한국위기관리논집 제8권 제6호 2012. 12 31~49쪽

미국 사이버테러 대응 시스템의 특징 및 함의*

박동균**.김태민***

미국의 국가사이버보안처(NCSD)는 효과적인 국가 사이버보안 대응시스템을 구축·유지하고, 국가중요 기반시설의 보호를 위한 사이버위기관리 프로그램을 실행하는 두 가지 주요한 역할을 수행한다. 2006년 2월부터는 이 기관의 주도로 격년제로 실시하는 사이버 스톰은 국가 차원의 사이버테러 대응훈련이다. 민・관・군이 참여하며, 매 훈련 때마다 2년 동안 새로 등록된 정부와 민간업체들이 추가로 훈련에 참가한다. 훈련은 주요 국가기반 시설(전력・통신・교통 등)을 공격한 뒤 공공기관이나 기업의 대응 속도를 확인하는 방식으로 이뤄진다. 사이버 스톰은 2006년 2월 6일부터 10일까지 정부주도로 대규모의 국가 사이버보안 훈련으로 실시되었는데, 공공, 민간, 국제기관 및 단체, 회사 등 110개 이상의 단체들이 사이버 스톰의 계획 및 실행단계에 참여했으며, 사이버 공격에 대응하기 위하여 정보기술(IT), 통신, 에너지, 교통부문 시스템을 보호하는 훈련을 실시했다. 사이버 스톰은 다양한 사이버공격에 대응하여 커뮤니케이션, 정책, 절차 등을 테스트해 보는 기회로 만들어졌고, 아울러 추가적으로 필요한 기획과 과정들은 무엇이 있는지를 알아보는 것이 주요 목적이다. 사이버테러에 가장 효과적인 방법은 사이버 보안을 가장 중요한 가치로 인정하는 것이다.

주제어: 사이버테러, 사이버테러형범죄, 사이버 스톰

Ⅰ. 서론

9·11 테러는 진주만 공격이후 외국의 미국영토에 대한 공격 취약성을 강조하였다. 그 이후 연방정부, 언론, 미국의 국민들은 유사한 공격 또는 핵, 생물학적 무기, 화학무기 등과 같은 파괴적인 대량살상무기로부터 자신들을 보호하는 정책들에 중점을 두어왔다. 하지만 미국은 이와 같은 물리적인 공격에 추가하여 국가안보와 경제성장에 중요한 컴퓨터 네트워크에 가해지는 '사이버공격(cyber attack)[1]'에 매우 취약한 상태이다. 테러리스트들은 은행과 금융기관, 이동통신사, 전기 및 재난구조 네트워크, 보건의료기관, 상수도, 석유 및 가스회사 또는 정부주요기관 등을 작동시키는 네트워크 시스템을 목표로 공격할 수 있다(Vatis, 2003: 220). 과거 1998년 6월, 인도가 핵 실험을 실시한 직후에 영국과 네덜

* 이 연구결과물은 2012학년도 경남대학교 학술연구장려금 지원에 의한 것임.

** 제1저자, *** 교신저자

1) 한희원(2011: 403-404)은 3대 사이버 공격(cyber attack)을 사이버테러(cyber-terrorism), 전자 전쟁(electronic warfare), 사이버 전쟁(cyberwar)로 구분하고 있다. 여기서 사이버테러는 사이버 공간에서의 여러 가지 공격을 표현하는 용어로 사이버테러(cyber-terrorism)라는 용어가 역설적으로 그 친근감으로 인하여 가장 널리 사용되고 있다고 보고 있다.

란드 대학생들이 인도 핵무기 연구소의 웹 사이트에 핵무기를 상징하는 버섯구름 사진을 무차별적으로 게재했다. 또 1999년 나토의 유고 주재 중국대사관 오폭 사건으로 인해 중국의 심각한 피해가 발생하자 일부 중국인들은 백악관과 국무성을 비롯한 웹 사이트를 해킹 했다. 이로 인해 백악관 웹 사이트는 중국어와 영어로 된 각종 낙서들로 장식 되었고, 장시간 동안 사용불능 상태까지 이르렀다.

1999년 4월 26일, CIH 대란은 대만의 대학생이 제작한 짧은 바이러스 프로그램이 인터넷을 통해 기하급수적으로 퍼져 우리나라에서만 30만여대의 PC를 손상시켰다. PC 수리비와 데이터 복구비용만 해도 20억원 이상 소요되었다. 전 세계적으로 그 피해액은 무려 2억 5천만 달러로 추정된다(박동균, 2009b: 55-66).

미국에서 사이버 테러리즘에 대한 공공의 관심은 1980년대에 시작되었다. 2000년대에 들어서면서, 밀레니엄 버그에 걱정과 불안감이 잠재적인 사이버 테러리스트들의 공격가능성에 더해 증폭되었다. 미국은 2001년 9·11 테러에서 테러리스트들의 세간의 높은 관심을 갖는 공격과 당국의 테러와의 전쟁 선포가 미래의 잠재적인 사이버테러 가능성을 예측하고 있다. 또한 주류 언론에서는 국가경제에 직·간접적으로 영향을 가하는 목표로 대규모 기간시설을 파괴하는 컴퓨터 네트워크를 사용한 공격 가능성에 대해 논의하고 있다.

미국국민들은 9·11 테러로 인해서 테러리스트들은 어떠한 수단도 사용할 수 있고, 대규모의 민간인 피해도 전혀 개의치 않는다는 점을 확신할 수 있게 되었고, 미국은 위험의 정도를 측정할 수는 없지만 더 이상 안전하지 않다는 것을 시민들은 알게 되었다. 또한 9·11 테러리즘으로 인해 미국의 대테러리즘 시스템은 여러 가지 문제점을 드러내었다. 미국의 대테러리즘 상태는 명백하게 허점이 존재하기 때문에 테러리즘의 영향을 예방하거나 완화시키고, 위기대응 능력을 극대화시키는 등 좀 더 날카로운 정책이 필요하게 되었다(Howitt & Pangi, 2003: 1). 즉 미국정부와 국민들은 아무리 비용이 소요된다고 하더라도 안전을 재확립해야 하는 방안들을 수립할 필요를 느끼게 된 것이다(Heymann, 2003: 57). 특히, 현대 산업사회에서 정보기술(information technology)은 테러리스트들에게 목표물 또는 무기로 활용될 수 있다(Branscomb, 2003: 93).

한편 우리나라에서도 정보통신기술의 발달과 인터넷의 확산으로 고도의 정보화 사회에 살고 있으며, 이에 따른 해킹, 바이러스 유포와 같은 사이버테러는 물론 인터넷 사기 등의 사이버범죄가 심각한 사회문제화되고 있는 실정이다. 경찰청 사이버테러대응센터 자료에 의하면, 2007년 1월에는 '한국형 봇넷'이라고 하는 대용량 스팸메일 발송 프로그램을 제작, 인터넷 사이트 수백 개를 해킹한 후, 해킹된 시스템을 피싱 및 스팸메일 발송의 경유지로 이용하고, 12,000건의 개인 정보를 수집하여 1억여 원의 부당이득을 챙긴 범인 2명이 검거되기도 하였다. 또 2005년 11월에는 국내 유명 은행의 홈페이지와 유사한 피싱 사이트를 제작하여 국내 및 미국의 웹호스팅 업체에 서버를 두고, 위치 추적이 어려운 무선 인터넷으로 관리하면서 인터넷 카페이 '낮은 금리로 대출을 해주겠다'라고 광고하여 피싱사이트로 접속을 유도한 뒤, 입력받은 개인정보를 이용하여 공인 인증서를 재발급 받아 12명의 피해자 계좌에서 총 1억2천만원을 인출한 5명이 검거되기도 하였다.

2011년에는 3·4 디도스공격, 현대캐피탈 사건, 농협 전산망 장애사건, SK컴즈 사건 등 대규모 해킹이 발생한 바 있으며, 이들 해킹의 특징은 개인정보피해 규모의 확대, 둘째, 외국서버를 통한 침투, 셋째, 북한에 의한 공격, 넷째, 악성코드에 감염된 PC(좀비PC)에 의한 공격 등이다(정기석, 2012: 91-92).

특히 우리나라는 남북대치라는 특수한 테러환경에 처해 있다. 북한으로부터의 테러 위험이 상존하고 있는 것이다.

