情 報 保 護 學 會 誌
第23卷 第2號, 2013. 4

사이버공격에 대비한 국방체계 발전방안 연구

안 유 성*

요 약

인터넷을 중심으로 하는 IT기술의 발전에 따라 이를 통한 사이버공격 혹은 사이버테러가 전세계적으로 급격히 증가하고 있다. 특히 우리나라는 속도 및 보급률에서 인터넷 최강국이며 IT 기술국이다. 그에 따라 사이버테러가 빈번히 발생하고 일단 발생하면 그 확산 및 피해가 엄청나다. 최근에 들어 DDoS 공격을 주축하는 여러형태의 사이버테러가 민간의 범주를 벗어나 국가의 안위를 흔들 정도로 발생하고 있다. 본 연구의 목적은 사이버테러에 대비하고자 외국의 사례들을 살펴 면밀히 분석하고 우리나라의 국방체계 수립에 반영하고자 한다.

Ⅰ. 서 론

인터넷이 발전되면서 우리는 여러 가지 편리한 서비스를 이용하며 사이버 세상을 누리고 있다. 그러나 이러한 편리한 사이버 세상에서 왜곡된 형태의 고의적인 범죄 및 테러들이 곳곳에서 발생하고 있다. 그러나 이러한 사이버범죄는 한 나라안에서 발생하는 범죄의 수준을 벗어나 국가 간의 전쟁 수준으로 이어지고 있다. 북한은 인민무력부 정찰총국 산하에 1000명 규모로 구축한 사이버 공격 조직이 있다. 북한 전역과 중국 등지의 기지에서 우리 정부 기관과 포털 사이트에 접근, 해킹 등 사이버 테러를 가하고 네티즌을 가장한 유언비어 유포 활동을 하고 있다. 그 사례가 2004년 이후 지금까지 무려 5만건에 이르고 있다. 또한 정부기관의 사이트가 중국발 DDoS(Distributed Denial of Service, 분산서비스 거부) 공격을 당하는 사고가 최근 들어 빈발하고 있다. 최근 행정안전부의 국가 대표포털 사이트에 이어 문화체육관광부의 해외문화홍보원과 법무부 홈페이지도 공격을 받았다. DDoS 공격은 단순한 서비스 방해로 끝나지 않고, 정보의 유출, 바이러스나 스파이웨어 같은 악성코드의 침투를 동반해 알려지지 않는 피해를 유발시킨다는 점에서 매우 심각한 결과를 낳을 수 있다. 특히 최근의 농협 전산망 사건은 한 금융기관을 공격한 것에 벗어나 국가의 경제뿐만 아니라 정치에도 영향을 주었다는 점에서 점차 가속화되고 있는 북한의 사이버테러에 대비하여 우리나라의 국방체계에 대한 발전 방안을 모색해 보고자 한다.

Ⅱ. 사이버테러 개념

인터넷이 발전되면서 우리는 여러 가지 편리한 서비스를 이용하며 사이버 세상을 누리고 있다. 그러나 이러한 편리한 사이버 세상에서 왜곡된 형태의 고의적인 범죄 및 테러들이 곳곳에서 발생하고 있는데 사이버범죄 혹은 사이버테러가 바로 그것이다. 사이버범죄(Cyber Crime)란 네이버 백과사전에는 “인터넷과 같은 정보통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로한 사이버 공간을 이용하여 공공복리를 저해하고, 건전한 사이버 문화에 해를 끼치는 행위이다. 사이버 범죄는 빠른 시간 안에 불특정 다수에게 많은 악영향을 미친다. 그러나 사이버 공간이라는 특성상 정보 발신자의 특정이 어렵고, 전자정보의 증거 인멸 및 수정이 간단하기 때문에 범죄 수사에 어려움이 많다. 그 범행 목적에 따라 사이버테러형 범죄와 일반 사이버 범죄로 나뉜다. 사이버 테러형 범죄는 해킹, 컴퓨터 바이러스와 같은 유형의 범죄이고, 일반 사이버 범죄는 사이버 명예 훼손과 전자상거래 사기, 개인정보 침해, 불법 사이트 개설, 디지털 저작권 침해 등을 말한다. 사이버 범죄는 국내 국외에 동시에 발생할 수 있다는 특성을 갖고 있는데, 이에 대처하기 위해 국가간의 법 제도의 상이성을 초월한 국제적인 형사 사법의 규칙도 필요하다.”라고 되어 있다.

