정보전자전의 이해와 사례

한림대학교 엄상용
한국전자통신연구원 최헌준
한림대학교 이광모*

1. 서 론

현재 사회를 '정보시대(information age)'라고 한다. 이는 현대 사회에서 정보가 갖는 중요성을 단적으로 말하는 것이라 할 수 있다. 즉, 정보와 정보 시스템이 국가나 사회 기관의 생존에 결정적인 요소로써, 얼마나 중요하고 정확한 정보를 가지고 있는가, 얼마나 신속 정확하게 정보를 처리하여 필요한 정보를 만들어낼 수 있는가 등이 모든 사회분야에서 절대적인 위치를 차지하기 위한 필수 요소로 작용하고 있다. 이러한 상황은 국가나 회사 등의 기구가 더욱 더 정보 시스템에 의존하게 하며 이로 인하여 필요한 정보를 선 점하거나 중요한 상대방의 정보를 파괴함으로써 상대적인 우위를 점유하려는 시도로 나타나고 있다. 즉, 정보 시스템에 침입하여 정보를 삭제 또는 변조하거나 정보 시스템의 기능을 중지시키는 등의 새로운 전쟁 형태를 만들어내고 있다.

이러한 정보나 정보 시스템에 대한 공격은 기존의 전쟁 형태와는 달리 소규모 전문 정보 관련 기술 인력에 의한 일부 정보 또는 정보 시스템에 대한 공격 및 파괴에 의해 원하는 전략 목적을 달성할 수 있다는데 중요성이 있다. 중요한 정보 기능을 제공하는 컴퓨터 시스템의 기능을 중지시킴으로써 수십 수백억 달러에 달하는 경제적 피해를 줄 수 있음은 물론 군사 정보 통신망의 기능을 파괴함으로써 전략적인 면에서도 큰 성과를 가져올 수 있다.

이 글에서는 21세기의 새로운 전쟁 형태로 간주되고 있는 정보전(information warfare)과 관련하여 최근의 사례를 살펴보고 현대 정보전과 컴퓨터 및 네트워크 보안과 관련된 사항을 정리해 보고자 한다.

2. 현대 정보전 사례

정보전에는 다양한 형태의 전쟁이 포함된다. 심리전을 위한 전단 살포나 방송, 적에게 아군에 대한 잘못된 작전 정보를 제공하기 위한 교란 작전 등이 그것이다. 그러나 방대한 양의 정보를 저장하고 조작 처리하여야 하는 요구에 따라 컴퓨터 시스템과 통신망의 활용이 증가한 현대는 컴퓨터 시스템과 통신망에 대한 침투와 방어가 정보전의 중요한 형태로 간주되고 있으며[5] 일부는 정보전이라는 용어를 컴퓨터와 네트워크 보안에 대한 공격을 의미하는데 사용하기도 한다. 이러한 정보 시스템의 침입에 의한 정보 삭제나 변경은 이 정보를 기본으로 수행되는 판단 결정이나 작전에 엄청난 영향을 갖게 된다. 정보전이란 무엇인가를 알아보기 전에 먼저 현대 정보전의 몇 가지 사례를 살펴보자.

2.1 해커 스파이 - Markus Hess

미국 군 컴퓨터 시스템에 대한 해커 침입으로 가장 잘 알려진 사건은 1986년 LBL(Lawrence Berkeley Laboratory)의 Cliff Stoll에 의해 밝혀진 것으로 독일 해커가 대학의 컴퓨터를 이용

* 종신회원

하여 민감한 데이터베이스에 접근한 사건일 것이다. 당시 Stoll은 자신이 사용한 LBL 계정 시스템의 75센트의 오류를 발견하였으며 이를 추적한 결과 Hunter라는 사용자가 자신의 75센트에 해당하는 컴퓨터 시간을 사용하였으며 Hunter에 대한 정당한 비용 청구 주소가 없음을 밝혀냈다[8]. 이를 바탕으로 사용 내용을 추적하여 Hunter가 컴퓨터 침입자이며 여러 컴퓨터 시스템을 이용하여 군 컴퓨터 시스템에 접근하였다는 사실을 밝혀냈으나 당시 아무도 믿지 않았다고 한다. 더욱이 이들 정보를 담당하는 사람은 이러한 침투 사실을 알지 못했으며 침투하였다는 사실도 믿지 않았다. 이 해커는 여러 군 컴퓨터에 성공적으로 접근하여 스텔스나 핵, White sands나 SDI 등의 키워드로 정보를 찾았으며 이를 자신의 컴퓨터에 복사하였다[9]. 1년에 가까운 조사 끝에 서독의 Markus Hess가 주범임이 밝혀졌으며 그는 German Chaos Computer Club의 일원으로 그룹내에서 Pengo라는 이름을 이용하였다. Hess와 두 동료는 1990년 2월 15일 기밀을 KGB에 판 간첩혐의로 유죄판결을 받았다[10].

이 사건은 미 의회가 1987년 Computer Security Act로 명명된 법안을 통과한 이후에 발생하여 당시 미국의 정보 보안이 방향만 설정되고 이를 충실히 구현하지 못했음을 보여주고 있다.

