘

출처: 주요기반시설 보호를 위한 사이버보안, 국가사이버안전센터(2004)

2) e-테러리즘의 공격유형

e-테러리즘의 공격유형은 다양한 형태로 나타나고 있는데, 대표적인 예가 사이버 해킹(Hacking)이라고 할 수 있다. 일반적으로 해커들은 시스템이나 네트워크 취약성을 이용하여 침입을 시도한다. 이들은 시스템의 정상적인 작동을 방해하여 시스템이 사용자가 요구하는 서비스를 처리하지 못하도록 하는 서비스 거부 공격을 감행하거나 시스템을 공격하기도 하고, 주로 웹 서버나 홈페이지를 공격하는 등 다양하고 복잡한 기법을 이용한다.

컴퓨터 바이러스는 일반적으로 컴퓨터에 이상을 일으키거나 파일을 손상시키며 자신을 복제하는 등의 행위를 하는 프로그램을 말한다. 따라서 바이러스에는 상주하는 곳에 따라 부트 바이러스[1]와 파일 바이러스[2]로 나누고 바이러스의 피해범위는 약간의 메모리에만 삭제하는

1) 컴퓨터를 처음 실행할 때에는 부트 섹터에 있는 프로그램이 제일 먼저 실행되는데, 이 곳에 자리잡는 컴퓨터 바이러스를 부트 바이러스라고 한다. 이것은 부트 섹터에 기생하면서 컴퓨터의 부팅을 방해하는 바이러스로, 메모리 상주형이다. 대표적인 것으로 미켈란젤로 바이러스와 브레인 바이러스, LBC 돌 바이러스 등이 있다. (Empas 백과사전)

2) 파일 바이러스란 실행 가능한 프로그램에 감염되는 바이러스를 말한다. 이때 감염되는 대상은 확장자가 COM, EXE인 실행파일이 대부분이다. 국내에서 발견된 바이러스의 80% 정도가 파일 바이러스에 속할 정도로, 파일 바이러스는 가장 일반적인 바이러스 유형이다. 국내에서는 예루살렘(Jerusalem)과 일요일(Sunday)을 시작으로, 1997년과 1998년 적지 않은 피해를 주어 잘 알려진 전갈(Scorpion), 까마귀(Crow) 그리고 FCL이 있다(http://kmh.ync.ac.kr).

바이러스부터 CIH바이러스나 예루살렘 바이러스처럼 모든 파일과 프로그램을 삭제하는 치명적인 바이러스까지 그 종류가 다양하다.

웜(worm)은 네트워크에 침입한 뒤 컴퓨터, 네트워크, 그리고 사용자에 대한 정보를 입수한 뒤, 다른 시스템의 소프트웨어적 취약점을 이용하여 해당 시스템에 침투하고, 자신의 복사본을 만들어 또 다른 시스템으로 옮기는 방법으로 컴퓨터의 정상적인 작동을 방해하고, 네트워크 전체를 마비시킨다.

트로이 목마(Trojan Horse)는 정상적으로 보이는 프로그램 내부에 숨어서 시스템이나 네트워크에 피해를 미치는 기능을 하는 코드로, SATAN(System Administrator Tool for Analyzing Networks)과 같은 시스템의 보안 취약성 점검 도구 같은 형태로 위장 할 수 있다. 또한 자신의 존재를 사용자들이 알아보지 못하도록 작성되어 있을 뿐 아니라 쉽게 탐지될 만한 피해를 입히지 않기 때문에 찾아내기가 매우 어렵다(백광훈, 2001: 111-114).

이외에도 사이버 테러리즘 기법의 하나인 스팸(Spam)에 해당하는 전자우편폭탄(E-mail Bomb), 신호인증과정에서 의도적으로 신호전송을 거부함으로써 상대방 컴퓨터시스템을 계속 신호대기 상태로 묶어놓아 시스템을 무력화시키는 방법인 서비스 거부(Denial of Service)등이 있다.

최근에 사이버테러와 현실테러와의 연계 중 가장우려를 낳고 있는 것이 전자총(HERF Gun)인데 이는 전파체계를 교란시킴으로써 사람에게는 피해를 주진 않지만 국가기간전산망을 일시에 무력화시킬 수 있다. 또 컴퓨터통신은 물론이고 전화와 방송, 금융거래 등을 일시에 정지시킬 수 있는 파괴력을 지니고 있다. 사이버 테러리스트들은 전자총을 목표 컴퓨터가 있는 건물에서 어느 정도 떨어진 자동차 등에 설치해 원격 조정한다. 이와같이 e-테러리즘의 공격유형을 정리하면 〈표 2〉와 같다.