북한은 1987년 11월 29일 인도양 상공에서 KAL 858기를 공중 폭파한 사건을 이유로 다음 해 1988년 1월 20일 미 국무부에 의해 테러지원국으로 지정되었고, 이후 2008년까지 계속해서 미 국무부의 테러지원국 목록에 올라 경제적 제재를 받아오기도 하였다(정웅, 2011: 375). 우리는 북한의 사이버 테러리즘 수행능력 및 역량강화에도 주의를 기울일 필요가 있으며, 이에 대비하여 미래지향적인 사이버 테러리즘 대응 능력을 배양해 나가야 할 것이다(최선우·류채형, 2012: 215). 이러한 북한으로부터의 잠재적 테러 위협은 물론 북한과 안보위해세력들이 해외 친북사이트·SNS 등 각종 인터넷 매체를 적극 활용, 북한체제를 찬양·선전하는 활동을 한층 강화하고 있다. 특히, 접속기록의 은닉, 우회접속, 익명서비스 이용 등 사이버공간 내 안보위해 행위의 수법 지능화로 단속의 어려움도 증대되고 있다(경찰청, 2012: 246). 사이버테러는 사이버 공간에서 범죄를 야기하는 등 일반적 차원에서 이루어지고 있지만 군사전략적 차원에서도 크게 진화되고 확산 될 수 있기 때문에 방어전략으로서 접근해야 할 필요성이 있다.

이러한 맥락에서 이 연구에서는 향후 테러리스트들이 활용할 가능성이 높은 사이버테러에 대한 기초논의와 함께 테러리즘에 대하여 강력한 대응정책을 실시하고 있는 미국의 사이버테러 대응 사례를 살펴보고, 아울러 이를 통해 우리나라에서 배워야 할 교훈과 시사점을 도출하고자 한다.

Ⅱ. 사이버테러의 기초 논의

1. 사이버테러의 이론적 근거

1968년 이래 테러는 매년 전 세계적으로 열병처럼 번지고 있다. 자유와 질서가 미묘한 균형을 이루고 있는 자유민주주의 국가에서 더욱 증가한다(이황우, 2011: 5). '테러(terror)'란 커다란 공포 또는 죽음이라는 심리적 상태를 이용하여 정치적 목적(주의나 주장)을 달성하려는 일체의 행동을 말하며, 일반적으로 테러와 테러리즘에 대한 명확한 구별없이 테러라는 용어를 사용하고 있다(이갑헌, 2010: 296). 심리학자들은 테러를 "특정 위협이나 공포조성으로 인해 사람들이 심적으로 느끼게 되는 극단적인 두려움의 원인이 되는 어떤 것"으로 해석하고 있다. 테러리즘은 폭력의 조직적, 의도적 이용으로 강압적이며, 희생자 혹은 희생자와 연관된 모든 사람, 그리고 대중들의 의지를 이용하기 위한 목적 지향적인 행위이며, 이를 위해 강제, 협박, 위협을 통해 폭력을 체계적으로 활용하는 것이라고 할 수 있

다. 이러한 차이성에 따라 테러는 테러리즘이 없이도 발생이 가능하며, 테러는 테러리즘의 중요한 구성 요소로 보기도 한다(최진태, 2006: 19). 한국의 「국가대테러활동지침」에서는 테러를 "국가안보 또는 공공의 안전을 위태롭게 할 목적으로 행하는 「외교관 등 국제적 보호인물에 대한 범죄의 방지 및 처벌에 관한 협약」 제2조, 「인질억류 방지에 관한 국제협약」제1조, 「폭탄테러행위의 억제를 위한 국제협약」 제2조, 「항공기의 불법납치 억제를 위한 협약」 제1조, 「민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약」 제1조, 「1971년 9월 23일 몬트리올에서 채택된 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약을 보충하는 국제민간항공에 사용되는 공항에서의 불법적 폭력행위의 억제를 위한 의정서」 제2조, 「항해의 안전에 대한 불법적 행위의 억제를 위한 협약」 제3조, 「대륙붕상에 소재한 고정플랫폼의 안전에 대한 불법적 행위의 억제를 위한 의정서」 제2조, 「핵물질의 방호에 관한 협약」 제7조에 규정된 행위의 어느 하나에 해당하는 행위"로 규정하고 있다(김태민, 2009: 178). 국제적으로 정립된 '테러'의 개념은 없다고 할 수 있으나 미국·일본·영국·독일 등 각국의 대테러 관련법 또는 국제협약 등이 정의한 내용을 보면 대체로 ① 정치적 목적이나 동기를 가지고 있다(범죄조직과 구별) ② 미리 계획되고 지속성을 가진 사건이다(시위 등 우발적 폭력 제외). ③ 공포심을 수반한 폭력의 사용이나 위협이 따른다(총격·폭파·납치 등)는 공통되는 요소를 내포하고 있다. 또 국가대테러활동지침(82.1.21 제정, 대통령 훈령 제47호)은 각국에서 규정하고 있는 보편적 정의를 준용하여 "테러란 정치적·사회적 목적을 가진 개인이나 집단이 그 목적을 달성하거나 상징적 효과를 얻기 위하여 계획적으로 행하는 불법행위"로 정의하고 있다(국가정보원, http://www.nis.go.kr/svc/affair.do?method=content&cmid=11312, 2012.11.15.검색)

미국은 정부정책의 문제로서 테러리즘에 대한 단일정의를 채택하지 않고, 대신 이따금씩 정부기관에 의해서 개발된 개념들에 의존한다. 이러한 개념들이 형사범들과 테러리즘을 구별하는 미국의 전통적인 법집행 접근방법을 반영한다. 다음은 테러리즘에 관한 공식적인 접근방법의 사례이다(Martin, 2011: 10). 미 국방부(The U. S. Department of Defence)는 테러리즘을 "정부나 어떤 사회에 강요하거나 위협하기 위하여 또는 종종 정치적, 종교적, 이데올로기적 목표를 달성하기 위하여 사람이나 재산에 가해지는 불법적인 폭력과 힘의 사용"이라고 정의하고 있고, 미국 FBI는 테러리즘을 "정치적 또는 사회적 목표를 달성하기 위해 정부, 시민, 단체 등에 강요하거나 협박하기 위해 사람이나 재산에 가해지는 불법적인 힘과 폭력의 사용"이라고 정의한다. 또한 미 국무부는 테러리즘을 "주로 일반 대중들에게 영향을 주기 위해 의도된 집단이나 은밀한 대리인들에 의해서 비전투적인 목표물에 대해 가해지는 사전에 계획된 정치적 폭력"이라고 정의하고 있다. 이와 같은 개념들을 종합하여 미국의 테러리즘에 대한 통합적인 개념모델을 제시하면 테러리즘이란 "사람과 재산에 가해지는 위협적인 힘과 폭력의 사용으로 사전에 계획되고 불법적인 행동이다. 또한 정치적인 목적을 중심으로 정책이나 행동에 영향을 미치도록 정부나 사람들에게 의도된 협박을 가하는 행동이다"(Martin, 2011: 10).

가장 최근에 테러리스트들이 공격하는 방법의 하나가 바로 사이버 테러[2]이다. 사이버 테러는 "보다

2) 사이버테러에 대한 개념은 다양하게 정의된다. 국가사이버안전매뉴얼(2005)에서는 '특정한 정치·사회적 목적을

정치적 또는 이데올로기적 목표를 달성하기 위하여 다른 사람들을 해치고, 강요하고, 위협하는데 목표를 둔 정보기술 및 컴퓨터의 사용 또는 파괴"이다(Bullock, Haddow, Coppola, & Yeletaysi, 2009: 201). 사이버(Cyber)란 '키잡이'란 뜻이며, 통신기술과 컴퓨터 시스템 제어를 총괄하는 용어인 사이버네틱스에서 파생된 단어이다. 통신망의 발달과 더불어 고성능 컴퓨터의 개발은 인터넷의 세계적 보급과 함께 정보화시대를 리드해 온 키잡이 역할을 했다. 개인이나 기업, 국가 간에 컴퓨터 네트워크 시스템으로 연결되는 '전자적 공간'을 '사이버 공간'이라고 부른다(이갑헌, 2010: 321). 미국 연방수사국(FBI) 산하 국가인프라보호센터(NIPC)가 2002년 발표한 자료에 의하면 "사이버테러는 정부를 위협하여 정책을 변경시킬 목적으로 컴퓨터를 이용해 폭력, 사망, 파괴를 초래하여 공포감을 조성하는 계획적 행위"라고 정의하고 있다(이갑헌, 2010: 324). 인터넷은 상업적, 사적, 정치적인 관심을 사람들과 교류하는 기회로 활용하게 되었고, 극단주의자들의 인터넷 사용은 현대사회의 보편적 특징이 되었다. 정보기술은 끊임없이 발전되었고, 뉴테러리즘의 중심에 있다. 이런 점에서 사이버 테러리즘은 미래의 테러리스트 환경의 중심에 자리잡을 것이다(Martin, 2011: 305).