2.2 Morris의 worm

웜(worm)은 스스로 네트워크를 돌아다닐 수 있는 능력을 가진 프로그램을 의미한다. 아마 여러 웜 중에서 1988년 Robert Morris에 의해 작성되어 배포된 것이 가장 유명할 것이다. Robert Morris는 미국 NSA(National Security Agency)의 관리의 아들로 아버지를 통하여 관련 분야의 지식을 어려서부터 얻을 수 있었다. 그는 인터넷을 스스로 돌아다니며 원격 컴퓨터에 스스로를 복사함으로써 인터넷의 사이트를 찾을 수 있는 웜을 작성하였다. 이 웜은 시스템 자체에는 피해를 주지 않도록 작성되었으나 그 프로그램의 설계에 오류를 범하였다. 이 오류는 스스로를 기하급수적으로 전파하여 인터넷 사이트의 속도를 떨어뜨리고 통신망을 정지상태로 만들게 되었다. 이 웜은 인터넷에 대한 동작을 시작한지 약 12시간만에 대략 6200여대의 컴퓨터에 퍼졌으며 이러한 사실을 발견한 시스템 관리자는 그 확산을 정지시키기 위하여 네트워크 연결을 끊어야 했다. 이후 조사에서 약 2000대만이 공격을 받은 것으로 밝혀졌으며, 이 사건으로 Robert Morris는 3년의 보호 관찰과 10,000달러의 벌금 및 400시간의 사회 봉사 명령을 받았다.

이 사건으로 인터넷과 운영 체제의 취약점을 이용하여 시스템에 침투하는 방법이 알려졌으며 당시 이용되었던 취약점으로는 FTP, sendmail, RPC 등이 있다.

2.3 Sundevil 작전

미국은 1990년 5월 7일부터 9일간 당시로는 가장 규모가 큰 컴퓨터 범죄 소탕 작전을 수행하였다. 이것이 Sundevil 작전으로 그 목적은 컴퓨터 시스템에 침투하는 방법에 대한 정보나 주요 미국 기관에서 불법으로 취득한 파일 및 신용 사기에 사용된 신용 카드 접속 번호 파일 등을 저장하고 있는 지하 조직의 수 백대의 컴퓨터 시스템으로 구성된 해커의 정보 배포 시스템이었다. 이 작전으로 약 42대의 컴퓨터와 23000장의 플로피 디스크 분량의 정보가 압수되었다[11].

2.4 걸프전과 정보전

Jack L. Brock은 미 국회 소위원회의 청문회에서 걸프전 직전 발생한 미국 국방부 컴퓨터 시스템에 대한 침투 조사에 대해서 증언하였다[6]. 이 증언에 따르면 1991년 4월과 5월 사이에 네덜란드로부터 5명의 해커가 미 국방부 소속의 34컴퓨터 사이트에 침투하였다. 이들은 잘 알려진 네트워크와 운영체제의 문제점을 이용하여 여러 컴퓨터에 사용자 권한을 획득하고 군 개인 신상 정보와 병참 정보 및 무기 체계 개발 자료 등에 접근하였으며, 에너지성의 CIAC(computer incident advisory capability) 담당자인 Eugene Schultz에 따르면 많은 양의 정보를 여러 대학이나 자신의 컴퓨터에 복사한 것으로 밝혀졌다[7]. 이들 해커는 TFTP의 취약점을 이용한 침투나 사용자 암호 추측이나 크랙 등을 사용하였다. Brock의 증언에 따르면 당시 미 국방부의 컴퓨터 시스템은 여러 번의 지적에도 불구하고 보안

상태가 매우 불량하여 지적된 문제점의 해결은 물론 사용자 암호에 대한 관리조차 제대로 수행되지 않았다. 또한 컴퓨터 시스템이나 시스템 보안에 대해 잘 알지 못하거나 심지어 전혀 경험이 없는 담당자도 있었다고 한다. 당시 대부분의 경우에 있어서 담당자는 침입 사실을 알지 못했으며 외부의 대학이나 도급 회사나 DOD 관리에 의해 이러한 사실을 통보 받은 것으로 증언하고 있다. 특히 Schultz는 정보 관리로부터 이들이 이 정보에 대해 사담 후세인에게 거래를 제안했으나 함정을 우려한 이란이 이를 거절했다고 들었다고 BBC에 전했다. 2차 대전이후 미국이 참전하여 승리한 첫 작전이 실패할 수도 있는 상황이었다.

