RESEARCH ONLINE

University of Wollongong
Research Online

Faculty of Arts - Papers (Archive)

Faculty of Law, Humanities and the Arts

2003

Cybermethods: An assessment

H. Megens
Tilburg University, The Netherlands

Brian Martin
University of Wollongong, bmartin@uow.edu.au

Publication Details

Megens, H & Martin, B, Cybermethods: An assessment, First Monday: Peer-Reviewed Journal on the Internet, 2003, 8(2). The original article is available here.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

RESEARCH ONLINE

f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Cybermethods: An assessment

by Hellen Megens and Brian Martin

Abstract

Cybermethods: An assessment by Hellen Megens and Brian Martin
Methods of communication and action on the Internet, such as e-mail, encryption and hacking, can be broadly grouped into four categories: expressing, protecting, information gathering and interfering. This classification helps explain the distribution of concern about cybermethods and offers a guide for assessing and designing future methods. As forms of technology, cybermethods are neither neutral nor autonomous. Methods of expressing and protecting are most suitable for promoting a society with greater equality and participation.

Contents

Introduction
Types of cybermethods
Theoretical contexts
Arenas of creation and application
Conclusion

Introduction

There are lots of ways of acting on the Internet, ranging from sending an e-mail to a friend to coordinating a mass denial-of-service attack against a government Web site. Some such "cybermethods," for example Web browsing by an adult, do not seem to generate much concern, whereas others, such as spamming, produce widespread aggravation. How can we make sense of the diverse methods of action on the Internet?

We begin with a classification of common cybermethods, describing typical responses to the four main categories of methods. We then look at cybermethods through two theoretical lenses, non-neutrality of technology and medium theory, arguing that cybermethods, as methods, send messages of their own independently of the formal content conveyed. We next comment on the origin and applications of cybermethods before concluding with an analogy to appropriate technology.

Types of cybermethods

We began our investigation by listing a range of common cybermethods; we then looked for their common features. As a result of this process, we concluded that it is revealing to divide cybermethods into four categories: expressing; protecting; information gathering; and interfering. Table 1 gives a list. The Appendix gives brief descriptions of each method plus examples. For a number of these methods Schneier (2000) is a convenient source of information.

Table 1: Some cybermethods.

Expressing

- e-mailing
- chatting
- Web site uploading
- file-sharing

Protecting

- authenticating
- filtering (self-chosen)
- encrypting
- remailing

Information gathering

- Web browsing
- Web data collecting
- hacking (looking)
- surveillance

Interfering

- spamming
- denying access
- denying service
- Web site removal
- sending malicious code
- domain grabbing
- cracking (altering, stealing)

Table 1 includes many common cybermethods but is far from exhaustive. There are other methods that could be added, such as downloading and online translating. There are also methods with no simple name, such as protecting one's identity by sending e-

mail from a newly created account at a cybercafé and then never using the account or cybercafé again. Further cybermethods will be developed in the future. Our aim is not to achieve completeness but rather to indicate an approach to classification.

The cybermethods of *expressing* are familiar to most users. Most of the problems that arise associated with these methods are caused by the content conveyed. For example, an e-mail message or a Web site may contain abusive or defamatory material. But those who are upset by chat comments or information on Web sites seldom complain about the medium itself. As in the case of the telephone and post, the medium is seldom blamed for the content it carries.

Sometimes, though, cybermethods of expressing bring into being new dimensions of old problems. For example, defaming someone on the Web, with its transnational reach, is a different matter from defaming them in a local newsletter. The seriousness of an action in part depends on the medium. Of the cybermethods of expressing, file sharing has been the most contentious, with the popularity of Napster and its progeny and the opposition of the record companies generating headlines. The main issue is not file-sharing *per se* but rather the sharing of material, especially music files, that is copyright. After all, copyright material can be easily sent by e-mail. Nevertheless, the ease by which file sharing can be done using particular types of software would lead some critics to oppose these file sharing systems altogether.

The cybermethods of *protecting* generate mixed responses. Most people are happy to use these methods to ensure confidentiality, to hide their identity or to screen out unwanted messages. Conflict can arise, though, when *someone else* uses these methods. Some government agencies oppose encryption, at least when used by others who might be criminals or security risks. Unlike the methods of expressing, the cybermethods of protecting can themselves be targets, not just the information protected. One famous case is the U.S. government's attempt to block export of encryption software (Diffie and Landau, 1998; Hoffman, 1995). Yet no government has ever opposed encryption for its own confidential communications, just for those of others. Methods of protecting thus are typically evaluated according to who is doing the protecting: nearly everyone thinks it is okay to protect their own communications but some don't want to allow others to have the same protection.

Cybermethods of *information gathering* evoke varying responses. Most of those who gather information think what they do is quite acceptable, but others may disagree. Least contentious is Web browsing: after all, those who put up public Web sites welcome readers. However, some repressive or censorious governments seek to restrict browsing by their own citizens. Gaining access to non-public Web sites, commonly called hacking, is often seen as a serious threat by the affected parties, equivalent to eavesdropping on a telephone conversation. Hackers may say that they are "just looking" and thereby doing no harm, but owners of the sites so visited may feel violated or threatened. Collection of information from cookies is done for commercial purposes, but some privacy advocates feel this is a serious concern. Other forms of surveillance, such as intercepting e-mails, are widely seen as an even greater invasion of privacy.

