INTER-ASIA ROUNDTABLE 2012

METHODOLOGICAL AND CONCEPTUAL ISSUES IN CYBER ACTIVISM RESEARCH

30-31 AUGUST 2012

ORGANISED BY

ASIA RESEARCH INSTITUTE, NATIONAL UNIVERSITY OF SINGAPORE

The Guardians of the Internet? Politics and Ethics of Cyberactivists (and of their Observers)

Stefania Milan

The Citizen Lab, University of Tornoto, Canada

stefania.milan@eui.eu

"Expect us": An introduction to cyberactivism

When in September 1995 President Jacques Chirac announced that France would run a series of nuclear tests in the Polynesian atoll of Mururoa, a group of Italian activists protested organizing an attack against the websites of the French government. The Muroroa netstrike, "a networked version of a peaceful sit-in" according to its promoters, showed how activists could exploit the technical properties of digital technology to make a political statement. Some fifteen years later, a decentralized network going under the mass noun of Anonymous creatively repurposed the peaceful sit-in of its precursors to launch a web disruption campaign in defense of online free expression. These "digital Robin Hoods" (Carter, 2012) used different variations of a technique known as distributed denial of service (DDoS) to make temporarily unavailable a wide array of business and institutional websites, in a sort of digital age equivalent to blocking the gates of a company headquarters in sign of protest. Anonymous mobilized also in support of WikiLeaks, an organization devoted to the online publication of classified documents leaked by unidentified sources. The Mururoa netstrike, Anonymous' online actions, and WikiLeaks are manifestations of cyberactivism.

By cyberactivism I mean collective action in cyberspace that addresses network infrastructure or exploits the infrastructure's technical and ontological features for political or social change.[1] Examples of cyberactivism include electronic disturbance tactics and online civil disobedience, self-organization and autonomous creation of infrastructure, software and hardware hacking, and hacktivism. Leaking is another example as it takes advantage of the distribution capacity of the internet.[2] Generally speaking, we can boil down these practices to two categories: subversion and disruption of the existing order in cyberspace, and self-organization for the creation of autonomous spaces or alternative tools. These two approaches have in common an emphasis on direct action, decentralization, and the rule of users and technical experts. At their core there is a widely shared perception of cyberspace as a digital commons that should be freely and equally enjoyed by all netizens. Currently, the most popular form of cyberactivism is hacktivism, exemplified by amorphous groups like Anonymous and LulzSec. Hacktivists seek to fix the world through software and online action: in other words, it is (disruptive) "activism gone electronic" (Jordan and Taylor, 2004, p. 1; Meikle, 2002). Cyberactivists are part of the organized civil society.[3] However, they dispute some of our fundamental interpretations of said civil society, and confront our conception of collective action. For example, they challenge the increasing professionalization of transnational activist networks by involving non-professional activists, and point to the disembodiment of activism by decoupling resistance and physical presence (Wong and Brown, 2012).

Cyberspace is both as an arena for civic engagement and an object of contention in its own right. As an arena for civic engagement, cyberspace is two things: firstly, it is a "gym" to practice political participation and digital citizenry, where alternative and often contradictory views about society are articulated and shared; secondly, it is a platform for collective action, like a city square would be for example, where to articulate, organize, and bring forward social struggles, and where cyber-specific forms of collective action can take place. But, far from being considered only a set of tools or a space to practice dissent, cyberspace has become a site of struggle in its own right, as it becomes increasingly threatened by commercialization, tightening state control, and restrictive legislation.

[1] Cyberspace encompasses the realm of digital electronic communication, including (but not limiting to) the internet.

[2] Vegh (2003) arranges cyberactivism tactics into three categories: awareness/ advocacy (e.g., carrying out action), organization/mobilization (e.g., calling for action), and action/reaction (e.g., hacktivism). In this paper, the focus is on *collective* actors such as networks and activist groups acting in a collective capacity—individuals, such as bloggers writing solely in their own capacity, will not be considered. Furthermore, criminal or 'black hat' hackers are excluded from the analysis.

