<뻔뻔한 미디어농장 포럼 2> 사이버해킹, 어떻게 볼 것인가? 발제문(20090717)

해킹문화운동! 지배적 기술문화 해킹하기

해ㅋ(hack.jinbo.net)

일러두기: 이 발제문은 미완성입니다. 풀어쓴 글로 정리하여 발표할 예정입니다.

intro_'2009 분산서비스거부(DDoS) 사태'가 남긴 것

'2009 분산서비스거부(DDoS) 사태'

- 한 국의 인터넷 기술 - 소프트웨어 문화는 획일적이다. 이번 "77 인터넷 대란"에 사용된 악성코드와 같은 바이러스나 웜은 근본적으로 이러한 획일적인 기술문화를 배경으로 한다(Galloway 2005: 26). 생물계의 바이러스와 컴퓨터 바이러스는 모두 네트워크 현상이지만 후자의 경우 항상 누군가가 의도를 가지고 만들어 배포하여 생기는 사회공학적 현상이다. 일탈이나 반론이 아예 없는 여하간의 총체화된 사회를 원하는 것이 아니라면, 컴퓨터 바이러스 등의 악성코드의 유포는 오히려 자연스러운 일로 볼 수 있다. 우리사회가 마이크로소프트(이제부터 M$)라는 특정 기업의 독점 소프트웨어가 90% 이상 지배하는 획일적인 소프트웨어 문화가 벗어나 있다면, 악성코드 유포 및 분산서비스거부 사태와 같은 일은 최소한 사이버 - '테러,' '대란,' '재난' 같은 수사가 전혀 통하지 않았을 것이다.
- 용어 설정과 사용의 문제: '2009 분산서비스거부(DDoS) 사태'
- 사 실 1990년대 후반부터 정부 컴퓨터, 상업과 교육용 컴퓨터를 대상으로 한 허가받지 않은 컴퓨터 침입으로서의 인터넷 해킹은 매우 흔한 일이다(데닝 2005: 336). 서비스거부 공격도 마찬가지인데 한국에서는 매년 30~40차례 디도스 공격이 있다(전자신문. 20090710). 그러나 이번에는 마치 국가 재난이라도 일어난 것과 같이 정부와 언론이 "호들갑"을 떨었다. 무엇이 달랐던 것인가?

    1. 특정 사이트나 서비스만이 아닌 주요 공공 및 상업 서비스에 대한 동시다발 공격이 이루어지면서 (그리고 미국과 동시에 이루어진 점에서) 국가 단위 사건으로 받아들여졌다. 국

정원의 북한 배후설 이외에도 중국 등의 해커집단을 그 주체로 지목하는 말들이 많았는데 이런 맥락에서 사이버 테러리즘이나 사이버 국가 안보에 대한 논리가 자연스러웠다.

2. 위와 관련해서 이번 '2009 분산서비스거부(DDoS) 사태'를 정치적인 사건으로 보는 것이다. 보통 이런 일들이 개인정보 유출이나 협박을 통한 금전 요구 등을 노리며 일어나는 것에 비해 이번에는 그렇지 않았기 때문이다.

이 사태가 남긴 2가지 우려

위와 같은 맥락에서 이 사태는 2가지 우려를 자아낸다.

1. 이미 알려졌다시피 이 사태에 대한 대응과 후속 대책 마련의 과정에서 국가 기구의 네트워크 통제 강화의 흐름이 형성되고 있다. 국정원의 북한 배후설과 같은 헛소동이 있기는 했지만, 되려 네트워크에 대한 국가 권력의 통제에 대한 알리바이로 삼기 위해 이 사태가 발생하기라도 한 것처럼 통제 강화의 흐름이 가속화될 수 있다.
    - 공 성진의원 등이 발의한 '국가사이버위기관리법': "예컨대 아주 단순한 해킹사고도 모두 국정원장에게 즉시 보고하고, 또 즉각 사고조사 결과를 통보해야 한다. ... 필요하면 언제든지 국정원장이 모든 시스템에 직접 접근할 수 있도록 권한을 부여하고 있다"(전응휘, 한겨레21).
    - 미국의 경우, 사이버사령부(cybercom) 창설 등의 움직임이 있어왔다(아이비스에너지전략연구소. 2009).
2. 아래에서 살펴보겠지만 해킹에 대한 왜곡된 언어 사용에서부터 네트워크 통제 강화에 이르기까지 해킹 및 해커문화에 대한 탈정치화(범죄화)와 탄압이 강화된다.
    - 아 래에서 자세히 살펴보겠지만, 1980년대 정보통신산업이 70년대의 석유파동과 세계경제 위기를 극복할 '신성장동력'으로 급부상하면서 컴퓨터 산업 및 소프트웨어 산업이 부양되는 동시에 정보에 대한 상품화와 이를 위한 재산권 체제의 확립(지적재산권)이 본격화되었다. 이 과정에서 해킹 활동, 해커공동체는 정보의 사유화에 걸림돌이 되었고, 곧 합법적(?) 기업 활동과 정부 정책을 방해하는 범죄자로 덧칠되기 시작하였다. 그러면서, 1988년에 있었던 컴퓨터 바이러스 사태와 1990년 해커에 대한 대대적인 검거 작전이 발생하면서 한편으로는 그러한 재현/이데올로기가 굳어져 가고, 다른 한편 새로운 법제화와 감시 통제 기구들의 설립이 탄력을 받았다.
    - 이에 비추어, 이번 '2009 분산서비스거부(DDoS) 사태' 등을 매개로 반-해킹 정서와 담론, 그에 따라 기술을 통한 문화저항까지도 범죄시하는 여론을 형성하고 관련 법제화를 수월하게 하는 흐름을 예상할 수 있다. 여기서 해킹은 다양한 전자적 행위, 특히 온라인의 정당한 표현의 자유 활동까지 포함된다. 각국에서 만들어져온 컴퓨터 범죄 관련 법들은 "사이버 테러리즘이나 핵티비즘에만 국한되는 것이 아니라 모든 형태의 해킹과 컴퓨터 네트워크에 대한 공격, 컴퓨터 및 통신 사기, 인터넷 아동 포르노, 그리고 디지털 저작

권 침해(소프트웨어, 음악 등)의 행위를 총체적으로 뿌리 뽑는 것을 목표"(데닝 2005: 344)로 해왔다는 점을 두고 볼 때. 우리의 디지털 네트워크 생활문화와 일상 정치활동에 검열과 감시를 다시 불러들이거나 강화시키고, 자유롭고 평등한 정보 접근 및 정보공유 활동을 옥죄게 하는 결과를 가져올 수 있기 때문이다.

- 결 국, 이러한 정치적 컴퓨터 바이러스나 웜 유포, 서비스거부 사태가 발생할 때마다 자연스럽게 사이버범죄, 사이버테러, 사이버전쟁의 온갖 언어와 담론, 그리고 실제로 진행되는 '사이버테러와의 전쟁'이 미국에서 1990년에 겪은 바 있는 '해커에 대한 전쟁'의 정당화, 전자 커뮤니케이션에서의 표현의 자유 위축과 억압을 정당화하는 것으로 가고 있는 것을 우려하는 것이다.
- 순수한 기술놀이, 보안 탐구, 해킹행동주의, 온라인 사회운동을 '사이버테러'로 규정하는 담론을 경계하고, 실제로 이런 것들을 빌미로 인터넷문화 전체를 옥죄는 법안들이 강화되고 있는 것도 예의 주시해야 한다. 오히려 이런 권력과 자본의 움직임에 맞서 저항하는 방식은 사실 해킹, 해킹행동주의, 해커문화임을 확인할 필요가 있다.
- 따 라서 이 발제문은 현재의 사이버테러 사태와 그 담론이 자율적인 기술탐구의 해킹을 포함한 전자 커뮤니케이션의 표현의 자유 활동까지 테러로 규 정하는 것을 경계하자는 주장을 담고 있다. 그러나 이 글은 사이버테러, 네트워크 전쟁 등에 대한 담론 비판을 위한 것은 아니다. 대신, 해킹 및 해커문화가 가져온 문화정치적 의미를 되살리고, 지배적 기술문화에 저항하는 유력한 운동 방식의 하나로 해킹문화운동을 제안한다.

해킹과 해커문화의 뿌리

해킹: 처음 뜻

- 해 크(hack)라는 말은 50년대부터 메사추세츠공대(MIT)에서 통용된 은어로서 "작업과정 그 자체에서 느껴지는 순수한 즐거움 이외에는 어떠한 건설적인 목표도 갖지 않는 프로젝트나 그에 따른 결과물"(레비 1996: 22)를 뜻했다. 컴퓨터 기술에 국한되지 않고 다양한 취미생활에 대해서도 사용된 은어였던 것이 컴퓨터 과학자들 사이에서 기술 문제에 대한 독창적이고 재미난 해결책을 찾은 것을 인정하는 표현으로 점차 많이 사용되었다. "컴퓨터와 놀 수 있는 즐거움을 누렸던 이들은 값비싼 장비들에 접근하면서 연구하고 '핵'(hack)할 수 있는 자율성을 누린 소수의 전문가들이었다"(Söderberg, 2007: 12).
- 조단(Jordan)은 이렇게도 설명한다. "'핵'(hack)은 기술의 혁신적인 사용을 가리킨다. 한 해커는 단적으로 이런 예를 든다. 차를 마시려는데 전기 주전자가 없지만 커피내리기(coffeemaker)가 있을 때 그걸 이용해 물을 끓여 차를 타마셨다면, 커피내리기를 다른 방식으

로 사용한 그것이 핵이다"(2002: 120).

해커문화의 역사

60년대 메사추세츠공대(MIT)의 해커공동체

- 경제부흥, 냉전, 시민불복종운동, 히피문화, 대항문화, 아나키스트운동 등
- 2 차 세계대전 이후 현대전에서 가장 큰 공훈을 세운 컴퓨터를 발전시키는데 핵심적인 역할을 한 메사추세츠공대(MIT)는 어느 곳보다 앞서서 컴퓨터 기술을 발전시킨 곳이었다. 당시 군사 프로젝트에 사용되던 컴퓨터 시스템에 대한 학교 당국의 관리는 엄격했다(김강호 1997: 26, 131).
- 철도의 내부 구조 시스템을 연구하고 모형을 만드는 이 대학 동아리였던 '테크모델철도클럽'(TMRC, Tech Model Railroad Club)의 회원들은 그들의 관심사인 기계와 제어장치의 새로운 형태인 학교 연구소에 들어온 컴퓨터를 보고 그냥 지나칠 수가 없었다. 인공지능연구소에 보관되어 엄격히 통제되던 컴퓨터를 사용하기 위해 이들은 열쇠를 부수고 컴퓨터 터미널이 설치된 방에 몰래 들어가 사용하기 시작하고 비교적 자유로운 연구소 분위기에서 그들의 접근과 프로그래밍은 비공식적으로 더러 공식적으로 허용되기는 했다(레비 1996: 13-44).
- 이들은 컴퓨터에 대한 접근이 관료주의 통제에 막힌 것, 지적 탐구로서의 자신들의 해킹으로 만들어진 프로그램이나 정보를 기업이나 연구소가 독점하는 것에 강한 반감을 가지며 접근 권리와 정보 공유 정신을 주장하는 해커 윤리를 만들어갔다(최세진 2006: 74).
- 최 초의 컴퓨터 해커공동체를 형성한 이들의 문화는 기술 엘리트들의 문화이기는 했지만, 전쟁을 위해 그리고 자본의 요구에 맞춰 개발되기 시작한 컴퓨터에 처음 접근했던 이 일탈자들이 가졌던 문제의식을 담은 이러한 해커 윤리는 대부분의 경우 청년(youth) 문화로 이어졌고, 해킹과 해커 활동은 1970년대, 1980년대까지 낭만적인 대항문화 경향을 갖는 것으로 제시되었다. 의식있는 기자들이 이를 칭송하기도 했고, 1980년대 말 "해커에 대한 전쟁"이 미디어 보도를 형성하기 시작하기 전까지 지배 미디어 재현은 "모뎀으로 하는 반란" 정도였다(Ross 1990).

70년대 대항문화로서의 전화 프리킹, 컴퓨터 하드웨어 해킹

- 전화 프리킹(phone phreaking)은 전화 교환 장치에 사용되는 컴퓨터 시스템의 허점을 뚫고 들어가 무료로 전화를 사용하거나, 전화 시스템의 운영에 개입하는 행위를 말한다(이광석 1998: 74 각주4).
- 오늘날의 사이버 공간, 네트워크문화의 기원은, 그리고 네트워크 해킹의 기원도 1876년 전화의 등장에서부터 찾을 수 있다(스털링). 프리킹(phreaking) 또한 전화의 상용화 시점부터 시작된 전통적 행위(윤여상 2001)였다.