As in the case of protecting, responses to information gathering depend strongly on who is gathering the information. When governments or large firms gather the information, opposition comes from individuals and privacy groups. When individuals gather the information, opposition typically comes from corporations and governments, including in the form of criminal penalties for hacking.

Cybermethods of *interfering* are the most contentious of all. They typically involve

actions that are annoying at a minimum and seriously damaging in some cases. Even so, each of these methods can be justified in special circumstances. For example, denying access to an e-mail account or Web server might be justified by the applicant's criminal record. Dissidents might justify altering the Web site of a repressive regime on the grounds that the regime is itself illegitimate.

As in the case of protecting and information gathering, some people condemn methods of interfering outright, irrespective of those involved. Many users oppose spam as a matter of principle; responsible hackers oppose the use of hacking techniques to steal, disrupt or destroy. Intentional creation or sending of viruses is almost universally condemned. Methods of interfering are harder to justify precisely because they involve interference.

The difficulty in justifying methods of interfering is reflected in the difficulty of thinking of "good" uses of these methods, at least from the point of view of those at the receiving end. For example, spam could be used, in principle, as an emergency warning system, though nearly all uses have been for commercial purposes. Some Web sites are removed because they are proven, in an open hearing, to be harmful to the public interest, but far more Web sites are removed by governments that oppose expression of political dissent.

Table 2 lists some common features of the four main types of cybermethods.

Table 2: Some common features of cybermethods.

Type of cybermethod	Characteristic debates	Sources of concern	Main opponents
Expressing	free speech versus censorship; intellectual property versus free information	content (what is expressed)	censors, repressive governments, copyright owners
Protecting	privacy versus protection of criminal activities	content (what is protected) and method	police; intelligence agencies
Information gathering	privacy versus nefarious activities	method	privacy advocates; owners of non-public Web sites
Interfering	freedom versus censorship; improper behaviour versus legitimate action	method	everyone subject to interfering methods

One of the prices of classifying cybermethods into just four categories — expressing, protecting, information gathering and interfering — is that complexities are not addressed. There are many ways to modify or extend the classification, depending on one's purposes. For example, for each of the methods of expressing, there is a counterpart that can be called "receiving", as shown in Table 3.

Table 3: Sending and receiving aspects of cybermethods of expressing.

Method	Sending aspect	receiving aspect
e-mailing	sending e-mail	receiving e-mail
chatting	sending chat messages	receiving chat messages
Web site uploading	Web site uploading	Web browsing and downloading
file sharing	making files available	copying files

For e-mailing, chatting and file-sharing, distinguishing between sending and receiving does not appear to add much insight, but a receiving counterpart of Web site uploading is Web browsing, one of the methods listed under the category of information gathering in Table 1. This suggests that Web browsing has more in common with methods of expressing, and less in common with other methods of information gathering, than might be apparent from a cursory look at Table 1.

The distinction between public and private is another basis for probing cybermethods. Look for example at the methods of information gathering. Web browsing involves looking at public information, whereas hacking and surveillance involve looking at or gathering information that is intended to be confidential. Web data collecting has elements of both public and private information gathering. People usually are much more hostile to gathering of their private information than of gathering of public information. Similarly, methods of expressing are seen as threatening when it is someone else's private information that is made available. The private-public distinction can be used to examine each of the cybermethods, though it is wise to keep in mind that the distinction itself can sometimes be misleading.

As well as the sending-receiving and public-private distinctions, other distinctions can be used to probe cybermethods, for example voluntary versus involuntary and welcome versus unwelcome. For instance, some people must use the Internet for banking or enrollment in university classes, which makes their use qualitatively different to purely voluntary use. Another way to assess each method is to prepare a table of users and recipients. For example, e-mails can be sent by individuals, governments or corporations; individuals can be classified as adults, children, parents, and so forth. It is easy to see how more elaborate classifications can be developed. How to proceed depends sensitively on the purpose of making the classification. Our purpose here is to elucidate inherent features of cybermethods.

Theoretical contexts

Any given cybermethod can be used for a variety of purposes. Sending an e-mail is seemingly innocuous, but if e-mail messages are threatening or abusive and targeted at an individual, e-mail becomes a medium for harassment. Intentionally sending a virus seems like a hostile act, but it could be beneficial to political prisoners if the virus is

specifically written to destroy files on them. Does this mean that cybermethods should be considered neutral? We think not.

The word "neutrality" implies impartiality or not taking sides. A perfectly neutral method would be impartial concerning all possible uses or, in other words, equally easy to use for any purpose. This is implausible, since any method is bound to be easier to use for some purposes than others. A filter is easy to use for screening out messages but, obviously enough, not for altering a Web site.

Langdon Winner (1986) has argued that technologies — and this would include cybermethods — have "politics". What this means is that technologies are designed to serve the interests of particular groups and, in practice, serve some purposes and groups more than others (though not always exactly as designers intended). Although Winner's stories of New York bridges has been challenged (Joerges, 1999), his general point can be better illustrated by other examples. Cruise missiles, for example, are designed for the military to cause death and destruction and are not much use for most other purposes.

From this perspective, it makes sense to say that any particular cybermethod is *selectively useful*, namely that it is more useful, or easier to use, for some purposes than others. It is also possible to say that cybermethods are nonneutral, or biased [1]. The actual ways that cybermethods are used depend sensitively on a range of factors, including technological implementation, skills and resources of users, opportunities, incentives and a range of contingencies.

