
Alleyne, Brian

“We are all hackers now”: critical sociological reflections on the hacking phenomenon

"We are all hackers now": critical sociological reflections on the hacking phenomenon

Brian Alleyne

Department of Sociology, Goldsmiths, University of London

b.alleyne@gold.ac.uk

The paper connects earlier work to more recent developments. It calls for a re-imagination of hacking against the backdrop of late capitalist network society. Hacking is discussed in terms of open and clandestine practices, 'hacktivism' and hardware hacking. The paper concludes by sketching the outlines of an integrated sociological understanding of hacking, one which can account for the varied representations and practices that constitute hacking in the contemporary world.

Keywords

Hackers, computer hacking, sociology of information technology, computer programming, activism

Introduction

Hacking is a contested term and this paper will explore the many and sometimes contradictory ways in which the activity is construed and represented, but as a first approximation I suggest that we view it as an activity which encompasses computer

programming, circumventing security systems designed to protect computer networks and digital data stores, designing and executing solutions to solve problems by combining software and hardware in unconventional ways, and modifying and re-purposing digital products of all kinds.

A 'hack' is an efficient, and often unconventional application of technology. According to Levy's (2010[1984]) canonical account, the hack was first an engineering accomplishment in hardware, and later came to take on the meaning of an original and efficient programming solution to problems in software. The term is one which carries a high evaluative semantic loading. In computer science a 'hack' is seen as an inelegant but effective solution to a programming problem; hacks may be at times necessary but only in the sense of a necessary evil. By contrast, in the computing cultures that emerged in the late 1960s and that have have been spreading and consolidating globally ever since, a 'hack' carries more positive connotations than in formal computer science: in this latter context, inelegant though the hack might be in formal academic or engineering terms, it is widely admired for its efficiency and ingenuity, and can then come to be regarded as elegant, in an intriguing semantic reversal. In the subcultures where breaking into secure computer systems is a central activity, the hack is an episode, an 'exploit', in which the hacker successfully circumvents layers of electronic and sometimes physical security in order to gain access to the innards of computer networks. Ideas of creativity, individuality, adaptability, and originality abound in discourses of hacking, as early identified by Turkle (1985; Turkle and Papert 1990).

Among the most widely cited works on hacking in the sociological literature are the studies by Taylor and Jordan (Jordan & Taylor 1998; Jordan 2004; Taylor 1999, 2005). Their writing has constituted a sociological understanding of the field of hacking, ranging from a criminalised subculture to a counter culture of hacking activists (‘hacktivists’). Their work highlighted the contested nature of the term hacking and explored on-going conflict between the computer security industry and many hackers; they directed attention to hacking as a

political activity where politics could and often did take on varied meanings.

Taylor (1999) found that hackers were mainly male, often unconventional in outlook, in some cases extremely individualistic. He cautioned against negative stereotyping of computer hackers, especially given the fact that the main opposition to many hackers, namely the computer security industry, has incomparably better resources with which to manipulate the public perception of hackers, and does so, Taylor shows, in a manner that actively encourages outsiders to view hackers as criminals. Within the overwhelmingly male population of hackers we find considerable variation in terms of age group, level of education, social class background, political affiliation, and with the increasing globalisation of information technology, ethnicity and national origin. What began as an activity centred on middle class, highly educated, socially reclusive white males in North Atlantic societies is expanding to incorporate a transnational spread of still mainly men, from a variety of socio-economic and cultural backgrounds.[1]

There may well be good reasons to think of hacking as a key element of the culture of late capitalism, but the aims of the present paper are more modest than to propose such. This paper revisits the on-going conflict over the definition of 'hacker', and suggests that we may usefully approach hacking in terms of a core dichotomy between open and closed/clandestine modes of hacking, though it must be noted that there is considerable overlap between the two modes in actual hacking practice. This core dichotomy is advanced as a starting abstraction, a framing device that marks the limits of a continuum along which exist actual hackers and their instantiations of hacking. The paper explores the following questions: What kinds of persons and activities are captured under the heading of 'hacker'? What are the elements of hacker cultures? Given an engagement with the above questions, what should be the form of a contemporary sociological understanding of hackers and hacking?

The core dichotomy of hacking: Clandestine vs. Open

A sociology of hacking, as any other sociology, is in part an exercise in the modelling of sociological objects, and these objects are not the same as the persons and structures and practices which we attempt to understand through the models that we build as sociologists (Bourdieu, Chamboredon, and Passeron 1991). In presenting a 'core dichotomy' as shaping the literature on hacking, I am not arguing that actual hackers and their practices fit tidily on one or the other side of that dichotomy, rather, I employ the dichotomy in terms of its utility as a high-level abstraction. Such an abstraction is useful in that it can help us to step back from both the complex reality of hacking and the considerable body of representations of hacking, in order to gain the epistemological distance necessary to exercise our sociological imagination.

The pioneering hackers of the late 1960s and early 1970s, were committed to sharing and openness (Levy 2010), which remain characteristic of most hacking cultures (Himanen 2001). Against this, the 1980s saw the emergence of a new breed of hacker who operated in a clandestine fashion, whose main aim was to circumvent security systems, whether for reputation, to do damage to these systems, or for personal gain (Taylor 1999). By the early 1990s the dual contradictory faces of hacking were apparent to most observers, and with growing public awareness of hackers and their activities came increased anxieties at public and official level. Then, in the wake of the attacks of September 2001, hacker activity that had been seen as criminal began to be discussed by many governments in terms of 'cyberterrorism', a term which is more indicative of moral panic than of any actual hacker activity.

Dichotomy between the open and the clandestine in the world of hacking is also articulated in terms of the interplay of Black Hats, who are clandestine and often portrayed as criminal, vs. White Hats, who work in both open and clandestine modes, but always (ideally) with the intention of upholding the law in their battles against the Black Hats. The simplistic character of this Manichean representation is recognised in much of the academic and professional information systems and security industry literature, if not in the mass media reporting on hackers. Complicating the matter even further is the case of ethical hacking, one form of which involves a hacker seeking to penetrate a secure computer network so as to aid the administrators of that network in strengthening their security measures (Harris et al. 2008).

