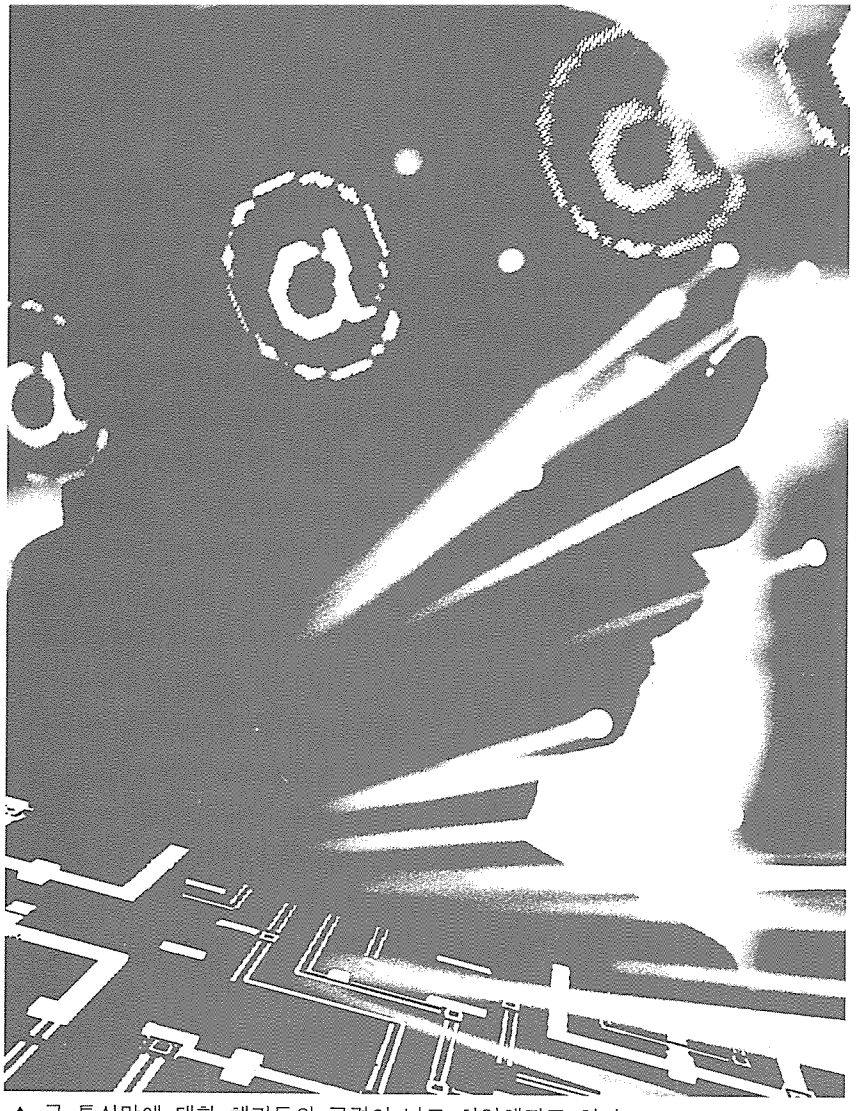


▲ 군 통신망에 대한 해커들의 공격이 날로 치열해지고 있다.

첨단과학기술현장

사이버전쟁시대 - 창과 방패

1999년 3월 27일 북대서양조약기구(NATO)의 전폭기들이 유고슬라비아에 대한 폭격을 개시한 뒤 꼭 3일만에 전쟁은 사이버공간으로 번져 나갔다. 컴퓨터 해커들이 NATO의 전자우편 통신시스템 교란작전을 개시한 것이다. 이것은 역사상 NATO 컴퓨터 시스템이 전시에 공격을 받은 최초의 사건이었다. 그러나 이 사이버전쟁은 오래 끌지 못했다. NATO는 '비장의 방패'로 해커들의 '창'을 물리쳤기 때문이다.