    - 전화 교환수 소년의 말썽(스털링).
    - 농 촌에서야말로 전화가 유용함에도 불구하고 농촌에서는 돈벌이가 안된다는 이유로 전화 서비스가 생기지 않자, 농부들이 직접 전화선을 놓고 신호 전달을 위해 철조망을 이용해 이웃과 연결한 농민전화선(farmer lines) 운동이 있었다. 이들은 그레헴 벨이 가지고 있었던 전화에 대한 특허를 무시하는 일이었지만, 1906년에 6천 개의 소농들이 자체 전화선을 이용하고 조합을 형성하고 있었다. 이후 전국 전화망으로 통합되었다 (Söderberg, 2007: 11). 한국에는 거의 활성화 안되어 있지만, 이는 무선 인터넷 접근을 위한 공동체 무선 네트워크 운동에서도 유사한 형태를 볼 수 있다.
    - 전화뿐만 아니라 무선 전파를 이용한 라디오가 현재와 같은 방송산업으로 제도화되기 이전에 아마추어 무선통신사들의 '시민라디오'가 또한 그러한 자율적인 해커공동체 네트워크를 형성했다. 이와 같이, 전(기)자적 네트워크가 등장할 때부터 기술 특허와 법제도 정책을 통한 시장 독점이 있었고 동시에 그에 대한 다양한 풀뿌리 저항운동이 있어왔다.
- 공룡 미국전신전화사(AT&T)의 횡포는 중소 전화사업자의 격렬한 저항; 정부와 결합한 도청과 시장독점의 전횡에 일반대중과 지역 전화사업자들이 격렬하게 저항하는 와중에 전화 프리커(phreaker)는 AT&T의 전화세 납부거부운동의 수단으로 공짜전화걸기 캠페인을 전개하였고(김강호 1997: 17), 전화 프리킹이 반전운동과 직접 연계된 것은, 미국 정부는 베트남전쟁 비용을 마련하기 위해 전화에 특별세를 붙이는 법안을 의회에서 통과시켰는데 이 법안은 반전 운동의 하나로 전화세 납부거부운동을 불러왔던 것이다(윤여상 2001).
- 이들은 신좌파의 정치적 자의식을 공유하기도 했는데, 아비 호프만(Abbie Hoffman)이 1971년에 시작한 선구적인 뉴스레터, '국제청년파티라인'(YIPL, Youth International Party Line)에 담겨져 있다. 이를 통해 기술적 노하우를 나누었는데 한편으로는 기술을 통한 해방 이데올로기를 앞세운 활동가들이 있었고 다른 한편에는 기술에 있어서 고수가 되는 것에 관심을 가진 기술자(techie)들이 있었다(Söderberg, 2007: 16).

  호프만은 이플 창간호에서 미국 정부와 미국의 통신망에 독점적인 통제권을 행사하는 벨사를 공개적으로 비난하였고, 무료 전화 걸기에 사용되는 프리킹 도구의 설계 도면과 사용법을 이플을 통해 계속 확산시켰다. 프리킹을 반정부 운동과 벨로 대표되는 거대 기업들에 도전하는 급진적 사회 운동에 접합시키려 한 것이다(윤여상 2001).

- 1960년대 미국에서의 반전 운동, 히피문화를 배경으로 한 최초의 정치적 해커공동체가 출현한 것이다. 해킹이 허가받지 않은 네트워크 시스템에 개입(침입)하는 행위라는 의미는 이때 덧붙여진 것이다.
- 메 모리 공동체(Community Memory)는 제3자의 판단에 맡기지 않고 사람들이 기탄없이 서로의 관심사를 이야기할 수 있는 통신 시스템으로 컴퓨터를 사용하고자 하였다(윤여상 2001). 세계 최초의 컴퓨터 공동체 네트워크이다(Douglas Schuler, 1996; 윤여상 2001에서 재인용). 사람들은 당시 이 컴퓨터에 입력돼 있는 데이터베이스에서 건강진료소의 위치를 확인하고, 좋은 레스토랑과 레코드 앨범에 대한 정보를 알아낼 수 있었다. 이처럼 PC를 이용한 사설 전자게시판이 등장하기 전에 태어난 메모리공동체의 컴퓨터 온라인통신의 가능성을 확인시켜 주었다(김강

호 1997: 112-3). 메모리 공동체에 참여한 펠젠스타인은 컴퓨터를 이용한 자유로운 네트워크 건설에 필요한 개인용 컴퓨터 개발이라는 정치적 목적을 가지고 홈브루클럽(Homebrew Club)을 이끌었다.(윤여상 2001).

- 개인용 컴퓨터의 구체적인 형태는 MITS사의 에드 로버츠가 만든 견우성이라는 뜻의 '알테어'였는데, 알테어8800은 개인용 컴퓨터를 가지고 싶다는 열망을 자극하며 수많은 사람들에게 팔려나갔고, 곧 알테어8800을 조립하고 필요한 정보를 교환하기 위한 공동체가 자생적으로 발생하였다. 알테어8800을 중심으로 모인 공동체는 1975년 금주법에 따라 술의 판매가 금지되자 집에서 밀주를 만들던 것에서 이름을 따와 공동체 이름을 홈브루클럽(Homebrew Club)이라고 지었다(김강호 1997: 134).
- 홈브루클럽에서의 기술혁신: 리 펠젠스타인이 75년 개발한 컴퓨터 모니터라는 개념을 낳게 해준 VDM(video display module)이라는 비디오 보드; 인류 최초의 데스크톱 컴퓨터인 '솔' 컴퓨터; 76년 스티브 워즈니악과 스티브 잡스의 애플컴퓨터 탄생(김강호 1997: 135) - 애플 컴퓨터는 해커공동체를 넘어선 소비자 시장 형성의 결정적 일보였다(Söderberg, 2007: 17).
- 당 시 거대 기업이나 연구소에나 있던 컴퓨터는 대형의 메인프레임 컴퓨터였는데, 하드웨어 해커공동체인 홈부르 컴퓨터 클럽의 활동은 이러한 컴퓨터 자원의 민주화를 위한 노력이었다(Söderberg, 2007: 18). 당시 홈부르 컴퓨터 클럽에는 정치 의식을 가진 활동가들이 있었지만 떠나기도 하고, 이와 같은 성과는 놀이나 기술 해킹에 욕망을 가진 사람들에 의한 것이었다. 비정치적 의식은 우익에 이용되기도 했지만, 소더버그는 암상자 디자인 매개로 권력관계 유지되는 계급사회에서 시스템 구축의 순수한 즐거움은 그 자체로 정치적인 것으로 평가한다(Söderberg, 2007: 18).
- 1972년 10월에 결성된 '피플즈 컴퓨터사'(People's Computer Company): "컴퓨터는 대부분 민중을 위해서가 아니라 민중에게 해를 끼치는데 쓰인다. 민중을 해방하는 게 아니라 민중을 통제하기 위해 사용된다. 이 모든 것을 변화시킬 때가 왔다. 우리는 필요하다" (김강호 1997: 133에서 인용). 반문명적 행동주의와 민중, 특히 아이들에게 컴퓨터를 전파하는 복음주의적 운동을 결합한 해커2세대 그룹이다(레비: 220-1).
- 네트워크 시스템 개입으로서 해킹이 전화 네트워크에서 먼저 시작된 것은 전화는 1876년 벨(Alexander Graham Bell)에 의해 발명된 이후 1960년대에는 이미 미국을 비롯하여 세계 전역에 걸쳐 광대한 네트워크를 형성하고 있었기 때문이다.(윤여상 2001). 반면, 1960년대까지 컴퓨터가 미국에서도 학교와 정부 또는 기업에서 주로 사용되었고 일반인에겐 잘 알려지지 않았으며, 1980년대 중반 이후 애플(Apple)사와 IBM 등이 개인용 컴퓨터를 개발하여 보급하면서 비로소 폭넓게 사용되기 시작한 것이다(윤여상 2001). 따라서 1970년대의 컴퓨터 및 컴퓨터 네트워크에서의 해커공동체는 무엇보다도 하드웨어에 초점이 가 있었다. 그리고 이들 컴퓨터 하드웨어 해커공동체가 1980년대 이후 개인 컴퓨터 및 인터넷의 대중화에 크게 기여한 셈이다.
- 1970년대는 반체제 운동과 히피 문화 속에서 해킹 또한 정치사회적 특성을 강하게 보인 시기(윤여상 2001)이자 컴퓨터 하드웨어와 자율적인 통신 네트워크를 구축하는 대안 기술 생산이 해킹이 동시에 발전한 시기였다.

80년대: 게임 해킹, 카피레프트와 자유소프트웨어운동, 네트워크 해킹

- 컴퓨터 게임 해킹
- 81년에 탄생한 독일의 '카오스클럽'; 1984년에 시작한 죽은소 숭배(cDc, Cult of the Dead Cow) 해커집단; ...
- 소프트웨어재단(FSF, Free Software Foundation)을 설립한 리차드 스톨만(R. Stallman): 카피레프트와 자유소프트웨어운동
    - 소프트웨어는 초기에 2차적 부산물이었다. 그러다가 하드웨어보다 소프트웨어가 더 가치가 커지면서 담당 기관이 그 배포에 대한 통제를 요구하기 시작했다(Söderberg, 2002): 유닉스(unix) 사례
    - 1980 년대 소프트웨어 코드에 대한 두 가지 종획(Söderberg, 2007: 18-9): 하나는 IBM이 저작권법 통해서 소프트웨어에 대한 강제적 라이선스를 채택하기 시작한 것이고, 또 하나는 1982년에 AT&T가 반독점법 해제되면서 컴퓨터 사업에 진출 가능해지고 곧 이미 널리 자유롭게 공유되고 있던 유닉스(unix)에 대한 소유권을 주장한 것이다; 이는 저작권이 그 작업들을 저자들(프로그래머 공동체)로부터 빼앗을 수 있다는 것을 보여준 것이었다.
    - 자유소프트웨어운동, 카피레프트운동은 이러한 정보 공유지의 공유지의 종획에 대한 저항으로 등장하게 된 것이다.
- 한 국의 경우: 개인용 컴퓨터가 본격적으로 보급되기 직전인 80년대 말에 등장한 국내 해커공동체 초기의 프로그램으로는 '엠팔'의 회원 묵현상(현재 삼보컴퓨터 이사)이 개발한 '엠팔의 반란'에서 찾을 수 있다. 당시 국내에서 고가에 판매되어온 PC용 통신용 소프트웨어(에뮬레이터)를 독자적으로 개발, 누구나 대가없이 사용할 수 있는 셰어웨어 형태로 공개; 최초의 한글 통신용 공개소프트웨어로 기록될 이 프로그램(김강호 1997: 109).
- 해킹의 범죄화 과정
    - 사설 BBS의 개발과 확산
    - 영화 '워게임'의 부정적 이미지
    - 1982 년 '414 Gangs'라고 부르는 네트워크 해커들이 경찰에 체포되었을 때, 언론이 이 사건을 보도하면서 해커를 위험한 컴퓨터 침입자로 묘사하였고, 이후 언론과 출판물들은 해커를 전자적인 불법 침입자들(electronic trespassers), 전자 반달족(electronic vandals), 장난꾸러기들(varmints), 첨단 기술의 길거리 갱들(high-tech street gangs) 등 일탈적인 인물로 묘사하면서 사악한 젊은이들'이란 부정적 의미로 고착(Denning, 1991; 윤여상 2001에서 재인용).
    - 89년 독일의 해커들이 미국 국방망을 침입하여 군사기밀을 소련으로 넘긴 일명 '카오스 사건'이 전세계 신문과 방송 등 매스미디어를 통해 알려지면서 해커의 역기능에 대한 우려의 목소리가 터져나오기 시작(김강호 1997: 35).
- 정 보혁명의 선구자인 해커들이 범죄집단으로 규정되기 시작한 때는 컴퓨터라는 도구가 하나의

산업군을 형성하는 시기와 일치; 소프트웨어가 더 이상 공유하는 산물이 아니라 상품으로 변모했기 때문이다.(김강호 1997: 48). 상품을 상품으로, 즉 그 교환가치를 보존하기 위해서는 이러한 자율적 기술 접근과 이용을 통제할 필요가 있었던 것이다.

- 물론, 그러면서 해킹이라는 기교를 가지고 돈벌이를 하려는 사람들에 의해 해커들은 변종되었고, "해커의 활동이 상업주의와 만나면서 범죄화하는 새로운 국면을 맞게 된 것"(김강호 1997: 57)이기는 하지만, 보다 큰 맥락에서 보자면 결국, 냉전시대와 (컴퓨터와 인터넷이 가전제품, 개전제품으로 등장한) 대량소비사회 속에서 정치적 정보와 상업적 시장에 대한 대중 통제의 산물이라고 볼 수 있다.
- 이러한 범죄 용어들이 해킹 행위들에 유비되는 것은 즉각적인 이해를 돕는다고 생각해서 그런지 모르겠지만 바로 그렇기 때문에 심각한 오해나 보다 근본적인 질문을 제약하는 문제를 안고 있다. 로즈(Ross 1990)가 볼 때, 해킹을 무단으로 다른 사람들의 집에 침입하는 것과 유비하는 것은 "사생활보호, 재산, 소유적 개인주의, 국가의 과잉 감시 등의 논쟁을 제약"한다. "대부분의 해커들이 거의 집중적인 '목표 대상'으로 하는 정보기술의 제도기구나 기업 소유자들의 활동에 대한 조사는 중단시키면서 말이다."