[3] By organized civil society I mean the realm of nonstate and nonbusiness actors, organized in formal (nongovernmental organizations) or informal (social movements, loose networks) groupings.

"Expect us", reads the motto of Anonymous. In fact, over the last few years, hackers, radical techies, and hacktivists have become a disruptive social force that can no longer be ignored. What were, back in the 1990s, sporadic cell-based cyber performances like the Mururoa netstrike are now tactics practiced on a regular basis by decentralized networks of individuals seeking to intervene in real-world struggles. The extraordinary visibility cyberactivism, and hacktivism in particular, have acquired with the WikiLeaks case encouraged more young people who do not care about the consequences to join the struggle. The popularity of cyberactivism is also linked to the dramatic increase in the number of people with access to technology and technical expertise. But it is also due to the impact of cyberactivism: compared to other tactics such as campaigning or street demonstrations, cyber disruption and electronic disturbance can have an intense and real-time impact with only a limited deployment of resources.

Although some of their critics consider these activists to be some sort of "anarchic cyber-guerillas" (Stone and Riley, 2011), cyberactivists reclaim for themselves a role of "guardians" of the internet. They embody a set of moral norms and develop a discourse on the ethics of technology and cyberspace that are grounded on values such as openness, transparency and self-expression, and react when these norms are threatened. In this paper, I explore these norms and ethical discourses. I also reflect on the politics and ethics of approaching cyberactivism as an object of study, taking into account epistemological considerations and methodological challenges.

In the next section, I offer an historical overview of cyberactivism, in order to help situating different forms of contemporary activism in relation to other progressive communities and subcultures. I then turn my attention to one of the forms of contemporary cyberactivism, namely 'radical tech activism', as a case study for looking more closely at the ethics of activists. Further, I discuss the methodological and epistemological challenges of approaching cyberactivism as a researcher, drawing on my own experience with investigating radical tech activism.

The rise of cyberactivism as a political subject

Contemporary activism targeting or exploiting internet infrastructure has roots in many realms of human activity, from computing to environmental and indigenous activism. Most of these sources of inspiration are visible in the cultural and ideological references of present-day groups. This section traces the relatively recent history of cyberactivism, focusing on the forerunner groups and subcultures that have most inspired contemporary activists. However, the category of cyberactivism is very diverse, and different groups associate different objectives and tactics under its umbrella, not all of which are compatible. For example, hacktivists' sabotage tactics crash with the freedom of information and no damage philosophy of earlier generations of hackers, for whom closing down a website is equivalent to censorship regardless of the content or owner of that website. What follows should be interpreted with this contention in mind, remembering that the different souls of cyberactivism embody slightly different ethical codes, which, nonetheless, share a set of core values and a similar history.

The hacker and open source culture that emerged in the 1970s around the Massachusetts Institute of Technology is one of the fundamental sources of inspiration of contemporary cyberactivists. Most notably, the idea of an e-commons developed in the realm of computer science. The first "computer hackers," highly skilled software writers who enjoyed experimenting with the components of a system with the aim of modifying and ameliorating it, operated under a set of tacit values that later became known as "hacker ethics." These principles include freedom of speech, access to information, world improvement, and non-interference with the system's functionality, and are encapsulated in the injunctions to "leave no damage"

and "leave things as you found them (or better)" (Levy, 1984). However, hackers were intrinsically apolitical.[4]

Around the same time, software developers and user communities started advocating and practicing freedom in managing and using technologies, for example redistributing and modifying software according to individual needs. They were the seeds of the emerging open-source software movement. Hackers and open-source advocates shared a hands-on attitude to computing; however, while hackers emphasized a "do not harm" approach, open-source advocates championed collective improvement and selfless collaboration.