* 성균관대학교 정보통신대학원 (dehan86@naver.com)

2.1 사이버테러의 특성

2.1.1 테러비용의 저렴성

사이버테러 혹은 사이버공격을 수행하는 데에 있어 국가적인 지원이나 많은 비용이 없어도 정보체계에 대한 지식만으로 사이버 기술과 사이버 무기를 개발할 수 있고 네트워크를 통해 접근만 할 수 있다면 개발된 사이버 무기를 사용하여 공격할 수 있다. 또한 정보체계들은 상호의존성이 높기 때문에 어느 하나의 정보체계 마비는 전체적으로 막대한 피해를 입히게 된다.

2.1.2 광역성 및 다양성

일반적으로 사이버테러는 테러리스트가 목표로 정한 공격 지점에 직접 접속하여 공격하는 것이 아니라 네트워크가 연결된 곳이라면 세계 어느 곳이든 공격을 감행할 수 있다. 특히, 네트워크망에 대한 보안시스템이 잘 완비되고 국민들의 보안의식이 높은 선진국보다는 보안시스템이 취약한 지역·국가에서부터 출발하여 여러 단계를 거친 다음 목표하는 전산망에 접근하여 필요한 정보를 빼가는 우회적인 방법을 선택하는 것이 일반적인 방법이다.

2.1.3 최소인원으로 최대의 피해

컴퓨터 네트워크를 이용하여 적의 정보통신망에 침투하기 위한 최소한의 기술자만 있으면 사이버테러는 가능하다. 물리적인 테러가 대규모 혹은 소규모라도 다수의 인원을 필요로 하는 것에 비해 목표 대상에 따라 필요 인원이 증가할 수는 있겠지만 사이버테러를 위한 인원은 다른 어떤 물리적인 테러를 수행하기 위한 인원에 비해 적다. 하지만 이러한 경우에는 타격대상이 되는 정보통신 시스템을 파괴·마비시키는 것에 따른 경제적·사회적 파급효과는 정보통신기반시설이 더욱 선진화되고 의존도가 높은 국가일수록 비례하여 커진다.또한 사이버테러 행위는 반복 가능성, 영속성의 속성이 있으므로 한 번의 범죄 행위는 그 규모나 피해가 작을 지라도 계속적으로 자동적인 프로그램의 실행, 확산을 통해 피해액이 계속 증가할 가능성이 높다.

2.1.4 증거의 은닉성과 비가시성

테러리스트들은 물리적 공간이 아닌 사이버 공간의 특수성을 활용하여 수사기관의 추적을 따돌리고 증거를 변조하거나 삭제하고 있다. 이와 같이 원본과 복사본의 구별이 어렵고 수사가 곤란한 디지털 증거에 법적 증거능력을 갖게 하는 방법인 컴퓨터 포렌식(Computer Forensics)은 최근 들어 크게 발전하고 있다. 수사 및 법적인 관점에서 디지털 자료는 눈에 보이지 않는 비가시성에 바탕을 두고 잠재성과 다양성·대량성 등의 특징을 가지고 있어 사법처리를 위한 증거자료를 확보하는 것에 특별한 방법과 절차를 요구하고 있다. 범죄의 혐의가 있을 때 범죄사실과 증거를 수사하여야 하는 것은 컴퓨터 관련 범죄에서도 다른 범죄나 마찬가지이나 컴퓨터와 관련된 증거를 수집함에 있어서는 데이터 프로그램 그 자체로는 유기물이 아니기 때문에 형사소송법상 압수수색 대상 여부 지위와 같은 전통적 증거수집과 다른 절차상의 새로운 문제가 야기된다.[국가안보를 위한 사이버테러 대응방안연구, 문재명, 석사논문, 2010.12]

Ⅲ. 사이버테러 유형과 대응실태

3.1 사이버테러의 분류

3.1.1 주체와 대상에 따른 유형

〔표 1〕 주체와 대상에 따른 사이버테러의 분류

구분	개인적 침해위협	조직적 침해위협	국가적 침해위협
주체	해커 컴퓨터 범죄자	산업스파이 테러리스트 조직화된 범죄집단	국가정보기관 사이버전사
목적	금전획득 영웅심발휘 명성획득	범죄조직 이익달성 정치적 목적달성 사회,경제적 혼란야기	국가기능마비 국가방위 능력마비
대상	민간사설망 공중통신망 개인용 컴퓨터	기업망 금융,항공,교통 정보통신망	국방 외교 공안망

표에서 보는 바와 같이 사이버 공격은 주체에 따라 개인적 침해, 조직적 침해, 국가적 침해로 구분할 수 있으며 그에 따라 목적, 대상에 차이가 있다.