<u>90년대: 네트워크 해킹, 사이버테러 담론, 해킹행동주의</u>

- 이미 80년대부터 등장한 네트워크 해킹은 90년대에 상당히 크게 확대
- 1988년 11월 코넬대 해커 로버트 모리스가 전국 네트워크 시스템(미국 펜타곤의 아르파넷 데이터 교환 네트워크를 포함한 인터넷)에 대한 바이러스 공격 - 약 6천 대의 컴퓨터 감염
- 1990년 봄 미국에서의 해커 대소탕 작전이라고 할 만한 선데블 작전
- 네트워크 해커공동체는 국가와 기업에 의한 감시 및 통제, 프라이버시 침해 그리고 컴퓨터-인터넷 시스템의 불안정성에 대해 문제를 제기한다.
  이와 같은 전통은 이플의 정신을 계승하고 선데블작전과 같은 단속 활동에 저항하는 가운데 자생적으로 형성된 것이다(윤여상 2001).
- 사이버 전쟁, 사이버 테러, 해킹행동주의가 함께 출현하였다.
- 해킹 행동주의의 등장
    - 정치적 배경: 처음 멕시코의 사빠띠스타 민족해방군(EZLN)을 지원하는 국제적인 활동의 일환으로 멕시코 정부와 다국적 기업들을 네트워킹 해킹 기술을 사용해서 공격하자는 제안에서 출발
    - 기 술적 배경: 인터넷을 통해 전세계에 퍼져있는 프로그래머와 컴퓨터 사용자들은 손쉽게 실시간으로 자료를 교환할 수 있었으며,이를 기반으로 1960, 70년대의 해커공동체와는 다른 전세계적이고 개방적인 해커공동체가 출현할 수 있었다.(윤여상 2001).
- 해킹행동주의가 전면적으로 부상하게 된 계기는 1999년 나토(NATO)와 미국의 유고 공격
- 유 고 전쟁은 인터넷을 이용한 사이버 전쟁의 최초 사례이다. 유고 전쟁을 계기로 언론사들은 사이버 전쟁에 대한 대비를 주장하기 시작했다.(윤여상 2001). 이와 같이, 해킹행동주의가 국제정치와 분쟁 속에서 부상하면서, 사이버테러나 사이버전쟁과 뒤섞여 존재하거나 그렇게 이해되

게 되었다고 할 수 있다.

정리: 독점 네트워크에 대한 해킹의 위반의 정치

- 역사적 흐름 (윤여상 2001).
    - 1960대 초반에서 1960년대 후반까지 MIT 해커공동체에 의한 해커윤리의 형성 시기,
    - 1960년대 후반에서 1970년대 후반까지 정치사회적 해킹과 프리킹의 시기,
    - 1980년대 초반에서 1990년대 초반까지의 본격적인 네트워크 해킹의 활성화 시기, + 프로그래밍 해킹과 정치적 네트워크 해킹이 동시에 발아한 시기
    - 1990년대 중반 이후의 리눅스의 등장과 사이버 테러리즘 및 핵티비즘의 확산이 보여주는 정치사회적 해킹의 재등장 시기
- 2000년대는? 좀 더 자세한 조사 연구가 필요하지만, 프리커 - 해커 - 네티즌으로 연결되는 흐름을 감지할 수 있다. 해킹행동주의 대중화 (정보운동 차원, 온라인 시위 차원)
- 해킹, 해커 이념의 두 축
    - MIT 해커 계열 해커공동체의 자유소프트웨어정신 및 리눅스 정신과, 프리커 계열 해커공동체의 해킹행동주의는 현재 해커 이념의 두 축을 형성하면서 확산되고 있다(윤여상 2001).
    - 혹은, 사회운동으로서의 해킹은 두 흐름: 정보운동, 사회운동과의 연대
- 해 킹과 해커의 다양한 변이에도 불구하고, 역사적으로 이들을 묶어주는 윤리이자 정치적 주체화의 핵심은 "정보의 자유와 권력의 해체"이다. 다시 말해서 "그들을 정치 집단화하는 근거는 디지털 정보 독점에 대한 저항과 자유로운 유통의 정신"으로서 "물리적으로 굳게 잠겨있는 모든 통제권과 이로부터 나오는 약화의 일방성과 규제를 거부하고 공개하려는 것"(이광석 1998: 80)에 있다.

명시적이든 잠재적이든 정치적 주체이자 문화로서 존재해온 해커와 해킹은 1990년대를 맞으면서 사회운동의 투쟁 과정에서 행동주의예술, 직접행동, 문화행동 등과 결합한 해킹활동가와 해킹행동의 형태로 발전한다. 이른바 해킹행동주의(hactivism)이 그것이다. 다음에서는, 해킹이 사회운동 차원에서 직접행동이나 선전선동, 사회적 관심 환기 등을 위한 전술로 활용한 해킹행동주의에 대해 특별히 살펴볼 필요가 있다. 이것이 이번 사태와 같은 해킹 방식을 사용하며 '사이버 테러'와 혼동시키면서 오해를 살 수 있는 부분이기 때문이다.

해킹행동주의 혹은 해킹의 정치학

개념과 역사

- 해 킹행동주의(hacktivism)라는 말 자체는 죽은 소 숭배(cDc, Cult of the Dead Cow)라는 해커집단이 해커들의 사회운동 참여를 선언하며 만들었다. "정치사회적 목적을 이루기 위해 벌이는 다양한 온라인 활동 방식을 말한다"고 정의하였다(최세진 2006: 74).
- 하지만 그 행동 자체는 이미 1988년까지 거스러 올라간다. "미항공우주국이 항의자들이 흔히 잠재적 핵폭탄으로 묘사되는 작은 핵 원자로를 포함하는 탐사선을 발사하는 것에 항의"해 알려지지 않은 사람(들)이 미항공우주국(NASA)의 컴퓨터 네트워크에 자기복제되는 WANK 웜(worm)을 심은 적이 있다(Jordan 2002: 119-200; 데닝 2005: 337).
- 1996년 '모두 함께 비판예술'(CAE, Critical Ats Ensemble)은 이를 아예 조직적으로 만들어가자는 제안을 한다. 점차 권력이 사이버공간의 정보 흐름에서 파생되어 나오고 이 세계를 재형성하고 있기 때문에 이러한 흐름을 차단하는 전술을 개발하고 해커의 정치화와 전자적 시민불복종을 발전시켜나가자는 것이었다(CAE, Electronic Civil Disoedience and Other Unpopular Ideas. New York. 1996; Jordan 2002: 120에서 재인용). 사이버공간에서의 편재된 권력의 작동에 해킹행동주의로 맞서자는 이러한 제안은 전자교란극장(EDT: Electronic Disturbance Theater)의 홍수넷(floodnet)을 통해서 구체화된다.
- 이전까지 해킹의 정치(학)가 주로 누구나 안전하게 접근할 수 있는 정보의 자유로운 흐름을 만들기 위해 가상 세계의 정치적 사안들 - 컴퓨터 시스템의 보안, 개인의 프라이버시, 인터넷 검열 등에 초점이 맞춰져 있었다면(Jordan 2002: 121), 1998년의 홍수넷과 같은 사례가 등장하면서 본격적으로 사회운동과 결합되는 해킹행동주의가 등장한 셈이다.
- 몇 가지 정의를 보면,
    - 해킹행동주의(hacktivism)은 정치적 행동주의와 해킹의 결합으로서 목표 대상의 정상적인 활동을 방해할 목적으로 대상 웹사이트를 해킹하는 것을 말한다(데닝 2005: 295).
    - 해커들이 불법적인 컴퓨터 침입을 별로도 크래킹(cracking)이라고 부르고 있는데, 위와 같은 의미에서 해킹행동주의은 해킹과 크래킹 모두를 포함한다고 볼 수 있다(Jordan 2002: 120).
    - 정 치적 행동주의의 맥락인만큼 이것의 목적은 대상에 대한 중대한 손실을 입히는 자체가 아니라, 관련 사안에 대한 정치적 의사 표현과 사회적 관심과 지지의 확보에 있다. 그런 차원에서 사이버테러와 구분된다. 정치적 동기를 가지고 해킹을 한다는 점에서는 같지만, "사이버테러는 인명 피해나 심대한 경제적 손실과 같은 중대한 손실을 입히는 것을 직접적인 목표로 하는 대규모 폭력을 의도"(데닝 2005: 296)하기 때문이다.
    - 조단(Jordan 2002: 119)은 "정치적으로 동기부여된 해킹"이라고 폭넓게 정의한 바 있고 이후에는 "컴퓨터 해킹과 풀뿌리 정치 시위의 조합"(Jordan & Taylor 2004; Samuel 2004: 2에서 재인용)으로 정의하고 있다.

    - 실제 51명의 해킹활동가들과의 인터뷰를 통해 박사논문을 작성한 사무엘(Samuel 2004)은 "정치적 목적을 추구하기 위해 불법적이거나 법적으로 애매한 디지털 도구의 비폭력적 사용"으로 이를 정의하고 있다. 여기서 '비폭력'은 인간에게 해를 끼치는 사이버테러리스트와 구분해주고, '불법적이거나 법적으로 애매한'이라는 말은 온라인 행동주의의 비-위반 형태들과 구분해 주며, '어떠한 디지털 도구의 사용'은 가끔 해킹행동주의로 명명되는 모든 형태의 비폭력적이고 위반하는디지털 행동을 명시적으로 포함한다 (Samuel 2004: 3). 그래서 해킹행동주의는 (테러리즘과 같은 폭력이 아니라) 위반과 비폭력을 핵심적인 규정 요소로 한다.
- 보통 해킹행동주의를 좁은 의미로 사회운동과의 연대 차원으로 보고 위의 해킹행동주의 정의들도 대체로 그런 경향이 있는데 앞서 살펴본 해커, 해킹의 역사를 고려한다면 직접행동과 같은 형태는 아니었더라도 지금의 정보 자본주의 사회가 형성되는 초기에 이미 비판적인 정보 정치학(informational politics)를 형성시켜온 흐름을 넓은 의미의 해킹행동주의로 포함시키는 것이 합당하다고 본다. 더군다나 실천 사례들을 볼 때 양자는 엄밀하게 구분되지 않는다. 1990년대 후반 이후 정보 정치의 다양한 사안들에 대한 직접행동 방식의 해킹행동주의가 존재왔기 때문이다.

유형

- 아 래의 유형은 다양한 사례들에서 사용된 해킹행동의 전술들을 놓고 분류한 것이다. 데닝(2005: 296)은 해킹행동주의를 가상 연좌시위(virtual sit-in)와 차단(blockade), 전자우편 폭탄, 웹 해킹, 컴퓨터 침입, 바이러스와 웜 유포 등으로 분류하고 있고, 사무엘(Samuel 2004)은 웹사이트를 지저분하게 하기(defacement), 다른 곳으로 가게 하기(redirect), 서비스거부 공격, 정보 탈취, 웹사이트 패러디, 가상 점거, 가상 태업/방해, 소프트웨어 개발로 분류하고 있다.
-

  나는 이 둘을 종합하여 아래와 같이 6개의 범주로 분류하였다. 위의 분류가 각 분류의 위상 간의 차이가 있어 다소 혼란스럽기 때문이다. 예를 들어, 사무엘(Samuel 2004)은 웹사이트를 지저분하게 하기(defacement)과 가상 점거를 동급으로 분류하고 있지만 내가 볼 때 전자는 하위, 후자는 상위 범주로 생각된다. 또한, 데닝(2005)이 분류하여 설명하고 있는 '웹 해킹'이나 '컴퓨터 침입'은 해킹 일반에 해당되는 것으로 침입 후에 무엇을 하느냐에 따라 분류되어야 할 것이다. 그래서 시스템 침입 후의 행위로서 크게 기존의 웹페이지를 다른 정치적 메시지로 바꾸는 것과 정보를 빼내는 것으로 나눌 수 있다. 전자는 '웹서비스 훼방'으로 후자는 '정보 입수, 훼손, 공개'로 분류 하였다.

