정보환경변화시대의 사이버테러 양상 및 대응체계에 관한 연구

조 광 래*

〈목 차〉

〈요 약〉

전자정보통신 기술의 발달로 인한 정보화의 수준이 계속 발전, 심화되면서 "언제 어디서나 존재한다"라는 의미를 가진 유비쿼터스(*Ubiquitous*) 컴퓨팅 시대는 20세기 후반부터 우리가 경험해왔던 것보다 더욱 큰 IT 패러다임의 변화와 이에 따른 삶의 커다란 변화를 가져다 줄 것으로 예상하고 있다.

기술의 발달은 새로운 위험을 초래한다. 테러리스트 들은 새로운 정보통신기술발전을 이용한 전혀 새로운 형태의 사이버 테러를 시도하고 있고 이러한 테러리스트들의 테러움직임에 대한 국가적인 대비태세 완비는 매우 시급한 것이 현실이다.

본 논문에서는 유비쿼터스 시대의 새로운 형태의 보안 문제로 첫째, 광대역 통합망(Broadband Convergence Network, BcN) 구축에 따른 보안위협 확산, 둘째, 무선 환경에 취약한 정보보안, 셋째, 개인정보의 유출 가능성 증대, 넷째 사이버위협을 통한 현실세계 위협의 증가, 다섯째, 군사작전상의 기밀유출 및 작전 마비 등을 지적하는 한편, 테러 대비 태세와 관련 우리가 현재 직면하고 있는 조직, 인력 및 기술 그리고 예산상의 문제점을 미국이나 일본 등의 외국과 비교하여 살펴보고 이에 대한 대안을 모색하였다.

【주제어 : 사이버테러리즘, 유비쿼터스시대, 사이버테러대응체계, 정보화사회, 시큐리티】

* 중부대학교 안전경호학과 교수

Ⅰ. 서 론

현재의 사회는 과거 우리 인류가 겪었던 커다란 변혁기의 하나를 경험하고 있는 시대라고 할 수 있다. 농경사회로의 변혁은 인류가 한 지역에 정착하게 하여 찬란한 문명의 시대를 열었고 산업사회의 등장은 기술의 발달로 인한 근대문명을 꽃피웠다. 이제 우리는 새로운 변혁의 시대인 정보화 사회를 맞이하여 인류 역사상 경험하지 못했던 급격한 변화의 물결을 경험하고 있다. 정보화 사회는 컴퓨터와 네트워크 기술의 비약적인 발전에 기초하고 있다. 이러한 정보화 사회는 정보의 생성, 저장, 처리, 가공, 운반, 검색 기능이 상호 연결된 네트워크 환경에서 이루어지고 있으며 원하는 정보를 언제라도 손쉽게 얻을 수 있어 우리에게 많은 생활의 편리를 제공하고 있다 정보화 사회에서 정보의 수집 분석 및 활용 등의 능력은 한 나라의 국익이나 경쟁력을 좌우하는 중요한 자산이 되고 있다.

정보화의 수준이 계속 발전, 심화되면서 앞으로 다가 올 변화는 지금 사람들이 상상하는 것을 모두 뛰어넘는 수준의 폭과 깊이가 될 것이고, 따라서 사회 전반에 걸쳐 일상의 혁명이 불가피하다는 것이다. 즉, 우리가 예상하고 있는 유비쿼터스 컴퓨팅 시대는 20세기 후반부터 우리가 경험해왔던 것보다 더욱 큰 IT 패러다임의 변화와 이에 따른 삶의 변화가 예상된다. 기존 정보화 혁명의 영향으로 우리는 편리하고 윤택한 삶을 영위할 수 있었지만 이에 따른 부작용도 만만치 않았다. 해킹·바이러스의 확산, 개인정보침해, 스팸메일 등의 각종 정보화 역기능은 정보화 시대에 있어 우리가 풀어야할 숙제를 남겨주었다.

이미 많은 사람들이 알고 있겠지만 유비쿼터스는 '어디서나 존재하다'라는 의미로써 라틴어에서 유래한 영어이다. 따라서 유비쿼터스 컴퓨팅은 언제 어디서나 컴퓨터를 사용할 수 있게 되는 컴퓨팅 환경을 의미하며 이는 차세대 정보화 사회에서 핵심적인 IT 기술의 패러다임이다. 유비쿼터스 혁명이 진행됨에 따라 글자 그대로 우리 삶 전체에 걸쳐 혁명이 시작되며 우리 삶의 모습은 기존과는 전혀 다르게 바뀔 것으로 예상된다. 예를 들어 광대역통합

망(Broadband Convergence Network; BcN) 구축 및 차세대 이동통신 확산 등으로 인해 언제, 어디서든지 양질의 디지털 콘텐츠를 고속으로 접속하여 서비스 받을 수 있게 될 것이다. 또한 전자태그(RFID)의 확산으로 개인별 맞춤형 서비스를 제공받는 것이 가능해지며 이를 바탕으로 새로운 형태의 다양한 유비쿼터스 비즈니스가 출현할 것으로 예상된다. 이렇듯 유비쿼터스 시대의 도래와 함께 우리 삶 전반에 걸쳐 혁명적인 변화가 일어날 것을 예상할 수 있다.

우리나라의 경우 2004년도 상반기에 인터넷 이용자수가 3000만명을 돌파했다. 이는 우리나라 총 4천8백여만명의 인구 중 약 73%에 해당하며 인터넷 뱅킹과 증권거래를 비롯한 전자상거래도 그 어느 나라보다 활발히 이루어지고 있는 실정이다. 인터넷은 일반인들도 정보에 대한 자유로운 접근, 정보의 유통 및 생산과정에 직접 참여할 수 있는 기회와 혜택을 제공하고 있으며 시간이 지날수록 그 규모와 인프라가 더욱 증대될 것이다.

그러나 이러한 발전적인 측면들은 한편으로는 정보화 역기능의 문제발생 가능성을 내포하고 있다. 따라서 인터넷의 발전과 더불어 인터넷 이용자의 증가는 컴퓨터 바이러스의 유포 및 해킹, 개인정보의 무분별한 남용과 유출, 사생활 침해, 스팸메일의 증가 등 정보화 역기능에 대한 피해가 갈수록 심각한 문제로 대두되고 있어 이에 대한 피해방지 및 대응책이 절실히 요구된다.