Work on hackers and hacking constitutes a diverse and uneven body of literature[2], and in some of it the methods of collecting data do not fit neatly within sociological research paradigms. We may illustrate this by looking at six peer-reviewed journals in which work on hacking has been published (these six are selected as representative of the field as a whole; no quantification of the published articles is done, as such it is not relevant to the current discussion; nonetheless, a quantitative analysis of what has been published on hackers may be in itself revealing in another context). While there is overlap in terms of discipline, coverage of hacking in this literature falls under three broad heads: first, we have journals that are interdisciplinary, but with emphasis on computer science and informatics; second, we have journals that are again interdisciplinary, but informed mainly by social sciences and cultural studies; and third we have journals with a focus on computer security from an industry perspective. As examples of the first we have Information and Organization, and Information Systems Journal; in both of these journals we have papers published in which hacking is a secondary concern. For the second type, in which the perspective is mainly social and cultural theory, we have New Media and Society which has published papers on hacking mainly form the perspective of activism and oppositional politics; and then there is the online journal First Monday, which has the broadest disciplinary spread, spanning information sciences and

social sciences, with somewhat more emphasis on social science. As examples of the third type of journal, we have Computer Law and Security Report , and Computer Fraud & Security, for both of which the titles are a good indicator of the content, which is written by and for persons working in the computer industry.

There is a tendency in the more professionally-oriented journals to divide hacking practice into a good/evil dichotomy, which certainly useful from the perspectives of the security industry and law-enforcement authorities for whom categorical distinctions are fundamental. Though a compelling narrative framework, 'Good vs Evil' is inadequate for a full sociological understanding of the actual practices of hackers, especially when we consider that an individual hacker may shift from one end to another of the open-clandestine continuum. Moreover, how particular hacking activities are read in moral or ethical terms is as much dependent on the perspective of the person doing the reading as it is on the actual content of the practices under scrutiny; added to this is the problem of accounting for the intentions of the hacker in question.

Clandestine hacking

The activities of clandestine hackers revolve around virtual breaking and entering, intelligence gathering, and technical attacks designed to make systems malfunction or fail altogether. For some clandestine hackers, circumventing the layers of security in corporate or government computer networks is an achievement in itself; for others it is the first step in getting information for subsequent trade or in order to gain direct access to electronically stored funds. These latter hackers may be individuals working on their own account, or as employees of criminal organisations (Chiesa 2009). For these hackers, the 'exploit' – a successful circumvention or penetration of a secure target – is the focus of their activity. Clandestine hacking ranges from the mildly anti-establishment to the criminal and even to the, rather more controversially, 'terrorist' (Conway 2003; Manion and Goodrum 2000).

Clandestine hacking activity is directed largely against the infrastructure of state and corporate computer systems (Chiesa 2009; P. Taylor 1999; Wall 2007). Given that clandestine hackers are just that – clandestine – it is not nearly as straightforward to locate individuals and groups for interview or observation as it is with open hackers. As such, there have not been the large scale surveys of clandestine hackers as we have seen for those who work in the world of Free and Open Source Software.[3]

Due to the methodological barriers that arise in trying to research any socially or legally marginal/'deviant' activity, what we know about clandestine hackers we know largely through work in which a researcher was able to cultivate a good relationship with one or a few hackers and then 'snowball' to others (Littman 1997; Jordan 2004), or through clandestine hackers' self-accounts (Mitnick & Simon 2005; Mitnick 2003, 2011), or through a wider journalistic literature that is frequently sensationalist.[4] From these sources we may build a picture of the person and practices of the clandestine hacker, but we must remain always mindful of the limited nature of the sample available to writers on this phenomenon.

The clandestine hacker sees information society with its laws, rules and regulations, all overseen by a computer security industry, as one vast challenge to his/her skills. What research there is on clandestine hacking leads to a further division of clandestine hackers into two camps (though individuals may shift from one camp to the other over the course of a career or even a specific project): first, those who claim to be motivated by a politics of libertarianism and for whom the computer security industry is the front line of repressive corporations and governments; second we have the clandestine hackers who are in the game for personal gain. Both types of clandestine hacker operate under the radar, in large measure because both tendencies are seen as criminal by the computer security industry. Insofar as we have sociologically coherent data on persons who fall under these categories, we are dealing with loners, known in their hacker identities only to a small circle of other hackers (and presumably sometimes, to the agencies that seek to police this kind of hacking).

Open Hacking

Open hackers, unlike those who aim to break into secure systems, articulate an interest in transparency and sharing, and while they may share with the clandestine hackers a distaste for the privatisation of information that underpins much of the computer security industry, their hacking work is built on sharing knowledge and resources; they practice their craft in the open. The open hacking tendency is best represented by those who work in Free and Open Source Software (Chopra and Dexter 2008; Moody 2001; Söderberg 2008; Torvalds, Himanen, and Castells 2001; Weber 2004).

One of the main spokespersons and advocates for open hacking is Eric Raymond (2003), for whom the pioneering hackers of late 1960s at the Massachusetts Institute of Technology computer labs were:

> … young, exceptionally bright, almost entirely male, dedicated to programming to the point of addiction, and tended to have streaks of stubborn nonconformism … [they] … tended to be shaggy hippies and hippie wannabes. (pp 44-45)

Raymond notes too that (crucially), these early hackers 'had a vision of computers as community-building devices' (p45).

For Raymond, the fundamental principle of the early hacker milieu, is that hackers, and users, are better off if information is freely shared. Hackers that fall under this rubric are committed to an open information space that ranges from the classically liberal through to the radical and even the anarchic. They are opposed in principle and in practice to exclusionary rights over information. For them, hacking is mainly about tackling difficult system design, engineering and programming problems, using a flexible mix of formal and informal

techniques of engagement (Hannemyr 1999).

Raymond has described himself, and has been described by some, as an ethnographer/anthropologist of free and open source software. He is certainly an insider and writes with critical insight and encyclopaedic knowledge, but if he is an ethnographer then it is an ethnographer-advocate, with the emphasis on the advocate: he discusses at length the technical merits of openness in software production and argues for the pragmatic business and economic value of his way of working, but he does not devote much space to presenting the viewpoints of those from whom he differs. Raymond's writing is not informed by the critical distance that is generally expected of the ethnographer in sociology or social/cultural anthropology, and his use of ideas of gift exchange are somewhat unconventional when viewed from the perspective of economic anthropology (e.g. Raymond & Steele 1996; Raymond 1999, 2003; Raymond is also a prolific speaker and online author) .