Another theory that is relevant for our classification of cybermethods is medium theory, which is a communication theory most widely associated with Marshall McLuhan, who became famous following his book *Understanding Media* (1964). In this book he treats technologies as *extensions* of the human body. An extension occurs when an individual or society makes or uses something in a way that extends the range of the human body and mind in a fashion that is new. Clothes, for example, can be treated as an extension of the skin; a microscope or telescope is an extension of the eye. The automobile can be seen as an extension of the feet: it allows people to travel places faster and with less personal effort than by foot, and in relative comfort in extreme weather conditions. Another example is the computer, which is an extension of the human brain, which is for McLuhan the highest of all technical extensions.

Because McLuhan's ideas are frequently reduced to one-liners and sound bites, he is difficult to access. However, the basics of his theory can be applied to cybermethods: in short, they can also be treated as extensions of the human brain. According to McLuhan, this means they are media: "You've got to remember that my definition of media is broad: it includes any technology whatever that creates extensions of the human body and senses, from clothing to the computer" [2]. When most people think of media they usually think of what are termed the mass media, including books, radio, newspapers, magazines, television and film, but for McLuhan something as common as a shirt or hat is a communication medium.

We are now in a position to use McLuhan's famous aphorism, "the medium is the message". Media are not simply neutral channels for conveying information between two or more environments, but are rather environments in and of themselves. Medium theory focuses on the medium itself rather than on what it conveys or how information is received (Meyrowitz, 1994). We might say that a medium is the symbolic environment of any communicative act. Although television technology, for example, can deliver a diverse range of programming, television as a medium of communication

also conveys a message of its own, independently of the program. Jerry Mander (1978) argues that an inherent bias of television is that it most effectively communicates gross, linear messages, especially advertisements.

Following this line of thinking, cybermethods can be considered media which, by their very construction, constrain and channel communication, and this constraining and channeling conveys a message of its own. For example, e-mail — perhaps the most generic cybermethod — can be used to send various contents but, whatever the content, e-mail usually implies certain communication features, such as asynchronicity, person-to-person messaging, and dependence on linear text and computers. Not all e-mails fit this model, but enough do to suggest that the medium of e-mail carries a McLuhan-style message. This is even more apparent in other cybermethods. Sending spam, for instance, conveys a strong implicit message, regardless of the content, even when the text says "This is not spam!" This is because most people already have a hostile attitude towards spam as a method. In the case of sending encrypted messages, the receiver already knows, without reading the content, that it is private information. Hence the receiver will probably look at it more closely than at a plain-text e-mail.

If a Web site is removed by a government, the government sends out a particular message to the owner of the Web site, namely that it disapproves of the content of the site. Another example is cracking. If some dissidents alter the Web site of a repressive regime, it is not only the altered information that counts. The regime may feel threatened or annoyed without even looking at the changes made. The breaking in and altering itself sends a message of disliking or not approving of the content.

The implicit messages associated with a cybermethod depend on the receiver, the circumstances and other factors. Sometimes many people seem to pick up the same message, as in the widespread hostility to spam, but for other cybermethods there is much greater diversity of response.

Arenas of creation and application

We have not tried to link cybermethods back to the software or hardware by which they are implemented. Looking purely at the code involved, some of the methods are trivial to execute. For example, a Web site can be removed simply by a system administrator deleting a Web address from a list. In technical terms, nothing special is involved. What is crucial for our purposes is the social meaning attached to the action. Similarly, spamming, in technical terms, is a relatively simple extension of sending e-mails, but the social impact of a piece of spam is greatly different from that of a personal e-mail. Because the significance of cybermethods lies in the meanings attached to them, we have not tried to link our classification to similarities and differences in software or hardware.

Lessig [3] distinguishes three "layers" in communication systems: the physical layer, such as wires; the code layer, such as Internet protocols; and the content layer, such as the text of an e-mail message. In this picture, cybermethods are conceptualisations of processes at the code layer.

From a social viewpoint, far more important than technical construction of cybermethods are two social realms: arenas of creation and arenas of application. By

arenas of creation we refer to the social and technical factors that led to cybermethods being developed in the first place. The history of computing and the early development of the Internet were preconditions for all cybermethods. To take a particular example, the cybermethod of encryption grew out a background of pre-computer code making and breaking, out of social contexts in which secure electronic communications were considered important, out of the great skills of individual mathematicians and programmers, and out of the computational possibilities inherent in the number system. The point here is that cybermethods have a social as well as a technical prehistory. Technologies are neither autonomous nor inevitable (Winner, 1977); instead, they are "shaped" by a range of social, political, economic, legal, technical and other factors (MacKenzie and Wajcman, 1999). Just because something is technically feasible does not mean it will be done. Domain grabbing, for example, appears to reflect a commercial, acquisitive culture.

In classifying cybermethods, we are taking a snapshot of a collection of methods that have arisen in particular circumstances. In different circumstances, the prevalent cybermethods could well be different and a different classification system more appropriate. If, hypothetically, commercial imperatives had been much less and the early ethos of sharing remained, then spamming might be unknown and file-sharing not subject to lawsuits.

Arenas of application are where cybermethods are used. Several key arenas are listed in Table 4.

Table 4: Some arenas for application of cybermethods.

