

CC3 Provocative Texts
Prof.dr.P.Pisters & dr.S.Dasgupta

Eindpaper
Jasper Moes
0357677

**The Global Order of Information:
On Internet, Control, and Power**

Abstract

This essay, which is a continuation of the Freedom of Speech manifesto presented at the CC3 Media & Politics conference, has its focus on one point namely *the freedom to access information*, in particular on the so called 'world wide web'. It is argued that the open character of the web as it was in the early days of the Internet, has disappeared due to new technologies deployed by different actors in their attempt to control the web, making it impossible to speak of just one 'web'. To restore 'the global order of information', the empire the Internet was, and undo the steps back due to the re-territorialisation and the regulation of the flows of information by governments and organizations, 'openness' has to be revitalized not only on a technological level, but also on a social-political one.

Keywords: Internet censorship, networks, power, Foucault, surveillance

Introduction

“The revolution will not be televised”, but it will be on Youtube, or at least somewhere on the net. Although very pre-Youtube, the images of rubber bullets and takedowns, firsthand accounts of peaceful protest and violent police reaction during the 1999 “Battle of Seattle” come to mind, which were delivered on the Internet while the mainstream news, the consciousness industry, reported that protesters were breaking windows and Seattle police were showing admirable restraint. This was one of the first examples of a different model of media consumption in action. Until then, media was controlled centralized and messages were dispersed from one or several epicenters. Nowadays the DIY media, facilitated by the ‘ever-price-dropping-yet-increase-in-performance’ technologies, give rise to public-journalism that circumvents the traditional media distributed via the Web. The reciprocity in communication that Enzensberger foresaw, the answer to the superstructure media he hoped for, is now possible; distributed (yet organized) production of media.¹

But can ‘the revolution’ still be seen on the web in the (near) future? Will information be freely available, and accessible to anyone at all times? Will cyberspace be ‘independent’, or were the words of John P. Barlow pre-mature and ill fated?² More and more ‘Governments of the Industrial World’ are, with or without moral right, trying to rule ‘us’ cyberspace inhabitants, with methods of enforcement that we really should fear. Research, conducted by Jonathan Zittrain et al (members of the OpenNet Initiative³), bundled in their recently published work *Access Denied: The practice and Policy of Global Internet Filtering* (2008), shows that at least 26 countries in the world are restricting their citizens the access to certain kind of online information. In several of these countries it is very dangerous to post comments to blogs, messages on forums or other places that are in conflict with the ideas and beliefs of their government because this has real life effects: punishment and jailing are not uncommon. Censorship is flourishing on different levels of the Internet, and in this essay it is argued that the open character of the web as it was in the early days of the Internet, has disappeared. The (re-)territorialisation of the world order the Internet once was and the regulation of the flows of information by governments and organizations, are rapidly

¹ Enzensberger, Hans Magnus, “Constituents of a Theory of the Media”, (1970), in Wardrip-Fruin and Montfort (eds), *the New Media Reader*, 2003, p.261-275.

² Declaration of Independence of Cyberspace: <http://homes.eff.org/~barlow/Declaration-Final.html>

³ OpenNet Initiative: <http://opennet.net>

changing the web as a whole converting it into different ‘small’ webs. In order for the web to grow, for information to be freely accessible, the openness of the web is a prerequisite. As a case study we will take a closer look at Internet filtering in countries like China, what it is and how this works, and the way it controls the flows of online-information on two levels: a technological one and a social-political one. As often is the case where there is suppression, an anti force can be seen so in this essay the means to circumvent this Internet filtering will be touched upon. But first let’s look at a brief recapitulation of the history, the diagram of the Internet, and how control (power) resides within this network of networks. It is not my intention here to give an exhaustive and complete overview of the actors who contributed to the development of the Internet as we know it today, but I feel it is necessary to write a brief account of the history of the Internet as it will serve me in my argument: although the Internet is a highly controlled environment, ‘openness’ and the open character on both a technological and a socio-political level was and is needed in order for the Internet to come into existence in the first place and for it to develop in the future.