특히 정보화 역기능의 확산은 일반 국민들의 인식부족과 정보화 역기능을 해결할 수 있는 다양한 제도적 장치의 미흡에 있으며 이러한 현실은 정보화 역기능의 피해를 더욱 심각하게 만들고 있다. 이러한 역기능은 일정 수준을 넘어서 테러의 양상으로까지 보이고 있는 실정이며 우리나라도 이러한 상황에서 예외가 될 수 없다. 오히려 정보기술면에서는 세계적인 강국으로 올라선 우리나라는 이라크 파병 등 국제적인 상황변화와 맞물려져서 테러대상국으로서 위치를 피해갈 수 없는 형편이다. 물리적 테러뿐만 아니라 사이버공간상의 테러문제 역시 상당한 위협이 되고 있다. 미래의 정보기술 발달은 조직의 사이버기술에 대한 의존성을 심화시킬 것이며 자신의 목표달성을 위해 목숨까지 버리는 테러리스트로서는 사이버공간에 대한 공격이야말로 적은 비

용으로 국가기간산업 및 국방 분야를 마비시켜 지난 9.11테러와 같은 물리적 테러의 효과에 못지않은 극적인 공포감 조성 및 정세불안을 야기할 수 있는 가장 매력적인 공격대상으로 보일 것이다. 이러한 사이버테러에 대한 대비는 매우 중요하다. 정보기술의 발달에 따라 사이버테러의 양상도 급격히 변화하고 있고 진화하고 있다. 여기에서는 급변하는 정보사회환경의 모습을 살펴보고 정보화의 역기능의 핵심으로서 사이버테러에 대한 외국 및 우리나라의 대응체계를 검토하는 한편 우리가 준비하고 있는 대응체계상의 문제점을 검토해보고자 한다.

Ⅱ. 정보환경의 변화 양상

이제는"산업사회로부터 정보사회로의 세기적 전환"이라는 표현이 진부하다고 할 만큼 사회 전반적인 정보화과정은 진행되었다. 지난 10 여 년간 숨가쁘게 논의되었던 정보의 의미, 정보사회의 정체성, 정보기술의 발전방향 등 엄청난 주제들에 대하여 명쾌한 해답을 마련하지 못하고 있지만 정보화에 따른 생활의 편익을 즐기기에 충분히 익숙하다. 2003년 말 현재, 전 가구의 75% 이상이 초고속 네트워크에 접속되어 있고, 3천2백만 명 이상이 휴대전화를 사용하고 있으며, 젊은 세대를 중심으로 모바일 인터넷의 이용이 크게 증가하고, 대다수 국민들이 상시적으로 인터넷을 활용하는 이른바 광대역 인터넷의 선진국으로 성장했다. 회사에 출근하면 언제 어떻게 침입할지 모르는 바이러스를 걱정하며 쏟아져 들어오는 전자우편을 정리하는 것이 하루의 시작으로 자리매김하였다. 이처럼 개인의 일상생활, 조직 관계 그리고 사회 활동 저변에 정보통신기술은 뿌리를 내렸다. 이는 기술혁명에 대한 호기심에 자극된 일시적인 반응이 아니라 짧은 시간이었지만 사회 전반적으로 누적되고 내면화된 변화의 표출이라는 점을 부정할 수 없다.

1. 정보기술 도입기(1980년대 중반~90년대 중반)

1980년대 중반 전용선에 의한 컴퓨터 통신이 도입되는 시기를 말한다. 1인 1PC 시대이며 단말기의 도입으로 누구나 컴퓨터를 소유하려는 정보기기 소유욕구 시대이기도 하다. 즉 Anyone 시스템의 시대라고도 할 수 있다. 전 세계적으로 약 1억대 이상의 단말기시대가 되면서 인터넷 환경으로의 진입하기 위한 기반이 갖추어진 시대이다. 이 시대는 線중심의 정보화단계라고 할 수 있다.

2. 확장기(90년대 중반~2004 현재)

Anytime의 시대로 접어들었다고 할 수 있다. 인터넷이 보급되면서 본격적인 on-line 시대를 열었으며 모바일 컴퓨팅 및 무선 LAN 인프라, 홈 네트워크화를 통한, 어디에서나 실시간으로 정보를 활용하려는 욕구를 충족시키는 시대라고 할 수 있다. 일종의 面중심의 정보사회라고 하겠다. 연간 수억대의 단말기 시대인 현대의 모습인 것이다.

3. 성숙기(현재~2010년경)

공간중심의 정보화시대라고 할 수 있다. 유.무선 통합을 통해 언제 어디서나 네트워크에 접속하여 정보를 구하고자 하는 시대이며 나아가 어떤 사물에라도 조그마한 chip(RFID)[1]을 심어 Computing, Communication, Connectivity, Contents, Calm(5C)을 실현시키는 시대이다. 모든 대상을 정보기술의 적용 및 정보화 영역으로 확장하여 새로운 가치를 창출하는 유비쿼터스 시대라고 하겠다. 즉, Anything, Anywhere의 시대라고 하겠다. 이 시대의 특징으로는 인터넷 연결 비용이 저렴해 지고 인프라가 지속적으로 발전하며, 각 가정의 컴퓨터뿐

1) RFID(Radio Frequency IDentification)는 IC칩에 내장된 정보를 무선주파수를 이용, 비접촉방식으로 읽어내는 기술로서 상품, 화물, 자재, 유가증권 등 모든 물건과 동식물 등에 부착하여 생산, 유통, 판매 등에 있어 관리 효율 및 고객만족도 향상을 도모하고 있다.

만 아니라 향후에는 가전제품에 이르기까지 네트워크가 연결되고 있다. 네트워크 형성의 범위가 넓어지며, 전 세계는 디지털 글로벌화 되어 간다. 이것은 과거와는 다르게 비즈니스 모델뿐만 아니라 삶의 양식 그리고 전쟁의 양상까지도 새롭게 바꿔놓고 있다.

Ⅲ. 유비쿼터스시대의 Security 위협요인

안전한 유비쿼터스 환경 구현을 위해서는 미래 환경의 위협요인에 대한 분석이 필요하다. 미래의 유비쿼터스 환경에서는 이용자의 컴퓨팅에 대한 노출이 확대되어 위협요소가 다양해지고, 위협으로 인한 침해가 심화될 것이다. 카네기 멜론대학의 K.코숄라는 유비쿼터스 시대가 정착되는데 있어서 최대의 결림돌은 바로 Security문제라고 지적하고 있다. 여기서는 대표적인 위협요인으로서 다음의 5가지를 들겠다.

1. 광대역 통합망(BcN) 구축에 따른 보안위협 확산

유선·무선 통신, 방송, 인터넷이 융합된 차세대 통합네트워크인 BcN 구축을 통해 방송, 통신, 인터넷망이 통합되면 보안위협도 증가될 수 있다. 시스템과 네트워크로 연결된 통신망은 복잡성이 증대되며 관리의 범위가 넓어지고 복잡한 시스템 연결망에서 보안적인 홀(Hole)이 커지게 된다. 관리의 범위에서 벗어나는 시스템이 늘어날 확률이 높아지고 이로 인한 위협의 범위는 확산된다. 우선 사이버 공격에 취약한 인터넷망을 이용한 공격으로 인해 상호 연계·융합되어 있는 방송망, 통신망의 장애가 가능하다. BcN의 개별망이 사이버 공격으로부터 침해를 받게 되면 전체 네트워크의 장애를 발생시켜, 사회적 혼란을 야기하게 된다. 모든 정보통신기기는 시스템과 네트워크로 연결되어 있어서 하나의 공격으로 많은 효과를 낼 수 있으며 이는 공격을 준비하고 있는 개인이나 집단으로서는 더 많은 기회를 부여할 것이다. 향후 VoIP(Voice over

Internet Protocol)의 일상화가 진행되면 기존의 회선 교환망에서 유·무선 인터넷망으로 전환되어 인터넷에서 발생한 해킹, 바이러스로 인해 음성통화가 자주 중단되는 등 일상생활에 많은 불편을 초래할 뿐 아니라 국가 통신체계 자체가 위험에 빠질 수 있고 이는 곧바로 국가경제에 타격으로 이어질 수도 있다.

