애셜론과 황금방패

지난 4월에 개봉한 영화 '기프트❶'는 전 지구적 전자통신 감시(Electronic Communications Surveillance) 시스템이라는 에셜론(Echelon)을 소재로, 컴퓨터 인공지능에 의한 인간통제 시도라는 영화의 단골 주제와 국가안보와 개인 사생활의 충돌이라는 난제가 함께 버무려져 있다. 현실에서 컴퓨터 프로그램에 인간의 사고와 지능을 불어넣는 작업은 영화적 상상보다는 한참 먼 길을 가야하는 일인지라 그건 그렇게 흘려버릴 수 있지만, 국가·사회의 안전을 위해 국민이 양보해야 하는 개인 사생활 영역은 어디까지일까, 그리고 그 합법적 침해 방법은 무엇일까 하는 해묵은 논제를 다시금 일깨우는 영화다.

글 **김홍근** | KISA 연구위원

정보보호 산업의 현주소

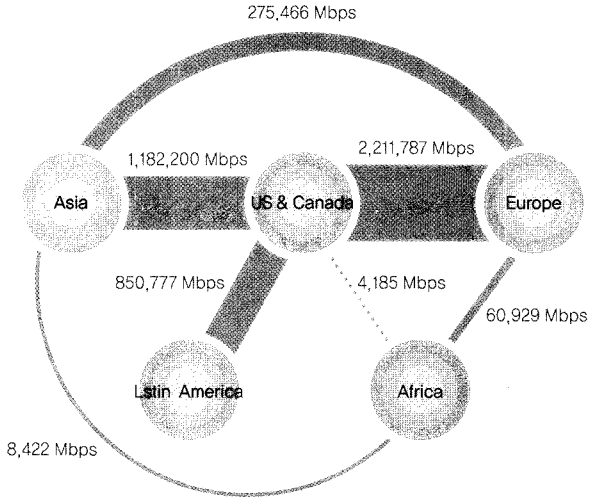
에셜론과 함께 영화에 자주 등장하는 USA의 NSA(National Security Agency)는 시그널 인텔리전스(Signal Intelligence)가 주요 임무 중의 하나인 정부기관이다. 2차 세계대전 당시 독일군과 일본군의 암호를 해독하는 일을 시작으로, 냉전시대를 포함해 전 세계의 전보, 전화 등 유무선 통신 내용을 가로채 정보를 수집한다는 사실이 1982년 James Bamford가 쓴 'The Puzzle Palace'가 출간되면서 알려졌다. 글로벌 통신 엿듣기(Eavesdropping❷)를 위해 수백 개 이상의 수집소(Intercept Station)를 운영하며, 이것의 한 형태로 또는 이것 전체를 또는 이를 위한 소프트웨어 시스템이 에셜론으로 불리며, 미국 영국 캐나다 호주 뉴질랜드 등 영국계 5개국이 공동으로 운영하는 것으로 알려져 있다. 2000년과 2001년에 유럽 의회가 나서서 에셜론의 정체를 밝히려는 노력을 했으며, 이것의 일환으로 '개인과 상업통신을 가로채기 위한 글로벌 시스템의 존재에 대한 보고서'라는 긴 이름의 보고서❸가 발간되기도 했다.

그림 1❹은 상기 보고서에 기술된 UK의 Yorkshire Men-with Hill에 위치하는 지상 감청소의 전경. 1956년에 설치돼 2001년 기준으로 30여개의 위성 안테나가 있으며, 이중에서 12개의 위성 안테나는 직경이 20미터 이상인 대규모였다고 한다.