The Internet: history and diagram

Whether or not the Internet was invented as a military system of command and control to withstand a nuclear attack⁴, fact is that it was build in a time when the possibility of such an attack was at its peak: the cold war during the nineteen sixties. Until then the military information networks that were available, were organized centrally, making them vulnerable and relatively easy to attack. The North American Aerospace Defense Command (NORAD), a radar surveillance system that provides early warnings of missile or other air attacks against Canada and the United States, is a perfect example of a centrally organized system with a rigid hierarchy of command and control. The regional control sectors are all ultimately controlled by the USSPACECOM Command Center at Cheyenne Mountain in Colorado Springs, Colorado. Take out this central node, or hub, and the whole network is down. (See fig.1)

⁴ Compare Galloway, 2004: p.29, and Charles Herzfeld’s (former director of DARPA) account of Internet history on: http://inventors.about.com/library/inventors/bl_Charles_Herzfeld.htm Herzfeld writes that it was a scientific need to connect the then few large computers in the US so scientists across the country could access and use them.

A different kind of network, non-centralized (much like a rhizome⁵) would make an end to the vulnerability of the centralized network and secure the future of the US military command and control. The Defense Advanced Research Projects Agency (DARPA), an agency of the US department of defense and responsible for the development of new technologies for the use of the US military, started funding what was to become the first internet called ARPA-net, out of which later the Internet as we now know it would arise. The idea of a ‘Galactic Network’ of machines came from J.C.R.Licklider, a professor at MIT (1950’s), and in 1962 he initiated and became head of the ARPA-net project.

As said, the Internet system would be very different from the NORAD network, with a totally different organizational design based on flexibility and adaptability. Alexander Galloway, associate professor at NYU and author of the (brilliant) book *Protocol: how control exists after decentralization* (2004), writes in this work that the “normal military protocol serves to hierarchize, to prioritize, while the new network protocols of the Internet serve to *distribute*”⁶. Galloway sees that where power once was dispersed via a central hub, on the Internet power is within ‘protocols’ that are “not by nature horizontal or vertical, but [...] algorithm[s], a *proscription for structure* whose form of appearance may be any number of different diagrams or shapes”. Borrowing from Foucault, Deleuze, Deleuze & Guattari, and many other authors, Galloway sees three kinds of diagrams. The centralized, the decentralized, and the distributed network (fig.1).

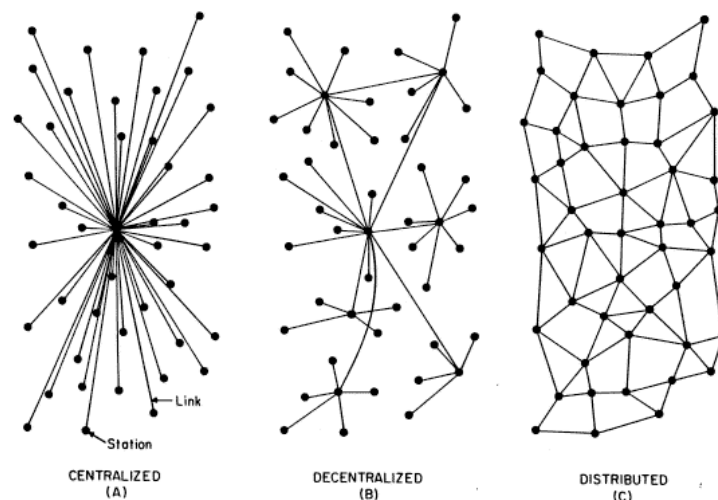


FIG. 1 – Centralized, Decentralized and Distributed Networks

⁵ Deleuze, Gilles, Felix Guattari, *A Thousand Plateaus*, trans. Brian Massumi, Minneapolis, 1987: p.7

⁶ Galloway, 2004: p.30

The centralized network is hierarchical. Each node is connected to the central hub. Foucault described in *Discipline and Punish*, Jeremy Bentham's panopticon⁷ where the guard is situated in the centre of the prison and the cells are in a circle around the central guard. This is a perfect example of a centralized network. Foucault thought of this kind of network as a diagram for the feudal society, where the hierarchical structure was evident: lords ruled over vassals who made sure that the revenue of the fiefs (land owned by the lord, but worked on by the vassals) went for the most part directly to the lord.

An example of a decentralized network is the worldwide airline system. There are some major airports which function as centralized hubs and between which you can travel directly. These major airports then are connected to smaller airports that can only be reached via one of the major hubs. As a diagram for a society, Foucault coupled the decentralized network to the disciplinary society in which the power that regulates our customs, that discipline our behavior and productive practices, comes from a set of 'apparatuses'. Think of schools, prison, factory, hospital and so on.