- Conventional economics, politics, war, law
- E-commerce
- E-politics
- Information warfare
- E-law
- E-life, cyberreality, Matrix-world

When a corporation sets up a Web site and sends out promotional e-mails but otherwise runs its operations as usual in the physical world, the corporation is using cybermethods as just another medium of communication. This could be considered to be application of cybermethods to conventional economic activity. When, though, a corporation does most of its business over the Internet, as in the case of Amazon.com, then this might be considered to be an application of cybermethods to e-commerce. The dividing line is a matter for discussion. Full-scale e-commerce might involve selling e-documents over the Internet using e-cash.

Similarly, cybermethods can be used in support of conventional politics but at some point there is a transition to e-politics, for example in electronic town meetings. Militaries use cybermethods as an adjunct to conventional methods of communication but can now mount new forms of information warfare, for example to shut down opponents' information systems. The legal system now deals with the Internet as a new arena, with new laws and interpretations. For example, legal frameworks have had to be extended or revised to cover defamation and intellectual property on the Internet, though it is debatable whether this constitutes a qualitative transition to what might be called e-

law.

Finally, there is an arena of application we call "e-life ". Still to be precisely defined, it could be said to cover forms of action and interaction that are peculiar to cyberspace, such as domain name disputes. Some cybermethods, such as remailing and denying service, might be said to be in the realm of e-life. It is always possible to draw analogies between cyberspace and material reality, but some analogies are far earlier to draw than others. Chatting is quite similar to face-to-face conversations and spamming is similar to putting advertisements in letterboxes, but physical world analogies to remailing or denying service are less familiar.

If, as we argue, cybermethods are biased — namely they are media carrying their own message independently of the content — then this bias or inherent message will have an effect in each arena of application where the method is used. For example, many people believe that spamming, as a method, is having a very damaging effect on e-commerce; therefore it is likely to have a similarly damaging effect if used in e-politics or e-law.

The wide scope of the arenas of creation and application points to a large number of possible research topics. Studying the social shaping of cybermethods would involve looking at military, commercial and other influences on the development, expression and use of cybermethods. Studying the impact of cybermethods would involve looking at each arena of application and seeing how particular cybermethods affect it. For example, hacking has implications in every arena of application.

Conclusion

By classifying cybermethods, it becomes easier to make various kinds of assessments. We have noted some characteristic debates, sources of concern and main opponents of the main types of cybermethods (Table 2), discussed cybermethods as "technologies with politics" and as media, and looked at the arenas of creation and application of cybermethods.

Many users have gut reactions to certain cybermethods, for example hating viruses and lauding the freedom of speech available through e-mail and the Web. Writings on "appropriate technology" provide a way of systematising such reactions [4]. Appropriate technology is a label applied to technologies designed to fit the needs of poor peoples in poor countries. Given a surplus of labour, shortage of capital and the urgency of satisfying basic human needs, examples of appropriate technology include simple-to-construct ox carts, small farm grain storage methods, techniques of growing tropical fruit trees, inexpensive water filtration techniques, self-built stoves, biogas generators, inexpensive techniques for house building, and community health care techniques (Darrow and Saxenian, 1986). Inappropriate technology for poor communities includes expensive, high-tech and expert-dependent power plants, large dams and genetically engineered crops, since these aggravate unemployment and perpetuate dependence. Appropriate technologies by themselves do not create social change, but they can be part of a process of local empowerment (Galtung et al., 1980).

In cyberspace, then, what are appropriate methods? We have argued that cybermethods are not neutral but instead can be thought of as media, each with an implicit message. So, in a sense, appropriate cybertechnology is choosing the appropriate medium, namely

the one that has an appropriate message built in to the method itself.

To speak of appropriate cybertechnology assumes access to the technology, which involves equipment, knowledge, costs and language skills. Assuming such access, those cybermethods that are most suited for interaction between equals and have the lowest potential for harming others are the methods of expressing and protecting. So we might conclude that these types of methods are most appropriate for promoting egalitarian communication. Methods of interfering, on the other hand, are less suited for interaction between equals and are easier to use for domination or inflicting harm. Methods of information gathering stand in an intermediate position. This suggests that if the goal is open and equal participation in cyberspace, methods of expressing and protecting are to be encouraged and developed, though their abuses should still be opposed. Similarly, development of methods of interfering and, to a lesser extent, information gathering, warrant closer scrutiny if they are to be used in a responsible fashion, if at all. After all, these are the methods most commonly used by repressive governments (Goldstein, 1999; Kalathil and Boas, 2001).

Of course, not everyone will share values such as equality and participation. But whatever one's values, it is important to realise that cybermethods are not neutral vessels but rather incorporate values of their own. To paraphrase McLuhan, "the cybermethod is the message".

About the Authors

Hellen Megens is a doctorandus student at Tilburg University. Her dissertation deals with cyberactivism.
E-mail: hellenmegens@hotmail.com

Brian Martin is associate professor in Science, Technology and Society, University of Wollongong, Australia. He is the author of 10 books and many articles on nonviolent action, dissent, information issues and other topics.
Web: http://www.uow.edu.au/arts/sts/bmartin/
E-mail: bmartin@uow.edu.au

Acknowledgments

We thank Fons Maes and Danny Yee for valuable comments on earlier drafts. Graham Barwell, Yoke Berry, Andrew Nicholson, Catherine Waerner and Brian Yecies offered helpful suggestions at a seminar.

