국가 사이버재난관리 시스템 구축 방안
(A Method of Establishing the National Cyber Disaster Management System)

김 상 욱 † 신 용 태 ††
(Sang Wook Kim) (Yong Tae Shin)

요 약 우리나라는 IT 기술의 급속한 발전과 인터넷의 급속적인 보급으로 인해 국가 정보화의 기반 인프라가 매우 잘되어 있지만 주변 강대국들의 위협 속에 사이버테러의 위협도 급격히 증가하고 있다. 아울러 전 세계적으로 사이버戰의 위협도 가속화 되고 있다. 지식 정보화 사회에 대한 사이버 공격은 산업과 경제활동은 물론 국가 안위를 근본적으로 위협하는 요인이 된다. 이미 해외 주요 국가들은 한 번의 사이버 공격으로도 국가 안보에 구멍이 뚫려 엄청난 경제적 손실을 가져올 수 있음을 인식하고, 사이버 공간에서 자국민이 안심하고 활동할 수 있도록 안정성을 최대한 보장하기 위한 정책을 마련하여 추진 중에 있다. 이와 더불어 우리나라뿐만 아니라 전 세계적으로 자연적, 환경적 재난의 위협도 증가하고 있다. 인도네시아나 필리핀처럼 쓰나미, 태풍, 지진 등 온갖 자연재해가 수시로 발생하는 국가는 사전 예방과 사후 복구 등 국가 차원의 체계적인 재난관리시스템이 구축되어 이에 대비하고 있다. 우리나라도 사이버테러 위협으로부터 사전 예방과 사후 복구를 위한 체계적인 관리가 필요하며, 이를 위해 국가차원의 사이버 재난관리(Cyber Disaster Management)에 대한 시스템 구축이 절실하다. 이에 따라, 본 논문에서는 해외 주요국의 사이버 안보정책을 분석하여 국가차원의 사이버 재난관리 시스템 구축을 위한 방안을 제안하고자 한다.

키워드 : 사이버재난관리, 사이버테러, 사이버재난, 사이버보안

Abstract In Korea, national information infrastructure has been grown well because of the rapid growth and supply of Internet, but threats of cyber terror and cyber war are also increasing. Cyber attacks on knowledge information society threaten industry, economy and security. Major countries realize that cyber attacks can cause national heavy loss. So, they are trying to adopt policy on their cyber safe. And natural environmental crisises are increasing around the world. Countries such as India and Philippine in which tsunami, typhoon and earthquake are often occurring have national systematic disaster management system that can prevent and recover. We need systematic management for prevention and recovery from cyber terror, and need to establish national cyber disaster management system. Therefore, in this paper, we analyze major countries's cyber security policy and suggest a method of establishing the national cyber disaster management system.

Key words : cyber disaster management, cyber terror, cyber disaster, cyber security

1. 서 론

우리나라는 국제전기통신연합(ITU)에서 발표하는 디지털기회지수에서는 세계 1위, 정보통신발전지수 세계2위를 차지하고, IT산업 생산규모는 2007년 229조로 세계 전체 생산의 7.1%를 차지하며 중국, 미국, 일본에 이어 세계 4위를 기록하며 비약적으로 성장하고 있다. 또한 UN 전자정부 준비지수 세계 6위이고, 인터넷 보급률 또한 OECD 국가 중 1위를 기록하고 있다.

그러나, 이와 같은 성장과 더불어 다양한 형태의 사이버테러의 위협에 놓여 있다. 2009년 7월 7일 발생한 DDoS 공격을 전후로 사이버테러의 위협에 대해 더 이

† 정 회 원 : 청와대 대통령실 총무기획관실 위민팀 국장
calvin@paran.com
†† 종신회원 : 숭실대학교 컴퓨터학과 교수
shin@ssu.ac.kr
논문접수 : 2010년 4월 13일
심사완료 : 2010년 6월 1일

정보과학회논문지: 정보통신 제37권 제5호(2010.10)

상 방치해서는 안 된다는 우려가 쏟아지고 있지만, 정부나 민간의 대책은 미흡한 실정이다. 그나마 언론에서 관심이 멀어지자 언제 그런 일이 있었냐는 듯 잊혀져가고 있으며, 구체적인 대책도 지지부진한 형태이다. 7.7 DDoS 대란으로 정부의 '사이버보안 종합대책'이 발표되고, 보안시스템 구축에 300억원의 예산을 긴급 투입하는 조치까지 나왔다. 2010년 공공기관 보안 예산도 300억원 이상 증액됐다.

사이버 공격이 날로 급증하고 있으며, 공격기법은 갈수록 지능화되어가고 있는 상황에서 사이버 공격은 단순 해킹에서 점진적으로 금전적인 목적을 갖는 해킹이나 국가간의 사이버 전쟁 등의 다양한 형태로 나타나고 있다. 이처럼 정보통신망에 대한 사이버 공격은 최악의 경우 금융·교통·산업·방송·의료 등의 마비로 국가 전체의 위기를 초래할 수 있으므로 사이버테러 위협에 대한 중요성이 부각되고 있다.

美 외교전문지 'Foreign Policy'는 2007년을 '사이버전쟁 원년'으로 규정하고, 미국 오바마 대통령은 해킹을 국가안보의 제 1위협으로 규정하는 등 세계는 사이버 냉전시대로 급속히 바뀌고 있다. 또한, 7.7 사이버테러 사태는 향후 스마트그리드(지능형 전력망)가 전면적인 수정·보완 없이 현재의 전력 및 지능망을 활용해 운용될 경우 해킹 등 사이버테러에 악용될 수 있다는 우려도 제기되고 있다. 미 의회에서는 국가 경계를 무색하게 하는 사이버테러에 대응하기 위해 '글로벌 사이버 안보 강화법' 제정을 추진한다고 한다. 이 외에도 사이버테러 대응을 위한 민관합동기구인 컨트롤 타워 설립과 전문 대응인력 양성 등 여러 의견들이 나오고 있다.

이를 계기로 국가기관은 물론이고 민간영역에서도 사이버안전대책을 강화시킨 위기관리체계의 점검과 대응매뉴얼 항목들에 대한 점검을 고도화하고 정형화하기 위한 노력과 이번 사건으로 인한 교훈을 잘 반영한 대책들이 앞으로 활발히 추진되어야 할 것이다.

시시각각 눈부시게 발전하는 정보통신 기술의 발달로 우리사회는 사이버 위험사회로 표현될 수 있으며 이런 사회에 대한 대응은 새로운 패러다임에서 준비되어야 한다.

최근에 발생하고 있는 사이버테러는 목적 및 대상이 불명확하고 예측 불가능한 결과도 발생시킴에 따라서 비정상적인 자연현상 또는 인위적인 사고가 원인이 되어 발생하는 사회적·경제적 피해인 재난과 유사하다. 이런 관점에서 본 논문에서는 사이버테러의 새로운 패러다임 변화를 '사이버 재난'이라는 용어로 표현하고자 한다. 이전 KISDI 연구조사 보고서에서는 '디지털 재난'이라는 용어로 표현하기도 했다[1].

재난 및 안전관리 기본법에서 "재난"이라 함은 '국민의 생명·신체 및 재산과 국가에 피해를 주거나 줄 수 있는 것으로서 ① 태풍·홍수·호우·강풍·해일·대설·낙뢰·가뭄·지진·황사·적조 그밖에 준하는 자연현상으로 인하여 발생하는 재해, ② 화재·붕괴·폭발·교통사고·화생방사고·환경오염사고 그밖에 이와 유사한 사고로 대통령이 정하는 규모 이상의 피해, ③ 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비와 전염병 확산 등으로 인한 피해'를 말한다.

사이버 재난은 해마다 증가하는 추세로 최근 발생된 사이버 재난은 유형이 다양해지고, 대규모화되고 있으며 재난 발생원인 및 영향도 정치적, 사상적 목적뿐만 아니라, 경제적, 사회적으로 확대됨에 따라서 단순 사이버 침해가 아닌 복합적 성격의 사이버 재난으로 진화되고 있다. 특히, 공공분야에서의 사이버침해 사고가 증가했고, 지난 5년간 기술 유출 피해가 총 160건 발생하여 전체 피해액이 253조원 규모에 달했다[2]. 또한 지난 7월에는 주요 기관들이 근원지를 알 수 없는 DDoS 공격을 받는 결과까지 낳았다.