Gilles Deleuze wrote in his article "Postscript on Control Societies" (2002) that the disciplinary power Foucault described has become more and more interiorized in the subjects themselves. This power can now also be exercised through machines and works not only within the 'apparatuses' we just talked about (schools, prisons etc) but also outside these confined spaces through flexible and fluctuating networks⁸. It is these kind of networks that resemble the diagram of the distributed network. As Galloway and others like Castells⁹ and Deleuze & Guattari¹⁰ write, the rise of the distributed networks is part of a larger shift in social life. Until then we dealt with hierarchies and bureaucracies, but now, as "[...] part of a larger process of postmodernization that is happening the world over"¹¹, we deal with networks without central hubs, with each entity as an autonomous agent. In figure 1 you can go from a to b almost in any way you want. If one node might fall away, it is still possible to get to your desired end point via the multiple 'road' the distributed network has to offer. It functions much like the actual roads of the highway system: if one road is obstructed for instance by a traffic jam, you can take a detour to get to your destination.

⁷ Foucault, Michel. *Discipline & Punish*, trans. Alan Sheridan, New York, 1997: p.197

⁸ Deleuze, Gilles, "Postscript on Control Societies", in Thomas Levin, Ursula Frohne and Peter Weibel (eds.), *Ctrl Space: Rhetorics of Surveillance from Bentham to Big Brother*, Cambridge, MA: p. 317-321

⁹ Castells, Manuel, *The Rise of the Network Society, The Information Age: Economy, Society and Culture*, Vol. I. Cambridge, MA, 1996

¹⁰ Deleuze & Guattari, 1987

¹¹ Galloway, 2004: p.33

It is this shape and mechanism that made the Internet as it is today possible along with a technique that Paul Barran, then working for the US airforce, invented called 'packet switching'. In a nutshell, packet switching is a communications method that divides a message into several discrete blocks of data. When you as a user behind your computer at the office, called 'client', click on a let's say a movie¹², you send a request for information via the Internet to another computer called server which hosts the movie. This request, your message, is divided in blocks and wrapped in what is called IP packets. Each IP packet then travels through your local network (LAN), to the router who sends them over the corporate internet to a proxy (a 'central' computer). This proxy has a 'corporate firewall', a wall that decides which messages can go out, and which can come in, then sends each packet separately to its destination over the 'big' Internet. Each block can (and most likely will) take a different route, and when all packets have arrived at their destination, they get put together again as a whole.

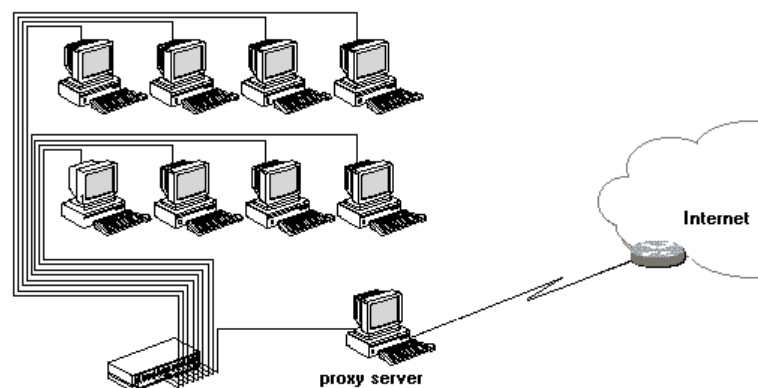


fig 2: LAN, router, proxy, and Internet

As you can see there are a couple of layers a message has to pass, and each layer has its own set of rules of how to communicate (fig 3). These rules are called 'protocols', and function much like the 'real world' protocols of communication (think of military protocols, but also the simple 'telephone' protocol; 'hi how are you', 'I'm fine thank you').

The layers of communication can be defined in four basic layers: (1) the application layer (the program/application you use), (2) the transport layer (Transmission

¹² Warriors of the net

Control Protocol, TCP), (3) the Internet layer (Internet Protocol, IP), and (4) the link layer (media access like Ethernet).¹³