〈표 2〉 e-테러리즘의 공격유형

e-테러리즘의 공격유형	
해킹(Hacking)	비 인가자의 컴퓨터 이용 / 자료의 불펌, 열람, 삭제 및 변조/ 컴퓨터 시스템의 이상 동작 유발
전자우편 대량발송	상대방 시스템에 email을 대량 반복 발송함으로써 시스템의 정상 동작을 방해 및 마비
서비스 거부	시스템을 계속 신호대기 상태로 묶어 놓아 시스템을 무력화
논리 폭탄	논리적 수식을 이용해, 특정날짜 및 시간 등의 일정 조건이 일치될 때, 특정 프로그램이 동작해 시스템의 정보 삭제 및 시스템 동작 방해
트로이목마	프로그램 내부에 악성코드를 심어 시스템과 네트워크에 지속적인 피해를 입히는 기능을 가진 코드

웜 바이러스	네트워크에 침입하여 사용자의 정보를 입수한 후, 소프트웨어에 상주하여 네트워크로 전파되는 악성 바이러스
고출력 전자총	고출력 전자파로 컴퓨터 전자회로에 이상현상을 일으켜 시스템 오작동 유발 및 정지시킴
칩핑(Chipping)	반도체 칩을 제조할 때, 칩 내부에 이상기능을 의도적으로 삽입하여 일정 시간이 흐르면, 이상기능을 유발
Microbes	원래는 기름 공해 물질을 제거하기 위해 만들어진 것이나, 컴퓨터 내부의 실리콘 재질을 먹어치우도록 개조될 수 있어, 컴퓨터 CPU에 치명타를 입힐 수 있음
EMP Shock	전자 장치를 파괴하는데 사용되는 것으로 전자총에 비해 그 범위와 면적이 넓어 해당 반경 내의 모든 컴퓨터 및 시스템을 일시에 파괴시킬 수 있음

출처 : http://blog.naver.com/adam037?Redirect=Log&logNo=150031425157

3. 사이버 네트워킹(Networking)

1) 사이버 네트워킹의 주체

한국 테러리즘 연구소에 따르면 e-테러리즘을 자행하는 집단은 다음과 같이 크게 3가지유형으로 분류할 수 있다.

첫째는 단순히 개인적으로 활동하는 해커들에 의해 자행되는 것이다.

둘째는 네덜란드의 '트라이던트' 그리고 러시아의 '지하 해킹 마피아' 등과 같은 범죄 조직화된 집단에 의한 것이다.

셋째는 정치적, 민족적 혹은 종교적인 목적을 달성하기 위해 조직된 단체나 혹은 주권국가에 의해 행해지는 사이버 테러리스트들이다(http://www.terrorism.or.kr. 한국테러리즘연구소, '사이버테러리즘 개념정립', 2009. 07. 20). 이중에서 가장 우려가 되는 것은 세 번째 유형의 집단에 의해 저질러지는 e-테러리즘이다.

지금까지 발생한 대부분의 컴퓨터 관련 범죄는 컴퓨터를 이용한 사기 등과 같은 단순 범죄였다. 그러나 최근에는 단순한 해킹 차원을 넘어 정치, 민족, 종교 혹은 사회적 목적을 달성하기 위해 테러리스트들이 가상공간을 이용하고 있다는 것이다.

인터넷이 일상 생활화되면서 현실 세계에서만 활동해온 급진 정치, 사회운동가들 중에 일부가 투쟁대상이 현실보다는 가상공간에서 더 취약하다는 해커들의 논리를 수용하여 가상공간을 투쟁의 수단으로 삼게 된 것이다. 더욱이 해킹 수법이 이미 인터넷 웹사이트나 서적을 통해 널리 유포된 상태에서 마음만 먹으면 어렵지 않게 배울 수 있고, 기존의 해커 중에서도 일부가 자기 과시나 자기만족보다는 정치적 명분을 추구하는 사이버 테러리스트로 바뀌고 있다는 것도 e-테러리즘 확산의 요인이 되고 있다. e-테러리즘은 이제 더 이상 특정 국가만의 문제가 아니며, 그 위협은 매우 심각한 상황에 이르고 있다.

2) 사이버 네트워킹의 특징

사이버 테러리스트의 사상은 일반적으로 컴퓨터의 해킹을 통한 바이러스의 유포와 정보의 도용, 그리고 웹사이트의 손상 등 다양한 형태로 나타나고 있다. 이러한 상황에서 테러리즘의 공포가 증가하고 있고 사이버공간에서의 알카에다와의 친분이 계속해서 증가하고 있으며 팔레스타인은 팔레스타인의 해커를 통해 미국과 이스라엘의 웹사이트에 대항하여 "사이버-지하드"를 꾸준히 활동시키고 있다.

정보화시대에서 사이버 네트워킹은 테러리스트에게 무기와 목표의 형태를 선택하는데 영향을 미칠 뿐만 아니라 그 조직의 구조와 운영형태까지 영향을 미친다. 사이버 테러리스트들은 IT정보를 이용하여 정보를 공유하고 인터넷을 이용하여 조직을 구성하여 효과적으로 분산활동을 하고 있다.