2.5 가상 시나리오 - 보스니아 1998

발칸반도의 긴장과 평화회담의 실패, 보스니아와 유고슬라비아와 해외의 세르비아인들에 의해 보스니아의 세르비아 해방 평의회(Serbian Council for the Liberation of Bosnia:SCLiB)가 조직된다. 이 단체의 구성원들은 인터넷을 이용한 PGP 암호문 통신을 통하여 자신들의 관심사과 목적을 교환하고 크로아시아인의 영토 탈취와 이에 대한 미국의 지원에 대한 불만을 시정하고 이 지역에서의 나토(NATO)의 철수를 위하여 세계 사람들에게 자신의 정당한 이유를 극적으로 표현하기로 한다. 이를 위하여 CNN 일기 예보를 통하여 Brcko 지역에 극심한 폭풍이 있는 날을 정하여 Brcko 비행장의 착륙 진입로와 방송탑 설비를 탈취하여 이착륙하는 두 대의 C-130 수송기를 충돌시키고 이를 자신의 소행이라는 전자성명(E-communique)을 발표하고 자신들의 웹사이트에 방문하도록 초대한다. 이 웹 서버는 암스텔담의 한 슬로베니아 학생에 의해 핀란드의 익명의 웹서비스 계정에 의해 제공되는 것이다. 그 결과는 대단한 것으로 각 유명 뉴스 매체는 웹사이트의 주소와 함께 이 내용을 전하고 소식이 전해진 후 1시간만에 접속자가 백만 명에 이른다. 여기에는 발칸 반도 주변 상황에 대한 이야기뿐 아니라 나토와 보스니아 회교단체 및 크로아티아 간의 불법적인 무기 거래, 레바논의 미국 주둔과 그 결정 과정 등의 정보가 있다. 첫번째 방문자의 시스템은 방문이 있은 후 24시간만에 평의회 해커가 설치한 트로이 목마 프로그램에 의해 시스템의 모든 파일이 복구될 수 없게 삭제되고 기능을 멈춘다. 이는 전세계 컴퓨터를 이용하는 일반 세계에 두려움을 갖게 하고, 특히 해당 웹 서버에 접속하였던 미 국방성 등의 조사 기관이나 방어 기관은 가장 치명적인 피해를 입는다. 평의회 웹 서버에 접속했던 모든 시스템은 접속 후 24시간 후 이와 같은 일이 발생함으로써 그 피해는 급속하게 퍼지게 되고 이는 미국 의회와 대통령에 압력으로 작용하여 미군의 철수로 이어지며 미국의 지원이 없는 나토는 이 지역에서 그 영향력이 현저하게 떨어지는 결과를 초래한다.

이 내용은 M. Devost 등이 1996년 [1]에 기술한 1998년 보스니아 주변 환경에 대한 가상 시나리오이다. 이와 유사한 상황은 더욱 확산된 인터넷의 접속과 활용에 의해 실제 가능한 시나리오가 되었다. 전통적인 다량 살상 다량 파괴에 의한 전쟁보다 소규모 인원에 의해 수행된 소규모 공격이지만 그 전략적 목적은 완벽하게 이룰 수 있다.

특히, 이 시나리오에서 등장하는 접속자 컴퓨터 시스템에 피해를 줄 수 있는 방법은 1996년 프린스톤 대학의 컴퓨터 과학자에 의해 발표된 DNS 공격 시나리오[2]이며, 이와 유사한 웹 접속을 통하여 접속자 시스템에 피해를 줄 수 있는 여러 방법이 나타나고 있다.

2.6 Operation Datastream

공개된 정보에 따르면 16살의 영국 소년이 약 7개월 동안 적발되지 않고 미국 국방성 컴퓨터 시스템에 침투할 수 있었다고 한다. 이 소년은 대륙간 탄도탄 미사일 연구, 항공기 설계, 개인 정보나 Email등에 대한 접근이 가능하였으며 백만개 이상의 암호가 손상된 것으로 밝혀졌다. 또한 이 해커는 북한에서의 핵사찰에 대한 상세한 정보와 관련된 극비 컴퓨터 데이터베이스에도 접근했을 것으로 생각된다고 기술하고 있다. 북한이 독자적으로 이러한 형태의 작전을 수행하였다고 믿을만한 증거는 없으나 만약 북한이 이러한 정보에 접근할 수 있었다면 핵무기의 개발을 지원하기 위하여 데이터베이스와 통신망을 조작하였을 가능성도 있었다고 한다. 이 영국 해커가 체포된 것은 그가 자신의 터미널을 밤새 미 국방

성 컴퓨터에 연결한 상태로 놔두었기 때문이라고 한다.

이 사건은 정보전 기술이 중요한 의미가 있음을 볼 수 있는 경우로 정보전이 핵무기 확산을 지원할 수 있음을 보여줌으로써 핵무기와 정보전이 두 주요 보안 관심사로 부각시켰다.

2.7 한국 원자력 연구소와 영국 소년

1994년 두 영국 소년이 뉴욕주 Rome에 있는 미 공군 Rome 연구소의 컴퓨터 시스템에 침투한 사건이 발생했다. 1994년 3월 28일 Richard Pryce라는 사람이 Rome 컴퓨터에 설치한 "sniffer" 프로그램이 발견되었다. 이는 해당 네트워크에 연결된 컴퓨터의 사용자명과 암호를 알아내기 위한 프로그램으로 이 프로그램의 발견으로 해당 사건을 대한 컴퓨터 과학자들의 조사가 시작되었으며 Matthew Bevan이라는 공범이 있음이 밝혀졌다. 특히 Pryce는 16세의 영국 소년으로 밝혀졌다. 1994년 4월 중순 미 공군 조사원들은 이들 침입자들의 행위를 지켜보면서 관련 경험을 얻기로 동의하였으며, 4월 14일 Bevan은 Latvia에서 메릴랜드주 Greenbelt에 있는 Goddard Space Center에 침입하여 자료를 발칸지역 국가로 복사하는 것이 발견되었다. 후에 이 발칸지역 국가의 컴퓨터도 Bevan이 중간 거점으로 이용한 것으로 밝혀졌다. 5월 12일 Pryce는 한국의 한국 원자력 연구소의 자료를 Rome의 미 공군 컴퓨터에 복사하였고 이후 오래지않아 영국 당국에 의해 체포되었다. 당시 한국 원자력 연구소의 침입은 국내에서 TV 뉴스나 신문 등에 크게 보도되었다.