▲**그림 1** 지상 감청소의 전경

❶ 原題 : 'Echelon Conspiracy', http://www.gift2009.kr/
❷ 감청인지 도청인지 견해가 다를 수 있다
❸ European Parliament : Temporary Committee on the ECHELON Interception System, "REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)", 11 July 2001.
❹ http://www.panoramio.com/photo/7633607

현재의 글로벌 장거리 통신은 대부분 해저에 깔린 광케이블로 이뤄진다. 국제 인터넷 트래픽의 90% 이상을 해저 광케이블이 담당하며, 인공위성에 의한 트래픽 처리 비중은 10%에 불과하다❺. 따라서 글로벌 통신 엿듣기를 위한 수집소는 위성 안테나가 줄지어선 장관을 더 이상 연출할 필요가 없다. 글로벌 인터넷 트래픽의 추적을 전문으로 하는 TeleGeography 사의 자료❻에 따르면, **그림 2**처럼 USA는 인터넷 국제 트래픽의 허브 역할을 하고 있다. 즉, 세계 각 지역 간의 트래픽이 USA를 거쳐 간다는 것이다. 글로벌 통신 엿듣기를 위해 전 세계에 위성 안테나가 설치된 수집소를 운영하지 않아도 된다는 것을 의미한다. 뉴욕 타임즈 기자 James Risen이 저술한 'State of War'에서 미국의 통신회사와 컴퓨터 기업들이 NSA와 밀접한 관계를 유지하고 있다는 내용을 CNET 뉴스❼는 언급하고 있다.



▲ **그림 2** 인터넷 국제 트래픽 현황

강대국의 감시 프로그램

에셜론의 실체에 대해서는 국가안보라는 이유로 공식적으로 알려진 것은 그리 많지 않다. 청문회 자료나 기자의 추적기사 등 장님 코끼리 만지기 식의 이야기만 분분할 뿐이다. 방대한 기구와 인력을 동원해 '1984'의 빅 브라더처럼 사람들을 감시하는지, 이 중 개인의 사생활 정보나 타국 기업의 영업정보는 완벽히 제외되는지 알 수는 없다. 냉전 시대와 대테러 시대의 요구에 따라 국가기관에 의한 대량 감시(Massive Surveillance)는 어쩌면 필요악일 수 있다. 유럽 의회 보고서는 유럽회원국의 시민들은 자신의 프라이버시 보호를 위해 암호통신을 일상화할 것을 권고하고 있다.

개인이나 기업의 통신을 엿듣는 대량 감시 프로그램이 정부기관에 의해 운영되는 사례는 에셜론에 그치지 않는다. 중국 공안부가 운영하는 황금 방패(金盾 · Golden Shield) 시스템은 인터넷 공간에 대한 대표적인 대량 감시 프로그램으로, 이미 여러 차례 언론에 보도돼 그 존재가 잘 알려져 있다. 1998년 개발 프로젝트를 입안한 이래, 2003년 9월에 개발을 시작해 2006년 11월 1차 시스템을 완료하였고, 중국 내 모든 인터넷 정보흐름을 실시간 파악할 수 있는 2차 시스템을 2008년 12월에 완성한 것으로 알려져 있다❽. 황금 방패가 에셜론과 다른 것은 정보의 수집에만 머물지 않고 정보의 흐름을 차단하는 기능에 있다. 즉, 중국 영토 안팎에서 인터넷 상의 텍스트, 오디오, 동영상 정보를 실시간으로 분석하고, 이를 바탕으로 특정 정보와 서비스에 대한 접근과 전송을 차단한다. 대만 대륙위원회가 출간한 '대륙공작보고'의 황금 방패에 대한 전망 중에는 황금방패 프로젝트를 통해 축적된 기술과 인재는 군사용으로 전용돼 미래 전자정보전

❺ 한국일보 뉴스, "인터넷 흐름 90% 책임 해저케이블을 지켜라", 2009년 4월 8일.

❻ Tim Stronge, TeleGeography, Asia-Pacific & Latin American Traffic : Trends & Forecasts, April 2009. http://ahciet.net/comun/pags/agenda/eventos/2009/205/ponencias/ahciet.ppt

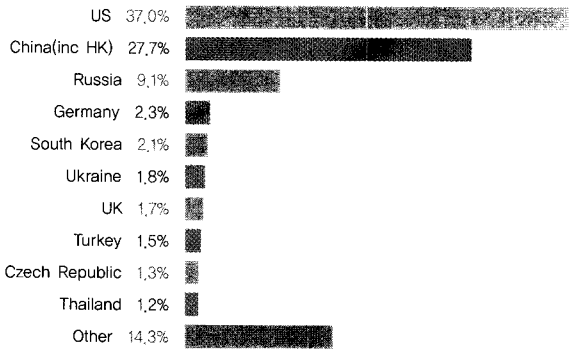
❼ CNET News, "NSA eavesdropping : How it might work", February 7, 2006. http://news.cnet.com/NSA-eavesdropping-How-it-might-work/2100-1028_3-6035910.html?tag=mncol