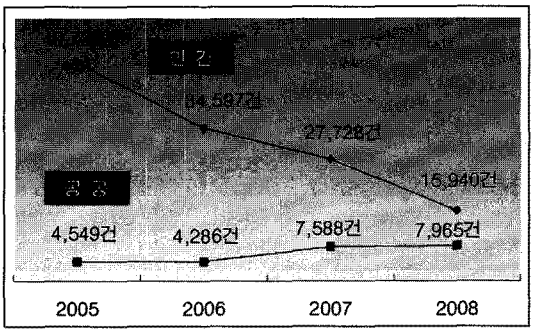

그림 1 사이버 재난 추이

2007년 한 해 동안에 자연재난으로 인한 피해액은 2,518억원 [3]으로 추정된데 반해, 사이버 재난으로 인한 피해액은 3,212억원 [4]으로 추정되고 있어 사이버 재난이 자연재난 보다 큰 피해를 가져온 것으로 추정되었다.

본 논문에서는 이와 같은 사이버 재난에 대해 국가차원의 사이버 재난관리 시스템이 필요하다는 것을 다른 국가의 사이버 재난 대응현황 조사를 통해 밝히고자 한다. 아울러 우리나라에 적합한 국가 사이버 재난관리 방안이 필요하다는 것을 밝히고자 하며, 이를 바탕으로 대한민국이 사이버 공간에서 최고의 선진 강국으로 도약할 수 있는 기틀이 마련되기를 기대한다.

2. 사이버테러 용어정의 및 개요

대한민국 테러방지법 입법시안(2002년)에 따르면 테러라 함은 정치적·종교적·이념적 또는 민족적 목적을

가진 개인이나 집단이 그 목적을 추구하거나 그 주의 또는 주장을 널리 알리기 위하여 계획적으로 행하는 각종의 폭력행위를 말한다.

사이버테러란 컴퓨터 통신망에 구축된 가상공간인 사이버 공간을 이용한 폭력행위를 가리키는 용어로, 컴퓨터 통신망을 이용하여 정부 기관이나 민간 기관의 정보시스템에 침입, 중대한 장애를 일으키거나 파괴하는 등의 범죄행위를 말한다.

사이버테러는 정보화시대의 산물로, 컴퓨터망을 이용하여 데이터베이스화되어 있는 군사, 행정, 인적 자원 등 국가적인 주요 정보를 파괴하는 것을 말한다. 21세기의 테러는 점점 이러한 컴퓨터망의 파괴로 집중될 것으로 예상되며, 앞으로는 전쟁도 군사시설에 대한 직접적인 타격보다는 군사통신, 금융망에 대한 사이버테러 양상을 띨 가능성이 높다.

사이버테러의 종류로는 서비스 거부공격과 논리 폭탄 등이 있다. 서비스 거부 공격은 공격 대상의 서비스 자원을 고갈시키는 등 정상 서비스를 방해하는 것이다. 논리 폭탄은 일종의 컴퓨터 바이러스로, 컴퓨터 시스템에 침입하여 기능을 마비시킨다.

각국에서는 사이버테러에 대비하여 외부의 침입을 막을 수 있는 침입 차단 시스템의 구축과 패스워드 및 암호화 시스템의 사용 등 주요 기관 정보 시스템의 보안대책이 강조되고 있다. 세계 각국에 컴퓨터 통신망이 광범위하게 보급되어 있으며, 이를 이용한 정부 기관이나 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[5].

우리는 이러한 여러 가지 현실들을 감안하여 사이버테러에 대응해 나가야 한다. 이미 세계 각국은 사이버 공격에 좀 더 안전한 사이버 공간을 만들기 위해 사이버안보 정책을 마련하여 추진 중에 있다. 특히 2007년에 있었던 러시아-에스토니아 간 사이버戰 이후 미국, EU 등을 중심으로 국가 사이버안보를 강화하기 위한 정책들이 마련되기 시작했다.

3. 재난관리시스템의 개요 및 기존 연구

3.1 재난관리 모형

1985년 논문에서 Petak이 재난관리모형을 발표한 바 있다. 인도네시아나 필리핀 등 자연재난이 빈번한 나라에서는 국가차원의 재난관리시스템이 구축되어 있는데, 대부분 Petak의 재난관리 모형을 따르고 있다.

재난관리의 과정은 보는 시각에 따라 여러 단계로 나눌 수 있으나 일반적으로 재난발생 시점이나 관리시기를 기준으로 볼 수 있다. Petak은 재난관리과정을 재난의 진행과정과 대응활동에 따라서 재난 이전과 이후 즉 사전 재난관리(pre-disaster management)와 사후 재난관리(post-disaster management)로 나눈 뒤 시계열적으로 이루어지는 재난관리과정을 ① 재난의 완화와 예방(mitigation and prevention), ② 재난의 대비와 계획(preparedness and planning), ③ 재난의 대응(response), ④ 재난의 복구(recovery)의 4단계로 설명하고 있다[6].

이상과 같은 재난관리의 4가지 과정은 상호 단절적인 과정이라기보다는 상호 순환적인 성격을 갖고 있으며 완화, 준비계획, 응급대응, 복구 등의 과정은 각 과정이 별개로 이루어지는 것이 아니고 시간적 활동순서이며 최종의 복구활동의 결과 및 노력 그리고 경험은 최초의 완화단계의 활동에 환류되어 장기적인 재난관리능력을 향상시키는 데 도움을 주게 된다.

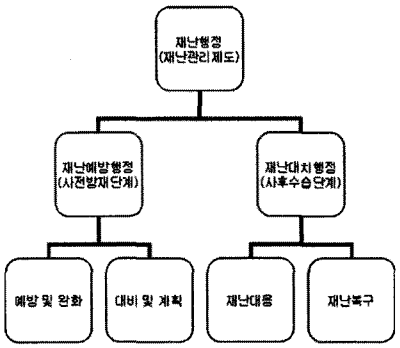

그림 2 재난관리 4단계 모형[8]

표 1 사이버테러의 종류

서비스 거부공격 (DoS: Denial of Service)	㉠ 공격대상 시스템의 서비스자원(CPU, 메모리, 네트워크 대역폭 등)을 고갈시키거나 시스템 상에서 동작하는 응용프로그램의 오류에 대한 공격으로 정상 서비스를 못하도록 만드는 공격 예) 특정 기관의 컴퓨터에 집중적으로 이메일 메시지를 발송하여 수신 측의 전산망을 마비시키는 이메일 폭탄 ㉡ 최근에 많이 발생하는 분산서비스 거부 공격(DDoS : Distributed DoS)은 여러 개의 시스템이 동시에 공격대상 시스템으로 DoS 공격을 함으로써 보다 강력한 공격을 시도할 수 있으며, 공격자에 대한 추적 및 공격차단을 어렵게 만드는 공격
논리폭탄 (logic bomb)	㉢ 특정 기관의 일반적 컴퓨터 프로그램에 중 대한 과오를 발생시키는 루틴이나 부호를 무단으로 삽입하여 데이터를 파괴하거나 변조, 유출 등 예상치 못한 파국적 장애를 일으키거나 부정행위를 실행시키는 논리폭탄

따라서 이러한 재난관리의 제 과정이 하나의 관리체제 속에서 각각의 고유한 기능을 지니고 있는 하부체제로서 작용하게 되고 이 네 가지 과정이 통합관리 될 때만이 효과적인 재난관리의 총체성으로 인해 여기에 참여하는 각 기관, 각 수준의 정부의 조정과 통제 등 필요한 활동체제를 갖추는 노력 또한 재난관리에 필수적인 요소이다[7].

