해킹의 문화정치에서 해킹문화운동으로

조동원 (dongwon@riseup.net 미디어운동/문화연구)
초안: 2009년 8월 16일

목차

요약

2009년 '77분산서비스거부 공격'과 정부의 대응 과정은 해킹을 다시 한 번 사이버 테러나 재난, 국가 안보의 위협으로 인식하도록 했다. 그러나 인터넷의 '서비스거부'는 저작권법 위반에 대해 인터넷 접속 제한으로 처벌하는 이른바 '삼진아웃제'를 통해서도 발생하게 생겼다. 사회 공공성에 대한 '서비스거부'는 신자유주의 정책과 권위주의 국가 운영에서 다양하게 나타나고 있다. 이와 비슷하게 해킹에 대한 국가 권력의 규제나 주류 미디어의 왜곡된 재현은 기술에 대한 자율적 탐구, 커뮤니케이션 네트워크에서의 표현의 자유, 온라인에서의 정당한 시위를 제약하고 통제하는 효과를 갖는다.

해킹이 점차 범죄나 테러의 방법으로 널리 사용되면서 우리는 보통 이를 사이버범죄, 사이버테러로 받아들이고 있지만 해킹은 애초에 기술에 대한 지적 탐구이자 혁신의 과정을 의미했다. 1960년대 이래 해킹은 개인용 컴퓨터, PC통신, 인터넷의 개발과 발전에 큰 기여를 했고, 정보와 지식의 공동 생산과 공유의 문화를 만들어 왔으며, 사회정의를 위한 직접행동의 방식으로 채택되기도 했다. 하지만 냉전, 신자유주의, 지구화, 저작권 체제 강화, 그리고 디지털 네트워크 기술의 복합적인 사회역동 속에서 해킹은 다양하게 변형되어왔다. 이 글은 표현의 자유와 대안적 생산방식(자유소프트웨어운동), 온라인 직접행동(해킹행동주의), 범죄 및 전쟁의 수단으로서의 해킹(해킹의 범죄화, 군사화)의 세 가지 갈래로 해킹과 해커문화의 역사를 추적하면서 해킹의 문화정치 지형을 탐색하고, 현재의 지배적 기술문화의 근본 독점을 극복하기 위해 해킹의 정치적 잠재력을 해킹문화운동의 차원에서 재배치해보자고 주장한다.

열쇠말

분산서비스거부(DDoS), 해킹, 해커문화, 자유소프트웨어운동, 해킹행동주의(hacktivism), 저작권, 사이버범죄, 사이버테러, 해킹문화운동

'77 분산서비스거부 공격'과 '서비스거부' 사태들

애초에 '서비스거부'는 '공격'이 아니었다. 1990년대에는 인터넷을 하다가 종종 '서비스거부' 화면을 볼 수 있었다. 당시 대부분의 웹사이트들은 갑자기 많은 사람이 '방문'하게 되면 그 접속량을 감당하지 못해 "서비스거부"(Denial of Service)라는 문구를 보여줬다. 그러다가 일부러 '서비스거부'를 유발하는 행위들이 나타났다. 이에 '공격'이라는 말이 붙었다. 이번 '77 분산서비스거부 공격'에 대한 대부분의 뉴스가 그랬듯이, '서비스거부'를 유발하거나 허가받지 않은 컴퓨터 네트워크 침입 따위를 한데 묶어 해킹(hacking)이라고 부른다. 어떤 해킹은 돈을 벌기 위해 일부러 '서비스거부'를 유발시키고, 어떤 해킹은 정치적 행동으로 그렇게 한다. 지금은 돈벌이를 위한 '서비스거부 공격'이 훨씬 많지만 처음에는 온라인 시위를 위한 것이었다. 이것이든 저것이든 '공격'으로 규정되고, 사사로운 이해관계로 '서비스거부'를 유발하는 경우 그것은 예를 들어 정보통신망이용촉진및정보보호등에관한법(망법으로 줄임)에 따라 '침해 사고'[1]가 되어 처벌받게 되고, 정치적 행동으로서 '서비스거부' 유발은? 이 역시 여타 법에 따라 범죄로 분류된다. 해킹이라고 다 같은 해킹이 아닌데 둘 다 불법이다.[2]

'서비스거부 공격'은 분산의 형태로 진화했다. 불법이다 보니 이를 행하는 '공격'자는 자신의 위치를 노출시키기 않기 위해 점차 수많은 일반 이용자 컴퓨터를 이용해 공격을 '분산'시키는 방법을 쓰게 된다. '악성코드'로 통칭되는 프로그램을 작성하거나 얻어 수많은 이용자 컴퓨터를 좀비컴퓨터로 감염시키기만 하면 자동화된 '분산' 공격을 할 수 있다. 그러나 해킹행동주의(hacktivism)의 사례를 보면, 그러한 소프트웨어의 개발이 없지 않았지만 정치적 의사 전달에 목표를 두기 때문에 수많은 사람들이 연좌시위 하듯이 목표대상이 된 웹사이트에 몰려가 '공격'하는 수동적인 '분산'의 방식을 취한다. 이때의 '분산'은 자동화된 것이 아닌 만큼 대부분의 가상 연좌시위에 참여하는 사람들은 어떤 나쁜 생각에 전염된 좀비가 아니다. 예를 들어, 2008년 6월 10일 대규모 촛불집회 현장에서 청와대 홈페이지의 '서비스거부'를 유발한 사태가 그렇다. '공격 명령'자는 집회의 사회자였고 '좀비컴퓨터'는 실시간 인터넷 생중계를 보고 있던 네티즌들이었고 그들을 '감염'시킨 '악성코드'는 "촛불 앞에 꿇어라!"[3]로 요약할 수 있는 '명령어'였다. 실제로 청와대 홈페이지는 이 '공격'으로 광화

1 "(제2조 7) 침해사고란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다."

2 경찰청의 사이버테러대응센터(http://www.ctrc.go.kr)는 해킹, 바이러스유포, 메일폭탄, DOS공격 등 전자기적 침해 장비를 이용한 컴퓨터시스템과 정보통신망 자체를 공격하는 행위를 '사이버테러형범죄'라 하고, 사이버도박, 사이버 스토킹과 성폭력, 사이버명예훼손과 협박, 전자상거래 사기, 개인정보유출 등의 행위를 '일반사이버범죄'로 부르고 있다.

3 작년 610 대규모 촛불집회의 참여를 독려하기 위해 소울드레서, 82쿡, 디브이디프라임, 마이클럽 등이 모금하여 한겨레 등에 낸 광고의 문안이었다.

문 거리 한복판에서 마이크잡고 있던 사회자의 '공격 명령'이 있은 지 몇 분 만에 '서비스거부' 되었다. 망법의 "침해 사고"에 해당하는 불법 행위였지만, 우리는 이를 불법 행위로 이해하지 않고 온라인 시위로 보았다.

'서비스거부' 형태의 해킹이 절도나 금품탈취를 위한 범죄가 아니라 해킹행동주의(hacktivism)로 명명되는 정 치적 가상 시위로 시작되었고 지금도 종종 그런 차원에서 발생한다. 물론 새로운 얘기가 아닌 것이 일본과의 독도 분쟁이나 교과서 왜곡 사태, 중국의 동북공정, 올림픽이나 월드컵에서 불공정 판정 시비가 있을 때마다 민족주의의 발로로 해킹 행동이 적극 채택되어 왔다. 컴맹은 아닌 범죄자들, 성질 급한 민족주의자나 애국 시민들, 그리고 신자유주의 세계화를 반대하는 활동가들은 각기의 목적으로 해킹을 자기 이해나 발언을 위한 행동 방식으로 이용한 것이지만, 법적으로 그리고 뉴스 보도에 따르면 모두가 나쁜 짓을 한 것이고 처벌받을 수 있다. 온라인에서의 정치적 발언과 행동을 별도로 구분하고 기본권으로 보장하지 않다보니, 지 난 6월 10일의 집단 해킹 행동이 직접적인 원인이 된 것은 아니었지만, 인터넷에서 뿜어져 나온 2008년 촛불시위의 위력 때문에 정부의 인터넷 통제는 더욱 거세져 온라인상의 표현의 자유는 심각하게 위축되었고 인터넷에 애초에 있지 않았던 국경을 넘는 '사이버망명' 사태가 대량으로 발생했다. 물론 그 전에라도 저작권을 관리하며 돈벌이하는 기업들의 로비와 압력을 받은 대형 상업 포털 사이트들이 명예훼손이나 저작권침해 가능성만으로 게시물을 함부로 차단시켜버리면서('임시조치') 익명성의 보장과 표현의 자유 실현이라는 인터넷 본연의 서비스를 거부해 왔다.

그렇다. 기대한 대로 기능하거나 역할하지 않는 어떤 시스템의 이상 상태를 '서비스거부'로 본다면, 온갖 '서비스거부' 사태가 지천이다. 신용 불량자라고 낙인찍고 그들에 대한 (사채를 제외한 공식 금융권의) '서비스거부'가 그렇다. 통계 수치에서도 '미디어법'이 대의가 아니라는데 대의를 위해 봉사하겠다던 국회를 장악한 정치인들의 '서비스거부'는 어떤가. 이제 그 법들이 허용하는 새로운 미디어 소유와 경영은 '공영방송'이라는 이름을 가까스로 지켜왔던 주류 미디어의 공공 서비스를 완전 거부할 것이 아닌가. 그런 비판 능력도 없어지면, 함께 어우러져 살고 있으나 '국민'이 아닌 사람들에 대한 공공 '서비스거부,' 그렇지 않아도 성문 벽으로 내몰려온 사람들을 다시 성을 짓겠다고 아예 성문 밖으로 내좇아 버리면서 사람이 죽어나가도 나 몰라라 하는 '서비스거부,' 이런 거부들이 늘 동반하는 공권력의 폭력과 공격, 더 나아가 국민이고 자시고 간에 아예 공공 서비스 자체를 없애버리는 원천적인 '서비스거부'를 실행하는 신자유주의 정책들은 살판나는 건가. 그야말로 공공 '서비스거부'의 신자유주의 공격을 위해 옛 것 새 것 할 것 없이 온갖 국가 기구와 법제들이 좀비처럼 되살아나 활보하고 있다. 두 달이 넘는 공장 점거 파업으로 예의 신자유주의 공격에 맞서 투쟁한 쌍용차 노동자들에게 물과 음식과 의료 서비스를 차단하기를 멈추지 않았던 기본 인권에 대한 '서비스거부'는 그 중에서도 야만적인 좀비였다.

'77 분산서비스거부 공격' 사태를 계기로 해킹의 의미를 두루두루 짚어보자는 얘기인데 '서비스거부'를 너무 확대 해석한 것인가. 그럼 좀 비슷한 사태와 연관시켜보자. 7월 초의 '분산서비스거부 공격' 사태가 발생하고 얼마 안 있어 행정권에 의한 인터넷 '서비스거부'가 준비 완료되었다. 일명 '삼진아웃제'를 포함한 개정 저작권법은 이를 위반한 복제물을 3번 올리면 특정한 전자게시판이나 이용자 계정(ID)을 6개월 동안 못쓰게 할 것이라는 인터넷 '서비스거부' 유발 사태다. 인터넷 서비스 이용의 차단 혹은 거부라는 점에서 결과적으로 두 가지 사태는 다르지 않다. 하나는 '불법'적인 "침해 사고"(망법 2조 7) 형태로, 또 하나는 '합법'적인 처벌 절차(저작권법 133조 2, 정보통신망을 통한 불법복제물 등의 삭제명령 등)로 이뤄지고 있는데, 어떤 것은 '불법인가 보다'하고 어떤 것은 '이건 아니잖아!'[4]라는 두 가지 우리 반응의 차이가 어디서 근거한 것인지 한 번 생각해 볼만 하다. 물 론, 이번 '분산서비스거부 공격'을 누가 했는지 왜 했는지 그 사람이 직접 나서서 알려주기 전에는 거의 알아낼 수 없다고 하는데, 일정한 불편(?)과 피해를 끼친 이런 해킹을 적극 옹호할 이유는 없다. 그러나 이러한 네트워크 문화 현상을 보다 복잡한 문화정치의 구도에서 보지 않는다면 현행법의 모순과 그 인위적 경계를 넘지 못한 채 우리의 기본 권리를 확장하기는커녕 어느새 크게 위축되고 축소되는 것에 동의해주는 순간에 닥칠 수 있다. 두 가지 때문이다.

