제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

정보기술 발전에 따른 사이버위협의 재조명

정 관 진*
* 안철수연구소 시큐리티대응센터

요 약

IT(정보기술)의 비약적인 발전은 사회전반의 시스템이 IT 인프라에 의존하게 만들었고, 21세기 큰 변화의 핵심 키워드중의 하나로 자리잡게 하였다. 정보기술은 비즈니스와 경제등 모든 영역 부분에서 그 역할의 범위를 넓혀가며 사이버공간 안에서 또 다른 가상의 세계가 만들어지고 있는 것이다. 빠르게 변화하고 있는 이러한 흐름에 과연 우리는 외부의 위협으로부터 어떻게 대처하고 있으며, 정보기술의 발전이 가져다 준 다양한 편익 앞에 사이버 위협의 또 다른 이면을 살펴보고 디지털의 변화와 위협을 재 정립해 보고자 한다.

Cyber Threat under growth of Information Technology

Jung Kwan Jin

ABSTRACT

IT, the information technology's dramatic growth made entire society's system to rely on it, and took its place as one of the core keyword of 21st centurie's big variety. It is enlarging its role boundaries to most territories such as business or economy, and making another cyber space within cyber space. This report is going to review how we are defending ourselves from external threat within such dramatic flow of changes.

I. 서론

디지털(Digital)기술의 출현은 과거 우리의 삶을 빠른 속도로 바꿔나가고 있으며, IT(Information Technology) 물결과 함께 변화를 더욱 가속화시키고 있다. 개인, 기업, 국가 그리고 더 나아가 전 세계가 하나의 네트워크로 형성되며 근본적인 생활 양식의 변화를 요구하고 있는 것이다. '0' 과 '1' 은 이제 경제의 흐름을 바꿔놓고 있으며, 기업들은 인터넷을 통하여 신기술을 이용한 비즈니스를 수행하고 있다. 이렇게 디지털은 생각했던 것 이상의만큼이나 우리 생활의 깊숙이 들어와 있다. 디지털이 생활의 일부분을 차지하고 있는 만큼 디지털의 병폐는 사이버상에서 많은 문제점들을 점점 야기하였고 지금 현존하는 사회에서의 위협들이 사이버 공간에서 또 다른 위협으로 자리잡은 것이다.

이제 디지털이라는 수식어는 우리의 일상에서 자연스럽게 사용되고 있고 산업, 경제 사회 전반의 시스템이 IT 인프라에 의존하고 있는 비중이 높아지고 있다. 이것은, 교통, 전력, 통신등 국가의 주요 인프라가 이제는 물리적 위협뿐만 아니라 사이버공간에서의 위협에도 노출되어 가고 있다는 점이다. 또한, 디지털화로 인한 큰 변화중의 하나가 바로 '속도' 이다. 시공간을 뛰어넘어 빠른 속도로 디지털에 의존하여 정보를 교환하고 시시각각 변화하는 흐름을 반영하고 있다. 바로 이 '속도' 라는 것이 현 사이버 공간을 더욱 크게 위협하고 있는 요소중의 하나이다. 세계는 인터넷이라는 거대한 네트워크에 연결되어 있으며, 사이버상의 작은 위협의 시작이 큰 영향을 줄 수 있는 것과 같이 오히려 역으로 보면 이 '속도' 의 개념이 사이버상의 위협에 큰 무기가 될 수 있는 것이다. 이러한 것을 증명해 주는 사례가 바로 2003년 1월 25일 국가적으로 인터넷마비를 가져온 슬래머(Slammer)웜이다. 376byte의 작은 패킷 하나가 전세계를 일순간 인터넷공황 상태를 몰고 온 것이다. 이렇게 큰 영향을 줄 수 있었던 것에 바로 디지털이라는 문명이 일조를 담당했고 전세계를 감염시키는데 까지는 채 10분이 걸리지 않을 만큼 빠른 속도로 전파될 수 있었다. [1]