<u>웹서비스 훼방</u>

- 데닝(2005)이 구분하는 웹 해킹과 컴퓨터 침입이 전제된, 웹사이트를 지저분하게 하기

(defacement), 다른 곳으로 가게 하기(site redirect), 사이트 패러디 등

- 미 국 중앙정보국(CIA, Central Intelligence Agency)의 웹사이트가 중앙바보국(Central Stupidity Agency)로 이름이 바뀐다거나 정치정당의 웹사이트에 그들을 풍자하는 만화가 들어가 있다거나 하는 사례(Jordan 2002: 133).
- 웹사이트를 지저분하게 하기(defacement)와 다른 곳으로 가게 하기(site redirect)가 동시에 이루어진 사례: 포르투갈의 한 해커 집단이 1998년 40개 인도네시아 사이트에 침투해 큰 검정 글자로 '동티모르에 자유를'(Free East Timor) 메시지를 남기고, 과거 포르투갈의 식민지였던 동티모르에 대한 인도네시아의 인권침해 사례들을 고발한 다른 웹사이트로 링크도 걸어놓았다(Harmon 1999; 데닝 2005: 331에서 재인용).
- 1998년 7월, 반핵을 주장하는 Milw0rm 해커들과 애시트레이럼버잭(Ashtray Lumberjacks)라는 해커집단이 300 여 개 웹사이트 침입하여 각 사이트 방문자들이 Milw0rm 사이트로 방문하도록 하고 거기에는 "세계 평화를 유지하고 바보 같은 핵 경쟁을 멈추기 위해 노력해 달라"는 메시지(Hu 1998; 데닝 2005: 331에서 재인용).

가상 점거시위

- 가상 연좌시위(virtual sit-in)와 차단(blockade), 가상 점거 등. 가장 대표적이고 해킹행동주의라는 용어가 고안되고 처음 실행된 것도 이 방식이다.
- 가 상 연좌시위는 수많은 사람들 혹은 활동가들이 동시에 한 웹사이트를 방문해서 그 서버가 감당할 수 없는 접속량(traffic)을 유발해 다른 사용자가 사이트에 접속할 수 없도록 하면서 차단 효과를 내는 것이다(데닝 2005: 322). 그런 의미에서 조단(2002: 122)는 이를 '대중 가상 직접행동'(MVDA, Mass Virtual Direct Action)으로 부르고 이를 비폭력 직접행동의 일종으로 보고 있다.
- 두 가지 모두 일상 활동을 교란하고 어떤 시설이나 서비스에 대한 접근을 차단함으로써 시위자와 그들의 대의에 대한 관심을 환기시키는 것이 목적인데(데닝 2005: 321), 차단은 고속도로나 철도를 막아 봉쇄하면서 상품 유통을 방해하는 시위와 같은 효과를 가진다.
- 1995년 12월 21일, 스트라노 네트워크(Strano Network)가 프랑스 정부의 핵무기 개발 정책에 반발하여 처음으로 이 가상 시위를 시도 - 참가자들은 정해진 시간에 여러 정부 기관의 웹사이트들 동시 접속하여 1시간 동안 시위를 벌여 일부 사이트들은 효과적으로 차단된 것으로 알려졌다(Schwartau 1996: 407; 데닝 2005: 322에서 재인용).
- 2000년 8월 26일 통신질서법안에 반대하는 네티즌들의 시위로 정보통신부 홈페이지가 오전 12시부터 10시간 동안 '접속불능' 상태가 된 사례도 있다. 당시 진보넷 개인 컴퓨터와 서버가 사이버범죄수사대에 의해 압수되었다(최은정 2001: 361). 1999년 10월, 온라인 머그게임 '리니지' 사용자들이 서버증설과 사용자들에게 불리한 게임 규칙을 조정해달라는 요구를 하며 게임에 등장하는 캐릭터를 이용해 게임 내 시위를 벌인 일이 있었다. 집단행동을 벌이는 이 캐랙터들을 해산시키기 위해 운영자가 몬스터를 풀자 이용자들이 단결하여 순식간에 처치해버리기도 했다. 결국 게임사 측은 사용자들의 요구를 받아들였다(최은정 : 362).

태업

- 가 상 태업/방해(sabotage)이나 첨단기술 사무노동 작업장(컴퓨터) 저항을 여기에 포함시킬 수 있다. 후자의 경우 꼭 가상공간에서만 이루어지는 것이 아니라는 의미에서 가상 태업(virtual sabotage)라고 하지는 않았다. 특히, 첨단기술 사무노동자들이 작업 현장에서 컴퓨터의 물리적인 손상을 통해 업무 속도를 저하시키는 등의 일도 포함되기 때문이다.
- 가 상 태업의 경우, 이에 대한 흥미로운 그리고 성공적인 사례는 2007년 이탈리아 IBM 노동자들과 그 연대 조직들의 세컨드 라이프에서의 가상 파업이다. 이는 가상 연좌시위의 방법을 사용한 것이라고 할 수 있는데, 이것이야말로 시각적인 차원에서도 가상공간의 점거시위였다.

물량 공격

- 데닝(2005) 등이 분류하고 있는 서비스거부 공격, 전자우편 폭탄, 바이러스와 웜 유포 등이 여기에 포함된다. 이러한 방식들은 가상 점거시위와 상당 부분 겹치지만 따로 분류한 것은 그 자체의 방법이 고유하고 사이버테러 쪽으로 규정되는 경향이 강하기 때문에 구분할 필요가 있다.
- 서비스거부 공격은 위의 가상 연좌시위의 결과면에서는 다를 것이 없지만, 과정 면에서 볼 때 큰 차이가 있다. 가상 점거시위가 수많은 사람들이 공개적으로 참여하는 반면 이는 꼭 그렇지 않다. 즉, "혼자 활동하는 개인이나 소규모 단체도 인터넷 서버 무력화 위해 DoS[서비스거부] 도구를 사용"(데닝 2005: 327)한다. 일례로, 코소보 분쟁 기간에 벨그라드의 해커들은 북대서양조약기구(NATO)의 서버에 이러한 공격을 가했다. "서버가 정상적으로 작동하며 인터넷에 연결돼 있는지를 테스트하는 '핑'(ping) 명령을 통해 북대서양조약기구(NATO)의 웹 서버를 폭격했다. 그 결과 목표가 된 서버는 과부하의 상태에 빠지고 말았다"(Allison 1999; 데닝 2005: 327에서 재인용).
- 전자우편 폭탄은 가상 점거시위의 효과이기도 한 차단(blockade))의 한 형태이다. 주로 어떤 일에 대한 보복이나 괴롭힘의 차원에서 행해질 때가 많지만, 정부 정책에 항의하기 위해 사용되기도 한다(데닝 2005: 327).
    - 1998 년 소수 타밀족의 독립국가 건설을 위해 투쟁하던 LTTE의 한 분파로 보이는(Wolf 1998) 스리랑카의 타밀 반군 게릴라들이 전자우편 수천 통으로 스리랑카의 대사관 사이트들을 뒤덮어 버린 적이 있다(데닝 2005: 327-8). 당시 2주 동안 하루에 전자우편이 약 800통 보내졌다(데닝 2005: 328).
    - 1999년 '지구적 에셜론 훼방의 날'(Global Jam Echelon day) 행동 사례가 있다. 에셜론은 미국 정부가 다른 정부들의 협조로 그 곳에 도청기지를 운영하도록 하는 전세계적인 감시 네트워크이다. 에셜론은 원격통신의 접 속에 개입할 수 있고, 그렇게 확보한 내용에 대해 열쇠말 검색이 가능하게 한 것으로 알려져 있다. 이 행동은 한 날에 수많은 사람들이 '폭탄,' '해킹행동주의,' '테러리스트'와 같이 에셜론에 의해 표적이 될 만한 50개의 열쇠말을 포함한 전자우편을 발송하는 것이었다. 의심스러운 전자우편이 갑자기 증

가하면서 에셜론에 과부하를 주도록 하여, 실제 결과를 알기 힘들지만 시스템의 과열이 '내부'의 사람들에게 저항의 메시지가 전달될 것을 기대했던 것이다. 여기에 사용된 기술이라고는 50개의 열쇠말을 포함한 전자우편을 보내는 것이었다(Jordan 2002: 123-4).

  - 2002 년 미국 솔트레이크시티 동계올림픽 쇼트트랙 스피드 스케이팅 경기에서 한국의 김동성 선수가 금메달을 박탈 당하는 사건이 발생했을 때, 네티즌들이 "김동성의 금메달을 되찾아주자"는 내용의 대규모 사이버 시위를 벌였는데 약 1만 6,000통의 항의성 이메일이 미국올림픽위원회(USOC)에 보내졌고, 미국올림픽 위원회의 서버가 약 9시간 동안 마비되는 사태가 발생했다(우형진 2007: 69-70).

- 바이러스와 윔 유포를 보면, 모두 컴퓨터에 손상을 입히고 컴퓨터 네트워크를 타고 퍼지는 악성 코드의 형태로서 항의 메시지 전파, 컴퓨터 시스템에 손상 입히기 위해 사용된다. 바이러스와 웜의 경계는 모호하지만, 웜이 스스로 확산되는 자동 소프트웨어라면, 바이러스는 다른 파일이나 코드에 첨부돼 이들을 통해 전파(전자우편에 첨부된 바이러스 파일을 연다든지 하는 사용자의 행동에 의해 퍼짐)된다는 특징이 있다(데닝 2005: 337). 앞서 언급한 1988년의 미항공우주국(NASA)의 컴퓨터 네트워크에 유포된 WANK가 웜(worm)을 사용한 최초의 사이버 시위이다(데닝 2005: 337). 한국에서도 예전에 'LBC'(이병철), '신토불이' '쌀수입반대' 같은 유형의 바이러스를 통한 시위가 있었다(김강호 1997: 82-3).

<u>정보 입수, 훼손, 공개</u>

- 데닝 (2005)과 사무엘(2004)은 정보 탈취(information theft)와 같은 용어를 사용하는데, 이는 주류 미디어의 재현이 한 몫을 한 표현이라고 할 수 있다. 온라인 과 오프라인의 유사성도 있지만 큰 질적 차이가 있는데, 온라인의 새로운 현상을 이해하기 위해 오프라인의 언어를 가져다 쓰는데 생기는 문제들이 있게 된다. '해킹'이 바로 그에 해당한다. "해킹을 절도나 강도와 같은 것으로 언어 사용하는데, 훔친다고 하지만 온라인에서는 정확히 같은 복제물이 남아 있다. 즉, 훔쳤는데 안 없어지는것이다!"(Jordan 2002: 122). 따라서 여기서는 사무엘 등이 '정보 탈취'라고 분류한 사례들을 검토하기는 하지만, 그 분류 용어는 정보 탈취가 아니라 '정보 입수, 훼손, 공개'로 하였다.
- 1998년 6월, 반핵운동에 참여하는 해커집단, Milw0rm는 인도의 핵실험에 항의하기 위해 인도의 바바 원자력 연구소(BARC: Bhabha Atomic Research Center) 웹사이트의 시스템에 침입해 "만약 핵전쟁이 발발하면 당신들이 가장 먼저 고통당할 것이다"라는 메시지를 남기면서, 수천 페이지의 전자우편과 연구 문건을 입수하고, BARC의 여러 서버 중 두 서버에 담긴 데이터를 삭제하기도 했다(Glave 1998; Carter 1998a, 1998b; 데닝 2005: 331에서 재인용).
- 2001년 스위스 다보스의 세계경제포럼(WEF)에 맞서는 신자유주의 세계화 반대 투쟁에 연대한 일부 해킹활동가들이 "참가한 세계 주요 인사 1천 400명의 신용카드번호와 사용내력, 핸드폰 번호, E-mail 주소 등을 해킹하여 일부는 인터넷에 공개"했는데, 결국 신변의 위협을 느낀 포럼

참가 인사들이 떠나면서 회의가 무산되었다(최세진 2006: 79).

소프트웨어 개발 및 지원

- 사 회운동을 선언하며 해킹행동주의(hackivism)라는 용어를 만든 바 있는 해커집단인 죽은 소 숭배(CDC, Cult of the Dead Cow)는 독점 소프트웨어 기업인 M$를 계속해서 문제 삼아 왔는데, 윈도 OS의 원격 작동을 향상시키고 그 운영체제인 윈도(Window)의 보안체계가 엉망이라 사용자들의 프라이버시가 심각하게 침해된다는 점을 보이기 위해 핼티비즈모(hactivismo)라는 작업집단을 만들고 '백 오리피스'(back orifice)를 개발했다(Jordan 2002:130; 최세진 2006: 74). 전세계 해커들의 축제인 데프콘(Defcon) 3(1998)을 통해 알려진 이것은 "컴퓨터 초보자라도 윈도95와 98을 설치한 어떤 컴퓨터든 쉽게 해킹할 수 있을 정도로, 당시까지 나온 해킹 프로그램 중 가장 쉽고 가장 치명적; 가장 많은 기능을 가진 것"(최세진 2006: 75-6)이었다.
- 그 외에도 가상 점거시위를 위한 홍수넷(floodnet), 인터넷 검열의 우회와 익명성 보장을 위한 삐까부띠 Peekabooty와 토르(tor) 등이 있다.