첫째, 이번 공격에 대처하는 국가 기관과 주류 미디어의 태도를 보면 명백한 불법 해킹이나 테러라고 수긍하며 그냥 넘어가기에는 깔끔하지 않은 게 많다. 해킹에 대한 정부 대책은 과도하게 국정원의 사이버테러방지법이나 방송통신위원회의 인터넷 통제 정책을 강화하는 쪽으로 흐르기 십상이다. 2003 인터넷대란 때는 모든 사람들이 네트워크를 못 쓴 사태가 난 것이었던 반면, 이번의 경우 인터넷 이용자들에게는 별다른 불편이나 피해가 없었기 때문에 나라 전체가 들썩거려야 할 사건이 아니라 그 사이트들의 보안 문제 해결로 국한되었어야 하지만, 정부 기관들이나 미디어의 태도는 2003년과 같은 '대란' 운운하며 모든 이들의 재난처럼 이 사태를 규정했다. 그래서 거의 모든 인터넷 이용자가 분산된 서비스거부 공격을 대리하는 좀비컴퓨터가 될 수 있는 잠재적 공격자로 내몰렸고, 감염된 것으로 보이는 개인용 컴퓨터의 인터넷 접근을 아예 못하게 하는 조치까지 거론되었다.[5] 또, 사태 초기부터 국정원은 '사이버 테러'를 들먹였고 북한 배후설을 내세웠고 모두 헛소동으로 끝났지만 그 효과는 컸다. 네트워크 보안 강화의 필요성은 국가 '재난'과 같은 표현을 거쳐 '테러'나 사이버 '국가 안보'의 논리로 자연스럽게 이어졌다. 그러나 네트워크의 보안이 국가 안보

4 프랑스에서 소위 '삼진아웃제'가 기본권을 침해한다는 위헌 판결을 받은 것처럼, 현재 '합법'화된 한국의 삼진아웃제가 검열의 소지가 있기 때문에 정보공유연대나 참여연대에서 위헌 소송을 검토하고 있다.

5 그에 따라 우리는 백신 프로그램의 설치를 강요당했다. 백신 프로그램만이 악성코드를 잡아내고 해킹 공격을 막을 수 있다는 사고방식이라면, 특정한 백신 프로그램이 설치된 컴퓨터는 인터넷 접속이 가능하고 아닌 것은 안 되는 식으로 인터넷 접근 구조 자체를 변경시키는 재앙에 가까운 '서비스거부' 사태로 가지 말란 법도 없다. "흘러나온" 얘기라지만 실제로 방송통신위원회는 백신 소프트웨어가 설치되지 않은 개인용 컴퓨터의 주요 웹사이트에 대한 접속 제한을 고려하고 있다(강진규 2009). 문화체육관광부의 저작권법 위반 인터넷 '삼진아웃제'에 못지않은 발상이다.

와 동격이 되는 것에 우리 모두가 동의할 때 벌어질 일은 이미 한나라당 공성진 의원 등이 발의한 '국가사이버위기관리법'에 잘 나타나 있다. 예컨대 단순한 해킹 사고조차 모두 국정원장에게 즉각 보고해야 하고 즉각 조사 결과를 통보해야 한다. 또, 필요하다면 언제든지 국정원장이 모든 시스템에 직접 접근할 수 있는 권한이 부여된다(전응휘 2009). 이 말은 곧 국정원 등이 모든 개인의 컴퓨터를 들춰 보겠다 이다. 후기-냉전 시대에 북한의 존재에만 의존할 수 없는 국정원의 자기 생존 전략이 아니더라도, 각 국에서 만들어져온 컴퓨터 범죄 관련법들이 "사이버 테러리즘이나 핵티비즘에만 국한되는 것이 아니라 모든 형태의 해킹과 컴퓨터 네트워크에 대한 공격, 컴퓨터 및 통신 사기, 인터넷 아동 포르노, 그리고 디지털 저작권 침해(소프트웨어, 음악 등)의 행위를 총체적으로 뿌리 뽑는 것을 목표"(데닝 2005: 344)로 해왔다는 점을 놓고 볼 때, 모든 해킹에 대한 전적인 국가 통제를 무작정 합의해 주는 일은 곧 우리의 디지털 네트워크 생활문화에 검열과 감시를 거듭 불러들이고, 자유롭고 평등한 정보 접근 및 정보공유 활동을 옥죄게 하는 결과로 이어진다.

둘째, 우리가 일상생활의 사건사고가 된 빈번한 해킹 현상을 현행법의 시각과 주류 미디어의 판단에만 의존할 때 생기는 또 하나의 문제는, 국가 기구나 독점 기업에 의한 정보 흐름과 네트워크 하부구조에 대한 감시, 통제, 착취에 저항해온 유력한 사회운동이 곧 해킹에서 비롯되었으며 현재도 계속되고 있는 해킹운동을 잘 살리기보다는 저버리고 만다는 점이다. 개인정보의 보호, 네트워크의 보안, 그리고 표현의 자유가 보장되는 가상 공간이 그나마 지금처럼 된 것이 그들 덕분이기도 하거니와, 한편에서 국가 권력에 의한 인터넷 검열과 통제, 다른 한편에서 거대 기업들의 네트워크 하부구조의 사유화와 공동체 생산의 착취에 맞서고자 할 때 줄잡아 1960년대부터 그에 저항하고 대항문화를 만들어온 해킹 활동을 제쳐둘 수는 없는 노릇이다. 애초에 해킹은 오늘날 '삼진아웃제'의 저작권법과 같이 정보의 자유로운 공유를 통제하는 '서비스거부'에 반대하는 행위로 시작되었고 카피레프트 운동의 뿌리였다. 그렇다면 현행법과 국가 기관들이 사사로운 돈벌이를 위한 해킹이든 정치적 저항과 표현의 자유를 위한 해킹이든 상관없이 한통속으로 때려잡고 있는 것을 우리가 곧이곧대로 받아들여야 쓰겠는가.

전자 상거래나 대기업의 웹사이트를 통해 대규모의 개인정보 유출 사건이 발생했을 때 개인정보 보호를 위한 대응이 상당히 있었던 것에 비해, 이번 사태에 와서 정부 기관이나 주류 미디어의 '호들갑'은 그렇다 치고, 시민사회나 사회운동 진영은 이 일에 무관심하거나 어떻게 봐야할 지 명확하지 않았던 것 같다. 당 장 눈에 보이는 피해가 발생하거나 희생자가 있는 일들은 쉽게 문제 삼고 여론을 형성해 내며 반론과 반대 행동이 터져 나오지만, 이러한 '희생자 정치'가 누락하기 마련인 일상의 지배 문화에 대한 대항과 대안의 창출은 국가나 시장에 맡길 수 없는 사회의 자기보호를 위한 기획과 노력으로 가능하다. 이를 위해 우선 우리는 해킹이 가진 드넓은 영역 – 기술 탐구와 혁신, 자유/오픈소스 소프트웨어 개발, 카피레프트운동, 해킹행동주의, 사이버범죄, 사이버테러 등의 복

잡한 정치적, 전술적, 기술적, 윤리적, 법적 속성을 토론하고 다양한 대안의 가능성을 모색할 필요가 있다. 이 글은 이를 목적으로 한다. 무엇보다도 더 늦기 전에 거부해야 할 '해킹 = 사이버 범죄, 사이버 테러'라는 단순 도식에 도전한다. 이를 위해 해킹의 복잡다단한 역사 중에서 오늘의 토론을 위해 필요한 부분만 다룬다. 우선 처음에 해킹은 어디서 어떤 의미로 생겨났는지 알아보고, 그 후 다양하게 분화돼온 해킹의 역사적 흐름을 세 가지 갈래 - 표현의 자유와 대안적 생산방식(자유소프트웨어운동), 온라인 직접행동(해킹행동주의), 범죄 및 전쟁의 수단(해킹의 범죄화, 군사화) -로 살펴보고, 이것들이 해킹의 문화정치의 장에서 어떻게 충돌하고 혹은 결합해 왔는지 짚어본다. 지난 반세기동안 냉전, 신자유주의, 지구화 그리고 디지털 네트워크 기술의 복합적인 사회역동에 함께 얽히고설킨 해킹과 해커문화의 몇 가닥을 간추려보는 것이다. 그리고 마지막에 해킹을 문화운동의 차원에서 다시 재배치해보자고 주장한다.

냉전, 컴퓨터, 해킹

해킹(hacking) 혹은 '핵'(hack)이라는 말은 1950~60년대 미국의 매사추세츠 공대(MIT로 줄임)의 컴퓨터 기술자들이 사용한 은어 중의 하나였다. 당시 MIT에는 철도 시스템을 연구하고 모형을 만드는 '테크모델철도클럽'(Tech Model Railroad Club, TMRC로 줄임)이라는 동아리가 있었고, 그 중에서도 '신호기와 동력분과'에 속한 회원들은 철도 시스템 설계를 위한 원리와 구조의 탐구에 푹 빠져 있었다. 이들은 오래 전부터 MIT의 학생들이 정성들여 만들어내던 고약한 농담을 가리킬 때 쓰던 '핵'이라는 말을 가져다가 자신들의 지적 탐구 작업에 적용하였다. 이들의 '핵'이라는 말은 "작업과정 그 자체에서 느껴지는 순수한 즐거움 이외에는 어떠한 건설적인 목표도 갖지 않는 프로젝트나 그에 따른 결과물"(레비 1996: 22)을 뜻했다. 한 회원이 철도 모형의 여러 계전기 사이의 정교한 연결망을 완성하고 그것을 '단순한 핵'을 했다고 표현하더라도 동료들은 그 정교한 장치를 혁신, 스타일, 기술 그 자체에 대한 탐구의 결과물로 받아들였다. 최소한 그 회원들은 스스로를 '해커'(hacker)라 부르며 상당한 자부심을 가졌다(23).

해킹과 해킹행동주의를 꾸준히 연구해온 조단(Jordan 2002)은 '핵'을 "기술의 혁신적인 사용"(120)으로 짧게 정의한다. 여기서 기술은 반드시 첨단 기술에 국한되지 않는다. 조단은 한 해커가 든 예를 소개하고 있는데, "차를 마시려는데 전기 주전자가 없지만 커피 끓이기(coffeemaker)가 있을 때 그걸 이용해 물을 끓여 차를 타마셨다면, 커피 끓이기를 다른 방식으로 사용한 그것이 핵이다"(120).

컴퓨터 해커문화의 형성

2차 세계대전 이후컴퓨터는 핵전쟁의 불가능성의 가능성이라는 냉전의 거대한 역설 하나를 해결하기 위한 도구로 주목받았다. 핵무기를 가진 양쪽이 실제 핵전쟁을 하는 것은 자살행위나 다름없지만 적군과 아군의 핵전력을 확신 할 필요가 있었고, 이를 시험하고 실제 상황에서도 활용할 수 있는 도구가 필요했던 것이다. 그런 맥락에서 아이비엠사(IBM으로 줄임)는 '방어계산기'(Defense Calculator)를 사용해본 한국전쟁 기간 동안 발전시킨 컴퓨터 연구를 미국 국방성의 의뢰와 지원을 받아 지속하며 최초의 프로그램 가능한 디지털컴퓨터를 제작했다(기어 2006: 83, 99; 바브룩 & 카메론 1996: 55). 그리고 MIT는 다양한 전쟁 시나리오의 모사(simulation)와 전투의 자동화를 위한 미국의 컴퓨터 개발 프로젝트와 연계된 정보제어학(cybernetics)과 인공지능 연구에서 그 어느 곳보다 앞선 곳이었다.

IBM의 관료적 컴퓨터 개발 분위기와 함께 MIT에 들어온 조기경보시스템과 인공지능 실험을 위한 대형 컴퓨터에 대한 학교 당국의 관리는 엄격했다. 하지만 1960년대 초기의 원시적 시스템에 존재하는 컴퓨터 보안이라는 것은 전적으로 물리적인 것이었다. 비싸고 신비한 하드웨어 장치 근처에 오도록 허용된 사람은 그 자격을 갖춘 전문가로 제한되었다(스털링 1993: 72). 그런데 TMRC의 신호기와 동력분과 회원들은 기계와 제어장치의 새로운 형태인 컴퓨터(IBM704)가 인공지능연구소에 들어왔다는 소식을 듣고 그냥 지나칠 수가 없었다. 물리적으로 통제되던 컴퓨터에 접근하기 위해 이들은 열쇠를 부수고 컴퓨터 터미널이 설치된 방에 몰래 들어가 사용하기 시작했고 비교적 자유로운 연구소 분위기에서 그들의 접근과 프로그래밍은 더러 공식적으로 허용되기도 했다(레비 1996: 13-44). 초기 컴퓨터 시스템은 집채만 한 크기의 메인프레임 컴퓨터였는데 단지 시동을 걸고 동작시키는데도 상당한 내부 작업이 필요했기 때문에 당시 컴퓨터 사용은 곧 "일상적으로 운영체제의 가장 깊고 비밀스러운 곳을 침범"하는 것과 다름없었다(스털링 1993: 72). 오늘날에도 널리 사용되는 컴퓨터 시스템의 '침입'을 위한 기초 기술(패스워드 파괴, 트랩도어, 백도어, 트로이 목마)은 컴퓨터 자원과 가상 공간에 대한 소유권이나 비밀의 개념이 없었던 1960년대의 상황에서 이들 초기 해커들이 만든 것들이다(스털링 1993: 73). 허가된 전문가들보다 뛰어난 전문 지식을 축적해간 이들은 컴퓨터의 작동 과정을 새로 고안하고 프로그래밍 하는 자신들의 탐구 활동에 대해서도 '핵'한다고 표현했다. 이렇게 시작된 해킹 혹은 해커공동체는 오늘날 컴퓨터 해킹과 해커문화의 기원이 된다.