2. 무선환경에 취약한 정보보안

미래의 네트워크 환경은 무선환경이다. 정보보호의 요소인 기밀성, 무결성, 가용성은 유선환경과 마찬가지로 무선환경에서도 주요한 특징으로서 중요한 위치를 차지한다. 무선환경은 이질적인 네트워크가 상호 연결되고, 다양한 정보기기들이 네트워크에 연결되어 보안 및 프라이버시 침해방법이 다양해지고, 복잡성도 증가함으로써 정보보호 영역이 확대된다. 개방형 무선 환경에서는 외부 공격자가 네트워크의 AP(Access Point)에 접근이 용이하므로 무선신호 범위내에 존재하는 공격자는 보안성이 취약한 네트워크 AP를 경유하여 정보의 기밀성을 손상시킬 수 있다. 무선환경은 유선환경에 비해서는 도청이 용이하고, 반면 도청탐지는 어렵다. 반면, 무선 네트워크의 단말기로 사용되는 정보기기들은 계산 및 저장능력의 제한으로 인해서 인증 메카니즘을 내부에 내장하기 어려운 한계로 인해 정보의 기밀성 보호에 매우 취약하다. 보안성이 취약성 정보기기들은 전체 네트워크를 공격하기 위한 공격의 통로로 이용될 수 있다. 다양한 무선환경의 위협에 대응하기 위한 현재의 무선보안 솔루션은 기능 및 성능에 있어 미흡한 실정이다. 현재의 보안솔루션은 무선통신의 안전성 확보에 필요한 상호운용성을 충분히 제공하지 못하고 있으며, 무선이용자에게 충분한 수준의 보안서비스를 제공하지 못하고 있다.

3. 개인정보의 유출 가능성 증대

개인정보에 대한 범위는 생존하는 개인에 대한 정보로서 성명, 주민번호 등

에 의해서 개인이 알아볼 수 있는 문자, 부호, 영상 등의 정보로 정의하고 있다. 주요한 개인정보침해유형은 개인의 주민등록번호 도용, 타인정보의 훼손·침해·도용, 법정 대리인의 동의 없는 아동의 개인정보 수집, 이용자의 동의 없는 개인정보의 수집, 개인정보 취급자에 의한 훼손·침해 또는 누설, 과도한 개인정보의 수집 등 다양하다. 현재 이용자의 개인정보보호에 대한 중요성은 저조해서 인터넷이용자의 96%이상이 프라이버시 침해를 우려하면서도 70%는 개인정보 제공 전에 사업자의 개인정보보호방침을 확인하지 않는 것으로 조사되었다.(KISA, 2003) 기업체도 관련 개인정보보호에 관한 법률에 대한 인식이 미흡하고, 실천의지가 부족한 상황이다. 유비쿼터스 환경에서 개인정보를 저장·가공하는 기술의 발달과 더불어 개인 정보의 수집 및 이용이 증가하면서 개인정보의 오·남용으로 인한 프라이버시 침해위협이 유비쿼터스 환경에 대한 두려움을 갖게 하는 중대한 요소로 작용할 것이다. 의료체계를 혁신적으로 개선할 수 있는 원격의료(e-Health)시스템에서는 개인의 건강, 진료 정보 등이 센서로 수집되어 전송되는 과정에서 유출·오용되면 개인의 프라이버시를 크게 침해할 수 있다. 텔레매틱스는 위치기반서비스, 차량정보서비스, 전자결재서비스를 이동 중에서 제공하면서 이용자의 위치정보, 신용정보 등이 보안이 취약한 무선 네트워크를 통해 유통되면서 유출될 수 있다. 유비쿼터스는 감시자의 역할로 악용되어 개인의 프라이버시를 크게 위협할 수 있다.

4. 사이버위협을 통한 현실세계 위협의 증가

유비쿼터스 사회에서는 국민생활과 밀접히 관련된 국가사회의 주요인프라인 에너지 기반구조, 물류 기반구조, 금융 기반구조, 생활필수 기반구조가 상호 연결되면서 상호의존성이 크게 증가한다. 정보통신 기반구조는 인터넷·통신·방송망 등으로 구성되어, 국가 인프라의 전체를 상호 연결하는 중추신경계(Digital Nerve System)로서 다른 국가사회의 기반구조를 구성 및 운영하는 핵심적인 요소로 작용한다. 국가기반구조가 정보통신 기반구조가 밀접하게 연결되면 다양한 정보서비스를 제공하는 긍정적인 측면과 더불어 새로운 위험요

인을 내포하게 된다. 사이버 공격으로 인해 정보통신기반구조가 장애를 일으키거나, 중단되는 경우에, 정보통신기반구조와 연계된 에너지기반구조, 물류기반구조 등 국가사회의 다양한 기반구조에 연쇄적으로 장애를 일으켜, 현실세계에 큰 위협으로 작용할 수 있다. 유비쿼터스 사회에서 일상생활의 모든 정보기기들이 상호 연결되면 사이버 위협이 현실세계로 전이될 가능성이 더욱 높아진다. 사이버 공격자들은 이러한 점을 노릴 것이고 이에 대한 대비책 마련이 요구된다. 컴퓨터로 통제되고 있는 국가 전력망에 사이버테러가 자행될 경우 국가 대정전 사태가 발생하고 연쇄적으로 모든 산업에 영향을 미치면서 모든 정부활동과 경제활동, 민간활동이 마비되는 엄청난 사태를 맞이할 것이다. 동시에 군사상 활동에도 영향을 미치게 되면서 일부 발전소에 대한 물리적 테러의 양상보다 더 큰 결과를 초래할 것이다.

5. 군사작전상의 기밀유출 및 작전 마비 등

국방정보화는 군의 정보우위 능력 확보와 국방업무의 효율적 수행을 위하여 추진되고 있다. 군사무기체계, 군사정보체계, 군사암호체계 등은 물론이고 군사통신분야, 전장감시체계, 군사지형정보(GPS) 군사부문의 각 분야는 어느 분야보다도 앞선 유·무선 통합체계를 구축하고 있으며 유비쿼터스 시대의 사이버 안전대책은 국가존립 차원에서 필수적이라고 하겠다.