3.2 공격방법에 따른 유형

3.2.1 해킹

사이버테러리스트들이 가장 많이 사용하는 수단이 바로 해킹이다. 해킹이란 컴퓨터를 이용하여 다른 사람의 정보처리장치 또는 정보처리조직에 침입하여 다른 사람의 정보처리장치가 수행하는 기능이나 전자기록에 부당하게 간섭하는 일체의 행위를 말한다. 해킹의 수법으로는 전산망의 운영체제나 운영 프로그램의 버그를 이용하는 방법과 해킹을 위해 전문적으로 제작된 해킹 프로그램을 사용하는 방법이 주류를 이루고 있는데, 종전에는 전산망에 단순 침해하는 수준이었으나 최근에는 시스템이나 운영체제를 직접 공격하거나 서버에 접속된 개인용 컴퓨터까지 접근하여 자료 절취, 시스템 파괴 등을 저지르는 무제한·무차별적 정보전쟁의 수준으로 비약하고 있다.

3.2.2 컴퓨터 바이러스

컴퓨터 바이러스가 처음으로 대두되어 일반 사용자들이 그것의 존재에 대해 인식하기 시작했을 때, 대부분의 사용자들은 바이러스에 걸린 디스켓을 접촉시키기만 하면 바이러스에 감염된다는 식으로 컴퓨터 바이러스를 생물학적 바이러스로 오인했다. 컴퓨터 바이러스는 컴퓨터 내부에서 작동하는 하나의 프로그램에 불과한 것이다. 컴퓨터 바이러스는 일반적으로 프로그램을 변형 또는 삭제하여 주변기기에 오작동을 일으키거나 파일을 손상시키며 자기 자신을 복제하는 등의 행위를 하는 프로그램을 지칭한다. 컴퓨터 바이러스의 특징은 일단 제작, 전파된 것은 완전한 퇴치가 힘들기 때문에 컴퓨터와 프로그램이 존재하는 한 계속될 것이며, E-mail 상요이 일반화되면서 그 확산속도가 더욱 빨라지고 있다.

3.2.3 분산 서비스 거부 공격

분산 서비스 거부(DDoS) 공격은 여러 대의 컴퓨터를 일제히 동작하게 하여 특정 사이트를 공격하는 방식이다. 특정 사이트를 공격하기 위해서 해커가 서비스 거부 공격을 위한 도구들을 여러 대의 컴퓨터에 심어 놓고 목표 사이트의 컴퓨터 시스템이 처리할 수 없는 엄청난 분량의 패킷을 동시에 범람시키면 네트워크의 성능 저하나 시스템의 마비를 가져 온다. 이 같은 분산 서비스 거부 공격은 시스템 침입과 같은 다른 유형의 공격에 비해 공격의 흔적을 거의 남기지 않아 가해자를 찾기가 어렵기 때문에 보다 큰 위협이 되고 있고 다른 공격에 비해 남용될 소지가 많다.