주요 사례

코소보 사태

홍수넷(floodnet):전자교란극장(EDT: Electronic Disturbance Theater)과 전자히피 집단 (Electrohippies collective)

- 가상 연좌시위 혹은 '대중 가상 직접행동'의 방식이고, 홍수넷(floodnet)은 이를 위한 소프트웨어다.
- 이 들의 첫 시위는 1998년 9월 9일 멕시코 사파티스타 봉기에 연대하면서 주로 멕시코 세디요 대통령의 웹사이트를 공격하고, 이후 클린턴 대통령의 백악관 사이트, 미 국방성 웹사이트, 미 육군 남미군사교육단(the School of the Americas), 프랑크푸르트 증권거래소, 멕시코 증권거래소 등을 연달아 목표 대상으로 하여 시위를 벌인 일이다(Jordan 2002: 121; 데닝 2005: 322). 1만 명 참여하였고, 1분당 60만 회의 접속 시도가 있었다. 이에 대해 미 국방성은 적대적 애플릿 포함하면 사용자 브라우저에 작은 윈도 계속 열리도록 반격하였다(데닝 2005: 323).
- 홍수넷(floodnet)은 사용자의 브라우저가 자바 애플릿 소프트웨어를 내려받으면 수 초에 한 번씩 목표 사이트들에 자동으로 접속할 수 있게 된다. 더군다나 각 시위자가 목표가 된 서버의 에러 로그에 자동으로 변형된 메시지를 남길 수도 있도록 하고 있다. 예를 들어 브라우저가 대상 서버에서 '인권'이나 '민주주의'를이름으로 하는 파일을 찾도록 설정하면, 서버는 '인권이 이 서

버에 존재하지 않습니다'(no human rights found on this server)라는 메시지 혹은 '민주주의가 이 서버에는 없습니다'(no democracy found on this server)가 화면에 나타나게 하는 것이다(Jordan 2002: 121; 데닝 2005: 323). 이를 개발한 스탈바움(Brett Stalbaum, "The Zapatista Tactical FloodNet")은 홍수넷을 "활동적이고 예술적인 표현을 통해 사람들에게 힘을 주는 개념적 네트 예술"로 규정하고 있다(데닝 2005: 323).

- 1999 년 11월 말, 12월 초 미국 시애틀에서 세계무역기구(WTO) 3차 각료회의와 그에 반대하는 국제 시위와 연계해 전자히피 집단(Electrohippies collective)이 가상 연좌시위를 벌였다(데닝 2005: 327). WTO 회의를 무산시키려는 거리의 행동들과 조화를 이루며 WTO 각국 각료들을 위한 정보 흐름을 차단하는 시도였다. 전 자히피집단에 따르면(Electrohippie Collective. 2000. "Client-side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?; Occasional paper no.1"), 행동이 전개된 5일동안 45만 여 개의 컴퓨터가 이 가상 행동에 참여했고 회의 기간 동안 WTO 네트워크는 상당히 속도 저하를 겪었고 두 번의 경우에는 멈추기도 했다(Jordan 2002: 122-3).
- 전 자교란극장의 경우(그리고 시애틀 이후의 전자히피집단의 시위에서), 목표 대상 웹사이트를 폐쇄시키는 것을 목표로 하지 않았고 그 속도를 저하시키고 갑자기 증가된 접속량(traffic)이 명백하게 정치적 목적과 관련된다는 점을 부각시키면서 정치적 시위를 만들어내려는 시도였다(Jordan 2002: 123).
- 홍수넷과 같은 소프트웨어 역시 표준 DoS나 분산 Dos(분산서비스거부) 공격을 위한 것들과는 근본적으로 다르다. "그것은 어느 시스템에도 해를 끼치지 않으며 소스 주소들을 훔쳐내지도 않는다. 또 대상을 마비시키지도 않는다. 더구나 이러한 시도가 효과를 얻으려면 수천 또는 수만 명이 동시에 대상을 타격해야 한다. 사람들 다수에 의한 이러한 동시 타격은 '떼지음'(swarming)이라고도 불린다. '떼지음'은 시위 행위가 단지 한 개인 또는 작은 집단에게만 문제가 되는 것이 아님을 확실히 보여주는 수단이다"(데닝 2005: 326).
- 이 러한 가상 연좌시위는 고도의 기술을 가진 해킹행동이 아니다. 이탈리아의 넷파업(Netstrike) 같은 경우 접속량(traffic)을 자동으로 폭주시키는 소프트웨어를 만들어 공개하는 것과 동시에 다음과 같은 방식을 제안하기도 했다: '주소창에 목표 대상 웹사이트 주소를 넣고, 계속해서 새로고침(Reload)를 누르세요'(Jordan 2002: 123).

인터넷 검열의 우회와 익명성 보장: 삐까부띠 Peekabooty와 토르(tor)

- 앞 서 본 '백 오리피스'(back orifice)를 만든 핵티비즈모(hactivismo)는 또한 2002년 데프콘7에서 "국가의 인터넷 검열 맞서기 위해 검열체계 무력화하는 삐까부띠 Peekabooty 프로그램 발표하였다. '분산된 협력적 프라이버시 네트워크'를 구축할 수 있는 프로그램으로서 검열에 의해 접속이 차단된 사이트의 주소를 입력하면 그 사이트의 내용을 프로그램이 자동으로 암호화해서 이 네트워크 상에 있는 그 검열이 미치지 않는 다른 곳의 컴퓨터에 요청하고, 자동으로 이 웹사이트를 암호화해 다시 검열 지역의 사용자에게 보내주는 방식이다. 이용자 간의 연대로 검열의 벽을 뛰어넘는 방식인 셈이다(최세진 2006: 78; Jordan 2002:129). 이들은 세계인권선언

에 기초해 인터넷 검열을 목표 대상으로 삼은 것이었다.

- 토르 (tor) 프로젝트 역시 인터넷 검열을 우회하기 위해 익명으로 인터넷을 이용할 수 있도록 하는 자유소프트웨어이다. 애초에는 익명 상태의 커뮤케이션 시스템이 필요했던 미해군의 프로젝트였던 것이 개발이 중단된 이후 해킹활동가들이 계속 개발하여 널리 활용되고 있다.
- 전자문서와 전자우편을 암호화하는 소프트웨어인 '매우좋은사생활보호'(PGP, pretty good privacy)는 과테말라의 인권운동가들은 자신들이 군부의 만행을 폭로한 증인들의 생명을 보호하기도 했다(Boyle 1999; 데닝 2005: 315에서 재인용). 손전화에서 암호화된 문자를 주고받는 것을 돕는 자유소프트웨어도 있다(http://cryptosms.net).
- 인 터넷 검열의 결과 이탈리아의 해킹활동가/활동가 웹사이트인 넷파업(netstrike)이 2001년에 사법 당국(magistrates)에 의해 압류당하는 일이 벌어졌는데, 거의 즉각적으로 다른 나라들에서 그 넷파업의 사이트가 복제되고 미러링(mirroring)되면서 이탈리아의 일국적 사법 권한을 벗어날 수 있었다. 또한 웹사이트의 파일들이 패키지되어 누구나 그 사이트를 미러링할 수도 있게 하여 한 곳의 미러 사이트가 폐쇄당하면 다른 곳에서 또 만들 수 있게 한 것이다.

해킹행동주의의 특징, 한계, 함의

<u>행동의 성과에 대한 판단, 해킹행동의 고유한 특질의 문제</u>

- 실제로 이들 행동의 성과는 무엇인가. 조단은 해킹행동의 한계로 이 행동의 의미가 반대편에게도 명확할 것인지는 확실하지 않고, 사이버 공간에는 지나가는 사람이 없다고 지적한다(Jordan 2002: 125).
- 또 한, 거리에서의 시위나 현장의 투쟁이 형성하는 직접 접촉을 통한 연대감의 형성이 사이버 점거시위와 같은 해킹행동에는 부족하다고 지적한다. 가상 시위 참여자들이 얼마나 많은 사람들이 동시에 참여하고 있는지 알지 못하는 경우조차 많다(Jordan 2002: 125).
- 조단은 또한 직접행동으로서 이것이 갖는 한계를 지적하고 있다. 세계무역기구(WTO) 반대 시위가 거리에서 그 회의를 중단시키기 위한 것처럼 가상 세계에서의 연좌시위는 (WTO 웹사이트에서의) 정보의 흐름을 중지시키는 차원에서 같은 직접행동으로 볼 수 있지만(Jordan 2002: 126), 직접행동으로서 명확하게 기능하는 것은 아니라고 본다. 사이버 스페이스에서는 대상들이 쉽게 복제될 수 있기 때문에 현실 세계에서의 거리나 도로를 봉쇄하는 것보다는 직접행동의 효과가 약하다는 것이다. 반면, 해킹행동주의를 포함한 온라인 직접행동은 직접행동으로서 보다는 상징적 시위로서 보다 더 큰 효과를 가진다고 할 수 있다: 정보 코드의 위반(Jordan 2002: 126-7).
- 그렇다고 할 때, 내용 층위, 논리[코드] 층위, 물리적 층위(레식)에서 코드 층위에서의 저항 방식 - 정보 코드의 층위에서 놀면서 새로운 행동주의적 정보 정치(학)와 새로운 시위 형식을 창출하는(Jordan 2002: 135) 놀이투쟁(Söderberg 2007)으로 그 고유한 특질을 이해할 필요가 있

다.

공개적인 해킹행동이자 집단행동 지향

- "대부분의 해킹은 익명의 개인 혹은 소수 그룹의 차원에서 은밀하게 이루어질 수밖에 없"고 "해킹 자체가 공격적이고 파괴적인 행위이기 때문에 사회적 공감대를 폭넓게 얻어내기 힘들다는 태생적 한계"(민경배 2006: 110)를 지적하기도 하지만, 해킹행동주의는 사회운동과 연계하여 공개적으로 진행되는 특성이 있다(최세진 2006: 79). '홍수넷'의 사례에서와 같이, 공개적으로 대중들의 참여를 통해 이루어지는 것을 하나의 전술적 원칙으로 삼기 때문이다.
- 조단은 "대중 가상 직접행동(MVDA, Mass Virtual Direct Action) 해킹활동가들은 단순히 목표 대상 사이트의 정지가 아니라 수많은 사람들을 관여시키는 것을 추구한다. 대량의 사람들이 핵심인데 왜냐면 한 사람의 기술적 능력에 대한 것이 아니라 시위하겠다고 하는 수많은 사람들의 선택에 대한 것이기 때문"(Jordan 2002: 125)이라고 말한다. 즉, 사람들이 관심을 가지고 참여를 하지 않는다면, 그리고 이를 위한 충분한 토론과 사전 조율 혹은 사후 평가의 과정이 없다면, 소수에 의한 서비스거부 전술 같은 것은 정치적 해킹행동으로 지지 받을 수 없게 되는 셈이다.
- 다른 한편, 해킹 및 해커공동체를 범죄시하는 분위기에서 이들의 공개 활동은 위험을 수반한다는 점을 고려해야 한다. 이러한 사정에 대해 로즈(Ross 1990)는 "그 기술정치적 하부구조가 점차적으로 보다 대규모의 감시에 의존하는 사회에서, 사이버네틱 행동주의는 필수적으로 은밀한 정체성의 정치에 보다 많이 의존한다. 폐쇄 시스템에 접근하는 것은 분별력과 시치미를 필요로 하기 때문"이라고 지적한다. 즉, 가상 시위의 전술적 특성 때문에 일정하게 익명과 폐쇄적인 진행 과정은 인정할 수밖에 없다는 것이다. 문제는 그것이 저항 운동임을 명확하고, 이를 통해 불법으로 간주될 수는 있으되, 우리는 해킹행동(주의)를 범죄나 테러로 혼동하지 않을 수 있다.

운동의 참여자들 및 사회운동과의 조율과 논쟁

- 지 금까지의 사례들을 보면 정보 정치(학)의 사안들을 넘어 확장된 해킹행동주의는 반전, 인권, 반핵, 반자본주의 등을 의제로 한 사회운동과 투쟁 과정에 결합해 이루어졌다는 특징을 보여준다. 물론 사회운동 조직 내부에 존재하지 않고, 독립적인 해커집단이 자체적으로 기획하고 실행한 것이라는 점에서 사회운동 조직과 그 방법을 놓고 논쟁이 벌어지는 일이 빈번하다. 여기서 중요한 것은 논쟁이다. 많은 해킹활동가들은 행동 이전과 이후에 인터넷 등을 이용한 논쟁을 요청한다. 이들의 정치적 목적은 많은 사람들이 관여하도록 하고 그들을 토론에 끌어들이고 성찰하고 행동하게 한다는 점에 있기 때문이다(Jordan 2002: 125).
- 그 래서 이러한 논쟁의 배치는 해킹행동이 자칫 소수 기술활동가들의 기술 능력을 과시한다거나 파편화된 개인들의 행위로 그치고 마는 것이 아니라 "여하간의 이유로 시위 참가를 할 수 없는 수많은 사람들에게 참여 기회를 제공하면서 운동을 구축하는 것"(Jordan 2002: 125)이 될 수 있다.

국가 단위 혹은 국제적인 사건으로 등장하는 경우가 많았다.