3.2 재난관리 문헌분석

Rubin은 Petak과 같이 재난관리의 4단계를 제안하면서 각 단계들이 상호작용 하고 있다고 강조한다. 예컨대 재난으로 피해 받은 지역사회를 재건할 때는 장래의 완화를 꼭 고려해야 하며, 과거 계속되는 개발이 재난의 재발을 부르는 것과는 달리 위험지역에서 주민을 이주시킨다든지 위험요인을 줄이는 토지이용을 해야 한다는 것이다[9]. 그러나, Petak의 위기관리모형은 시계열상의 단순분석으로 파악되며, 위기상황과 같은 전략적인 재정적, 기술적 고려 이외에 정치적 고려가 필요함에도 여기에 대한 관심이 적었다고 할 수 있다[10].

기존 문헌을 분석해 보면, 재난관리 과정의 단계별로 학자들이 주장한 논리가 다음과 같이 구분할 수 있다.

예방 및 준비단계에서 Godschalk(1991)은 위기완화 활동의 효과적 집행을 통해 얻을 수 있는 편익에 대해 언급하고 있다. Clary(1985)는 위기발생시의 위기대응을 위한 운영능력을 개발시키려는 활동(자원확보, 대응기관 동의, 재산손실 감소, 생명보호, 대응계획 사전개발, 위기를 관리하는데 필요한 계획이나 정보체계 및 다른 수단 등을 준비)에 대하 자세히 기술하고 있다.

대비단계에서 Zimmerman(1985)은 특히 자원조달에 있어서 무엇보다도 대응활동을 위한 특정한 자원조달 계획을 확인하는 것이 필요하며, Kreps(1991)은 지속적이고 연속적인 과정으로서의 준비단계가 과학적 지식과 계획에 의해 합리적이며 대응단계의 활동과 연계되는 것이 필요하다고 주장하였다.

대응단계는 재난이 발생하였을 경우 완화 및 준비단계가 본격적으로 가동하는지 확인하는 단계라고 할 수 있다. Drabek & Petak(1985)은 완화 및 준비단계와 상호연계로 제 2의 손실 발생 가능성을 감소시키고, 복구단계에서 발생할 수 있는 문제들을 최소화시키는 실제 활동의 국면이라고 하였다. 또한 Perry & Nigg(1985)은 재난의 대응상황에 대한 주민의 인식정도도 중요한 요소라고 강조한다. 우리나라의 경우 주민들의 안전 불감증에 의한 인식태도가 피해를 최소화하는 대응전략에 있어서 커다란 장애요인으로 작용한다고 하겠다.

복구단계에서 Waugh(1994)는 복구단계가 단순한 생존지원체계인 전력망 수리, 임시가옥, 식량, 의복제공 등을 포함하는 것이며, Rubin(1991)은 복구에 필수적인 주요요소로서 개인적 리더십, 활동능력, 활동내역에 대한 지식을 예시하며 효과적인 복구전략을 제시하고 있다. 이것은 재해재난의 수습이 단순한 차원에서의 문제가 아닌 조직이나 국가의 운명을 좌우할 수 있는 재난관리 차원에서 전략적으로 대응방안이 요구된다고 할 수 있다.

지금까지 재난관리의 단계인 예방 및 준비단계, 대비단계, 대응단계, 복구단계의 4단계 국면을 중심으로 논의가 전개되어 왔는데, 학자들의 논의를 정리하면 아래 표 2와 같다.

재난관리의 4단계 과정은 상호 단절적인 과정이라기보다 상호 순환적인 성격을 가지고 있으며, 각 단계별 과정의 활동결과 및 내용은 다음 단계로의 활동에 영향을 미치고, 마지막 복구활동의 결과, 노력 그리고 경험 등은 다시 최초의 완화단계에 환류되어 장기적인 재난관리 능력 발전에 영향을 미친다.

재난관리의 모든 과정이 하나의 관리체계 속에서의 고유한 기능을 지니고 있는 하부체제로서 작용하게 되고 이 네 가지 과정이 통합관리 될 때만이 효과적인 재난관리가 이루어질 수 있다. 또한 재난관리의 총체성으로 인해 여기에 참여하는 각종 기관, 각 수준의 정부의 조정과 통제 등 필요한 활동체제를 갖추는 노력 또한 재난관리에 필수적 요소이다[7].

표 2 재난관리과정의 단계별 학자들의 논리[8,11]

단계별	학 자	주요내용
예방 및 준비 단계	Petak (1985)	위기가 발생하기 전에 위기촉진요인을 미리 제거 혹은 예방
	Rubin (1985)	완화활동은 복구과정을 통해 개발된 계획으로 개선 가능
	Godschalk (1991)	위기완화 활동의 효과적 집행을 통해 얻을 수 있는 편익
	Clary (1985)	위기발생시 위기대응을 위한 운영능력을 개발시키려는 활동
대비 단계	Zimmerman (1985)	무엇보다도 대응활동을 위한 특정 자원조달 계획 확인 필요
	Kreps (1991)	지속적 과정으로서의 준비단계가 과학적 계획에 의해 대응단계로의 연계 필요
대응 단계	Drabek & Petak (1985)	복구단계에서 발생가능한 문제최소화시키는 위기관리의 실제 활동 국면
	Perry&Nigg (1985)	위기관리의 대응국면에 대한 주민의 인식정도도 주요 요소임
복구 단계	Waugh (1994)	구체적 활동에는 생존지원체계인 전력망 수리 등을 포함
	Rubin (1991)	복구에 필수적인 주요소로 리더십, 활동능력, 지식 등 제시

표 3 재난관리의 단계별 활동 내용[12]

단계	재난관리 활동의 내용
예방 및 준비 단계	위험성 분석 및 위험지도 작성, 건축법 정비 및 제정, 재난보험, 토지이용관리, 안전관련법 제정, 조세유도
대비 단계	재난대응계획, 비상경보체계 구축, 통합대응체계 구축, 비상통신망 구축, 대응자원 준비, 교육훈련 및 연습
대응 단계	재난대응계획의 적용, 재난진압, 구조, 주민홍보 및 교육, 응급의료체계운영, 사고대책본부 가동, 환자수용, 간호 보호 및 후송
복구 단계	잔해물 제거, 전염 예방, 이재민 지원, 임시주거지 마련, 시설복구

3.3 사이버안전(국가 · 공공)분야 위기대응 매뉴얼

국가정보원은 '국가위기관리기본지침(대통령훈령 제229호)' 및 '사이버안전분야 위기관리 표준매뉴얼'을 근거로 '사이버안전 국가 · 공공분야' 위기상황 발생시 국가정보원이 적용할 세부 대응절차 및 제반 조치사항 등을 표 4와 같이 만들어 각 공공기관에 비치하고 있다.

국가정보원은 위기 징후를 포착하거나 위기발생이 예상되는 경우, 그 위협 또는 위험의 수준을 평가하기 위한 자체 위기평가회의를 구성하고 회의를 통해 도출된 평가 및 판단 결과에 따라 위기경보를 발령한다. 위기평가회의는 국가사이버안전센타장을 의장으로 하고 국방 · 행안부 · 방통위 등 6개부처 파견관 및 의장이 지명하는 사이버안전센터 3급 공무원을 위원으로 구성한다. 국가정보원은 위기경보 발령시 국가위기상황센터 및 유관기관에 신속하게 통보하고, 범정부차원의 평가와 조치가 요구되는 수준의 경보를 발령하는 경우에는 국가위기상황센터에 통보한다. 중앙행정기관은 경보 접수시 산하기관 · 소속기관 및 지방자치단체에 경보발령 사실을 신속히 전파한다.

위기대응 지침은 사이버공격에 대한 신속 대응 · 복구로 피해를 최소화하기 위한 것으로 사이버위기경보 발령 및 대응요령을 전파하고, 사고원인을 파악하여 대응책을 수립하며 신속한 복구 지원을 하고, 피해확산 방지를 위해 공격진원지 · 경유지를 차단하고, 국내외 사이버안전관련 유관기관 및 업체와 공조하며 사고재발 방지대책을 수립하고 이행한다. 심각단계의 경우 범정부 차원의 합동조사본부를 구성하여 운영하게 되어있다. 아울러 복구지원본부를 구성하여 국가안보 관련기관, 핵심기반시설 운용기관, 대국민 행정서비스 제공기관 등의 순으로 피해복구에 임한다[13].