사이버 테러리스트들은 최소의 비용과 다칠 위험과 적발의 위험으로 자신들 스스로 어디든지 공격할 수 있다. 게다가 그들은 암호를 이용하여 자신들의 행적을 감출 수 있으며, 이 암호화는 테러리스트들 사이에서 보다 안전한 커뮤니케이션을 가능하게 한다(Purpura, 2007: 61; Denning, 2001). 사이버 테러리스트들이 다른 해커들보다 사악하고 파괴적이라 하더라도 이 모든 것은 컴퓨터 시스템을 침투시키는 기본적인 방법에 의존한다(Vatis, 2003: 249).

미국 등 정보화 선진국에서 인터넷과 같은 범세계적 컴퓨터 통신망을 이용한 각종 범죄 단체의 테러 위험성이 현실화되고 있기 때문에 사이버 테러 또는 사이버 테러리즘이 지구촌의 새로운 공동 관심사로 부상하고 있다. 세계 각국에 컴퓨터 통신망이 광범위하게 보급되어 있으며, 이를 이용한 정부기관이나 공공 기관, 은행, 기업 등의 중요한 컴퓨터 데이터베이스 등 정보 시스템의 교란, 파괴 또는 악용 행위가 각종 테러리스트 집단의 목표 달성 수단이 될 것으로 관측되고 있다. 최근 등장하고 있는 사이버 테러의 주요 수법은 ㉠특정 기관의 컴퓨터에 집중적으로 전자 우편(e-mail) 메시지를 발송하여 수신 측의 전산망을 마비시키는 전자 우편 폭탄, ㉡컴퓨터 바이러스나 트로이 목마 등 파괴적인 프로그램이 삽입된 파일을 전자 우편 메시지에 첨부하여 발송하는 전자 편지 폭탄, ㉢특정 기관의 통상적 컴퓨터 프로그램에 중대한 과오를 발생시키는 루틴이나 부호를 무단으로 삽입하여 데이터를 파괴하거나 변조하여 예상치 못한 파국적 장애를 발생시키거나 부정 행위를 실행시키는 논리 폭탄(logic bomb) 등이다(한국정보통신기술협회 표준용어사전, 2012.11.10.검색).

사이버테러에는 사이버 공격을 포함하는데, 사이버 공격(cyber attack)은 목표물 컴퓨터 시스템의

가진 개인·테러집단이나 적성국 등이 해킹·컴퓨터바이러스의 유포 등 전자적 공격을 통해 주요 정보기반시설을 오동작·파괴하거나 마비시킴으로써 사회혼란 및 국가안보를 위협하는 행위'로 정의된다. 한국정보통신기술협회의 표준용어사전(2012.11.10.검색)에서는 사이버 테러리즘으로 '컴퓨터 통신망상에 구축되는 가상 공간인 사이버 공간을 이용한 폭력 행위를 가리키는 용어로, 컴퓨터 통신망을 이용하여 정부 기관이나 민간 기관의 정보 시스템에 침입, 중대한 장애를 발생시키거나 파괴하는 등의 범죄 행위'로 정의하고 있다.

기능을 파괴 또는 방해하거나 정보를 변조, 삭제, 훔치기 위해 사용되는 컴퓨터와 컴퓨터 사이의 공격을 말한다. 이러한 공격에는 세 가지 일반적인 유형이 있다(Vatis, 2003: 221).

첫째, 허가받지 않은 침입(unauthorized intrusion)으로서, 공격자들이 다양한 해킹이나 크래킹을 통해서 컴퓨터 시스템에 침입하거나 공식적이 허가를 받지 않고 네트워크에 접근하는 것을 말한다.

둘째, 파괴적인 바이러스나 웜을 말하는데, 이메일이나 자료교환 과정에서 네트워크의 중요한 부분에 손실을 일으키는 바이러스나 웜을 퍼뜨리는 것을 말한다.

셋째, 서비스 거부공격[3](Dos)으로서 관리자의 공식적인 권한이 없이도 특정서버에 처리할 수 없을 정도로 대량의 접속 신호를 한꺼번에 보내 해당 서버가 마비되도록 하는 해킹 기법이다.

2. 국내의 사이버테러

우리나라 인터넷 사용 인구는 2011년 7월 기준 약 3,718만 명으로 2000년 인터넷 도입 초기의 1,940만 명에 비해 약 2배 가량 증가하였고, 이 중 초고속인터넷 사용자는 2011년 기준 1,786만 명을 넘어섰다. 무선 인터넷과 스마트폰 보급의 확대로 트위터 등 '소셜 네트워크 서비스(Social Network Service)'가 대중화되어 우리 국민의 활동영역은 사이버공간까지 무한히 확장되고 있는 실정이다. 위와 같은 시대상을 반영하듯, 인터넷 매체의 익명성과 이동성을 악용한 해킹, 악성코드 유포, 인터넷상 명예훼손·도박개장·물품거래사기 등이 사회문제로 대두되고 있다(경찰청, 2012: 99-100). 이미 우리는 2009년 7월 정부 주요기관 사이트에 7·7 분산 서비스거부(DDoS : Distributed Denial of Service) 공격을 받아 국민들을 당황하게 한 바 있다. 국가주요기관에 사이버테러를 가한 것으로 서비스를 거부하게 하고 마비시켜 정부는 물론 국민들을 혼란에 빠뜨리게 한 것이다.

경찰청에서는 사이버범죄를 사이버테러형범죄와 일반사이버범죄로 구분하고 있다. 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 정보통신망 자체에 대한 공격행위를 통해 이루어지는 것은 사이버테러형범죄로, 전자상거래 사기, 프로그램 불법복제, 불법사이트 운영, 개인정보침해 등과 같이 사이버공간이 범죄의 수단으로 사용된 유형은 일반사이버범죄로 구분한다. 사이버테러형범죄는 해킹과 악성프로그램으로 구분하며, 해킹(Hacking)은 일반적으로 다른 사람의 컴퓨터 시스템에 무단 침입하여 정보를 빼내거나 프로그램을 파괴하는 전자적 침해행위를 의미한다. 해킹은 사용하는 기술과 방법 및 침해의 정도에 따라서 다양하게 구분된다. 경찰청에서는 해킹에 사용된 기술과 방법, 침해의 정도에 따라서 단순침입, 사용자도용, 파일 등 삭제변경, 자료유출, 폭탄스팸메일, 서비스거부공격[4]

---

3) DoS는 한 사용자가 시스템의 리소스를 독점하거나 파괴함으로써 다른 사용자들이 이 시스템의 서비스를 올바르게 사용할 수 없도록 만드는 것을 말한다. 컴퓨터에 침투 흔적을 남기지 않으며, 주로 시위의 목적으로 이용된다.

4) ①단순침입: 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입 하는 것 ②사용자 도용: 정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의 없이 사용하는 것 ③파일 등 삭제와 자료유출: 정보통신망에 침입한 자가 행한 2차적 행위의 결과로, 일반적으로 정보통신망에 대한 침입행위가 이루어진 뒤에 가능함 ④폭탄메일: 메일서버가 감당할 수 있는 한계를 넘는 많은 양의

으로 구분하고 있다. 악성프로그램은 정보시스템의 정상적인 작동을 방해하기 위하여 고의로 제작·유포되는 모든 실행 가능한 컴퓨터 프로그램은 악성프로그램으로 규정하고 이를 유포하는 행위를 처벌하고 있다. 악성프로그램은 리소스의 감염여부, 전파력 및 기능적 특징에 따라 크게 바리어스, 웜, 스파이웨어[5] 등으로 구분할 수 있다. 악성프로그램에 감염된 컴퓨터는 처리속도가 현저하게 감소하거나 평소에 나타나지 않았던 오류메시지 등이 표시되면서 비정상적으로 작동하기도 하고 지정된 일시에 특정한 작동을 하기도 한다(경찰청 사이버테러대응센터, 2012.11.10.검색).

<표 1> 국내 사이버 범죄 발생 검거현황

구 분	총 계			사이버테러형 범죄			일반사이버 범죄		
	발 생	검거		발생	검거		발생	검거	
		건수	인원		건수	인원		건수	인원
2008	136,819	122,227	128,635	20,077	16,953	17,649	116,742	105,274	110,986
2009	164,536	147,069	160,656	16,601	13,152	13,619	147,935	133,917	147,037
2010	122,902	103,809	111,772	18,287	14,874	16,777	104,615	88,935	94,995
2011	116,961	91,496		13,396	10,299		103,565	81,197	

※ 자료: 사이버경찰청 통계자료실(http://www.police.go.kr) ; 경찰청(2012: 100)의 재구성.