3.3. 외국의 사이버테러 대응 실태

3.3.1 미국 사이버 안전 정책

최근 주요기반시설 및 자원의 사이버 의존도가 중대해 왔고, 사이버상의 전쟁수준에 버금가는 공격들이 전세계적으로 발생함에 따라 (예; 에스토니아 및 그루지아 사이버전 등) 사이버안전에 대한 인식이 높아져 사이버안전 향상을 위한 대응책 마련에 집중적으로 투자하기 시작했다. 이는 2008년 초부터 국가사이버 종합전략(CNCI : Comprehensive National Cybersecurity Initiative) 프로젝트 등을 통해 사이버공간에 대한 통제 강화 및 안전성 강화 노력을 기울인 것으로 잘 드러난다. 이와 동시에 민간영역에서도 2008년 미국 대선을 기점으로 사이버공간 보호를 위한 새로운 접근 방법을 모색하고 다양한 시도들이 진행되어 왔다. 2001년 9.11 사태이후 미국정부는 사이버 안전에 대한 물리적 보안과 대응 수준을 넘어서 사이버 보안과 대응을 위한 체계와 전략을 고심했던 흔적을 엿볼 수 있다. 현재 국가사이버종합전략 CNCI 프로젝트는 대부분의 프로젝트 내용이 비밀로 분류되어 있으나 신문기사 등과 미국의회 청문회 의견 등을 종합해 볼 때, 상당한 양의 예산을 투자하여 사이버상의 악의적 행위에 대한 처단을 강화하고, 불온행위 발생을 철저히 차단하여 미국 사이버 인프라의 안전성과 신뢰성을 공고히 하겠다는 의지가 명확한 것으로 판단된다.

3.3.2 미국 법 체계

미국의 사이버안전 법 체계는 국토안보 전략 및 관련

법, 대통령 명령 및 이를 실행하기 위한 국가계획으로 구성되어 있다. 먼저 국토 안보전략으로 국토안보 국가전략, 주요 기반 시설 및 자산의 물리적 보호를 위한 국가전략, 미국의 국가정보 전략, 사이버공간 보호를 위한 국가전략, 정보공유를 국가전략(개정), 대테러 국가전략(개정), 국토안보를 위한 국가전략이 있다. 국토안보 국가전략은 주요 기반시설 및 자산보호를 국토안보 주요 임무로 설정하고 여러 기관이 관련된 주요 기반시설 및 자산을 보호하기 위한 공동의 노력을 촉구할 수 있는 근거가 된다. 주요 기반시설 및 자산의 물리적 보호를 위한 국가전략은 주요 기반시설 및 핵심자산을 식별하고 보호의 우선순위를 설정하며 활동 수행을 위한 정부기관 및 민간영역과의 협력을 명시한다. 사이버공간 보호를 위한 국가전략은 사이버공간을 통한 주요 기반시설 위해요소 식별 및 이에 대응할 수 있는 전략을 제공하고 주요 기반시설 및 주요자산에 대한 사이버공격 예방을 위한 사이버안전 대응 시스템 개발, 위협 및 취약점 감소 프로그램 실시 등을 제시한다.

3.3.3 프랑스 사이버 안전 정책

프랑스는 사이버 범죄의 예방 활동이 온라인상의 신뢰와 보안을 향상시키는 가장 효과적인 방법으로 간주하였다. 사이버 범죄를 예방하기 위해 필요한 기술과 관리상의 통제 및 프로세스가 필요함을 인식하고 정보시스템 보안관리 및 사이버 위협에 대처하기 위해 정부 액션 프로그램(PAGSI)을 실시하고 안전한 통신채널 확보, 정부정보시스템 보호, 침해사고 대응을 위한 운용능력 설정 등 국가정보시스템 보안강화 계획을 2004년부터 2007년까지 시행하였다. 정보시스템보안(SSI : Security of Information System) 정책으로 두 가지 목표를 설정하고 있는데 첫째는 부처간의 정보시스템보안 위원회에 도움을 주어 일반인과 민간부분에게 전문지식을 제공하는 것이다. 둘째는 다양한 정부 부처 및 부서간의 정보시스템보안활동을 조정하는 것이다. 이런 활동 뿐만 아니라 암호의 사용을 완전히 자유화하기로 결정함과 동시에 불법적인 목적으로 사용하는 행위에 대해서는 강력한 단속 대책을 강구했으며 데이터 프라이버시 준수를 위해 1978년에 설립된 독립 행정기관인 국가 데이터 보호위원회(CNIL)가 주관한다.