최근 생성된 테러리스트 단체는 조직구조가 사이버세계를 통해 때로는 분산적이고 때로는 집합적인 유연성 있는 네트워크 구조를 가지고 있다. 이러한 테러리스트 조직은, 때로는 개인의 자금력으로 국가를 지원하고 있으며, 때로는 독립적으로 테러의 전술을 꾀하는 등 다양한 형태로 나타나고 있다.

사이버 네트워킹은 외부의 통제가 가능하고 그러한 조정 메커니즘은 IT를 통해 가능하게 된다. 이러한 사이버 네트워킹은 다음의 세 가지 특징을 통해 알 수 있다(Michele Zanini & Sean Edwards, 2004: 30-35).

첫째, 사이버 네트워킹은 산재되어 있는 조직들간의 의사소통 및 조직의 임무를 전달하는데 용이하게 작용한다. 이러한 사이버 네트워킹은 초기보다 치밀하고 은밀하게 커다란 조직을 작은 조직들로 분산화 할 수 있는 도구로 사용되며, 보다 효율적인 조직운영을 가능하게 만들었다.

둘째, 사이버 네트워킹을 통해 통신비용을 크게 줄일 수 있도록 하였고, 정보를 모으고 네트워크의 조직을 형성하는데 보다 용이하게 만들었다. 이는 과거의 조직보다 집중력 있고 강력한 조직을 유지할 수 있으면서도 비용을 낮춤으로 인하여 집중과 분산의 적절함을 통해 강력한 테러를 구성할 수 있는 힘이 되고 있다.

셋째, 복잡한 정보의 공유가 가능하게 되었고, 근접한 위치가 아니더라도 그룹웨어, 인터넷 채팅, 웹사이트를 통하여 지리적으로 분산되어 있는 테러조직의 개별적인 테러수행이 가능하게 되었다.

이러한 사이버 네트워킹의 특징으로 인하여 인터넷을 이용한 커뮤니케이션은 멤버들 간에 대화를 가능하게하고 운영에 있어서 보다 신속하게 일을 처리하여 조직의 유연성을 증가시키며, 전술의 변화를 쉽게 조정할 수 있게 하였다.

Bruce Hoffman 은 사이버 네트워킹은 테러리즘의 폭력행위를 선전하고 메시지를 알리

는 수단으로 이용할 수 있다고 언급하고 있다.

현재 테러리스트들은 인터넷을 이용하여 자신의 정당성을 선전하고 노출의 기회를 확대하고 있다. 인터넷 이전에는 전화나 팩스를 통한 테러리스트들의 요구가 있었으나, 현재는 테러리스트의 요구가 그들의 웹사이트 등을 통해 즉각적으로 나타난다. 많은 테러리스트들은 자신들의 메시지의 내용에 대하여 직접적으로 통제할 수 있을 뿐만 아니라 교묘히 이미지를 조작할 수 도 있다. 이러한 형태의 사이버 네트워킹은 테러의 연결고리로서의 작용을 돕고 있으므로 더 큰 재앙으로 연결될 수 있는 기폭제라고 할 수 있다(Monge & Fulk, 1999: 84).

3) 사이버 네트워킹의 활용

사이버공간은 테러리스트들에게 쉽고 편리한 접근성, 규제·통제 또는 제한이 거의 없다는 점, 전 세계에 걸친 관객의 확보, 익명성, 대량정보의 신속한 교류, 매우 저렴한 비용, TV·신문 등과 같은 전통적인 미디어의 총합을 능가하는 멀티미디어 환경, 전통적인 매스미디어들의 테러리즘 보도 형태에의 영향 등을 제공한다.

즉, 인터넷은 테러리즘의 목적 달성을 용이하게 하여 주는 가장 이상적인 매개체로서, 테러행위 수행 능력을 증가시켜 주는 기제의 역할을 하고 있는 것이 사실이며, e-테러리즘은 웹사이트와 인터넷을 테러수행을 위한 도구로 이용하고 있음을 보여주고 있다.

〈표 3〉에서 테러조직의 인터넷 웹사이트 활용 추이를 보면 아래와 같이 점차 증가하고 있는 것을 알 수 있다.

〈표 3〉 테러조직의 인터넷 활용추이

	1998년 1월	2002년 1월	2005년 초	2006년 5월
테러사이트 수	16개	19개	4,300개	4,800개

출처 : http://blog.daum.net/goodsoil/15307509

또한 테러조직의 홈페이지에서는 표현의 자유와 정치적문제, 사랑과 평화의 수사적인 메시지를 풍부하게 이용하는 공통적인 특징이 있다. 이렇듯 테러리스트들은 웹사이트를 이용한 테러를 적극적으로 이용하고 있는 상황이다.

Ⅲ. e-테러리즘의 실태 및 문제점

1. e-테러리즘의 사례를 통한 실태분석

최근 e-테러리즘의 경향을 살펴보면 목적과 피해범위에 따라 크게 세 가지 정도로 나누어 사례를 살펴 볼 수 있다. 첫째, 불특정 다수에 대한 공략. 둘째, 국가나 특정 단체에 대한 공격 및 항의를 목적으로 한 사이버 테러. 셋째, 사이버 네트워킹을 통한 현실 테러리즘과 사이버 테러리즘의 결합이다.