정부는 복지서비스 같은 곳에 컴퓨터를 사용할 생각은 하지 않고 죽음의 핵무기를 제어하는데 사

용할 뿐이었고, 기업들은 보통 사람들이 접근하지 못하도록 엄청난 가격으로 최첨단 장비들을 생산해 관료주의의 철제 벽 속에 보관하고 있었다(스털링 1993: 77). 초기 해커들은 컴퓨터에 대한 접근이 관료주의 통제에 막힌 것, 지적 탐구로서 자신들의 해킹으로 만들어진 프로그램이나 정보를 기업이나 연구소가 점차 독점해 가는 것에 강한 반감을 가지며 컴퓨터 자원에 대한 접근 권리와 정보 공유 정신을 담은 '해커 윤리'를 만들게 된다. 이들의 해킹은 '순수한 즐거움'에서 자율적인 컴퓨터 이용을 위한 반권위주의적 정치윤리로 확장된 것이다. 이들의 해커윤리는 다음과 같다(레비 1996: 46-59).

- 컴퓨터에 대한 접근은 완전히 자유를 보장받아야 한다.
- 모든 정보는 개방되어야 하고 공유해야 한다.
- 모든 권력을 불신하고 분권화를 촉진하라.
- 해커들은 그들 자신의 해킹에 의해서만 심판받아야 하며 나이, 성, 지위나 재산 같은 판단 기준에 의거해서는 안 된다.
- 컴퓨터를 통해 예술과 아름다움을 창조할 수 있다.
- 컴퓨터는 모든 생활을 보다 나은 방향으로 변화시켜줄 수 있다.

위 내용은 오늘날 정보공유를 주장하는 다양한 운동들의 뿌리가 최초의 해커공동체에서 나왔다는 것을 단적으로 보여준다. 이들은 컴퓨터와 놀면서 '헥'할 수 있었던 소수 엘리트들이었지만, 전쟁을 위해 그리고 자본의 요구에 맞춰 개발되기 시작한 컴퓨터에 허가받지 않은 접근을 시도하며 컴퓨터 기술의 상당한 혁신을 일궈내는 동시에 정보의 자유로운 접근을 위한 철학을 만들어낸 것이다.

해킹의 전개와 분화

미국의 한 대학에서 등장한 해커문화는 1960년대 이후 다른 곳으로 퍼져나가며 다양한 형태로 분화되어 왔다. 1970년대는 대학 연구소를 중심으로 한 엘리트 해커들 외에도 지역 공동체에 기반을 둔 아마추어 해커공동체들이 형성되었고, 이들은 민중의 손에 들려질 컴퓨터 하드웨어와 커뮤니케이션 네트워크를 탐구하는데 주력했다. '메모리 공동체'(Community Memory), '홈부르클럽'(Homebrew Club), '민중컴퓨터사'(People's Computer Company) 등 하드웨어 해커공동체들은 1970

년대 후반 개인용 컴퓨터(PC)를 개발하고 대중화하는데, 그리고 초기 풀뿌리 인터넷인 전자게시판(BBS)으로 점차 세계를 연결하는데 크게 기여했다. 그러는 동안, 반전운동과 히피문화를 배경으로 최초의 정치적 해커공동체들이 출현했다. '프리커'(phreaker)라고 불리는 전화 해커가 그 선두에 있었다. 1980년대로 가보면, 컴퓨터 네트워크 해킹이 서서히 많아지고 프로그래밍(소프트웨어 개발) 해킹과 정치적 네트워크 해킹이 동시에 발아하였다. 인터넷이 대중화되기 이전에 풀뿌리 해커들이 개발한 개인용 컴퓨터 통신(PC통신으로 줄임)을 통해 지역들을 연결하는 컴퓨터 네트워크가 구축되면서 네트워크 해킹이 점차 증가하고, 전화 시스템에 대한 프리킹과 함께 금품을 노리는 컴퓨터 범죄가 나타나기 시작했다. 정부 기관이나 군사 시설의 컴퓨터에 대한 침입 및 반핵 항의와 같은 정치적 네트워크 해킹도 몇 차례 이뤄졌다. 그러나 1980년대 해킹의 역사에서 무엇보다도 중요한 사건은 소프트웨어 해커들의 자유소프트웨어운동과 카피레프트운동이 시작되었다는 사실이다.

1990년대의 해킹은 다양한 형태로 분화되어 현재에 이르는 양상을 보여준다. 우선 소프트웨어 해킹은 리눅스(Linux)의 등장으로 초기 인터넷을 타고 지구적 규모로 발전해 나갔다. 한편에서 네트워크 해킹이 범죄의 수단이 되고 사이버테러나 사이버전쟁에 대한 우려도 커졌다면, 다른 한편에서 해킹행동주의(hacktivism)라는 이름으로 해킹은 정치적 행동주의와 만났다. 1990년대부터 다양하게 분화된 해킹은 2000년대에 양적으로 더 확산되는 추세다. 사이버범죄 등을 위한 수단으로 해킹이 빈번히 이용되고, 자유소프트웨어운동은 지구적인 네트워크를 형성하며 확산되고 있다. 해킹행동주의는 2000년대 초반까지 신자유주의 세계화 반대 투쟁과 결합하며 활발히 전개되다가 대중 투쟁이 벌어지는 상황에서 해킹활동가들뿐만 아니라 일반 이용자들이 해킹 행동에 나서는 사례들도 많아지고 있다.

한국의 경우, 개인용 컴퓨터가 본격적으로 보급되기 직전인 1980년대 말에 전자게시판에서 '엠팔'과 같은 해커공동체가 등장했는데, 이들은 최초의 한글 통신용 오픈소스 소프트웨어라고 할 수 있는 '엠팔의 반란'을 개발하고 보급했다. 당시 고가에 판매된 PC통신용 소프트웨어(에뮬레이터)를 독자적으로 개발해 누구나 대가없이 사용할 수 있도록 공개한 것이다(김강호 1997: 109). PC통신이 활발하던 1980년대 말부터 1990년대 중후반까지 '참세상'과 같은 독립적인 네트워크가 나타나면서 한편으로는 사회운동에 대한 정보의 수집과 교환을 위해, 다른 한편으로 전자 커뮤니케이션 영역의 독자적인 운동 의제들 – 온라인 검열반대, 정보의 사유화 반대, 프라이버시 등의 계발과 운동을 위한 움직임들이 있었다.

자유소프트웨어운동: 저작권 비판과 대안 생산방식

MIT 인공지능연구소에 있다가 자유소프트웨어재단을 세운 리처드 스톨만(Richard Stallman)은 1960년대 해킹의 '황금시대'에 생겨난 정통 해커윤리의 세례를 받았지만, 1980년대 컴퓨터와 소프트웨어 산업은 더 이상 해커윤리를 가만두지 않았다. 레비(1996)는 스톨만을 '마지막 해커'라고 부른다. 1980년대 초반, 마지막 정통 해커가 MIT를 뛰쳐나가며 주창한 자유소프트웨어운동은 소프트웨어 개발에 국한되지 않고 다양한 지식과 문화 생산영역에서 저작권 강화에 반대하고 대안을 모색하는 카피레프트운동의 진원지다.

소프트웨어의 상품화

그런데 왜 1980년대 초반에 소프트웨어 영역에서 카피레프트운동이 시작되었는가? 그 전까지만 해도 소프트웨어는 컴퓨터 연구와 해킹의 이차적 부산물이었다(Söderberg, 2002). 소프트웨어는 교환가치를 갖는 상품으로 전혀 인식되지 않았고, 자유롭게 나눠 쓰고 누구나 기능을 향상시킬 수 있는 공동 생산물이었다. 소형 컴퓨터에 적합한 운영체제(OS) 소프트웨어인 유닉스(Unix)도 마찬가지였다. 유닉스는 미국전신전화사(American Telephone and Telegraph, AT&T로 줄임) 산하의 벨(Bell) 연구소에서 일부 연구원들이 소형 컴퓨터의 운영체제를 해킹하며 비공식적인 취미 프로젝트로 개발되었다. AT&T 내부에서 먼저 인기를 얻고 점차 대학들과 아마추어들에게까지 확산되었다. 유닉스는 소스 코드를 포함하여 자유롭게 배포되었기 때문에 누구나 원한다면 수정할 수 있었다(Söderberg, 2007: 14-5).

1980년대 초반, 소프트웨어에 대한 자본의 두 가지 종획(enclosure)은 그런 공유의 문화를 파괴하기 시작했다. 하나는 IBM이 저작권법을 이용해 소프트웨어에 대한 강제적 이용허락(license)을 채택하기 시작한 것이다. 이는 일본 통상산업성(Ministry of International Trade and Industry, MITI)이 1980년대 초에 소프트웨어에 별도의 지적 재산 법률을 적용하면서 촉진된 것이었다. 이 법은 15년의 보호기간, 강제적 이용허락을 제안한 것이었고 당시 세계지적재산권기구(WIPO)에도 비슷한 내용의 초안이 올라갔다(Söderberg, 2007: 18). 이때부터 마이크로소프트사(M$로 줄임)는 강력한 소프트웨어 이용허락을 도입하며 IBM보다 우위에 서게 된다(19). 또 하나는 1982년에 AT&T가 반독점법 규제에서 해제되고 컴퓨터 사업에 진출할 수 있게 되면서 특별히 누구 것이라

고 할 것도 없이 공유돼온 유닉스의 소유권을 주장하고 나선 일이다. 1956년에 반독점법으로 AT&T가 한시적으로 컴퓨터 사업에 진입하지 못하게 되었고, 이는 유닉스가AT&T 내부에서 개발되었지만 수많은 사람들이 재작성하고 기능을 향상하며 혁신을 이루는데 중요한 조건이었다. 그런데 1982년에 AT&T가 그 규제에서 벗어나면서 자기 것을 다시 되찾겠다고 나선 것이다. 이는 저작권을 정당화되는 '저자'의 권리 보호라는 이데올로기와는 정반대로 기업이 하나의 생산물을 공동 저자들(프로그래머 공동체)로부터 빼앗을 수 있다는 것을 보여주었다(Söderberg, 2007: 18-9).[6]

자유소프트웨어운동은 이에 저항하면서 등장했다. 어떤 이념 하에 조직된 운동이 아니었다. 당시 연구소, 대학, 지역의 해커들은 자 신들이 만든 것을 빼앗긴 상실감을 느끼며 분노했다. MIT의 인공지능연구소에 있으면서 소프트웨어가 상업화, 상품화되는 과정을 지켜본 스톨만 역시 분노하였고 '마지막 해커'가 될 수밖에 없었다. 그는 1985년에 자유소프트웨어재단(Free Software Foundation)을 설립하고, 그누(Gnu is Not Unix, GNU)라는 자유 소프트웨어 프로그래밍 프로젝트를 통해 소스 코드에 대한 공중접근(public access)을 주창하며 소프트웨어 저작권 체제에 반대하고 나섰다(Söderberg, 2007: 19).

공동체 기반 생산의 성공

한글로는 명확하게 구분되지만 영어로는 자유소프트웨어(free software)에서의 자유(freedom)가 무료(free of charge)의 의미도 가지고 있기 때문에, 스톨만은 공짜 맥주(free beer)에서의 free가 아니라, 자유 언론(free speech)에서의 free라고 끊임없이 강조하면서 자유소프트웨어는 소프트웨어 이용자의 권리를 보장하기 위한 사회운동임을 천명한다. '그누-일반공중이용허락'(GNU - General Public License, GPL로 줄임) 하 에 배포되는 자유소프트웨어를 이용하는 사람은 네 가지 자유를 누린다: 이용자는 프로그램을 어떠한 목적으로도 실행할 권리가 있다. 프로그램이 어떻게 작동하는지 공부할 수 있다. 적합하다고 생각되는 대로 프로그램을 배포할 수 있다. 프로그램을 변경하고 수정된 판본을 배포할 자유가 있다. GPL이 프로그램의 소스 코드를 공개하는 것도 다른 이유가 아니라 이런 자유를 보장하기 위해서다. 코드에 접근할 수 있다는 것은 곧 "프로그램이 어떻게 작동하는지를 근본적으로 이해할 수 있는 능력, 그 작동방식을 변화시키면서 프로그램에 개입할 수 있는 능력"(Jordan 2009)에 대한 접근을 의미하기 때문이다. 또한 스톨만(Stallman 2009)

6 현재도 그렇다. 저작권법의 '업무상 창작'은 고용된 창작자의 모든 창작물이 이들을 고용한 기업에 귀속되도록 규정하고 있다. 이전까지는 기업이 기획하고 이를 위해 프로그래머를 고용한 것이 아니면 고용된 프로그래머더라도 자신이 작성한 프로그램의 저작권을 가질 수 있었는데, 이번에 개정된 저작권법은 컴퓨터프로그램보호법을 통합하고, 모든 고용된 프로그래머의 소프트웨어 작성물을 기업의 저작물로 귀속시켰다.

