情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

정보전 위협과 사례

박 상 서*, 박 춘 식*

요 약

미래의 분쟁은 비대칭적인 형태로 나타날 것이며, 특히 사이버공간에서 사이버수단을 이용하여 전개될 것으로 예측되고 있다. 특히, 군사 강대국들뿐만 아니라 분쟁의 주체가 되는 여러 국가들은 정보전을 새로운 국가 전력의 핵심 요소로 판단하고 관련 능력 확보에 박차를 가하고 있다. 본 고에서는 정보전 위협과 사례를 고찰함으로써 이러한 국제 상황하에서 우리가 대비하여야 할 방향을 정립하는데 도움이 되고자 한다.

Ⅰ. 서 론

공식견해가 아니라는 단서를 붙이기는 하였지만, 일본 방위청이 20년후 전개될 세계의 전략환경을 예측하고 향후 추진해야할 일본의 방위전략 방향을 공개한 보고서[1]에서는 미래 군사력의 행사 양상은 다음과 같이 4가지로 구분하였다.

- ○ 핵병기라는 "압도적인 힘"에 의한 통제
- ○ "효율적인 힘"의 행사
- ○ "억제된 힘"의 행사
- ○ "비대칭적인 힘"의 행사

이 중에서 정보전 측면에서 관심있게 보아야 할 부분은 "억제된 힘"의 행사 측면에서 비살상무기(non-lethal weapons)의 도입을 하나의 과제로 식별하였으며, "비대칭적인 힘"의 행사 측면에서는 향후 "압도적인 힘"이나 "효율적임 힘"을 가지지 못하는 분쟁주체는 비대칭적인 수단을 사용할 것이고, 향후 여러 국가가 사이버 병기 등의 개발에 주력하게 되어 사이버전쟁으로 발전될 가능성이 증대될 것이라고 전망한 부분이다. 이 보고서에서는 20년후의 일본의 안보정책에 있어서 정보전 분야는 핵전략과 버금가는 위상을 갖게 될 것으로 보고 있으며, 사이버전쟁에 대한 국가간 경쟁을 어떻게 해결해나갈 것인지에 대하여 국가적인 차원에서 해결해야할 관건으로 제시하고 있다.

고도화된 탈 산업사회와 경제는 서로 연결된 컴퓨터의 정보와 통신 시스템에 매우 의존적일 수밖에 없다. 그리고 이들이 정교하게 연결되고 있다는 사실 자체가 적이 이용할 수 있는 취약성으로 나타나고 있다. 정보통신 기반을 파괴하는 것은 전통적인 전장에서 교전할 능력이 부족한 국가와 단체가 선택하기에 적합하다. 또한, 중요한 것은 보다 많은 국가들이 정보 기반에 대한 공격을 전략적 타격과 동일하게 여기고 있다는 것이다.

정보전은 그 의미와 포함되는 영역이 광범위할 뿐 아니라, 바라보는 시각에 따라 다양한 형태로 설명될 수 있다. 하지만 정보전은 개인 또는 기업 차원보다는 테러리스트나 정부에 의해 발생한다는 것은 분명하다. 또한, 우리나라에서는 아직까지 정보전이라는 개념이 명확하게 정의되어 있지도 않은 실정이다.

본 고에서는 정보전을 협의의 정보전 즉, 사이버공간과 사이버공간을 구성하는 제 요소에 대한 공격과 방어의 측면에 한정하여 위협을 식별하고, 최근에 발생하였던 사례를 고찰해보고자 한다. 또한, 사이버범죄, 사이버테러, 사이버전, 그리고 정보전은 서로가 구분되는 것이기는 하지만, 사이버테러, 사이버전 그리고 정보전을 같은 의미로 사용하기로 하되, 사이버범죄는 다루지 않기로 한다.

* 국가보안기술연구소 ({sangseo, csp}@etri.re.kr)

Ⅱ. 정보전 위협

1. 사이버 공격을 감행하는 이유

사이버 공격을 감행하는 첫 번째 이유는 심리적 효과이다. 사이버 공격에 의한 데이터 훼손의 심각성에 비해 목표 집단에 대한 장기적인 심리적 효과가 크기 때문이다[2]. 또한, 컴퓨터 네트워크에 대한 공격이 성공하면 컴퓨터에 의존하고 있는 여러 시스템들에 대한 신뢰성이 훼손을 받게 되므로 사이버 공격은 대량 피해를 일으킬 수 있기 때문이다. 이외에도 다음과 같은 이유 때문에 사이버 공격이 활용된다.