우리는 이 디지털 속도와 시큐리티 패러다임의 변화에 능동적으로 대처할 필요가 있는 것이다. 이제 사이버상의 위협이 사이버테러로 까지 불리고 있는 이 시점에 위험수위 변화를 계속 주시해야 한다. 이것은 시대의 변화에 맞춰 변화해 가는 것이 기업에 있어서 생존경쟁이고 사이버위협은 변화에 따라 당면한 새로운 과제이며 우리가 풀어나가야 할 문제이다. 사이버위협의 공격과 이에 대한 방어 수준이 변화하고 있고, IT 변화의 흐름에 발맞춰 새로운 디지털 시대에 사이버상의 위협에 대해 재 조명해 볼 필요가 있다.

II. IT 변화의 흐름

오늘날 디지털 기술의 발전에 따라 IT는 괄목한 만한 성장을 이뤄왔다. 앞으로 발전의 속도는 더욱 빨라질 것이며, 그 주기는 지금과 비교해 크게 앞당겨질 것이다. 이것은 곧 기술의 발전속도에 따라 위협 수준 또한 같이 증대된다는 것이다. 변화의 속도가 위협의 속도 또한 바꿔놓고 있다. 더불어 발

전되는 IT 현상은 더욱더 고도화 되어 가고 있으며, 복잡화 그리고 관리의 어려움을 보여주고 있다. 이런 현실은 사이버위협 대상의 범위를 더욱 넓혀주고 노출의 범위가 늘어나 위험을 가중시키게 된다. 이러한 위협 요소는 다음과 같이 정리될 수 있다.

첫째, 컴퓨팅파워의 증대가 또 다른 위협을 가져올 수 있다. 컴퓨팅파워는 빠르게 발전하여 개인용 컴퓨터의 수준이 과거 중형급 이상의 컴퓨터성능을 지니고 있다. 이러한 고 성능이 역 이용되어 사용된다면 그 피해는 현재의 위협을 배가시키게 될 것이다. 분산서비스 거부 공격에 에이전트로 이용되거나 웜에 감염되어 또 다른 전파대상자를 찾는다면 이 속도는 컴퓨팅파워의 발전속도에 따라 같이 증대될 것이다. 최근의 UCI(University of California,Irvine)의 연구조사 팀에 의하면 나노 기술을 이용한 나노튜브 트랜지스터를 이용하여 훨씬 더 빠른 속도의 컴퓨터를 만들 수 있을 것이라 하였다. 이론적으로는 테라헤르츠(1 THz=1,000GHz) 속도가 가능하여 현재 컴퓨터 속도의 1,000 배 이상의 빠른 속도를 가질 수 있을 것이라 전망한 것이다. [2] 이뿐만 아니라 클러스트링(Clustering), 그리드(Grid) 기술의 발전과 다양한 프로젝트들은 더욱 빠른 속도를 갈망하는 인간의 욕구를 해소하기 위하여 계속 증대될 것이다.

둘째, 초고속인터넷의 보급과 네트워크 형성이다. xDSL의 대중화로 이제는 일반가정에서도 쉽게 인터넷을 사용할 수 있게 되었다. 특히, 한국의 경우는 전 세계에서 초고속 인터넷 보급률 세계1위를 차지할 만큼 인터넷 인프라의 발전은 빠르게 성장하고 있다. 국제전기통신연합인 ITU(International Telecommunication Union)에서 발표한 2002년 보고서에 따르면 초고속 인터넷 서비스 보급률이 인구 100명당 21명으로 다른 나라에 비해 높은 수준을 보여주고 있다. [3] 한국뿐만 아니라 전세계적으로 인터넷 연결 비용이 저렴해 지고 인프라가 지속적으로 발전하며, 각 가정의 컴퓨터뿐만 아니라 향후에는 가전제품에 이르기까지 네트워크가 연결될 것이다. 네트워크 형성의 범위가 넓어지며, 전 세계는 디지털 글로벌화 되어 가고 있다. 이것은 과거와는 다르게 비즈니스 모델뿐만 아니라 삶의 양식 그리고 전쟁의 양상까지도 새롭게 바꿔놓고 있다. 이제는 전세계가 네트워크화 되어 가고 있다.