<표 2> 국내 유형별 사이버 범죄 발생 현황

구분	총계	사이버테러형범죄		일반사이버범죄					
		해킹	바이러스	통신사기 게임사기	명예훼손 성폭력등	개인정보 침해	불법사이트 운영	불법복제 판매	기타
2008	136,819	19,950	127	36,591	9,543	5,769	7,723	33,537	23,579
2009	164,536	16,558	43	41,644	8,640	4,516	29,589	36,768	26,778
2010	122,902	18,163	124	47,105	9,747	4,529	8,306	18,818	16,110
2011	116,961	13,253	143	48,755	8,882	3,160	6,908	17,161	18,699

※ 자료: 경찰청(2012: 100)의 재구성.

사이버 범죄는 2011년 총 116,961건이 발생하여 그 중 91,496건을 검거하였다. 유형별로 살펴보면 인터넷 사기(통신사기, 게임사기 포함)가 32,803건으로 가장 많았고, 불법복제(프로그램, 음란물 포함)가 15,087건, 해킹·바이러스가 10,299건, 명예훼손·성폭력이 7,848건으로 그 뒤를 이었다. 사이버 범죄는

메일을 일시에 보내 장애가 발생하게 하거나 메일내부에 메일 수신자의 컴퓨터에 과부하를 일으킬 수 있는 실행코드 등을 넣어 보내는 것. 서비스거부공격(정보통신망에 일정한 시간 동안 대량의 데이터를 전송시키거나 처리하게 하여 과부하를 야기시켜 정상적인 서비스가 불가능한 상태를 만드는 일체의 행위)의 한 유형(경찰청 사이버테러대응센터, 2012.11.10.검색).

5) ①트로이목마: 프로그램에 미리 입력된 기능을 능동적으로 수행하여 시스템 외부의 해커에게 정보를 유출하거나 원격제어 기능 수행. 트로이목마처럼 유용한 유틸리티로 위장하여 확산되기 때문에 마염사실 알아채기 어려움 ②인터넷웜: 시스템 과부하를 목적으로 이메일의 첨부파일 등 인터넷 이용하여 확산됨. 확산시 정상적인 파일이 이메일에 첨부되기도 하기 때문에 개인정보 유출의 위험 내포 ③스파이웨어: 공개프로그램, 쉐어웨어, 평가판 등의 무료 프로그램에 탑재되어 정보를 유출시키는 기능이 있는 모든 종류의 프로그램(경찰청 사이버테러대응센터, 2012.11.10.검색).

2000년 이후 증가추세에 있으며, 특히 2009년에는 불법 도박 사이트에 대한 대대적인 단속으로 검거 건수가 대폭 증가하였다(경찰청, 2012: 100). 또한 친북게시물 급증 등 사이버 안보위해행위가 증가하는 경향과 함께, 법원이 디지털 증거에 대한 엄격한 기준을 적용하는 공판중심주의를 강화함에 따라 경찰은 이에 적극 대응하기 위하여 여러 가지 방안을 마련하고 있다. 그 중 하나로 디지털 포렌식9 등 전문가 양성을 위한 각종 IT 심화교육을 실시하고 디지털 포렌식 장비의 기능을 개선하는 등 수사장비 고도화를 추진하여 보안사이버 수사역량을 강화시키고 있는 실정이다(경찰청, 2012: 248-249).

Ⅲ. 미국의 사이버테러에 대한 대응

1. 사이버테러의 등장 배경과 특징

폴 윌킨슨,(Paul Wilkinson) 브루스 호프먼(Bruce Hoffman) 등의 학자들을 포함해 미국에서는 테러리즘의 개념으로 '비국가 행위자에 의한 정치적 폭력'이라 규정하고 있다(김응수, 2012: 22). 테러리즘의 유형 중에서 사이버 테러리즘은 테러리스트들의 목적을 달성하기 위하여 해를 끼칠 방법으로서 사이버공간에 공격을 가하는 것이다. 최근에 정보기술, 전자통신, 인터넷 등의 광범위한 도입으로 인하여 사이버 공간은 테러리스트들에게는 매우 유혹적인 목표물이다. 공격 목표물에는 전기회로, 국제금융거래, 항공운항 통제, 상수도 기타 등을 파괴하는 것을 포함해서 끝이 없다. 이미 미국의 국가기간시설은 해커와 바이러스 등과 이미 전쟁 중이다(Purpura, 2007: 61). 정보 기술과 진보된 통신의 확산은 테러조직들을 네트워크화함과 동시에 사이버테러리즘이라는 신종 테러의 탄생을 불러온 요소로 작용했다. 또 신자유주의의 기조에서 진행된 세계화의 물결이 한 국가의 경제와 타국가의 재정구조가 상호 의존하는 관계를 형성해 국가의 취약성이 증대되었으며 이는 또 사이버공간에서도 같은 작용을 하여 사이버테러에 대한 국제적인 공조를 필연적으로 성립시키고 있다(박한나, 2012: 57).

사이버테러는 첨단 정보기술을 이용해 가상의 세계로 전환되어 있는 공간을 무차별적으로 공격하는 행위로, 그 피해가 엄청나게 방대하고 개인 및 기업부터 기간산업, 군사시설, 국제기구 등 다양한 형태의 공격대상을 선택할 수 있다는 특징을 갖는다(남길현, 2002: 165-167). 사이버테러는 세계 최강국임을 자처하는 미국에서도 예외가 될 수 없다. 사이버테러는 익명성이 보장되고 별도의 신분위장을 필요로 하지도 않는다. 또 세계 전역에서 해커들이 네트워크를 활용하여 집단적 사이버테러를 자행하기도 한다.

미국의 유명서점인 반스 앤드 노블 등 유통회사 9곳 이상의 사이트에서 4,100만 명의 개인 신용정보가 도난당한 사상최대의 해킹 범죄가 발생했다. 미국당국이 적발 기소한 해킹 조직의 구성원을 보면 미국인 3명과 우크라이나인 3명, 중국인 2명, 에스토니아와 벨로루시인 각 1명 등 11명과 터키와 독일 등 다른 나라에도 용의자가 숨어있는 것으로 밝혀지기도 하였다(이갑헌, 2010: 323).

문재명(2011: 15)은 미국의 사이버테러 대응체계의 특징으로 사이버안보와 국가안보, 테러와 사이버

테러 등을 동일한 국가안보 체계하에서 수행한다는 것과 모든 국가조직의 역량을 통합으로 극대화하고 있고, 행정부와 법집행기구, 의회의 긴밀한 협조관계를 확립하고 있으며 중앙정부와 지방정부의 역할, 또 기능적으로는 정보의 공유와 사고보고 및 대응조치 활동 기능을 강화하여 정부나 기업은 물론 국민 개개인에게 까지 역량이 미칠 수 있도록 하고 있다고 평가하고 있다.

2. 미국 사이버테러 대응법규

미국의 사이버테러관련 대응법규와 관련하여 백광훈(2001: 141-157)은 다음과 같이 서술하고 있다.

미국 연방의회는 컴퓨터에 의해 범해지는 범죄유형을 포괄하기 위해 1993년 보안법(Securities Act of 1993)을 개정하였고, 새로운 컴퓨터 사기와 남용에 관한 종합적인 장을 연방법에 신설하고자 연방형법전(United State Code Title 18 - Crimes and Criminal Procedure)을 개정한 바 있다. 이것은 컴퓨터범죄에 대응하는 가장 중요한 법률로서 1986년 제정되고 1996년에 개정된 제1030조의 컴퓨터남용·오용법(CFAA : Computer Fraud and Abuse Act)이다. 1998년에는 연방법 121장의 제2701조의 전자통신프라이버시보호법(Electronic Communications Privacy Act)이 개정되었고, 이는 사이버범죄의 수사와 관련하여 의미있는 개정으로서 제2701조로 준용되어 있는 제2703조는 일정한 요건 아래 연방정부에 의한 네트워크 엑세스를 허용하는 것이고 네트워크상의 수사에 관련하는 조문으로서 의미가 있다(백광훈, 2001: 142). 연방정보와 정보시스템 보안에 관한 법률로서 1986년 '컴퓨터 사기 및 남용에 관한 법(Computer Fraud and Abuse Act)'을 필두로 1987년의 '컴퓨터보안법(Computer Security Act)', 1988년의 'Warner 개정법(Warner Amendment to the Brooks Act)을 제정하였고, 1993년 행정명령(EO: Executive Order) 12864 즉, NII 구축을 위한 IITF(Information Infrastructure Issue Form)를 발표하였으며, 동년 '정부프로그램수행과 결과평가법(GPRA: Government Performance & Result Act)을 제정하였으며, 1995년에는 대통령지시사항(PDD: Presidential Decision Directive) 39 즉 테러대응정책(Counter-Terrorism Policy)을 공포하였다. 1996년에는 테러리즘방지 및 사형법(AEDPA: Antiterrorism and Effective Death Penalty Act)을 제정하였다. 국가기반구조보호센터(NIPC)의 전신인 국가기관은 FBI가 1996년 국가안보에 위협적인 잠재적 취약요소를 해결하기 위해 설립한 '사이버범죄수사 및 기반구조위협평가센터(CITAC: Computer Investigations and Infrastructure Tree Assessment Center)이다. 1998년에는 국가정보기반보호법에 의거하여 FBI를 중심으로 이루어진 '국가기반구조보호센터(NIPC: National Infrastructure Protection Center)'를 발족시켰다. NIPC는 컴퓨터수사·운용섹션(CIOS), 분석·경고섹션(AWS), 그리고 훈련·협력촉진·전략섹션(TOSS)으로 구성되어 역할을 수행한다. 2000년에는 급증하고 있는 컴퓨터·인터넷을 이용한 사기행위에 대처하기 위해 FBI와 법무부 그리고 NW3C(National White Collar Crime Center)가 공동으로 IFCC(Internet Fraud Complaint Center)를 설치하여 컴퓨터사기행위로부터 피해를 당한 사람이면 누구나 인터넷상으로 피해신고를 할 수 있도록 하는 시스템을 마련하였다(백광훈, 2001: 150-155).