은 그 자유가 단지 개인 이용자의 자유가 아니라 공유하고 협업하는 사회적 연대를 위한 자유임을 강조한다. 사실, 창작자 혹은 프로그래머가 가장 적극적인 향유자이자 이용자이기 때문에 이용자의 자유를 보장한다는 것은 저작권에 전제된 생산자-소비자 분업 구조를 넘어서는 생산자-이용자의 공동 생산과 공유를 활성화시킨다는 의미를 갖는다.

1991년 헬싱키 대학의 리누스 토발즈(Linus Torvalds)가 개발한 그누(GNU)의 핵심 커널이 공개되고 공동 개발되면서 자유소프트웨어 개발 프로젝트들은 한층 활기를 띠었다. 인터넷을 통해 전 세계에 퍼져있는 프로그래머와 이용자들은 실시간으로 자료를 교환하며 이전의 해커공동체와는 다른 지구적인 공동체를 형성해 나갔다. 1998년 자유소프트웨어 공동체의 일부가 '오픈소스'라는 이름으로 분리되기 시작했다. 오픈소스는 자유소프트웨어가 공짜 소프트웨어로 오해받는 것을 피하기 위해 처음 제안되었고 점차 이용자의 자유보다는 보다 나은 소프트웨어 개발을 위한 방법에 초점을 뒀다(Stallman 2009). 오픈소스 주창자들과 지지자들은 기업들이 오픈소스소프트웨어 프로젝트에 투자할 수 있도록 뛰어다녔고 서서히 소프트웨어 산업에서 새로운 사업모델로 주목받았다. 자유/오픈소스 소프트웨어는 1990년대 후반 이후 성공 가도를 달려왔다. 물론, 일반 이용자들은 기술적 수행보다 시각적 인터페이스에 더 친근해져 그누/리눅스를 개인 컴퓨터의 운영체제로 쓰는 사람은 상대적으로 적다. 하지만, 시스템 관리와 같은 특별한 기능이 필요한 영역에서는 크게 성공해왔다. 예를 들어, 아파치(Apache) 웹서버 프로그램은 2001년 월드와이드웹(www로 줄임) 서버의 60% 이상을 차지했고(카스텔 2004: 30) 2006년에 70%의 시장 점유율을 기록했다. (1980년대 초반과 다르게) IBM은 자기가 만든 것을 포기하고 자유소프트웨어를 지원하기로 결정했다(Söderberg, 2007: 24).[7] 그 외에도 도메인네임을 IP숫자로 변환하는 BIND, 이메일 트래픽 관리하는 Sendmail 등이 있다(25). 그리고 우리의 일상적인 인터넷 방식이 된 www도 자유소프트웨어인 HTTP프로토콜, 하이퍼링크 등으로 가능한 것이다.

자본주의 해킹

정보는 저작권 없이는 어떠한 교환가치도 갖지 않는다. 하지만 정보는 저작권 없이도 사용가치를 갖는다. 교환가치를 당장 확보하지 않더라도 그 사용가치를 위해 생산하는 수많은 정보 생산자들이 있다(Kleiner 2007). 그 중에 일찍이 첨단기술 자본주의 사회 내부에서 선물경제를 부활시킨 자유소프트웨어 해커들이 있다. 자유소프트웨어 생산 방식의 가장 큰 특징은 소외된 노동 관계를

7 자본의 입장에서 보면, 자유/오픈소스 소프트웨어 해커공동체는 공짜 노동력을 얻을 수 있는 매력을 가진다. 실제 자유/오픈소스 소프트웨어를 사업모델로 하거나 가져다 쓰는 기업들은 내부의 생산(개발) 비용을 낮추는 한편, 컴퓨터 산업 전체의 임금과 노동조건에 대한 압박을 가하고 있다(Dafermos & Söderberg 2009: 55).

벗어나 집단적이고 개방적인 생산자-이용자 공동체에 기반을 둔 과정이라는 점이다(김영식 2006; Dafermos & Söderberg 2009: 54). 우선, 필요에 따라 생산한다. 자유소프트웨어 생산자들은 사람들이 필요하기 때문에 생산하지 시장에서 교환할 목적으로 생산하지 않는다. 교환가치를 갖지 않고, 즉 저작권을 무시하면서 혹은 그 체제의 외부에서 사용가치를 위해 생산한다. 둘째, 생산물에 대한 보편적 접근을 허용한다. 자유소프트웨어를 사용할 수 있는 권리는 공동체에 기여한 사람에게만 주어지는 것이 아니라 그것을 필요로 하는 사람 모두에게 주어진다. 셋째, 생산 관계가 비시장적인 공동체 관계로 된다. 자유소프트웨어 공동체는 시장 관계를 벗어나 있으면서도 전 세계적으로 자유로운 생산자들의 협동 노동을 이끌어 내며 끊임없이 발전해 왔다.

이와 같이 자유소프트웨어운동은 독점 소프트웨어의 지배적 시장구조에 맞서며, 더 나아가 자본주의의 임노동 관계에서 벗어나 새로운 정보 생산과 유통의 흐름을 만들어 왔다. 시 장 보상 구조나 기업의 위계구조, 정부의 규제 하에 제약되어 있었다면 만들어지지 못했을 PGP(pretty good privacy)와 같은 강한 암호화 프로그램, 익명의 또래간(p2p) 파일공유 네트워크, 아파치 서버, php 프로그래밍 언어, 리눅스, Sendmail, BIND, www(HTTP, HTML, URI) 등이 모두 가능했던 것이다(Dafermos & Söderberg 2009: 54-5).

한국에서는 최근까지 그누/리눅스 운영체제나 관련 응용 프로그램들을 한글화(지역화)하거나 이용방법을 문서화하는 이용자 공동체는 여기저기에서 형성돼 왔지만, 자체적으로 자유소프트웨어를 개발하는 공동체는 많지 않고 있더라도 개인 차원에서 국제 프로젝트에 참여하는 수준이다. 반면, 자유소프트웨어운동의 철학에 영향을 받아 1990년대 초중반 정보연대(SING) 등의 활동을 시작으로 현재의 정보공유연대 활동에 이르는 사회운동의 차원의 카피레프트운동이 있었다. 그런데 한국의 카피레프트운동은 해커공동체와 거의 아무런 관계를 형성하지 않은 채 시작되고 지속되었다. 해커윤리의 핵심인 정보의 자유와 권력의 해체, 곧 "디지털 정보 독점에 대한 저항과 자유로운 유통의 정신"(이광석 1998: 80)은 카피레프트운동의 원칙과 다름없는데, 윤여상(2001)이 "정보 운동으로서의 카피레프트는 정보 생산의 중요한 실천자인 해커들과 연관성을 가져야 했으나 ... 적극적인 실천자를 잃어버린 운동으로 전개되었고 모호한 상태에서 제대로 확산되지 못했다"고 지적하듯이, 한국의 카피레프트운동은 가장 적극적인 (잠재적) 실천 주체들과의 연계 없이 이론과 정책적인 실천에 집중해왔다.

해킹행동주의: 온라인 직접행동

해킹행동주의(hacktivism)라는 말은 죽은 소 숭배(Cult of the Dead Cow, cDc로 줄임)라는 해커 집단이 해커들의 사회운동 참여를 선언하며 만들었다. "정치사회적 목적을 이루기 위해 벌이는 다양한 온라인 활동 방식"을 말한다(최세진 2006: 74). 해킹행동주의는 크게 두 가지로 나눠볼 수 있다. cDc처럼 독점 소프트웨어 및 네트워크의 취약한 보안 문제들을 공개적으로 드러내고 국가의 인터넷 검열을 문제 삼으며 대안 프로그램을 배포하는 해킹행동주의는 정보의 자유로운 흐름과 표현의 자유를 우선에 둔다. 반면, 신자유주의 세계화 반대 투쟁과 대항 지구화운동의 맥락에서 행동주의 예술, 독립 미디어, 직접행동과 결합한 해킹행동주의는 사회정의와 연대에 초점을 두고 있다.

표현의 자유를 위한 해킹

cDc는 독점 소프트웨어 기업인 M$의 심각한 문제들을 가만 두고 볼 수 없었다. M$의 운영체제인 윈도(Window)의 보안 체계가 엉망이라 사용자들의 프라이버시가 심각하게 침해된다는 것을, 그리고 허술한 원격 작동이 어떻게 향상될 수 있는가를 보이기 위해 핵티비즈모(Hactivismo)라는 작업집단을 만들고 '백오리피스'(back orifice)를 개발했다. 전 세계 해커들의 축제인 데프콘3(Defcon3, 1998)에서 자유소프트웨어로 발표된 백오리피스를 이용하면, 컴퓨터 초보자라도 윈도95와 98을 설치한 어떤 컴퓨터든 무슨 내용을 작성하고 있는지 어떤 파일을 복사하고 있는지 훤히 알 수 있었다(Jordan 2002:130; 최세진 2006: 74-6). 1999년 3월에 한 대학생이 이 프로그램을 이용해 한국과학기술원 전산망의 개인용 컴퓨터 20~30대에 들어가 국산 인공위성 '우리별 3호'의 제원과 성능 임무 등에 관한 자료를 가져다 개인 홈페이지에 올린 일도 있었다(정보통신부 1999: 51).

핵티비즈모(hactivismo)는 또한, 데프콘7(2002)에서 인터넷 검열에 반대하며 삐까부띠(Peekaboty)라는 소프트웨어를 발표했다. 방화벽에 막혀 있는 사이트에 접속하기 위해 그렇지 않은 컴퓨터가 대신 전달해주는 삐까부띠 네트워크는 '분산된 협력적 프라이버시 네트워크'라고 할 수 있는데, 검열에 의해 접속이 차단된 웹페이지의 주소를 입력하면 그 내용을 자동으로 암호화해서 삐까부띠 네트워크상에 있는 검열이 미치지 않는 컴퓨터에 요청하고, 자동으로 그 웹페이지 내용을 암호화해 다시 검열 지역의 사용자에게 보내주는 식이다. 충분히 많은 사람들이 참여한다면 계속 그 링크들을 바꾸고 모두 익명으로 연결되기 때문에 한 국가의 네트워크 검열을 무력화시킬 수 있게 된다. 이용자 간의 연대로 검열의 벽을 뛰어넘는 방식인 셈이다(최세진 2006: 78; Jordan 2002:129). 이들은 세계인권선언에 따라 인터넷 검열에 반대하기 위해 이를 개발했다고 밝혔다(Jordan 2

002: 128).[8]

사회정의를 위한 해킹

정치적 해킹 행동은 멀게는 1970년대 반전운동과 결합한 프리킹에서 찾아볼 수 있지만 컴퓨터 네트워크를 놓고 이루어진 것은 1980년대 후반부터 부각되었다. 1989년 미 항공우주국(NASA)이 잠재적 핵폭탄으로 알려진 작은 핵원자로를 포함한 우주 탐사선을 발사하는 것에 항의해 호주의 한 해커가 미 항공우주국의 컴퓨터 네트워크에 자기 복제되는 'WANK' 벌레 프로그램(worm)을 심은 적이 있다(Jordan 2002: 119-200). 벌레 프로그램을 사용한 최초의 사이버 시위로 기록되고 있다(데닝 2005: 337). 또, 1998 년 봄 "JF"로 알려진 영국의 젊은 해커가 300여 개의 웹사이트에 접속해서 반핵을 주장하는 글귀와 이미지가 뜨도록 한 일이 있었다. 당시 이 사건은 가장 대규모의 정치적 해킹이었다. 사이트의 원래 내용을 정치적인 메시지로 뒤바꿔놓는 이런 해킹은 멕시코 정부 웹사이트를 목표대상으로 한 경우를 포함하여 1998년에 여러 곳들에서 활용하기 시작한 방식이었다. 영국, 호주, 인도, 중국 등에서 다양한 정치적 해킹 활동에 대한 보고서들이 나왔다(Wray 1999). 1998년은 해킹행동주의가 전면에 나선 해였다.