❽ 중일일보, 중, 인터넷 감시 '황금방패' 편, 2008년 12월 13일. http://china.joins.com/portal/article.do?method=detail&total_id=3418296

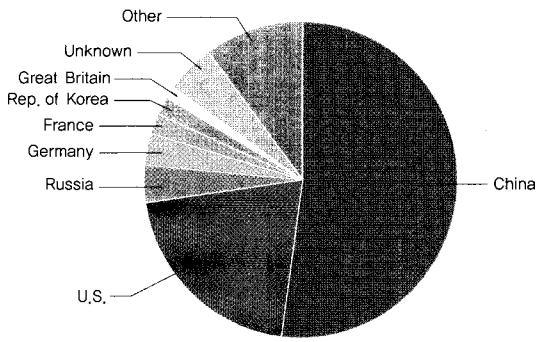
쟁의 주역이 될 수 있다는, 우리도 주목할 내용이 있다[9]. 최근 언론에 보도[10]된 공군 본부의 '2009 외국 군구조 편람' 책자에는 중국의 해커부대가 주미 한국공관, 독일 정부부처, 미 국방부 등을 해킹했다고 한다. 이는 글로벌 인터넷 공간의 신뢰를 심각하게 훼손시키는 일이 아닐 수 없다.

감시 프로그램과 인터넷 보안

에셜론, 황금 방패와 같은 대량 감시 시스템을 운영하고 있는 미국과 중국은 국가적으로 고도화된 데이터베이스와 네트워크 통제 기술이 축적돼 있을 것으로 예상된다. 기술적으로 인터넷 상에 유통되는 정보의 흐름을 통제할 수 있다면, 이 기술은 악성코드의 흐름도 통제하는데 사용될 수 있을 것이다. 그것이 불온 정보이든 (누구에게나) 악성코드이든 컨텐츠 통제라는 측면에서는 동일한 기술 영역 내에 있다. 그렇다면 미국과 중국의 국경 내에 위치하는 인터넷 공간의 보안 수준은 어떨까? 악성코드는 전체 사이버 사용자에게 불온한 것이니 말이다.



▲ 웹 악성코드 호스팅 상위 10개국(2009년 1월)



▲ 국가별 Badware 사이트 비율(2008년 5월)

영국의 보안업체 Sophos 社의 2009년 1월 보안위협 보고서[11]에 의하면, 악성코드를 전파하는 웹 사이트가 존재하는 국가는 전 세계에 150여개 이상인 것으로 나타났다. 이 중에서 상위 10개 국가는 위 좌측 그림과 같으며, 미국(37%)과 중국(27.7%)이 64.7%로 전체의 3분의 2를 차지한다. 동 보고서에는 악성코드를 작성한 언어에 대한 통계도 제시되어 있는데, Sophos 사가 발견한 악성코드 전체의 11.6%, 즉 악성코드 10개 중에 1개 정도가 중국어로 작성된 것이다. 한편 미국 하바드 로스쿨의 Berkman Center for Internet & Society에서 운영하는 StopBadware.org에서 2008년 5월 발간한 보고서[12]에는 위 우측 그림과 같은 국가별 Badware 사이트 비율이 제시되어 있다. 중국(52%)과 미국(21%)이 전체의 약 4분의 3(73%)을 차지한다. 또한 인터넷 사용인구 대비 Badware 사이트의 수의 비율도 분석한 바 있는데 평균적으로 인터넷 사용자 백만명 당 210개 사이트가 Badware를 가지고 있으며, 이중 중국이 689개로 최고로 많은 Badware 사이트를 가지며 세계 평균