Another defining work in this area is Hackers: Heroes of the computer revolution, by Steven Levy (2010; first published in 1984), that has taken on canonical status in the field. Levy's work is based on interviews with many of the pioneering hackers, and he takes up the story from 1959. A s indicated by the title, Levy's book constructs the pioneering hackers as heroes, in a representational register that makes compelling reading as quality journalism, but sometimes reads as hagiography when viewed from a more sociological perspective.

Celebratory passages notwithstanding, it is in his discussion of the formative (for the field of hacking) years of the 1960s that Levy's work has most to offer to sociological reflection. He makes a number of intriguing references to interaction between the hackers and the wider political movements at the MIT campus and beyond, but these are not developed. Even though he wrote an updated preface to the 25th anniversary edition of 2010, which includes a discussion of recent developments in free software, the rise of Google and such, the account remains completely US-centric.[5]

In Kelty's Two Bits; The Cultural Significance of Free Software and the Internet, we have a work by a cultural anthropologist, based on extensive fieldwork supported by

documentary research. Kelty devotes considerable energy to the kinds of identities and practices that have arisen in free software projects. Hackers and hacking are central to his work. In discussing 'geeks' (the overlap between ‘geek’ and 'hacker’ is such that the terms may be used interchangeably, as both Kelty and Raymond do indeed suggest), Kelty (2008, pp.34-36) has rendered geek ideology (read hacker ideology) in terms of a Protestant Reformation against the centralised authority of the Catholic Church/State, figured as the capitalist software industry and its state supporters and guarantors. This is a compelling image and is well–supported in the thought of his, i.e. Kelty's, interlocutors, but is I suggest, an image that is most relevant to a North American and partly Western European constituency of hackers (and even within this grouping , there may well be dissenters: why should French, Spanish, or Italian hackers identify with this image?) and when we leave the confines of the North Atlantic, the Reformation metaphor seems of little use. Moreover, while a libertarian politics might well be apt for rendering North American open hackers, Italian hackers, for example, frequently articulate a collectivist radical left politics that they claim informs their hacking work.[6]

So, though all open hackers are concerned with extending the frontiers of democracy in their work, the politics of particular hackers and groupings is articulated in varied terms that may be seen to reflect the different outlines of political thought and practice on either side of the North Atlantic. But even this distinction, though useful for a first abstraction, is itself too crude: political cultures do not map neatly into national or regional boundaries. Insofar as the rest of the world is concerned, there is work still to be done in analysing the political imaginaries of open hackers in a globalised context: what definitely should not be assumed is that open hackers outside the world of the North Atlantic would account for the politics of their work in terms of discourses that are in wide circulation in that space. In the global of open hacking, we must seek out the local.

Hacktivism

Somewhere between the two extremes of open and clandestine, we have hacking as activism, where the hackers work in the open and/or in secret toward the ultimate aim of using hacking skill to achieve political activist aims (Dunbar-Hester 2009; Lindgren and Lundström 2011; Manion and Goodrum 2000; Jordan 2004; P. A. Taylor 2005). In this case the hacker is using his or her hacking skills towards clearly defined political ends that cannot always be reduced to the politics of either clandestine or open hacking. As the term implies, hacktivist combines 'hacker' with 'activist'. Given the varied political motivations of hackers as discussed earlier, we should not expect in all cases to make a tidy distinction between hackers and hacktivists; depending on the circumstances, perspective or project, the same person may shift between both types.

Hacktivism is closely related to cyberpolitics and cyberactivism, two terms that emerged in the 1990s to capture the new possibilities and constrains of political action in cyberspace (Donk et al. 2004; Landzelius 1999; Jordan 1999; McCaughey and Ayers 2003; Price 2000), but is distinguished from these by being strongly influenced by hacker practices and perspectives. Cyberactivsm can, does, but need not draw upon hacker cultures. Hacktivsm is manifested in various forms: attacks on websites in order to deny access through overloading – Denial of Service attacks; changing the content of websites to fit the aims of the hacktivst in question; using the Internet communication channels, and more recently web 2.0 social networking such as Facebook and Twitter to disseminate an alternative viewpoint and to organise protest and actions.[7] Much of the cyberactivist literature seems overly enthusiastic about the democratizing potential of Web technologies,

and is thereby vulnerable to the kind of critique raised by Morozov (2011), who reminds us that repressive states can and do make use of digital communication technology to further their own political ends. The enthusiasm for digital communication technology in the service of political activism may be partly explained by many of those who have researched this area being affiliated to to the movements they study, in the established modes of participatory action research.

In late 2010 hacktivism came to global media prominence with the leaking of classified US State Department documents by Wikileaks.[8] Apparently under pressure from the US government, VISA and Paypal blocked donations to Wikileaks, and Wikileaks' bank accounts were frozen. Hacktivists in support of Wikileaks founder Julian Assange soon responded by launching cyber-attacks against the online operations VISA and Paypal. A furious controversy ensued, with some on the conservative Right in the USA calling for the execution of Wikileaks founder Julian Assange, while on the other side, many took up Assange's cause (in the wake of his arrest and detention in the UK regarding accusation of sexual assault on two women in Sweden) as that of a persecuted freedom fighter. To many commentators it appeared that the world was witnessing a full-blown cyber-war.

The transnationally dispersed hackers who responded to what they saw as the persecution of Assange (and related on-going attempts to silence Wikileaks) employed well-established techniques, for example, flooding target websites with millions of requests in a short period of time in order to overload the servers, and altering or defacing 'enemy' websites (For a detailed study of activist discourse around the controversy, see: Lindgren and Lundström 2011). Hacktivism, as shown in the 'Wikileaks war', is enabled and constrained by the same technological, political, and sociocultural factors that set the field for hacking more generally: first, the infrastructure of the internet and web; the various structures of private capitalist and state control over these infrastructures; contestations of private and state control structures by hackers; and the accumulated skills and practices of hackers themselves. But who are the hacktivists who took up the keyboard in Assange's defence? What are their connections and

motivations? Their identities are cloaked by myriad anonymous points of entry and exist on the internet. So we are left to speculate: perhaps they are civil libertarians, passionate advocates of free speech, or anarchists? Their defence of Wikileaks was pursued in the clandestine register, but that cannot be taken to mean that they all usually operate in this manner.