늘어나는 군사목표

최근의 NATO 공격에서 해커들이 택한 전술의 하나는 한대의 컴퓨터가 자동·반복적으로 다른 컴퓨터를 호출하는 이른바 '핑' 공격이었다. 다른 하나의 전술은 전자우편의 '폭격'이었으며 대량의 메시지로 목표네트워크의 서버(클라이언트/서버 시스템에서 클라이언트의 의뢰에 응하여 서비스를 제공하는 컴퓨터 또는 프로그램)에게 과중한 부담을 주어 기능을 마비시키는 것이다. NATO로 들어오는 전자우편의 수는 금새 2천통으로 불어났다.

NATO 공격자들의 실체는 확인되지는 않았으나 이들은 1998년 10월 코소보정보센터 웹사이트를 침범한 '크르나 루카(검은 손)'로 불리는 5인조의 세르비아인 그룹으로 지목되었다. 이들은 당시 베오그라드의 한 신문에서 다음 목표는 NATO가 될 것이라고 발표했기 때문이다. 그런데 사이버 공격자들은 지구상에서 어떤 컴퓨터를 통해서도 인터넷과 연결할 수 있어 이런 그룹을 포착하여 차단한다는 것은 거의 불가능한 일이어서 이들은 쉽게 정체를 감출 수 있다.

아무튼 이들의 공격을 받은 NATO의 컴퓨터들은 2~3시간 기능을 멈추었으나 곧 회복했다. 그러나 비록 짧은 동안이나마 이들의 공격은 군사상 주목할만한 사건이었을 뿐 아니라 군으로서는 전자 적(電子 敵)과의 최초의 전투라는 점에서 관심을 모으고 있다.

NATO에 대한 이번 공격은 10대의 장난만으로 생각할 수 없는 최근의 일련의 해커사건중의 하나이기도

했다.

지난 1년간만 해도 미군의 여러 부서에서는 이를테면 조건부의 해커공격을 경험했다. 1998년 9월에는 미 해군이 이와 비슷한 공격을 받았으나 해커들과는 타협하지 않았다. 미 항공우주국(NASA)과 로스알라모스 미 국립연구소 그리고 보잉사와 같은 미 군수산업체도 역시 해커들의 표적이 되었다.

사이버공격의 대상은 미군만 아니라 다른 나라 군사시설까지 번져 나갔다. 해커들은 1999년 2월에는 영국 군용 통신위성을 장악하고 이것을 볼모로 삼으려고 했으나 실패하고 말았다. 1998년 10월에는 중국 정부의 전산망과 인도의 육군본부 전산망사이트가 침범을 당했다.

1999년 5월 27일에는 미 의회 상원 웹사이트를 비롯하여 미국 정부 전산망을 공격했다. 해커들은 조사에 착수한 미 연방조사국(FBI)에 대해 조사중단을 요구하면서 5월 31일 미 내무부와 미 연방 슈퍼컴퓨터연구소의 컴퓨터에 침입하여 웹사이트를 파괴했다. 이들은 수사를 중단하지 않으면 FBI의 인터넷 페이지를 공급하는 컴퓨터를 파괴하겠다고 으름장을 놓고 있다.

인터폴(국제형사경찰기구, 1923년 국제범죄의 정보·수사협력을 위해 설치, 본부는 파리)에 따르면 인터넷에는 약 3만개의 해커지향의 웹사이트가 있고 줄잡아 1천7백만명의 사람들이 다른 컴퓨터에 피해를 줄 수 있는 능력의 컴퓨터기술을 갖추고 있어 바야흐로 인터넷은 해커들의 놀이마당이 되어 버렸다고 해도 놀랄만한 일이 못된다.

갈고 닦는 방패

오늘날 미 국방부는 날마다 60~80건의 사이버공격을 받고 있으나 거의 대부분은 심각한 정도는 아닌 것으로 알려졌다. 그러나 미 국방당국은 일찍부터 이런저런 해커들의 전술을 반격할 수 있는 기술을 개발하여 대비하고 있었기 때문에 이번의 NATO 피격사건에서 처럼 이들을 지체없이 물리칠 수 있었던 것이다. 미 국방당국에게 미래의 사이버전쟁에서 어떻게 군이 대처해야 할 것인가를 가르쳐 준 매우 중요한 사건이 발생한 것은 1997년 초였다. 하루는 미 버지니어주 랭글리 공군기지에서 이상한 일이 벌어졌다.