3.3.4 프랑스 법 체계

프랑스의 사이버안전기관의 핵심은 중앙정보시스템보안국(DCSSI)이다. 따라서 프랑스의 사이버안전에 관련된 전체 법체계를 일반론적으로 언급하기 보다는 중앙정보시스템보안국(DCSSI)의 사이버안전 규정을 살펴보는 것이 프랑스의 사이버안전 법체계를 이해하는데 도움이 된다 .중앙정보시스템보안국(DCSSI)의 3개 하위부서중 하나인 법제실은 정보보안인증과 산업체간 협력 및 국제협력을 맡고 있지만 가장 중요한 업무는 정보보안분야의 규정을 작성하고 집행하는 것이다. 사이버안전 규정은 정보시스템, 정보통신, 평가 및 인증, 암호화로 구분되어 있다. 정보시스템은 비밀정보를 다루는 시스템에 관한 지침, 물리적 보호 훈령, 정보시스템 보안 훈령, 민감한 정보를 다루는 시스템보호에 관한 권고로 규정되어 잇다. 정보통신은 정보보호를 위한 보안방법 제공 기관간 지침, 민감한 정보를 다루는 시스템과 시설설치에 관한 권고, 비밀을 다루는 하드웨어 및 소프트웨어 설치 훈령, 탬퍼 방지 훈령으로 규정되어 있다. 평가 및 인증은 평가 및 인증 구조 기술 규정으로 되어 잇다. 암호화는 디지털 경제의 안전성을 위한 법, 암호장비와 서비스에 관련한 선언서 및 조직에 관한 규정, 암호장비와 서비스 목록화 규정으로 되어 있다.

3.3.5 노르웨이 사이버 안전 정책

노르웨이는 사이버안전 신뢰구축을 위해 eNorway 3.0 Plan을 추진하였다. 주요 내용은 사이버 위협을 차악하여 중요 데이터 네트워크를 보호하기 위한 조치를 평가하고 정보통신기술취약점 및 보안에 관한 연구 프로그램을 추진하며 사이버 범죄 및 정보보안 인증체계 후속조치와 스마트카드 인프라 시험 프로젝트 지원 및 사용에 따른 인센티브 및 조화로운 보안규제의 실천이다. 또한 EU 집행위원회에서 채택한 정보통신기술 신뢰구축분야의 전문국가로서 프로그램에 참여하여 인터넷 사의 불법 컨텐츠 소탕을 통해 정보통신기술의 신뢰구축을 도모하고 있다. 통신보안은 교통통신부(MTC : Ministry of Transport and Communication) 산하 우정통신국에서 통신부문의 정보보안 책임을 맡고 있다. 사이버안전에 관련해 관심을 갖는 다른 분야는 위협평가와 조기경보이다. 정보행정개혁부(Ministry of Govern-

ment Administration and Reform) 산하의 정보보안센터와 국가보안국(NSM) 예하의 디지털인프라경보시스템(VDI)이 중추적인 역할을 담당하고 있다.

3.3.6 노르웨이 법 체계

노르웨이 사이버전에 관련된 법은 보안법(The Security Act), 전자통신법(The Electronic Communications Act), 데이터보호법(Personal Data Act)속에 관련 내용이 포함되어 있다. 보안법은 구가보안을 위협하는 사고로부터 정보와 사물을 보호하는 데 적용되며, 전자통신법은 전자통신의 전송과 인프라 구조, 서비스 장비, 시설물과 연관된 접속 등의 활동에 적용된다. 데이터보호법은 개인정보 시스템의 일부 또는 일부를 구성하는데 있어서의 개인정보 처리에 적용되며 개인정보의 전체 또는 부분적인 처리에 적용된다.

3.4 북한의 사이버테러 준비상황

북한은 인민무력부 정찰총국 산하에 1000명 규모로 구축한 사이버 공격 조직이 있다. 북한 전역과 중국 등지의 기지에서 우리 정부 기관과 포털 사이트에 접근, 해킹 등 사이버 테러를 가하고 네티즌을 가장한 유언비어 유포 활동을 하고 있다. 그 사례가 2004년 이후 지금까지 무려 5만건에 이르고 한다. 또한 정부기관의 사이트가 중국발 DDoS(DDoS · 분산서비스 거부) 공격을 당하는 사고가 최근 들어 빈발하고 있다. 최근 행정안전부의 국가 대표포털 사이트에 이어 문화체육관광부의 해외문화홍보원과 법무부 홈페이지도 공격을 받았다. DDoS 공격은 단순한 서비스 방해로 끝나지 않고, 정보의 유출, 바이러스나 스파이웨어 같은 악성코드의 침투를 동반해 알려지지 않는 피해를 유발시킨다는 점에서 매우 심각한 결과를 낳을 수 있다.