Notes

1. See Feenberg (1991) on the bias of technology.

2. McLuhan and Zingrone, 1997, p. 239.

3. Lessig, 2001, pp. 23-25.

4. Illich, 1973; McRobie, 1981; Riedijk, 1986; for a critique see Willoughby, 1990.

5. Schneier, 2000, pp. 135-150.

6. Wishart and Bochsler, 2002, pp. 266-271.

7. Schneier, 2000, pp. 181-186.

8. Jordan, 2002, pp. 119-135.

References

2600, at http://www.2600.com/, accessed 11 November 2002.

Roger Clarke, 2001. "Cookies,"at http://www.anu.edu.au/people/roger.Clarke/II/Cookies.html, accessed 2 January 2003.

Matt Curtin and Marcus J. Ranum, 2000. "Internet firewalls: Frequently asked questions," at http://www.interhack.net/pubs/fwfaq/, accessed 3 January 2003.

Ken Darrow and Mike Saxenian, 1986. *Appropriate technology sourcebook: A guide to practical books for village and small community technology.* revised and enlarged edition. Stanford, Calif.: Appropriate Technology Project, Volunteers in Asia.

Whitfield Diffie and Susan Landau, 1998. *Privacy on the line: The politics of wiretapping and encryption.* Cambridge, Mass.: MIT Press.

Andrew Feenberg, 1991. *Critical theory of technology.* Oxford: Oxford University Press.

Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, 1997. "Web spoofing, an Internet con game," 20th National Information Systems Security Conference (Baltimore, Maryland) (October), at http://www.cs.princeton.edu/sip/pub/spoofing.html, accessed 13 December 2002.

Johan Galtung, Peter O'Brien and Roy Preiswerk (editors), 1980. *Self-reliance: A strategy for development.* London: Bogle-L'Ouverture.

Steve Gibson, 2002. "The strange tale of the denial of service attacks against grc.com," at http://grc.com/, accessed 2 January 2003.

Emmanuel Goldstein, 2002. "Hackers: Knight-errants or knaves," at http://www.msnbc.com/news/178451.asp?cp1=1, accessed 28 October 2002.

Eric Goldstein, 1999. *The Internet in the Mideast and North Africa: Free expression and censorship.* New York: Human Rights Watch.

Roger A. Grimes, 2001. *Malicious mobile code: Virus protection for Windows.* Cambridge, Mass.: O'Reilly.

Wendy M. Grossman, 1997. *Net.wars.* New York: New York University Press.

Nicky Hager, 2000. "International co-operation in Internet surveillance," *Telepolis: Magazin der Netzkultur* (22 November), at http://www.heise.de/tp/english/special/enfo/4306/1.html, accessed 17 December 2002.

Nicky Hager, 1996. *Secret power: New Zealand's role in the international spy network.* Nelson, N.Z.: Craig Potton.

Janice J. Heiss, 2000. "Email just got radical," at http://java.sun.com/features/2000/04/emailrad.html, accessed 11 December 2002.

Lance J. Hoffman (editor), 1995. *Building in big brother: The cryptographic policy debate.* New York: Springer-Verlag.

Michael Howard and David C. Leblanc, 2002. *Writing secure code.* Redmond, Wash.: Microsoft Press.

Ivan Illich, 1973. *Tools for conviviality.* London: Calder & Boyars.

Bernward Joerges, 1999. "Do politics have artefacts?" *Social Studies of Science,* volume 29, number 3 (June), pp. 411-431.

Tim Jordan, 2002. *Activism! Direct action, hactivism and the future of society.* London: Reaktion Books.

Shanthi Kalathil and Taylor C. Boas, 2001. "The Internet and state control in authoritarian regimes: China, Cuba, and the counterrevolution," *Working Paper, number 21.* Washington, D.C.: Carnegie Endowment for International Peace.

The Knightmare, 1994. *Secrets of a super hacker.* Port Townsend, Wash.: Loompanics.

Lawrence Lessig, 2001. *The future of ideas: The fate of the commons in a connected world.* New York: Random House.

Steven Levy, 2001. *Crypto: Secrecy and privacy in the new code war.* Harmondsworth: Penguin.

Donald MacKenzie and Judy Wajcman (editors), 1999. *The social shaping of technology.* Second edition. Buckingham: Open University Press.

Jerry Mander, 1978. *Four arguments for the elimination of television.* New York: William Morrow.

Mark Manion and Abbey Goodrum, 2001. "Terrorism or civil disobedience: Toward a hacktivist ethic," In: richard A. Spinello and Herman T. Tavani (editors). *Readings in cyberethics.* Sudbury, Mass.: Jones and Barlett.

Carolyn Duffy Marsan, "DDos attack highlights 'Net problems," at http://www.nwfusion.com/news/2002/1028ddos.html, accessed 5 November 2002.

Brian Martin, 2000. "Defamation havens," *First Monday,* volume 5, number 3 (March), at http://firstmonday.org/issues/issue5_3/martin/, accessed 17 December 2002.

Eric McLuhan and Frank Zingrone (editors), 1997. *Essential McLuhan.* London: Routledge.

Marshall McLuhan, 1964. *Understanding media: The extensions of man.* London: Routledge & Kegan Paul.

George McRobie, 1981. *Small is possible.* London: Jonathan Cape.