현재 랭글리 공군기지 정보시스템 책임자인 데일 마이어로즈준장이 당시 수상한 전자우편을 열면서 사건이 터졌다. 이 우편은 당시 공군대령이던 그에게 클린턴대통령이 직접 보낸 것인데 지휘계통을 무시하고 본인에게 대통령이 메시지를 보낸다는 것은 있을 수 없는 일이었다. 그 내용도 불쾌하기 이를데 없었다. "그의 어머니의 혈통에 미심쩍은 점이 있으니 지체없이 조사해서 보고할 것"이라는 내용이었다. 당황한 그는 누군가가 랭글리기지의 컴퓨터시스템을 몰래 도용하고 있다는 것을 알게 되었다.

그런데 랭글리 공군기지는 미 국방부가 공군에게 전세계에 산재한 미 전투 및 폭격기들에게 임무를 수행하도록 지시를 내리는 미 공군전투사령부(ACC)가 있는 곳으로서 이런 따위의 전자우편이 랭글리기지를 통해 발송된다면 심각한 후유증을 남길 것은 뻔한 일이었다. 당시 마이어로즈 대령이 내린 첫번째 명령은 들어오는 전자우편 메시지에 부착된 로그파일을 조사하는 것이었다. 문제는 디스크의 스페이스(공간)를 아끼려고 로그파일에 관한 정보량을 최소한 기록해 왔다는 것이다. 그래서 들어오는 전자우편에 관한 데이터량을 최대한 제공하기 위해 전자우편시스템을 개편했다. 이때 랭글리공군기지 전자우편 시스템의 관리책임자인 항공병 크리스 수베이는 이상한 현상을 발견했다. 공군기지 네트워크 서버를 통해 외부로 나가는 통신량이 기지로 들어오는 통신량보다 훨씬 많았던 것이다. 이것은 뜻밖의 일이었다. 그런데 조사에 착수한 사람들은 더 큰 문제가 도사리고 있다는 것을 발견했다. ACC컴퓨터가 매일 약 8백통의 '헤이트메일(혐오편지)'과 포르노사진을 몰래 아메리칸 온라인 사용자에게 보내는데 사용하고 있었던 것이다. 이것은 미 공군의 이미지를 위기로 몰아넣는 중대한 사건이었다. 일반국민들에게 미 공군이 혐오우편과 포르노사진의 배포처로 낙인찍힌다면 그 영향은 심각하지 않을 수 없었다. 그런데 문제는 기지가 의존하고 있는 전자우편시스템을 폐쇄하지 않고 네트워크의 통제권을 다시 장악하는 방법을 찾는 일이었다. 다행히도 이 문제를 해결하는 적임자를 발견하게 되었다. 독립적인 컴퓨터컨설턴트인 팀 바스는 미국 최고의 컴퓨터프로그래머중의 한사람이었으며 그의 전문분야는 군과 금융계의 컴퓨터보안 분야였다.

바스가 내놓은 해결책은 매우 단순하기는 했지만 전에 시도해 본 일이 전혀 없었다. 바스는 서버에서 의심

이 가는 우편을 제거하고 이것을 별도의 검사용 대기행렬에 배치하는 프로그램을 작성했다. 그래서 만약에 의심나는 우편이 '나쁜 우편'이나 또는 '스팸(쓰레기 전자우편물)'이라면 다시 다른 대기행렬에 가둬 둔다. 이 방법이 채택된 것은 두가지 이유 때문이다.