1) 불특정 다수에 대한 공략

불특정 다수에 대한 공략은 주로 바이러스를 이용해 자행된다. 특히 바이러스가 E-mail을 통해 전파되면서, 이에 대한 피해가 광범위해지고 무서운 전파속도에 따라 손해 정도도 순식간에 대규모가 되고 있다. 목적성이 비교적 약하기 때문에 테러리즘적 성격이 적다고도 볼 수 있겠으나, 이러한 방법에 특정한 목적성이 부과된다면 그 피해가 엄청날 수 있다.

사례 1.

1999년 3월에 등장한 멜리사바이러스와 4월 26일에 있었던 CIH바이러스, 2000년 5월 4일 등장한 러브바이러스는 이것이 단순하고 널리 알려졌음에도 불구하고 그 피해는 엄청났다. 멜리사 바이러스의 경우 국외의 약 5만대의 PC시스템과 100여 개의 기업체를 감염시킨 사례가 있었고, CIH바이러스는 국내 보급된 전체 PC 800만대 중 3% 이상에 해당하는 30만여 대가 감염되었으며, 러브바이러스의 경우는 전세계적으로 수천만 대의 컴퓨터를 감염시켰다. 뿐만 아니라 미국의 백악관과 연방수사국을 비롯하여 각국 정부 주요기관의 시스템까지 한때 마비상대에 빠뜨린 것으로 보고됐다(서울경제신문 2005. 04. 25).

사례2.

2003년 1월 25일 슬래머 웜, Slammer 등으로 우리에게 알려진 Worm. SQL. Slammer 바이러스에 의해 우리나라의 인터넷이 마비되는 사태가 발생했다. 그 원인은 해커의 악의적인 공격이 아니라 정보화 사회에서 수시로 출몰하는 신종 웜 바이러스 때문으로 바이러스가 대량의 네트워크 트래픽을 유발, 인터넷 접속장애를 일으켜 발생한 것으로 밝혀졌다. (국가정보원, 2004: 26). 슬래머 웜은 취약성을 갖고 있는 SQL서버를 감염시켰고, 감염된 서버는 초당 1만~5만개의 패킷을 생성하여 네트워크 트래픽을 폭발적으로 증가시켜 감염 서버가 있는 대학, 연구소, 기업은 물론 주변 이용자들의 인터넷 접속 경로를 차단하였다.

사례 3.

2004년 9월 10일 마이둠 웜이라는 변종 바이러스에 대한 긴급경보가 내려졌다. 이 바이러스는 안철수연구소가 9일 첫 발견하여 차단서비스에 의해 231건이 차단되었으나, 이메일로 확산되며 네트워크 과부하를 유발시키며 급속히 퍼져나갔다. 이로 인해 전 세계적으로 2,145,703대의 컴퓨터가 피해를 입었고, 한국에서도 2,019대의 컴퓨터가 피해를 입었다(국가보안기술연구소, 2005: 84).

2) 국가나 특정단체에 대한 공격 및 항의를 목적으로 한 사이버테러

사이버테러리스트들은 어떠한 목적을 가지고 주요 기관에 대한 공격이나 항의 표시로 사이버 테러리즘을 가하기도 한다. 주로 국가나 대규모 단체에 대한 테러리즘일 경우는 그들의 중요 웹사이트나 시스템에 침입해 공격 또는 시위를 한다. 주된 방법으로는 소수의 전문가에 의한 해킹과 일반인들을 선동한 메일폭탄 등이 있다.

사례 1.

1991년 걸프전 개전시 미 해군이 전자기탄두(전자공격무기의 일종)를 장착한 미사일을 사용하여 이라크 남부 국경에 있는 방공망을 마비시킨 바 있고, 걸프전 중에는 독일 해커가 미국 국방부 정보시스템에 단순 해킹기법을 활용·침투하여 입수한 군사정보를 이라크 정보기관에 팔려고 시도한바 있다. 1997년 2월에는 크로아티아의 10대 해커가 미국 국방부의 정보시스템에 침입하여 약 50만불의 피해를 입힌 사례이다.

사례2.

1999년 8월 대만해협의 긴장이 고조된 가운데 중국해커들이 대만 내 10개 정부기관 컴퓨터에 침입하여 화면을 대만 총통의 양국론 발언 비난성명으로 바꿔놓고 컴퓨터망을 마비시키자, 대만 해커들이 중국 기관내 컴퓨터시스템에 침입하여 철도부 홈페이지를 대만 국기와 '중화민국만세' 등의 구호로 장식하는 한편, 중국 주요기관의 웹사이트 목록을 공개하고 대만 해커들에게 효과적인 공격방법까지 제시한 사례가 있다.

사례3.