셋째, 구조의 복잡화다. 시스템과 네트워크의 의존도가 증가함에 따라 구조는 더욱 복잡해 지고 관리의 범위가 넓어지게 되어 이러한 복잡한 구조에 따라 발생되는 보안적인 홀(Hole)이 커지게 된다. 시스템이 많아지게 되면 관리의 범위에서 벗어나는 시스템이 발생할 확률이 높아지게 되고 이로 인한 위협의 범위가 늘어나게 된다. 네트워크 구조 및 보안정책 또한 마찬가지로 구조가 견고하게 설계되어 있다 하더라도 잘못된 구성, 방화벽과 IDS 룰 오류 등으로 전체 시스템, 네트워크가 위험해 질 수 있는 결과를 낳을 수가 있다. 갈수록 고도화 되어 가고 있는 공격과 늘어나는 다양한 위협으로부터 보호하기 위한 다단계로 구성되는 하드웨어, 소프트웨어 본질 자체가 취약점을 가질 수 있어, 구성의 복잡성과 관리의 어려움으로 인한 문제가 더욱 커지게 될 것이다.

앞서 언급한 것과 같이 발전하는 IT의 변화로 인한 사이버위협은 증대되고 있다. 이런 위협요소의 존재는 정보전으로 까지 활용되어 사이버범죄, 전쟁, 테러에 이용될 수 있는 잠재적 위협을 안고 있는 것이다. 특히나 교통, 금융, 에너지 그리고 국가 시스템망에 대한 인프라의 보호가 더욱 중요해 지고 있다. 이러한 국가 정보 인프라는 경제 및 사회 전반적으로 근간이 되는 기반 망으로써 어떤 위협으로부터도 안전하게 보호되고 운영될 수 있어야 하며, 국가의 인프라가 위협을 받아 흔들리는 경우 큰 혼란을 가져오게 될 것이다. 개별적인 단위 시스템이 아닌 사회전반적으로 인프라에 대한 보호와 함께 IT변화의 흐름에 따라 외부의 사이버위협에 대처할 수 있는 대응능력이 필요하며, 기술이 변화의 발전을 겪듯이 사이버상의 공격과 방어 또한 함께 진화한다는 점을 되새겨야 한다.

III. 사이버공간의 위협

전세계가 인터넷이라는 거대한 네트워크에 연결되며 과거에는 상상할 수 없었던 위협들이 사이버공간에서 발생하고 있다. 사이버공간에서는 물리적으로 떨어져 있어 할 수 없었던 많은 일들이 몇 초 사이에 이뤄지고 있는 것이다. 초기의 위협대상도 비록 전세계라는 대상 범위가 있었지만 특정 범위로 그 영역이 한정되어 있었던 것에 비해 공격대상의 범위가 더욱 넓어져 가고 있다. 초기 정보통신 인프라가 비교적 빠르게 적용되고 있었던 국가 기간망 및 기업의 범주에서 벗어나 초고속 인터넷망이 각 가정에까지 빠르게 확산되며 일반 개인에게 까지 영역이 넓어지고 있는 것이다. 빠른 속도로 발전하고 있는 IT 인프라가 역으로 위협대상의 범위를 넓혀 주고 있으며, 향후에는 모바일 및 가전산업에 까지 그 영역대상이 확대될 것이다. 이처럼 늘어나는 사이버위협에 대해 다양한 각도에서 조명해 보고자 한다.

1. 사이버공격 유형과 전망

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. 이것을 기준으로 사이버공격의 주요 유형에 대해 진단해 본다.

(1) 악성코드(Malicious Code)

과거 인터넷이라는 사이버 공간에 연결되어 있던 컴퓨터가 많지 안았던 시절에는 바이러스[1]의 비중이 높았지만 이제는 악성프로그램[2]으로 통합되어 웜, 트로이목마, Hoax 등을 지칭하는 것이 되었다. 네트워크화 되어 가며 수 많은 컴퓨터들이 인터넷에 연결되며 이제는 바이러스가 아닌 웜이 큰 비중을 차지하게 되었다. 환경변화에 따라 악성코드의 형태가 변화하며 다음과 같은 특징을 지니게 되었다.