4. 각국의 사이버테러 대응현황 분석

4.1 국내외 주요 사이버테러 사례 분석

4.1.1 7.7 사이버 침해사고

국내에서는 2009년 7월 발생한 '7.7 사이버 침해사고'의 피해에 따른 사회적 파장이 커지면서 사이버 보안의 중요성 및 사이버테러 대응이 주요 이슈로 부상되고 있다. 방송통신위원회 보고에 따르면, 이번 공격은 74개국 16만6천대의 컴퓨터가 감염되었고, 한국에서만 7만8천대가 감염되었다.

이번 공격은 마치 2년 전에 개봉된 영화 '다이하드 4.0'을 연상케 한다. 공격대상 사이트 25개 중 국내 사이트는 청와대, 국회, 국방부, 외교통상부, 한나라당, 조선일보, 옥션, 농협, 신한은행, 외한은행, 네이버 등 11개, 미국 사이트는 백악관 외에 국토안보부, 연방항공청, 국무부, 문화재부, 연방거래위원회, 연방우체국, 뉴욕증권거래소, 주한미군, 옥션(미국 사이트), 야후, VOA뉴스, 워싱턴포스트, US뱅크 등 14개다. 이번 사이버테러는 정부기관, 정당, 포털, 금융기관, 언론 등 각계의 국내 주요기관을 동시에 마비시켜 우리나라의 사이버테러 대비 · 대응 체계가 얼마나 취약한가를 드러냈다.

이번 공격은 해커가 공격대상으로 삼은 웹사이트뿐만

표 4 위기정보 수준[13]

구분	판단기준	비고
관심 (Blue)	○위험도가 높은 웜 · 바이러스, 취약점 및 해킹기법 출현으로 피해발생 가능성 증가 ○해외 사이버공격 피해가 확산되어 국내 유입 우려 ○사이버위협 징후 탐지활동 강화 필요	징후감시
주의 (Yellow)	○일부 정보통신망 및 정보시스템 장애 ○침해사고가 일부기관에서 발생했거나 다수기관으로 확산될 가능성 증가 ○국가정보통신기반시설 전반에 보안태세 강화 필요	보안강화
경계 (Orange)	○복수 정보통신서비스제공자 망 · 기간 통신망에 장애 또는 마비 ○침해사고가 다수기관에서 발생했거나 대규모 피해로 발전될 가능성 증가 ○다수 기관의 공조대응 필요	긴급대응
심각 (Red)	○국가차원의 주요 정보통신망 및 정보시스템 사용 불가능 ○침해사고가 전국적으로 발생했거나 피해범위가 대규모인 사고 발생 ○국가적 차원에서 공동 대처 필요	전면대응

아니라 인터넷 서비스를 제공하는 인터네사업자 및 인터넷사업자의 백본망에 영향을 주어 사회적 혼란을 가져온 점에 유의해야 한다.

원세훈 국정원장은 2009년 10월 29일 국회 정보위 국정감사 현안보고에서 "한국, 미국 등 인터넷 사이트에 대한 DDoS 공격 경로를 추적한 결과, 중국에서 들어오는 회선이 있었다"며 "그 회선은 북한 체신청이 임대해 쓰는 IP인 것으로 확인됐다"고 밝혔다.

미국 국가 사이버안보 및 커뮤니케이션 통합 센터(NCCIC; National Cybersecurity and Communication Integration Center)는 2009년 7월 7일 발생한 미국과 한국을 대상으로 한 DDoS 공격에 대해 보고서를 통해 '시끄러운 시위'로 규정했다. 이는 이번 공격이 매우 기본적인 기술만 사용했으며 '전쟁'으로 규정할 수 있는 실질적 피해는 유발되지 않았기 때문이다. 또한 미국 국내외적으로 사이버 분쟁에 대한 적절한 규제 프레임워크가 부재하여 사회기반을 뒤흔들 수 있는 대대적 공격 행위가 성공하지 않는 한 총괄적 대응 프레임워크 구축은 어렵다고 판단하고 있다.

대신 미국, 이스라엘, 프랑스, 영국, 중국, 러시아만이 사이버 공격을 통해 심각하고 장기적 피해를 가할 만한 선진 기술을 보유하고 있으나, 사이버전이 갖는 성격적 불확실성으로 인해 각국은 정치적 부담을 지닌 채 사이버공격 행위를 대응 및 계획해야 하므로 쉽게 공격에 나설 수 없을 것으로 판단했다.

또한 사이버테러리스트들 또한 특정 국가의 국민인 사이버공격 기술자를 고용할 수밖에 없어 이들의 적극적인 공격 도발 행위도 당분간은 없을 것으로 추정하고 있다. 또한 공격자를 외부에서 고용하지 않는 경우, 암시장에서 관련 기술이나 툴을 구입해서 전문가를 양성해야 하나, 일반 암시장과 선진국들이 보유한 기술에는 3~8년 정도의 기술격차가 있어서 당분간은 적극적 공세가 어려울 것으로 추정하고 있다. 그러나 향후 10년 이내에 테러리스트들이 사이버 암시장에서 가공할만한 파괴력을 가진 사이버 공격에 필요한 기술이나 툴을 획득할 수 있을 것이라고 경고하고 있다.

同 보고서는 핵무기 보유로 인한 국제정세 변화 및 안보정책 변화처럼 사이버공격기술 발달에 따른 국제정세 및 안보정책의 변화가 필요하다고 주장하고 있으나, 구체적 방법론은 제시하지 못하고 있다. 특히 핵무기 사용의 결과는 방사선 피해 정도처럼 객관적 계량화가 가능하지만 사이버공격의 피해 결과는 계량화하기 어려운 내재적 한계가 있으므로 이를 어떻게 적용할 것인지가 관건이 될 것이다[14].

4.1.2 공성진 의원의 주장

2006년 공성진 한나라당 최고위원(한나라당 미래위기대응특별위원회 위원장, 국회 위기관리포럼 대표)은 국방위와 정보위 국정감사에서 '21세기 신 10만 양병. 사이버방호사령부 창설의 필요성'과 '사이버테러방지법의 필요성'이라는 정책자료집을 통해 적의 사이버공격에 대비할 것을 주장했다.

2009. 7. 17일 공성진 최고위원은 7.7 DDoS 사이버테러가 발생하자 "'국가사이버위기관리법'의 조속한 통과에 야당의 적극적인 협조를 요구한다"며 "국방부는 사이버방호사령부 창설과 사이버전 정예 요원 10만 양병을 조속히 추진해야 한다"고 목소리를 높였다.

공성진 의원은 이를 위한 구체적 방안으로 "공익근무요원제도를 활용해 사이버전부대 요원을 양성하고 의무경찰에 사이버전 특기병을 선발해 사이버범죄수사에 활용하며 병역특례제도를 활용, 사이버 전문인력을 양성하는 것이 필요하다"고 설명하고 수도권대학에 사이버전학과를 설치해 졸업 시 사이버전전문지휘관급 장교 요원으로 활용하는 방안도 제시했다[15].