The first social experiments using digital communication technologies for civic engagement emerged in the 1980s, long before the World Wide Web as we know it even existed. The Bulletin Board System (BBS), a precursor of the modern internet that allowed users to exchange messages and files by means of a common landline, was one of the first widely used applications. North American and European nongovernmental organizations (NGOs) started providing civil society groups with cheap access and connections. In 1984 a group of NGOs from four continents signed the Velletri Agreement committing to use telephone lines to network their computers, thereby recognizing the potential of cyberspace as an arena for collective action. As a result, the Canadian International Development Research Centre funded Interdoc, a series of connection experiments geared toward civil society organizations. Between 1985 and 1990 several networks were created to provide progressive activists with cheap systems for sharing text-based information: Fidonet, which relied on the BBS system; the London-based GreenNet oriented towards the "progressive community working for peace, the environment, gender equality and social justice"; PeaceNet and EcoNet in the US, which later merged into the Institute for Global Communications; and the European Counter Network, based in Italy and connected to the most radical fringes of European social movements. Some still operate today. In 1988 PeaceNet and GreenNet teamed up to create the first NGO-owned transatlantic digital communications network. They shared "the Internet vision of global communications unfettered by commercial barriers" (Murphy, 2000). In 1990 a number of nonprofit Internet providers joined forces in the Association for Progressive Communications (APC) to ensure that "all people have easy and affordable access to a free and open internet to improve their lives and create a more just world."[5]

Following the diffusion of the internet in the 1990s, a new type of grassroots activism emerged which had direct action in cyberspace at its core. As one activist put it, "finally technology and politics were talking the same language, and the links between the physical and electronic spaces were becoming real" (Milan, 2010a, p. 89). The 1994 Zapatista uprising inspired Western activists: exploiting the ontological qualities of the internet, such as its ability to reach out to remote nodes, insurgents managed to transform a local indigenous struggle in the remote Mexican state of Chiapas into the first "information guerrilla movement" (Martinez-Torres, 2001). The internet allowed the nascent indigenous rights movement to speak for itself and control information vital to its survival. It also served as the backbone for the creation of supportive transnational networks able to amplify its message. In 1996 the Zapatistas called for "mak[ing] a network of communication among all our struggles and resistances" (Hamm, 2005). Partially inspired by the Zapatista cyber-struggle, activists protesting against the World Trade Organization summit in Seattle in 1999 created the first Independent Media Centre (IMC) or Indymedia. For the first time in the brief history of the internet, thanks to a open source software called "Active" developed by activists in Sydney,

[4] With some exceptions: in 1985, for example, the Berlin-based hacker organization Chaos Computing Club (CCC) exploited a flaw in the German Bildschirmtext home terminal system to raise awareness of its security risks. CCC activists hacked the Bildschirmtext, operated by the telecommunications agency Deutsche Bundespost and used by the general public for daily payments, to organize a massive transfer of money in their favor. However, they called a press conference the next day to return the cash. The CCC is still active today, and regularly engages in similar operations.

[5] "The APC Vision," APC website.

Australia, users could publish texts and pictures online without editorial filter or registration. In this respect, activists rightly consider Indymedia "the mother of all blogs" (Milan, 2010a, p. 89). In 2002, three years after its foundation, there were already eighty-nine IMCs across six continents. For over a decade Indymedia served the communication needs of social movements across the world. Similar do-it- yourself projects appeared that put self-organization, free speech, and the cooperation of countless individuals at the center of social change.

In 1996 US cyber-libertarian activist John Perry Barlow had launched the "declaration of independence of cyberspace." The declaration read:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather ... I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us" (Barlow, 1996).

Based on Dave Clark's famous creed from 1992—"We reject kings, presidents and voting. We believe in rough consensus and running code"—cyber-libertarians oppose state interventions into the innovations and the creativity of developers. They preserve freedoms in online interaction, and reject state interference in cyberspace, including surveillance. In their view, cyberspace has to remain free of proprietary layers because it belongs primarily to those who create and use it. Cyber-libertarians believe in openness, transparency, and the power of users and technical experts, in other words, the self-regulation of those who create and use the infrastructure is the only legitimate form of governance of cyberspace, and should be based on the prerogative "First, do no harm" (Cerf, 2004, p. 13).