- 비대칭성(Asymmetry): 개인 또는 작은 집단만으로도 대량 피해를 일으킬 수 있다.
- 접근성(Accessibility): 물리적 수단에 의하여 정상적으로 보호되고 있는 핵심 기반에 대해서도 피해를 입힐 수 있다.
- 익명성(Anonymity): IP 스푸핑과 같이 일반적으로 이용가능한 도구 또는 여러 대의 중간 매개체 컴퓨터를 이용하고, 여러 국가와 사법권을 통과하기 때문에 전세계적인 정보 네트워크에 은닉할 수 있다. 클린턴 대통령 국가안보 보좌관이었던 앤소니 레이크(Anthony Lake)는 ① 사이버 공격을 감행하였다고 해서 범죄자에게 직접적으로 물리적인 위험을 가하지는 않고, ② 공격은 원격지에서 시작될 수 있으며 익명성을 제공하며, ③ 공격에 사용된 도구와 기술이 상대적으로 간단하다면 대규모 그룹 또는 정부에 의존하지 않고도 개인이 쉽게 독자적으로 행동할 수 있다고 주장하고 있다[3].
- 공격범위(Range): 공격시 물리적으로 가까이 있을 필요없이 전세계 어디든지 목표를 공격할 수 있다. 레이크는 최근에 발간한 그의 서적 Six Nightmares에서 정보 폭발의 시대에서 세계는 점차 통신망으로 연결되고 있기 때문에 사이버테러는 여러 목표를 동시에 겨냥할 수 있다고 설명하고 있다.

2. 정보전 무기[4]

전쟁 무기는 크게 살상(hard-kill) 무기와 비살상(soft-kill) 무기로 구분할 수 있다[5,6]. 정보전에서는 주로 비살상 무기들이 사용되는데, 정보전사(infowarrior)들에 의해 이용될 수 있는 비살상 무기들은 크게 열 네 가지 유형이 있다.

2.1 해킹 기술

해커들은 시스템이나 네트워크의 취약성을 이용하여 해킹을 시도한다. 이들은 시스템의 정상적인 동작을 방해하여 시스템이 사용자가 요구하는 서비스를 처리하지 못하도록 하는 서비스 거부 공격을 감행하거나, Back Orifice를 이용하여 Windows를 공격하기도 하고, 주로 Unix 계열 운영체제의 런타임 스택이 갖는 특성을 이용하여 버퍼 오버플로우 공격을 하거나, CGI 취약점을 이용하여 웹 서버나 홈 페이지를 공격하는 등 다양한 기법과 도구를 이용한다.

2.2 컴퓨터 바이러스

컴퓨터 바이러스는 '70년대 미국방성 Alpha-Net에서 처음 발견된 이래, 최근에는 하루에도 5 - 10개의 새로운 것이 만들어지는 것으로 파악되고 있다. 바이러스들은 인터넷의 영향으로 인해 점차 그 확산 속도가 빨라지고 있다. 불과 5년 전만 해도 컴퓨터 바이러스가 전세계적으로 퍼지는데 2년이 걸렸으나 최근의 조사에 따르면 불과 몇 시간밖에 걸리지 않고 있다.

2.3 웜

웜은 스스로 전파되는 악성 코드로서, 전파를 위하여 사람이 개입하여야 하는 바이러스와 달리 웜은 스스로 전파될 수 있다. '88년 11월 2일 최초로 발견되었을 당시, 웜은 컴퓨터, 네트워크 그리고 사용자에 대한 정보를 입수한 뒤, 다른 시스템의 소프트웨어적 취약점을 이용하여 해당 시스템에 침투하고, 자신의 복사본을 만들어 또 다른 시스템으로 옮기는 방법으로 수천 대의 컴퓨터들의 정상적인 동작을 방해하였으며, 인터넷을 며칠 간 마비시켰다. 최근들어, 웜은 고수준으로 자동화되어 있을 뿐 아니라 그들이 이용하는 취약성이 상대적으로 광범위하기 때문에 몇 시간만에 수많은 시스템을 감염시킬 수 있다. 실례로, Code Red는 2001년 7월 19일 단지 9시간만에 25만대 이상의 시스템을 감염시켰다. 또한, 서비스거부 공격을 위한 페이로드(payload)를 내장하고 있고, sadmind/IIS와 Code Red는 웹

사이트 변경 페이로드를 가지고 있을 뿐 아니라, W32/Leaves와 같은 웜은 동적으로 변형되는 능력을 보유하고 있기도 하다.

2.4 트로이 목마

트로이 목마는 정상적으로 보이는 프로그램 내부에 숨어서 시스템이나 네트워크에 해를 끼치는 코드이다. 트로이 목마는 SATAN과 같은 시스템의 보안 취약성 점검 도구와 같은 형태로 위장될 수 있으며, E-mail을 통해 전달될 수도 있다. Net Bus, School Bus나 BO 2K와 같이 강력하고, 사용이 편리한 도구들을 인터넷에서 쉽게 구할 수 있다.

2.5 논리폭탄

논리폭탄은 독립적인 프로그램의 형태, 또는 시스템 개발자나 프로그래머에 의하여 의도적으로 삽입된 코드의 형태를 갖는다. 논리 폭탄은 트로이 목마의 일종으로서 바이러스나 웜 등을 전파하기 위하여 사용될 수 있다. 해니는 정보전에 관련된 그의 논문에서 다음과 같이 언급하고 있다[7]. "MS Windows나 Unix와 같은 소프트웨어들은 대부분이 미국에서 작성된 것이기 때문에, 미국에서는 트로이 목마를 숨긴 소프트웨어만을 외국에 수출하도록 할 수 있다. 논리 폭탄에는 '미국에 대한 전쟁(War against USA)'과 같은 내용을 포함하고 있는 문서가 발견될 경우 컴퓨터 하드디스크를 포맷하거나 특정 정보들을 CIA로 보내는 기능이 숨겨져 있을 수 있다." 이와 같은 의문은 마이크로소프트사에 대해서 아직까지도 의구심을 버리지 않는 프랑스가 open source solution을 정책적으로 선호하고 있음이 언급되고 있고, 전직 CIA 요원이었던 Wayne Madison이 상용 소프트웨어 제품들에 백도어가 있을 가능성이 높다고 경고하면서 논리 폭탄이 정보전 무기로서 갖는 효용성을 입증하고 있다. 논리 폭탄은 이와 같은 내부적 요인뿐 아니라 특정 주파수 등과 같은 외부 요인에 의하여 동작하도록 제작될 수도 있다.