7.7 사이버테러에 앞서 2009. 6. 24일 워싱턴포스트(WP)는 미국 국방부가 사이버테러에 맞서고 사이버 전쟁을 능동적으로 수행하기 위해 10월중 전략사령부(STRAT-COM) 산하에 '사이버 사령부(Cyber Command)'를 창설할 예정이라고 보도했다. 우리나라 국방부도 '국방개혁 2020'의 일환으로 2010. 1월에 정보본부 산하에 '사이버 사령부'를 만들었다. 사이버 사령부는 국방정보본부 예하의 소장급 장성이 지휘하는 200여명의 독립부대로 골격이 잡혀 있다. 국방부는 국방정보본부 예하에

표 5 국내외 주요 사이버 침해사고 사례

일자	주요현황
2003. 1. 25	1.25대란으로 윈도우 MS SQL 서버의 취약점을 이용한 '슬래머 웜 바이러스에 의해 전세계 7만5천대, 국내 8천8백대 컴퓨터 감염
2007. 6. 30	에스토니아의 증권거래위원회 등 공공기관 웹사이트 300여개가 러시아로 추정되는 해커들의 공격에 의해 마비
2008. 8	러시아가 그루지아 공격전 정보관련 사이트를 해킹
2009. 2. 5	해킹에 의해 옥션사용자 1천81만명 정보유출
2009. 3	국방부 3군사령부 자료 해킹으로 2천여건의 국가기밀 자료 유출(2009. 10. 17 주간조선)
2009. 7. 7	청와대, 백악관 등 한미주요기관 웹사이트와 일부 포털이 해커들의 DDoS 공격에 의해 다운되거나 접속장애 사태 발생

'사이버사령부' 창설을 골자로 하는 '국방정보본부령 일부 개정안'을 2009년 12월 17일 입법예고했다. 국방부는 우선 각 군에 흩어져 있는 사이버 전문가들을 모아 400~500여명 규모로 사이버 사령부를 창설하고 오는 2012년에는 사령부의 모습을 완전하게 갖출 계획이다[16].

4.1.3 공공기관 사이버침해사고 현황

김충조 위원(민주당)이 공개한 '공공기관 사이버침해사고 현황'에 따르면 국가기관, 지방자치단체, 연구기관 등 공공기관에서 사이버침해사고 횟수는 지난 2003년 623건에서 2004년 3,970건, 2005년 4,549건, 2006년 4,286건, 2007년 7,588건으로 매년 증가한 것으로 나타났다. 특히 2008년 상반기만 무려 4,104건이 발생한 것으로 집계됐다. 또한 지난 2006년 하반기부터 2008년 상반기까지 2년간 2,624개 공공기관에서 18만2,666건의 개인정보가 누출된 것으로 나타나 개인정보를 비롯한 공공기관의 전산망 관리 및 보안이 매우 허술한 것으로 밝혀졌다.

사이버침해사고가 매년 급증하고 있고 공공기관의 개인정보 유출 정도가 심각한 수준인 반면 365일 상시체제로 사고를 예방해야 하는 전자정부 사이버침해대응센터의 인력은 고작 11명에 불과한 실정이다. 사이버 침해사고를 감소시키기 위한 총체적인 대안이 필요한 것이다.

4.2 해외 주요국 사이버테러 대응전략 분석

해외 주요국은 강력한 정부 리더십을 강조하면서 종

표 6 공공분야 사이버침해사고 대응현황[17]

공공분야 사이버침해사고 대응현황

(2008년 10월 현재, 단위 : 건수)

연도별	합계	악성코드 감염	경유지악용	홈페이지변조	자료훼손유출	기타
2003년	623	0	558	34	8	28
2004년	3,970	2,287	378	297	126	882
2005년	4,549	2,504	1,214	687	87	57
2006년	4,286	2,548	1,316	253	129	48
2007년	7,586	6,194	767	379	176	72
2008년6월	4,104	2,895	550	134	361	164

연도별 공공기관 홈페이지 개인정보 노출현황

(2008년 10월 현재, 단위 : 건수)

연도	2006년 하반기	2007년 상반기	2007년 하반기	2008년 상반기	노출합계
노출건수	72,927	25,428	67,159	17,152	182,666
대상기관	304	531	721	1,068	

공공분야 사이버침해사고 대응현황

(2008년 10월 현재, 단위 : 건수)

연도별	합계	국가 기관	지자체	연구 기관	교육 기관	산하 기관	기타
2003년	623	10	75	7	477	37	17
2004년	3,970	798	701	155	1,537	558	221
2005년	4,549	332	768	184	2,548	672	47
2006년	4,286	458	1,470	260	1,484	620	16
2007년	7,586	625	3,827	198	2,148	706	84
2008년6월	4,104	482	1,582	359	1,040	386	246

표 7 주요국의 사이버 보안 추진 전략[18]

국가총괄 조정기능 강화	미국	사이버보안을 국가핵심 어젠다로 설정하고 사이버보안정책관 신설
	영국	사이버보안실, 사이버보안운영센터 설립 추진
	일본	내각관방의 정보보호센터 설립
법제도 개선	미국	정보통신네트워크 법률의 통합·체계확립 검토
	영국	기관간 제휴를 통한 법령 프레임워크 개발
기술혁신 및 연구개발 고도화	미국	연구개발 프레임워크 설계
	영국	안전한 사이버공간 이용을 위한 R&D 체계구축
	일본	'그랜드 챌린지'형 연구개발 추진
보안문화 확산	미국	전 국민 사이버보안 의식 향상 추진
	영국	사이버보안 인식 전환 촉구
	일본	정부주도의 정보보호교육 역량 확대

합적인 사이버보안 국가전략을 수립 중에 있다. 사이버보안 전담조직인 사이버컨트롤타워 신설, 사이버보안 법률체계 정비, 연구개발 역량 강화, 보안문화 확산을 통해 사이버 공간의 신뢰도 제고 및 복원력 확보 등 미래의 안전한 디지털 인프라 구축을 위해 노력중이다.

4.2.1 미국

미국은 1998년 5월 대통령훈령(PDD63)에 따라 급증하는 사이버테러로부터 자국내 정보통신 기반구조를 보호하기 위해 범정부 차원의 대응체계를 마련하고 이를 시행해 나가고 있다. 특히, 9.11테러 직후로부터 사이버테러 발생 가능성에 대한 우려의 목소리가 높아지면서 이에 대비를 강화해 나가고 있다.

먼저 조직체계 측면에서는 2001년 국토안보국(Office of Homeland Security)을 설립하여 사이버테러 대응 및 복구활동을 조정하는 임무를 부여하였으며, 대통령 사이버보안특별보좌관을 임명하여 정보시스템 보안을 위한 각 부처의 활동을 총괄 조정하고, 침해사고 복구를 총괄하며 주요정보통신시설을 운영하고 있는 민간 분야와의 업무를 조정하고 협의하는 역할을 부여하였다[19].

또한, 대통령주요기반보호협의회(President's Critical Infrastructure Protection Board)를 설립하고, 미국 국가기반시설 보호를 위한 최고 정책기관의 임무를 부여하였다.

2002년에는 국토안보부(Department of Homeland Security)를 설립하여 국가정보보안업무를 담당하게 했다. 2003년 3월 '안전한 사이버 공간을 위한 국가 전략'을 발표하여 국가차원의 사이버안보 정책의 틀을 마련하였다. 또한, 2006년 6월 주요 기반시설 및 자산 보호를 위해 국가기반보호계획(NIPP)을 수립하여 17개 분야의 위험관리절차 등 방법론을 제시했고, 2009년 1월 개정된 국가기반보호계획(NIPP)은 1개 분야를 추가해 총 18개 분야를 주요기반시설분야로 지정했다. 2006년 국토안보부의 국가사이버안보처(NCSD) 주관으로 IT·교통·금융·통신 등 주요 민간분야와 합동으로 대규모 사이버안보 훈련(코드명 '사이버스톰')을 실시했고, 이후 2008년 3월 제2차 훈련을 수행했다. 아울러, 2007년 3월 국토안보부는 국가전력시설의 제어시스템과 동일한 시스템을 조성하여 모의해킹 실험을 실시, 발전기의 가동을 중지시켜 실제 사이버공격에 대한 취약점을 입증하고 해결방안을 모색했다.

2008년 1월 대통령령으로 국가보안국(NSA)이 모든 연방정부기관의 컴퓨터 네트워크를 감시할 수 있는 권한을 부여하고, 국토안보부는 정보통신 시스템에 대한 보안대책, 국방부는 공격자에 대한 대응공격을 담당하도록 역할을 규정하였다. 同 年 1월 '국가 사이버 안보 종합전략(CNCI)', 同 年 2월 '국토안보부의 2008-2013 전략' 등이 발표되었다. 同 年 1월 부시대통령이 승인하고, 7월 의회가 예산의 90%를 승인한 비밀전략인 '국가 사이버안보 종합전략(CNCI)'이 사이버상의 공격에 대해 사전 대응 체계를 구축하는 것을 목표로 추진하였다. 同 年 12월 차기 대통령을 위한 '안전한 사이버 공간을 위한 44대 대통령의 추진 전략'이라는 제안서가 발표되었다.