2004년 4월, 국내 한 군수업체 직원을 통해 주요 국가기관 시스템들이 중국 측으로 추정되는 가해자에게 공격을 받아 해킹당한 사실을 확인하였다. 위장된 악성프로그램을 통해 관계인을 사칭하는 등 교묘한 방법으로 Email 등에 첨부, 유포하여 방화벽 내부의 소수 시스템을 장악하고 이를 통해 내부에서 다수의 시스템을 직접 해킹한 후 저장된 파일 및 Email

정보 등 주요 정보를 유출하는 치밀한 수법이 사용되었으며 국회, 원자력연구소, 해양경찰청, 국방연구원등 10여 개 기관 220여 대의 시스템이 해킹 피해를 입은 것으로 밝혀졌다(http://blog.naver.com/phpins?Redirect=Log&logNo=100009535586, 2009. 07.15).

3) 현실 테러리즘과 사이버 테러리즘의 결합

최근에는 사이버 공간에서 테러리즘을 자행해 현실세계를 공격하는 수법이 많이 쓰이고 있다. 바로 물리적 공간이 가상화되어지는 부분을 공략하는 것이다.

그 대표적인 예로 미국 '9.11테러'를 들 수 있다. 이는 인터넷을 통한 다양한 네트워크 기술과 해킹기술 등으로 중무장한 테러집단의 치밀한 준비에 의한 관제시스템 해킹 등의 사이버 테러리즘이 결합됐을 가능성이 높다고 할 수 있다(국방저널, 2004).

이러한 현실 테러리즘과 사이버 테러리즘의 결합은 특히 정보통신 인프라적인 측면에서 커다란 문제점을 일으킬 소지를 가지고 있다. 특히 전기공급 중단, 금융・통신시스템의 마비 등 사회기반시설을 파괴하여 궁극적으로 경제활동의 혼란과 마비를 초래할 수 있다. 지식기반경제로의 이행이 진행되는 가운데 정보통신 인프라는 에너지・제조・통신・금융시스템 등의 정부 및 공공기관 뿐만 아니라 주요 민간기업의 중추신경계 역할을 수행하고 있으므로 이에 대한 심각한 사회・경제적 문제로 대두될 것이며, 나아가 국가안보를 위협하는 심각한 사태를 초래할 가능성이 크다.

유비쿼터스 사회에서의 정보통신망에 대한 의존도는 가정과 사회 전 부문으로 확대되어감에 따라, 피해범위 또한 정치・경제・사회・군사・가정 등 국가와 사회의 모든 분야로 확대될 수밖에 없게 될 것이다.

2. 한국 e-테러리즘 대응상의 문제점

한국에서는 e-테러리즘이라 부를 수 있는 심각한 테러리즘은 아직 발생하지 않았다고 볼 수 있다. 그러나 한국의 경우 인터넷의 기반이 다른 어느 국가보다 잘 이루어져 있고 그 사용인구가 폭발적으로 증가하면서 국내의 사이버테러와 더불어 국제적인 사이버테러의 경유지로써의 창구 역할을 할 수 있는 중요하고도 심각한 상황에 직면하여 있다.

법・제도적 측면에서도 어느 정도 정비를 하고 있기는 하지만, e-테러리즘 수준을 염두에 둔 조치들이 이루어져야 할 것으로 사료된다.

현재 국내에서 e-테러리즘 관련해서 나타나고 있는 대응상의 문제점은 크게 세 가지로 구분하여 살펴볼 수 있을 것이다. 먼저, 국내 사이트의 해킹사고 증가를 들 수 있다. 국내에서의 해킹사고는 국가・공공기관까지 포함하여 급증하고 있는 실정에서 이에 대한 대책마련이

시급하다는 인식이 생겨나고 있다(http://www.terrorism.or.kr. 한국테러리즘 연구소, 2009. 07. 15). 그러나 이러한 인식과는 달리 우리의 전산시스템은 해커의 해킹능력에 비해 현저히 떨어지는 방비시설을 가지고 있다. 국가·공공기관의 해킹사고는 월평균 100건이상이 발생하고 있고 이 또한 매년 증가추세를 보이고 있는 상황(http://news.nate.com/view/20020724n00101, 2009. 07. 15)에서 그 문제의 심각성은 더 클 것으로 예상된다.

둘째, 한국은 인터넷 보안문제에서 외국 해커들의 경유지가 되고 있다. 외국의 보안전문지에 "한국이 해커들의 경유지로 부상하고 있다"고 보도될 만큼(http://www.kbs.co.kr/1tv/sisa/kbsspecial/vod/1249007_11686.html, 2009. 07. 16) 한국이 해킹에 있어서 취약지대로서의 문제가 심각함을 알 수 있다.

다른 나라의 해킹을 시도하기 위해 경유지로 각광받고 있는 상황이라면 우리나라의 정보시스템 보안 수준을 짐작할 수 있다. 이렇게 무방비 상황에서 해커들이 우리의 통신망에 침투하여 야기할 사회적 혼란과 피해는 상상 이상으로 엄청날 것이다.