- 정 보운동 차원의 해킹행동주의는 전자문화, 가상세계, 사이버스페이스 등에서 보안, 프라이버시, 특히 검열 같은 사안들이 국가 권력과 직접 관련된 것이라는 점, 그리고 가상세계를 넘어서는 현실의 사 회운동과 결합되기 시작한 1990년대 후반에는 신자유주의 세계화에 반대하는 국제행동이 등장하고 1990년대 후반의 코소보 사태, 2000년대 초반의 이라크 침략 전쟁을 비롯한 전쟁이 발생한 시기와 맞물렸던 역사적 맥락에서 이는 자연스러운 일이다.
- 이 때, 국가간 전쟁이나 분쟁의 상황에서 해킹행동이 동반될 때 종종, 해킹의 피해자들이 해킹의 책임을 실제로 해킹을 실행한 소규모 해커 집단이 아닌 그들의 정부로 돌리기도 하는데(데닝 2005: 335-6), 해킹행동주의가 민족주의 정서와 친연성을 갖는 한계를 보기도 한다.
- 그 러나 인터넷 검열의 경우를 보면, 이탈리아의 넷파업(netstrike) 사이트에 대한 미러 사이트 지원 활동처럼 보통 국가 단위의 법제도를 통해 인터넷 검열이 자행되는데 이에 대항하는 해킹 행동들은 보통 국제적인 지원과 연대의 형태로 이루어진다.

전술의 잠재적 폭력성 및 위험에 대한 논란

- 가상 점거시위 등의 온라인과 네트워크 시스템의 약점을 이용한 정치적 (직접)행동이 보통 약한 사이버테러 형태로 받아들여지고 있는 물량 공격(서비스거부, 전자우편 폭탄 등)과 구분이 애매하다는 점이다.
- 해 킹행동주의의 하나의 방식(가상 연좌시위 및 차단)이 정보의 자유로운 흐름을 차단하여 정보 접근을 막을 수 있고, 심지어 검열을 불러들일 수 있다. 즉, 서비스거부 공격을 활용함으로써 해킹활동가가 선택한 폭력은 검열을 구성한다는 점이다(Jordan 2002: 126).
- 해킹과 저작권의 관계: 해킹이 저작권을 강화시킨다? 의도하지 않게 최소한 그 빌미를 제공한다.
- 반면, 해킹 일반이나 해킹행동주의가 발생시키는 일반적인 효과 중의 또 하나는 이러한 행위나 행동을 통해 네트워크 시스템이 기본적으로 불안정성하다는 점을 상기시킨다는 점에도 주목해야 한다.

해커들의 계급적 성격

- 해 킹행동주의를 검토하는 글들을 보면, 해커 혹은 해커 활동가들의 계급적 성격이 모호하다는 이유로 해킹행동주의가 기술 사회운동으로 자리잡을 수 있을지 의구심을 던지고 있다. 이광석 (1998)은 능력있는 여성 해커를 전혀 볼 수 없다는 점, 일반적으로 10대들이고 생업에 종사하지 않는 대학생들이라는 점, 해커들 대부분이 해킹을 게임으로 생각한다는 점, 그들 스스로가 엘리트이고 무언가 그들이 특수하다고 느끼며 서로의 능력[만]을 인정해준다는 점 등을 그들의 계급적 특성으로 묘사하면서 남성적, 경제적, 교육적, 제1세계적, 백인의 특권 속에 있는 그들이 "과연 대안의 주체가 될 수 있는지는 미지수"(80-2)라고 하였다. "이들의 불분명한 계급적 성격

은 사회운동으로서의 핵티비즘의 정체성을 모호하게 만든다. 서구의 경우 대부분의 해커들은 10~20대의 백인으로 중류층 이상에 소속되어 있는 사람들"(민경배 2006: 110)이라는 것이다. "끊임없는 조직과 선전, 교육, 토론 등으로 준비하고, 생존하고, 투쟁하는 대중투쟁과는 달리 소수의 결의와 활동으로 인한 공격 전술"로서 테러리즘과 유사하다는 점과, 더불어 위와 같은 해커들의 사회경제적 출신배경에 따라 "부르주아 백인들의 사회적 반항일 뿐 계급 운동으로 보기는 무리 있다는 평가"(최세진 2006: 81)를 전하기도 한다. 한국의 해커 주체들도 인종의 문제를 빼면, 그리고 중간계급의 속성이 다를 수 있다는 여지를 남겨두고, 크게 다르지 않을 것이다.

- 하지만 기술문화에 대한 비판과 대안 기술에 대한 접근 그리고 하위문화 정치의 고유한 저항 형식들에 대한 고찰없이 기존의 사회운동의 관점과 구도를 그대로 유지한 채 해킹, 해커문화를 바라본다면 그 계급적 성격은 계속 모호할 수밖에 없다.
    - 우선 로즈(Ross 1990) 역시 그러한 점을 토론하고 있는데, 문화적 '저항'의 특정한 형식들의 정치적 의미는 있는 그대로 드러나지 않는다고 지적하면서 "특히, 좌파들은 성숙한 정치적 헌신을 표하지 않는 문화적 표현의 힘을 알아차릴 수 있는 문화정치의 부재를 겪어왔다. 마찬가지로 지난 20여 년간 전문영역에서의 행동주의의 성장이 보여주는 것은, 해커 충동을 그 계급적 구성 하나만을 놓고 경멸하는 것은 실수라는 점이다. 엘리트 집단이 불공정하게 기술주의 지식에 대한 특혜받은 접근을 즐길 것이라는 점 때문에 '앎의 능력'을 외면하는 것은 미래의 너무 많은 것을 외면하는 것"(Ross 1990)이라고 말하고 있다.
    - 다른 한편, 60년대 미국 메사추세츠공대(MIT)에서 발원한 엘리트 해커공동체나 청소년 하위문화나 청소년범죄로만 해킹과 해커문화를 바라보기 때문일 수도 있다. 실제 노동과정 및 작업장 - 첨단기술 사무노동자와 탈숙련노동자 - 에서의 수많은 비조직적인 형태의 태업과 작업 방해의 해킹이 존재함에도, 이에 대해서는 조사 분석이나 연구, 저항의 조직화를 위한 실천적 작업들이 거의 없는 듯 하다.

해킹행동주의에서 해킹문화운동으로!

- 지 금까지 해킹행동주의의 사례들과 그 특징, 한계를 짚어보았다. 그런데 애초의 핵, 해킹, 해커공동체의 역사적 의미를 되새겨 보면, 지금까지 다룬 컴퓨터 네트워크 시스템에 대한 침입을 중심으로 한 의미는 좁은 (그리고 지배 미디어의 지배적 재현을 따르는) 의미라면, 조단(Jordan 2002)이 간단하게 정의하듯이 "기술의 혁신적인 사용"(120), 풀뿌리 기술 개발과 활용 활동으로 해킹 개념을 확장하여 사용하는 것은 어떨까?
- 아래에서는 해킹행동주의가 갖는 직접행동의 특징에서 그것이 꼭 직접행동의 정치투쟁 현장에만 국한될 필요가 없다는 점, 더 나아가 직접행동 보다는 좀 더 일상적이고 지속적인 문화행동과 문화운동의 차원에서 해킹행동주의 원리가 적용될 수 있다는 차원에서 나는 해킹행동주의의 확장으로서 해킹문화운동을 주장하고자 한다. 지금까지 선의든 악의든 해킹, 그리고 해킹행동주의

가 기술 엘리트나 전문 기술활동가의 몫이나 (전문) 영역으로만 규정되어온 것을 벗어날 수 있다면 말이다.

해킹: 작업장에서의 노동자 저항

- 해킹행동주의가 엘리트 중심의 해커나 청소년 하위문화만이 아니라, 다양한 노동 관계를 재구축하려는 노동자 투쟁과 문화 투쟁의 과정에서 어떻게 적용되어 왔고 확대되고 있는지 살펴볼 필요가 있다. ... ...
- " 대부분 여성인 사무직 노동자의 주류 일상생활에서 매년 더 많은 끊임없는 컴퓨터 '다운타임'과 정보 손실을 설명하는 넓게 확산된 비조직적 태업/방해의 문화가 있다. 데이터 저장과 운영체제에 대한 그들의 공학적으로 전자기적인 공격에서 사무 노동자들에 의해 채택되는 태업, '시간 절도,' 전략적 업무 방해(monkeywrenching)는 시간의 심기(planting of time) 혹은 논리 폭탄에서부터 전자기적 테슬라 코일(Tesla coil) 혹은 단순한 신체적 마찰의 분리된 사용까지 있을 수 있다"(Ross 1990).
- "몇 안되는 컴퓨터 이용자들만이 스스로를 '해커'라는 명칭 아래 자기를 인지하고 포함시키고 있는 동안, 시스템 분석가, 디자이너, 프로그래머, 작동자의 카스트 체계를 가로질러 가는 해킹에 대한 제한된 정의를 확장하여, 그들이 얼마나 비전문적인지와 무관하게, 그들의 노동 일정의 시간성을 결정하고 교환의 사회적 네트워크에서 그들의 위치를 지시하는 구조화된 커뮤니케이션의 부드러운 흐름에 개입하여 뒤집어놓고 방향을 뒤바꿀 수 있는 모든 첨단 노동자들을 포함시키는 것에 충분한 근거가 있다"(Ross 1990).
- 그런데, 잘 알려지지도 않고 연구가 되지도 않은 다양한 노동 현장, 작업장에서의 해킹과 같은 행위는 비단 개인적인 태업과 같은 수동적인 저항의 형태만을 갖는 것이 아니다. 1970년대 이래 탈숙련화되어온 노동과정 속에서 노동자들의 재숙련화와 이를 위한 다양한 기술 습득, 노동과정에 대한 노동자들의 자율적 기술 활용이라는 적극적인 저항의 형태까지 이러한 작업장에서의 노동자 해킹에 포함될 수 있기 때문이다: "기술적 재숙련화의 희망에 의존하고 있는 직업 위치 상에서, 그들에게 커뮤니케이션의 합리성에 대한 태업이나 방해가 덜 사용되고, 그들에게 파괴적/해체적이기보다는 재구축하는 해킹의 정의가 더 적합한 수많은 사회적 수행자들이 있다. 적절한 예는, 자동화와 탈숙련화에 대항한 노동자 투쟁에서 노동자들의 기술 리터러시의 결정적인 역할이다"(Ross 1990).
- 해킹이라는 사회적이고 개인적인 행위는 사회의 생산관계 내의 다양한 계급 관계 속에서 존재하고 있다. 따라서 해커문화 혹은 해킹행동주의의 시야를 넓힐 수 있다면, 그리고 이에 대한 좀 더 심도깊은 성찰, 연구, 이론의 작업이 가능하다면 이는 지금까지 누락된 혹은 절합되지 못한(해킹 - 노동자투쟁) 우리의 실천의 주제가 된다.

온-오프라인 사회운동과 대중 해커행동

세계 곳곳의 대중투쟁에서 사회적 미디어 활용과 온라인 지원 활동

- 보 다 엄밀한 분석이 필요하지만, 적어도 2000년대 이후 세계 곳곳에서 터져나온 네트워크된 대중투쟁 과정에 서 발견할 수 있는 공통점은 인터넷과 모바일 미디어가 적극 활용되고 있는 동시에 이들 인터넷과 모바일 네트워크에 대한 정치권력의 검열과 통제가 빠짐없이 일어난다는 점이다. 그에 따라 대중투쟁이 커뮤니케이션 미디어의 정치적 활용(해킹행동 포함)과 그에 대한 통제 자체가 그 대중투쟁의 (최초의 계기는 아니더라도) 주요 사안이나 의제로 포함되는 경향을 볼 수 있다. 2009년 여름에 일어난 일들만 보더라도 이란, 온두라스, 중국(위구르) 그리고 한국 등에서 인터넷과 모바일 네트워크에 대한 정치권력의 통제는 빠짐없다.

2008 촛불시위와 대중 해킹행동

- " 우리나라의 경우, 소수의 해킹공격보다는 다수가 참여하는 온라인 시위 형태를 띠고.. 각종 사회 이슈 때마다 다양한 온라인 토론을 함께 진행하면서 때때로 실제적인 대중행동으로 연결시"키는 방식이 주종을 이루었는데(최세진 2006: 81-2), 2008년 촛불시위는 모두가 말하듯 그 절정을 이뤘다. 온라인과 오프라인이 지속적으로 결합되어 진행된 그야말로 네트워크된 시위 형태였고 다양한 형태의 해킹행동들이 나타났다.
- 5월 31일~6월 1일 경찰기동대의 잔인한 시위대 폭력진압 직후 경찰기동대 웹사이트 해킹: 웹사이트 지저분하게 하기(defacement)
- 전자우편 폭탄 보다 더 나아간 것으로, 한나라당 국회의원에 정치 후원금 18원 보내기
- 광고지면불매운동 차원에서 조중동에(만) 광고 내는 기업의 웹사이트에 대한 대량 접속과 다대1의 집단 항의 전화
- 6월 10일, 백만 집회의 사회자가 네티즌들에게 청와대 웹사이트 항의 접속을 요청하여 청와대 웹사이트 서비스거부 발생
- 게임 해킹을 통한 게임 변형(mod)과 패러디
- 2008년 12월 26일 언론노조 총파업 출정식 참가자들과 네티즌들의 한나라당 의원들을 향한 집단 문자 발송
- 이 렇게 볼 때, 2008 촛불시위의 전술 미디어 행동에서 가장 두드러졌던 인터넷 생중계는 거리시위와 온라인 시위 및 해킹행동을 연결시키는 중요한 매개로서 중요한 역할을 한 셈이다. 그럼으로써 해킹행동주의의 한계로 지적된 연대감의 부재나 개별화의 문제를 실시간으로 거리와 온라인을 연결시킴으로써 극복했다고 볼 수 있다.
- 이와 같이, 가상 점거시위 혹은 대중 가상 직접행동(MVDA, Mass Virtual Direct Action)은 2008년 촛불시위에서 상당히 중요한 대중 시위 전술로 창조적인 방식으로 사용되었다. 전문적인 해킹활동가에 의한 고도의 기술을 사용한 차원이 아니라, 대중적인 해킹행동이 활발하고 적극적이었다는 점이 2008년 촛불시위를 특징짓는 또 하나의 특징이었다.