Joshua Meyrowitz, 1994. "Medium theory," In: David Crowley and David Mitchell (editors). *Communication theory today.* Cambridge: Polity Press, pp. 50-77.

Geoff Mulligan, 1999. *Removing the spam: Email processing and filtering.* Reading, Mass.: Addison-Wesley.

Fred Piper and Sean Murphy, 2002. *Cryptography: A very short introduction.* Oxford: Oxford University Press.

Willem Riedijk, 1986. *Technology for liberation: Appropriate technology for new employment.* Delft: Delft University Press.

Heath Row, 1998. "Remember netiquette? Now there's chatiquette!," *FastCompany,* issue 15 (June-July), at http://www.fastcompany.com/online/15/chatiquette.html, accessed 17 December 2002.

Julia Scheeres, 2002. "Porn spam, it's getting raunchier," *Wired News* (30 September), at http://www.wired.com/news/culture/0,1284,55420,00.html?tw=wn_ascii, accessed 17 December 2002.

Bruce Schneier, 2000. *Secrets and lies: Digital security in a networked world.* New York: Wiley.

Andrew Schulman, 2001. "Computer and Internet surveillance in the workplace: rough notes," at http://www.sonic.net/~undoc/survtech.htm, accessed 13 December 2002.

Simon Singh, 2002. *The code book: How to make it, break it, hack it, crack it.* New York: Delacorte.

Marc Slayton, 1996a. "An Introduction to cookies," *Webmonkey* (7 November), at http://hotwired.lycos.com/webmonkey/geektalk/96/45/index3a.html, accessed 13 December 2002.

Marc Slayton, 1996b. "The risks of cookies," *Webmonkey* (3 January), at http://hotwired.lycos.com/webmonkey/geektalk/96/53/index4a.html, accessed 13 December 2002.

Jeff Tyson, 2002. "How firewalls work," *HowStuffWorks,* at http://www.howstuffworks.com/firewall.htm, accessed 3 January 2003.

Sandor Vegh, 2002. "Hacktivists or cyberterrorists? The changing media discourse on hacking," *First Monday,* volume 7, number 10 (October), at http://firstmonday.org/issues/issue7_10/vegh/, accessed 17 December 2002.

Jonathan Wallace, 1997. "The X-Stop files," *First Monday,* volume 2, number 12 (December), at http://firstmonday.org/issues/issue2_12/wallace/, accessed 8 December

2002.

Kelvin W. Willoughby, 1990. *Technology choice: A critique of the appropriate technology movement.* Boulder, Colo.: Westview Press.

Langdon Winner, 1986. *The whale and the reactor: A search for limits in an age of high technology.* Chicago: University of Chicago Press.

Langdon Winner, 1977. *Autonomous technology: Technics-out-of-control as a theme in political thought.* Cambridge, Mass.: MIT Press.

Adam Wishart and Regula Bochsler, 2002. *Leaving reality behind: The battle for the soul of the Internet.* London: Fourth Estate.

Appendix: A catalogue of cybermethods

Expressing

E-mailing

Description
E-mail is the abbreviation for electronic mail, a method of transferring messages using the Internet.

Examples
E-mails can be used to send messages to and receive them from a friend, a co-worker, a business organization or a government. Whether an e-mail sent by a robot, as in an automated reply, counts as expressing is a matter for debate.

More information
Heiss (2000) tells about the impact of e-mail and the changes it has gone through.

Chatting

Description
On the Internet, chatting is exchanging messages or talking with other people in real time. This chatting can be done in special chat rooms, or via a chat server.

Examples
MSN Messenger: http://www.msn.com is an example of a chat client. Examples of chat rooms can be found on Yahoo (http://chat.yahoo.com/?myHome), ICQ.com (http://web.icq.com/) and Lycos (http://clubs.lycos.com/live/Chatrooms/ChatHome.asp?Area=1).

More information
Row (2000) describes chat etiquette.

Web site uploading

Description
Web site uploading is simply the migration of Web content or pages to a server, so other

users can access them.

Examples
Commercial, political, nonprofit and personal sites can be uploaded using programs such as Cute FTP (http://www.cuteftp.com/).

More information
On the practicalities of Web site uploading, see:

- City Collegiate http://www.citycollegiate.com/web_publishing.htm
- Digital revolution: Web site uploading http://www.angelfire.com/bc3/digitalrev/Websiteupload.htm
- Uploading your site: http://www.vidocpublications.com/uploading/uploadindex.htm.

File sharing

Description
File sharing is the public or private sharing of computer data or space, in a network with various levels of access privilege.

Examples
Files can be shared between students and instructors, between business associates, or between friends.

More information
On the practicalities of file sharing, see:

- Winmix, at http://www.winmx.com/
- Intranet file sharing, at http://www.ostafiev.com/ifs/
- File sharing, at http://www.webdesk.com/file-sharing/

Protecting

Authenticating

Description
Authenticating means verifying one's identity or access rights.

Examples
Passwords are used in most e-mail accounts. They can also be used to limit access to certain pages on a Web site to specific users, for example private pictures to friends, an online CV to authorised persons only, a draft of a novel or article to a chosen few. Other methods of authenticating are biometrics, such as fingerprints or voice recognition, and challenge-response systems, where correct answers must be give to questions.