셋째, 전문 보안 인력과 기반시설의 부족을 들 수 있다. 보안인력의 경우 우리나라는 보안서버 등의 보급비율이 매우 낮고 이를 위한 기술개발과 산업인력 양성에 지속적인 노력이 미비한 실정이다. 또한 사이버공격과 관련된 요소들은 공공의 안전뿐만 아니라 민간부분의 위험요소도 매우 큰 것이므로 다양한 정책과 지원이 이루어져야 함은 물론 정부와 민간의 협력을 통한 보안인력의 양성과 기반시설의 확충이 이루어져야 할 문제이다.

Ⅳ. e-테러리즘의 효율적 통제방안

e-테러리즘은 국내뿐만 아니라 세계 각국의 노력이 연계되어야 하는 특수한 상황의 테러리즘이라고 할 수 있다. 특히 국제성범죄의 성격이 강하고 사이버상의 특징과 가상과 현실에서의 위험이 도사리고 있다는 것도 그 문제를 더 크게 만드는 하나의 요소일 것이다. 현재 전세계적으로 이러한 e-테러리즘의 문제가 가장 큰 나라가 미국을 비롯한 선진국가일 것이다. 또한 이러한 국가들은 항상 사이버 테러리스트들의 표적이 되어온 것도 사실이다. 따라서 선진국의 e-테러리즘의 대응방안을 살펴보고 그중 우리나라의 경호적인 입장에서의 테러대응에 효과적으로 적용할 수 있는 방안에 대하여 고찰해 보고자 한다.

미국의 국방부는 일주일에 수 백 차례의 해킹시도를 당하는데 이들 대부분은 영웅심을 위한 단순한 해커들이지만, "국가 차원의 해킹 시도도 예상되고 있다는 것이 미국의 공식 입장이다. 미국은 9.11을 통해 e-테러리즘의 심각성을 인지하고 적극적인 경호적 대처를 실행해 나가고 있다. 구체적인 예로 'The Nation Strategy to Secure Cyberspace' 전략이 수립

되어 국토안전부 산하에 NCSD(Nation Cyber Security Division)가 설립되고 NIPC(Nation Infrastructure Protection Center)도 연방수사국에서 국토안전부로 이전되어 공공 또는 민간 부분의 기반시설 소유자와 운영자간의 직접적인 연락 체계를 확장하고 있으며, 사이버 공격과 관련한 정보의 공유를 촉진하고 있다. 또한 법무부는 불법적인 컴퓨터 범죄의 사후 처리 방법에 대한 전문지식을 개발해 오고 있고, 컴퓨터 범죄의 대응을 위한 법률적 해석과 전자적 증거를 확보하는 기술 등을 마련해 나가고 있다 (http://blog.daum.net/goodsoil/15307509, 2009. 07. 20).

일본 역시 해킹 등 전자적 침해행위에 적극 대응하기 위해 부정 접속 행위의 처벌 등을 내용으로 하는 '부정 액세스 행위 금지 등에 관한 법률'을 공포하고 시행에 들어갔으며, 구체적으로 'e-Japan 전략'을 통해 빠르게 정보통신 환경을 구축하여 일부 정부기관의 서버에 대한 부정침입의 대응책 마련에 적극적인 자세를 보이고 있다. 이외에 선진 각국들은 EU, APEC, G8, OECD등의 국제협력 기구들과 공조하여 e-테러리즘의 공동대처를 위한 국제적 협력체제 구축에 노력하고 있다(박춘식・김현수, 2003: 172).

국내의 e-테러리즘 방지 대책은 아직 미미한 수준이지만, 최근 국방부, 국가정보원, 경찰청, 정보통신부 등 관련 부처와 민간 전문가로 구성된 특수부대를 창설하여 운영하고 있다. 이러한 사이버 특수부대의 창설에 대해 네트워크 전문가들은 "인터넷을 통한 어떤 형태의 공격으로부터 100% 완전하게 방어할 수는 없다"라고 가정하지만 이러한 노력이 선행되어야 한다는 점에는 모두가 공감하고 있는 부분이다.

현재의 상황에서 우리가 e-테러리즘에 효과적으로 대처하기위한 방법을 크게 세가지로 제시하고자 한다.

첫째, IT기술의 급변으로 국제 e-테러리즘에 적극적으로 대응할 수 있는 사이버 정보군 등의 인력양성과 예산확보이다. 앞에서 살펴본바와 같이 선진국을 비롯한 외국의 경우 적극적인 투자와 대책이 제시되고 있다. 우리나라의 경우 인터넷 보급률이 세계적인 수준이라는 것은 누구나 알고 있듯이 사이버의 고급인력에 대한 기반은 충분히 갖춰져 있는 상태라고 할 수 있다. 다만 이러한 기반을 중심으로 좀 더 체계적인 지식교육과 투자로 사이버 정보군을 지원한다면 세계적인 수준의 조직적인 시스템을 구축할 수 있으리라고 본다.