3. 정보전이란

정보전에 대해서는 여러 정의가 있으나 이 글에서는 군사측면에서 본 정의를 보자. 미국의 DISA(Defense Information Systems Agency)에서는 정보전을 "국가의 군사 전략에 따라서 적의 정보와 정보 시스템에 영향을 주는 동시에 자국의 정보와 정보 시스템은 보호함으로써 정보우위를 차지하기 위한 행위"로 정의하고 있다[3]. 이 정의에 따르면 정보전은 다시 방어 정보전과 공격 정보전으로 나눌 수 있다.

3.1 방어 정보전(defence IW)

이는 정보나 정보 시스템 등의 정보 자원을 세 가지 형태의 공격으로부터 방어하는 것을 말한다: 증가되는 공격 가능성, 감소되는 방어 가능성, 감소되는 무결성(integrity). 목표는 비용 효율적인 방어이다. 즉, 방어 비용이 해당 정보 자원의 손실에 의한 피해보다 작아야 한다는 것이다.

3.2 공격 정보전(offensive IW)

이는 목표가 되는 특정 정보 또는 정보 시스템의 가치를 공격자 측면에서는 향상시키고 방어자 측면에서는 감소시키는 것을 의미한다. 즉, 공격자는 해당 정보를 얻거나 정보 시스템의 파괴나 오동작 등으로 인하여 원하는 가치를 얻는 반면 방어자는 정보나 정보 시스템을 잃음으로써 정보나 정보 시스템 자체뿐 아니라 경제적 가치나 사회의 신뢰 등에 피해를 받게 된다.

3.3 정보전의 7가지 형태

Martin Libichi는 [4]에서 정보전은 하나의 전쟁 형태를 의미하는 것은 아니며 명확히 정의하기는 힘들다고 하였다. 따라서 정보전을 정의하기보다는 정보전을 7가지 형태로 분류하고 각 형태의 기능과 영향 등을 정리하였다.

3.3.1 Command-and-Control Warfare(C2W)

미 국방부 전문가에 따르면 "C2W는 전장에서 정보전을 구현하고 물리적인 파괴와 통합하는 군전략으로 그 목적은 적 명령체계에서 수뇌부를 제거하는 것"으로 정의하고 있다. 이는 걸프전에서 이라크의 명령 지휘 체계에 대한 많은 물리적인 파괴에서 그 예를 찾을 수 있다. 즉, 명령 수뇌부를 저격 등으로 제거하거나 지휘 본부의 파괴 또는 통신망의 파괴 등을 통하여 명령 체계의 기능을 제거하는 것을 말한다. 이를 위해서는 적의 명령 지휘 체계를 정보의 흐름과 관련하여 파악할 필요가 있다. 계급적 구조를 가진 체계는 C2W에 많은 취약점을 가지고 있는 반면 정보시대에 정보 기술을 바탕으로 나타난 비계급적 명령 지휘 체계는 탄력성을 가져 C2W로 명확한

결과를 가져오기 힘들다. 이 두 가지의 혼합형 명령 지휘 체계에 대한 C2W에 있어서는 어느 부분을 대상으로 수행할 것인가에 대한 명확한 판단이 앞서야 한다. 그렇지 않을 경우 명령 지휘 체계가 비계급적 체계로 전화되어 이후 C2W가 더욱 어려워지는 결과를 초래할 수 있다.

3.3.2 Intelligence-Based Warfare(IBW)

이 형태는 정보가 목표를 정하거나 전장의 피해를 평가하는 등 작전에 직접적으로 이용되는 경우 나타난다. 즉, 발달된 기술로 만들어진 센서와 통신망을 이용하여 실기간 또는 거의 실시간에 가깝게 정보를 전달받은 관련 시스템은 이 정보를 바탕으로 목표에 대한 보다 정확한 공격이 가능하다. 이는 정보가 지휘자의 작전 계획을 수립하는 데 사용되던 시대에서 실제 전쟁터에서 작전을 위한 상황 판단에 직접 정보를 사용하는 환경으로 변화되고 있는데서 볼 수 있다. 예를 들어 적 탱크의 이동에 대한 정보를 바탕으로 아군의 대응을 계획하던 시대에서 적 탱크의 정확한 위치를 파악함으로써 직접 교전을 피하고 원거리에서 공격하는 시대로의 변화가 IBW의 형태라고 할 수 있다. GPS(Global Positioning Systems)의 등장으로 아군의 위치를 파악하는 문제가 해결되었으며 센서와 정찰 및 감시 시스템의 발전으로 적군의 위치를 파악하는 것이 가능해졌다. 더욱 중요한 것은 이들 정보가 통신기술의 발전으로 빠른 시간 내에 이를 필요로 하는 대상에게 제공될 수 있다는 것이다.