명쾌한 해결책

먼저 미 공군이 해커를 제소하기로 결정할 때 필요한 증거로 사용하기 위해서는 '스팸' 우편을 보관해야 한다. 둘째, '스팸' 발송자에게 피드백(출력측의 신호를 입력측으로 다시 보내어 이용하는 것)의 기회를 주지 않기 위한 것이다. 따라서 ACC서버를 통해 따돌리게 된 전자우편은 그 길로 '불랙홀' 속으로 사라져 버렸다. 이렇게 되자 48시간 내에 해커 게시판에는 ACC가 더 이상 전자우편 중계소 역할을 하지 않는다고 고시되었다. 그런데 해커들은 일반적으로 일종의 피드백루프를 넣어 그들의 '폭탄'이 목적지까지 전달되었다는 것을 알고 싶어한다. 그래서 랭글리 기지가 불랙홀전략을 착수하자 피드백루프는 단절되었고 해커들은 기가 꺾이게 되었다.

이들은 곧 반격에 나섰다. 해커들은 '전자우편 홍수작전'으로 나선 것이다. ACC네트워크는 별안간 매일 약 3만통의 전자우편으로 범람하기 시작했다. ACC의 우편번호는 인터넷에서 무료로 얻을 수 있는 많은 해커프로그램 속에 이미 코드되어 있어 마우스를 만지면 자동으로 계속적으로 발송된다. 따라서 이를테면 해커들의 폭탄투하는 ACC이름을 더블클리킹하는 것처럼 간단하다. ACC의 합법적인 전자우편량은 매일 평균 5천~6천통 정도였는데 이것은 486 시스템이 다룰 수 있는 양이었다. 그런데 별안간 매일 7만5천통으로 급증하자 바스는 '스팸' 우편에 대처하기 위해 매일 새로운 규칙을 첨가해 나갔다. 마침내 우편량이 넘치면서 전자우편서버가 기능을 잃어 버리고 랭글리 공군기지의 전자우편서비스도 중단되어 버렸다.

그러나 해커들의 승리의 도취는 불과 2~3시간으로 끝나 버렸다. ACC 컴퓨터단은 전자우편시스템의 용량을 펜티엄급 프로세서로 끌어 올렸다. 자욱이 덮힌 구름이 걷혀 별안간 푸른 하늘이 활짝 열리는 기분이었다. ACC는 데이브 그루버중령 휘하에 '타이거팀'으로 불리는 컴퓨터그룹을 조직하여 이 문제를 전담시켰다.

해커들도 만만치 않았다. '타이거팀'이 새로운 규칙을 만든지 48시간 내에 이것마저 무찌르고 침범했다. 한번은 백악관 공군전자 우편서버를 사용하여 랭글리기지 폭격에 나섰다. '타이거팀'도 새로운 수단으로 이와 맞섰다. 이들이 개선한 블랙홀전략은 복잡한 소프트웨어 패키지 속으로 침투되었고 이 패키지는 '봄브셀터(방공호)'라고 불렸다. 해커들의 전자우편은 계속 블랙홀로 사라졌다. 해커들은 가짜 송신자주소와 함께 메시지를 보내기 시작했다. 그들은 ACC가 사용하는 전술을 캐내려고 안달하고 있었다.

치열한 공방전

바스, 수베이를 포함하여 '타이거팀'은 해커들과 새로운 방위책으로 맞섰다. 마침내 ACC는 해커들의 협동공격의 과녁이 되었다. ACC는 실리를 위한 사이버전선을 구축했다. 그러나 재래식 전쟁과는 달리 이 전선의 상대방의 형편은 알 길이 없었다. 그중 일부는 에스토니아와 호주의 어떤 장소라는 것은 확인했으나 그런 것은 거의 무의미한 일이었다. 이런 위치는 단지 중계점에 불과할 수 있기 때문이다. 실제로 지리적인 위치와는 무관하게 집에서 세계 도처의 서버로 로그할 수 있고 그 곳을 공격점으로 사용할 수 있기 때문이다. 전자우편공격은 다음 한달동안 계속 줄지 않았고 전자우편의 약 80%인 '스팸'은 모두 '봄브셀터'가 관장하는 블랙홀 속으로 사라졌다. 어느새 전자우편의 양은 크게 줄어들어 하루 5천통 이하로 떨어졌다. 수베이는 해커웹사이트를 통해 ACC가 더 이상 공격이나 중계점으로 리스트에 올라있지 않다는 것을 발견하게 되었다. '봄브셀터'가 훌륭하게 주어진 임무를 완수한 것이다.