As protest extended to cyberspace, the 1990s saw also the emergence of hacktivism, which took advantage of the low cost, speed, and flexibility of network-mediated communication for protest purposes. In mid-1990s, the US tactical media collective Critical Art Ensemble (CAE) theorized electronic disturbance and electronic civil disobedience as the most meaningful forms of political resistance in times of nomadic and decentralized power (Critical Art Ensemble, 1993 and 1996). According to CAE, electronic disturbance was not a mass movement, but a cell-based hit-and-run media intervention taking advantage of the decentralization typical of the information society. In 1996, the Texas-based computer underground group known as Cult of the Dead Cow coined the term hacktivism, a portmanteau of 'hacking' and 'activism', to indicate the politically motivated use of technical expertise like coding (Delio, 2004).

Around the same time it became clear to activists that "grass-roots 'social movements' needed new networks of communication (…) but also that the way these networks were created, run and developed, mirrored, as much as possible, the direct, participatory, collective and autonomous nature of the emerging social movement(s) themselves" (Milan 2010, pp. 88-89). Networking infrastructure became an object of contention in its own right. "Radical tech" activists aimed at creating autonomous cyber-infrastructure independent from the state and the market, in order to provide like-minded citizens with public access to the internet as a tool for individual and collective empowerment in the information society. When internet connections in households were still rare, activists offered public access points, often in occupied buildings. Later, they started operating as non-commercial internet service providers (ISPs), offering at no cost 'secure' e-mail accounts, mailing lists and web hosting. Self-organized servers like Autistici/Inventati in Italy and Riseup in the United States are still very popular. Riseup, for example, hosts some 50,000 email accounts and over 1 million people subscribe to the mailing lists hosted on its servers.

Over the last couple of years, hacktivism has become more popular as Anonymous' nuisance campaign started making the news. The community originated in online chat rooms focused on politically incorrect pranks but later mutated into a politically engaged group, maintaining an orientation to the "lulz"—a neologism indicating the fun associated with pranks (Gorenstein Massa, 2010). Membership is informal

and fluctuating, and includes techno-savvy activists but also digital natives who believe in the potential of the internet for collective action. They take action against companies, governments, and individuals in retaliation for behaviors that threaten activist values and the uncensored internet (c.f., Coleman, 2010).

Cyberactivists continue to seek and defend spaces of autonomy in cyberspace, for example by creating encryption tools and alternatives to corporate social-networking services. Among the newest project are Crabgrass, a Riseup 'spin-off' an open-source software and social networking platform for activists, and Diaspora, a distributed social networking service based on the federation-of-servers model. Their developers aim at putting users back in control of their data, implementing privacy protection and collective user-based ownership. To respond to security and surveillance threats, hackers have created hands-on fixes such as Tor, an 'onion routing' encryption system designed to protect users' anonymity in online interactions. Meanwhile, following a call for the Hacker Space Program in summer 2011, a group of hackers proposed to build a satellite ground station and a distributed network that would provide a self-managed, cheap and secure Internet.

"Running servers for revolution": The ethics of radical tech activists

"Socializing knowledge, without creating powers", reads the manifesto of a collective of technology experts that offers 'secure' email accounts and web hosting at no cost to progressive activists. Since the early 2000s, this tech collective has operated as a nonprofit internet service provider, offering the digital tools and platforms that enabled the creation and coordination of many European activist networks. The manifesto goes on: "We want to open up the web in order to be able to act on two levels: on the one hand, to defend the right of each individual to free communication, anonymity, privacy, and access to the resources of cyberspace; on the other, we want to contribute to offline activism projects linked to our social reality."[6] Alternative ISPs are an example of cyberactivism focusing on self-organization for the creation of autonomous spaces. Their servers, whose location is carefully selected to avoid restrictive legislation and is sometimes kept secret, host websites, blogs, emails and list-servs. Platforms for self-production of information and knowledge sharing, such as etherpad services and wikis, may also be on offer.