3.4.1 사이버테러 조직

북한의 해커 양성은 크게 3단계로 이뤄진다. 1단계는 컴퓨터 관련 교육을 중점적으로 진행하는 금성 제2고등중학교에서 맡고 있으며, 2단계는 전문가 수준의 컴퓨터 전문교육을 진행하는 북한이과대학 컴퓨터 전문학부를 비롯한 모란대학, 미림군사대학, 압록강대학 각종 대학 교육 기관이 담당한다. 마지막 3단계는 실전응용 교육 기관인 중앙당 및 인민무력부 산하의 해커 양성소에서 교육한다. 북한은 각 단계별로 교육 내용을 달리하고 있으며, 해커로 성장할 수 없다는 판단이 들면 보안 유지를 위해 상급학교에 진급을 시키지 않고 있다. 즉 최적의 해커를 양성하기 위해 기초부터 전문가 수준까지 분업화된 교육을 진행하는 것이다.

3.4.2 사이버테러 방법

북한의 사이버전은 북한이 전쟁 또는 전쟁에 준하는 의도를 갖고 정보통신망이나 기반 시설에 불법 침입해 교란 또는 마비·파괴시키거나, 정보를 절취·훼손해 자신들에게 유리한 상황을 조성하고자 하는 일체의 전자적 공격행위라고 규정할 수 있다. [대한민국사이버통일안보국연합 홈페이지, 2011년 7월 14일, http://www.cyberhmw.org/detail.php?number=3683&thread=15r11] 2011년 7월 20일, 대한민국사이버통일안보국민연합 홈페이지에 게재된 윤규식 육군종합행정학교 교수의 “북 GPS 교란전파 발사”라는 기고에 따르면 북한이 차후에 재래전과 함께 자행할 것으로 예상되는 전쟁은 전자전과 사이버 공작이 대표적이다. 전자전은 위성위치정보시스템(GPS) 교란이나 전자기 펄스(EMP) 폭탄이 주로 이용된다. 사이버 공작은 사이버 심리전과 정보수집, 사이버 통일전선 구축, 사이버 테러와 사이버 간첩교신 등 다양하다. 북한군의 대표적인 사이버전 공격 수단으로는 러시아로부터 도입해 성능을 개량한 ‘GPS 재머(Jammer)'와 현재 개발 중인 ‘전자기 펄스’(EMP:Electronic-Magnetic Pulse) 폭탄 등이 있다. 이 가운데 개량형 GPS 재머는 북한군이 가장 많이 활용하는 무기다.

3.5 우리나라의 사이버테러 발생상황

최근 대한민국은 군과 민간 동시에 심각한 수준에서 북한 사이버테러 내지는 공격을 당하고 있다. 지난 2005년 1.25인터넷대란, 2009년 7.7 DDoS공격, 올해 3.4DDoS 공격, 그리고 지난 4월 농협전산망테러가 그 대표적인 실례이다. 지난 4월 중순, 한국의 제1금융권 농협 전산망에 대한 공격이 일례이고 북한은 2009년 61개국에 있는 435대의 공격명령 서버를 이용해 총35

개 사이트를 공격한 이른바 7.7 사이버대란을 일으켰고, 2011년 3월 3일-5일에도 70여개국 746대의 서버를 활용하여 국내 40여개 공공망에 대한 D-dos(DDoS)공격을 행한바 있다. 북한의 사이버테러 역량을 과시한 사건이다.특히 지난 4월 12일 발생한 농협 전산망의 해킹사건을 수사해온 사법당국은 5월 3일 수사결과 발표를 통해, 농협 전산망 마비사태가 북한에 의한 사이버테러라고 규정하였다. 북한의 사이버공작부서는 2010년 9월 이전에 웹하드에 악성코드와 해킹프로그램을 심어놓아 여기에 접속한 국내 200여개의 PC(파악된 통계)를 감염시켰고, 이중 하나가 농협전산망을 관리하는 직원의 노트북임을 파악하고 백도어 프로그램, 도청프로그램, 범행흔적 삭제프로그램 등을 추가 설치하여 7개월 이상 집중관리한 끝에, 마침내 4월 12일 농협전산망 파괴 공격명령을 내려 1분 만에 농협전산망 전체서버 587개 가운데 273대를 파괴시켰고 30분도 안되어 서버를 완전 다운시켜 농협 금융전산망이 마비되어 버린 초유의 사태가 벌었졌던 것이다. 이후 농협전산망이 완전 복구되기 까지는 무려 18일이나 소요되었다.