Work on hacktivism suggests that multiple factors are significant for activism to take on the skillset and practices of open and/or clandestine hacking, and so morph into hactivism; a multidimensional analytical approach is advised by all those who have done research in this area. Unfortunately, sociological complexities have been overlooked in the media coverage of the 'Wikileaks War': the cult of personality that seemed to have grown up around Assange is precisely the kind of epistemological obstacle that must be overcome if we are to enhance the academic and public understanding of the place of hacking in the contemporary world. It is unlikely that the figure of Julian Assange is some kind of model for the hacktivist; those who seek to render the complex reality of hacktivism through focus on one high-profile figure such as Assange are substituting metonymy for epistemology.

We must guard against the attraction of the new in thinking about hacktivsm. Hactvism has lines of descent that reach back to the pirate radio of the 1970s, even earlier to samizdat and indeed the pamphleteering traditions that are as old as social movements themselves (d' Anjou 1996). The aims are similar, i.e. making an intervention into existing dominant systems of communication; what is perhaps new is the terrain that is contested and techniques employed in such contestation (Kahn and Kellner 2004). But even the new terrain and techniques of web hacktivism have lines of continuity that reach back to established forms of media activism: subverting the intended meaning/message of advertising is a form of media activism that has considerable overlap with the conception of hacktivism presented here (Downey and Fenton 2003; Downing 2001).

Material Improvisers: 'the invisible hackers'?

For as long as humans have made objects there have been tinkerers: persons who combine made objects in a way not intended nor envisaged by the original creators of these objects. If this assertion is believed then it opens up the possibility to think about 'hardware hacking'. Indeed, such a field does exist and has evolved numerous projects and practices, with a growing literature on how to design and execute various projects (Collins 2009; Capello and Phillips 2004; Fullam 2004). Hardware hacking can be seen to have a history that stretches from the early radio kits of the late 1960s and 1970s, to the DIY microcomputer scene that emerged in the late 1970s, and through to the programmable robot kits (most famously in the form of Lego Mindstorms, born out of the constructivist vision of Seymout Papert (1993; 1994). Hardware will not in the foreseeable future be as malleable as software is now, yet, there are several current hardware hacking projects which display many of the characteristics of hacking as discussed so far in this paper, and I will introduce two such here.

First, we have the Arduino project (Banzi 2009), which makes available a small affordable collection of microchips on a board that is programmable by open source software. The project describes itself as follows:

> Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. It's intended for artists, designers, hobbyists, and anyone interested in creating interactive objects or environments.
>
> http://www.arduino.cc/

The device can be programmed to control devices such as toys, appliances, and robots. It is aimed to bring the openness and accessibility of the Free and Open Source Software ecosystem into the realm of hardware, to provide 'open source hardware':

> Open-source hardware shares much of the principles and approach of free and open-source software. In particular, we believe that people should be able to study our hardware to understand how it works, make changes to it, and share those changes. To facilitate this, we release all of the original design files (Eagle CAD) for the Arduino hardware. These files are licensed under a Creative Commons Attribution Share-Alike license, which allows for both personal and commercial derivative works, as long as they credit Arduino and release their designs under the same license.
>
> The Arduino software is also open-source. The source code for the Java environment is released under the GPL and the C/C++ microcontroller libraries are under the LGPL.
>
> http://arduino.cc/en/Main/FAQ

There are obvious limitations to 'open source hardware': unlike with software, the costs of producing copies from a working piece of hardware are not virtually zero, nor are the costs of distributing copies of that hardware (machines that make other machines at virtually zero cost remain in the realm of science fiction, at least for the foreseeable future). 'Open source hardware', as conceived and deployed in this field of hardware hacking, does not have the free of cost character of free and open source software: the 'open source' in 'open source hardware' is more a marker of ideological affiliation with the broader free software movement than it as an actual description of a revolutionary new kind of hardware. Nonetheless, Arduino is made from cheap mass produced components; it is modular, flexible, and extensible, and provided that the hacker has the appropriate hardware and software skills, does in fact allow a very low cost entry into the world of computer controlled objects.

For the second example of hardware hacking we shift to Africa, where, as in the Global South more generally, there are many projects that fit the conception of hardware

hacking discussed here. The motivator for hardware hacking in poorer societies is acute need in the face of material deprivation, which drives invention and recombination of objects. Take the case of the dual-SIM card phone. Several initiatives have successfully addressed the widespread need in this part of the world for dual-SIM card mobile phones, in order for people to take advantage of different network's rates and services in the most economical way. In advanced capitalist societies, one would simply purchase a second phone/contract in order to access services on another mobile network, but this is a costly option in the poorer parts of the world. As discussed in on the Afrigadget website (http://www.afrigadget.com/2008/04/15/mobile-phone-ingenuity-in-africa/), the hardware hack that produced this product entails considerable practical engineering knowledge and skill. The dual-SIM mobile is part of a wider collection of projects in which African hardware hackers are adapting existing objects and developing new ones to fit specific local circumstances.

This last African example illustrates why I think of hardware hackers as relatively invisible, first because in the advanced capitalist societies out of which the hacker cultures emerged they are far less visible and numerous than software hackers; and secondly, as seen with the example of hardware hacking in Africa, many hardware hacks emerge from places characterised by levels of material deprivation and inventive necessity not typical of the very same advanced capitalist centres where established hacker cultures emerged and are still predominant (despite the pervasive impact of the World Wide Web).

Interpretations of Hacking: subculture, revolution, pragmatism

We may summarise the existing interpretations of hackers and hacking that have been offered in the literature in terms of three broad categories: hacking as a subculture; hacking as a revolutionary intervention; and hacking as a pragmatic way of operating in the existing

structures of software production and circulation. As with the earlier typology of 'open', 'clandestine', hacktivist', and 'hardware hacker', these are elements intended to form part of an interpretative framework. There is considerable overlap among them. The hacker ideal types of open, clandestine, and hacktivist map somewhat untidily unto the interpretative framework of subculture, radical politics and pragmatism.