미국의 사이버테러관련 법체계들은 국토안보 전략, 관련법, 대통령 명령, 그리고 이를 실행하기 위

한 국가계획으로 구성된다. ① 국토안보전략으로서는 국토안보 국가전략, 사이버공간 보호를 위한 국가전략(사이버공간을 통한 주요 기반시설 위해요소 식별 및 이에 대응할 수 있는 전략을 제공하고 주요 기반시설 및 주요 자산에 대한 사이버공격 예방을 위한 사이버안전 대응 시스템 개발 등), 정보공유를 위한 국가전략, 대테러 국가전략 등이 있다. ② 관련법은 국토안보법, 테러방지법(2001), 연방정보보안관리법(FISMS), 주요기반시설정보법(2002), 사이버보안 연구개발에 관한 법(2002, 컴퓨터 네트워크보안 및 지원 연구인원과 훈련을 강화하여 연구개발을 촉진하기 위한 법), 정보개혁테러예방법(2004), 9·11위원회 권고사항 실행법(2007) 등이 있다. ③ 대통령 명령은 HSPD-1, 3, 5, 7, 8, 20, 23 등이 있다. 여기서 HSPD-23은 포괄적 국가 사이버보안 전략(CNCI)을 구현하기 위해 기존 취약점 해소, 침입방지 등의 지속적 노력을 통한 전방위적 방어태세 구축을 정의하고 첩보능력 활용, 공급망 보안강화, 기술개발 및 교육강화, 최신 선도기술 투자를 위한 미래 환경구축 등을 규정하고 있다. ④ 국가계획은 국가사고관리시스템(NIMS), 국가기반보호계획(NIPP), 국가대응계획(NRP), 국가대응프레임워크(NRF) 등이 있다(서현준, 2009: 8-11; 정재영, 2010: 48-50).

3. 미국 사이버테러에 대한 대응 조직과 시스템

2001년 9월 11일, 미국은 세계무역센터의 쌍둥이 빌딩에 충돌한 무시무시한 비행기의 이미지에 잠이 깼다. 45분 내에 쌍둥이 빌딩은 잿더미로 변했으며, 2752명이 사망하였다. 미국은 조지 부시 대통령에 의해 테러의 위협으로부터 자신을 보호하는 길에 들어서게 되었다. 2001년 9월 20일 조지 부시 대통령은 의회에서 다음과 같이 연설하였다. "9월 11일, 자유에 대한 적들이 우리나라(미국)에 전쟁의 행동을 저질렀습니다. 미국인들은 지난 136년 동안 1941년 어느 일요일[6]을 제외하고 외국 땅에서 전쟁을 해온 것을 알고 있습니다. 또한 미국인들은 평온한 오전의 위대한 도시 중심부가 아닌 전쟁의 사상자들을 알고 있습니다."(Campos, 2007: 1). 9·11테러는 2001년 9월 11일 알카에다에 의해 저질러진 일련의 조직적이고 통합된 자살 공격이다. 11일 아침에 19명의 테러리스트들이 4대의 민간항공기를 납치하여 의도적으로 세계 무역 센터의 쌍둥이 빌딩을 두 대의 비행기가 충돌했고, 또 다른 한 대는 버지니아 주 알링턴에 있는 펜타곤 건물에 충돌했으며, 나머지 한 대는 미국 수도 워싱턴DC로 향하던 중 펜실베니아 시골 Shanksville벌판에 추락하였다(윤민우, 2011: 137). 이와 같이 미국인들은 미국 역사 이래 자국의 땅이 공격당한 것은 처음이라는 사실에 자존심을 상했으며, 자국 영토가 이제 더 이상 테러로부터 안전하지 않다는 사실을 인식하기에 이르렀다.

9·11테러 공격에 대해 미국은 사전예방정보 활동과 사후 복구 및 수사활동을 체계적으로 총괄할 기구의 부재를 절감했다. 9·11진상조사위원회는 정보기관 상호 간의 정보교류, 종합적인 분석정보 도출의 실패를 인식하고 부시 행정부에게 테러문제에 대한 종합적 대처기구 창설을 권고했으며, 이에 따

6) 미국은 이전에도 국제 테러리즘의 목표물이 되어 왔으나, 자신의 영토에서 이 정도 규모의 공격을 받은 것은 처음이다. 이와 유사한 역사적 사건은 1941년 12월 7일 하와이 진주만 해군기지에 대한 일본의 공격이었다(Martin, 2011: 43).

라 부시대통령은 2003년 5월 1일 대통령령 제13,354호를 발령하여 CIA 내에 테러위협정보센터(Terrorist Threat Intelligence Center)를 설치했다. 이후 2004년 미 의회는 대통령 명령에 의해 CIA 내의 부처 수준으로 운영되던 테러위협정보센터를 정보개혁과테러방지법(IRTPA)에 명문화하여 법적 기구로 격상하고, 이를 국가정보국장(DNI)산하에 배속했다. 이것이 2004년 창설된 국가테러대응센터(NCTC)이다. 9·11테러 공격 후 미국과 북대서양조약기구(NATO) 연합국은 알카에다 조직을 지원하는 것으로 의심되는 아프가니스탄을 상대로 전쟁을 개시했으며, 이에 아랍권 일부에서는 "사이버 지하드(Cyber Jihad)"를 조직하여 미국에 대해 사이버테러 공격을 감행할 것이라고 선언하기도 했다(한희원, 2011: 373, 401).

2009년 10월부터는 각종 사이버테러 대응 및 IT인프라 보호를 위해 정부 기관들의 사이버 안보기능을 통합하는 '사이버보안·커뮤니케이션 통합센터(NCCIC)'를 개소해 운영 중으로 사이버테러 대응과 관련해 정부와 민간 전문가들 사이의 조정자 역할을 수행하고 있다(김연준·옥정석, 2011: 61).

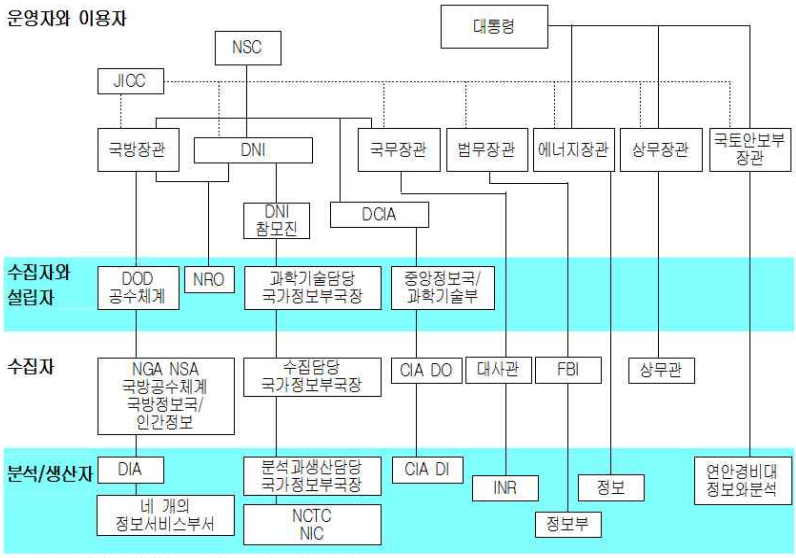
미국 공공시설을 목표로 한 사이버 공격이 지난 3년간 17배 급증했다고 뉴욕타임스(NYT) 인터넷판이 2012년 7월 26일 미 국가안보국(NSA)을 인용해 보도했다. 이 보도에 따르면, 키스 알렉산더 NSA 국장은 2009~2011년 전력망과 수도 공급, 컴퓨터 및 휴대전화망 등 공공시설을 목표로 한 범죄집단, 해커, 다른 나라들의 사이버 공격이 급증했으며, 사이버 공격이 금융범죄나 컴퓨터 스파이 보다 위험하다고 강조했다(연합뉴스, 2012. 7. 27).