이러한 IBW는 적에 노출되는 아군에 대한 정보는 최소화하여야 한다.

3.3.3 Electronic Warfare

2차 세계 대전에서 두드려졌던 전자전은 기본적으로 정보의 전송을 위한 물리적 기반을 붕괴시키기 위한 것으로 레이더 전파 방해나 레이더의 송출 전파를 추적하여 공격하는 미사일을 이용하여 파괴하거나 통신망에 대한 통신 방해와 암호화와 디지털 송수신에 의한 안전한 통신 등이 이에 속한다. 또한 센서를 이용한 감시 시스템의 발전으로 센서에 의한 정보 수집시 잘못된 정보를 제공할 수 있도록 하는 것도 이에 속한다.

3.3.4 Psychological Warfare

이는 단어 뜻대로 사람의 마음을 움직이기 위한 작전 형태를 말한다. 이는 작전 대상에 따라 ①국민의 의지, ②적 지휘자, ③군대 그리고 ④문화 차이에 대한 작전으로 구분할 수 있다. 상대방에 대해 두려움이나 우호적임을 강조함으로써 관련 정보를 습득한 사람 개개인의 마음을 동요시켜 투항하거나 작전 수행 의욕을 감소시키는 것이다. 전통적인 선전 전단이나 TV나 라디오 방송 외에 위성을 통한 직접 방송 등 여러 경로를 통해 수행될 수 있다. 또한 인터넷의 확산으로 이를 통한 정보 요구자에 대한 정보 제공도 또 다른 형태로 간주된다.

3.3.5 Hacker Warfare

Winn Schwartau 등 많은 사람들이 정보전이라는 용어를 거의 컴퓨터 네트워크에 대한 공격만을 의미하는데 사용하고 있다. 이는 공격 목표가 되는 시스템의 보안 구조의 취약점을 공격한다는 점에서 물리적인 공격과 달리 특정 시스템의 특성에 대한 공격이다. 공격의 목적도 시스템의 작동을 정지시키거나 정보를 삭제 또는 훔치거나 서비스를 제공하지 못하도록 하는 등 다양한 형태로 나타날 수 있으며, 더욱이 공격에 필요한 인원이나 자원이 물리적인 공격에 비해 적은 반면 공격에 대한 피해는 그에 상응할 수 있다는 점에서 많은 관심의 대상이 되고 있다. GAO Executive Report-B-266140에 의하면 미국방성은 여러 방면의 업무를 위하여 2백10만대를 이용한 정보 기술에 의존하고 있다고 한다. 더욱이 DISA가 예측하기로 1995년 이들 컴퓨터 시스템에 대해 약 250,000건의 해킹 사건이 있었으며 이중 150건당 1건의 비율로 적발되었다고 적고 있다. 더욱 심각한 상황은 민간 부분의 컴퓨터 시스템으로 보안 관련 개념이 희박하거나 아예 없어서 사회 전반에 큰 혼란을 가져올 수 있다는 것이다.

3.3.6 Economic Information Warfare

정보전과 경제전의 결합은 정보 차단(blockage)과 정보 제국주의(imperialism)의 두 가지 형태로 나타날 수 있다. 정보 차단의 경우 국가 경제 정보의 흐름을 차단함으로써 국가 경제에 피해를 주기 위한 방법이며 정보 제국주의는 경제 제국주의처럼 고도의 지식 정보 분야에서 특

정 국가가 선 점하고 이를 통하여 우위를 차지하는 것으로 생각할 수 있다.

3.3.7 Cyber Warfare

이는 정보 테러리즘, 의미(semantic) 공격, simula warfare, Gibson-warfare 등이 속한다. 정보 테러리즘이란 개인 신상 정보를 수집하여 이를 해당 개인에 대해 테러의 도구로 이용하는 것이다. 이는 컴퓨터 시스템에 의한 개인 신장 정보의 저장과 처리가 증가할수록 그 가능성이 증가하고 있다. 샌드라 블록이 주연한 영화 "The Net"이 이로 인하여 발생할 수 있는 한 예라 할 수 있다. 의미 공격은 대상 시스템의 동작을 중지시키는 것이 아니라 정상적으로 동작하는 것처럼 인식되지만 실제로는 잘못된 정보를 제공하도록 하는 것이다.

모의전(simula warfare)의 경우 실제 전쟁이 아니라 모의전을 통하여 실제 충돌의 결과를 제공하거나 시위를 위한 무기 구입 등

이상의 7가지 분류에서 보면 정보전의 공격 대상은 군뿐 아니라 일반 시민 사회도 포함됨을 알 수 있다. 경제 정보전과 사이버전은 그 대상이 시민 사회인 반면 C2W와 IBW, EW는 군을 그 대상으로 하고 있으며, 심리전과 컴퓨터 해커는 두 가지 모두를 대상으로 수행될 수 있다.

4. 정보전의 무기

현대 정보전은 컴퓨터나 통신망 등 전기 전자적인 요소에 대한 침입이나 파괴를 주로 의미하고 있다. 그럼 이러한 공격 목표에 사용되는 무기는 어떠한 것이 있는가.