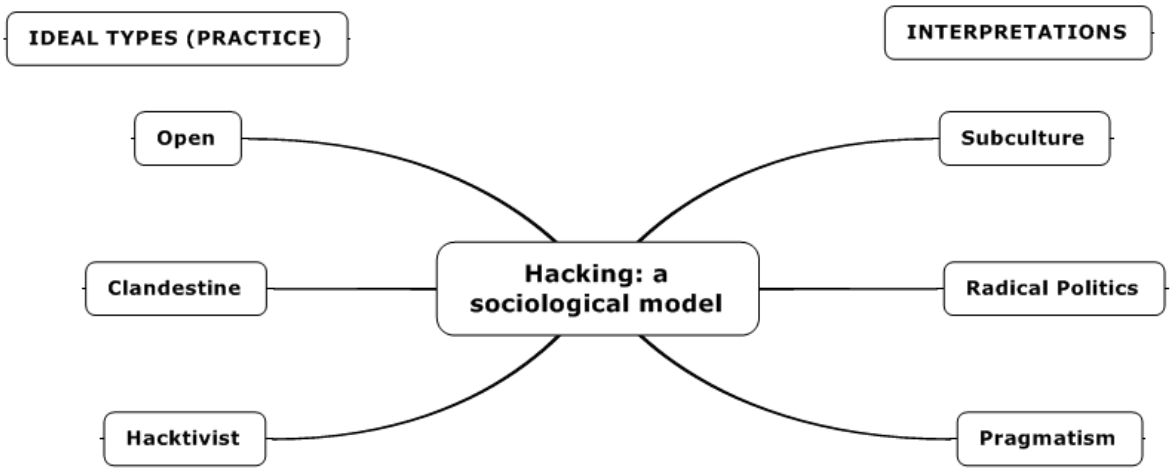

Figure 1.

The dominant representations of hacking in the existing literature is as a subculture. From this perspective hacking is seen as an activity either on the margins of mainstream network society, or as a minority counterculture within – hence subculture. The emphasis here falls under two broad heads: first, on the clandestine conflict between hackers and the computer security industry; secondly on the challenge to conventional intellectual property norms and capitalist working practices posed by Free and Open Source Software hackers. The

oppositional identities articulated by clandestine hackers are central to this body of work; this material has frequently been based on interviews with hackers whose identities are concealed, or with hackers' self-representations (e.g. Dr. 2004; Mitnick 2011; Verton 2002), which presents two methodological problems: the first is that we have no easy way to determine the population from which the clandestine hacker interviewees come; and second, we have to allow for a wide range of motives to have shaped the autobiographical accounts of individual hackers, and many of these motives are unlikely to support the classical sociological interest in establishing representativeness and estimating the extent and composition of a social milieu. With these caveats in mind we suggest that the key elements of the subculture representation are: self-identification as an outsider grouping, with a set of norms and an outlook at odds with that of a mainstream; and practices and modes of expression in support of the outsider status. From the perspective of the other side, i.e. the 'mainstream' from which hackers differentiate themselves, hacker subculture emerges from construal by a majority -- states, the computer security industry and the proprietary software industry, the media, -- of hackers as a deviant minority, who work against a set of established norms. It is obvious that subculture here cannot easily be distinguished from counterculture.

Related to subculture representations of hacking, though partly distinct, are representations of hacking as a radical political and cultural intervention, or hacking as a counterculture. Here we are on firmer ground for building a sociological synthesis, mainly because the hackers and hacktivists under this head generally work in the open and are often keen to have their projects known as widely as possible, not surprising since many hacktivists this case are connected to social movements. This perspective encompasses much of the hacking as subculture representation, but with two key differences. First, the radical hackers self-identity is framed in terms of an explicit political praxis, ranging from the liberal democratic, to the social democratic, to the autonomist and anarchist; in each instance the work of hacking is seen as itself, or fundamentally supportive of, a clearly stated political aim; this is seen, for example, in the emergence of radical hacker projects from the Italian

centri sociali (e.g. www.hackmeeting.org), which have themselves long been sites of invention of new modes of politics, as discussed by Ruggiero (2000). Secondly, when outsiders represent hackers in these radical terms, they too include the subcultural representation, but add to this a labelling of the hackers as political radicals, such that in many instances, hackers as radicals are construed in criminal terms, as a danger to society. Hackers who self-identify as political radicals draw on ideas of autonomy and self-valorisation in representing their praxis. They stress self-development through learning and sharing, while rejecting the neoliberal agenda of skilling oneself for the world of work in information society. This is seen in the case of people working in the video games industry, which is one of the largest employers of programmers across the globe. Developing techniques to resist the harsh working conditions of the videogame industry, finding ways to circumvent the industry's systems for intellectual property protection, and building alternative gaming experiences, are all at the core of contemporary hacker cultures (Dyer-Witheford 1999; Kline, Dyer-Witheford, and De Peuter 2003; Dyer-Witheford and Peuter 2009).

There exists a wide body of work that takes the view that open models of software development constitute a pragmatic and viable approach to doing business (Benkler 2005; Garcia and Steinmueller 2003; Ghosh 2005; Lerner and Tirole 2002; McKelvey 2001). Much of this work has been done form a social science perspective, so it is the area where our knowledge is greatest. This work revolves around Free and Open Source Software, which is software which people may use, distribute and modify without restriction, save and except that users pass on the same freedoms to others.

Perhaps counter-intuitively to capitalist market logic, Free software is not a suicidal (how can you make a living by giving away your work?) nor even an ill-judged model of production and distribution; it is in fact proving in some cases to be both commercially viable and radically democratic (Berry 2008; Weber 2000). Open Source software is Free Software in the sense of freedom to examine and change the source code, and is analogous to Free

Software in the sense of freedom to examine and change the source code, but it can also be a conventional commodity. While Free and Open Source Software (FOSS) covers both variations, must not overlook a tension within the FOSS field (Berry 2004): for followers of Richard Stallman the legendary US hacker who is the charismatic leader of the Free Software movement and head of the Free Software Foundation (www.fsf.org), software should be free in all senses, and therefore largely outside of restrictive licensing market relations. For Stallman (Williams 2002; Stallman and Gay 2002), it is only ethically defensible to charge for the cost of distribution media (less important in the age of expanding broadband Internet access). In contrast, some in the FOSS world see open source as a pragmatic approach to building software. From a pragmatic perspective open hacker techniques are of value mainly due to whatever technical merits they possess when compared to other ways of working with computer systems. The Open Source Initiative (http://www.opensource.org/) is the best-known institutional representative of this perspective. It began in part as a reaction to what its founders saw as the over-politicisation of Stallman's Free Software Foundation, which itself represents a radical libertarian praxis.[9] For Eric Raymond and others involved with the OSI, the open way of working, which includes the open tendency of hacking, is primarily about a new and effective way to produce software, and to run a software-based enterprise. This approach is pragmatic and entirely at ease with finding its own niche in a capitalist information technology industry; many of the 'thought leaders' here see no problem with mixing free and proprietary code in building an overall system.