사이버테러는 일반시민들, 지방공무원들, 언론, 경찰 및 소방관 등 위기초기 대응자들에 대한 상당한 교육투자가 필요하다. 특히, 교육 및 훈련에 대한 투자뿐만 아니라 보안장비, 전문화된 기술역량, 국민보건 네트워크 등이 중요하다(Bullock, Haddow, Coppola & Yeletaysi, 2009: 205).

미국의 연방정부는 수십 년간 자국의 정보 인프라를 구축하기 위해서 많은 자원을 투자해왔다. 1960년대에 정부출연기관에 근무하는 연구원들은 핵공격에도 생존할 수 있는 커뮤니케이션 시스템을 미국 군대에 제공하는데 목표를 둔 연구 프로젝트에서 인터넷에 필수적인 패킷 스위칭(packet switching) 기술을 개발하였다. 또한 1990년대 중반에는 사이버테러에 대해 집중적인 연구를 시작하였다. 1995년 오클라호마 도시 내 연방정부 빌딩 폭파사건[7]에 의해서, 클린턴 행정부는 국가의 중요국가시설의 위험성을 평가하고, 이를 방어할 수 있는 방법을 만들어 대통령에게 보고하게 되었다. 여기서 CIWG(Critical Infrastructure Working Group)이 만들어졌다. CIWG는 모든 수준에서의 정부가 순

7) 1995년 4월 19일 오전 9시 5분, 미국 중부 오클라호마 주의 주도 오클라호마시티 중심가에 있는 알프레드 머라 빌딩에서 폭탄 테러 사건이 일어났다. 9층짜리인 이 건물에는 마약단속국 등 미국 연방정부의 각 기관 사무실과 탁아소 등이 들어 있었다. 이 폭발로 건물은 완전히 파괴되었고 폭발 지점에는 폭 10m, 깊이 2.45m의 큰 구덩이가 패었다. 공무원들이 출근한 시간에, 탁아소가 있는 건물을 택한 점으로 미루어 보아 범인이 테러에 대한 선전효과의 극대화를 노렸다는 점이 주목되었다. 또 사고 당일은 바로 2년 전 사교집단인 다윗파의 방화 자살 사건 날짜와 같다는 점이 중요한 단서였다. 맥베이는 사건 발생 2년 전 텍사스에서 집단 자살한 사교집단 다윗파에 대한 연방정부의 불만족스러운 처리 때문에 범행을 저질렀다고 밝혔다. 이 사건으로 168명이 죽고, 600여 명이 부상당했다(두산백과, 2012.11.8).

조로운 기능을 수행하고, 미국의 국방 및 경제안보에 필수적인 재화와 서비스의 계속적인 공급을 하는 상호의존적인 시스템과 네트워크라고 할 수 있다. 여기서 중요한 것은 국가중요시설은 오클라호마 테러사고와 같이 물리적인 공격뿐만 아니라 중요한 서비스를 전달하기 위해 필요한 컴퓨터 네트워크에 대한 사이버 공격에 의해서도 치명적인 피해를 입을 수 있다는 것이다(Vatis, 2003: 239).



<그림 1> 미국의 다양한 정보공동체 : 기능적 분류

※ 자료: Lowental, 김계동 역(2008: 48).

부시 행정부는 연방의 국가기간시설을 보호하기 위한 조정과 정보시스템을 보호하기 위한 국가전략을 개발하기 위하여 PCITB(the President's Critical Infrastructure Protection Board)를 설립하였고, 민간부문과 공공부문의 협력을 중시하였다. 특히, 사이버테러 및 각종 테러를 효과적으로 예방하기 위하여 국토안보부(Department of Homeland Security)를 신설하였다(Vatis, 2003: 243). 국토안보부는 현재 20만여명이 넘는 직원으로 국방부(DOD), 원호부(VA : Department of Veterans Affairs)에 이어 행정부처 중 세 번째로 큰 부서이다(한희원, 2011: 498). 국토안보부(DHS : Department of Homeland Security)는 2001년 9월 11일 테러이후 2002년 11월 조지 W. 부시 미국 대통령이 사인한 '국토안보부 법안(Homeland Security Act of 2002)'에 의해 2003년 3월 정식 출범한 부처로(Bullock, Haddow, Coppola & Yeletaysi, 2009: 11), 테러방지관련 부서와 인력을 편입, 확대시킨 부처이다. 국토안보부는 미국 행정부 내의 각 부처에 분산된 대 테러, 위기관리 기능을 통합하여 효율적으로 위기를 관리하기 위해 설립되었다. 이 부처는 국경 경비, 재난대비 활동, 화생방 공격대비 활동, 정보 분석 등의 업무를 관할하며, 세관, 이민귀환국, 국경순찰대, 비밀경찰국, 연방비상계획처 등 기존의 조직을 흡수하였다.

국토안보부는 자신의 정보조직을 보유한 연안경비대 및 정보와 분석국(Office of Intelligence and

Analysis)과 같은 정보공동체의 일부인 여러 조직들을 보유하고 있다(Lowental, 김계동 역, 2008: 48). 국토안보부의 주요 임무는 테러리즘 예방 및 안전보장, 국경 안전 및 관리, 이민법 집행·관리, 사이버 공간 보호와 안전, 재난 대비·복구이다.

※ 자료: 서현준(2009); 정재영(2010: 52) 재인용.

<그림 2> 국가보호프로그램국(NPP) 조직도

또한 미국의 국토안보부 산하 기관인 국가사이버보안처(NCSD, National Cyber Security Division)는 효과적인 국가 사이버보안 대응시스템을 구축·유지하고, 국가중요 기반시설의 보호를 위한 사이버 위기관리 프로그램을 실행하는 두 가지 주요한 역할을 수행한다(Bullock, Haddow, Coppola & Yeletaysi, 2009: 203).

국가사이버보안처(NCSD)는 국토안보부의 부차관이 이끄는 국가보호 프로그램에서 사이버 공간과 미국의 사이버 자산을 보호하기 위해 공공부문, 민간부문, 국제적 조직과 상호협력을 수행하는 기관으로 사이버 위협 및 취약점을 식별·분석하여 위협을 감소시키고, 위협경보의 발령, 침해사고 대응 조정업무를 수행함과 동시에 연속성 및 복구계획을 수행하는데 기술적인 도움을 제공하고 있다. 국가사이버보안 대응시스템은 주요기반 보호를 위하여 24시간 7일 대응태세를 목표로 사이버 사고 발생시 취해야 할 행위를 결정하는 사이버 리더십, 프로세스, 프로토콜을 조정한다. 사이버위기관리 프로그램은 사이버 기반에 대한 위험을 평가하고, 자원을 분배하며 대응책을 마련하는 역할을 하고 있다(정재영, 2010: 51-52). 9·11테러 이후인 2006년 2월부터는 이 기관의 주도로 격년제로 실시하는 사이버 스톰(Cyber Storm)은 국가 차원의 사이버테러 대응훈련이다. 민·관·군이 참여하며, 매 훈련 때마다 2년 동안 새로 등록된 정부와 민간업체들이 추가로 훈련에 참가한다. 훈련은 주요 국가기반 시설(전력·통신·교통 등)을 공격한 뒤 공공기관이나 기업의 대응 속도를 확인하는 방식으로 이뤄진다.

최초로 실시된 사이버 스톰은 2006년 2월 6일부터 10일까지 정부주도로 대규모의 국가 사이버보안

훈련으로 실시되었는데, 공공, 민간, 국제기관 및 단체, 회사 등 110개 이상의 단체들이 사이버 스톰의 계획 및 실행단계에 참여했으며, 사이버 공격에 대응하기 위하여 정보기술(IT), 통신, 에너지, 교통부문 시스템을 보호하는 훈련을 실시했다.