This section illustrates the features and ethical values of the subcategory of cyberactivists operating nonprofit ISPs. As we will see, these activists are particularly concerned with the ethics of technology. They call themselves different names, as this call for action shows: "radical techies, anar(cho)geeks, hacklab members, keyboard squatters, tech-aware activists, autonomous administrators... we've often directly participated in that [i.e., the internet] evolution, advocating subversive uses of new technologies, hacking free software and sharing knowledge with passion, running servers for revolution".[7] For the sake of clarity, I refer to them as radical techies. I have spent some four years in the field observing closely the workings of several radical tech groups, interviewing over 40 activists from 16 countries in the five continents (Milan, 2009 and 2013).

Radical techies usually organize in small action-oriented cells of volunteers known as grassroots tech collectives. A typical tech collective would consist of half a dozen activists who are often, but not necessarily, based in the same town. Some groups have weekly meetings, some even operate a computer lab, but most of their work and communications takes place online. Daily tasks include managing webservers; larger projects may involve the development of open source software. They perform a crucial

[6] The manifesto has been slightly modified to prevent the identification of the group.

[7] "[IMC-Tech] meeting to defend our autonomous servers – an invitation", personal communication, 18 June 2006. A People's Global Action meeting on communication infrastructure identified alternative ISPs as "organizations running a server to support movements for political change to get direct access and participatory access to the web and media" (People's Global Action, 2006).

role for the contemporary social movement scene, as they provide the digital backbone for activists to network, communicate, and protest. In Europe, in particular, they emerged in the milieu of the squatted social centers, with strong linkages to the more radical and antagonist scene. One of the biggest European alternative ISPs hosts about 4,000 e-mail accounts, and over 30,000 people subscribe to the mailing lists hosted in the server. Annual revenues from donations do not exceed €5-6,000, which are largely insufficient to cover the operational costs.

Radical tech collectives become more visible when they step out of cyberspace. Tech groups have established media centers at major protest events such as G8 meetings and United Nations summits. Over the last decade Indymedia activists have set up tents with computer equipment in the middle of actions to allow other activists to upload their reports directly from the streets. A collective once transformed a countryside barn in a remote North German village into a media hub that provided thousands of environmental activists with a sophisticated communication infrastructure to report on a protest against nuclear waste shipments.

Radical tech groups are mostly located in the Western world, due to the availability of cheap technology, fast connections, expertise, but also a certain degree of internet freedom. There are two or three such groups in each Western country, and a few others in Latin America, South-East Asia, and Australia. Over the last decade, their activities have been increasingly targeted by state repression because of their role as backbones of activist organizing. Server seizures have affected, among others, the Indymedia network (2004 and 2008), Autistici/Inventati (2004), Riseup, May First/People Link, and European Counter Network (2012).

Radical tech groups generally take very seriously the ethical principles regulating their internal organizational dynamics. But, most importantly, these principles are mirrored in the very same services they run and in the ways they are designed. Although their services might look similar to what corporate servers offer (free email accounts, for example), they are inspired to the values of openness (e.g., open standards, open process and open architecture), horizontal collaboration, and decentralization. Rather than profit, they put at the center the user and his/her right to anonymity, autonomy, free expression and knowledge sharing. For example, groups commit to protect user anonymity and individual privacy, and promise not to release user data to third parties, including security forces. In doing so, they may act in open violation of data retention and user traceability legislation such as the European Union Data Retention Directive (no. 2006/24/EC), which forces all providers of electronic communication to retain users' connection meta-data and release them upon request. Further, they design and supply privacy-protection tools such as anonymous remailers and encryption systems, in order to, as a mission statement reads, "form and inform on the need to protect one's own privacy and avoid the plunder of personal data by governments and businesses alike".