Ⅳ. 사이버테러리즘

1. 테러리즘

테러리즘의 정의는 다양하다. 테러리즘 개념 정의 주체의 사상이나 정치적 환경, 국제적 역학관계가 서로 다르기 때문이다. 미국 CIA는 "정치적 상징효

과를 얻기 위한 폭력의 사용 또는 그 위협으로서 직접적인 피해자보다는 다수 대중에게 심리적인 충격을 가하려는 목적을 가진 것"이라고 정의하고 있으며 우리나라의 경우 대통령훈령 제47호로 발하여진 "국가대테러활동지침" 제2조에서는 "국가이익과 국민에 대하여 국제테러분자 등이 각종의 목적을 위하여 국내외에서 불법적으로 자행하는 각종 범죄행위"를 국제테러로 규정하고 있다.

테러리즘의 정의는 시대적 상황에 따라 테러의 목표와 유형이 변화하기 때문에 그 개념도 변화된다고 하겠다. 테러의 목표가 일국의 정부에서부터 일반 사회 전체의 체제도 포함된다고 하겠으며 테러의 요소로서 폭력 혹은 폭력사용의 위협이나 조직적인 사전준비 및 무차별적인 공격양상 등이 테러의 공통사항이라고 하겠다. 그러나 시대적 상황의 변화로 인해 테러의 목표도 정치적 목표뿐만 아니라 민족적, 종교적, 문화적 이질성에서 비롯된 경우가 새롭게 대두되고 있으며 첨단 기술의 발전에 따라 특정 기술을 이용하여 폭력행사 없이도 국가나 사회에 극단적인 공포심이나 불안감을 조성하여 마치 폭력을 사용한 것과 같은 심리적 효과를 나타낼 수 있는 시대로의 변화가 이미 일어나고 있는 것이다. 미국에서의 9.11테러에 이은 테러로 의심되는 탄저균 공격, 연성목표(soft target)에 대한 무차별적인 테러 등은 새로운 테러의 양상을 보여주는 좋은 예라고 할 수 있다.

21세기는 정보통신 기술의 발달로 말미암은 대변화의 시기이며 위에서 살펴본 바와 같이 유무선 통합기술의 혁신적 발전은 편리함과 아울러 우리 인류가 새로운 위험에 직면하게 하였다. 새로운 기술은 새로운 위험을 동반한다. 사회가 어느 정도의 위험을 수용할 수 있느냐는 것은 기술로 인해 얻을 수 있는 편익과 신기술에서 발생할 수 있는 위험의 비용을 고려할 때 결정되어진다고 하겠다. 인터넷과 모바일이 결합하는 새로운 유비쿼터스 사회의 도래는 또다른 새로운 위험을 내포하고 있는 것이다.

2. 사이버 테러리즘

사이버공간의 중요성과 패러다임 전환적 변화의 양상과 비교해 볼 때 사이버공간 상에서 나타날 수 있는 위험, 특히 사이버 테러리즘에 대한 연구는 비교적 최근에 와서야 활발하게 진행되고 있으며 기술발전의 속도와 비례하여 사이버테러리즘의 개념 변화 및 양상 등의 변화 또한 급속도로 이루어지고 있다. 사이버테러리즘 개념 정의는 사이버 공간과 물리적(off-line) 공간의 차이로 인하여 우리가 사용하는 테러리즘의 정의를 그대로 적용하는 것은 다소간 무리가 있다고 하겠으며 단순한 컴퓨터 공격(attack)을 사이버테러로 규정짓는 것 또한 무리라고 하겠다. 온라인의 특성상 상당한 시간이 경과한 뒤에야 비로소 공격자의 의도, 정치적 목적 유무 등을 확실하게 확인할 수 있기 때문이다.

미국의 국토안보부(The Department of Homeland Security) 내에 설치되어 있는 국가기간시설보호센터(National Infrastructure Protection Center; NIPC)는 사이버테러리즘을 "정부를 위협하여 정부정책을 변경시킬 목적으로 컴퓨터를 통하여 폭력, 사망, 파괴를 초래하여 공포감을 생기도록 하도록 계획된 범죄행위"로 개념을 정리하고 있다. 공통적으로 지적되고 있는 사이버테러리즘의 정의를 종합하자면 "네티즌 사이에 공포감을 조성할 목적으로 행하는 사이버상의 일체의 만행으로서 특정한 집단이나 개인이 자신의 정치적 목적이나 이념 관철을 목적으로 대중, 정부요인, 정부기관, 공공기반시설 등에 대해 위협을 가 할 수 있는 무기로서 컴퓨터를 사용하며, 컴퓨터 네트워크 시스템에 장애를 초래하는 물리적 또는 소프트웨어적인 일체의 불법 행위"라고 정의할 수 있다. 공간적, 지리적, 시간적 개념의 적용을 뛰어 넘는 사이버공간의 특성상 사이버테러의 문제는 한 국가의 문제라기보다는 국제적인 차원에서 이를 검토하고 대비하여야 하는 문제이다.

사이버테러리즘은 사이버상의 비파괴적 행동이 결국 물리적 피해로 이어지는 사이버 공격을 말한다. 어떤 측면에서는 미사일이나, 핵무기, 생화학무기 등 대량살상무기 보다 더 위험하며 동시에 그 파괴력은 우리가 상상하는 것보다 더 심각할 수도 있다는 것이다. 우리 주변에서 볼 수 있는 컴퓨터로 제어되는 모

든 주요기반시설은 모두가 사이버테러의 대상이 되며 이 때문에 선진 국가들은 관련 법규 제정과 함께 대응조직을 신설하여 물리적 테러의 수준으로 대응방안을 강구하고 있는 것이다. 사이버테러의 목표물은 군사적 시설뿐만 아니라 주요기반시설을 포함한다. 전력이나 가스. 수도의 공급시설, 통신망, 금융시스템, 유통시스템, 육해공의 교통시스템 등 국가 사회생활 유지에 필수적인 시스템 모두를 포함하고 있다. 주요기반시설에 대한 테러는 무차별적인 요소를 포함하고, 또한 경제시스템 전반을 마비시킬 목표로서 행해질 것이 예상된다. 여기에서 테러의 특성상 시설 자체에 대한 파괴행위는 2차적 목적에 지나지 않는다. 결국 테러행위가 노리는 것은 이러한 공격으로 발생하는 상대진영의 정세불안 및 심리적인 공황상태의 유도, 경제적인 타격 그 자체인 것이다.