- 다중전파 방법
- 다중공격 방법
- 다중보호 방법

위와 같은 '다중' 방법은 확산과 피해를 극대화하기 위한 웜 스스로의 진화 발전과정에 기인한 것이다. 웜의 기본적 전제인 확산을 극대화하기 위해서는 메일, 네트워크, 공유폴더, 취약점이용과 같이 1개 이상의 전파경로를 사용한 다중전파방법과 안티바이러스(Anti-Virus) 제품의 진단과 치료를 방지하기 위한 자기보호 차원에서는 스텔스 기법, 암호화, 압축등의 방법을 이용한 것들이 다중보호 방법의 일환이다. 이것은 생물학적인 바이러스가 백신 예방접종에 시간이 지나면 점차 내성이 생기는 것과 마찬가지로 자기 스스로를 외부로부터 보호하기 위한 방안중의 하나이다. 더불어, 이제는 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. 이러한 사이버위협 증대에 더해주는 것이 웜의 효율적인 확산을 위하여 취약한 시스템을 스캐닝(Scanning)하여 감염시키는 'Warhol Worm' 개념으로 인터넷의 모든 시스템을 15분 안에 감염시킨다는 이론이다. 이 보다 더 나아가 30초안에 감염시킨다는 'Flash Worm' 이론 또한 이러한 위협에 큰 힘을 실어주고 있다. [5][6]

최근의 웜 사례를 들여다 보면 "보안적인 취약점"을 이용했다는 공통점을 가지고 있다. 2003년 1월 25일 사상 초유의 인터넷 마비라는 사건의 주인공인 Slammer 웜은 마이크로소프트 SQL 서버의 취약점을 이용하였고, Blaster 와 Welchia 웜은 RPC(Remote Procedure Call)의 버퍼오버플로우(Buffer Overflow)취약점을 이용한 것이다. 가장 최근의 2004년 5월에는 마이크로소프트사의 윈도우 운영체제의 LSASS 취약점이 발표되고, 해당 취약점을 이용하는 공격코드가 발표된 후 얼마 지나지 않아 '새서(Sasser)' 가 나타나 전세계에 확산되어 큰 피해를 안겨주었다. 새서로 인하여 유럽의 한 대규모 텔레비전 방송사가 피해를 입었으며, 대만의 우체국 3곳에서도 업무가 일시 중단되는 등 크고 작은 사고들이 발생하였다. [7] 이외에 Witty 웜은 ISS(Internet Security Systems)사의

---

[1] 사용자 몰래 다른 곳에 자기 자신을 복제하는 프로그램

[2] 다른 사람에게 심리적, 실질적인 피해를 입히는 컴퓨터 프로그램 또는 실행 가능한 부분. 제작자 실수로 포함된 버그는 제외되나 광범위한 피해가 예상될 경우는 포함 [4]

BlackICE 방화벽 취약점을 이용한 것으로 외부의 침입으로부터 시스템을 보호하기 위한 보안소프트웨어 제품이 취약점에 노출되며 일순간 보안 소프트웨어의 제 기능을 발휘하지 못하도록 한 것이다. 보안 소프트웨어만으로는 안전할 수 없다는 것을 단적으로 보여주고 있으며, 악성코드가 사이버상의 위협에 얼마나 큰 영향을 줄 수 있는가를 보여주고 있다.