소규모 집단인 '전자교란극장'(Electronic Disturbance Theater)이 '전자 시민불복종' 차원에서 벌인 해킹 행동 역시 이 때 있었다. 1997년 말, 치아파스에서 45명의 선주민이 죽음을 당한 아크테알(Acteal) 학살 뉴스가 사빠띠스따 연대를 위 한 지구적 네트워크를 통해 순식간에 퍼져나갔다. 며칠 만에 전 세계 멕시코 대사관 앞에서의 항의 시위가 조직됐고 멕시코 정부 웹사이트에 해킹이 있었다(Wray 1999). 멕시코에서 벌어지는 학살과 투쟁에 대한 연대를 목적으로 전자교란극장은 '홍수넷'(Floodnet)을 개발하고, 1998년 9월 9일 오스트리아 린츠에서의 전자예술축제(Ars Electronica Festival)에서 "떼 지음 프로젝트"(swarm project)라는 이름의 전시를 통해 첫 시위를 벌였다. 멕시코 정부, 미국의 백악관과 국방성과 육군의 남미군사교육단(the School of the Americas), 프랑크푸르트 증권거래소 등을 목표 대상으로 한 가상 연좌시위였다(Jordan 2002: 121; 데닝 2005: 322). 예술 행위이자 온라인 시위인 이들의 해킹 행동에 이틀에 걸쳐 2만 명이 참여했고 한 때 1분당 60만 회의 접속 시도가 있었다.[9]

---

8 이와 비슷한 토르 프로젝트(tor project) 역시 인터넷 검열을 우회하기 위해 익명으로 인터넷을 이용할 수 있도록 하는 자유소프트웨어이다. 애초에는 익명 상태의 커뮤니케이션 시스템이 필요했던 미 해군의 프로젝트였던 것이 개발이 중단된 이후 해킹활동가들이 계속 개발한 것으로 현재 널리 활용되고 있다.

9 홍수넷(floodnet)을 통해 사용자의 브라우저가 자바 애플릿 소프트웨어를 내려 받으면 수초에 한 번씩 목표 사이트들에 자동으로 접속할 수 있게 된다. 더군다나 각 시위자가 목표가 된 서버의 에러 로그에 자동으로 변형된 메시지를 남길 수도 있었다. 예를 들어 브라우저가 대상 서버에서 '인권'이나 '민주주의'라는 파일을 찾도록 설정하면, 서버는 '인권이 이 서버에 존재하지 않습니다'(no human rights found on this

1999년 11월 말 미국 시애틀에서 세계무역기구(WTO로 줄임) 3차 각료회의에 반대하는 국제 시위와 연계한 전자히피집단(Electrohippies collective) 역시 홍수넷을 이용해 가상 연좌시위를 벌였다(데닝 2005: 327). 신자유주의 세계화 회합을 무산시키려는 거리의 행동들과 조화를 이루며 WTO 각국 각료들을 위한 정보 흐름을 차단하는 시도였다. 행동이 전개된 5일 동안 45만 여 개의 개인용 컴퓨터가 이 가상 행동에 참여하여 회의 기간 동안 WTO 네트워크는 상당한 속도 저하를 겪었고 두 번 멈추기도 했다(Jordan 2002: 122-3).

2000년에 우리나라에서도 이 같은 해킹 행동이 통신질서확립법 반대 운동, 여러 노조들의 파업투쟁, 그 해 말 '개혁과제 실현을 위한 사이버 공동행동'을 위해 계획되거나 실행되었다(문성준 2001: 7). 실제로 8월 26일 통신질서법안에 반대하는 네티즌들의 가상 연좌시위로 정보통신부 홈페이지가 10시간 동안 '서비스거부' 상태가 되었고, 사이버범죄수사대가 진보넷을 방문(?)하기도 했다. 당시 온라인 시위는 다수의 접속자가 같은 시간에 같은 웹페이지에 접속해 '새로고침'(reload)을 연속적으로 누르는 그야말로 '서비스거부 공격'이었다. 뒤집어 말하면, 당시까지만 해도 '서비스거부 공격'은 온라인 시위의 방법이었다.[10]

비폭력과 위반의 정치학

우리나라에서의 해킹행동주의는 소수의 해킹 공격보다는 다수가 참여하는 온라인 시위 형태를 띠어왔고 굵직한 사안들이 터져 나올 때마다 다양한 온라인 토론이 벌어지면서 때때로 거리의 대중행동으로 연결되는 경향이었다(최세진 2006: 81-2). 그런 만큼 큰 논란은 없었다. 그러나 전체적으로 보면, 목표 대상 사이트의 차단이 아니라 수많은 사람들이 공개적으로 상징적 저항 몸짓에 참여하는 것을 추구하면서 한 두 사람의 기술적 능력에 의존하는 것이 아니라 시위해야겠다고 결심한 수많은 사람들의 선택을 중시하는 전자 시민불복종 형태에서부터, 개별적으로 가능하고 감수해야 할 위험성이 높은 만큼 익명과 비밀로 이루어지는 정치적 해킹 행동까지 다양한 해킹행동주의가 나타났고 내외부의 논쟁도 거셌다. 독일의 한 해커가 '분산서비스거부 공격'이 가능하도록 홍수

server) 혹은 '민주주의가 이 서버에는 없습니다'(no democracy found on this server)가 화면에 나타나게 한 것이다(Jordan 2002: 121). 이를 개발한 스탈바움(Brett Stalbaum)은 홍수넷을 "활동적이고 예술적인 표현을 통해 사람들에게 힘을 주는 개념적 네트 예술"로 규정하고 있다(데닝 2005: 323). 이에 대해 미 국방성은 적대적 애플릿을 포함시켜 사용자 브라우저에 작은 창이 계속 열리도록 해 공격을 무력화시켰다(323).

10 당시 통신질서확립법 제48조(정보통신망 침해행위 등의 금지) 3항이 "누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하여서는 아니 된다"고 하고 이를 위반 시 "5년 이하의 징역 또는 5천만 원 이하의 벌금"에 처한다고 한 것도 항의의 대상이었다.

넷을 한층 개선한 '부족의 홍수넷'(Tribal Floodnet)을 발표했을 때 특히 그랬다.[11] 그 목적이 불법적인 것을 통한 사적인 이해의 달성에 있는 것이 아니라 정치적 개입이고 기존 질서의 위반이 수반될 때 그 결과로 불법이 될 수 있는 해킹행동주의는 합법과 불법의 구도를 넘는 위반의 정치에 대한 다각도의 토론이 필요한 쟁점이 되어왔다.

51명의 해킹활동가들과의 인터뷰 내용을 포함한 사무엘의 연구(Samuel 2004)는 "정치적 목적을 추구하기 위해 불법적이거나 법적으로 애매한 디지털 도구의 비폭력적 사용"으로 해킹행동주의를 정의하고 있다. 여기서 '비폭력'은 해킹행동주의가 사람에게 해를 끼치는 사이버 테러와 구분되는 지점이고, '불법적이거나 법적으로 애매한'이라는 말은 온라인 행동주의의 비-위반 형태들과 구분해 주며, '디지털 도구의 사용'은 비폭력적이고 위반하는 모든 형태의 디지털 행동을 명시적으로 포함한다는 것을 말한다(Samuel 2004: 3). 그래서 해킹행동주의는 (테러리즘과 같은 폭력이 아니라) 위반과 비폭력을 핵심으로 한다고 볼 수 있다. 그러나 해킹행동주의가 한창 부상했던 1990년대 후반에는 사이버범죄, 사이버테러, 네트워크전쟁과 같은 주류 담론이 이미 해킹에 대한 해석의 지평을 장악하고 있었다. 늘 체제에 대한 저항은 범죄나 테러의 이미지로 뒤덮여 왔는데, 더 나아가 해킹행동주의는 해킹이 범죄나 전쟁의 보조 수단으로 사용되는 것과 혼재됐기 때문에 더욱 그랬다.

해커 길들이기와 해킹의 범죄화, 군사화

여기서는 해킹을 이용한 범죄의 규모나 현황 등을 다루지는 않는다. 해킹을 폭력이나 군사적 목적으로 활용하는 사이버테러나 사이버전쟁의 구체적인 내용도 없다. 오히려, 이런 것들이 어떤 역사적 배경에서 생겨났는지에 초점을 맞춘다. 해킹 및 해커를 일탈문화나 범죄자로 보는 것은 실제로 존재하는 사회 현상이기 때문에 자연스러워 보이지만, 그 현상의 이면에서 작동하고 있는 해킹에 대한 정치 권력의 통제나 왜곡된 재현이 갖는 역사적인 맥락과 그 문화정치적 효과를 드러낼 필요가 있다.

컴퓨터 범죄의 재구성

11 '부족의 홍수넷'은 2000년 2월 야후와 주요 미국 사이트들을 폐쇄시키는 데 사용되었고(아퀼라 & 론펠트 2005: 417), 온라인 직접행동 전술로 등장한 (분산)서비스공격은 이후 정치 없이 기술만 남게 되었다.

해킹은 저항으로 시작되었고 대안 생산방식이나 정치적 직접행동 형태로 발전해왔다. 무엇보다도 해킹은 기술과 정보의 사유화에 저항하는 것이었지만, 그렇지 않았던 비물질적인 정보, 지식, 문화생산물들이 법의 보호를 받는 사유 재산으로 종획되면서 해킹은 점차 사유 재산에 '침입'하거나 '절도'하는 행위로 받아들여졌다.[12] 해킹을 활용한 범죄의 여타 규정은 현행 법체계 하에서 판단하는 것이지만, 해킹 행위 자체의 정치적 속성은 그 법체계가 바탕을 두고 있는 정보, 지식, 문화생산물에 대한 인위적 소유관계의 설정이라는 사회 체제의 문제를 건드리고 있다. 이는 실제 해킹을 통한 사이버범죄가 빈번해지기 이전부터 해킹을 범죄시했던 역사적 과정을 통해 잘 드러난다. 지금 우리가 알고 있는 뭔가 불법적이고 위협적인 해킹의 의미와는 달랐던 초기의 해킹과 해커문화가 어떠한 계기들과 조건 속에서 범죄의 이미지로 뒤덮였는가.

최초의 정치적 해커 공동체의 출현은 미국에서의 반전운동과 히피문화를 배경으로 1970년대에 널리 유행한 전화에 대한 해킹, 프리킹(phreaking)에서 찾을 수 있다(Söderberg, 2007: 16). 프리킹은 전화 교환 장치에 사용되는 컴퓨터 시스템의 허점을 뚫고 들어가 무료로 전화를 사용하거나 전화 시스템에 침입하는 행위를 말한다. 당시 AT&T는 통신시장을 독점하며 횡포를 부렸고 정부의 전화 도청을 도우며 국민 사찰 행각을 벌였다. 그에 더해 미국 정부는 베트남전쟁 비용을 마련한다고 전화 서비스에 연방 누진세를 부과했다. 사람들의 격렬한 항의와 전화세 납부거부운동의 일환으로 프리커들은 공짜 전화걸기 캠페인을 전개했다(김강호 1997: 17). 히피 아나키즘 운동을 배경으로 발행된 프리킹 잡지, '국제청년파티라인'(Youth International Party Line, YIPL - 이플로 줄임)은 프리킹 기술을 대중화하는데 결정적인 역할을 했다(31). 그러나 컴퓨터 시스템에 접속하기 위한 모뎀 사용료를 절감하는 차원에서도 프리킹이 유행했고, 이에 필요한 정보와 기술 그리고 프리킹의 정치적 의미들을 교환하며 프리커들은 1970년대에서 1980년대 초반까지 주요한 전자 지하세계를 형성했다. 그와 동시에 1980년대 컴퓨터 네트워크가 점차 대중화되면서 범죄를 목적으로 한 해킹 정보가 널리 퍼졌다. 일부 프리커와 해커는 도둑질하는 법을 배웠고 일부 도둑들은 프리킹이나 해킹하는 방법을 배웠는데, 전화나 통신 도둑의 숫자는 점차 지적인 도전과 탐구에 매달린 프리커와 해커의 숫자를 압도해갔다(스털링 1993: 63-4).

1980년대 초반 컴퓨터 네트워크의 확산은 개인용 컴퓨터의 보급과 함께 이뤄졌다. 애플 컴퓨터의

12 해킹에 범죄 용어들이 유비되는 것은 직관적인 이해에 효율적인데 바로 그렇기 때문에 심각한 오해나 보다 근본적인 질문을 제약하는 문제를 안고 있다. 로스(Ross 1990)가 볼 때, 해킹을 다른 사람의 집에 무단으로 침입하는 일처럼 묘사하는 것은 "사생활보호, 재산, 소유적 개인주의, 국가의 과잉 감시 등"에 대한 논쟁에 재갈을 물리는 효과를 낳는다. 대부분의 해커들이 거의 집중적인 '목표 대상'으로 삼고 있는 정보기술의 독점적 제도 기구나 기업 소유자들의 불법적 활동에 대한 조사도 없다.