2009년 2월 오바마 정부는 해킹을 국가안보의 제1위협으로 규정하고 정부주도로 수행된 사이버 안보 강화 계획·프로그램·활동의 일관성, 통합성, 자원 배분의 적절성을 재검토할 것을 지시했다. 이는 단순히 사고에 대한 대응 수준으로 각 기관의 사이버안보 강화 역할을 정의하는 것은 부족하며, 사이버안보에 대한 국가적 차원의 협의가 지금 시작되어야 함을 강조한 결과이다. 이는 대내적으로는 강력한 국정주도권 확보를 위함이고, 대외적으로는 각국 사이버테러 및 사이버戰 능력 강화로 내부적 긴장이 고조된 탓으로 볼 수 있다.

그 결과 최상위 리더십에 기반을 둔 강력한 추진 촉구, 디지털 국가를 향한 역량 축적, 사이버 보안에 관한 책임 분배 등의 전략 제시했고, 사이버 공격에 대한 심각성을 인식한 오바마 행정부는 국가의 사이버안보에 대한 감사를 실시하여 범정부적으로 추진할 계획을 수립하고 있다. 또한 부시 행정부가 지난 수년간 전산 방어에 투입한 170억 달러보다 훨씬 많은 규모의 예산을 사이버안보 강화에 배정할 예정이다. 同 年 2월 대통령 지시에 따라 사이버 안보 정책 검토가 시작되었고, 사이버 예산을 전년대비 13% 증액을 결정하였다. 同 年 3월 사이버 안보 책임을 국토안보부에서 백악관으로 이양을 제안하였다. 2009년 4월에는 미 상원에서 '사이버안보법'으로 명명된 법률안을 입법 상정하였으며, 국방부는 사이버 사령부를 신설하였다.

同 年 5월 백악관은 5대 사이버 안보 어젠다를 발표하였다. 5대 사이버 안보 어젠다에는 ① 최상의 리더십 발휘 ② 디지털 국가 역량 구축 ③ 사이버 보안 책임 공유 ④ 효과적인 정보공유 및 사고대응 체제 구축 ⑤ R&D 투자확대 등 혁신 촉진을 담고 있다. 아울러 대통령직속으로 사이버 보안 정책관을 신설하도록 제안하였다. 2009년 6월 23일 군사 네트워크 방어 및 사이버 무기개발을 전담할 전략사령부(STRATCOM) 산하 '사이버사령부'를 창설하였다.

미국은 사이버안보와 관련해 가장 적극적으로 정책을

그림 3 미국 사이버보안 체계 위상 강화[18]

수립하고 있다. 1998년 대통령령 PDD63을 발표하여 주요기반시설 보호를 위한 초석을 마련했고, 9.11 사태 이후 사이버안보 강화를 위해 국토안보부(DHS) 설립 근거법인 국토안보법을 제정하여 국가 사이버안보 관리체계를 일원화했다. 또한 同 法을 지원하는 대통령 행정명령 및 국가전략을 지속적으로 수립해 관련 업무를 추진해왔다. 同 法에 따라 미국 전역에서 발생하는 사이버공격 방어 등 사이버안보 관리 및 초동대응 업무는 US-CERT가 담당하여 사이버위협 분석 및 취약점 보강, 사이버위협 경고전파, 사이버공격 대응활동 조정 등의 임무를 수행하고 있다.

각 연방기관은 2002년 전자정부법 제3편으로 제정된 '연방정보보안관리법(FISMA)'에 따라 보안활동을 수행하고 있다. 同 法에 의거해 국립표준기술원(NIST)은 연방정보 및 정보시스템의 보안강화를 위한 관련지침 및 표준을 개발하고 있으며 관리예산처(OMB)는 연방 기관의 자체 보안활동을 매년 의회에 보고하고 각 기관의 정보보안 프로그램을 관리하고 있다. 또한 일반회계 감사원(GAO)은 관리예산처(OMB) 보고서에 대해 현장검증 등 심층검토를 거쳐 그 결과를 의회조사국(CRS)의 보고서로 발표하고 있다.

2009년 10월 국토안보부는 US-CERT, 국가텔레커뮤니케이션조정센터(NCC), 국가사이버안전센터(NCSC), 산업제어시스템 사이버대응센터(ICS-CERT)를 흡수·통합하여 NCCIC를 설립했다. 同 센터에는 향후 3년간 최대 1천여 명의 사이버안보 전문가를 채용할 예정(DHS)이다.

同 센터는 각종 사이버테러 대응 및 IT 인프라 보호를 위해 미국 정부기관들의 사이버안보 기능 통합하여 IT 산업과 통신 인프라에 가해지는 위협들을 감시하고 대처하기 위해 365일 24시간 가동할 예정이다. 同 센터는 연방정부기관 네트워크, 주요기반시설 네트워크 등 민·관을 아우르는 최종적 사이버안보 활동을 수행(DHS 장관은 NCCIC가 "중앙 저장소"가 될 것으로 표현)할 것으로 예상된다. 특히 관제업무를 실시하기 위해 민간영역의 사무소가 같은 공간에 설치되어 있음을 강조했다.

同 센터의 설치로 모든 사이버안보 관련 정보의 집결지를 한 곳으로 통일시키고, 각기 다른 명령체계를 지닌 기관원들이 상주함으로써 공통의 정보를 공유하고 필요한 대응을 유기적으로 실시할 수 있을 것으로 판단된다[14].

4.2.2 일본

일본은 1997년 통산성 산하에 네트워크보안대책위원회를 설립하고 사이버테러 예방과 피해방지 연구에 착수하였다. 1999년에는 사이버테러 방지를 위해 "부정접속행위금지 등에 관한 법률"을 제정하고 관방성, 경찰성, 방위청 및 금융감독청 등 국가 13개 기관의 국장급으로 구성된 "정보보안관계성청국장회의"를 설치하여 국가 사이버테러대응방안 강구에 주력하였다.

특히 9.11테러 후에는 총리가 주재하는 긴급 관계성·청회의를 거쳐 생화학·핵에 대한 대응과 함께 사이버테러 대책 강화 등을 중점추진사항으로 의결하였다. 또한, 2001년 10월에는 사이버테러 특별행동계획에 대한 후속조치를 통하여 행정, 전력, 교통 등 국가 주요 인프라의 사이버테러 대응협력체계를 구축하였으며, 이는 현재까지도 추진 중이다.

2002년에는 내각관방 정보보안대책추진실에 국가긴급대응팀(National Incident Response Team)을 설치하고, 정부부처 정보보안 상담대응, 사이버테러 관련 정보의 수집, 분석 및 사이버테러 피해확산 방지 및 복구에 대한 기술적 지원 등의 임무를 부여하였다. 아울러, 2005년 4월 정보보호센터(NISC)를 설치하여 국가차원의 위기대책을 수립하였다. 또한, 2006년 2월 Secure Japan 계획을 세워 매년 시행하고 있다.

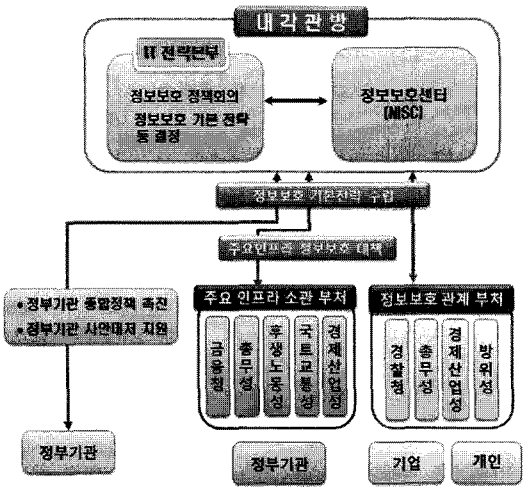

그림 4 일본의 사이버보안 체계[18]

4.2.3 영국

영국은 2000년 5월 "국가기반시설 보안조정기구"를 설립하였으며, 2001년 무역산업부, CSSA(Computing Services & Software Association), 전자비즈니스연합회, NHTCU(National Hi-Tech Crime Unit)가 참여하여 사이버 보안단체인 SAINT(Security Alliance for Internet New Technology)를 발족하였다. 이후 내각부에 사이버보안실을 신설하고, 산하에 정보통신본부에 사이버보안운영센터를 신설하였다.