둘째, 사고 대응체계를 종합화하고 체계화하기위한 네트워크 관리가 필요하다. 사이버상에서는 신속하고 저렴하고 익명성이 보장되는 공간이다. 이는 테러조직의 활동을 통제하는데 있어서 국경을 초월하는 구성원의 네트워크 관리가 필요할 것이다. 실제로 테러집단의 경우 법집행 당국의 정보수집, 분석을 인지하고 허위작전을 인터넷에 유포하는 경우까지 자행되고 있다. 이러한 예에서도 알 수 있듯이 사이버상의 문제는 광범위하고 복잡하지만 이러한 위협에 대비하기위한 체계화된 네트워크 관리가 선행된다면 큰 피해를 줄일 수 있는 하나

의 계기가 될 것이다.

셋째, 사이버 공격현황의 정보수집 및 분석·교환을 강화하여야 한다. 인터넷은 정보의 바다로 비유될 만큼 많은 정보를 획득할 수 있는 공간이다. 테러리스트도 마찬가지로 대부분의 정보를 인터넷으로부터 얻고 있는 실정이고 온라인 정보수집은 작은 비용과 노력으로 테러리스트에게 있어 매력적인 도구로 이용되고 있다. 이러한 상황에서 테러리스트들의 사이버 공격기법 등의 빠른 변화를 대처하기 위해 인터넷상에서 발생하는 공격 형태를 파악하고, 공격정보를 중앙으로 수집 분석할 수 있는 전담기구를 강화하여 발전시켜야 한다. 이와 같은 조직을 선진외국에서는 조직적으로 설치 운영하고 있으므로 이를 벤치마킹하여 운영하는 것도 하나의 좋은 예라고 할 수 있을 것이다. 이러한 노력이 선행될 때 사이버를 이용한 위성해킹이나 GPS 해킹 등 고난위도 e-테러리즘에 적극적으로 대처할 수 있을 것이다.

V. 결 론

현대사회에 있어서 인터넷이라는 도구는 손쉽게 접근이 가능하고, 통제에 대하여 비교적 자유로우며, 접근대상이 광범위하다라는 특징 때문에 편리한 도구로 이용되어지고 있다. 그러나 이러한 효과는 테러집단에게 e-테러리즘이라는 도구로 이용되어 자신의 목적을 달성하는데 매우 유용하게 작용하고 있고 이로인한 피해는 전세계적으로 나타나고 있다. 최근에 일어나고 있는 테러사건들도 사이버라는 공간이 전략적 도구로 이용되었다는 것이 분명하게 밝혀지고 있다.

이러한 특성으로 인해 e-테러리즘은 점차적으로 확대될 것이 분명하다. 사이버 테러리스트들은 그들의 목적을 달성하기 위해 최소한의 위험만으로도 큰 성과를 얻을 수 있고, 이러한 매력 때문에 e-테러리즘이 급속히 확산될 것이다. 따라서 인류의 시급한 문제가 될 e-테러리즘에 대한 대책을 마련해야한다.

이 논문에서는 e-테러리즘을 정의하고 이에 따른 개괄적인 내용과 이를 효과적으로 통제하기 위한 방법을 모색하고자 하였다.

e-테러리즘의 심각성은 불특정 다수에 대한 공략으로 목표물에 대한 사전차단이 쉽지 않다는 것에 있다. 특히 국가나 특정단체에 대한 공격 및 항의를 목적으로 한 사이버상의 테러가 주로 이루어지고 있으나 이외의 사이버테러도 그 문제성이 높다고 판단되어 진다.

현재 전세계적으로 e-테러리즘의 공포가 확산되는 것은 사이버상의 공격뿐만 아니라 현실에서의 테러리즘과 사이버 테러리즘의 결합을 들 수 있을 것이다. 이는 사이버상에서의 테러선전과 홍보, 테러요원모집, 재정조달, 정보수집과 교환, 네트워크 등을 통해 현실세계에서

테러가 자행된다는 것이다.

이러한 문제의 심각성은 비단 국제적인 문제를 넘어 우리나라에서도 심각한 상황을 만들고 있다. 사이버공간이라는 특수성으로 인해 개별국가에 적용되어지는 문제가 아니라는점을 감안한다 하더라도 현재 나타나고 있는 국내의 해킹사고 급증, 특히 외국 해커의 경유지로서의 한국이 이용된다는 점 그리고 이러한 상황임에도 불구하고, 외국에 비해 전문 보안인력이나 기반시설이 선진외국에 비해 부족하다는 점을 문제점으로 제시 할 수 있었다.

이에 대한 대안으로 e-테러리즘에 대응할 수 있는 사이버 정보군 등의 인력양성과 예산확보, e-테러리즘에 대응체계를 종합화 · 체계화하기위한 네트워크 관리, 사이버 공격현황의 정보수집 및 분석 강화를 제시하였다.

e-테러리즘은 인터넷이라는 획기적인 기술발달의 산물로 전세계 사람들에게 수많은 편리성과 다양성을 제공하지만 이를 악용하고자하는 테러리스트들에게는 자신들의 목적을 달성하는 이상적인 활동체계가 되고 있는 현실에서 이를 효과적으로 통제하기 위한 한국과 전세계의 노력이 필요하다는 것을 명심해야 할 것이다.