More information
Schneier [5] gives a nice summary of strengths and weaknesses of methods of authentication. On the practicalities of password protecting, see:

- JavaScript Kit, at http://javascriptkit.com/script/cutindex6.shtml
- Password protecting Web pages, at http://www.hwg.org/lists/hwg-servers/passwords.html
- Personal Web server documentation, at http://www.uchicago.edu/docs/home-

doc/password.html

Filtering (self-chosen)

Description
Filtering is the process of screening out undesired material. This category includes only voluntary filtering; for involuntary filtering, see the entry "Denying access".

Examples
Filtering programs can be used to block spam and other undesired messages in an e-mail account. Filtering can be carried out at any network level, from firewalls to personalised software. At the physical level, filtering can be accomplished by pulling the plug!

More information
To use filters against undesired e-mail, see:

- Mulligan (1999)
- A plan for spam, at http://www.paulgraham.com/spam.html
- Electric Mail Company Services, at http://www.electricmail.com/ele/64

On firewalls, see Curtin and Ranum (2000) and Tyson (2002).

Encrypting

Description
Encryption scrambles data so others can't understand it. Usually some kind of key system is needed to unscramble it.

Examples
People can use encryption for different purposes, for instance sending or storing private data, business data, or secret government information.

More information

- "How electronic encryption works and how it will change your business", at http://www.viacorp.com/crypto.html
- Encryption Tutorial, at http://hotwired.lycos.com/webmonkey/programming/php/tutorials/tutorial1.html
- Howard and LeBlanc (2002) and Piper and Murphy (2002) give technical accounts of encryption.
- Levy (2001) describes the politics of encryption.

Remailing

Description
Anonymous remailers allow you to send and receive e-mail while hiding your identity.

Examples
A few people use anonymous remailers to express their opinions or leak information without risking the wrath of their boss or government authorities. For example, dissident scientologists sent secret information to e-mail lists, remaining anonymous by using remailers. Scientologists used a court order to obtain the senders' identity from a remailer (Grossman, 1997).

More information

- The Official Remailing Guide, at http://www.remail-snailmail.com/contents.html
- Continental Relay.com, at http://www.continentalrelay.com/br/

Information Gathering

Web browsing

Description
Web browsing is simply the act of using a Web browser to visit Web sites.

Examples
Web browsing can be used to find information on virtually any topic. Sometimes people randomly "surf" from site to site, but often a search engine is used to give possible links. Examples of search engines are AltaVista, Google and Yahoo.

More information

- Guide to Web browsing, at http://www.doi.gov/octc/web.html
- Letizia, an agent that assists Web browsing, http://lieber.www.media.mit.edu/people/lieber/Lieberary/Letizia/Letizia.html

Web data collecting

Description
When people use the Web, information can be gathered about which specific sites are visited, including when and how frequently.

Examples
Cookies are messages given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of a cookie is to identify users and possibly prepare customized Web pages for them. Instead of seeing just a generic welcome page, you see a welcome page with your name on it. Cookie collecting nominally involves users gathering information from Web servers, but in practice the more important gathering of information is from the other end, such as when corporations build databases from cookie files. Even without cookies, information on Web use can be obtained by analysing Web server logs.

Traffic analysis involves collecting information on communication patterns, such as the timing and length of e-mails between two individuals.

More information

- Clarke (2001); Slayton (1996a, 1996b).
- Cookie Central.com, at http://www.cookiecentral.com/

Hacking

Description
Hacking is a way to gather information by breaking into a computer system of an organization or an individual user. Hackers do this in various ways, for example through

repeated attempts using different passwords, by exploiting flaws in computer security systems, or by social engineering. Social engineering is getting information by persuading people, often deceptively, such as by phoning a system administrator saying "I've forgotten my password" or by finding passwords in trash cans.

The meaning of the word "hacking" has changed over time. Originally it meant building hardware and software and was considered admirable. Media coverage has increased public awareness of hacking but changed the meaning in a negative way.

Examples
Gathering information by surreptitiously entering the computer system of a government or company.

More information

- *2600: The Hacker Quarterly*, a magazine of comment and technical information, at http://www.2600.com/
- *Blacklisted! 411*, a hacker magazine, at http://www.blacklisted411.com/
- *The Knightmare* (1994) is a hacker's inside story.

Surveillance

Description
Internet surveillance means monitoring or intercepting e-mail and Web use.

Examples
Some employers monitor Web and e-mail use by their employees. Some government agencies intercept satellite and other transmissions. Police and private investigators may directly intercept electronic communication by using wire taps or emission detectors. Internet service providers can monitor e-mails, legitimately for technical reasons or less legitimately for personal amusement or criminal purposes.

More information

- Hager (2000), Schulman (2001)
- On Echelon, a global electronic monitoring system, see Hager (1996) and Echelon at http://www.echelon.com/
- Internet Surveillance Software, at http://www.internet-surveillance-software.com/

Interfering

Spamming

Description
Spamming is the mass distribution of unrequested e-mail messages to individual e-mail accounts, e-mail lists or newsgroups, typically with robots.

Examples
Chain letters, promotion of pornographic Web sites or sales promotions.

Spam can be considered a type of denial-of-service attack, in which the result is a degradation of service for the entire Internet rather than for a single user.

More information

Scheeres (2002) discusses porn spam.