1997년 사이버공격 이래 ACC는 전자우편시스템을 보완하여 서버가 더 이상 중계점으로 사용될 수 없게 만들었다. 그리고 '봄브셀터'은 미군과 NATO동맹군을 위한 사이버방어의 방파제구실을 하게 되었다. 대신 '스팸' 우편을 걸러내기 위한 종래의 '방화벽'이 더 이상 네트워크를 보호할 것이라는 생각은 사라져 버렸다.

사이버공격은 아직도 그 근원을 탐지하기 어렵다. '봄브셀터'가 그 원인을 파헤치려고 활약하고 있으나 머리좋은 해커들은 이런 방어책을 거꾸로 이용하려고 시도하고 있다. 미 국방부는 미군의 정보시스템 보안율을

끌어 올리기 위해 1999년 여름 '컴퓨터망 방어 합동기동대'를 창설하여 활동을 개시한다. 미국의 각 군도 자체의 정보보안기구를 갖고 있다. 예컨대 미 해군은 방어용 온라인 제2차 발견분석(SHADOW)부대를 갖고 있다.

한편 비판자들은 해커들이 군을 공격대상으로 하고 있다는 주장에 대해 적어도 공식기록에는 아무 증거도 없기 때문에 미 국방부가 함부로 거짓 경고를 남발하고 있는 것이 아닌가고 의문을 제기하고 있다. 그러나 1997년의 랭글리 공군기지와 1999년의 세르비아사건이 명백하게 보여주듯 군에 대한 해커들의 사이버공격은 장난의 경지를 확실히 넘어서고 있다는 것도 사실이다.

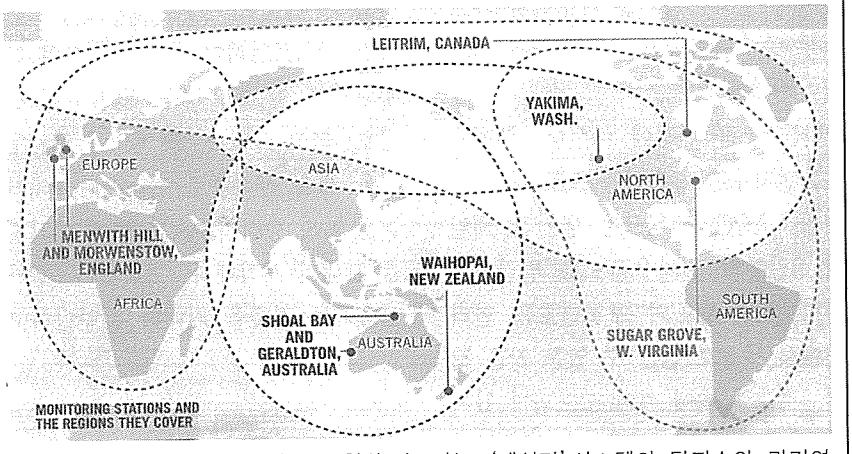
세계전자통신을 감청하는 '에셜란' 정보시스템

인터넷이 프라이버시에 중대한 새로운 위협을 가져온다고 걱정을 하고 있는 오늘날 전세계가 주고 받는 통신을 모조리 감청할 수 있는 시스템이 새삼 정치 및 실업계 지도자들의 큰 관심거리가 되고 있다. 세계 최고의 극비기관인 미 국가안전보장국(NSA)이 운영하는 '에셜란(Echelon)' 시스템은 첩보위성과 민감한 지상정보수집소를 묶어 국경을 넘나드는 전화통화, 팩스, 텔렉스, 전자우편은 물론 단파, 항공 및 해상주파를 포함한 무선신호 등 지구의 거의 모든 전자통신을 감청할 수 있다. 물론 대부분의 원거리통신과 지방의 휴대폰통화도 감청할 수 있다.