3. 유비쿼터스 시대의 사이버테러리즘 유형

1) 기술적인 유형

사이버위협이 변화의 변화를 거듭하며 위협의 범위가 더욱 확대되어 나가고 있다. 사이버공간에서의 위협범위 확대는 공격의 지능화, 다양한 도구로 인한 손쉬운 공격, 추적의 어려움, 네트워크화의 가속화, 인프라의 활용 등으로 넓어지고 있다. 공격의 지능화는 과거 공격기술 수준이 낮았던 반면 사용자의 많은 지식을 필요로 하였으나 최근에는 공격기술의 수준은 높아지고 사용자가 많은 지식을 필요로 하지 않는다는 점이다. 이것은 공격도구가 발전함에 따라 위협이라는 것은 누구에게나 쉽게 접근할 수 있는 형태로 변화하고 있는 것이다. 또한 인터넷상에서 손쉽게 접할 수 있는 다양한 도구와 문서를 이용하면 사이버범죄에 쉽게 동참할 수 있다는 점도 과거와 비해 크게 달라진 점이다. 따라서 누구라도 공격자로 변모할 수 있고, 제 3자에게 위협을 줄 수 있는 것으로 앞으로의 위협 수준은 더욱 높아질 것이며 사용하기 쉬운 도구로서 발전할 것이다. 이렇게 사이버공격이 다각도로 발전할 수 있었던 것은 첫째 위협대상의 범위가 다각화 되었고, 둘째 인프라의 발전, 셋째 정보접근의 용이성이다.

정보기술의 발달로 전 세계 컴퓨터가 네트워크화 되어 가며 서로 시스템

적으로 인터넷에 연결되면서 이제는 바이러스가 아닌 웜이 큰 비중을 차지하게 되었다. 웜의 기본적 전제인 확산의 극대화를 위해 스텔스기법, 암호화, 압축 등 방법을 이용하여 자기 스스로를 방어하는 한편 악성코드 스스로가 공격하기 위한 도구로까지 활용되며 피해자인 동시에 외부의 시스템을 공격하는 가해자로 변모되고 있다. 자가복제 기능을 가지면서 전파속도는 초고속 네트워크 인프라와 점점 증대되는 컴퓨팅파워를 기반으로 고속화 되고 피해규모가 광범해질 수 있어, 사이버공간에서의 위협에 치명적인 결과를 가져올 수 있다. 더욱이 향후 사이버공격 양상은 웜 바이러스를 비롯한 사이버 공격도구들이 기존 한 가지 공격 기능만을 가지는 것이 아니라 복합적으로 다양한 공격 방법들이 예상된다는 점이다. 전쟁 등 물리적 공격에도 복합적인 형태가 나타나는 경우에도 커다란 위협을 가져다 줄 수 있는데, 테러 공격시 한 곳을 목표로 하는 것이 아니라 동시 다발적으로 일으켜 혼란상태를 더욱 가중 시키는 것이 피해를 극대화할 수 있는 것과 같은 것이다. 복합적 공격은 또 다른 공격을 위한 공격의 준비로서 피해의 극대화라는 결과에 도달하기 위해서 자연스럽게 이행되어온 것이라 할 수 있다. 단편적인 공격 양상뿐만 아니라 복합적인 형태의 피해 가중이 관리자로 하여금 어떻게 대처할 수 있도록 준비되어 있는가 의문을 제기해 볼 필요가 있다. 관리의 범위에는 한계가 있기 마련이며, 복합적 공격은 대응을 더욱 힘들게 하여 향후 이러한 복합적 공격 양상이 더욱 증대될 것이다.

2) 테러리스트의 공격 가능성 증대

9.11 테러사건은 전 세계를 일순간에 공포로 몰아넣은 사건이었다. 이 사건으로 3000 여명의 사람들이 안타까운 생명을 잃었고, 100여개 이상의 기업에서 50억 달러 이상의 인프라가 손실 것으로 추정되고 있다. 이러한 물리적인 테러 공격이 사이버공간에서 자행된다고 가정하면 물리적인 영향 보다는 사회적 혼란을 초래하고 경제적으로 막대한 영향을 미칠 수 있다. 이것은 IT 발전의 변화에 따라 기간망의 IT 인프라 의존 비율이 높아 사이버 위협에 노출되는 범위가 더욱 넓어지는 유비쿼터스의 시대에서는 더욱 더 심화될 전망이다.

테러리스트들에겐 사이버라는 자체가 공격 무기로서 훌륭하게 사용될 수 있기 때문인데, 이런 위협에 대한 조짐이 이미 감지되고 있다.

전 백악관 사이버보안 고문인 Richard Clarke 의 PBS(Public Broadcasting Service)와의 인터뷰에서 테러리스트중의 하나인 알 카에다(Al Qaeda) 컴퓨터에서 패스워드를 크랙(Crack)해 주는 프로그램인 L0phtCrack 과 같은 해킹툴이 발견되었으며 미국의 주요 인프라인 철도교차점, 대형 천연가스 보관소, 인터넷 백본망이 지나는 주요 선로 정보들을 찾을 수 있었다고 한다. 이미 테러리스트 그룹들은 IT 인프라를 이용하기 시작했으며, 이것은 새로운 전쟁의 서막을 예고하고 있다. 각 그룹간 정보를 교환하기 위한 방법으로 인터넷은 좋은 장소가 되고 있으며, 오사마 빈 라덴(Osama Bin Laden)과 다른 극우 회교도 그룹들은 인터넷상에서 정보를 암호화하여 교환하며 사진 및 메시지를 전달하기 위한 방법으로 웹 사이트가 이용되고 있다고 미국의 정부 관계자는 밝히고 있다.

테러리스트 그룹들이 인터넷을 활용하는 비중이 늘어나며 이에 대한 우려는 더욱 불거지고 있다. 현재 크게 활동하고 있는 사이버 테러리스트들로 추정되는 곳은 알카에다, 이슬람교 그룹인 하마스(Hamas), 오사마 빈 라덴, E-Jihad 등이 있으며, 이러한 현상은 다른 테러리스트 그룹으로 까지 더욱 넓게 확산될 것이다. 이외에 사이버테러리즘으로 발전될 수 있는 해커 그룹의 주의도 필요하다. 이슬람교를 지원하는 해커 그룹인 USG(Unix Security Guards), 인디언 사이트를 공격한 WFD(World's Fantabulas Defacers), 인디아에 대하여 많은 공격을 수행하는 파키스탄 그룹의 AIC(Anti India Crew) 와 같이 해커들의 테러리즘으로 인하여 자칫 국가간에 사이버 위협을 조장하는 결과가 발생할 수도 있기 때문이다. 이제 사이버 공간과 물리적인 피해를 입힐 수 있는 공격이 동시다발적으로 일어날 확률이 높아지게 되었다. 이것은 IT 인프라가 비교적 잘 발달되어 있는 나라보다는 그렇지 않은 곳에서 이런 디지털 기술을 이용하여 피해를 주기 위한 방법들이 더욱 활발히 연구될 가능성이 크기 때문에, IT 인프라 의존비율이 높은 국가에서는 이에 대한 준비가 이뤄져야 한다.