For opposing spam, see:

- CAUBE.AU, Coalition Against Unsolicited Bulk Email, Australia, at http://www.caube.org.au/
- Slamming Spamming, at http://www.uic.edu/depts/accc/newsletter/adn29/spam.html
- Internet Society, All about the Internet, at http://www.isoc.org/internet/issues/spamming/
- Anti-Spamming Act, at http://members.tripod.com/antispamming/asa.htm

Denying access

Description
E-mail access can be prevented by rejecting applications or by terminating accounts. Web access can be blocked by imposing filters.

Examples
A parent may deny a child Internet access or require a filter. An employer may terminate an employee's e-mail account. A government can block access to certain political Web sites.

Anti-spamming software could be considered as denying access. This raises the question of whether robots (which are usually used to send spam) have free speech.

More information

- Wallace (1997) discusses issues concerning Internet filters.
- A Dozen reasons why schools should avoid filtering, at http://www.fno.org/mar96/whynot.html

Denying service

Description
A denial of service (DoS) attack aims to overload a Web site or e-mail account. The tactic of making repeated attempts to communicate with a computer is called flooding. Sending massive numbers of e-mails to an account is called mail bombing. There are programs that can mount an attack automatically from a single point. Alternatively, attacks can come from many sources simultaneously, called a distributed DoS attack.

Examples
Steve Gibson (2002) provides an entertaining account of DoS attacks against his site. In the domain-name struggle between etoy, an artistic collective, and eToys, an online toy company, the group @TMark organised a denial-of-service attack against eToys [6].

More information

- Tackling Network DoS on Transit Networks, at http://www.dante.net/pubs/dip/42/42.html
- Marsan (2002); Schneier [7]
- Denial of Service Attack (DoS) at

http://securityresponse.symantec.com/avcenter/venc/data/dos.attack.html

Web site removal

Description
Web site removal is the closure of Web sites by system administrators, at their own initiative, or at the instruction of owners or judges.

Examples
An employer shuts down an employee's site; an ISP shuts down a site after receiving a defamation threat; a government shuts down a site run by political opponents.

More information

- Attorney General urged to shut down racist Website, at http://www.ontariondp.on.ca/news/publish/printer_31.shtml
- Martin (2000) tells about the use of defamation threats against Web material.

Sending malicious code

Description
Malicious code — also called malware — includes viruses, worms and Trojan horses. A virus is computer code that can attach itself to files or applications and cause problems related to the performance of a computer. Like a biological virus, a computer virus cannot live on its own and can only replicate by attaching copies to other programs. Viruses these days are usually sent through e-mail, intentionally or inadvertently.

A worm, in contrast, can replicate itself, eating up storage space and slowing down the computer, and may also delete files or do other damage. A Trojan horse is a damaging program disguised as something benign such as a screen saver. When loaded onto your machine, a Trojan horse can capture information from your system — such as user names and passwords — or could allow a cracker to remotely control your computer.

Examples
Recent examples of viruses can be found on Expanded Threat List, at http://securityresponse.symantec.com/avcenter/vinfodb.html/.

More information

- Grimes (2001)
- Introducing the Secure Enterprise, at http://www.symantec.com/
- Virus Information, at http://www.mcafee.com/anti-virus/default.asp
- Virus Information Center, at http://www3.ca.com/virusinfo/

Domain grabbing

Description
Domain grabbing involves illicitly obtaining traffic intended for another domain. It can be accomplished by:

- typo pirating: setting up a site with a name almost identical to a legitimate site;
- domain vampiring: purchasing an accidentally expired domain name;
- spoofing: manipulating Web addresses so that a user unknowingly browses via a spoof site, allowing the attacker to eavesdrop on the victim's activity and

passwords;
- page-jacking: setting keywords and meta tags on a Web site so that search engines list the site ahead of a popular site, thereby getting unsuspecting users to visit the fake site (often a porn site).

Examples
Domain vampires can capture company domain names and fan sites. Spoofing has been used against bank sites, tourist organization sites and other types of commercial sites.

More information

- Felten et al. (1997)
- DomainVampires.Com at http://domainvampires.com/victims.html
- Why spoofing is the number one security problem on the Internet, and how we should fight it, at http://www.xs4all.nl/~rmeijer/spoofing.html

Cracking

Description
Cracking is breaking into a computer system of a corporation, individual user, or a government agency and then stealing altering or destroying information. Both hacking and cracking involve breaking into a computer system. We have distinguished between hacking ('just looking') and cracking (stealing or altering), though many people call both of these hacking.

A related concept is hacktivism, which can be defined as political motivated hacking or cracking. Hacktivism cuts across our distinction between hacking and cracking.

Examples

All sorts of sites have been altered by intruders, including government and business sites. Criminals have stolen passwords and other information.

More information

- Goldstein (2002) distinguishes between hackers and crackers.
- Vegh (2002) discusses media representations of hacking and cracking.
- Jordan [8] describes hactivism.
- Manion and Goodrum (2001) discuss whether hacktivism is terrorism or civil disobedience.
- Singh (2002).

Editorial history

Paper received 20 January 2003; accepted 1 February 2003.

Contents Index

Copyright ©2003, First Monday

Copyright ©2003, Hellen Megens

Copyright ©2003, Brian Martin

Cybermethods: An assessment by Hellen Megens and Brian Martin
First Monday, volume 8, number 2 (February 2003),
UrL: http://firstmonday.org/issues/issue8_2/megens/index.html