(2) 서비스거부공격(Denial of Service)

다양한 사이버 위협요소중 DoS(Denial of Service)는 정상적인 서비스를 방해하는 형태로 최근의 윔, 트로이목마에 까지 쓰이며 일반적인 공격형태 중의 하나가 되었다. DoS 의 공격형태도 초기 특정 시스템에서 특정 시스템을 공격하는 1:1 의 관계에서 벗어나 특정 시스템이 여러 시스템을 공격하는 1:N 으로 변모하였다. 하지만, IT 의 급격한 발전은 하드웨어의 성능과 네트워크 대역폭을 크게 확장시키게 되었고 단순한 1:1, 1:N 의 공격으로는 한계를 갖게 되었다. 결과적으로는 공격이 큰 효과를 발휘하지 못하기 때문에 또 다른 변화가 필요하였고 바로 네트워크에 연결되어 있는 분산된 컴퓨터 인프라를 이용하는 구조인 DDoS(Distributed Denial of Service)공격으로 발전하게 된 것이다.

N:1 또는 N:N 의 관계가 현재의 IT 인프라로 인하여 나타난 또 다른 위협대상인 셈이다. 이미 지난 2000년2월 인터넷상에서는 Yahoo, eBay, Amazon, ETrade Group, CNN 의 유명한 사이트들이 DDoS 의 공격을 받아 언론에서도 크게 언급된 적이 있다. 이외에도 코드레드(CodeRed)웜은 www.whitehouse.gov 에 DoS 공격이 이뤄지도록 설계되어 있어 코드레드에 감염된 시스템들이 일제히 미 백악관 웹 사이트에 수 많은 트래픽을 유발시켰다. DoS 공격 형태에도 다양화, 고급화를 추구하고 있어 IP Spoofing, TCP (SYN|ACK|FIN|RST) Flooding. UDP Flooding, ICMP Echo Request/Reply 와 같은 다양한 형태들이 존재한다. 이러한 다양한 방법에 DDoS 보다 한 단계 발전한 DRDoS(Distributed Reflection Denial of Service)가 나타났다. [8] 이것은 인터넷 흐름의 중심이 되는 라우터를 이용한 것으로 인터넷의 인프라를 역으로 공격에 활용한 예이다. 발전단계에 따라 공격방법의 진화를 보여준 공격형태의 하나로 이러한 DoS 공격은 현재의 구조상 뚜렷한 근본대책이 없어 시스템 자원의 고갈과 네트워크 대역폭 소모를 가져와 정상적인 서비스를 방해하고 있다. 이런 위협요소를 줄이기 위하여 대역폭의 제한과 QoS(Quality of Service), Spoofing 되어 발생되는 DoS 트래픽을 분석하기 위한 BackScatter [9]등의 다양한 대응방법들이 마련되고 있다. 바로 공격의 발전에 따라 대응방법도 다양해 지고 있는 것이다.

(3) 복합적 공격(Compound Attack)

사이버공간에서의 디지털 공격뿐만 아니라 물리적인 공격 피해 또한 극대화하기 위한 방법은 복합적인 공격형태를 취하는 것일 것이다. 이러한 것은 비단 공격도구의 변화 형태를 보기만 하더라도 알 수 있는 것으로서 사이버 공격도구들이 기존 한가지 공격 기능만을 가지는 것이 아니라 복합적으로 다양한 공격 방법들을 포함하고 있다는 사

실이다. 사이버 위협요소 중의 하나인 웜 바이러스도 한 가지의 공격패턴을 갖는 것이 아니라 앞으로는 지금보다 더욱 다양한 공격형태 양상을 갖추게 될 것이다. 사이버 공간을 떠나 물리적 공격에 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.

(4) 구조적 환경을 이용한 공격 고도화와 인프라의 복잡화

위협의 지능화는 현재의 IT인프라 발전과도 밀접한 연관관계를 맺는다. 변화 추이와 구조적 환경을 사이버 위협에 반영하기 위한 결과이다. 공격기법이 고도화 되어감에 따라 자연스럽게 방어기술 또한 같은 행보를 걷는 것은 당연한 이치이다. 최근의 위협범위와 그 피해가 증가함에 있어 내부의 인프라를 보호하기 위한 조치로 네트워크는 더욱 견고하게 설계되며 다단계 층의 보호장벽 마련을 하고 있다. 이러한 조치는 복잡함을 가중시키게 되지만 외부로부터의 위협에는 더욱 안전해진다. 하지만 이런 복잡한 인프라에 따른 설정오류 증가와 방화벽의 정책 및 IDS(Intrusion Detection System), IPS(Intrusion Prevention System)를 우회하여 위협을 가중시키는 전문적인 지식들이 계속 결합될 것이다. Welchia 웜이 사용한 역방향 쉘(Reverse Shell) 코드 실행이나 일반적으로 방화벽 정책에서 오픈 하는 TCP 80번 포트의 웹 애플리케이션 취약점을 이용하는 방법들이 방어망을 뚫기 위한 시작단계이다. 바로 IT인프라의 구조적 환경을 이용한 공격수법과 함께 전문지식이 결합되어 넓게 사용될 것이다.