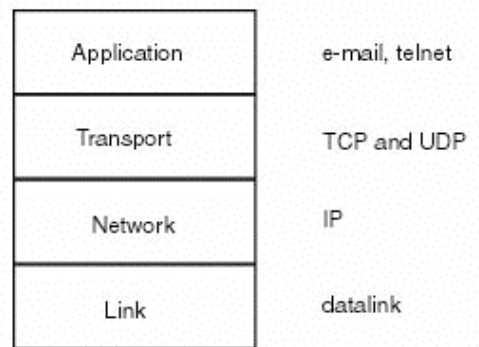


fig 3: protocol layers

As said, each layer has its own protocol. These protocols are essential in the communication between machines; there is no communication possible *outside* these protocols! The protocol is therefore a very powerful ‘management style’ as Galloway eloquently puts it¹⁴, which shows the society of control at its best: as long as your computer handles the right protocol at the right time, you have access to the network of networks, it is open to anyone who knows the protocol. These protocols are developed and promoted by the Internet Engineering Task Force (IETF). When the existence of a network of networks became publically known, many actors (universities, corporations, etc) jumped on the bandwagon and helped develop the network. To coordinate this was a huge task, a task DARPA didn’t want to fulfill any longer so the IETF was created by volunteers with a hackers mentality¹⁵, and organized in a ‘anarchistic’/democratic manner. The IETF is open to anyone who is willing to contribute to the development of Internet protocols and can put his/her ideas down in documents, which are called Request For Comments (RFC’s). The IETF has formally no board of directors, no hierarchy, but in practice the ones who contribute the most are ‘in charge’. Even though the IETF is open to anyone, in reality it is only the elite, the ones with the technological knowledge who can contribute. This group of happy few is what Harry Halpin, researcher at the university of Edinburgh, calls the Immaterial Aristocracy of the

¹³ Robert Braden, “Requirements for Internet Hosts”, RFC1122, October 1989: p.6.

<http://www.faqs.org/rfcs/rfc1122.html>

¹⁴ Galloway, 2004: p.3

¹⁵ Mentor, the, The Hackers Manifesto <http://phrack.org/issues.html?issue=7&id=3#article> (original from 1986)

Internet.¹⁶ Unlike Galloway who sees that power mostly resides in the technology, the management style protocol is and exercises over humans¹⁷, Halpin writes that it is still the human with all its politics who writes these protocols and ultimately controls the net. Halpin thinks protocols embody social constructs, and are created by actors that can benefit from it (like corporations and governments, “[...] although it seems that hackers usually create the protocols that actually work and gain widespread success”¹⁸). I think it is a little bit of both.

Access, Control, Freedom, and Censorship

Internet is the most highly controlled environment there is while at the same time a very open and free space. This weird split between control and lack of it can be best described in a debate between two scholars; Danah Boyd and Fred Scharmen. Danah Boyd holding a PhD at Berkeley and doing research on socio-networking sites and youth culture, writes in her article "Identity Production in a Networked Culture: Why Youth Heart MySpace" that MySpace is the environment where the ‘American youth’ (age 14-24) simply ‘hangs out’ and get’s socialized into peer groups.¹⁹ The reason these kids hangout on MySpace, according to Boyd, is because this is the place to escape the control of ‘adult-culture’, which thinks hanging out is a waste of time. Lack of mobility and access to youth space where they can hang out interrupted is the main reason why youth spends its time online. In this context, Boyd sees three main classes of space: public, private and controlled.

For adults, the home is the private sphere where they relax amidst family and close friends. The public sphere is the world amongst strangers and people of all statuses where one must put forward one's best face. For most adults, work is a controlled space where bosses dictate the norms and acceptable behavior. Teenager's space segmentation is slightly different. Most of their space is controlled space. Adults with authority control the home, the school, and most activity spaces. Teens are told where to be, what to do and how to do it. Because teens feel a lack of control at home, many don't see it as their private space.²⁰

¹⁶ Halpin, Harry, “the Immaterial Aristocracy of the Internet”, Mute Magazine – Culture and politics after the net, May 2008. <http://www.metamute.org/en/Immaterial-Aristocracy-of-the-Internet>

¹⁷ Galloway, 2004: p.81

¹⁸ Halpin, 2008: p.4

¹⁹ boyd, danah. 2006. "Identity Production in a Networked Culture: Why Youth Heart MySpace." *American Association for the Advancement of Science*, St. Louis, MO. February 19.

²⁰ Boyd, danah, 2006: <http://www.danah.org/papers/AAAS2006.html>

This, coupled with the facts that outside locations to hangout are considered dangerous by most parents, and after school activities (sports, jobs etc) also take place in a very controlled environment make the youth take their refuge to cyberspace to create their own 'youth space'. Free from adult control, according to Boyd.