카피레프트, 자유오픈소스소프트웨어운동, 열린 문화생산

- 정 보 자본주의 사회에서 생산수단 통제의 지배적 형식으로 재산에서 임대로 이동하고 있다: 상표, 특허, 저작권 등의 라이선스 체제(Söderberg 2002). 즉 접근의 시대 혹은 소유의 종말 시대(리프킨)에서는 그 접근을 막거나 통제하는 것으로서 지적재산권이 작동하고 있는 것이다. 생산력과 일반지성을 족쇄 채우고 있다.
- 재산에서 라이선스로 생산관계가 재편되고 있는데(Söderberg 2002), 이미 자유소프트웨어운동은 그 라이선스의 대안을 만들어왔다. 그누 일반공중문서(GNU GPL)의 함의(Söderberg, 2007: 19-21)
    - 사적 재산의 작동 방식에 직접 개입하는 것이다.
    - 개별화하는 저작권을 집단적 권리로 만든다.
- 정보는 저작권 없이는 어떠한 교환가치도 갖지 않는다. 하지만 저작권 없이도 사용가치는 가지고 있다. 교환가치를 당장 확보하지 않더라도, 바로 이 사용가치를 위해 생산하는 수많은 정보생산자들이 있다(Kleiner 2007).
- 집단적이고 개방적인 개발 과정 - "생산자-이용자 공동체"
    - 필요에 의한 생산: 자유소프트웨어 생산자들은 사람들이 필요하기 때문에 생산하지, 시장에서 교환할 목적으로 생산하지 않는다.
    - 생산물에 대한 보편적 접근 허용: 자유소프트웨어를 사용할 수 있는 권리는 그 공동체에 기여(노동)한 사람에게 주어지는 것이 아니라 그 소프트웨어를 필요로 하는 사람 모두에게 주어진다(접근이 허용된다).
    - 비시장적, 공동체 관계: 자유소프트웨어 공동체는 비시장적 관계(nonmarket relations)를 유지하면서도 전세계적으로 자유로운 생산자들의 협동 노동을 이끌어 내며 끊임없이 발전한다.
- 독점 소프트웨어에 맞선 새로운 정보 생산과 유통의 흐름을 만들어 내고 있다.
- 노동관계 조직화의 대안적 모델(Söderberg, 2007: 2-3)이 되고 있다: 시장 교환의 제약 외부에서 노동의 자기조직적 구성권력 방식, 자발적 진입과 집단적 노동 활동의 새로운 노동 주체성, 놀이투쟁

- 한 국의 경우 그누 일반공중문서(GNU GPL) 라이선스, 그누/리눅스(GNU/Linux) - 자유소프트웨어운동, 리눅스 오픈소스소프트웨어 개발 등의 영향으로 1990년대 초중반부터 정보연대(SING)의 활동을 시작으로 사회운동의 맥락에서 카피레프트운동이 본격화된다. 그런데 이것이 시작된 미국과 다른 특이한 점은, 한국의 카피레프트운동은 해커공동체와 거의 아무런 관계를 형성하지 않은 채 시작되고 지속되었다는 점이다. 말하자면, "해커의 윤리와 강령"의 핵심인 "정보의 자유와 권력의 해체" 곧 "디지털 정보 독점에 대한 저항과 자유로운 유통의 정신"(이광

석 1998: 80)은 카피레프트운동의 원칙에 다름 아닌데, 윤여상(2001)이 "정보 운동으로서의 카피레프트는 정보 생산의 중요한 실천자인 해커들과 연관성을 가져야 했으나, 이 실천자들을 도외시하고 이론적 자원만을 가져와 지적 재산권 철폐 운동에 결합시킴으로써 적극적인 실천자를 잃어버린 운동으로 전개되었고 모호한 상태에서 제대로 확산되지 못했다"고 지적하고 있듯이, 가장 적극적인 (잠재적) 실천 주체들과의 연계없이 카피레프트운동이 이론적인 실천으로 이루어져왔다고 볼 수 있다.

    - 왜 카페리프트운동에서는그렇게 하지 않/못했을까? 나의 추측은 이렇다(이 내용은 '풀뿌리 커뮤니케이션 연구모임' 블로그에 있는 것을 가져온 것이다 http://hack.jinbo.net/?p=46): 윤여상(2001)이 “우리나라의 경우 좌파적 진보 진영에서 반저작권 운동의 일환으로서 스톨만의 카피레프트를 이론적 기반으로 받아들여 좌파적 정보 운동과 결합시키려 하고 있다. 이것은 1990년대 중반 이후 학생 운동과 좌파적 진보 진영의 침체와 맥을 같이 한다”고 진단한 것을 받아들인다면, 당시 학생 운동과 좌파적 진보 진영 일부가 카피레프트운동을 주창하고 나설 때, 그들의 운동권 문화가 해커문화와 잘 조응하지 못한 것은 아닐까. 부족하나마 자유소프트웨어 혹은 공개소프트웨어를 개발하는 해커들도 없지 않았던 것 같고 네트워크를 침입하는 실력을 가지면서도 사회 문제에 관심을 갖는 해커가 없지 않았을 텐데, 공통의 이념을 형성할 가능성이 있다 하더라도, 조직화나 운동/실천의 방식에서 서로 궁합이 맞지 못했던 것이다. 사실 지금도 운동권의 조직 문화는 그것이 맞서 싸우려는 권력이나 시스템을 닮아 있으니, 당시 운동권의 입장에서는 개인주의 문화를 갖기 보통인 해커공동체를 운동 주체로 보기는 쉽지 않았을 것이다.

- 소프트웨어, 하드웨어에서 네트워크 문화생산으로 - 문화 콘텐츠(음악, 영화, 게임 등), p2p 생산, 오픈소스 프로젝트 등으로 확장되어왔다.
- 패러디를 위한 저작물 무단사용 역시 문화적 해킹이라고 할 수 있다. 그에서 더 나아가 오프소스 프로젝트, 오픈콘텐츠운동이 진행독 있다: 새로운 방식의 디지털로 네트워크된 협력창작
- 다 시 한 번 햌 혹은 해킹의 애초 어원을 되돌아 보자: "작 업과정 그 자체에서 느껴지는 순수한 즐거움 이외에는 어떠한 건설적인 목표도 갖지 않는 프로젝트나 그에 따른 결과물"(레비 1996: 22). 주로 이 은어를 사용한 공동체는 컴퓨터 기술과 관련된 엘리트 하위문화 공동체였지만, 이 말 자체는 반드시 기술에만 국한되어 사용된 은어는 아니었다는 점이다. 그리고 위에서 보았듯이 자유로운 소프트웨어 개발과 공유의 과정이 소프트웨어 영역만이 아니라 다양한 대중 문화생산 과정에도 폭넓게 적용될 수 있고 되고 있다는 점은 이를 잘 드러낸다. 다른 곳에서 보았듯이, 현재 전세계의 다양한 해커공동체들과 해킹활동가들은 시스템 해킹 보다는 하드웨어나 전자제품, 의식주와 관련한 생산물들에 대한 해킹을 하고 있기도 하다. 그야말로 문화해킹을 통한 해커문화의 확산인 셈이다. [이와 같은 여기서 문화-경제적인 측면의 해킹, 해커문화에 대한 본격적인 논의는 별도의 논의가 필요하고 이는 다른 기회를 통해 정리할 예정이다.]
- 덧붙여, 좀 더 자세한 조사가 필요한 얘기이지만 한국에서 해킹, 해커문화에 대한 연구는 1990

년대 중후반에 몰려 있고 그 이후의 변화 상황에 대한 연구는 정보통신공학이나 범죄사회학 차원 이외에는 거의 없다. 북미와 유럽의 경우에도 1990년대 비교적 많은 연구들이 있었고 2000년대 초중반까지 해킹행동주의에 대한 연구가 있다가 최근에는 별로 없는 반면, 자유오픈소스소프트웨어운동을 비롯해 공격적 해킹보다는 생산적 해킹, 이 글에서 말하는 해커문화에 대한 연구들은 점차 많아지고 있다.

해킹문화운동: 지배 기술문화의 근본 독점 깨기!

- 역사적으로 지배계급의 지배를 위한 기술의 도입에 저항한 형태는 크게 두 가지로 볼 수 있다: 기계 파괴(러다이트) + 대안 기술의 개발
- 넓은 의미의 해킹을 후자로 재정의해야 한다.
- 프 리킹과 해킹이 전화 기술과 컴퓨터 기술을 통해 본격적으로 등장했다는 점은 특기할 만하다. 전화와 컴퓨터의 결합이 인터넷이고 인터넷은 현재의 디지털 네트워크 기술문화를 대표하고 있다. 디지털 네트워크 기술은 자본주의 체제 전체를 새롭게 재구축하는 기술이다: 정보 자본주의 사회.
- 해킹은 필연적인 것이다. 해킹은 게속 발생해왔고, 계속 발생할 것이다. 왜냐하면, 인간과 시스템에 대한 하나의 커뮤니케이션 방식이기 때문이다. 해킹이 절대 없는 사회라는 것은 곧 오류없는 시스템의 전일적인 지배가 관철되는 사회에 다름없다. 이런 사회가 존재하기는힘들다는 점에서 해킹은 필연적이다.
- 이를 정보 자본주의 사회에서의 저항과 대안 사회를 만들어나가는 운동으로 정치화할 수 있어야 한다. 이를 위해서 나는 해킹문화운동을 제안한다.

해킹문화운동: 목적과 지향

'해킹문화운동'을 통해 무엇을 어떻게 하려는 것인가? 크게 두 가지 운동의 목적이자 지향을 제시할 수 있다.

우리가 살고 있는 현재의 정보 자본주의 사회의 지배적인 기술문화의 근본 독점을 깨기 위한 것이다.

- 근본 독점(radical monopoly)이라는 개념은 이반 일리히(Ivan Illich)가 제시한 것이다.
    - " 일반적으로 '독점'하면 하나의 기업이 생산수단이나 상품 또는 서비스를 배타적으로 통제하는 것을 뜻"(일리히 2004: 90)하는 반면 '근본 독점'은 "하나의 브랜드가 지배하는 상태가 아닌, 한 가지 유형의 생산물이 지배하는 상태이다. 근본적인 독점은 산업생산의 과정이 절실한 필요의 충족에 대한 배타적인 통제를 행사하며 비산업적인 활동을 경

쟁에서 축출하는 상태"(91)다.

    - "근본적인 독점은 강제적 소비를 부과함으로써 개인의 자율성을 제약한다. 근본적 독점은 특수한 종류의 사회통제를 구성하는데, 이는 표준 생산물을 생산하고 강제로 소비하게 만드는 일은 거대 제도만 할 수 있기 때문이다"(91-2).