2.6 전자우편폭탄/스팸메일

적대국에 악의적 또는 별 의미없는 내용을 담은 전자우편을 대량으로 발송하여 컴퓨터나 네트워크를 마비시킬 수 있다. 유고전에서는 발신처가 벨그라드인 메일이 해군 항공기지에 200통이 전달된 사례가 있으며, 하루에 2000통씩의 메일이 계속적으로 나토와 미국방성 관련 사이트에 발송된 사례도 있다.

2.7 치핑(Chipping)

특정 조건을 만족하면 동작하는 기능이나 회로를 칩(chip)의 일부분에 하드웨어적으로 삽입하는 공격방법이다. 이 칩에는 얼마간의 시간이 지나면 동작할 수도 있고, 외부로부터 특정 주파수의 전파를 받는 경우 동작하도록 회로가 구성되어 있을 수도 있다.

2.8 나노 머신(nano machine)

나노 머신은 적의 정보 센터 등에 살포되어 컴퓨터 하드웨어를 파괴하는 작은 크기의 로봇이다. 나노 머신들은 컴퓨터를 찾아 사무실 등을 돌아다니다가 슬롯 등의 틈을 통해 컴퓨터에 잠입한 뒤, 기판이나 회로 등을 파괴한다.

2.9 미생물

컴퓨터 기판을 부식시키는 미생물이 있다. 미 육군에서는 컴퓨터 칩에 대하여 공격을 하는 실리콘 박테리아에 대하여 언급하고 있다.

2.10 재밍(jamming)

예전에는 재밍이 적 통신장비간의 통신 채널을 방해하는데 사용되었지만, 앞으로는 정보통신망을 통해 전달되는 패킷들의 유통을 전자적으로 방해하거나 내용을 변경하는 무기로 사용될 것으로 예측되고 있다.

2.11 HERF(High Energy Radio Frequency) gun

라디오 주파수대의 고출력 전파를 발생시켜 전자장비들을 마비시킨다. 이 무기는 수백개의 라디오 기지국에서 수백만 와트의 전파를 한 곳으로 집중시켜 동시에 발사하는 것과 동일한 출력을 발생시키는 무기로서 컴퓨터를 포함하여 전자회로로 구성된 모든 장비들을 셧다운(shutdown)시킬 수 있다.

2.12 EMP(Electro Magnetic Pulse)

EMP 폭탄은 핵폭발이 발생하는 것과 동일한 수준의 전자기파를 발생시킴으로써 이 전자파에 노출

된 컴퓨터나 통신 시스템의 모든 전자회로들이 파괴된다.

2.13 AMCW(Autonomous Mobile Cyber Weapon)

이 무기는 자신이 외부의 조종이나 도움없이 스스로 네트워크를 따라 목표를 찾아 돌아다니며 바이러스 기술 등을 이용하여 적의 컴퓨터나 네트워크 시스템을 파괴하거나 정보를 조작하는 무기로서, 마치 지능을 갖춘 순항 미사일에 비교할 수 있다.

2.14 (분산)서비스 거부((Distributed) Denial of Service: (D)DoS)

서비스 거부 공격은 피해 시스템을 합법적으로 사용하는 사용자가 서비스를 이용하지 못하게 하는 것으로서, 분산 서비스 거부 공격의 경우에는 하나이상의 피해 시스템을 공격하기 위하여 여러 시스템이 활용된다. 또한, 공격 도구의 자동화 정도에 따라 한 명의 공격자가 수만 개의 시스템에 침입하여 도구를 설치하고 제어할 수도 있다. 서비스 거부 공격이 가능한 이유는 첫째, 네트워크가 기본적으로 제한되고 소비가능한(consumable) 자원으로 구성되어 있으며, 둘째, 네트워크 보안이 여러 시스템간에 서로 많은 영향을 미치기(highly interdependent) 때문이다.

3. 최근의 경향[8]

3.1 자동화 공격 도구의 속도 증가

공격 도구의 자동화 수준이 계속 증가됨에 따라 자동화된 공격의 일반적 단계가 "스캐닝 → 침입 → 전이 → 통합관리"로 발전하고 있다.