Fred Scharmen, a US student, opposes Boyd's opinion. In his article "You must be logged in to do that! MySpace and Control" Scharmen argues that "[...] it is exactly control in the Deleuzian sense that these teenagers and other users of MySpace are submitting to".²¹ First of all, you only have access to MySpace if you have a password, a code. Without a password you cannot work within the MySpace area; if you want to be included you have to work with the MySpace protocol. Next to that Scharmen thinks that online 'spaces' like MySpace are highly controlled environments not only because of the nature of online environments, (communication is only possible within the above written protocols, which 'open' and controlled), but he also builds his argument by looking at the Terms of Service (TOS) that MySpace has. When reading the TOS it becomes quite clear what kind of information of the users (the 'youth') is being harvested and in what manner MySpace has the 'right' to do with this valuable information as it pleases. (Not to mention the fact that all uploaded content becomes MySpace's property!).

But this is for most parents not the biggest concern. The facts that their offspring is spending much time online and their online behavior (and online whereabouts) can't be overseen are the real problem. A 'problem' that can easily be 'fixed'. As we have seen in the above protocol layer map and the route a message or request has to take from the client to the host, the message will have to pass the router and (corporate) firewall before it enters the net. This firewall can, with a little knowledge, be easily set to 'closed' for certain online information. The access to a website like MySpace can then be blocked, or only allowed to be watched at certain times a day, websites with certain content can be blocked by prohibiting certain keywords, and even whole domains (countries, like .nl) can be excluded from the internet experience. This is censorship on a micro scale.

On a little bit larger scale this kind of censorship is also happening at companies and offices worldwide. The use of instant messaging programs like MSN (Microsoft's instant messenger) is seen as distracting the employee from its work. The ports these programs use in the corporate firewall can be closed and thus making the use of MSN

²¹ Scharmen, Fred. "You must be logged in to do that! MySpace and Control." 2006: <http://www.sevensixfive.net/myspace/myspacetwopointoh.html>

impossible. Again, here some type of sites can be blocked as well so an employee doesn't do his shopping on e-bay during work hours, or pays visits to websites with adult content.

Censorship on a Macro Level

Censorship on a macro level has become more and more in use over the past decade and as governments start to also govern the 'free' cyberspace by filtering the information on the web, different kind of webs with different kinds of access to information start to emerge. The research done by the Open Net Initiative, published in the book *Access Denied*²², sees three basic rationales for Internet censorship: (1) Politics and Power, (e.g. blocking sites from rivaling countries) (2) Social norms, morals and religion, (e.g. blocking pornography) (3) Security concerns (attacks from 'outside').

For instance China, at the time of this writing vastly in the news with the whole Tibet affair and the Summer Olympics 2008 around the corner, is blocking the Internet and the access to information on several levels of the Internet Protocol system. Next to filtering and blocking automatically, they currently have 30.000 people manually checking their online citizens behavior and scanning the web looking for 'wrong content' and denying access to it for their inhabitants. The army of 30.000 search and block pages with keywords concerning the topics 'Tibet, 'Taiwan', and 'Tiananmen' to name the biggest topics, but there are lots of others like 'Falun Gong', 'Mein Kampf' and of course 'Democracy'. By doing this kind of filtering, China does not have to block entire domain names (like .nl). This censorship is quite extensive and with an army of 30.000 people working to monitor 221 million Internet users it is almost an impossible task. But the Chinese have come up with a nice solution: Sometimes small cartoon characters in police uniforms pop up on the screen in response to questionable search terms as a reminder that Big Brother is always surfing alongside you.

²² Deibert, Ronald, et al, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: 2008.



fig 4: China's cartoon police

Other countries, less dynamic and exhaustive as the 'Great Firewall of China' (officially it is called Golden Shield), 'simply' legislate to control what can and cannot be said, downloaded or linked to. India filters only a few sites; Saudi Arabia tries to block all pornography and Syria blocks everything from the Israeli domain ".il", to name but a few examples. But who thinks this is only limited to countries in Asia is wrong. Sweden and Finland have an agreement with most major ISP's (Internet Service Providers) that they will block everything on a list composed by the police, which happens without regulation and transparency. This delegating of censorship to Internet companies is another concerning development. Google gave in to the will of China and build them a censored search engine, which is in violation of their motto "don't be evil".

Closer to home: in the Netherlands, governments try to "make" public opinion on their websites and forums by allowing certain topics and blocking others²³. (see *Information Politics on the Web*, by Richard Rogers).