참 고 문 헌

1. 국내문헌

박춘식 · 김현수(2003). 「사이버테러」, 진한도서.

박형민(2002).「컴퓨터사용 사기범죄의 현황과 처리실태에 관한 연구」, 형사정책연구원 연구보고서.

백광훈(2001). 「사이버테러리즘에 관한 연구」, 형사정책연구원 연구보고서.

오영민(2004). 「미국연방 행정부 조직의 새로운 변화: 국토안보부의 설립사례를 중심으로」. 육군3사관학교논문집, 59: 409-430.

윤영성(2005). "사이버테러리즘에 대한 안전보장 및 대응체계 연구", 연세대 행정대학원 석사 학위논문.

윤우주(2002). 「한국의 대테러대비태세와 발전방향」. 테러리즘과 문명공존, KIDA포럼 02-10, 한국국방연구원: 89-125.

이성우(1999). 「국제테러리즘에 대한 법적 규제 및 대응방안에 관한 연구」. 국방대학원 안보과정수료 논문.

이윤호(2008), 「현대사회와 범죄」, 도서출판 다해.

이진수(2000), "사이버테러리즘의 실태와 대책", 형사정책연구 제11권 제2호(통권 제42호 여름호).

주수기(2006), "e-테러리즘: 테러 웹사이트와 인터넷테러리즘", 「안보논단 Ⅳ」해병대전략연구소.

최진태(2006), 「테러리즘의 이론과 실제」, 도서출판 대영문화사.

2. 국외문헌

Arquilla, John & David Ronfeldt.(2002). *Networks and Netwars.: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand.

Bowden, Mark.(1999). *Blackhawk Down: A Story of Modern War*. New York: Atlantic Monthly Press.

Edwads, Sean J. A.(2000). *Swarming on The Battlefield :Past. Present, and Future*. Santa Monica, Cali.: Rand, MR-1100-OSD.

Gerlach,Luther P.(1987). "Protest Movements and The Construction of Risk." B.B. Johnson and V.T.Convello, eds., *The Social and Cultural Construction of Risk*, Boston: D. Reidel Pub. 103-145

Hoffman, Bruce.(1998), *Inside Terrorism*. New York: Columbia University Press.

Homeland Security Advisory Council. (2007). *Report of the Culture Task Force*.

Lesser, Ian O. et al.(1999). *Countering The New Terrorism*. Santa Monica, CA:Rand

3. 기타

http://blog.naver.com/adam037?Redirect=Log&logNo=150031425157
http://www.terrorism.or.kr.
http://blog.daum.net/goodsoil/15307509
http://blog.naver.com/phpins?Redirect=Log&logNo=100009535586,
http://www.terrorism.or.kr
http://news.nate.com/view/20020724n00101
http://www.kbs.co.kr/1tv/sisa/kbsspecial/vod/1249007_11686.html
http://blog.daum.net/goodsoil/15307509
연합뉴스(http://www.yonhapnews.co.kr)
엠파스 뉴스(http://news.empas.com)
조선일보(http://www.chosun.com)
전자신문(http://www.etimesi.com)
IT-business(http://www.itbiz.co.kr)
국가 정보원(http://www.nis.go.kr)
경찰청(http://www.police.go.kr)
시사 컴퓨터(http://www.sisait.co.kr)
정보통신부(http://www.mic.go.kr)
한국테러리즘 연구소(http://www.terrorism.or.kr)
해킹 바이러스 상담 지원센터(http://www.cyber118.or.kr)
해커스 아카데미(http://www.hackersacademy.co.kr/)

Abstract

Efficient countermeasures against e-terrorism

Lee, Yoon-Ho · Kim, Dae-Kwon

In e-terrorism, terrorists use cyber spaces including the internet in order to strike terror into the heart of a nation. It is revealed that recently happening terror cases use cyber spaces as a strategic tool.

This research aims to investigate efficient countermeasures against various types of terror attacks made by terrorists and their cyber networking, in order to contribute to the prevention of terrors from a modern standpoint.

Based on the results of the investigation, relevant problems are suggested such that terrors are not cases happening in a specific country only because they take place in cyber spaces, that hacking incidents frequently happen in Korea which is used as a footstool by foreign hackers, and that Korea has poor professional security manpower and foundational facilities in comparison with other advanced countries. Answers to the problems include cultivating cyber information manpower to cope with e-terrorism, making an appropriate budget, setting up networks to integrate and systematize anti-e-terrorism organizations, and intensifying the collection of information of cyber attacks and the analysis of the information.

Key Word : E-terrorism, Cyber Terrorism, Cyber Terror, Cyber Networking, Net-war

논문투고일 2009.07.30, 심사일 2009.08.10, 게재확정일 2009.09.01