- 1단계 - 잠재적 희생자 선택을 위한 스캐닝: 1997년 이후 광범위한 스캐닝이 보편화되었다. 최근의 스캐닝 도구는 그 효과와 속도를 최대화하기 위하여 고도의 스캐닝 기법을 사용하고 있다.
- 2단계 - 취약한 시스템 침입: 이전에는 광범위한 스캐닝 완료후 취약성들을 발견하였다. 현재는 공격 도구들이 스캐닝을 일부 수행하면서 취약성을 탐지하고 있고, 이에 따라 취약성의 전파 속도가 증가하고 있다.
- 3단계- 공격의 전파: 2000년 이전에는 공격 도구들이 추가적으로 공격을 진행하기 위해서는 중간 단계에서 사람의 개입이 필요하였다. 현재는 공격 도구들이 스스로 공격을 진행시킨다. 특히, Code Red와 Nimda와 같이 스스로 전파되는 도구들은 18시간 이내에 전세계적으로 확산된 바 있다.
- 4단계- 공격 도구의 통합 관리: 1999년 이후, 분산 공격 도구의 등장으로 공격자들은 여러 망(인터넷 등)에 걸쳐 분산 배치된 수많은 공격 도구들을 관리·조종할 수 있게 되었다. 현재는 분산 공격 도구들은 서비스 거부 공격을 시작하고, 희생자의 스캐닝 및 취약한 시스템의 침투를 보다 효율적으로 수행할 수 있는 능력을 가지고 있다. 또한, Internet Relay Chat(IRC)와 instant messaging(IM) 등과 같이 쉽게 이용할 수 있고 대중적인 프로토콜들을 이용하고 있다.

3.2 공격 도구의 능력 향상

개발자들은 이전에 비해 고도의 기술을 사용하고 있다. 이에 따라, 예전에 비해 분석을 통해 공격 도구의 흔적을 발견하기가 더 어려워졌으며, 백신 소프트웨어나 침입탐지시스템과 같이 공격 흔적을 기반으로 하는 시스템으로 탐지하기도 어려운 실정이다. 정교한 공격 도구들의 한 예로서, 많은 수의 도구들이 침입자와 침투된 시스템간의 자료 및 명령의 전송을 위해 IRC나 HTTP 프로토콜을 사용한다. 결과적으로, 공격 시도와 정상적이고 합법적인 네트워크 트래픽을 구분하기가 어려워진다.

- 포렌식 방해(Antiforensic): 공격자들은 공격 도구의 성질(nature)이 잘 알려지지 않게 하기 위한 기법들을 사용한다. 이를 통해 보안 전문가들이 새로운 공격 도구를 분석하고, 새롭고 빠르게 발전하는 위협을 이해하기 어렵게 하거나 이해하는데 많은 시간이 소요되게 한다.
- 동적 행동(Dynamic Behavior): 예전의 공격 도구들은 하나의 정의된 순서에 따라 공격을 진행하였다. 현재의 자동화된 공격 도구들은 임의 선택(random selection), 사전정의 결정 경로(predefined decision paths) 또는 공격자의 직접적 선택(direct intruder management) 등의 방법을 통해 그들의 패

턴과 행동에 변화를 줄 수 있다.

- 공격 도구의 모듈화(Modularity of Attack Tools): 한 가지 유형의 공격만을 수행하던 예전의 공격 도구와는 달리, 요즘의 도구들은 업그레이드 또는 도구의 일부분을 교체함으로써 재빨리 변경될 수 있다. 이렇게 함으로써 공격이 스스로 진화될 수 있도록 하고 있으며, 각각의 인스턴스가 상이한 형태를 갖도록 스스로 진화되는 다형성 도구가 만들어질 수 있다. 게다가, 공격 도구들은 여러 운영체제 상에서 실행될 수 있도록 개발되고 있다.

3.3 취약성의 신속한 발견

최근 보고되는 새로운 취약성들의 수는 매년 두배 이상씩 증가하고 있다. 이에 따라, 시스템 관리자들이 패치를 적용하기도 어려운 상태이다. 게다가, 매년 새로운 종료의 취약성들이 발견되고 있다. 새로운 취약성을 확인하기 위하여 현존하는 코드를 검토하기 위해서는 수백 개의 소프트웨어 제품에 취약성이 존재하는지 반복적으로 확인하여야 한다. 반면, 공격자들은 취약성 사례를 개발자(또는 제작사)보다 먼저 발견하고 있다. 공격자들이 기술적으로 새로운 취약성을 신속히 발견하고 있기 때문에, "패치 시간"은 점점 더 작아지고 있다.

3.4 방화벽 침투(permeability) 증가

방화벽은 침입자로부터 시스템을 보호하기 위한 초보적인 보호 수단으로 인식되고 있다. 현존하는 방화벽의 문제점은 우선, 전형적으로 구성(configuration)된 방화벽을 통과하도록 설계된 기술이 존재한다는 것이다. 예를 들어, IPP(Internet Printing Protocol) 및 WebDAV(Web-based Distributed Authoring and Versioning) 등이 있다. 또한, "방화벽을 지원하는(firewall friendly)" 것으로 알려지고 있는 몇몇 프로토콜들이 실제로는 전형적으로 구성된 방화벽을 통과하도록 설계되어 있다는 점이다.

3.4 비대칭적 위협 증가

인터넷에서의 보안은 그 특성상 서로 연관관계가 깊다. 인터넷에 연결된 한 시스템이 공격에 노출되면 전세계 인터넷에 연결된 나머지 시스템의 보안 상태도 영향을 받는다. 공격 기술이 발전함에 따라, 한 명의 공격자는 하나의 희생자를 효과적으로 공격하기 위하여 수많은 분산 시스템을 쉽게 이용할 수 있다. 공격 도구 배치의 자동화와 공격 도구 관리의 정교화에 따라 위협의 비대칭성은 계속 증가할 것이다.