4.1 HERF 총

HERF(High Energy Radio Frequency) 총은 다양한 목표물에 대한 서비스 거부 공격[1]을 가능하게 한다. HERF 총의 기본 원리는 아주 간단하며 제작하기도 매우 쉽다. 사용되는 전원의 크기와 요구되는 정확도에 따라 여러 형식과 모양으로 제작될 수 있다. HERF 총은 일반 송신 안테나나 휴대용 전화기처럼 무선 송출기와 유사하나 상당히 강력한 에너지를 방출하기 때문에 목표는 적어도 잠시동안은 기능을 상실하게 된다. 이는 컴퓨터 다운이나 모든 네트워크의 고장 등을 가능하게 할 수 있다.

4.2 EMP/T 폭탄

EMP/T 폭탄(Electromagnetic Pulse Transformer Bomb)은 HERF 총과 같은 원리로 동작하나 수천배 더욱 강력한 성능을 갖는다. 또한 EMP/T 폭탄에 의한 피해는 영구적인 것으로 원자폭탄의 발명과 더불어 나타난 위협이다. 1980년 연방 재난관리국(Federal Emergency Management Agency)은 컴퓨터와 컴퓨터 전원 공급 장치, 트랜지스터를 이용한 전원 공급 장치와 반도체 소자 등 다양한 분야에 걸쳐 EMP/P 폭탄에 가장 민감한 장치의 목록을 발표하였다.

4.3 컴퓨터 침입

현대 사회는 정보의 저장이나 조작 처리 등을 위하여 컴퓨터 시스템을 이용하며 정보 교환을 위한 통신망을 이용하고 있으며 그 의존도는 급속하게 증가하고 있다. 이는 컴퓨터 시스템이나 통신망의 급속한 확산을 가져오며 이는 이러한 자원에 대한 공격 가능성을 높이고 있다.

이러한 정보 자원에 대한 공격은 초기에는 목표 컴퓨터 시스템이나 통신망에 대한 전문적인 지식이 요구되었다. 이것이 해커라는 용어가 원래의 의미에서 벗어나 요즘 사용되는 의미를 갖게된 이유이기도 하다(요즘 매스컴 등에서 사용되는 해커는 크래커의 의미). 다양한 공격 목표가 존재하게 됨으로써 자신이 갖고 있는 지식을 이용하여 재미 또는 흥미거리로, 혹은, 경제적인 이익을 얻기 위한 수단으로 컴퓨터 시스템이나 통신망에 대한 침입하는 사례가 증가하게 되었다.

요즈음 이러한 경향이 갖는 심각한 문제점의 하나는 이제는 이와 같은 컴퓨터 시스템이나 인터넷 등의 통신망에 대한 침입을 위하여 전문 지식을 공부하지 않아도 된다는 점이다. 인터넷을 이용한 정보 공유가 급속하게 증가하면서 예전에

1) 서비스 거부 공격(Denial of Service Attack) : 특정 서버가 제공하는 서비스를 제공하지 못하도록 하는 공격으로 얼마전 발생한 YAHOO 서버의 다운 등이 이 공격에 의한 피해로 발표되었다. 다양한 공격 도구가 소개되었으며 요즘은 DDOS(Distributed DOS) 도구를 이용한 피해 사례가 종종 발표된다.

는 비밀리에 주고받던 크래킹과 관련된 정보가 공공연히 제공되고 있으며 이러한 기법들을 구현한 소프트웨어가 패키지 형태로 제공되고 있다. 누구나 인터넷에 연결된 컴퓨터와 사용자 설명서만 읽을 수 있다면 해당 패키지를 이용하여 다른 곳의 컴퓨터나 통신망에 침입할 수 있다. 공격자는 쉽게 도구를 얻어 공격할 수 있으나 이를 방어하는 쪽은 대부분 준비가 되어있지 않은 점도 문제로 지적된다. 빠른 인터넷 연결 망과 허술한 보안 환경이 우라 나라를 크래커들이 중간 거점으로 이용한다는 뉴스가 방송된 적이 있었으며 국내 컴퓨터 수 백대가 크래커에 의해 공격을 받았다는 기사가 발표된 적도 있다. 이러한 상황은 KISA(Korea Information Security Agency)에서 지속적으로 발표하는 피해 사례를 통하여 확인할 수 있다.

4.4 포획(capture)과 정탐(espionage)

컴퓨터를 비롯한 각종 전기 전자 장비에서 방출되는 정보를 다양한 도구를 이용하여 취합함으로써 원하는 정보를 얻을 수도 있다. 특히, 현 미국 정부 규정은 비정부 기관에서 TEMPEST[2] 를 이용하여 이를 방지하는 것을 금지하고 있다.