Ⅳ. 사이버공격에 대한 대응방안

4.1 민간 기구를 적극 활용

현재 국방부에 국방정보전대응센터가 있지만 전반적으로 군에 사이버에 대비한 인력, 구조, 장비 등은 미미한 실정이다. 사이버전에 대비한 여러 계획 및 준비가 이루어져 제대로 시스템을 이루고 운영되려면 짧게는 10년에서 길게는 20년 정도가 걸릴 것으로 보인다. 결국 시스템이 갖추어지기 전까지인 10~20년 정도는 과도기라고 볼 수 있다. 대내외적인 사이버테러는 점점 심각해지고 있는데 이러한 기간을 기다리고 있을 수만은 없다. 정보보안 업체와 민간 기구 그리고 정부 기관 등을 적극 활용하여 과도기 동안 사이버테러에 대비하여야 한다. 그러나 민간 업체나 기구 등은 사이버테러 발생시 보고나 처리 등의 책임 소재를 갖기가 쉽지 않다. 따라서 민간 업체나 기구 혹은 그곳의 책임자를 사이버 군부서나 장교 등으로 임명하여 어느 정도의 책임감을 갖고 신속한 보고 및 대응을 할 수 있도록 하는 것이다.

4.2 사이버테러에 대비한 시스템 구축

2009년 7월 7일 발생한 “7.7 DDos 대란”이나 최근에 발생한 농협 전산망의 해킹사건을 볼 때 범국가적인 대응 시스템이 여전히 갖추어지지 않고 있는 것으로 판단된다. 사이버 테러 발생시 초기에 이를 파악하고 등급별 대응이 이루어져야 한다. 국민이나 국가적인 불편이 있더라도 사이버테러의 확산을 막기 위해 인터넷 차단이나 PC나 서버 Power Off와 같은 극단적인 조치가 이루어져 한다. 백신이나 방화벽 설치와 같은 일반적인 방법은 평상시에 이루어지는 대응방법이고 실제 사이버테러가 발생하면 어떤 유형인지가 파악되지 않기 때문에 일단 확산을 막는 것에 대응의 초점을 맞추어야 한다. 그리고 이러한 대응 방법은 범국가적으로 군•관•민이 일체가 되어 신속하게 이루어져야 한다. 그러기 위해서는 사이버테러에 대비한 체계적인 범국가적인 대응 시스템을 구축하여야 한다.

4.3 군과 사이버 관련 법률의 정비

사이버테러나 범죄에 관련한 군이나 민간 법률은 현재 제대로 정립이 되어 있지 않고 기존의 법률에서도 처벌이 가능하다고 아예 수립을 생각하지 않고 있는 분야도 있다. 또한 이러한 사이버 범죄나 테러범이 체포되어도 현행법의 테두리에서 재판이 이루어지다보니 다소 약하게 처벌받고 있는 것이 사실이다. 예를 들면 정보통신관련 법률에 명시되어 있지 않는 사이버상의 위법 행위들은 사실상 처벌이 불가능한 것이다. 이러한 현 법률체계는 사이버범죄나 테러를 더욱 조장하고 있으며 사이버테러나 범죄 자체도 문제이지만 천안함 사건 발생 후,“예비군 동원령 등의”의 루머를 문자나 이메일 등으로 유포하여 사회를 혼란스럽게 하는 행위도 사회를 혼란시키는 사이버테러이다. 그런데 그런 루머를 유포한 사람들에 대한 처벌도 사실상 불가능한 상태에 있다. 앞에서도 살펴보았듯이 사이버테러는 총알을 사용하지도 않고 한 국가를 몰락시킬 수 있는 공격 방법이다. 따라서 사이버테러에 대한 보다 강력한 처벌을 할 수 있는 군・민간 법률의 정비 및 제정이 신속히 필요하다.

4.4 사이버테러의 공격에 대한 연구

우리나라는 “7.7 DDos 대란”에 비해 최근에 발생한 농협 전산망의 해킹사건 때에는 신속하게 사태를 파악할 수 있었다. 앞으로도 군・관・민의 사이버테러에 대한 모니터링 시스템이 어느 정도 정립이 되어 초동대처를 할 수 있으리라 예측된다.