3) 군사적인 측면

군사적인 측면에서도 세계 각국은 정보전 능력 증강을 통한 군사적 우세확보에 노력하고 있다. 군사위성이나 순항미사일과 같은 논리사고능력을 탑재한 정밀유도 전자무기와 고속 네트워크 기술과 밀접한 관계가 있는 차세대 무기가 계속해서 연구 개발되고 있다. 사이버 공격에 의해 상대의 군사시스템을 다운시켜서 테러리즘의 목적인 사회 불안감을 증폭시키고 컴퓨터 시스템에 의존된 기능을 저하시키려는 테러리즘 집단의 노력은 계속될 것이다. 21세기의 전쟁의 양상은 사이버 무기가 승패를 좌우하는 열쇠를 가질 것이 예상된다. 사이버무기의 개발비용은 정밀 전자무기와 비교해 볼 때 상대적으로 아주 저렴하다. 경제력을 가진 강대국만이 아니라, 개발도상국 등 경제력이 없는 나라들도 개발이 가능하기 때문에 어디에서 어떠한 형태의 사이버 무기가 개발될지는, 예측하기 어렵다. 경제적, 군사적 약소국은 강대국에 대하여 사이버 테러를 동시에 사용하면서 공격을 가하는 방법을 계속 모색할 것이다.

Ⅴ. 사이버테러리즘 현황 및 대응체계 분석

1. 현 황

<표 1> 5년간 사이버 침해사고 발생 현황

연 도	1999년	2000년	2001년	2002년	2003년	합 계
공공분야	18	102	613	1,315	1,323	3,371
민간분야	572	1,943	5,333	15,192	26,179	49,219
합 계	590	2,045	5,946	16,507	27,502	52,590

자료 : 2003년 사이버 침해사고 사례분석, NCSC(국가사이버안전센터)

위의 표에서 보듯이 지난 5년간 사이버테러의 약 90%가 민간부문에서 발생한 것을 알 수 있다. 초기만 해도 사이버 공격에 불과하였으나 점차 사이버 테러 양상을 보이고 있으며 공격이 중간 경유지인 경우가 많으며 시스템이 네트워크

화 되면서 사실상 민/관/군의구별이 점차 모호해지고 있다. 또한 사이버 영역의 특성상 각 분야별 대응이 어려운 점이 지적되고 있으며 따라서 국가적 대응차원에서 각 기관간 유기적 협조를 통한 실시간 정보공유 등 대책이 요구되고 있다.

2. 외국의 사이버테러 대응체계

사이버 위협 증가와 인프라의 급격한 발전은 사회 전반에 있어 많은 변화를 가져오고 있으며, 사이버 공간이라는 가상세계에서 위협이라는 또 다른 도전을 받고 있다. 이러한 도전에 각국은 사이버 보안대응체제의 필요성을 인식하고 보안 전략을 수립하고 있다. 앞서 언급하였지만, IT 인프라가 발전된 나라일수록 정보시스템 인프라에 의존하는 비중이 높고 경제 및 사회 각 기반시설의 활용비중이 높아 상대적으로 정보접근의 용이성과 비용이 저렴하여 목표에 대해 큰 위협을 받을 가능성이 높기 때문에 체계적인 대응 마련이 시급하다.

미국방정보국 Lowell Jacoby 부 제독은 2003년 2월 상원 정보위원회에서 미국에 대한 위협이 점차 다양해지고 있으며 기술적으로 복잡해지고 있다고 경고하며 이는 다양한 기술의 등장과 인터넷을 통한 정보 접근 용이성 때문이라 지적한 점에서 보면 사이버위협은 우리 가까이 다가와 있는 것이다 이러한 위협준비로 미국은 이미 국가인프라 기반 보호센터인 NIPC(National Infrastructure Protection Center), DHS(U.S. Department of Homeland Security), NCSD(National Cyber Security Division), US-CERT 등의 다양한 조직을 통하여 사이버상의 각종 사건사고를 탐지하고 대응할 수 있는 기반을 마련하여 미국의 주요 사이버자산을 지키는 역할을 수행하고 있다. 지리적으로 가까이 있는 일본의 경우는 2002년4월 e 정부 사이버공격에 대한 대응하기 위한 팀으로 정보공유와 사이버 테러리즘에 대한 긴급대응을 미션으로 하는 NIRT(National Incident Response Team)가 있고, NPA(National Police Agency) 하에 "Cyber Force" 는 전문기술을 다루는 인원으로 구성된 조직이 있다. 유럽연합은 회원국 정부들간 인터넷을 보호하는 기구를 설립하여 진행중인 유럽네트워크정보보안청(ENISA: European Network Information Security Agency)이 있다.

3. 우리나라 사이버테러 대응 체계

1) 국가 사이버 안전센터

우리나라 또한 다양한 사이버테러 대응체계를 갖추고 있었지만 2003년 1월 25일 인터넷대란에 큰 허점을 보이면서 국가적으로 사이버테러 대응을 위한 행보가 발 빠르게 이어지며 2003년7월24일 국가사이버테러대응체계 구축 기본계획이 대통령 재가를 받은 후, 2004년 2월 20일 기존 국가정보원의 "정보보안 119"를 확대 개편하여 국가사이버안전센터(NCSC: National Cyber Security Center)가 개소하게 되었다.

국가사이버안전센터는 국방(국방정보전 대응센터)분야와 민간(인터넷침해사고대응지원센터)분야 및 공공분야의 사이버보안 위협정보를 공유·분석하여 위험도를 산정, 예·경보를 발령하는 등 국가 사이버테러 대응 업무를 총괄한다. 특히 공공분야 CERT(Computer Emergency Response Team)로서 국가·공공기관에 대해 정보보안 기술을 제공하고, 사이버전 모의훈련을 실시하는 등 예방활동과 함께 사고발생시 각급 기관 및 분야별 CERT/ISAC(Information Sharing & Analysis Center)등으로부터 사고접수 및 상담을 수행하고 사고조사 및 복구지원 업무를 수행한다.

2) 국방정보전대응센터

국방 분야의 사이버테러 대응 역량강화와 군의 주요 정보체계에 대한 보호지원을 위해 국군기무사령부 내에 국방정보전 대응센터가 구성·운영되고 있다. 국방정보전지원센터는 국방 분야에 대해 사이버테러 예·경보를 발령하고 국방전산망에 대한 24시간 위협정보 탐지·분석과 침해사고 예방활동, 사고발생시 원격·현장 피해복구 지원 및 국내외 정보전·사이버전과 관련된 정보 분석 업무를 수행한다. 또한 정보작전 방호태세 훈련중 모의공격과 국방정보통신기반시설에 대한 취약점 분석·평가, 정보 시스템 보안측정 및 진단, 정보통신 보안컨설팅 등의 업무를 수행한다.

3) 인터넷 침해사고 대응지원센터

민간분야의 사이버테러 대응역량 강화를 위하여 한국정보보호진흥원(KISA) 내에 인터넷침해사고대응지원센터가 설치·운영되고 있다. 동 지원센터는 인터넷서비스제공자(ISP), 인터넷데이터센터(IDC) 등 민간분야 전산망에 대한 사이버테러 예·경보를 실시하고, 침해사고 발생시 침해사고 원인을 분석하여 신속정확한 대국민 대응요령을 전파하며 사고지원 업무를 수행하는 등 민간부문의 CERT역할을 수행한다. 그리고 국가사이버안전센터, 국방정보전대응센터 등과도 연계하여 민간분야의 각종 사이버위협정보를 공유하며 백신업체, 소프트웨어 개발업자 등과도 협력하여 인터넷 침해사고 정보, 보안패치 정보 등을 수집·전파하는 업무를 수행한다.