4.5 바이러스와 트로이 목마 및 웜

이들 공격 도구는 모두 가공할 파괴력을 가지고 있다고 할 수 있다. 현재로써는 컴퓨터 바이러스가 가장 강력한 기능을 나타내고 있으나 최근 바이러스와 웜의 성능을 조합한 웜 바이러스도 출현하고 있다. 일반적으로 바이러스는 전이 매개가 되는 프로그램에 의해 전이되며 특정 조건이 만족될 때까지 잠복하고 있는 것이 일반적이다. 특정 날짜나 명령이 수행될 때 지정된 작업을 수행한다. CIH 바이러스의 경우 플래시 메모리의 BIOS를 삭제하거나 디스크의 파일을 삭제하는 등의 치명적인 피해를 주기도 하였으며 요즘은 E-mail을 통하여 전파되는 새로운 바이러스 기법이 개발되어 더욱 강력한 기능을 가지게 되었다. 반면에 트로이 목마 프로그램은 유용한 프로그램인 것처럼 가장하고 있으나 실제로 수행시킬 경우 바이러스처럼 파괴 기능이 수행되는 프로그램을 통칭한다. 그러나 바이러스처럼 스스로 복사하는 기능은 갖지 않았으므로 바이러스에 비해 상대적으로 간단히 대처할 수 있다.

웜은 앞의 사례에서 기술한 Robert Morris에 의해 소개된 것으로 바이러스나 트로이 목마 프로그램과는 달리 스스로 네트워크를 통해 복제되는 기능을 가지고 있다. 즉, 웜 스스로가 알고 있는 여러 시스템의 취약점을 이용하여 스스로를 다른 컴퓨터 시스템에 복제하는 방법으로 동작한다. 물론 복제된 컴퓨터 시스템에서 수행되는 기능은 바이러스와 동일하다.

4.6 기타 정상적인 사고

정상적인 시스템의 사고에 의해 발생할 수 있는 위협으로 컴퓨터나 정보 시스템에 같은 위협으로 생각할 수 있다.

5. 방어 정보 시스템 네트워크(DISN)

미국의 DISN(Defense Information System Network)은 WAN, LAN, MAN 및 longhaul 네트워크간에 음성, 데이터, 비디오 전송 및 교환과 점대점(Point-to-point) 대역 서비스를 제공하는 네트워크이다. 이를 위하여 DISN은 100 여개 이상의 국방부 네트워크를 하나의 네트워크로 통합하여 하나의 비용 효율적인 유용한 공통 사용자의 전역 정보권(infosphere)을 구성하게 된다. 음성/영상 및 데이터 정보 전송이 통합된 DISN은 전투원에게도 그대로 제공되며 정보 자원의 관리를 용이하게 하고 모든 조건하에서 국가 보안과 방어 요구에 가장 효율적인 방법으로 반응하게 될 것이다.

이러한 DISN은 먼저 북미 대륙에서 구현하려고 하며 이를 CONUS(Continental United States)로 부른다. 이후에 ONONUS를 구현하도록 하고 있다.

DISN CONUS는 다음을 목표로 하고 있다.

① 전투원(warfighter)의 요구 만족
② 배치 군과 모 기지간의 seamless 연결
③ 새로운 기술에 대한 투자

2) The Transient Electromagnetic Pulse Emanation Standard로 미국 정보에 의해 전자 장비에 대해 물리적인 접촉 없이 감청 장비에 의해 감청되는 것을 방지하기에 충분히 낮은 전기전자 방출 단계를 표시

④ 모든 DoD 서비스, 정부 기관 및 연합군과의 공동 이용 가능

⑤ 전투원에 대한 필요한 능력과 연결 제공

⑥ 장소 시간과 관계없이 쇄도하는 요구 만족

⑦ 전투원의 요구에 대처하기 위한 빠른 재구성 가능성

⑧ 가격 효율적인 알맞는 서비스

⑨ 전시나 비전시 관계없이 모든 조건하에서 실시간 관리 가능성

⑩ 효율적인 사용량 기준 billing을 통한 비용 회복

다음은 DISA의 웹 페이지에서 제공되는 CONUS의 구성도[3]이다.

이 구성도는 DISN CONUS의 목표 구조를 보여주고 있다. 그림에서 볼 수 있듯이 초기 DISN CONUS는 35개의 BWM과 12개의 스위치, PBX, 4-wire 가입자(subscriber), 점대점 전용 가입자, VTC 허브, 네트워크 관리, 백본에 대한 접속과 전송을 담당하는 CONUS 제공자인 DISN 전송 서비스와의 연결로 구성되어 있다.

SONET(Synchronous Optical Network) 백본이 각각의 BWM과 정부 기지 또는 post Service Delivery Points(SDP)를 연결함으로써

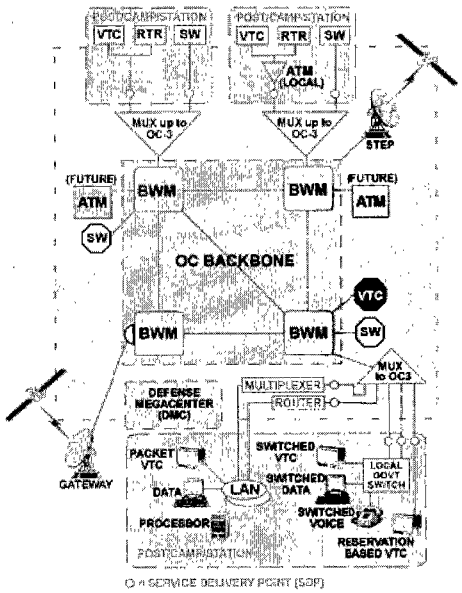

그림 2 CONUS 구성도

3) http://www.disa.mil/org/disncnfg.html

각 DISN CONUS 서비스에 대한 회로망을 제공한다. 이러한 DISN CONUS 서비스에는 회로 교환과 자료 서비스, 전용 점대점 서비스, VTC 등의 부가가치 서비스가 포함된다.