그러나 그에 상응하여 공격 근원지를 찾아내고 근원지에 대한 사이버 응징을 가하는 방법도 연구되어야 한다. 미국은 자국에 대한 사이버 공격 국가에 미사일로 응징하겠다고 했지만 실제로 그렇게 될지는 의문이다. 공격 근원지를 찾아내는 것도 시간과 노력이 들며 점차 사이버 공격은 교묘하고 공격 흔적을 지우기 때문에 근원지를 파악하기가 어려워지고 있다. 근원지를 찾는 것도 어렵지만 설령 찾았다고 하더라도 사이버 공격에 대한 응징으로서의 물리적인 공격은 세계 여론에 악영향을 끼칠 수 있으며 공격에 따른 재정적인 문제 그리고 전면전으로 확산 등의 부작용을 유발시킬 수 있다. 따라서 사이버 공격 근원지에 대한 사이버 응징이 가장 최선의 수단이 될 수 있다. 그에 따른 기반적인 연구가 국방관련 연구소에서 이루어 져야 한다.

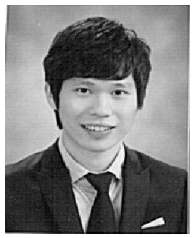
Ⅴ. 결 론

인터넷을 통한 사이버테러가 점차 빈번하게 발생하고 발생할 때마다 그 피해가 커지고 있다. 뿐만 아니라 이제 국지적인 민간인 상호간의 테러가 아니라 국가간의 물밑전쟁 형태로 확산되어지는 양상을 띄고 있다. 그에 따라 군은 물론 산업계 그리고 학계에서도 사이버테러에 관한 연구가 활성화되고 있다. 최근에는 학술대회나 논문지는 물론 학위논문의 주제로도 언급되어 지고 있다. 우리나라는 인터넷 강국이지만 그에 따라 잘 발달된 인터넷을 통하여 사이버테러를 당하기 쉬운 형편에 놓여 있다. 인터넷을 기반으로 하는 IT 기술은 급속히 발전되었지만 전반적으로 보안은 연구되어 있지 못하다. 아울러 군의 사이버 국방에 대한 시스템 및 체계 또한 다른 나라에 비해 뒤처지고 있는 것이 사실이다. 본 연구에서 우리나라의 사이버 체계 발전에 조금이나마 활용 및 도움이 되길 바란다.

참고문헌

[1] 최광복, “사이버전 대응을 위한 국방 정보보호환경 분석과 보안관리모델 연구방향 고찰”, 정보보호학회지, 2011년 10월
[2] 김승권,김상국,최종화, “미래 사이버전 및 대비방안”, 정보과학회논문지, 2008년 11월
[3] 문종식,이임영, “사이버테러 동향과 대응,”, 정보보호학회지 2010년8월
[4] 김배현,나원식,유인태,권문택, “국방 정보보호 기술발전 동향,”, 정보보호학회지 2002년 12월
[5] 박상서,박춘식, “사이버전에 관한 주요국의 견해,”, 정보보호학회지 2004년 12월
[6] 박대우, “국가사이버보안정책에서 해킹에 대한 소고,”, 정보보호학회지 2011년 10월
[7] 서동일,조현숙, “사이버전을 위한 보안기술현황과 전망,” 정보보호학회지 2011년 10월
[8] 장월수,최중영,임종인, “국방 클라우드 컴퓨팅 도입에 관한 보안체계 연구,” 한국정보보호학회논문지 2012년 6월
[9] 권문택, “북한의 비대칭 전략-‘사이버 기습 공격’에 대한 대책 연구”, 정보·보안논문지 2010년 12월
[10] 남길현,원동호, “정보시스템 보안론”
[11] 정재영, “사이버테러에 관한 국가별 대응실태연구,”, 학위논문 2010년 6월
[12] 문재명, “국가안보를 위한 사이버테러 대응 방안연구”, 학위논문 ”2012년 12월

〈著者紹介〉



안 유 성 (Yoo-seong An)
정회원
2011년 9월~현재 : 성균관대학교 정보보호학과 석사과정
<관심분야> 사이버보안, 정보보호