3.5 기반 공격의 위협 증가

또 다른 주요 경향중 하나가 DNS와 라우터 등과 같은 정보통신기반에 대한 공격이 증가한다는 것이다. DNS에 대한 공격으로서, DNS가 허위(bogus) 정보를 캐쉬에 저장하도록 함으로써 합법적인 사이트에 대한 트래픽을 공격자가 제어할 수 있는 사이트로 변경한다거나, 취약한 DNS 서버에 침투하여 사용자에게 제공되는 데이터를 변조하는 공격이 발견되고 있으며, TLD 서버(예: ".com")에 대한 대규모 서비스 거부 공격 또는 도메인 등록 정보 가로채는 공격이 나타나고 있다.

라우터 공격으로는 공격자는 보안이 취약한 라우터를 다른 사이트에 대한 공격 근원지로 사용하고나, 스캔 또는 감시(reconnaissance)하기 위한 플랫폼으로 사용하는 경우를 들 수 있다.

이와 같이 주요 정보통신 기반에 대한 공격이 증가함에 따라, 여러 가지 문제점이 함께 발생하고 있다. 우선, 서비스 지속성의 문제가 발생하고 있다. 위협의 비대칭적 특성 때문에 공격자들에게 서비스 거부는 적은 노력으로(low-effort) 많은 영향을 미치는(high-impact) 방법이다. 대부분의 기관에서 인터넷은 초당 1에서 155Mbps 사이의 대역폭을 가진다. 공격은 수백 Mbps 이상의 대역폭에서 발생한 것으로 보고되고 있다. 두 번째는 민감한 정보가 유출되고 있다. 어떠한 바이러스는 자신이 감염시킨 시스템의 파일에 자신을 덧붙인 뒤 감염된 파일을 다른 사람에게 전송한다. 이렇게 함으로써 작성자의 동의도 구하지 않은 채 기밀 정보가 외부에 흘러나가게 된다. 세 번째로, 시간과 자원 소모이다. 보안 사고의 가장 큰 영향은 이를 처리하는데 소요되는 시간과 자원일 것이다. Computer Econimics지는 Code Red의 경제적 영향을 26억달러로 추산했고, Sircam은 13억 달러로 추산했다. 한편, 911 테러로 인하여 IT 및 통신 능력을 복구하는 비용을 158억달러로 추정했다.

Ⅲ. 정보전 사례

정보전 사례중에서 최근에 발생한 미국과 중국간

의 네트워크 전쟁은 직접적으로 상대국을 대상으로 하였으며, 핵티비스트 조직의 최신 수준을 보여주었다는 측면에서 의미를 갖는다. 특히, 중국 홍객 연맹(the Honkers Union of China: HUC)이 주도한 이 전쟁은 어떻게 중국의 핵티비스트들이 그들의 해킹 솜씨를 발전시킬 수 있는지와, 연합 해킹 작전을 수행하기 위하여 관련 그룹들이 어떻게 연합할 수 있는지 보여준 중요한 사례라 할 수 있다.

1. 평시 불특정 다수 대상 정보전 사례

1.1 서비스거부 공격[9]

2000년 2월 eBay, Amazon.com, Yahoo.com, E*Trade.com, 그리고 CNN.com 등과 같이 접속 빈도가 높은 웹 사이트들이 거의 동시에 서비스 거부 공격으로 피해를 입었다.

1.2 Love Letter 바이러스[10]

2000년 5월 출현한 LoveLetter 바이러스는(백신 업체인 시만텍사는 80개 이상의 변종을 찾아냈음) 수백만대의 컴퓨터를 감염시켰으며, 수십억 달러의 피해를 야기하였다. 추적결과, 이 바이러스 원형(original variant)은 단독으로 작성된 것으로 밝혀졌다.

1.3 Code Red[11]

2001년 7월 출현한 Code Red 웜과 변종들은 불과 9시간만에 25만대의 컴퓨터를 감염시켰으며, CERT/CC와 NIPC를 포함한 주요 정보보안 관련 기관들은 이 웜을 인터넷에 대한 가장 현실적인 위협으로 인식하고 있다. 이 웜의 작성자는 아직까지 밝혀지지 않고 있다.

2. 평시 특정 목표 대상 정보전 사례

2.1 미공군 로마 연구실(Air Force Rome Lab) 공격[12]

1994년, 뉴욕에 위치한 미공군 로마 연구실에 대한 공격이 탐지되어 추적한 결과, 당시 16세의 영국 소년이 공중전화를 통하여 인터넷에 연결한 뒤 워싱턴, 시애틀, 뉴욕을 거쳐 로마 연구실에 공격을 시도하였다. 이 소년은 나토사령부, 가다드 우주비행센터(Goddard Space Flight Center), 라이트-패터슨 공군기지(Wright-Patterson Air Force Base) 등도 목표로 하고 있었던 것으로 밝혀졌다. 이 소년은 한국원자력연구소에서 자료를 유출한 것으로 확인된 뒤 체포되었다.

2.2 동남아 위기시 중국의 공격[13]

1997년에 발발하였다. 이때, 동남아시아 경제 위기 때문에 인도네시아에 거주하는 중국인에 대한 격렬한 시위가 있었다. 중국 해커들은 "중국인 반대" 웹사이트를 공격하여 변조하였다.