인공위성이나 극초단파중계를 통해 전달되는 전화통화나 메시지도 '에셜란'에게 잡힐 가능성이 많다. 심지어 해저전화케이블과 광지상통신시스템도 어디엔가는 극초단파 링크를 갖고 있기 때문에 모든 전기통신은 대부분 도청되고 있다고 해도 지나친 말은 아니다. 그래서 미국인들은 국제전화를 걸 때마다 NAS에게 감청되고 있다고 미 과학자연맹의 군사분석가 존 파이크는 주장하고 있다.

한편 유럽에서도 머지 않아 '빅 브라더'(조지 오웰의 소설 1984년에 등장하는 독재자)는 두번째의 감청용 귀를 갖게 된다. 유럽 의회가 '에셜란'의 축소판을 설치하기 위한 작업을 하고 있기 때문이다. 이들은 인터넷과 같은 신기술을 도청하기 위한 기술표준을 설정하는 결의문을 1999년 5월 7일 승인했다.

암호화도 프라이버시를 보장하지 못한다. 매릴랜드주 포트 미드의 본부에서 '에셜란'을 운용하고 있는 NSA(미국 중앙정보국보다 규모가 큼)로서는 대부분의 상용 암호 소프트웨어로 암호화된 메시지를 해독하는 일은 식은 죽 먹기와 다름없다. '에셜란'의 주요한 임무는 민간 전기통신량을 걸러내서 테러 음모, 마약 밀수, 정치적 불안 그리고 국방부와 정부전략가와 사법기관이 요청하는 그밖의 정보의 단서를 찾아내는 것이다. 슈퍼컴퓨터들이 이런 일과 관련된 키워드(핵심단어)를 걸러낸다. 만약에 슈퍼컴퓨터가 미심쩍은 것을 전혀 찾지 못하면 이 테이프는 한달 뒤에 지워진다. 그런데 다른 기술적 수단과 마찬가지로 '에셜란'도 정치적인 악용의 대상이 되어 있다. 예컨대 레이건행정부시절 '에셜란'이 당시 매릴랜드 출신 미 민주당의원인 마이클



▲ 거의 모든 국제전자통신을 도청할 수 있는 '에셜란' 시스템의 탐지소와 관리영역. 유럽지역은 영국의 멘위즈힐과 모웬스토우, 아시아지역은 호주의 솔베이와 제랄드턴, 미주지역은 워싱턴주의 야키마와 웨스트 버지니어주의 슈거그로브 등이다.

반즈가 니카라구아 관리에 건 전화통화를 도청했는데 이것이 언론으로 새어 나갔다. '에셜란'은 또 역효과를 낼 수도 있다. NSA와 협력관계에 있던 캐나다의 정보원들은 '에셜란'을 사용하여 진행중인 미-중국간 곡물거래에 관한 정보를 포착하여 이보다 더 싼 가격을 제시함으로써 거래를 빼앗았다.

'에셜란'은 수십년간 외부에 드러나지 않는 가운데 조용히 운영되어 왔다. 당초 '에셜란'은 현재 '에셜란'의 주요한 도청소를 운영하고 있는 미국, 호주, 영국, 캐나다, 뉴질랜드가 1984년에 체결한 비밀조약에 따라 탄생했다. 그런데 1998년 이 시스템은 영국사장 연구기관인 오메가재단이 유럽 의회를 위해 작성한 연구로 일반에게 자세히 알려지게 되었다. 그러나 유럽사람들은 '유럽 내의 모든 전자우편, 전화 및 팩스통신이 주기적으로 NSA에게 도청된다'는 사실을 알고 분노하게 되었다. 냉전중 개발한 전자간첩시스템과는 달리 '에셜란'은 주로 비군사적 목표를 위해 설계되었으며 그 목표중에는 사실상 모든 국가의 정부, 단체 및 실업계가 포함되어 있다. 실상 NSA의 전자간첩용의 가장 큰 기지는 영국의 요크셔 무어즈 소재 멘위즈힐에 있다. 이곳은 NSA와 같은 역할을 하는 영국의 정보통신본부와 공동으로 운영하고 있다. 세계에 산재한 25개의 거대한 축구장과 같은 이 구조물에는 각각 특정한 전기통신표적을 도청하게 조율된 첨단기술 안테나가 감춰져 있다.