Most Internet censorship is technical because this is easy to achieve; websites or entire domains get blocked. But some censorship is legal because some countries have laws against publishing certain content. Or in the case of Youtube, some movies that are uploaded by users are copyrighted and the material cannot be shown openly on the web due to these rights. Youtube therefore actively and constantly checks its own database and deletes any content that is copyrighted.²⁴

²³ Rogers, Richard, *Information Politics on the Web*, Cambridge, MA, 2004

²⁴ Check the Youtube watchdog 'youtomb': <http://youtomb.mit.edu/>

Resistance & ways forward

Where there is power there is resistance. In the case of China and the prohibited search/keywords, bloggers circumvent these words and create new terms: Information on the Tiananmen Square Massacre of June 1989 can be found via 198 964 (although this is now blocked too...). Not on a cultural/social/content level but more on a technical one, Chinese Internet users use tools like Gladder (great ladder), also known as “open proxies” which function like the above described proxy, but now to get you to access information outside the reach of China’s internet filter without them knowing which websites you visit. Many of these proxies are available on the net²⁵. But they come and go very fast because these, once known by the Chinese government, get blocked very quickly as well.

But these are merely short-term solutions to an increasing censorship problem. It is a cat and mouse game, and even though circumventing filtering with proxies and writing about it like many bloggers or ‘watchdogs’ do (Youtomb) is a good thing, it is time for activists to take more rigorous action against the proprietary control of the big companies and the forced control of the governments. If this doesn’t happen the openness of the Internet as it now (relatively) still is will disappear and only small, highly controlled spaces will remain. The distributed network, will become decentralized and we will take a step back in time. Where on a global social-economic scale the distributed network is slowly growing towards one big empire²⁶, online a (re)territorialisation is taking place and the empire called Internet is deteriorating. It is time for activists to give a fundamental answer to this development. An example of such an answer is the Open Search project (<http://www.open-search.net>); a distributed, p2p search engine as an alternative to Google. This project is totally open to anyone who would like to join, much like the IETF and the RFC’s are. Still, projects like these are in its infant’s years; there is a long way ahead in the battle for a renewed open net.

²⁵ Check for a detailed list of (some) available open proxies: www.proxy.org

²⁶ Hardt & Negri, *Empire*. USA, 2001

- Barlow, John Perry, "A Declaration of the Independence of Cyberspace", visited June 15, 2008: <http://homes.eff.org/~barlow/Declaration-Final.html>
- Boyd, Danah. "Identity Production in a Networked Culture: Why Youth Heart MySpace." *American Association for the Advancement of Science*, St. Louis, MO. February 19, 2006: <http://www.danah.org/papers/AAAS2006.html>
- Castells, Manuel, *The Rise of the Network Society, The Information Age: Economy, Society and Culture*, Vol. I. Cambridge, MA, 1996
- Deibert, Ronald, et al, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA, 2008.
- Deleuze, Gilles, "Postscript on Control Societies", in Thomas Levin, Ursula Frohne and Peter Weibel (eds.), *Ctrl Space: Rhetorics of Surveillance from Bentham to Big Brother*, Cambridge, MA, 2002
- Deleuze, Gilles, Felix Guattari, *A Thousand Plateaus*, trans. Brian Massumi, Mineapolis, 1987
- Enzensberger, Hans Magnus, "Constituents of a Theory of the Media", (1970), in Wardrip-Fruin and Montfort (eds), *the New Media Reader*, Cambridge, MA, 2003
- Foucault, Michel. *Discipline & Punish*, trans. Alan Sheridan, New York, 1997
- Galloway, Alexander, *Protocol: how control exists after decentralization*, Cambridge, MA, 2004
- Halpin, Harry, "the Immaterial Aristocracy of the Internet", Mute Magazine – Culture and politics after the net, May 2008.
<http://www.metamute.org/en/Immaterial-Aristocracy-of-the-Internet>
- Hardt, Michael, Antonio Negri, *Empire*. USA, 2001

Herzfeld, Charles, “On ARPANET and Computers”, website Inventors.com. June 15, 2008: http://inventors.about.com/library/inventors/bl_Charles_Herzfeld.htm

Mentor, the, The Hackers Manifesto, visited June 15, 2008:

<http://phrack.org/issues.html?issue=7&id=3#article> (original from 1986)

OpenNet Initiative. ONI homepage. June 15, 2008: <http://opennet.net>

Robert Braden, “Requirements for Internet Hosts”, RFC1122, October 1989

<http://www.faqs.org/rfcs/rfc1122.html>

Rogers, Richard, *Information Politics on the Web*, Cambridge, MA, 2004

Scharmen, Fred. “You must be logged in to do that! MySpace and Control.” 2006:

<http://www.sevensixfive.net/myspace/myspacetwopointoh.html> (visited 15 June 2008)