2.3 솔라 선라이즈(Solar Sunrise)[12]

1998년 2월, 미 국방부는 솔라리스 운영체제의 취약성을 이용한 공격을 받았다. 이 공격은 하버드대학교와 아랍에리레이트연합(United Arab Emirates: UAE)에서 시작되었다. 그 후 UAE와 유타주립대학교에서 공격이 시도되었으며, 나중에는 독일, 프랑스, 이스라엘, UAE, 그리고 대만에서도 시도되었다. 미국방부에서는 이 공격을 매우 조직화되고 체계화된 공격으로 평가하고 있다.

2.4 블랙 타이거 사례[14]

스스로를 인터넷 블랙 타이거라고 부르는 사람들이 1998년 8월에 발생한 전세계 스리랑카 외교 기관(미국 소재 포함)의 전자우편 시스템을 공격한 장본인이라고 주장하였다.

2.5 대만 독립 주장에 이은 공격[13]

1999년 7월에 대만의 리 덩후이(Li Denghui) 총통이 대만과 중국 본토는 분리된 국가로 취급되어야 한다는 주장이 있은 직후 발생하였다. 공격은 대만의 공공 및 상용 사이트 수백개를 대상으로 하였다.

2.6 일본 성청 웹사이트 침입 및 변조[15]

2000년 1월부터 2월에 걸쳐 다수의 중앙 성청 사이트가 침입 및 변조의 피해를 입었다. 많은 경우 홈페이지를 변조하여 중국어나 영어로 일본이나 러시아를 중상하는 메시지를 기술하였다. 과학기술청과 총무성 통계국은 단기간에 2번의 피해를 입었다.

- 1월 24일: 과학기술청 홈페이지 변조
- 1월 25일: 대장성과 통상산업성에 대한 공격

이 시도되었지만 미수로 그침. 총무성 통계국의 홈페이지 데이터와 프로그램이 완전히 소거

- 1월 26일: 과학기술청의 홈페이지가 재공격 당함. 총합연구개발기구(NIRA)의 홈페이지가 변조. 문부성과 방위청에 공격이 시도되었으나 미수에 그침
- 1월 27일: 운수성과 농림수산성의 홈페이지에 공격이 시도되었으나 미수에 그침. 총무청 통계국 홈페이지가 두 번째 침입을 당하여, 변조
- 1월 28일: 일본은행에 공격이 시도되었으나 미수에 그침
- 2월 1일: 참의원 홈페이지 변조

2.7 난징 대학살 왜곡 관련 공격[13]

2000년 1월, 일본의 "난징 대학살(Nanjing Massacre)" 왜곡 및 사과에 관련되어 중국 핵티비스트 그룹이 일본 우익을 공격하였다. 이 사건에서, 외국에 거주하는 중국인들이 본토 중국인 해커들의 행동에 동참하였다.

2.8 일본 제국주의 비난 공격[13]

2001년 2월과 5월에 발생하였다. 중국 핵티비스트들이 일본을 목표로 하였다. 가장 대표적인 공격 이유는 "일본 제국주의의 타도"이었다.

3. 주요 기반시설 침해 사례

3.1 인도 원자력 연구소 침투[15]

1998년 6월, 핵실험에 반대하는 해커 그룹 "miw Orm"이 인도의 바바원자력연구소(BARC)의 컴퓨터 네트워크에 침입, 홈페이지의 일부를 변조하고, 5MB분의 전자메일 파일을 다운로드하였다. 인도 원자력 위원회는 이 사건에서 기밀정보가 누설되었다는 것을 부인하고 있다. 이번 사건을 일으킨 miw Orm의 멤버는 17-18세의 3인으로, 침입시 NASA, 미 해군, 미 공군의 서버를 경유하는 형태로 BARC에 침입한 것으로 알려져 있다.

3.2 루즈벨트 댐 침투[16]

1998년, 당시 12세 해커가 아리조나의 루즈벨트 댐의 컴퓨터 시스템에 침입하였다. 이 댐은 489조 갤런의 물을 담고 있었는데, 이 정도의 양은 피닉스시 일대를 약 5피트 정도의 높이로 덮으면서 흐를 수 있는 양이다. 조사결과 이 해커는 댐의 수문을 조종하는 SCADA 시스템에 대한 완전한 제어 명령을 알고 있었던 것으로 밝혀졌다.

3.3 호주 SCADA 시스템 제어권 상실[16]

2000년 4월, 호주의 퀸즈랜드에서 SCADA 시스템에 침투하여 실제로 제어권을 상실했던 사건이 발생하였다. 혐의자는 훔친 컴퓨터를 이용하여 폐기물 처리 회사의 SCADA 시스템에 침투하여 제어권을 확보한 뒤, 약 40여회 이상 폐기물 운반 차량을 제어하여 호수, 공원, 상업지역 등 여러 곳에 폐기물을 쏟도록 하였다. 이 사건은 SCADA 시스템 제어에 성공한 첫 번째 공격 사례로 기록되고 있다.