(5) 인터넷 운영 중요 인프라 공격

인터넷과 같은 전체 큰 네트워크를 효과적으로 공격하기 위한 방법은 무엇일까? 바로 인터넷 운영에 기반구조가 되는 인프라일 것이다. 기반 구조에 큰 위협을 줄 수 있다면 이것은 사이버공간 전체에 큰 영향을 주게 되는 결과를 가져오기 때문이다. 2002년 13 개의 상위 DNS(Domain Name System) 서버에 가해졌던 DoS 공격[3]으로 인하여 DNS 라는 중요 인터넷운영시스템 하나가 인터넷에 얼마나 큰 영향을 주는지 보여주었던 계기였다. 이뿐 아니라, 인터넷 흐름에 중요한 역할을 담당하고 있는 라우터가 정상적인 흐름의 경로가 아닌 공격자에 의도된 경로로 변경된다고 가정하면 큰 혼란을 초래할 것이다. 인터넷의 영역은 더욱 확장되고 있으며 이에 따른 인터넷 운영인프라의 의존 비중 또한 크게 높아질 것이다. 공

[3] ICMP(Internet Control Message Protocol)를 이용한 서비스거부공격

격에 있어서도 하위 여러 시스템 보다는 상위 관문이 되는 곳을 목표로 한다면 이루고자 하는 목적을 빨리 달성할 수 있게 되는 것과 같은 원리이다. 즉, 인터넷운영 주요 인프라에 대한 위협이 증가될 것이다.

2. 테러리스트 그룹의 위협

2001년 9월 11일 뉴욕 금융가에 위치한 세계무역센터의 테러공격은 전세계를 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 사이버 공간에서 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 넓어지기 때문이다. 바로 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 알카에다(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. [10] 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. [11]

테러리스트 그룹들이 인터넷을 활용하는 비중이 늘어나며 이에 대한 우려는 더욱 붉어지고 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. [12] 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. 총성 없는 사이버 전쟁

물리적 공간의 영역이 사이버공간으로 이동하며 이제 과거의 해킹이나 취약점을 이용하여 공격하는 불법적 행위를 넘어서 인터넷 여론을 형성하거나 국가나 단체에 대항하는 압력수단으로 이용되고 있다. 해커, 크래커에서 정치적 목적 성향을 가진 핵티비즘(Hacktivism)이 확산되며 사회와 국가안보에 또 다른 위협범주로 발전하고 있는 것이다. 이러한 일례로, 2003년 초 전쟁에 대한 불안감으로 인한 유가상승, 금융불안, 경제성장 악화가 지속되며 마침내 3월 20일 우려했던 미·영 연합군의 이라크 공격이 시작되었다. 전 세계의 도시 곳곳에서는 반전시위로 들끓었으며, 전쟁에 반대하는 메시지를 담은 웹 페이지의 변조가 하루에도 몇백 건씩 발생하였다. 웹 페이지 변조뿐만 아니라 분산서비스거부공격, Wanor(No War)[13] 와 같은 전쟁관련 웜들이 나타나며 공격양상이 더욱 다양하게 이뤄지며 사이버 공간에서의 위협이 크게 증대되며 우려를 자아냈다. 이렇게 물리적인 공격이 사이버공간으로 까지 확대되어 나타나고 있으며 주요 사건으로는 다음과 같다. [14]