[9] 신경진의 서핑 차이나, 인터넷 만리장성(황금방패) 완공 카운트다운, 2008년 12월 14일
http://blog.joins.com/media/folderListSlide.asp?uid=xiaokang&folder=10&list_id=10326619

[10] 보안뉴스, 중국 해커부대, 전 세계 상대로 해킹, 2009년 5월 14일
http://www.boannews.com/media/view.asp?idx=16049&kind=1

[11] Sophos Security Threat Report 2009,
http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

[12] May 2008 Badware Websites Report,
http://www.stopbadware.org

보다 3배 더 많은 것으로 나타났다. IBM의 X-Force 팀[13], Scan-Safe[14], McAfee[15], Microsoft[16] 등 주요 보안기업의 사이버 보안에 대한 통계 보고서들에서도 미국과 중국의 웹 사이트에 존재하는 악성코드의 심각성을 찾아볼 수 있다. 우측 그림은 미국 샌디에고에 위치한 보안업체 Websense사가 제공하는 글로벌 위협 지도[17]로, 미국과 중국에 분포하는 crimeware의 위협이 가장 높은 수준임을 보여주고 있다.

▲ 지난 12달 동안 crimeware 분포도(Websense Security Lab, 2009년 5월 기준)

그린 환경을 위한 공유지를 위해

글로벌 통신 네트워크인 인터넷이 만들어내는 사이버 공간은 共有地에 비견할 수 있다. 구성원 모두가 자기 이익만 추구하면 피폐해지는 그런 공유지 말이다. 사이버 공간에서는 함께 사용하는 시스템이 다른 시스템으로의 공격에 사용되기도 하며, 소수의 무지한 사용자가 전체 네트워크의 무결성을 훼손시키기도 하기 때문에, 일부의 허술한 보안으로 인한 비용을 모두가 나누어 부담하게 되고, 비용의 규모도 확대되기도 한다. 인터넷 사이버 공간에 넘쳐나는 악성코드, 잘못된 정보, 낡은 정보 등 부정확하거나 유해한 정보들은 인터넷 공유지를 오염시키는 공공의 적이다. 인터넷 전자우편의 80% 이상이 스팸이라는 사실[18]을 심각하게 받아들여야 한다. 오늘날 현대 과학기술을 집대성한 에셜론과 황금방패가 인터넷의 글로벌 신뢰를 갉아먹는 감시와 통제의 도구가 아니라, 그런 인터넷을 가꾸는데 쟁기로 활용하는 현명함이 절실해진다. 그런 의미에서 미국과 중국은 최강의 나라답게 인터넷을 그런 환경이 되도록 앞장서는 모범을 보여야 한다.

역사적으로 인류는 개인의 프라이버시 권리를 신장하기 위한 부단한 노력이 이어지고 있다. 그런데 정보기술이 발전을 거듭함에 따라 보안과 프라이버시의 충돌이 곳곳에서 발생하고 있다. 기술의 편리함, 국가·사회 안전, 신변보호 등을 이유로 그 동안 쟁취했던 프라이버시를 후퇴시키고 있다. 아무도 빅 브라더를 원하고 있지 않지만, 이런저런 이유로 오히려 빅 브라더를 키워가고 있다. 영화 '기프트'에서 보여주었던 인공위성을 통한 영상감시와 네트워크 통제 능력으로 주인공이 숨을 곳이 없게 하는 장면은 섬뜩한 전율을 느끼게 한다. 물이 배를 띄울 수도 있지만 배를 뒤집을 수도 있다는 것을 항상 염두에 둬야 한다. S

[13] IBM Internet Security Systems, X-Force 2008 Trend & Risk Report, January 2009.
www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf

[14] ScanSafe, Annual Global Threat Report, March 2009.

[15] McAfee, Mapping the Mal Web, Revisited, June 2008.

[16] Microsoft Security Intelligence Report volume 6 (July-December 2008)
http://www.microsoft.com/presspass/newsroom/security/factsheets/04-08SIRv6FS.mspx

[17] 2009년 5월 13일 액세스.
http://securitylabs.websense.com/content/CrimewarePhishing.aspx

[18] messagelabs intelligence 2008 annual security survey