'스파이의 세계'

'에셜란'은 캐나다의 NSA 제휴기관인 통신보안처(CSE)의 부국장이었으며 지금은 은퇴한 정보원인 마이크 프로스의 1995년의 저서 '스파이세계'(Spyworld)를 통해 이미 공개되었음에도 불구하고 오메가재단의 폭로는 많은 유럽인들에게 커다란 충격을 주었다. 특히 유럽대륙의 지도자들은 신문내용이 '에셜란'은 영국에 근거를 둔 기업들에게 경쟁정보를 제공할 것 같다고 비쳤을 때 격분했다. 그러나 CIA가 기업과 정보를 공유할 것을 제의할 때 1979년 NAS를 이끈 퇴역 해군제독 바비 레이 인만은 "절대로 안된다"고 말했다. 그는 기업의 다국적 지위 때문에 그렇게 하기에는 매우 어렵다고 주장하면서 예컨대 "파리에 있는 IBM에는 정보를 제공하고 테네시 소재 닛산 자동차회사에는 주지 않을 수 없지 않는가"고 말하고 있다. NSA는 기업과 정보를 나눠 갖지 않는다고 강조하고 있다.

인만에 따르면 '에셜란'의 중요한 임무중의 경제정보 목표는 '공정거래문제와 교역위반'과 같은 일이다. 캐나다의 프로스는 냉전이 기울어지면서 경제정보가 중요성을 얻게 되었으나 민간분야와 이런 정보를 공유하지 말아야 하는 확고한 정책이 있었다고 주장하고 있다. 그러나 비(非)영어 사용국가의 실업가들에게는 '에셜란'은 영국계의 음모라고 보고 있다. 1948년 UKUSA협정 아래 NSA가 우두머리이고 미국의 영국계 동맹국들은 '제2진'이 되었다. 대부분의 북대서양동맹국(NATO)들을 포함하여 몇몇 아시아국가들은 '제3진영'에 속한다. 방대한 양의 정보가 주요 도청소와 독일, 일본, 중동 그리고 다른 곳에 있는 소형 도청초소로부터 부단히 유입된다. 이중에서 많은 도청소는 미군이 운영하고 있어 주재국가의 정보기관도 무엇을 수집하는 것인지 알지 못한다. 이밖에도 NSA는 적어도 5개의 도청용 첩보위성을 보유하고 있다. 이 위성들은 너무나 민감하기 때문에 지상에서 수백 또는 수천마일이나 되는 고공에서 지상의 신호를 모니터할 수 있다.

그런데 NSA는 너무 많은 정보를 수집하여 인간의 분석력으로는 감당할 수 없을 정도다. 그래서 NSA는 슈퍼컴퓨터와 인공지능에 의존하고 있다. 첨단음성인식 및 문장탐색프로그램이 방대한 양의 정보를 가려내서 특정한 낱말과 구를 찾아 낸다. 또 주요 감청초소는 저마다 지리학적 지역 내에서 특정한 정보임무를 수행할 수 있게 '딕셔너리'라고 부르는 자체의 '키워드' 목록을 갖고 있다. 컴퓨터가 예컨대 테러리스트의 가명이나 마약의 방언을 발견하면 이 메시지는 지체없이 인간전문가에게 보내진다.

그런데 오메가보고를 둘러싸고 유럽인들이 법석을 떤 것 중의 일부는 쇼일지 모른다는 주장도 있다. 프랑스 비밀기관은 미국 기업을 염탐한다는 비난을 미 연방조사국(FBI)으로부터 여러번 받았다. 독일 정부는 자체의 미니 '에셜란'을 보유하고 독일을 드나드는 국제전기통신의 내용을 도청하고 있다. 한편 테러와 그밖의 중대한 범죄와 싸울 목적으로 유럽 법무장관들이 추진중인 계획은 기본적인 관리규제가 없어 비판자와 프라이버시운동가들의 분개를 사고 있다. 아무튼 감시기술이 너무 뛰어나기 때문에 도청시스템이 조지 오웰의 황당한 꿈을 앞지를 날이 곧 다가올지 모른다. ST