성공은 개인용 컴퓨터의 시장성을 검증하며 컴퓨터 산업을 지배하고 있던 IBM을 긴장하게 했다. 위협을 느낀 IBM도 서둘러 중앙처리장치, 기억장치, 저장장치, 운영체제, 응용프로그램이 어설프게 갖춰진 개인용 컴퓨터(PC)를 개발해 1981년에 내놨다.[13] 개인용 컴퓨터를 통해 증대하는 컴퓨팅의 편재성과 가시성은 주류 대중문화에서 두드러졌는데, 비디오 게임과 컴퓨터 게임은 많은 사람들에게 새로운 시각 미디어로서의 컴퓨터에 대한 최초의 경험을 제공했고(기어 2006: 245), 새로운 문화적 욕구로 충만한 신세대에게 개인용 컴퓨터가 갖는 최초의 쓸모는 게임이었다.[14] 10대들은 새로운 게임을 구하기 위해 불법 복제된 혹은 무료로 배포된 게임을 찾으며 전자게시판을 돌아다니다가 해킹을 접하게 되었다. 프리커와 해커들이 살다시피 한 디지털 지하세계인 전자게시판에는 전화번호 탐색 프로그램, 신용카드 회사에 침입하는 프로그램, 불법복제 소프트웨어, 암호해독, 파란상자(bluebox, 장거리 전화를 공짜로 거는 장치) 회로도, 침입 설명서 등이 퍼져있었다(스털링 1993: 89-92). 1982년 전후로 복제방지장치가 풀린 '아타리 800'이나 '코모도 C64'와 같은 게임을 유통시키는 최초의 소프트웨어 해적 게시판이 나타났고 10대들은 여지없이 이 게시판들을 드나들었다. 개인용 컴퓨터의 보급, 컴퓨터 게임의 확산, 전자 게시판의 성행은 1980년대 초반 이후 컴퓨터 해킹이 프리킹만큼 많아진 조건이었다.

1983년, 해커가 주인공으로 나오는 할리우드 괴기물, '전쟁게임'(Wargames)의 개봉과 흥행은 어린이들과 10대들이 해킹에 특별한 관심을 갖는데 한몫했다. 영화는 불법으로 게임을 얻기 위해 컴퓨터에 침입한 10대들이 핵전쟁까지 일으킬 뻔 한다는 얘기로 해커가 분명 말썽을 일으키는 컴퓨터 침입자라는 이미지를 굳히는데 크게 기여했다.[15] 같은 해, 10대들이 주로 들락거리던 '414 프라이빗'이라는 사설 전자게시판에서 모인 6명의 해커집단, '414 갱들'(414 Gangs)이 의료 및 군사시설을 포함해 60여 대의 컴퓨터에 9일 간 '침입'한 일로 결국 경찰에 체포된 일이 있었다(스털링 1993: 102). 이때 미디어 보도 또한 여지없이 위험한 불법 컴퓨터 침입자를 해커라 이름 붙였다. 1

13 IBM은 전쟁과 공동체 통제 수단으로 컴퓨터를 개발하는 회사로 표상되며 1960년대 내내 대중적 지지를 잃어갔고, 베트남 전쟁에서도 컴퓨터가 사용된 사실은 많은 사람들에게 비난을 산 일이었다. 그러나 기술을 통한 사회 해방을 주창한 반문화의 일부 담론은 사람들이 나의 능력을 십분 발휘하기 위한 유용한 도구이자 소유할 만한 것으로 개인용 컴퓨터를 받아들이는 것을 도왔고(기어 2006: 171), 무엇보다도 개인용 컴퓨터는 후가산업사회 담론과 신자유주의 구조조정을 겪고 있던 현실 변화에도 잘 어울리는 기술이었다(157). 신자유주의는 점차 컴퓨터의 비범한 능력, 특히 서로 연결된 복잡한 시장들의 관리를 가능하게 하는 네트워킹 능력에 주목했고, 반문화의 한 특징이었던 쾌락주의는 소비자의 자기 권리에 대한 신자유주의적 호소와도 맞아떨어진 것이다(192-3).

14 비디오 게임과 컴퓨터 게임의 성황에 위협을 느낀 디즈니사는 3차원 컴퓨터 그래픽을 영화에 최초로 사용하며 컴퓨터 안에서 사건들이 발생하는 '트론'(Tron, 1982)을 제작하기도 했으나 흥행에 성공하지는 못했다. '트론'은 히피이자 반권위주의적 프로그래밍 해커를 등장시킨 최초의 영화이기도 했다(기어 2006: 248-50).

15 '위장접근수단, 컴퓨터사기 및 컴퓨터남용법'(the Counterfeit Access Device and Computer Fraud and Abuse Law)은 1984년에 제정되고 1986년에 개정되었는데, 이 과정에서 '전쟁게임'에 나온 해킹과 해커가 거론되기까지 하면서 이런 범죄를 막기 위해 법이 통과돼야 한다는 주장이 정당화됐다(Ryan 2004: 9). 그러나 이 법으로 유죄 판결이 내려진 적은 한 번도 없었다(스털링 1993: 125).

989년 독일의 해커들이 미국 국방망을 침입하여 군사기밀을 소련으로 넘겼다고 알려진 일명 '카오스사건'이 전 세계 신문과 방송을 통해 알려지면서 해킹은 자유세계를 위협하는 가공할 행위로 비춰지기까지 했다.

위와 같은 일련의 사건들이 위치한 시대적 맥락으로 각도를 달리해 보자. 정보통신기술의 하부구조가 경제 활성화를 위해 재인식되고 컴퓨터, 인터넷, 이들을 위한 소프트웨어가 더 이상 공동 생산과 공유의 산물이 아니라 팔아야할 상품으로 변모해 가고, 그 교환가치를 보존하기 위해 해킹과 같은 자율적 기술 접근과 이용은 통제되어야 했다. 냉전시대와 대량소비사회 속에서 정치적 정보와 상업적 시장에 대한 대중 통제는 그 희생물을 해킹에서 찾은 것이다. 해킹과 해커문화가 거대 통신자본과 신흥 정보산업 자본의 이해를 반영한 국가의 사법적 통치 대상으로 확립된 것은 미국에서 1988년의 컴퓨터 바이러스 사태와 1990년의 전국적 해킹 단속 사건을 통해서였다.

컴퓨터 바이러스 공포, 해커와의 전쟁

1960년대 벨연구소, 제록스의 팔로알토연구센터(Palo Alto Research Center, PARC), MIT와 같은 곳의 컴퓨터 연구자들은 '코어 전쟁'(Core War)을 하며 놀았다. 각자 만든 자기복제 프로그램들을 시스템에 배포해 누가 시스템 자원을 가장 많이 차지하느냐로 승부를 겨루는 게임이었다. 지금으로 치면 '벌레 프로그램'(worm)을 만들어 서로 프로그래밍 실력을 겨룬 것인데, 누가 가장 짧은 자기복제 프로그램을 짜느냐도 중요했다. 프로그래밍 게임은 곧 탐구, 창조, 혁신의 과정이었다(Galloway 2005: 25). 1988년부터 이런 일을 저지르면 창조가 아니라 파괴 행위가 되었다. 1988년 11월 2일과 3일, 미국 코넬대에 재학하고 있던 해커이자 국가안보위원회 핵심 과학자의 아들이었던 로버트 모리스는 인터넷의 전신인 아르파넷(ARPANET)에 벌레를 하나 배포했다. 그는 해를 끼치는 일 없이 인터넷을 탐험하도록 벌레 프로그램(worm)을 정교하게 만들었다고 했지만, 오류를 일으키는 바람에 무한정 복제되어 약 6천 대의 컴퓨터를 감염시키고 정부 기관과 대학들의 시스템을 마비시켰다(스털링 1993: 104). 최초의 대규모 컴퓨터 바이러스 사건이었다. 이 사건 이후 한편으로, 규모는 훨씬 작지만 이와 유사한 인터넷 해킹이 디지털 지하세계 엘리트들의 표준이 되었다(104). 다른 한편, 실제 데이터 피해가 크지 않았음에도 일상의 컴퓨터문화를 변형시키고만 컴퓨터 바이러스 공포 분위기가 뒤따랐다. 당시 주류 미디어는 컴퓨터 바이러스에 대해 에이즈 공포와 비교하며 히스테리 증상을 보였고, 미 국방성은 그 해 11월 카네기멜론대학에 컴퓨터비상대응팀(Computer Emergency Response Team, CERT)을 설립하는 등 바이러스 통제 센터들이 속속 생겨났으며, 이런 행위에 최대 10년 징역으로 처벌한다는 골자의 새로운 법안의 제정이 이어졌다

(Ross 1990). 더 나아가 이 사건은 미국뿐만 아니라 세계 각국의 기업과 정부, 연구기관이 본격적으로 보안 문제에 관심을 가지게 된 계기였는데(김강호 1997: 81), 이와 같은 잠재적 위협으로부터 기술 및 정보 상품을 보호할 필요성과 네트워크 보안 사업을 통한 이윤 창출의 가능성이 공명했기 때문이었다.

당시 컴퓨터 바이러스 공포가 결과적으로 새로운 법제화와 연방수사국(FBI로 줄임)의 수사권 강화에 대한 대중의 동의를 이끌어내는 편리한 알리바이로 기능했다면(Ross 1990), 1990년 '해커와의 전쟁'은 실전에 들어간 것이었다. 1990년 봄 '선데블 작전'(Sundevil operation)으로 불린 해커 일제 단속이 벌어졌는데, 이는 컴퓨터 통신 세계 혹은 가상 공간에 대한 최초의 사법적 권력의 직접적인 행사였다. 미국시크릿서비스, 전화회사의 보안부서, 주와 지역의 법률 집행 집단이 미국 14개 도시에서 체포, 형사 책임 공방, 재판, 몇 건의 유죄 판결, 그리고 데이터와 장비에 대한 대대적인 압수 등을 조직적으로 벌인 일이었다(스털링 1993: 11). 전례 없는 해커 일제 단속은 전자 범죄, 처벌, 표현의 자유, 수색과 압수의 문제 등에 대한 격렬한 논쟁을 불러왔고 이 사건을 계기로 가상 공간에서의 시민의 자유를 확립하고 보호하는데 앞장선 '전자개척재단'(Electronic Frontier Foundation, EFF)이 만들어졌다(11).[16] 1990년 해커 일제 단속을 위한 선데블 작전은 정치를 가상 공간 속으로 초대한 사건이었던 셈이다.

이제 모든 해킹은 싸잡아 범죄화 되었다. 1990년대 초반 스털링(1993)의 관찰에 따르면, 컴퓨터 사기 범죄와 도용에 대한 거의 모든 법률가들과 경찰들은 컴퓨터를 도구로 사용하거나 컴퓨터에서 행해지는 거의 모든 범죄를 해킹으로 표현했다. 심지어 해킹을 수단삼아 컴퓨터 범죄를 저지른 혐의자들은 스스로를 컴퓨터 침입자나 파괴자 따위가 아니라 '해커'로 불렀다는 것이다(72). 공권력의 동원과 사법적 통제의 강화, 그와 관련된 일련의 사건들, 그리고 미디어의 과장되거나 왜곡된 재현은 보다 근본적인 차원에서 "새로운 정보 기술들이 지적 재산의 사유화와 부조화를 이룬 탓에 근대 권력이 집행되고 유지되는 방식을 변형시켜 재산법을 다시 쓰는 시도들의 중심"(Ross 1990)을 구성했던 것이다.

사이버테러, 사이버전쟁의 압도

기술과 정보의 사유화, 지식 재산권의 강화가 사법 제도의 꼴을 갖추는 1990년대 초반은 또한 세계적인 군사정치적 구도가 재편되는 시기였고, 이 또한 해킹에 새로운 의미를 부과하는데 기여했다. 소련의 해체와 미국의 이라크 침공(걸프전)을 겪으면서 냉전 수사가 더 이상 무용해지자 미국

16 얼마 전 프랑스에서 저작권 위반에 대한 인터넷 '삼진아웃제'가 위헌으로 판결나는 과정에서도 전자개척재단의 개입과 노력이 컸다.

군사-정보 공동체와 금융-기업 부문은 새로운 군사 교의를 창안해야 했다(Wray 1999). 그 때 '정보 전쟁'(Information Warfare), 사이버전쟁, 사이버테러 같은 말들이 생겨났다. 이런 용어들은 실재보다 큰 담론의 효과를 냈다.