4) 국가보안기술연구소

방대한 전산망과 시스템을 운용중인 교육기관의 중요성을 감안, 교육분야의 인터넷 침해사고 대응역량 강화를 위하여 국가보안기술연구소(NSRI)내에 교육기관 침해사고대응센터를 구성·운영중이다. 국공립대학 및 초·중·고를 대상으로 대응업무를 수행중이며 인터넷 침해사고 처리 뿐 아니라 인터넷 보안 취약점 연구, 홍보와 교육활동을 수행하고 있다. 또한 교육기관 침해사고대응센터는 최신 해킹 및 보안취약점에 대한 분석을 통하여 기반 기술을 확보하고 분석자료를 바탕으로 사고대응 기술을 연구·개발, 침해사고에 적극 대응하고 있다.

5) 정보공유분석센터(ISAC)

정보통신기반보호법 제16조를 근거 규정으로 주요 정보통신기반시설에 대한 보호업무를 수행하는 정보공유분석센터는 현재 통신부문과 금융부문에서 운영중이다.

2002년 1월 설립된 통신분야 정보공유분석센터는 KT, 데이콤, 하나로통신 등 국내 통신사업자를 회원사로 하여 정보보호위원회를 운영하고 회원사 정보, 침해사고, 취약점 등에 대한 자료조사 및 DB를 구축, 운영하면서 회원사들에 대하여 온라인 정보제공 및 침해사고 처리 등의 업무를 수행하고 있다.

2004년 현재 통신사업자연합회 소속에서 KISA로 이관되어 운영 중에 있다.

2002년 12월에 설립된 금융 정보공유분석센터는 금융 ·증권 관련 회원사간 침해사고, 취약점 등에 관한 자료조사 및 DB를 구축 ·운영하고 회원사간 보안 정보를 제공하며 금융증권분야 주요정보통신기반시설에 대한 취약점 분석 ·평가 및 보호대책 수립 지원 등의 업무를 담당하고 있다.

6) 사이버범죄 수사기구

대검찰청 및 서울지방검찰청에 설치된 인터넷범죄수사센터는 해킹, 바이러스유포, 개인정보침해, 컴퓨터 이용사기, 전자상거래 사기, 명예 ·신용 훼손, 음란물, 도박 등 각종 인터넷 범죄행위에 대한 수사 활동을 하고 있다.

경찰청에 설치된 사이버테러대응센터는 사이버범죄의 수사 및 지도, 사이버범죄관련 수사기법의 연구 ·개발, 국제경찰기구 등과의 對사이버범죄 협력 등을 담당하고 있다.

4. 문제점 검토

첫째로 조직의 문제이다. 사이버테러 위협에 대한 범국가적 대응태세 확립을 위해 국가안전보장회의(NSC)를 중심으로 위에서 설명한 각 분야별 사이버테러 대응기구가 상호 유기적으로 운영되고 있다. 그러나 핵심적 조정역할을 담당하고 있는 국가안전보장회의 내에는 정보보안 문제를 통괄하고 조정할 수 있는 전문가 그룹이 부족한 현실이다. 또한 '국가사이버안전센터'는 국가 ·공공분야, '국방정보전대응센터'는 국방분야, '인터넷침해사고대응지원센터'는 민간분야의 대응 업무를 각각 지원하면서 사이버테러 정보 분석을 통한 경보를 발령하고 상호간에 전파하고 있다. 그러나 사실상 각 대응센터 간 정보공유 및 협조체제가 미미한 것으로 지적되고 있으며 실무 주도기관이 부재한 실정이다. 침해사고 발생시 대응기구별로 조기경보 발령체제가 상이하여 체계적인 대응이 곤란한 것도 문제점으로 지적할 수 있다. 한편 미국에서는 국토안보부(DHS)내에 National Cyber Security Division(NCSD)를 신설, 각 기관별 사이

버공격에 대한 업무를 조정·통괄하는 기능과 임무를 수행토록 조직체계를 구성하고 있다.

둘째로 인력 및 기술의 문제이다. 각 대응센터 및 사이버범죄 수사기관의 전문 인력은 공공분야와 국방 분야, 민간 분야 할 것 없이 모두 절대적으로 부족한 현실이다.

기반요소기술 및 응용기술 능력이 부족한 것이 현실이며 급격한 정보기술이 발전과 사이버테러 집단의 기술습득 능력에 대응하기 위한 각 기관별 전문인력 배양이 절실하다. 이를 위해 군, 경, 민간 기관에서 각각 사이버테러 기술을 습득할 수 있는 병과나 대학 등을 신설하여 인력을 배출하고 공무원 임용이나 군·경 채용시험에서 사이버 보안직을 신설하여 채용하는 등의 방안을 강구하여야 할 것이다.

셋째로 예산의 문제이다. 2003년도 미국의 정보보호 예산은 46억달러인데 비해 우리나라의 2003년도 정보보호예산은 368억원에 불과한 실정이다. 지난 2003년 1월25일 발생한 인터넷 대란시 피해규모가 대략 7조원으로 추정되고 있는데, 그해 발생한 태풍 매미의 피해규모 4조원과 비교했을 때 정보보호의 중요성은 더욱 심각하다고 하겠다.

마지막으로 법적 문제점을 지적할 수 있다. 보안관련 규정 개정은 매우 어려운 것이 현실이다. 정보보호의 중요성은 인식하면서도 여러 비정부민간기구의 개입 등 주변 여건으로 인해 법개정이 곤란한 실정이다. 이제는 민주성 확보 측면은 법적, 제도적으로 보장되고 있는 만큼, 적절한 견제 조항을 신설하여 조속하게 '테러방지법' 등 사이버테러에 대응할 수 있는 관련 근거를 확보하여야 한다.