Free software may be viewed as primarily ideological, while open source may be seen as a technical approach, but as Kelty (2008) has reminded us, they are two ways of thinking about what is essentially the same object - source code, and practice - code-sharing. Hackers of all types are evenly distributed on both sides of this divide, and while some dismiss it as irrelevant, most are committed to FLOSS in some form or other.

Conclusion: critical questions for the sociology of hackers and hacking, or, are we all hackers now?

The programme of work I envisage here is predicated upon a structural context in interaction with which individual hackers, who are differentially empowered, seek to realise their projects. What are some of the questions that would emerge from this initial conception? I suggest that they are: what are the political, economic, social and cultural structures that enable and constrain contemporary hacking? What are the components out of which hacker identities are constructed in today's world? What are the kinds of capital characteristic of hacking? I will do no more that suggest outlines in answer to these questions: part of my aim in this paper was to acknowledge the rich body of work that exists on hacking and to suggest lines for future sociological enquiry that builds on that work.

Steven Levy (2010) writes of a 'hacker ethic' as the gift of hackers to the rest of us. There is clearly a political vision articulated here, but what kind of politics? To make a politics out of the chosen activity, or rather to frame the chosen technical activity in terms of a politics, the stated political principles must be accompanied by strategies to translate these into action. To claim that sharing code among a group of hackers is a political act is one thing, to translate that sharing ethic into a politics that can engage the world outside the hacker lab is quite another. There are a few intriguing references to contact between these pioneering hackers and other political actors: Levy notes that the MIT hackers came into conflict with anti-war protesters, while Raymond (2003), writing on the same milieu, asserts that many of the pioneering hackers were 'hippies' or 'wannabe hippies'. What seems a most

promising line of investigation is pursued by neither of these authors. We are left wanting to know more about how the hackers' political ideas fared in the wider world. What is missing here is a full exploration of the politics of the early US hackers against the backdrop of the US counter-culture of the 1960s. On Levy's account I can see no reason not to read his MIT hackers as people who sought to justify their chosen technical activities in terms of a political imaginary that struck an uneasy balance between individualistic libertarianism and a somewhat vague centrist communitarianism. If as is suggested, the pioneering hackers had a clear politics, then it is reasonable to want to find out what happened when these political ideas were translated into action. The hacker ethic as set out by Levy and Raymond is undoubtedly political, but does not stand up well to a searching radical political critique as this would be articulated in terms of the New Left as it emerged in the US and Western Europe in the same period as the appearance of the early hackers.

When we turn to consider the structural transformations in economy and society out of which hacking emerged, we again see a need to move beyond canonical insider accounts. When computers became personal as they did in the late 1970s, it was as part of a capitalist consumer electronics industry. It is a commonplace for veteran US hackers to attribute credit to themselves for the expansion of the Internet and of personal computing, and they are justified in so doing. If, however, we follow Edwards's (1996) sombre account of the emergence of the computing industry from the Cold War concerns of US governments and how that industry and those concerns were shaped and responded to by a fast growing military-industrial complex, then the key dynamic underlying the expansion of the computer industry, seen here as a necessary but not sufficient condition for the emergence of a hacker culture, appears driven as much by top-down as by the bottom-up populist forces implied in accounts by leading figures in hacker culture. However located on the top-down versus bottom up continuum, any sociocultural-historical account of the emergence of hacking would have to render a history of computing as the structural context that enabled and constrained both open and clandestine versions of hacking; it should be clear that such an

account would have to reach beyond the internal conversations of hackers of all types as well as those of their sometime opponents in the computer security industry. We need to understand better how the growth of information society both enabled and constrained different types of hacking activity. Doing so requires us to engage with globalisation, and therefore to move beyond the rich yet somewhat parochial US-centered work that has formed most of what we read on hacking. How do hacker cultures interact with the political cultures and social structures in different parts of the Global South? This is an urgent question.

All hacking involves complex forms of capital. As Bourdieu (1986) has shown, forms of capital can be exchanged and transformed. More work needs to be done on how hackers accumulate and deploy cultural capital in the form of technical skills and knowledge that they have acquired through informal as well as formal training and education. This cultural capital is both knowledge as specific technical know-how and broader knowledge of fields of software production and circulation. Such knowledge is also political knowledge, as is most obvious in the case of hacktivists, but all hackers are political actors. This last is an assertion that itself calls for further research. The Internet is a key enabling technology for collaborative work among software developers and thus a key sphere of innovation in working methods for hackers of all types. Hacking is enabled by the internetworked structure of the web, which is materialised and instantiated in real human relations among hackers and their opponents. These relations constitute social networks and can be read as a form of social capital. The social capital of hackers thus consists in the main of a network of relationships sustained largely through the Internet but also through face-to-face meetings. Among hackers, forms of social and cultural capital interact through widespread practices of code-sharing and informal skills exchange and learning, which is characteristic of the field of free and open source software development, with which hackers of all kinds are intimately involved. To understand better the accumulation and transformations of hacker capital(s), we need more in-depth ethnographic study of the kind done by Kelty (2008), but with greater emphasis on understanding the local outside of the US, and even outside the advanced

capitalist nations, more broadly. Hackers are human and humans exist locally; the local thus remains important for sociological understanding of hacking, not in spite of but because the work of the hacker is projected into the virtual, the realm created by software.

The value in many consumer and producer goods today is represented by intellectual property/capital, most often in the form of software. Software is pervasive. The software stack is key to the working of the Web and of mobile telephony, as well as new media. We all use software, and while most of us do not build it, the lines between software and content are becoming more blurred. We are increasingly involved in creating content, so we are therefore increasingly implicated in the blurring of the lines between software and content. The hacker is a particular kind of person who works with software, but the 'hack' is no longer the exclusive act of the hacker. When we make a web mash-up, a music or video remix, we are involved in this blurring of the line between software and content , and we are also part of a blurring of the lines between hackers and everyone else. These ideas are the starting point for a programme of sociological work on the phenomenon of hacking as a metaphor for how we engage with ubiquitous digital technologies. We are all hackers now..

REFERENCES

d' Anjou, Leo. 1996. *Social Movements and Cultural Change: The First Abolition Campaign Revisted*. New York: Aldine De Gruyter.

Banzi, Massimo. 2009. *Getting Started with Arduino*. 1st ed. Make, March 24.