6. 결 론

1998년 가을 발행된 [12]에서 George Smith는 미국이 가지고 있는 사이버 공격에 대한 취약점에도 불구하고 "전자 진주만(Electronic Pearl Harbor)"을 시나리오일 뿐이라고 하였다. 여러 가지 상황으로 볼 때 컴퓨터 바이러스나 Email, 해커의 공격에 의한 미국에 대한 공격은 상당히 회의적이라는 것이다. 그러나 newsmax.com의 웹 사이트에 게시된 2000년 10월 11일자 글에서는 중국 관리의 보고서를 인용하여 여러 형태의 전자전(electronic warfare) 공격이 가능하다고 밝히고 있다. AFPC(American Foreign Policy Council)의 믿을 만한 소식통에 따르면 이 중국 보고서는 중국이나 다른 나라가 미국에 대해 어떻게 전자전을 활용할 수 있는가를 설명하고 있다고 한다.

이처럼 정보전 및 전자전에 대한 각국의 관심에 고조되고 있는 시점에 있으며 방어 및 공격 전략 수립에 많은 시간과 노력을 투자하고 있으며 실제 전쟁의 한 수단으로 인정되고 있다. 특히 나날이 증가하는 컴퓨터 시스템에 의한 정보의 저장 및 처리와 인터넷 등의 통신망을 이용한 정보 교환은 점차 새로운 형태의 전쟁을 낳고 있으며 새로운 곳, 즉, 사이버 공간을 새로운 전쟁터로 만들고 있다. 미국 국방성은 매일 보이지 않는 전쟁을 하고 있다고 발표한 적이 있다. 매일 국방성 컴퓨터를 공격하는 해커의 공격을 방어하고 침입자를 확인하는 작업이 지속적으로 발생하고 있다는 것이다.

참고문헌

[1] M. G. Devost, B. K. Houghton, and N. A. Pollard, Information Terrorism:Can You Trust Your Toaster?(http://www.terrorism.com/documents/suntzu.pdf).

[2] D. Dean, E. W. Felten, and D. S. Wallach, "Java Security: From HotJava

to Netscape and Beyond," 1996 IEEE Symp. on Security and Privacy, May 1996(http://www.cs.princeton.edu/sip/pub/oakland-paper-96.pdf).

[3] G. Kovacich, "Information Warfare and Information Systems Security Professional," Information Systems Security, Summer 97, Vol.6, Issue 2.

[4] M. Libichi, "What is Information Warfare,", Washington:National Defense University, Aug. 1955(http://www.ndu.edu/inss/actpubs/act003/a003.html).

[5] M. G. Devost, The Digital Threat: United States National Security and Computers, New Engliand Political Scicene Association 1994(http://www.devost.net/mgd/documents/digitalthreat.html).

[6] J. L. Brock, Testimony in Hackers Penetrate D.O.D. Computer Systems: Hearings before the Subcommittee on Government Information & Regulation, Committee on Governmental Affairs, United Stated Senate, Nov. 20, 1991.

[7] D. E. Denning, Information Warfare and Security, ACM Press, Addison-wesley, 1999.

[8] C. Stoll, The Cuckoo's Egg:Tracking a Spy Through the Maze of Computer Espinage, New York, Doubleday, 1989.

[9] K. Hafner and J. Markoff, Cyberpunk: Outlaws & Hackers on the Computer Frontier, New York, Simon & Schuster, 1991.

[10] P. J. Denning, Computers Under Attack: Intruders, Worms & Viruses, New York, ACM Press, 1991.

[11] B. Sterling, The Hacker Crackdown: Law and Disorder on the Electronic Frontier, New York, Bantam Books, 1992.

[12] G. Smith, "An Electronic Pearl Harbor? Not Likely", ISSUES in Sci. and Tech. Fall, 1988(http://205.130.85.236/issues/15.1/smith.htm).

엄 상 용

1987 한림대학교 전자계산학과 학사
1997 한림대학교 컴퓨터공학부 석사
1999 한림대학교 컴퓨터공학부 박사수료
1999~현재 한림대학교 교양교육부 강의전담교수
E-mail:suhmn@ekus.ce.hallym.ac.kr

최 현 준

1988 숭실대학교 전자계산학과 졸업
1990 한국외국어대학교 응용전산학과 졸업
현 한국외국어대학교 경영학과 박사과정
1990~1992 한국국방연구원 전산체계연구부 연구원
1992~1998 국방정보체계연구소 선임연구원
1999~1999 국방과학연구소 선임연구원
2000~현재 국가보안기술연구소 선임연구원
E-mail:chj@dingo.etri.re.kr

이 광 모

1975 서울대학교 공과대학 응용수학과 학사
1984 서울대학교 계산통계학과 전산학 전공 석사
1992 서울대학교 계산통계학과 전산학전공 박사
1980-1985 조선대학교 전자계산학과 조교수
1992~1993 Florida State University 방문교수
1985~현재 한림대학교 정보통신공학부 교수
E-mail:kmlee@sun.hallym.ac.kr