Ⅵ. 결 론

인류에게 디지털 기술은 또 다른 혁명이라고 할 수 있다. 과거에는 생각하지 못했던 일들이 디지털 업적에 힘입어 현실로 나타나고 있으며 정보기술로

인한 인프라의 발전은 전 세계를 하나로 묶어주고 앞으로 변화할 세상을 말해주고 있다. 정보기술의 발달은 앞으로 유비쿼터스 시대의 도래를 예견해주고 있다. 미래의 변화에 대한 예측은 변화가 가져다 줄 편익과 동시에 발생하는 위험에 대한 사전 대비를 할 수 있도록 해준다. 정보기술의 발전은 사이버공간의 영역을 더욱 넓혀줄 것이며, 이에 따른 위협은 각 대응체계 간의 협력(Cooperation)을 더욱 강조하게 될 것이다. 협력대응체계를 통하여 공동목표 가치인 위협으로부터의 안전을 달성하고 이러한 협력을 위해서는 전략적인 체계와 표준이 필요하다. 사이버 공격기술은 계속적으로 진화할 것이고 이에 맞서는 사이버테러대응 대비 태세도 동시에 진화하여야 한다. 점증하는 사이버테러 가능성에 적극적으로 참여함으로써, 위협을 예상하고 그에 맞춘 보호조치가 지속적으로 이뤄져야 한다. 9.11테러사건 이후 전 세계는 무차별적인 테러와의 전쟁중에 있다. 테러와의 전쟁에서는 어느 나라도 예외일 수 없다. 시간적, 공간적, 지리적 제약요인을 뛰어넘는 유비쿼터스 시대의 사이버테러문제는 국가안보차원의 문제이며 국제적으로 대응해야 할 문제이다. 이제 정보의 통합망은 복잡한 네트워크로 연결되어 민/관/군의 구별조차 하기 어려우며 하나의 위협은 도미노 현상으로 곧바로 다른 것의 위협으로 발전한다.

전 세계 국가들은 사이버테러에 대비하기 위한 모든 조치를 강구하고 있으며 우리나라도 대응태세 구축을 위해 노력하고 있다. 그러나 정보기술의 발전속도는 법과 제도가 따라가기에 너무 빠른 속도이므로 대응체계의 낮은 탄력성은 곧바로 위협의 증대로 나타난다. 따라서 장기적인 관점에서 볼 수 있는 시각으로 계속적으로 진화하는 기술과 이에 맞서 사이버테러에 대비에 적극적으로 참여함으로써, 위협을 예상하고 그에 맞춘 보호조치가 지속적으로 이뤄져야 한다.

구체적으로 국가안보를 위한 사이버테러 대응은 부처간의 이해관계를 떠나 국가와 국민의 안전을 책임질 수 있는 곳에서 이끌어야 한다. 위에서 살펴본 3곳의 대응센터를 비롯한 2개의 수사기관 중 확실한 책임의식과 능력이 수반되는 기관에서 총괄하는 체제로 전환되고 이를 법적으로 보장받는 체제가 되어야 한다. 기관간 갈등으로 이것이 어렵다면 새로운 총괄기구인 Leader 기구

의 신설을 고려해야 한다. 다행히도 지난 2005년 1월31일자로 대통령훈령 제141호로 『국가사이버안전관리규정』을 제정하여 국가정보원장을 의장으로 하고 외교부, 법무부, 국방부, 행자부, 정통부차관, NSC사무차장 등을 위원으로 하는 「국가사이버안전전략회의」를 구성하고 산하에 실무 국장급으로 「국가사이버안전대책회의」를 구성한 것은 국가차원에서 사이버 위협에 대비하기 위한 본격적인 조치라고 할 수 있겠다.

미래의 전쟁양상은 더 이상 물리적 공간에만 한정되지 않을 것이다. 유·무선 통합, 통신과 인터넷의 통합 등 새로운 유비쿼터스 시대의 전쟁은 사이버 공간으로까지 확산되어질 것이다. 사이버 공간에서의 전쟁이 물리적 공간인 국가간 전쟁으로 까지 확산되어질 가능성에 대비한 대책 마련을 하여야 한다. 물리적 공격이 사이버공간으로 확대되는 것 이외에 의도적으로 준비되는 사이버전쟁에 대한 대처 또한 필요하다. 정보통신 인프라가 일찍이 잘 갖춰진 나라는 사이버위협의 현실을 발 빠르게 인식하고 이에 대한 준비를 지속적으로 해오고 있다. 정보 강국으로 발돋움 한 우리나라는 어느 나라보다 앞서 사이버테러 대응체계를 완비하여 새로운 위협을 극복하고 보다 안전한 사회를 준비해야 할 것이다.

참 고 문 헌

국가사이버안전센터(2004). 「2003년도 사이버 침해사고 사례분석」.

국가사이버안전센터(2005). 「사이버안전관리규정」.

권문택(2004). "유비쿼터스시대의 사이버안전". 「제5회 사이버테러정보전 컨퍼런스 2004」 21-40

김문일(1998). 「정보화사회에 있어서의 컴퓨터 범죄와 그 방지대책에 관한 연구」. 박사학위논문, 중앙대 대학원.

김원준(2002). 「사이버테러리즘에 대한 대응방안 연구」. 석사학위논문, 고려대 대학원.

김형섭(2004). 「사이버범죄의 대응실태와 그 대응력 제고방안에 관한 연구」. 석사학위논문, 성균관대 대학원.

안보 카츠야 외(2003). 박춘식 ·김현식 역. 『사이버테러』. 서울: 진한도서.

안창훈(2001). "사이버테러의 현황과 대책에 관한 연구". 「한국경호경비학회 국제학술발표회」. 74-103.

양기근(2001). "사이버범죄와 정보보호전문인력 양성". 『한국공안행정학회보』, 12:163-203.

이범준(2004). 「사이버테러 대응방안에 관한 연구」. 석사학위논문, 목원대 대학원.

정관진(2004). "정보기술 발전에 따른 사이버위협의 재조명". 「제1회 한국사이버테러정보전학회 춘계학술세미나」.

정준현 · 김귀남(2004). "사이버테러대응체제와 법치주의". 「제5회 사이버테러정보전컨퍼런스 2004」 9-20.

최응렬 · 황영구(2004). "사이버경찰의 수사한계와 수사력 강화방안". 『경호경비연구』, 8: 379-407.

한국형사정책연구원(2001). 『사이버테러리즘에 관한 연구』. 서울: 형사정책연구원.

http://www.nipc.gov

http://ctrc.go.kr/main.jsp

http://www.ncsc.go.kr

http://www.krcert.or.kr

http://www.kisa.or.kr

http://icic.sppo.go.kr

http://www.kias.or.kr

ABSTRACT

A Study on the Aspects and Counter Systems of the Cyber Terrorism in the Era of Changing Information Circumstances

Cho, Kwang Rae

Development of IT technology as well as arrival of information-oriented society raise the curtain of "the era of Ubiquitous Computing", implying accessing computers beyond boundary of time and space. In this era, it is expected that IT paradigms and life-styles would be transformed immensely above the experiences of 20th century. However, improvement of technology summons a new risk of cyber terrorism which have not been in the past. Thus, it is urgent to prepare for the threats in the national level.

This paper point out five major threats relating to "the security in the era of *Ubiquitous Computing*". : First, spread of threats in connection with BcN establishment, second, vulnerable information-security for wireless communication, third, leakage of private information, fourth, cyber terror and deterioration of security, fifth, security problems of Korea including the drain of military information and solutions in the views of organization, personnel, technology and budget, comparing with other countries.

【Key Words : Cyber Terrorism, Ubiquitous, Security, Information Society, Cyber terror counter system】