Benkler, Yochai. 2005. Coase's Penguin, or, Linux and the Nature of the Firm. In *CODE: collaborative ownership and the digital economy*, ed. Rishab Aiyer Ghosh, 169-208. Cambridge, Mass. ; London: MIT.

Berry, David M. 2004. "The Contestation of Code: a preliminary investigation into the discourse of the free/libre and open source movements." *Critical Discourse Studies* 1 (1) (April): 65-89.

Berry, David M. 2008. *Copy, Rip, Burn: The Politics of Open Source*. Pluto Press, September 20.

Bourdieu, Pierre. 1986. The Forms of Capital. In *Handbook of Theory and Research for the Sociology of Education*, ed. John G Richardson, 241-258. New York: Greenwood.

Bourdieu, Pierre, Jean-Claude Chamboredon, and Jean-Claude Passeron. 1991. *The Craft of Sociology: Epistemological Preliminaries*. Berlin & New York: Walter de Gruyter.

Capello, Paul, and Jon Phillips. 2004. *Maximum PC Guide to Hardware Hacking*. 1st ed. QUE, December 21.

Chiesa, Raoul. 2009. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton, Fla: Auerbach.

Chopra, Samir, and Scott Dexter. 2008. *Decoding Liberation: The Promise of Free and Open Source Software*. Routledge studies in new media and cyberculture. London: Routledge.

Collins, Nicolas. 2009. *Handmade Electronic Music: The Art of Hardware Hacking*. 2nd ed. Routledge, July 9.

Conway, Maura. 2003. "Hackers as terrorists? why it doesn't compute." *Computer Fraud & Security* 2003 (12) (December): 10-13. doi:10.1016/S1361-3723(03)00007-1.

Donk, Wim van de, Brian D. Loader, Paul G. Nixon, and Dieter Rucht. 2004. *Cyberprotest: New Media, Citizens and Social Movements*. 1st ed. Routledge, May 27.

Downey, J., and N. Fenton. 2003. "New media, counter publicity and the public sphere." *New Media & Society* 5 (2): 185.

Downing, John. 2001. *Radical media : rebellious communication and social movements*. Thousand Oaks, Calif.; London: Sage Publications.

Dr., K. 2004. *Hackers' Tales: Stories from the Electronic Front Line*. London: Carlton.

Dunbar-Hester, C. 2009. "'Free the spectrum!' Activist encounters with old and new media technology." *New Media & Society* 11 (1-2) (February): 221-240. doi:10.1177/1461444808100160.

Dyer-Witheford, Nick. 1999. *Cyber-Marx : cycles and circuits of struggle in high-technology capitalism*. Urbana: University of Illinois Press.

Dyer-Witheford, Nick, and Greig de Peuter. 2009. *Games of Empire: Global Capitalism and Video Games*. University of Minnesota Press, February 16.

Edwards, Paul N. 1996. *The closed world: computers and the politics of discourse in Cold War America*. Cambridge, Mass ; London: MIT Press.

Erskine, Ralph, and Michael Smith. 2011. *The Bletchley Park Codebreakers*. Biteback, January 20.

Fullam, Scott. 2004. *Hardware Hacking Projects for Geeks*. 1st ed. Pragma, February 10.

Garcia, Juan Mateos, and W. Edward Steinmueller. 2003. *The open source way of working : a new paradigm for the division of labour in software development*. Brighton: SPRU.

Ghosh, Rishab Aiyer. 2005. Cooking-Pot Markets and Balanced Value Flows. In *CODE: collaborative ownership and the digital economy*, ed. Rishab Aiyer Ghosh, 153-168. Cambridge, Mass. ; London: MIT.

Hannemyr, Gisele. 1999. "Technology and pleasure: Considering hacking constructive." *First Monday [Online]* 4 (2) (February 1). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/647/562.

Harris, Shon, Allen Harper, Chris Eagle, and Jonathan Ness. 2008. *Gray Hat Hacking, Second Edition: The Ethical Hacker's Handbook*. 2nd ed. McGraw-Hill Osborne, February 1.

Jordan, Tim. 1999. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge.

———. 2004. *Hacktivism and Cyberwars: Rebels with a Cause?* London: Routledge.

Jordan, Tim, and Paul Taylor. 1998. "A sociology of hackers." *Sociological Review* 46 (4): 757-780. doi:10.1111/1467-954X.00139.

Kahn, Richard, and Douglas Kellner. 2004. "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging." *New Media & Society* 6 (1) (February): 87-95. doi:10.1177/1461444804039908.

Kline, Stephen, Nick Dyer-Witheford, and Greig De Peuter. 2003. *Digital play : the interaction of technology, culture, and marketing*. Montréal: McGill-Queen's University Press.

Landzelius, Kyra. 1999. *Native on the Net: Indigenous Cyber-activism and Virtual Diasporas Over the World Wide Web*. 1st ed. Routledge, October 15.

Lerner, J., and J. Tirole. 2002. *Some Simple Economics of Open Source*. Vol. 50. http://www.ingentaconnect.com/content/bpl/joie/2002/00000050/00000002/art00174.

Levy, Steven. 2010. *Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition*. 1st ed. O'Reilly Media, May 20.

Lindgren, Simon, and Ragnar Lundström. 2011. "Pirate culture and hacktivist mobilization: The cultural and social protocols of #WikiLeaks on Twitter." *New Media & Society* 13 (6): 999 -1018. doi:10.1177/1461444811414833.

Littman, Jonathan. 1997. *Fugitive Game Online with Kevin Mitnick*. 1st ed. Little, Brown & Company, September 1.

Manion, M., and A. Goodrum. 2000. "Terrorism or civil disobedience: Toward a hacktivist ethic." *ACM SIGCAS Computers and Society* 30 (2): 19.

McCaughey, Martha, and Michael D. Ayers, eds. 2003. *Cyberactivism: Online Activism in Theory and Practice*. 1st ed. Routledge, March 20.

McKay, Sinclair. 2011. *The Secret Life of Bletchley Park: The History of the Wartime Codebreaking Centre by the Men and Women Who Were There*. Reprint. Aurum Press Ltd, August 1.

McKelvey, Maureen. 2001. *Internet entrepreneurship : Linux and the dynamics of open source software*. University of Manchester, Centre for Research on Innovation and Competition.

Mitnick, Kevin. 2011. *Ghost in the Wires: My Adventures As the World's Most Wanted Hacker*. Little Brown & Co (T), August 15.