사이버 테러리즘 혹은 사이버테러라는 말은 1980년대 캘리포니아 안보정보연구소(Institute for Security and Intelligence)의 배리 콜린(Barry Collin)이 "사이버공간과 테러리즘의 융합 현상"을 가리키기 위해 만든 용어였다.[17] 그리고 FBI의 특수요원 마크 폴릿(Mark Pollitt)이 더 실무적인 정의를 내렸는데, "사이버 테러리즘이란 정보, 컴퓨터 시스템, 컴퓨터 프로그램, 데이터 등에 대해 정치적 동기를 가지고 미리 계획된 공격으로, 국가 하위 조직이나 비밀 요원에 의해 실행되며, 비전투적 대상에 대한 폭력이다."[18] 그런데, 한 가지 주의할 것은 사이버테러는 이 정의대로 실제로 발생한 적이 거의 없다는 점이다. 데닝에 따르면, 그가 글을 썼을 당시(1999)까지 사이버테러의 범주에 들어갈 만한 일이 발생하지 않았다.[19] 그 이후로도 위의 정의대로 사이버테러가 발생한 적이 없는 것 같다. 수많은 네트워크 해커나 '분산서비스거부 공격' 도구를 구해 악의적으로 이용해본 모든 이들을 테러리스트로 보지 않는다면 말이다.[20] 반면, 그 가능성을 대비하자는 차원의 군사-안보 논리 강화의 담론 효과는 더욱 커져왔다.

사이버전쟁의 경우 1990년대 초, 미국의 보수주의 성향의 비영리 국가정책 연구소인 '란드연구소'(RAND Corporation)는 정보전쟁에 대한 이론적 작업[21]을 꾸준히 해왔다. 이들은 또한 사이버전쟁과 비슷하면서도 시민사회 영역에서 나타나는 '사이버갈등'을 가리키기 위해 '네트워크전쟁'(Netwar)이라는 개념을 만들었다. 이는 "네트워크 형태의 조직과 정보 시대에 걸맞은 관련 교리, 전략, 기술 등을 활용하는 사회적 갈등(또는 범죄)의 새로운 형태"(아퀼라 & 론펠트 2005: 48)로서 전통적 군사행동과는 달리 무력과 직접적으로 연관되지는 않은 것으로 정의된다. 이들이 이론적으로 선취한(연역한) 네트워크전쟁은 얼마 안 있어 실제로 그렇게 부를 만한 것이 나타났다. 그들은 멕시코 사빠띠스따 민족해방군의 무장봉기와 인터넷을 통한 국제연대 공동체의 활동을 네트워크전쟁으로 분석했다(론펠트 & 아퀼라 2005: 6장 "사파티스타 사회적 네트워의 출현과 그 영향"). 이들은 인종 민족주의자, 테러리스트, 게릴라, 범죄자, 사회운동가 등을 모두 동등하게 취급

17 Barry Collin, “The Future of Cyberterrorism,” Crime and Justice International, March 1997, pp.15-8(데닝 2005: 340에서 재인용)

18 Mark M. Pollitt, “Cyberterrorism: Fact or Fancy?” Proceedings of the 20th National Information Systems Security Conference, October 1997, pp 285-9(데닝 2005: 340에서 재인용).

19 1998년 스리랑카의 타밀 반군 게릴라 소속의 자칭 '인터넷 블랙타이거(Internet Black Tiger)'가 전자우편 수천 통(2주 동안 하루에 약 800통)으로 스리랑카의 대사관 사이트를 뒤덮어 버린 적이 있는데, 미국의 정보 당국이 한 국가의 컴퓨터 시스템에 대한 최초의 공개적 테러 공격이었다고 평가한 적은 있다(341).

20 사이버테러대응센터를 운영하는 경찰청은 사이버테러'형'범죄를 규정하면서 거의 그렇게 보고 있다.

21 대표적으로 John Arquilla and David Ronfeldt, "Cyberwar is Coming!," Comparative Strategy 12. April-June 1993.

하려는 것이 아니며 시민사회에 긍정적인 영향을 끼치는 사회운동을 폄하하려는 것은 아니라고 하지만(48), 이런 유의 정보전쟁에 대한 대부분의 자료들은 국방대학, 국방부, 미 공군, 혹은 기업들에서 만들어져 왔고 "디지털 재산을 지키기 위해 혈안이 된 자들과 네트워크 보안 기업들에 의해 확산되었다"(Wray 1999). 해리 클리버 등이 급진적인 풀뿌리 관점에서 지배적 정보전쟁 담론을 비판적으로 재구성하려는 작업[22]을 진행했지만, 해킹행동주의나 온라인 직접행동이 그렇게 함몰돼 가는 것을 막기에는 역부족이었다.

1999년 북대서양조약기구(NATO, 나토로 줄임)와 미국의 유고 공습 사태는 '최초의 인터넷 전쟁' 혹은 '사이버전쟁'으로 명명된다. 인터넷이 전쟁에 적극 활용되었고 그에 따라 다양한 해킹 사례들이 등장했다(데닝 2005; 히매넌 2002: 136-8). 분쟁과 폭격의 한가운데에 있는 주민들과 전 세계의 반전평화 활동가들은 나토와 미국의 공격으로 초래된 전쟁의 참상을 인터넷을 통해 전 세계에 알렸는데, 인터넷은 정보 전달 수단으로만 사용된 것이 아니었다. 수많은 사람들이 다른 미디어에서 접할 수 없는 글과 사진, 비디오를 교환하며 이 사태에 대해 직접 토론했다(데닝 2005: 294). 또, 유고 공습이 진행되는 동안 나토와 미국의 주요 기관들의 홈페이지가 훼손되는 사건들이 많았다. 이들 중에는 세르비아의 해커들뿐만 아니라, 나토와 미국의 공습에 반대하는 유럽과 미국 내 반전 해커들도 많았다(윤여상 2001). 물론 해킹은 공습과 학살을 중단하는데 영향을 미치지 못했다. 그러나 유고 전쟁을 계기로 전 세계의 미디어는 사이버전쟁에 대한 대비를 촉구하느라 여념이 없었다.

해킹문화운동: 지배 기술문화의 근본 독점 깨기

'컴맹'은 생산된다

지난 반세기동안 디지털과 네트워크 기술은 산업혁명 시기 과학기술의 발전과 마찬가지로 자본의 운동을 심화시키는 주요한 기반이 되었다. 현재의 정보 자본주의 사회 혹은 신자유주의가 지배하는 사회는 디지털 네트워크 기술을 그 핵심적인 사회운영 원리로 배치했다.[23] 노동의 불안정화, 삶

22 Harry Cleaver. "The Zapatistas and The Electronic Fabric of Struggle." 1995. http://www.eco.utexas.edu/faculty/Cleaver/zaps.html 등

23 신자유주의는 어떻게 모든 인간 행동을 시장 영역으로 끌고 들어갈 수 있는가? 하비(2007)는 시장 거래의 밀도 증가의 문제를 시공간의 압축을 통해 해결해 왔고 그 압축은 정보통신기술을 발전시키며 가능했다고 본다(17). 즉, "세계시장에서 의사결정을 유도하는 거대한 데이터베이스를 누적·저장·이전·분석·사

전체에 대한 수탈과 착취, 자연과 생명 그리고 정보와 지식의 독점 체제가 심화되어 온 것에 디지털과 네트워크 기술이 큰 몫을 해온 것이다. 특히, 생산수단 통제의 지배 형식은 재산의 직접 소유에서 임대로 이동해 왔다. 공동체의 사용가치 생산과 자율적인 공유문화를 착취하는 일은 새로운 기술과 미디어로 더욱 능란해졌고, 재산(생산수단)의 소유와 이윤 창출이 물질적 그리고 비물질적인 생산물에 대한 접근을 막거나 통제하면서 가능하게 된 것은 첨단기술이 보장했다. 그에 따라 상표권, 문서나 미디어 포맷과 하드웨어에 대한 특허, 복제방지 기술, 문화생산물에 대한 저작권 강화의 지적재산권 체제가 인위적인 희소성을 조장하며 작동하고 있다. 디지털과 네트워크 기술에 기초한 생산력의 발전에 기대면서도 그에 족쇄를 채우고 있는 것이다.

현재의 대규모 저작권 위반은 불법복제로 돈벌이를 하는 차원에서 수많은 이용자들의 비용 감소 차원으로 이동해왔다. 이제 너무도 많은 사람들이 스스로 알든 모르든 저작권법을 위반한 범법자가 되고 있고 이를 훈육하고 동시에 감시하기 위해 전 방위적인 통제 시스템이 첨단기술로 무장한 지적재산권법제 하에 갖춰져 왔다. 해커들이 '디지털제약관리'(Digital Restriction Management)로 고쳐 부르고 있는 디지털권리관리(DRM)는 개 중의 하나다. 또한, 자 본의 사유 재산 체제를 뒷받침하는 기술 적용 방식은 최소 기술 이용자에 맞춰지고 있다. 이른바 역설적인 표현에 다름 아닌, 이용자 친화적 기술(user-friendly technology)이 그것이다(Söderberg 2002). 앞서 해커에 대한 대대적인 단속은 지배적인 시스템에 대한 보안을 확보하는데 있어서 전문 기술자의 개입을 막는 차원이었지만, 그 효과로서, 그리고 보다 더 큰 지배적 시스템의 감시와 통제를 확보하려는 움직임은 평균 이용자들의 기술력을 저하시키는 차원에서 이뤄지고 있다. 우 리는 부지불식간에 기술에는 바보가 돼가고 점차 스스로 해결하는 능력과 협력의 문화를 저버리고 있다. 그렇다면 사람들이 서로 상호작용하며 공유하는 장치들과 방식들을 계속 재사용하고 재창조할 수 있는 권리를 빼앗는(Kranenburg 2008: 33) 이런 배타적 기술지배와 법제도가 오히려 더 거대한 (사이버)범죄이자 문화적 강탈이 아닐까.

그런데 이 모든 것들이 점차 실체를 드러내기 시작할 즈음, 해커들은 네트워크사회를 위한 전자 기술에 알을 깐 첫 사회운동을 구성해 왔고, 그들의 독립적이고 자율적인 기술 장인의 면모는 새로운 정치적 운동 주체로 포착되기도 했다(Riemens 2003). 인위적인 희소성을 폭력적으로 창출해 내는 지적재산의 생산 관계에 대해 이미 1980년대 자유소프트웨어운동이 그 저항의 물꼬를 트며 대안적 생산-분배 방식과 생산 관계를 형성해왔고, 전자 커뮤니케이션 네트워크와 소프트웨어 산업의 독점에 반대하고 신자유주의 세계화에 저항하는 운동의 맥락에서 지배적 네트워크 시스템에 대한 교란과 위법적 개입의 정치적 기술운동도 계속돼왔다. 해커들을 싸잡아 사이버범죄자로 내몰아왔던 것도 그런 맥락이 컸다. 해킹의 정치는 바로 여기에 있다. 해킹 및 해커문화는 기술문화 전체

용할 수 있는 정보 창출 기술과 정보 처리 역량"(17)을 갖는 정보기술의 발전은 신자유주의와 보조를 맞춰왔다.

에서 인위적인 희소성의 논리와 산업 제도의 독점 구조를 깨고 대안을 만들 수 있는 풍부한 잠재력을 품고 있다.

근본 독점 깨기

해킹문화운동을 제안한다. 해킹행동주의가 정치사회운동과 해킹이 결합하여 전자적 공공영역에 직접행동을 도입하며 항의의 메시지를 띄우거나 상징적인 점거 시위를 하는 형태였다면, 해킹문화운동은 해킹을 현재의 자본주의 문화 전반에 적용하면서 지배적 기술문화를 교란하고 이미 몸에 밴 이용자 친화적 기술 환경이 정작 우리를 기술의 노예로 만든다는 것을 문제 삼으면서 대안적인 기술문화를 만들어나가는 문화운동으로 확장하자는 차원이다. 한마로 해킹문화운동은 우리 사회의 지배적인 기술문화의 근본 독점을 깨기 위한 것이다. '근본 독점'(radical monopoly)이라는 개념은 이반 일리히(Ivan Illich)가 제시했다. "일반적으로 '독점'하면 하나의 기업이 생산수단이나 상품 또는 서비스를 배타적으로 통제하는 것"(일리히 2004: 90)을 뜻하는 반면 근본 독점은 "하나의 브랜드가 지배하는 상태가 아닌, 한 가지 유형의 생산물이 지배하는 상태이다. 근본적인 독점은 산업생산의 과정이 절실한 필요의 충족에 대한 배타적인 통제를 행사하며 비산업적인 활동을 경쟁에서 축출하는 상태"(91)이다. 우리가 우리 자신과 공동체를 위해 스스로 발휘할 수 있는 타고난 능력을 포기할 때, 그리고 알지도 못한 채 규격화된 도구에 의해 제공되는 뭔가 더 나아보이는 것을 얻으려 할 때 근본 독점이 구축된다(94). 기술은 과학기술자들의 연구소나 첨단장비들이 갖춰진 공장에서 따로 발전하고 있는 게 아니다. (이번에 서비스거부 사태를 겪은 사이트들만 보더라도) 정치, 경제, 금융, 문화, 언론을 포함한 사회 제도 및 공공 영역, 그리고 사적 영역 모두를 컴퓨터와 네트워크가 매개하고 있는 현실을 놓고 볼 때, 지배적 사회제도들이 구축한 근본 독점은 곧 우리의 일상 생활문화를 통해 견고하게 굳어져왔다.