4.3 국내 사이버테러 대응기관 운영 현황분석

국내 사이버테러 대응기관은 국가정보원, 방송통신위원회, 검찰청, 경찰청, 국방부, 한국인터넷진흥원, 국가보

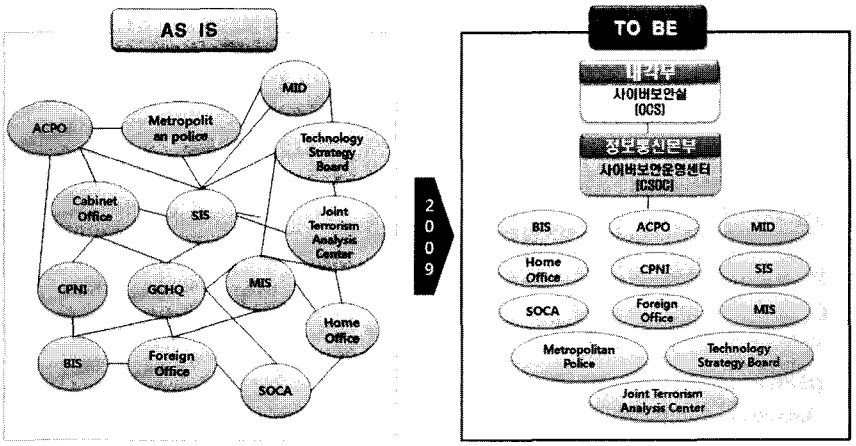

그림 5 영국 사이버보안 체계 변화[18]

안기술연구소 등으로 구성되어 있다.

본 논문에서는 국가정보원, 방송통신위원회, 검찰청, 경찰청 및 국방부를 사이버테러 범죄에 대한 수행기관으로, 한국인터넷진흥원, 국가보안기술연구소 등을 사이버테러 범죄에 대한 지원기관으로 나누어 국내 대응 기관조직들의 체계 및 정책을 알아보고자 한다.

4.3.1 수행기관 측면의 대응현황

국가정보원내 국가사이버안전센터(NCSC)는 국가·공공기관 및 국가 안보관련 시설 정보보호와 관련된 사이버테러 대응업무를 담당하는 기관으로, 국가정보보안업무 기획, 조정 및 보안정책을 수립하고 국가기관 및 공공단체를 대상으로 정보시스템의 보안대책을 지원하며 국가·공공기관용 암호장비나 보안시스템 개발 보급, 정보보호시스템의 인증업무 등을 수행하고 있다.

방송통신위원회는 민간부문에 대한 정보보호 정책 및 법제도를 수립하고 시행하는 기관으로, 정보화 역기능에 관한 대책을 수행하고 있다. 또한, 검찰청·경찰청은 주로 사이버 범죄와 관련된 대응업무를 수행하고 있으며, 이들은 컴퓨터 범죄에 대한 적극적인 대응과 조직적인 수사를 위하여 대검찰청 인터넷 범죄수사센터를 운영하고 있다. 특히 경찰청 사이버 대응센터는 2000년 7월 전문인력 및 장비의 대폭적인 보강으로 사이버테러대응센터로 개편되었다.

아울러, 국방부는 국방CERT, 국군기무사, 한국국방연구원 및 국방과학연구소 등을 통해 사이버테러에 대응하는 국방기본정책을 수립, 연구 및 개발하고 있으며 국방에 필요한 병기, 장비 및 물자에 관한 기술개발도 수행하고 있다.

4.3.2 지원기관 측면의 대응현황

2009년 한국인터넷진흥원으로 개명된 KISA는 주요 정보통신기반시설 보호를 지원하기 위해 정보보호시스템 평가, 민간분야의 해킹·컴퓨터바이러스 침해사고 대응 담당, 침해사고 대응을 위한 기술개발 및 국제협력, 전자서명 인증체계 기반 강화, 개인정보 침해 신고센터 운영 등의 기능을 수행하고 있다.

국가보안기술연구소(NSRI)는 국가 정보보안 분야의 통합 연구기관으로 국가정보기반구조의 안전을 위한 범국가적인 사이버테러 대응체제를 구축하고 있다. 국가용 암호이론체계 연구, 암호분석 기술연구, 정보전 기술연구, 위성·유선·무선통신보호기술 연구 및 국가 정보보안정책연구 등을 수행하고 있다.

그 외에 민간업체로서 안철수연구소, 시큐아이닷컴 등 정보보호전문업체들이 주요 정보 통신기반시설에 대한 취약점 분석, 평가 및 보호대책 수립업무를 지원하고 있다[20].

5. 국가 사이버 재난관리시스템 구축방안

기존연구 3.3 사이버안전분야 위기대응 매뉴얼에서 분석한 대로 위기대응 매뉴얼에는 사이버분야 위기시 각 단계별 역할 및 활동이 자세히 기술되어 있지만 7.7 DDoS 대란에서 보듯이 제대로 작동하지 않았다. 본 논문에서는 앞에서 정리한 분석을 바탕으로 국가 사이버 재난관리시스템 구축방안에 대해 4단계로 나누어 각 단계별 구축방안을 제시해 보고자 한다.

첫째, 예방 및 준비단계는 사이버 재난에 대한 예방을 위해 사이버안전대책을 강화시킨 위기관리체계의 점검과 대응매뉴얼 항목들에 대한 점검을 고도화 및 정형화하는 노력과 관련 법 정비가 필요하다.

우리나라는 아직 국가차원에서 사이버위기를 체계적으로 관리할 수 있는 제도와 구체적 방법·절차가 정립되어 있지 않아 사이버위기 발생 시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있다. 따라서

표 8 사이버 재난관리의 단계별 활동 내용

단계	사이버 재난관리의 단계별 주요 활동
예방 및 준비 단계	위기관리체계 점검과 대응매뉴얼 점검. 국가사이버위기관리법 조속히 통과 필요
대비 단계	주요기관 정보시스템 보안대책 강조 필요. 국가 사이버 안보정책 수립 및 대책 마련. 전문인력 육성 필요
대응 단계	민관합동기구인 컨트롤타워 설립과 각기관사용자 교육. 실질적인 DDoS 대응장비가 주요안보기관과 인터넷 사업자 백본망에 구축
복구 단계	민관합동 추진 체계 마련을 통한 신속한 복구로 피해 최소화

정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 2009년 10월 공성진 의원이 제출한 '국가사이버위기관리법' 통과가 조속히 이루어져야 할 것이다. 이를 통하여 사이버공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있도록 해야 한다.

이 법안이 통과될 경우 평시 사이버위기 예방 및 준비를 위한 각급기관의 역할과 위기발생시 범국가 차원의 대책기구 구성 등 효율적이고 체계적인 위기관리체계 구축이 가능하다. 또 민간과 공공의 구분이 없이 발생하는 사이버위기에 민간기관의 참여와 지원을 보장할 수 있는 법적 근거를 확보함으로써 공동대응이 가능하다. 아울러 사이버위협정보를 체계적으로 수집·분석·대응하는 체계를 구축함으로써 위기발생을 사전에 탐지·예측 및 피해확산 차단 가능하고 정부 합동 사이버위기 대응훈련을 주기적으로 실시함으로써 체계적이고 효율적인 사이버위기 대응능력 배양이 가능하다.