- 카슈미르지역에 대한 인도와 파키스탄 대립
- 이스라엘과 팔레스타인의 유혈사태
- 코소보사태
- 중국 남부지방의 공해상에서 미 해군 정찰기와 중국전투기 충돌사고
- 이라크전쟁

21세기 정보통신의 발전에 따라 미래의 전쟁은 현재와는 다른 전쟁형태를 예고하고 있으며, 사이버공간은 이제는 더 이상 단순한 정보이상의 공간으로 IT 발전에 따라 자연스럽게 전쟁의 장소가 사이버공간으로 까지 넓어진 것이다. 이러한 사이버전쟁의 양상은 국가간 전쟁으로까지 비화될 수 있으며 이것은 사회 전반에 큰 영향을 주게 될 것이다. 물리적 공격이 사이버공간으로 확대되는 것 이외에 의도적으로 준비되는 사이버전쟁에 대한 대처가 필요하다. 정보통신 인프라가 일찍이 잘 갖춰진 나라는 사이버위협의 현실을 발 빠르게 인식하고 이에 대한 준비를 지속적으로 해오고 있다. 이것은 사회전반의 많은 인프라들이 IT 환경에 의존하는 비중이 높아지며 이에 따른 당연한 결과이다. 국가적인 차원에서의 준비도 필요하지만, 기업들의 인프라 보호를 위한 CERT(Computer Emergency Response Team)의 운영과 같은 자체적인 노력의 준비도 잊어서는 안 된다.

IV. 사이버위협의 대응 체계

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. [15] 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. [16] 유럽연합은 회원국 정부들간 인터넷을 보호하는 기구를 설립하여 진행중인 유럽네트워크정보보안청(ENISA: European Network Information Security Agency)이 있다. [17]

사이버 위협을 인지하고 사전에 대비하기 위하여 각 국은 사이버 위협을 전담하는 조직을 창설하고 관련 법규를 정비하는 등의 다각적인 노력을 보이고 있다. 우리나라 또한 다양한 사이버테러 대응체계를 갖추고 있었지만 작년 초 1월25일 인터넷대란에 큰 허점을 보이면서 국가적으로 사이버테러 대응을 위한 행보가 발 빠르게 이어지며 2003년7월24일 국가사이버테러대응체계 구축 기본계획이 대통령 재가를 받은 후, 2004년 2월 20일 국가사이버안전센터(NCSC: National Cyber Security Center)가 개소하게 되었다. 사이버안전센터는 국가, 공공분야를 담당하며 KISA(Korea Information Security Agency)의 인터넷침해사고대응지원센터는 민간분야, 국방부의 국방정보전대응센터는 국방분야를 맡아 체계적인 사이버위협 대응체계를 갖춰나가고 있다.

하지만, 이러한 조직체계만으로는 사이버공간상에서 일어나는 위협에 효과적으로 대처할 수가 없다는 점을 잊어서도 안되겠다. 한쪽만이 잘 해서 위협에 대응할 수 있는 체계가 나오는 것이 아니기 때문이다. 사이버공간에서의 다양한 위협으로부터 보호하기 위한 방법은 기업이나 개인간의 팀워크에서 나오는 팀 플레이와 같은 협업이 필요한 것이다. 개인, 기업 그리고 국가의 독립적인 행동으로는 인프라를 보호하기 어려운 것이며, 모든 각각의 분야에서 유기적인 협력만이 위협으로부터 안전하게 정보 인프라를 보호할 수 있다. 이런 협력 대응 체계 조직이야 말로 개별 독립체 혼자서 성취할 수 있는 것 이상의 커다란 성과를 이룰 수 있게 만들어 줄 것이다.