그래서 해킹을 통한 문화운동 혹은 기술문화에 대한 해킹으로서 해킹문화운동은 전자 커뮤니케이션 네트워크와 소프트웨어 영역으로 제한되지 않는 문화 전체에서 인위적인 희소성의 논리와 산업제도에 의존하게 만드는 근본 독점을 깨고 대안을 만들어나가는 일상의 저항 문화운동이다. 이미 해킹은 문화생산 영역 - 문화 콘텐츠(음악, 영화, 게임 등), 또래 간(p2p) 생산, 오픈소스 프로젝트 등으로 확장되어 왔다. 자율적인 기술 개발과 공유의 과정이 소프트웨어 영역만이 아니라 다양한 대중 문화생산 과정에도 폭넓게 적용될 수 있고 또 그렇게 되는 것은 오히려 자연스러운 흐름이다. 현재 전 세계의 다양한 해커공동체들과 해킹활동가들은 컴퓨터 네트워크 해킹 못지않게 하드웨어나 전자제품, 의식주와 관련한 다양한 생산물들에 대한 해킹을 하고 있기도 하다. 그야말로 문화해

킹을 통한 해커문화의 확산이다. 자본주의를 넘는 문화운동으로서 '스스로해결하기'(do it yourself, DIY로 줄임) 문화이다. 해킹과 해킹문화는 일상생활에서 자본주의를 넘어설 수 있는 DIY 문화이고, DIY 문화는 자본주의를 해킹하고 있다. 일리히가 가치의 산업적 제도화로서 근본 독점을 비판하면서 "무엇보다 개인적인 방식으로 개인적인 필요를 충족하는 능력을 박탈함으로써 근본적 독점은 – 제도적 서비스에 반대되는 의미의 – 개인적인 서비스를 근본적으로 희소하게 만들어버린다"(일리히 2004: 94)고 할 때, 해킹문화와 DIY 문화는 (그 주체들이 의식하든 의식하지 않든) 바로 자본주의 체제의 근본 독점을 극복하기 위한 공동체의 정치 투쟁이다.

그와 같이 해킹문화운동은 결코 소수 전문가 해커들에 의한 것이 아니라, DIY 문화가 그렇듯이 대중 문화(운동)로 접근하는 것이 필수적이다. 다시 일리히의 말로 하자면, 일반적인 독점은 독점하는 소수 기업이 문제이지만, 근본 독점은 대중의 문제이기 때문이다. "근본 독점은 대중에 의해 탄생되었다. 따라서 대중이 이 독점을 유지하는 비용을 계속 대지 않기로 결정하여 독점을 끝내는 대가를 지불하는 것이 더 낫다는 점을 깨달을 때만 근본적 독점은 깨진다"(96). 해킹은 그 어떤 문화현상 못지않게 저항의 정치에서부터 범죄와 전쟁의 수단에 이르기까지 다양한 영역의 문화정치적 함의를 가져왔다. 저항이든 범죄든 해킹은 기술과 문화의 근본 독점을 통한 이윤 창출과 지배를 위해서 법으로 금지된 지식이 되어야 했다. 다시 말해서, 해킹은 근본 독점, 금지된 지식, 우리의 필요나 욕구가 교차하는 문화 투쟁의 격전장이다. 그러니 현행법과 각종 지배 담론이 해킹의 불법성, 시스템 불안정화, 테러의 공포를 비춰주는 평면상에 시선을 가둘 일이 아니다. 거기에 해킹 정치학의 프리즘을 들이대어 펼쳐지는 다채로운 기술문화의 "가치와 의미를 놓고 벌이는 문화 투쟁"(Ross 1990) 안으로 들어가야 한다.

'서비스거부 공격'에 대처하는 자세

한국의 인터넷 기술과 소프트웨어 문화는 획일적이다. '77 분산서비스거부 공격' 사태에 사용된 악성코드류의 컴퓨터 바이러스나 벌레 프로그램이 종종 파괴적인 결과를 불러오는 것은 근본적으로 획일적인 기술문화 때문이다(Galloway 2005: 26). 생물계의 바이러스나 컴퓨터상의 바이러스 등은 모두 네트워크 현상이지만, 후자는 항상 누군가가 의도를 가지고 만들어 배포하여 생기는 네트워크 문화 현상이다. 일탈이나 반론이 아예 없는 어떤 식으로든 총체화 된 사회를 원하는 것이 아니라면, 컴퓨터 바이러스나 벌레 프로그램의 유포는 네트워크문화에서 오히려 자연스러운 일로 볼 수 있다. 우리 사회가 M$라는 특정 기업의 독점 소프트웨어가 90% 이상 지배하는 획일적인 소프

트웨어 문화에서 벗어나 있다면, 악성코드 유포나 분산서비스거부 사태와 같은 일이 있더라도 최소한 사이버 '테러,' '대란,' '재난' 같은 수사가 통하지 않는 규모에 그칠 것이다.[24] 기술문화의 다양성을 위해서는 우리의 해킹에 대한 견해도 다양해야 하며 해킹의 문화정치라는 프리즘을 통해 보면서 기술과 정보와 지식과 콘텐츠에 대한 근본 독점의 악성 코드들을 경계하고 제압하는 문화운동으로 치료해야 한다. 국가 권력과 기업들의 온갖 '서비스거부 사태는 또 그것대로 맞서야 하는 바쁜 와중이지만, 이것만이 '77 분산서비스거부' 사태와 같은 일에 근본적으로 대처하는 우리의 자세이다.

해킹은 멀게는 19세기말 전화의 등장으로 전자 커뮤니케이션 네트워크가 구축되기 시작한 때부터 다른 방식의 이용을 탐구하고 혁신하며 끊임없이 계속 되어왔고 앞으로도 계속 될 것이다. 해킹은 인간과 시스템 사이의 하나의 유력한 커뮤니케이션 방식이기 때문이다. 해킹과 같은 인간의 활동이 절대 없는 사회라는 것은 곧 오류 없는 시스템의 전일적인 지배가 관철되는 사회에 다름 아니다. 이런 사회를 단 한 명만이라도 원하지 않는다면 해킹이라는 커뮤니케이션, 특히 저항과 대안을 창안하는 커뮤니케이션은 필연적이다. 전자 커뮤니케이션 네트워크가 보편화된 지금 사회에서 더더욱 그렇다.

참고문헌

- 강진규. 2009. "DDoS 대처 부처공조 '삐걱'." <디지털타임스>. 7월 27일. http://www.dt.co.kr/contents.html?article_no=2009072702010151739001 (2009년 7월 26일 접속).
- 기어, 찰리. 2006. [디지털문화: 튜링에서 네오까지]. 임산 옮김. 루비박스
- 김강호. 1997. [해커의 사회학 - 해커를 해킹한다]. 개마고원
- 김영식. 2006. “위키페디아에서 대안사회로.” '한 과학기술노동자의 잡소리들' 블로그. 2006년 02월 27일. http://blog.jinbo.net/yskim/?pid=47 (2007년 11월 3일 접속).
- 데닝, 도로시 E., 2005. "액티비즘, 핵티비즘, 사이버테러리즘: 인터넷은 대외 정책에 영향을 미칠 수 있는가?" 아퀠라 & 론펠트. 2005
- 레비, 스티븐. 1996. [해커, 그 광기와 비밀의 기록]. 김동광 옮김. 사민서각
- 문성준. 2001. "통신질서확립법과 온라인 시위." <제1회 전국정보운동 포럼 자료집>. 2001년 2월 10-1일.
- 바브룩, 리처드 & 앤디 카메론. 1996. "캘리포니아 이데올로기." 안정옥 옮김. <문화과학> 통권10호, 1996년 가을
- 아퀠라, 존 & 데이비드 론펠트. 2005. [네트워크 전쟁 - 테러, 범죄, 사회적 갈등의 미래]. 한세희 옮김. 한울
- 윤여상. 2001. "한국 해커공동체의 정치사회적 특성 연구." 부산대학교 사회학과 석사학위 논문. htt

24 이번 사태에 대한 한 보고서는 취약한 정부의 보안 하부구조와 함께 "과도한 마이크로소프트 인터넷 익스플로러 편중과 액티브엑스 의존도를 개선해야 보다 근원적인 보안 취약점이 보완될 수 있다는 주장"을 전하고 있다. 서비스거부 공격을 대리한 좀비 컴퓨터 대부분이 액티브엑스를 통해 악성코드에 감염됐을 것으로 추산된단다(전자신문 미래기술연구센터 2009: 44). 이에 대한 보다 자세한 내용은 김기창, 한국 웹의 불편한 진실, 디지털미디어리서치. 2009 참조.

p://korea.gnu.org/people/chsong/yys (2009년 3월 4일 접속)
- 일리히, 이반. 2004. [성장을 멈춰라! - 자율적 공생을 위한 도구]. 이한 옮김. 미토
- 전응휘. 2009. "7·7 인터넷 대란과 '국가의 주책'." <한겨레21> 769호. 2009년 7월 17일. http://h21.hani.co.kr/arti/society/society_general/25370.html (2009년 8월 14일 접속)
- 전자신문 미래기술연구센터. 2009. <사이버 테러와 IT코리아 현주소: 7.7 DDoS 해킹 대란의 원인과 현실적 대안 모색>. 2009년 8월 7일. http://report.etnews.co.kr/report_detail.html?id=636 (2009년 8월 10일 접속)
- 정보통신부. 1999. <정보화역기능 방지 종합대책(안)>.
- 최세진. 2006. "해커도 운동한다!" [내가 춤출 수 없다면 혁명이 아니다! - 감춰진 것들과 좌파의 상상력]. 메이데이.
- 히매넌, 페카. 2002. [해커, 디지털 시대의 장인들]. 세종서적.
- 하비, 데이비드. 2007. [신자유주의: 간략한 역사]. 최병두 옮김. 한울
- Dafermos, George & Johan Söderberg. 2009. "The hacker movement as a continuation of labour struggle." Capital & Class. Issue no.97. Spring 2009. http://www.cseweb.org.uk/pdfs/CC97/C&C_97_Art3.pdf (2009년 8월 4일 접속)
- Galloway, Alexander R., 2005. "Global Networks and the Effects on Culture." The ANNALS of the American Academy of Political and Social Science. Vol. 597, No. 1
- Jordan, Tim. 2002. Activism! Direct Action, Hacktivism and the Future of Society. Reaktion Books
- Jordan, Tim. 2009. "Hacking and power: Social and technological determinism in the digital age." First Monday, Vol.14, No.7. http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2417/2240 (2009년 7월 23일 접속)
- Kleiner, Dmytri. 2007. "Copyfarleft and Copyjustright," Mute magazine - Culture and politics after the net. http://www.metamute.org/en/Copyfarleft-and-Copyjustright (2008년 7월 18일 접속)
- Kranenburg, Rob van. 2008. The Internet of Things. A critique of ambient technology and the all-seeing network of RFID. Network Notebook #2. the Institute of Network Cultures (http://networkcultures.org/wpmu/weblog/2008/10/02/book-launch-the-internet-of-things-by-rob-van-kranenburg)
- Riemens, Patrice, "Some thoughts on the idea of hacker culture." Compléments de Multitudes 8. http://multitudes.samizdat.net/Some-thoughts-on-the-idea-of.html (2009년 7월 22일 접속)
- Ross, Andrew. 1990. "Hacking Away at the Counter-culture." Postmodern Culture. Vol.1 No. 1. http://muse.jhu.edu/journals/postmodern_culture/v001/1.1ross.html (2009년 7월 19일 접속)
- Ryan, Patrick S., 2004. "War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics." Virginia Journal of Law & Technology. Vol.9, No.7 http://ssrn.com/abstract=585867 (2009년 8월 4일 접속)
- Samuel, Alexandra Whitney. 2004. Hacktivism and the Future of Political Participation. PhD Thesis. Harvard University Cambridge, Massachusetts. http://www.alexandrasamuel.com/dissertation (2009년 7월 4일 접속)
- Söderberg, Johan. 2002. "Copyleft vs. Copyright: A Marxist Critique." First Monday. Vol.7, No. 3. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/938/860 (2008년 12월 18일 접속)
- Söderberg, Johan. 2007. Hacking Capitalism: The Free and Open Source Software(FOSS) Movement. Routledge.
- Stallman, Richard. 2009. "Why Open Source misses the point of Free Software." GNU Project - Free Software Foundation (FSF). 2009년 6월 22일 갱신. http://www.gnu.org/philosophy/open-source-misses-the-point.html (2009년 8월 2일 접속)
- Wray, Stefan. 1999. "Electronic Civil Disobediance and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics." http://switch.sjsu.edu/web/v4n2/stefan/ (2009년 8월 3일 접속)