4. 분쟁시 정보전 사례

4.1 유고전시 백악관 웹 페이지 공격[17]

백악관과 같이 눈에 잘 띄고 대중적으로 접근 가능한 웹사이트들은 반미 메시지를 게시하기 위한 좋은 목표이다. 1999년 나토의 유고슬라비아 폭격에 흥분한 전자적 침입자들이 백악관 웹페이지를 24시간 동안 정지시켰다. 실제적으로 물리적 피해는 별로 없었지만 수천 명의 미국인들에게 비록 전자적이기는 하지만 백악관의 보안이 다소 미약하다는 인식을 갖게 하는 큰 효과가 있었다.

4.2 유고전시 중국 대사관 오폭에 따른 미국에 대한 공격[13]

1999년 5월 7일, 유고의 벨그라드에 있는 중국 대사관에 대한 나토의 오폭에 대한 반발로 발생하였다. 이 사건이 발생하자 저항자들은 즉각적으로 사이버 시위를 시작하였다. 첫 번째 전술은 웹사이트를 변조하는 것이었다. 중국 해커들은 미국 에너지부, 내무부, 그리고 백악관 웹사이트 등을 공격하였다. 이 때, 인터넷에 몇 개의 특수 목적용 사이트가 개설되어 시위에 대한 기사를 전문적으로 다루었으며, 어떤 사이트에서는 사이버 시위대를 모집하였다. 중국 ISP들은 오폭에 대응하기 위한 방법의 일환으로써 미국과 영국 제품에 대한 불매운동을 제안하였고, 사고에 대한 대응 기록을 알려주는 서비스를 제공하였다. 그 후, 몇 개의 사이트에서는 미국 사이트에 대한 대량 컴퓨터 공격을 시도하도록 권유하였고, 미국 금융 사이트를 대상으로 한 컴퓨터 바이러

스를 배포하기도 하였다.

4.3 중동 무력충돌에 따른 사이버전쟁[15]

2000년 10월말 이후, 미국과 이스라엘에 관련된 사이트, 미국기업사이트, 이스라엘 정부 웹사이트, 그리고 이슬람교 정치세력(팔레스타인 측) 웹사이트에 대한 상호 공격이 발생하였다. 2000년 9월말에 이스라엘과 이슬람과격파 사이에 무력충돌이 발생한 이후 쌍방의 웹사이트에 대한 공격이 되풀이되었다. 각 그룹이 온라인으로 공격의 지원자를 모집하여, 초보적인 전자메일 공격이나 서비스거부공격을 위한 도구를 배포하였으며, 크래커 집단에 의한 조직적 공격도 행해졌다. 11월들어 피해는 미국의 사이트에도 파급되었다. 미국 네트워크 관련 기업이 서비스 거부공격의 대상이 되고, 친이스라엘 압력단체의 웹사이트가 친 팔레스타인 집단의 침입을 받아, 사이트의 변조(슬로건의 게시, 전자메일 통신내용의 폭로), 신용카드 번호나 회원기록의 도난 등을 겪었다. 그 후에도 공격수법은 분산형 서비스 거부공격(Smurf 공격)이나 조직적 침입행위로 격화되었다. 2001년에 들어서도 성명을 게재한 홈페이지의 변조사건이나 정부기관에 대하여 대량의 메일을 발송하는 바이러스의 발견 등이 보고되었다.

4.4 미-중 공군기 충돌 사건에 이은 사이버 전쟁[13]

2001년 5월 1일부터 7일 사이에 발생한 위협은 언론에 많이 공개되어 있다. EP-3 정찰기 사고에 의해 촉발되었으며, 공격 목표는 미국이었다. 사건이 발생하자 심리전이 먼저 시작되었다. 이 때, 미 당국에 의한 보도 기관의 확인을 제외하고는 전세계에서 접할 수 있는 유일한 소식은 신화사에 의해 제공되는 것이 전부였다. 이로 인해, 중국 정부는 초기의 심리·보도전에 있어서 통제권을 갖게 되었다. 중국 당국이 중국 전투기를 추락시킨 공중 충돌의 원인은 미군 초계기라고 비난하자 중국 인터넷 사용자들은 미국에 대한 전쟁을 선언하였다[18]. 특히, 중국 인터넷 사이트의 대화방은 중국과 홍콩의 웹사이트가 반중(anti-PRC) 해커들에 의해 변조되었다는 기사로 가득찼고, 중국 정부 웹사이트가 공격을 받은 몇 시간 후부터 HUC와 China Eagle을 중심으로 본격적으로 반격이 시도되었다. 공격은 워싱턴 해군통신기지국(Washington Navy Communications Station)과 해군광역수송국(Navy Service Wide Transportation) 사이트를 시작으로 백악관 웹사이트 마비까지 이어졌다. 중국측의 보도에 따르면, 백악관 웹사이트에 대한 공격에 8만명이 참여했다고 하며, 중국 이외의 언론 보도에 따르면, 백악관 웹사이트는 거의 6 시간동안 접속이 불가능했다.

〔표 1〕에서 보인 바와 같이 미국은 1,038개의 웹사이트가 변조되었고, 중국은 1,600개의 웹사이트가 침입을 당하였다.