Mitnick, Kevin D. 2003. *The Art of Deception: Controlling the Human Element of Security*. Wiley, October 17.

Mitnick, Kevin D., and William L. Simon. 2005. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons, March 4.

Moody, Glyn. 2001. *Rebel code : Linux and the open source revolution*. London: Allen Lane.

Morozov, Evgeny. 2011. *The Net Delusion: How Not to Liberate The World*. Allen Lane, January 6.

Papert, Seymour A. 1993. *Mindstorms: Children, Computers, and Powerful Ideas*. New edition. Perseus Books,U.S., July 14.

———. 1994. *The Children's Machine: Rethinking School in the Age of the Computer*. New edition. Basic Books, April 8.

Price, Tom. 2000. *Cyber activism: Advocacy groups and the internet*. Foundation for Public Affairs.

Raymond, Eric S. 1999. *The cathedral and the bazaar : musings on Linux and open source by an accidental revolutionary*. Beijing ; Cambridge: O'Reilly.

———. 2003. *The art of Unix programming*. Harlow: Addison-Wesley.

Raymond, Eric S, and Guy L Steele. 1996. *The New hacker's dictionary*. 3rd ed. Cambridge, Mass ; London: MIT Press.

Ruggiero, Vincenzo. 2000. "New social movements and the 'centri sociali' in Milan." *The Sociological Review* 48 (2) (May): 167-185. doi:10.1111/1467-954X.00210.

Shimizu, Hiroyuki, Jun Iio, and Kazao Hiyane. 2004. "The realities of Free/Libre/Open Source Software developers in Japan and Asia." *First Monday [Online]* 9 (11) (November 1). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1190/1110http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1190/1110.

Söderberg, Johan. 2008. *Hacking Capitalism: The Free and Open Source Software Movement*. Routledge research in information technology and society. London: Routledge.

Stallman, Richard, and Joshua Gay. 2002. *Free software, free society : selected essays of Richard M. Stallman*. Boston, Mass: GNU Press.

Taylor, P. A. 2005. “From hackers to hacktivists: speed bumps on the global superhighway?” *New Media & Society* 7 (5) (October): 625-646. doi:10.1177/1461444805056009.

Taylor, Paul. 1999. *Hackers: Crime and the Digital Sublime*. 1st ed. Routledge, September 9.

Torvalds, Linus, Pekka Himanen, and Manuel Castells. 2001. *The Hacker Ethic*. Martin Secker & Warburg Ltd, February 1.

Turkle, Sherry. 1985. *Second Self: Computers and the Human Spirit*. Reprint. Pocket Books, January 1.

Turkle, Sherry, and Seymour Papert. 1990. “Epistemological Pluralism: Styles and Voices within the Computer Culture.” *Signs: Journal of Women in Culture and Society* 16 (1) (January 1): 128. doi:10.1086/494648.

Verton, Dan. 2002. *The hacker diaries: confessions of teenage hackers*. McGraw-Hill Professional, March 26.

Wall, David. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Crime and society series. Cambridge, UK: Polity.

Weber, Steve. 2000. *The political economy of open source software*. Berkeley: Berkeley Roundtable on the International Economy.

———. 2004. *The success of open source*. Cambridge, Mass. ; London: Harvard University Press.

Williams, Sam. 2002. *Free as in freedom : Richard Stallman & the Free Software Foundation*. Sebastopol, Calif. ; Farnham: O’Reilly.

NOTES

1 Large scale surveys of free and open source programmers were carried out in the EU in 2001 http://www.ist-world.org/ProjectDetails.aspx?ProjectId=1e3859fb33f7435ea223f60575302397 , USA in 2003 www.stanford.edu/group/floss-us/report/FLOSS-US-Report.pdf, and parts of East Asia in 2004 (Shimizu, Iio, and Hiyane 2004). While not all hackers are free software produces, most free software producers are happy with the term 'hacker', subject to some qualification. These data and issues of definition regarding free software will be discussed as the paper develops.

2 There is a vast body of writing on hackers in the news media as well as representations in print fiction, non-fiction. In addition we have a considerable body of film and television programming in which hacking is central. A discussion of these is beyond the scope of the present paper.

3 Free and Open Source Software is 'free' in two senses: the first sense of which concerns free as in having no price; the second sense concerns free as in free access to the source code describing how the software works; Open Source software is 'free' in the sense of freedom to examine and change the source code. Over the last decade there has been an exponential growth in the spread of Free and Open Source software and a hacking culture associated with it. Most social science writing on hacking from the 1990s and early 2000's, while aware of this phenomenon, did not accord it a central place.

4 Searches for articles on hackers in the archives of The BBC, The Guardian, and the New York Times, return hundreds of articles referring to hackers, of which the majority address the issue in terms of threats to security.

5 The veil of secrecy that has until recently surrounded the activities at Bletchley Park has meant that pioneering work carried out there has not found its way into canonical histories of computing, on which the sociology of hacking depends. Recently, a substantial amount has been published on the pioneering work in computing carried out at Bletchley Park in in England (Erskine and Smith 2011; McKay 2011). A contemporary sociology of hackers would have to be based on an historical account that engages with the British pioneers in computing; work remains to be done in this area.

6 See for example: http://it.hackmeeting.org/; Personal communication, Glasgow KDE conference, 2007; London, various, 2010.

7 In the wave of student protest in the UK in November and December 2010, the London Metropolitan Police indicated that they intended to make greater use of social networking for intelligence gathering. See: 2010. Police chief predicts 'disorder'. *BBC*. Available at: http://www.bbc.co.uk/news/uk-11839386 [Accessed December 23, 2010].

8 The issue was extensively covered in the UK and international news media. As examples, see:
BBC News - At a glance: Wikileaks cables. Available at: http://www.bbc.co.uk/news/world-us-canada-11914040 [Accessed December 12, 2010].
BBC News - Profile: Wikileaks founder Julian Assange. Available at: http://www.bbc.co.uk/news/world-11047811 [Accessed December 12, 2010].

9. A leading figure in the Open Source Initiative is Eric Raymond, who, though vociferous in arguing for an understanding of hackers in terms of the open end of the continuum and for a radical libertarian and individualistic approach to software enterprise in which anything goes so long as the code is open and free to modify, has taken issue with what many see as the hard-line approach of Stallman and the Free Software Foundation.