사이버 스톰훈련은 전력, 수도, 금융 등 기간산업과 정부기관을 겨냥한 사이버테러에 대응하는 대규모 훈련으로 국토안보부 주도로 국방부, 상무부, 법무부, 재무부, 국가안보국(NSA) 등 정보, 사법 당국과 함께 11개 주정부와 12개국의 60개 민간기업(정보기술, 통신, 화학, 전기, 교통관련 업체) 등이 참가하는데 사이버보안·커뮤니케이션 통합센터(NCCIC)가 컨트롤타워 역할을 하고 있다(김연준·옥정석, 2011: 61-62). 사이버 스톰은 다양한 사이버공격에 대응하여 커뮤니케이션, 정책, 절차 등을 테스트해 보는 기회로 만들어졌고, 아울러 추가적으로 필요한 기획과 과정들은 무엇이 있는지를 알아보는 것이 주요 목적이다.

여기에는 다음과 같은 내용들이 포함된다.

- 사이버테러 대응기관간의 조정
- 정부간, 정부 내 다양한 기관간의 조정 및 대응
- 사이버 보안을 지지하거나 방해하는 요소들의 파악
- 사이버 및 물리적 기반시설의 상호의존성 확인
- 주요한 사이버테러와 관련된 경제적, 국가적 보안에 대한 인식제고
- 사이버 사고 대응 및 복구를 위한 도구와 기술 진작(Bullock, Haddow, Coppola & Yeletaysi, 2009: 203).

미국 언론들은 9·11테러 이후 잠재적 가능성이 가장 높은 테러공격 방법으로 사이버테러를 지목하고 있다. 미국에 적대적인 국제 테러조직이 국가 기간시설망에 대한 사이버 공격을 감행해서, 원자력발전소 등의 오작동으로 방사선 누출을 야기하거나 또는 원자력발전소 자체 폭발을 야기한다거나, 가스 유출, 발전 장치 손상, 열차 선로의 충돌 야기, 항공 제어시스템의 오작동으로 국가기간시설망에 엄청난 손상과 파괴를 초래하거나, 컴퓨터 시스템의 오작동을 야기하여 국가경제에 대혼란을 초래하는 등 사이버테러를 가장 위험스럽게 예측하고 있다(한희원, 2011: 408-409).

현재 미국에서는 이러한 사이버테러 방지를 위해 제도적으로 많은 시행착오를 겪으며, 꾸준히 좀 더 나은 대응책 마련에 부심하고 또 노력하고 있다.

IV. 결론 및 제언

미국 뉴욕의 9·11 테러 발생 이후 각 국가 마다 자국의 안전을 핵심적인 정책과제로 채택해 대테러 방지대책 마련에 심혈을 기울이고 있다. 여기서 우리가 간과해서는 안 될 중요한 부분이 있다. 그것은 바로 향후 테러집단들이 활용할 가능성이 높은 방법 중의 하나가 '사이버테러'라는 것이다. 이와 같은 사이버테러는 유비쿼터스의 과학기술을 이용한 신종테러방식이다.

간단한 사례로서 사이버 상으로 병원 응급실에 입원 중인 중요 인물의 의료전산기록 중에서 혈액형 한 글자만을 고의로 변경해서 살해한다든지 인공호흡기를 멈추게 하는 것 등을 생각해 볼 수 있다. 또한, 착륙하려는 비행기의 레이더에 침투해 교란시키는 테러 유형도 있을 수 있다. 이와 같이 테러범들이 사이버테러 방식을 선호하게 되는 이유는 폭탄 설치나 인질납치 같은 종래의 방식 보다 인터넷으로 공격 대상에게 손쉽게 침투할 수 있기 때문이다(박동균, 2009b: 55-66). 사이버테러는 최근 들어 주요한 위협으로 나타난 재난이다. 이는 해마다 한 국가나 세계가 정보기술, 컴퓨터, 인터넷의 성장에 의존하는 함에 따라 더욱 심각성이 증대되고 있다. 이러한 의존성은 경제성장 엔진에서부터, 중요국가기반시설(통신, 전력발전, 물 공급, 교통 등) 심지어는 군대 통제에 이르기까지 사회의 모든 부분에 실제적으로 존재한다. 사이버 보안 또는 사이버 테러리즘은 1980년 이후에 미국군과 FBI를 포함하여 정부와 민간부문에 관심을 끌기 시작하였다. 특히, 9·11 테러 이후에 테러위험으로서 사이버보안이 국토안보부의 국가관심 사항으로 대두되었다(Bullock, Haddow, Coppola & Yeletaysi, 2009: 203).

미국의 국가사이버보안처(NCSD)는 사이버테러와 관련하여 국가 사이버보안 대응시스템을 구축하고, 국가중요 기반시설의 보호를 위해 사이버위기관리프로그램을 효과적으로 실현하고 있다. 2006년부터는 격년제로 국가적 차원에서 사이버 스톰(Cyber Storm)이라는 사이버테러 대응훈련을 국가사이버보안처 주도로 실시하고 있다. 여기에는 민・관・군이 합동으로 참여하며, 2년 동안 새로 등록된 정부와 민간업체들이 추가로 훈련에 참가한다. 훈련의 방식은 주요 국가기반 시설을 공격한 뒤 공공기관이나 기업이 사이버테러에 대응하는 절차와 속도를 확인하게 된다.

사이버 스톰은 다양한 방법으로 공격되는 사이버테러에 대응하여 커뮤니케이션, 정책, 절차 등을 테스트해 보는 기회로 만들어졌고, 추가적으로 요구되는 기획과 과정들을 찾아보는 것이 주목적이라 할 수 있다. 여기에는 사이버테러 대응기관 간의 조정, 정부 간 혹은 정부 내 다양한 기관간의 조정 및 대응, 사이버 보안을 지지하거나 방해하는 요소들의 파악, 사이버 및 물리적 기반시설의 상호의존성 확인, 주요한 사이버테러와 관련된 경제적, 국가적 보안에 대한 인식제고, 사이버 사고 대응 및 복구를 위한 도구와 기술 진작 등이 포함되고 있다.

학자들은 사이버테러야 말로 적은 비용으로 최대의 타격을 줄 수 있는 전략으로 입을 모으고 있다. 사이버전에 대한 완벽한 대책을 마련해야만 국가적인 평화를 도모할 수 있는 것이다. 특히 2009년 미국과 한국을 대상으로 동시다발적으로 발생한 “분산 서비스 거부(DDoS)”공격의 배후로 북한이 지목됨을 계기로 북한에 의한 테러리즘 가능성이 대두되고 있는 상황이다. 특히 이 사건의 직접적 당사자인 북한이 사이버 테러리즘을 감행하였다는 직접적인 증거가 국가정보기관에 의하여 밝혀짐으로써 북한에 의한 사이버 테러리즘의 가능성이 높아진 것이다. 이러한 북한이 600여명 규모의 해킹전문요원을 양산하고 있으며 이들이 중국 등 해외 여러 국가에서 사이버테러를 준비하고 있다(박동균, 2009b: 55-66).

따라서 북한의 사이버테러의 능력정도를 판단하고 그들의 사이버테러에 대한 대책을 마련해야 할 것이다. 더하여 우리나라는 전 세계적으로 유일한 분단국가이며, 북한이라는 특수한 관계 속에 있다.

테러로부터 안전지역이 아니라는 것이다. 또한 세계최고의 인터넷 강국이면서도 정보 보안 의식은 매우 낮고, 실제로 관련 조직과 예산, 전문 인력이 부족하다. 사이버 테러에 가장 효과적인 방법은 사이버 보안을 가장 중요한 가치로 인정하는 것이다.

사이버테러 학자들은 한국에서 사이버테러 대응체제 구축방안으로 마국 국토안보부와 같은 기능을 총괄·조정하고 기능을 통합할 수 있는 컨트롤타워의 설치, 위기상황에서 신속하고 효과적으로 대응할 수 있도록 정보 수집·전파의 체계 구축, 단일화된 법률의 제·개정과 사이버테러 대응 시스템의 체계적인 정비, 인터넷 등 네트워크의 견고성 및 방어력 고취, 국가기반시설별 보호프로그램 마련, 국민들의 인식 전환 등을 요구하고 있다. 그리고 세계적으로도 사이버 테러로부터 안전을 확보하기 위하여 패스워드 및 암호화 시스템의 사용 등 사이버테러 방어시스템의 구축과 정보 시스템의 보안 대책을 강조하고 있다.

요컨대 정부는 미국과 같이 체계화된 제도의 도입과 정비는 물론 사이버테러에 대응하기 위한 인적, 물적 자원을 확보하고, 사이버 테러리스트들에 대한 수사와 기소에 있어 공식적·비공식적 사이버 국제협력을 강화시켜야 하며, 국가중요시설 및 기반시설에 대한 보호를 위해 투자를 아끼지 말아야 한다.