4.5 911테러에 관련된 미국 지지자의 아랍 공격[19]

911 사건이 발생하자 미국 지지자들은 곧 아랍과 빈 라덴에 연결된 컴퓨터 시스템에 대한 사이버 공격을 시작하였다. 9월 14일, 자신이 "디스패처(Dispatchers)"라고 주장하는 그룹이 자신들이 벌써 중동의 ISP를 무력화시켰으며 그 최종 목표는 아프가니스탄의 ISP라고 주장하는 글을 웹에 게재하였다. NIPC(National Infrastructure Protection Center)는 디스패처가 아랍 및 회교도 컴퓨터 시스템에 피해를 입히기 위하여 분산 서비스 거부 공격을 시도하는 동안 의도하지는 않았지만 미국 컴퓨터 시스템에 유사한 피해를 가져올 수도 있다고 경고하였다.

5. 맺음말

본 논문에서는 정보전 위협 요소와 사례를 고찰하였다. 서방세계에 적대적인 것으로 알려져 있는 이라크, 리비아, 중국, 북한, 쿠바, 러시아이외에, 미국을 중심으로 프랑스, 이스라엘, 영국 등에서도 상당한 수준의 정보전 능력을 확보하고 있다. 특히, 미국은 정보전 공격팀을 1999년부터 운영해온 이래, 2002년 10월 1일부로 정보전 공격·방어팀을 전략사령부 산하에 합동으로 편제하기에 이르고 있다.

이제는 미래 정보전에 대비하기 위하여 국가안전보장에 대한 위협요소로서의 정보전 개념을 명확하

〔표 1〕 4월30일부터 5월8일 사이의 중국에 의한 미국 웹사이트 피해 통계

날짜	4/30	5/1	5/2	5/3	5/4	5/5	5/6	5/7	5/8	계
피해사이트 수	26	78	197	383	93	59	89	87	26	1038

게 정의하고, 국가적 차원의 대응 방향과 대응 태세를 정립할 시기이다. 정보전 대응은 국가나 군만의 책임이나 고유의 업무영역이라기 보다는 민관군산학연이 함께 능력과 지혜를 결집하여야 할 분야이다. 특히, 정보전 대응을 위한 기술개발과 함께 인적 능력 양성을 위한 대책 마련에 나설때이다.

참 고 문 헌

[1] 일본 방위전략연구회의, *2020년을 향한 방위전략연구회의 보고서*, 2001. 5.

[2] Ed Sbrocco, Tom Ward, and Chris Baden, *CyberTerror: Potential for Mass Effect*, IA Newsletter, Vol. 4 No. 4, Information Assurance and Technology Analysis Center, 2001.

[3] Lake, Anthony, *6 Nightmares: Real Threats in a Dangerous World and How America Can Meet Them*, Little, Brown and Company, Boston, 2000.

[4] 박상서, *정보전 개념과 대응 기술*, 2001.

[5] 박상서, *정보전 대응체계 구축 현황*, WISC 2000 튜토리얼 자료집, pp. 73-177, 2000. 9.

[6] 박상서, "정보전: 새로운 전쟁 패러다임," *공군 창군 50주년 기념 국제 학술 세미나 논문집*, 교리 발전 분야, pp. 25-86, 1999.

[7] R. E. Haeni, "Information Warfare: An Introduction," The George Washington University, 1997.

[8] CERT/CC, *Overview of Attack Trends*, May 2002.

[9] http://news.cnet.com/news/0-1007-200-1545348. html

[10] http://securityresponse.symantec.com/avcenter/venc/data/vbs.loveletter.a.html

[11] CERT/CC, *Joint Alert on the Code Red Worm and mutations*.

[12] Steven A. Hildreth, *Cyberwarfare*, CRS Report for Congress, Library of Congress, 2001. June.

[13] 박상서, *중국 네트워크 보안 위협*, 2002.

[14] Serabian, John A., Jr. *Information Operations Issue Manager*, Central Intelligence Agency, Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, Feb. 2000, http://www.cia.gov/cia/public_affairs/speeches/archives/2000/cyberthreats_022300.html.

[15] 정보처리진흥사업협회 시큐리티센터, *정보시큐리티의 현상: 2001년판*, 2002. 5.

[16] 전상훈, *Critical Alert for Cyber Terror: Security for Nation's Infrastructure*, 2002. 10.

[17] http://abcnews.go.com/sections/tech/DailyNews /whhack990511.html

[18] *China chatroom seethes after plane collision*, Reuters in Beijing, Monday, April 2001.

[19] OCIPEP, *Al-Qaida Cyber Capability*, THREAT ANALYSIS, TAV01-001, November 2, 2001.

〈著 者 紹 介〉

박 상 서 (Sangseo Park)

1991년 : 중앙대학교 전자계산학과 공학사

1993년 : 중앙대학교대학원 전자계산학과 공학석사

1996년 : 중앙대학교대학원 컴퓨터공학과 공학박사

1996년~1998년 : 국방정보체계연구소 선임연구원

1999년~1998년 : 국방과학연구소 선임연구원

2000년~ 현재 : 국가보안기술연구소 선임연구원

박 춘 식(Choonsik Park) 종신회원

1981년 : 광운대학교 전자통신공학과 공학사

1983년 : 한양대학교 전자통신공학과 공학석사

1995년 : 일본동경공업대학교 전기전자공학과 공학박사

1989년~1990년 : 일본 동경공업대학 객원연구원

1982년~1999년 : 한국전자통신연구원 책임연구원

2000년~현재 : 국가보안기술연구소 책임연구원