- 해 킹문화운동의 목표는 이러한 근본 독점을 깨는 것이다. 기술이 별도로 존재한다기보다 현재의 정치, 경제, 금융, 문화, 언론 등(이번에 분산서비스거부를 사태를 겪은 사이트들만 보더라도)의 사회적 제도 및 공공 영역, 사적 영역 모두 컴퓨터와 네트워크가 매개하는 기술사회임을 놓고 볼 때, 그러한 제도가 갖는 근본적 독점은 곧 기술을 통해서 더 확고하게 굳혀져왔다. 더군다나 현재의 정보 자본주의 사회 혹은 신자유주의가 지배하는 사회는 정보기술을 그 핵심적인 사회운영 원리에 배치하고 있다.
- 이러한 정보기술은 곧 소프트웨어의 형태로 작동하는데, 편재하는 컴퓨팅 기술 환경과 생활 곳곳에 스며들어가 있는 소프트웨어들은 곧 우리의 "사회적 상호작용과 커뮤니케이션 방식을 (재)형성"(Kranenburg 2008: 33)하고 있다. 이렇다고 할 때 오히려 "절도 행위는 사람들이 공유하는 장치들과의 상호작용에 대한 그들 자신의 구상(scheme)을 재사용하고 재창조할 수 있는 권리를 빼앗는 곳에 있다"(Kranenburg 2008: 33)는 것이 맞다. 다시 말해서, "지적재산권(특허, 상표, 저작권), 복제방지 기술, 문서 포맷에 대한 특허, 하드웨어에 대한 특허"(Suoranta & Vadén 2008: 63) 등이 바로 그러한 인위적인 희소성의 조장을 통한 절도 행위나 다름 없는 근본 독점을 만들어 내고 있기 때문이다. 그런 의미에서 해킹, 특히 생산적 해커공동체가 소프트웨어 개발의 영역에서 본격적으로 불붙었다는 점도 의미심장하다. 해킹문화운동은 이를 소프트웨어 영역과 함께 기술문화 전체에서의 바로 이러한 인위적인 희소성의 논리와 산업 제도를 깨고 들어가는 것을 지향하는 저항문화운동이다.
- 그 와 동시에 해킹문화운동은 결코 소수 전문가 해커들에 의한 것이 아니라, 대중 문화(운동)의 접근이 필수적이다. 왜냐하면 "어떠한 기술적 불가결성, 새로운 통제 기계의 도입도 이전의 대중의 욕구와 욕망과의 상호작용, 대중 동의의 격전장에서의 어느 정도의 협상 없이는 존재하지 않"(Ross 1990)기 때문이다. 일리히의 말로 하자면, 일반적인 독점은 그 독점의 소수 기업이 문제이지만, 근본 독점은 대중의 문제이기 때문이다. "근본적 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"(일리히 2004: 96). "70년대 초기에 해킹 전문지식으로부터 나온 PC가 '구축'된 것은 바로 이런 종류의 대중 관념에서이다: 거대하고, 비개인적이고, '폐쇄된' 하드웨어 시스템에 대한 불신 주위에서, 그리고 상호개인적 커뮤니케이션을 촉진하는 작고, 탈중심적이고 상호작용적인 기계에 대한 욕망 주위에서 형성된 대중 관념 말이다"(Ross 1990).
- 따라서 현재의 지배적 기술문화의 근본 독점을 깨는 것은 앞서 살펴본 해킹의 확장된 형태로서 사회적 해킹 또는 문화적 해킹 혹은 (고립된 기술운동만이 아니라) 해킹문화운동을 통해 가능하다. 즉, 근본 독점의 문제 상황을 드러내고 그것을 깬다는 것은 그러한 지배적 기술과 문화에 의존하지 않고도 살아갈 수 있는, 일리히가 말하는 공생공락의 사회를 만들어가기 위한 도구(tools for conviviality)를 손수 만들고 사용하며 나누어서 발전시키는 것까지를 포함한다. 비판과 대안

을 함께 해나가는 것은 이미 해킹의 뿌리에서부터 존재해온 것이라고 할 때, 그에 기반을 두고 "지구적으로 연결되고 접근이 제한된 정보 시스템의 요새화된 네트가 중앙집중적 통제로부터 이윤을 창출하려는 자들의 '의도'적 환상인 것만큼이나 공중 데이터 네트워크, 게시판 시스템, 대안 정보와 미디어 링크, 점차 저렴해진 데스트탑 출판, 위성 장비들과 국제적 데이터베이스는 국지적 정치적 '의도들'의 결과였다"(Ross 1990)고 할 때, 그 국지적인 정치적 의도들 혹은 공생공락은 특히 자율적인 생산공동체로서의 자유소프트웨어운동을 염두에 둔 소더버그의 '놀이투쟁'(play struggle)과도 맞닿아 있다. 이러한 자율적 문화생산, 공생공락의 도구와 놀이투쟁으로서 그리고 현 정보 자본주의 기술문화에 대한 비판과 대안 기획으로서 해킹문화운동을 주창하는 것이다.

근본 독점을 깨기 위한 보다 구체적인 실행 목표로서 기술의 누드화 작업이 필요하다.

- 후 기 디지털 시대라는 말들이 나온다. 눈 앞에서 계산과정이 사라지고 디지털이 사라지고 있기 때문이다. 여기서 사라지는 기술은 침투하는 컴퓨팅, 편재 컴퓨팅(ubicomp), 환경 지성, 조용한 기술 등과 같은 말이다(Kranenburg 2008: 19-20). 기술이 점차 환경이 되고 환경이 (인간과 인간, 인간과 기계, 기계와 기계 사이의) 인터페이스가 되는 상황이다. 이 때, 보이지 않는 기술, 비가시적인 기술에 의한 대량 감시(mass surveillance) 시대가 된다.
    - "GPS, RFID 칩들, 폐쇄회로 텔레비전, 휴대폰 위치추적 장비, 유/무선인터넷 등은 현대 권력의 폭력성과 촉수를 숨기기엔 안성맞춤이다. 이들 디지털 장비들은 일종의 탈중심화된 권력 촉수가 되고, 일단 'u-'로 연결되어 공간 기동성을 부여받게 되면, 이들 촉수들을 관리하는 권력의 중앙 상황 조정실의 위치를 가늠하기가 힘에 부친다"(이광석 2009: 185).
- 감 시와 통제가 눈 앞에서 사라지며 편재하고 있다면, 이에 대한 저항은 그것들이 의존하는 기술을 가시화하는 것이다. 이런 의미에서 의도가 무엇이든지 간에 해킹 자체는 "시스템이 안전하지 않다"는 것을 부정적인 방식으로 보여주는 것이며 다양하고 저항과 대안 창출의 의도를 가진 해킹 방식을 통해 이러한 기술을 드러낼 수 있다(전자여권의 개인정보 유출의 위험성에 대한 해킹 검증).
- 기술의 누드화를 위한 시도들: 자유소프트웨어운동 및 오픈소스 소프트웨어/하드웨어 프로젝트들은 이를 위한 풀뿌리 해킹 활동이다.
    - 브리코랩(bricolab) 국제 네트워크: 전화 프리킹(phreaking)의 현재적 형태로서, 이 핵심 프로젝트 중의 하나가 브리코전화(bricophone)
- 결국, 기술의 누드화는 현재 우리 생활 곳곳에 스며들어 작동하고 있는 사회기술 시스템의 작동원리와 기작(mechanism)을 공개하고 누구나 자유롭게 접근할 수 있게 만들어 사용하고 변형하며 나눌 수 있게 일이다.

이와 같이 해킹문화운동은

- 일상 삶 속의 우리 모두의 실천으로서의 기술이 넉넣고 있으면서 기술 파시즘으로 빠지는 것이 아니라 자율적이고 대안적인 기술 문화로 갈 수 있도록 하는 개입과 투쟁으로서 중요한 의미를 갖는다고 생각한다.
- 해 킹, 해커공동체, 해커문화를 통해 정보 자본주의 사회와 네트워크문화 전반의 핵심 쟁점이라고 할 수 있는 표현의 자유와 검열, 정보 사유화와 정보 공유, 사생활 보호와 보안, 디지털 행동주의(온라인 행동주의), 지적재산권 체제의 문제들을 재배치할 수 있다.
- 즉, 해커문화는 지금의 정보 자본주의와 네트워크문화를 아래로부터 비춰볼 수 있는 프리즘으로서 새롭게 연구되어야 할 주제이자 현재의 실천에 접목되어야 항목이다.
- 이를 위해 빅브라더나 전일적인 국가의 감시와 통제 사회에 대한 서사에만 매달릴 것이 아니라 그에 대한 저항의 문화에 주목하고 이미 풀뿌리 차원의 대안들이 싹트고 있는 것에서 출발할 수 있다.
- 그 래서 77 분산서비스거부 사건을 놓고, 그 원인이야 어떴든 그것의 효과는 국정원을 위시한 권력기구들의 인터넷 통제과 이를 합법화하는 법안들을 강화할 것으로 보는데, 이것은 이미 절망하는 서사로 몸과 의식을 내맡기고 마는 것이다. 이러한 해킹은 해킹대로 기술의 절대주의 - 기술 파시즘으로 가는 경향들을 부정적인 방식으로 견제하는 의미가 있다고 보는 한편, 그러한 문제들을 직간접적으로 가시화하는 이러한 사건에서 그렇다면 과연 어떠한 보안과 안전의 커뮤니케이션 시스템이 구축되어야 하는가에 대한 논란에 개입하고 보다 근본적인 논쟁을 맞대야 한다.
- 해킹문화운동과 같은 정치 기획을 통해 지배 기술문화의 논리에 무장해제된 채 국정원 따위의 권한 강화에 동의해주는 일에서 벗어나 보다 적극적인 사회적 해킹들을 해나갈 수 있다. 기술 관료나 전문가 혹은 기술활동가들의 전문 영역이 아니라 "가치와 의미를 놓고 벌이는 문화 투쟁"(Ross 1990)이기 때문이다. "재숙련화할 수 있는, 그래서 새로운 기술을 위한 여지를 만들어내는 사회적 가치를 재프로그래밍하고 문화적인 프로그램을 재작성할 수 있는 해커의 지식, 인간의 재능(ingenuity)을 대안적으로 사용하는 것에 대한 새로운 대중적 낭만을 발생시킬 수도 있는 해커의 지식"(Ross 1990) 운동으로서의 해킹문화운동, 혹은 놀이투쟁!

활동 제안: 해킹문화운동을 위한 기획과 실천

- 협의의 컴퓨터네트워크 기술 해킹 전술 + 광의의 문화적 해킹 전술
- 다양한 해킹/해커 모임과 학습의 장 마련: 대중 해킹문화의 형성
- 인터넷문화 전체를 옥죄는 법안들에 대한 대응 - 기술에 대한 자유롭게 평등한 접근과 이용에 대한 권리 주창!
- 해킹문화운동 네트워크 구축을 중기적으로 모색하는 해크랩[hacklab] 설치
    - 기술 개발, 정보교환, 국제연대 및 국내외 사례 조사 공유, 월례/연례모임 조직, 교육 및 홍보 사업, 법제화 대응

참고문헌

- 김강호. 1997. [해커의 사회학 - 해커를 해킹한다]. 개마고원
- 김영식. 2006. “위키페디아에서 대안사회로.” 현장에서 미래를. 제117호. 혹은 '한 과학기술 노동자의 잡소리들' 블로그, 2006년 02월 27일 http://blog.jinbo.net/yskim/?pid=47
- 데 닝, 도로시 E.. 2005. "액티비즘, 핵티비즘, 사이버테러리즘: 인터넷은 대외 정책에 영향을 미칠 수 있는가?" 존 아퀼라 & 데이비드 론펠트, [네트워 크 전쟁 - 테러, 범죄, 사회적 갈등의 미래]. 한세희 옮김. 한울; Denning, D. 1999. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy". http://www.iwar.org.uk/cyberterror/resources/denning.htm
- 아이비스에너지전략연구소. 2009. "디도스, 미국 사이버 사령부 창설 그리고 시민권 후퇴." 2009.07.12 http://blog.daum.net/sibad/173
- 우형진. 2007. [넷 전쟁과 인터넷 보안군]. 삼성경제연구소
- 윤여상. 2001. "한국 해커공동체의 정치사회적 특성 연구." 부산대학교 사회학과 석사학위 논문. http://korea.gnu.org/people/chsong/yys
- 이광석. 2009. "유비쿼터스 시대의 권력 변화와 웹2.0 미디어 양식에서의 문화 지형." 문화과학, 2009 봄
- 일리히, 이반. 2004. [성장을 멈춰라! - 자율적 공생을 위한 도구]. 이한 옮김. 미토
- 전응휘, 한겨레21
- 전자신문. 20090710. "박재완 수석 "국가 사이버테러 컨트롤 타워는 국정원"." http://www.etnews.co.kr/news/sokbo_detail.html?id=200907100162
- 최은정, 2001. "그들을 해커라 부르지 마라," 사이버문화연구소 엮음, [Cyber is ... - 네트에서 문화 읽기], 역사넷
- Galloway, Alexander R.. 2005. "Global Networks and the Effects on Culture." The ANNALS of the American Academy of Political and Social Science 2005 Vol. 597, No. 1
- Jordan, Tim. 2002. *Activism! Direct Action, Hacktivism and the Future of Society*. Reaktion Books
- Kleiner, Dmytri. 2007. "Copyfarleft and Copyjustright," Mute magazine - Culture and politics after the net http://www.metamute.org/en/Copyfarleft-and-Copyjustright
- 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/

- Ross, Andrew. 1990. "Hacking Away at the Counter-culture." Postmodern Culture - Volume 1, Number 1, September 1990 http://muse.jhu.edu/journals/postmodern_culture/v001/1.1ross.html
- Samuel, Alexandra Whitney. 2004. *Hacktivism and the Future of Political Participation*. PhD Thesis. Harvard University Cambridge, Massachusetts. http://www.alexandrasamuel.com/dissertation
- Söderberg, Johan. 2002. "Copyleft vs. Copyright: A Marxist Critique." First Monday. Volume 7 Number 3. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/938/860
- Söderberg, Johan. 2007. *Hacking Capitalism: The Free and Open Source Software(FOSS) Movement*. Routledge.
- Suoranta, Juha & Vadén, Tere, 2008, *WIKIWORLD: Political Economy of Digital Literacy and the Promise of Participatory Media.* http://wikiworld.wordpress.com