collaborative filtering. We need a language in which to appraise the Google page rank algorithm. An examination of the de-politicization of algorithms will help.

A final ramification of protocological organization and control is that it mandates the creation of new models for political intervention. Networks, rhizomes, 'grass roots' movements – these were all effective diagrams for political control under modernity. But after the powers-that-be have migrated into the distributed network, thereby co-opting the very tools of the former Left, new models for political action are required. A new exploit is necessary, one that is as asymmetrical in relationship to distributed networks as the distributed network was to the power centers of modernity. In the meantime anti-protocological movements have emerged such as Hakim Bey's model of the temporary autonomous zone (2003), or the Electronic Disturbance Theatre's system of online electronic swarming. And in the realm of the non-human, computer viruses and worms have innovated, perhaps totally haphazardly, a new model of protocological infection and disruption that takes advantage of the homogeneity of distributed networks and their ability to propagate information far and wide with ease. At the same time hackers seek out logical exploits in software that allow for inversions and modulations in the normal functionality of code. These techniques, if not fully formed themselves, will provide a way forward for understanding protocological control and counter-protocological practices.

References

Arquilla, J. and D. Ronfeldt (2001) *Networks and Netwars*. Santa Monica, CA: RAND.

Bey, H. (2003) *T.A.Z*. New York: Autonomedia.

Baran, P. (1964) *On Distributed Communications*. Santa Monica, CA: RAND.

Deleuze, G. (1986) *Foucault*. Minneapolis, MN: University of Minnesota Press.

Deleuze, G. (1990) *Negotiations*. New York: Columbia University Press.

Deleuze, G. and F. Guattari (1987) *A Thousand Plateaus*. Minneapolis, MN: University of Minnesota Press.

Foucault, M. (1978) *The History of Sexuality, Vol. 1*. New York: Vintage.

Foucault, M. (1997) *Ethics: Subjectivity and Truth*. New York: New Press.

Hall, E. (2000) *Internet Core Protocols: The Definitive Guide*. Sebastopol, CA: O'Reilly.

Shannon, C. and W. Weaver (1998) *The Mathematical Theory of Communication*. Champaign, IL: University of Illinois Press.

Stevens, W.R. (1994) *TCP/IP Illustrated, Volume 1*. New York: Addison-Wesley.

Thacker, E. (2004) *Biomedia*. Minneapolis: University of Minnesota Press.

Von Bertalanffy, L. (1976) *General System Theory*. New York: George Braziller.

Wiener, N. (1965) *Cybernetics, or Control and Communication in the Animal and the Machine*. Cambridge, MA: MIT Press.

Alexander R. Galloway is an assistant professor at New York University. He is the author of *Protocol: How Control Exists After Decentralization* (MIT Press, 2004) and a founding member of the software development group RSG.

Hackers

McKenzie Wark

Keywords class, computing, ethics, information, intellectual property

The figure of the 'hacker' is a new and distinctive one in the social history of the late 20th century. The hacker probably first emerged out of the electrical engineering labs at the Massachusetts Institute for Technology (MIT). As on many campuses, MIT students had a tradition of creating attention seeking pranks – which at MIT were called 'hacks'. The term hack migrated from this general student inventiveness to a more specific sense of creative invention with given materials in the context of electrical engineering, out of which computing as a distinct discipline was to grow.

Not all computing at MIT or elsewhere qualified as 'hacking'. It had distinct qualities. 'To qualify as a hack, the feat must be imbued with innovation, style and technical virtuosity' (Levy, 1994: 23). Hacking was at once an aesthetic and an ethic, in which cooperation among hackers

was achieved through their mutual desire for recognition, achieved via improvements or modifications to each other's programming code. As Richard Stallman, a legendary figure in hacker culture, says: 'It was a bit like the garden of Eden. It hadn't occurred to us not to cooperate' (Williams, 1992: 76).

The academic environment in which hacking first emerged contributed greatly to the ethic of collaboration on shared goals via competition for recognition. What was distinctive was the extension of recognizably academic social processes into this new technical area. Hackers were, at the same time, largely indifferent to formal recognition within the academy or industry. The recognition of one's peers was what mattered.

Early development of computing at MIT, Stanford and elsewhere was heavily dependent on funding provided by the Pentagon, which offered very broad support for basic computing research in the 1950s and 1960s. This certainly contributed to the rather special culture of hacking. As the Pentagon narrowed its research interests, and commercial computing industries grew, hacker culture came under pressure from administrative and commercial imperatives. It survived, for a time, due to the high demand for scarce computing skills.