둘째, 대비단계에서는 외부의 침입을 막을 수 있는 침입 차단 시스템의 구축과 패스워드 및 암호화 시스템의 사용 등 주요 기관 정보 시스템의 보안 대책이 강조되어야 하며, 국가 차원의 사이버 안보 정책 수립 및 대책 마련이 필요하다. 아울러 전문인력 육성이 필요하다.

다양한 신규 서비스들이 시장에 선을 보이면 얼마 지나지 않아 서비스에 내재돼 있는 보안 취약성을 지능적으로 악용한 새로운 공격 방법들이 만들어질 수 있다. 최근 빠르게 시장을 확대하고 있는 스마트폰의 경우, 앱스토어와 같은 통로를 통해 전파되는 다양한 응용소프트웨어들이 실행되는 환경 속에 새로운 보안 취약성들이 존재하게 된다. 또 최근에 차세대 IT 환경으로 대두된 클라우드 컴퓨팅 서비스의 경우도, 기업 및 개인의 정보 통제권 및 프라이버시의 침해 우려가 매우 큰 것으로 분석되고 있다. 이와 같은 신규 서비스에서 발생 가능한 모든 공격을 사전에 차단한다는 것은 현실적으로 불가능하다. 이에 대비하기 위해서는 침해 사고 이후 사태를 파악하고 추이를 분석하는 기존의 한계를 뛰어넘어 정보 분석을 통해 선제적으로 대응할 수 있는 능력을 갖춘 전문 인력을 발굴 육성해야 한다.

셋째, 대응단계에서는 사이버테러 대응을 위한 민관합동기구인 컨트롤 타워 설립과 각 기관 사용자 교육이 필요하다. 아울러, 7.7 DDoS 대란이 재발되지 않도록 주요 공공기관과 주요 인터넷사업자의 백본망에 실질적인 DDoS 대응장비가 구축되어야 한다. 2009년 말에 200억규모로 DDoS 대응장비가 일부 구축되었으나 전체적으로 재정비해서 미흡한 기관과 백본망에 추가로 구축해야 할 것이다.

넷째, 복구단계에서는 사이버 재난으로 인한 피해에 대해 긴급 복구해서 피해를 최소화하는 노력이 필요하다. 이를 위해 민간과 공공의 공동대응으로 원활한 협조 속에 국가차원의 추진체계를 마련하여 재난 발생 시 신속한 대응이 이루어지도록 해야 할 것이다.

6. 결 론

미국·일본·영국의 사례는 우리에게 많은 시사점을 제시해준다. 미국의 사례에서 보듯이 사이버테러에 대한 대응체계는 여러 갈래로 나누어져서는 안 되며, 통합적으로 이루어지는 것이 예방의 효율성과 대응의 적시성 등에 있어 바람직하다.

7.7 DDoS 사이버테러 이후 국정원, 방통위 중심으로 대책마련에 총력을 모아 DDoS 방어장비 구축을 위한 예산 200억이 마련되고, 물리적 망분리가 되지 않은 기관들에 대한 망분리 예산 확보도 긍정적으로 추진되고 있는 점은 다행이다. 그러나, 사이버테러의 위협은 7.7 DDoS로 끝나는 것이 아니라 지속적으로 벌어질 것이며, 앞으로 국가의 존폐를 다툴 위협으로 다가오므로 다가올 위협에 대해 국가 차원의 대책이 필요하다. 이를 위해 사이버테러를 사이버 재난으로 규정하고, 정부, 민간 및 군 등 국가사회 전 분야에 모두 적용되는 통치권 차원의 대책을 수립해야 한다.

이러한 대책 수립 시 Petak의 재난관리 모형을 참고하여 예방 및 준비·대비·대응·복구 등 각 단계별로 국가 차원의 사이버 재난관리 활동을 통해 시스템을 구축해야 할 것이다.

국가정보원의 사이버안전분야 위기대응 매뉴얼에도 사이버분야 위기시 각 단계별 역할 및 활동이 자세히 기술되어 있지만 7.7 DDoS 대란 등 국가 사이버 위기시에 작동하지 않은 것처럼 본 논문에서 제시한 시스템이 실제로 유사시 작동되도록 체계적인 활동이 필요하다.

기존 KISDI의 디지털 재난 관련 논문 외에 특별히

참고할 만한 사이버 재난관리시스템 관련 논문이 발표되지 않은 상황에서, 본 논문은 국가차원의 사이버 재난관리시스템의 각 단계별로 구축해야 할 체계 및 활동에 대한 방안을 정리함으로써 사이버 재난관리시스템 구축 시 참고할 수 있는 문헌으로써 기여할 것으로 기대된다.

참 고 문 헌

[1] G. Jung, J. Yoo, "Digital Disaster, A New Paradigm of The Meaning and Countermeasure," *KISDI, ISSN 1976-9733*, pp.11-27, Aug. 2009. (in Korean)

[2] "253 trillion won, The Amount of Damage by technology drain," *Eyenews24*, Oct. 2009.(in Korean)

[3] "2007 An Annual disaster report," *NEMA*, Feb. 2009. (in Korean)

[4] S. Chae, J. Kim, S. Kim, "Analysis of Damage by 2007 Infringement in The Internet," *Proc. of KMIS Conference*, pp.585-586, Jun. 2009. (in Korean)

[5] D. Lee, "A Study on Cyber Crime," *A Master's Thesis*, pp.10-22, Youngsan University, Jan. 2004. (in Korean)

[6] Petak, William J., "Emergency Management: A Challenge for Public Administraton," *Public Administrative Review*, vol.45, Special Issue, pp.3-5, 1985.

[7] S. Im, "A Study on Disaster Countermeasure System Model : Incident Command System," *KRILA*, vol.11, no.4, pp.95-99, 1996. (in Korean)

[8] W. Baek, "A Study of Efficient Disaster Management System," *A Master's Thesis*, Kangwon University, pp.21-27, Feb. 2009. (in Korean)

[9] Rubin, Clare, "Managing the Recovery From a Natural Disaster," *Management Information Service Report*, vol.14, Int'l City Management Association, pp.3-6, 1982.

[10] G. Sung, "Disaster Management and Partnership," (in Korean)

[11] Zimmerman, "The Relationship of Emergency Management to government Policies on Man-Made Technological Disasters," *PAR*, vol.45, pp.29-39, 1985.

[12] G. Kim, C. Yoo, "Theory and Reality : Essay on Disaster Countermeasure," *Van*, 1997. (in Korean)

[13] "Cyber Security(National, Public) Disaster Countermeasure Manual," *NIS*, 2009. (in Korean)

[14] Y. Son, Y. Shin, "Analysis of America Cyber Security Policy," *IT Policy Management Society*, pp.2-5, Dec. 2009. (in Korean)

[15] S. Gong, "The Law National Cyber Crisis Management," Oct. 2008. (in Korean)

[16] The Chosun Daily newsletter, Dec. 2009. (in Korean)

[17] "The Present State of Cyber Infringement Accident in Public Institution," *Disaster Focus*, Nov. 2008. (in Korean)

[18] E. Yoo, M. Yoon, "Major Counties's Cyber Security Strategy and Suggestion," *NIA, CIO Report*, vol.15, pp.2-9, Aug. 2009. (in Korean)

[19] M. Kim, S. Park, H. Kwon, I. Kim, J. Im, "A Study of a Need of Integrated Cyber Crisis Management System," *KIAS*, vol.9, pp.30-35, Mar. 2009. (in Korean)

[20] J. Lee, G. Yang, S. Ryu, "A Study on a Method of Strengthening National Cyber Crisis Management System," *NCEMRI*, Chungbuk University, pp.5-19, Nov. 2008. (in Korean)

김 상 욱

1991년 한국외국어대학교 독일어학과 학사. 1993년 한국외국어대학교 대학원 경영정보학과 석사. 현재 숭실대학교 IT정책경영학과 박사과정 재학중. 2008년~현재 대통령실 총무기획관실 위민팀장 (국장/행정관)

신 용 태

1985년 한양대 산업공학과 학사. 1990년 미국 아이오와대 대학원 전산학과 석사 1994년 미국 아이오와대 대학원 전산학 박사. 1995년~현재 숭실대학교 컴퓨터학부 교수