참고문헌

경찰청. 2012. 2012 경찰백서. 서울: 경찰청.

김연준·옥정석. 2011. 국가위기관리를 위한 사이버테러 대응체계 구축방안. 인문사회논총(용인대학교). 18: 43-71.

김열수. 2005. 21세기 국가위기관리체계론. 서울: 오름.

김응수. 2012. 글로벌 테러리즘. 서울: 한울 아카데미.

김태민. 2009. 뉴테러리즘 대응을 위한 지방자치단체와 민간경비의 정책과제. 한국지방자치연구. 11(2): 175-193.

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

문재명. 2011. 국가안보를 위한 사이버테러 대응방안 연구. 한국테러학회보. 4(2): 5-32.

박동균. 2008. 테러리즘에 대비한 한국 민방위제도의 발전방향. 대테러연구. 31: 201-223.

박동균. 2009a. 한국의 테러리즘 발생 가능성과 국가대비전략. 한국테러학회보. 2(1): 81-111.

박동균. 2009b. 북한의 사이버 테러공격 가능성 및 대비전략. 국가위기관리학회보. 1: 53-66.

박한나. 2012. 사이버테러리즘의 등장 배경에 대한 연구. 숙명여자대학교 국제대학원. 석사학위논문.

백광훈. 2001. 사이버테러리즘에 관한 연구. 한국형사정책연구원 연구보고서01-07.

서현준. 2009. 해외 사이버안전 체계. 국가보안기술연구소.

윤민우. 2011. 테러리즘의 이해와 국가안보. 인천: 진영사.

이갑헌. 2010. 첩보에서 정보까지. 서울: 형성출판사.

이창용. 2005. 테러리즘 방지를 위한 한국형 위기관리시스템 구축방안. 지방정부연구. 9(2): 204-226.

이헌경. 2003. 테러의 본질과 한국의 대테러 방향. 통일전략. 3(1): 341-360.

이황우. 2011. 테러리즘. 파주: 법문사.

장석헌. 2005. 국가중요시설의 대테러방안에 관한 연구. 한국민간경비학회 학술세미나 발표논문집.

정기석. 2012. 최근의 사이버테러에 대한 대응방안. 정보·보안논문지. 12(1): 89-96.

정 웅. 2011. 북한 테러억제를 위한 효과적 전략물자 수출통제체제 구축방안. 대테러정책 연구논총. 8: 373-420.

정재영. 2010. 사이버 테러에 관한 국가별 대응실태 연구 : 한국에 대한 함의 도출을 중심으로. 국민대학교 정치대학원 석사학위논문.

채재병. 2004. 국제테러리즘과 군사적 대응. 국제정치논집. 44(2): 55-74.

최선우·류채형. 2012. 북한의 사이버 테러리즘에 관한 연구. 한국공안행정학회보. 46: 213-239.

최진태. 2006. 테러리즘의 이론과 실제. 서울: 대영문화사.

한희원. 2011. 국가정보학원론. 서울: 법률출판사.

연합뉴스. 2012. 7. 27.

Branscomb, Lewis M. 2001. *Cyber-attacks as Amplifier in Terrorist Strategy in Committee on Counterterrorism Challenge for Russia and the United States, Terrorism - Reducing Vulnerabilities and Improving Responses.* Washington, D. C.: The National Academics Press.

Bullock, Jane, George Haddow, Damon Coppola, and Sarp Yeletaysi. 2009. *Introduction to Homeland Security - Principles of All-Hazards Response.* Amsterdam: Elsevier.

Burns, Vincent and Dempsey Peterson. 2005. *Terrorism - A Documentary and Reference Guide.* Westport, CT and London: Greenwood Press.

Campos, H. Joseph. 2009. *The State and Terrorism: National Security and the Mobilization of Power.* Ashgate.

Caulkins, Jonathan P., Mark A. R. Kleiman, and Peter Reuter. 2003. Lessons of the War on Drugs for War on Terrorism. in Arnold M. Howitt & Robyn L. Pangi. eds. *Countering Terrorism: Dimensions of Preparedness.* Cambridge: The MIT Press.

Clark. Ben. 2008. Effective Counter-Terrorism: Sound Foreign Policy, Intelligence Gathering, Social Engineering and Necessary Use of Force. in *Responding to Terrorism.* ASHGATE.

Committee on Counterterrorism Challenge for Russia and the United States. 2001. *Terrorism: Reducing Vulnerabilities and Improving Responses.* Washington, D. C.: The National

Academics Press.

Denning, D. 2001. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. in Arquilla and Ronfeldt. eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica, CA: RAND.

Fromkin, N. 1992. The Strategy of Terrorism. *Foreign Affairs*. 53(July): 692-693.

Heymann, Philip B. 2003. Dealing with Terrorism after September 11, 2001: Overviews in Arnold M. Howitt & Robyn L. Pangi. eds. *Countering Terrorism: Dimensions of Preparedness*. Cambridge: The MIT Press.

Arnold M. Howitt & Robyn L. Pangi. 2003. *Countering Terrorism: Dimensions of Preparedness*. Cambridge: The MIT Press.

Imre, Robert, Brian Mooney, and Benjamin Clarke. 2008. *Responding to Terrorism*. ASHGATE.

Law, D. Randall. 2009. *Terrorism: A History.* Cambridge: Polity Press.

Mark M. Lowental. 김계동역. 2008. 국가정보: 비밀에서 정책까지. 서울: 명인문화사.

Martha Crenshaw & John Pimlott. eds. 1998. *International Encyclopedia of Terrorism.*

Martin, Cus. 2011. *Essentials of Terrorism: Concepts and Controversies*. 2nd eds. LA: SAGE.

Matusitz, Jonathan. 2005. Cyberterrorism.. *American Foreign Policy Interests*. 2: 137-147.

Purpura, Philip. 2009. *Terrorism and Homeland Security: An Introduction with Applications*. Amsterdam: Elsevier.

Ronczkowski, Michael R. 2004. *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*. New York: CRC Press.

Silke, Andrew. 2011. *The Psychology of Counter-Terrorism*. London and New York: Routledge.

Vatis, Michael A. 2003. Cyber Attacks: Protecting America's Security against Digital Threats. in Arnold M. Howitt & Robyn L. Pangi. *Countering Terrorism: Dimensions of Preparedness*. Cambridge: The MIT Press.

Wardlaw, Grant. 1994. *Political Terrorism: Theory and Counter-Measure*. 3rd ed. New York: Cambridge University Press.

Williamson, Myra. 2009. *Terrorism, War and International Law: The Legality of the Use of Force against Afghanistan in 2001*. Ashgate Publishing.

Wilkinson, Paul. 1986. *Terrorism and the Liberal State*. 2nd ed. New York: New York University Press.

Wilkinson, Paul. 2001. *Terrorism versus Democracy: The Liberal State Response*. London: Frank Cass.

Zimmermann, Doron & Andreas Wenger. 2007. *How States Fight Terrorism: Policy Dynamics in*

the West. London: Lynne Rienner Publishers.
경찰청 사이버테러대응센터(http://www.ctrc.go.kr, 2012.11.10.검색)
국가정보원(http://www.nis.go.kr, 2012.11.15.검색)
사이버경찰청(http://www.police.go.kr, 2012.10.30.검색)
한국정보통신기술협회. 표준용어사전(http://word.tta.or.kr/terms/terms.jsp, 2012.11.10.검색)

朴炯均: 동국대학교에서 행정학박사 학위(논문제목: "지방정부의 위기관리행정에 관한 연구 - 서울시 인적재난의 사전대비를 중심으로", 1996년 2월)를 취득하였으며, 현재 대구한의대학교 경찰행정학과 교수로 재직 중이다. 주요 연구 및 관심분야는 경찰행정, 위기관리, 민간경비 분야이며, 현재 한국치안행정학회장, 국가위기관리학회 부회장, 한국테러학회 부회장으로 활동 중이다(police@dhu.ac.kr).

金泰玟: 용인대학교에서 경호학박사 학위(논문제목: "한국 민간경호업무 운용시스템 모델 설정에 관한 연구", 2006년 2월)를 취득하였으며, 현재 경남대학교 경호비서학과 교수로 재직 중이다. 주요 연구분야는 경호학, 민간경비 등이며, 현재 한국치안행정학회 편집이사, 한국공안행정학회, 한국경찰연구학회 이사 등으로 활동 중이다(neoguard@daum.net).

투 고 일: 2012년 11월 20일
수 정 일: 2012년 12월 18일
게재확정일: 2012년 12월 24일