Hacking persists as something of a governing ideal in programming. A 'hacker ethic', with roots in early computing research experience, exists as something like a craft sense of what programming as a kind of labor ought to be. Hackers, who 'want to realize their passions', present 'a general social challenge', but the realization of the value of this challenge 'will take time, like all great cultural changes' (Himanen, 2001: 7, 18, 13).

As computing became a pervasive force with the rise of the Internet, 'hacking' developed a second meaning – it named the process of exploring computer networks. In many cases this was benign. The Internet was a new and not well-understood phenomenon, and hackers in this sense were explorers of this new terrain. However, once computer networks were conceived as a new form of 'property', transgressions of these putative property boundaries were quickly criminalized (Sterling, 1993). A 'moral panic' ensued, in which the hacker appeared as a new kind of folk devil, recklessly invading networks, interrupting essential services, stealing state secrets or credit card numbers. In order to preserve the original meaning of the term hacker, those who exploit weaknesses in computer networks for criminal reasons are sometimes referred to as 'crackers'.

Nevertheless, even the most benign, creative, ethical and aesthetic version of the idea of the 'hacker' presents something of a challenge to the social order, for the hacker is a figure that speaks to the ideal of a kind of labor that finds its own time, that sets its own goals, and that works on common property for the good of all. As Michael Hardt and Antonio Negri argue, many of the new kinds of labor processes that emerged in the late 20th century have a distinctively cooperative element. 'The central forms of productive cooperation are no longer created by the capitalist as part of the project to organize labor but rather emerge from the productive energies of labor itself' (Hardt and Negri, 2004: 113). The hacker is the embodiment of this self-organized labor.

The rise of the hacker meets an antithetical development in the rise of strict and extensive intellectual property law. At MIT, hackers worked freely on each other's code, gave code to others and did not secure their files – to do so would only invite others to circumvent the security. This model of free, self-organized labor took place under very special conditions – in research labs with large amounts of Pentagon funding. Yet it provided an ethic of working with information that spread far beyond this academic setting. The sharing of information became a hallmark of early Internet culture. This was perceived to be an obstacle to its development as a commodity by the new forms of business that wanted to invest in it.

The crackdown on hacker culture in its more transgressive sense, and the containment of the hacker ethic in its more benign sense, are two parts of the process of the commodification of computing networks in the interests of restricting the free movement of information and the expansion of the concept of information as private property. If an early slogan of hacker culture has it that 'information wants to be free', it finds itself, to borrow from Rousseau, 'everywhere in chains' (Wark, 2004: 126).

With the rise of corporations based on computing as labor and information as property, hacker culture responded with new legal models within which hacker culture might survive. These would include the Free Software Movement, and its more corporate offshoot, the Open Source Movement (Moody, 2001). The Creative Commons Movement seeks a broader platform for collaborative labor with information (Lessig, 2004). Where corporations dependent on information generally seek policy solutions that turn copyrights and patents into absolute private property rights, the Creative Commons Movement extends the hacker ethic to all information, seeking forms of legal protection for collaborative labor.

More broadly still, the hacker may be the symptom of a broader class struggle over information, which pits those who produce it – hackers in the very broadest sense – against those who own

the means of realizing its value – the corporations whose value is increasingly defined not by tangible assets, but by portfolios of patents, copyrights and brands. Thus, the hacker may turn out to be a very important social category for understanding labor, the commodity and private property in the information age.

References

Hardt, M. and A. Negri (2004) *Multitude*. New York: Penguin Books.

Himanen, P. (2001) *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House.

Lessig, L. (2004) *Free Culture*. New York: Penguin.

Levy, S. (1994) *Hackers: Heroes of the Computer Revolution*. New York: Penguin.

Moody, G. (2001) *Rebel Code*. Cambridge, MA: Perseus Publishing.

Sterling, B. (1993) *The Hacker Crackdown*. New York: Bantam.

Wark, M. (2004) *A Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Williams, S. (1992) *Free as in Freedom: Richard Stallman's Crusade for Free Software*. Sebastapol, CA: O'Reilly.

McKenzie Wark is the author of *A Hacker Manifesto* (Harvard University Press, 2004), *Virtual Geography* (Indiana University Press, 1994) and other works. He teaches at Eugene Lang College and The New School for Social Research in New York City.