V. 결론

디지털 환경 변화에 따라 전세계는 빠르게 움직이고 있다. 과거에는 생각하지 못했던 일들이 디지털 업적에 힘입어 현실로 나타나고 있으며 IT 인프라의 발전은 전세계를 하나로 묶어주고 앞으로 변화할 세상을 말해 주고 있다. 다가올 미래를 예측하는 것은 어렵지만 현재의 IT 상황과 기술 발전

속도를 가늠해 본다면 변화를 미리 예상해 보는 것은 가능하다. 이런 요인들을 통해 사이버 공간에서의 변화를 이해함으로써 개인과 기업 그리고 국가에까지 어떤 변화가 닥쳐올 지에 대해 예견하여 위협으로부터의 준비를 마련해야 한다.

정보기술의 발전은 사이버공간의 영역을 더욱 넓혀줄 것이며, 이에 따른 위협은 협력(Cooperation)을 더욱 강조하게 될 것이다. 협력대응체계를 통하여 공동목표 가치인 위협으로부터의 안전을 달성하고 이러한 협력을 위해서는 전략적인 체계와 표준이 필요하다. 단기적 관점이 아니라 장기적인 관점에서 볼 수 있는 시각으로 계속적으로 진화하는 기술과 이에 맞서 사이버테러에 대비에 적극적으로 참여함으로써, 위협을 예상하고 그에 맞춘 보호조치가 지속적으로 이뤄져야 한다. 앞으로의 미래 정보기술 발전은 생활양식의 패턴을 변화시키며, 글로벌화를 더욱 가속화 시키고 과학기술의 발전에 따라 또 어떤 위협이 우리에게 다가올지 알 수 없다. 바로 IT 발전과 이에 따른 위협의 상관관계를 잊지 말아야 할 것이다.

참고문헌

[1] CAIDA, "Analysis of the Sapphire Worm", Jan. 2003, http://www.caida.org/analysis/security/sapphire/

[2] Cal-(IT)² (California Institute for Telecommunications and Information Technology), "Nanotransistors Promise Super Speed", Apr. 2004, http://www.calit2.net/

[3] ITU, "Top 15 economies by 2002 broadband penetration", 2002 http://www.itu.int/ITU-D/ict/statistics/at_glance/top15_broad html

[4] 안철수연구소, "컴퓨터 바이러스 vs 악성프로그램", 2001년4월

[5] Nicholas C Weaver, "Warhol Worms: The Potential for Very Fast Internet Plagues",http://www.cs.berkeley.edu/~nweaver/warhol.html.

[6] Stuart Staniford, Gary Grim, Roelof Jonkman, "Flash Worms: Thirty Seconds to Infect the Internet", Aug. 2001,http://www.silicondefense.com/flash/,Silicon Defense.

[7] 연합뉴스, "컴퓨터 바이러스 새서 전세계 확산", 2004년5월4일자 기사

[8] Steve Gibson, "Distributed Reflection Denial of Service", Feb. 2002, http://grc.com/dos/drdos.htm

[9] David Moore, Geoffrey M. Voelker, Stefan Savage, "Inferring Internet Denial-of-Service Activity", Proc. of USENIX Security Symposium, 2001

[10] PBS, "Interview with Richard Clarke, the former White House cyber security adviser, from October 2001 to March 2003", Mar. 2003 , http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html

[11] USA TODAY, "Terrorist instructions hidden online", Feb. 2001

[12] Mudawi Mukhtar Elmusharaf, "Cyber Terrorism : The new kind of

Terrorism", Apr. 2004,
http://www.crime-research.org/news/04.12.2004/207

[13] 안철수연구소,
"Win32/Wanor.worm.71168",
2003년3월21일,
http://info.ahnlab.com/smart2u/virus_detail_1137.html

[14] Michael A. Vatis, "Cyber Attacks During The War on Terrorism : A Predictive Analysis", Sep. 2001

[15] 국가보안기술연구소,"미국의 국가 사이버보안 및 국방 정보전 대응 체계", 2003년4월

[16] @police,
http://www.cyberpolice.go.jp/english/index.html

[17] ENISA(European Network and Information Security Agency),
http://www.enisa.eu.int/

정관진

1997년 ~ 2000년 NEXTEL System Engineer
2000년 ~ 2002년 PSINet Korea System and Network Security Engineer
2002년 ~ 현재 안철수연구소 주임연구원