Radical techies reject top-down power in the form of institutions and state control. They tend to share an anti-establishment ethos and a political radicalism that translates into a principled scepticism towards power-holders and power structures. The challenge to authority is present in both their organising principles and the services they offer. They practice grassroots autonomy, which refers both to the autonomy of the group from the socio-political context in which it is embedded and the autonomy of the individual within the group. Hierarchical forms of organisation and representation (e.g., spokespersons) are typically rejected.–Instead, radical techies lean towards what has been called a "community without structure" (Leach, 2008, p. 1059), with decentralisation and horizontality as primary organising principles. Informal hierarchies are kept in check by a continuous collective reflexive exercise. Decision-making is typically based on consensus, i.e. reaching an agreement that is acceptable to all members. This preference for consensus versus the majority rule mirrors the network metaphor of the internet where all bits are created equal. From decentralized social production (e.g., an approach to collaboration typical of the open source subculture) follows a tendency towards decentralized and distributed forms of organization. In this, tech activism embraces self-organization and the do-it-yourself' (DIY) and 'maker' cultures as its

constituent features. Autonomy is often inspired to the organizational principles of anarchism and anarcho-syndicalism (c.f. Day, 2005).

Radical techies emphasize communitarianism and participation. Communitarianism can be seen as a social conception of freedom: it gives weight to the differences created, for example, by languages and gender, and tries to incorporate them in the group internal dynamics. However, this communitarian dimension coexists with libertarian and individualized traits, which are particularly prominent in tech activism, because activities like coding and hacking are experienced individually, and expertise is owned at the individual level.[8] Participation means that groups are potentially open to anyone willing to get involved. However, members tend to share, often priori to action, a certain degree of social and political proximity (frequently friendship precedes the involvement with activism) that may alienate newcomers. To encourage participation, activists organize knowledge sharing workshops.

Similar to the organizations working on media democratization or internet freedoms, independent servers have a progressive agenda that includes the right to access communication platforms and share knowledge, freedom of information, privacy protection, and the defense of the right to dissent. They are an integral part of the current global mobilizations on media justice (Hackett and Carroll, 2006; Padovani and Calabrese, 2012), which include the recent protests against the US Stop Online Piracy Act, in support of net neutrality (Stein et al., 2009), or against data retention (Löblich and Wendelin, 2012). However, rather than engaging in advocacy, they tend to privilege a hands-on approach, creating and socializing spaces of autonomy in cyberspace and fuelling alternative practices.

The guardians of the internet? Ethical codes for cyberactivism

Like the hackers described by cyberpunk novelist Bruce Sterling, cyberactivists are

> "very serious about forbidden knowledge. They are possessed not merely by curiosity, but by a positive lust to know ... The intensity of this desire (…) may represent some basic shift in social values—a harbinger of what the world may come to, as society lays more and more value on the possession, assimilation and retailing of information as a basic commodity of daily life" (Sterling, 1993).

As active citizens of cyberspace and self-appointed "guardians" of the Internet, cyberactivists claim to embody a "shift in social values" away from the predominant commercialization and enclosure of cyberspace. What is this "shift in social values" about? We have seen how the services offered by radical techies represent an alternative to profit-oriented digital communication infrastructure: like its commercial counterpart, services are generally available free of charge, but they are modeled on values such as openness, knowledge sharing, and protection of personal communications. In this section, I move from the case of radical techies to offer a synthesis of the ethical codes of cyberactivists. I distinguish between an internal code, regulating interpersonal relations and group dynamics, and the ethics of technology, describing how technology should look like according to activists. The two are strictly linked to each other; they overlap in the design of technology and infrastructure (the "how" technology is designed, and the outcome of the process).

The internal code of cyberactivists revolves around three notions: equality, participation, and autonomy. Equality indicates the (alleged) lack of internal hierarchies, and the fact that groups tend to recognize to

[8] In this respect, radical tech groups embody what might seem to be a contradiction between individualism and collectivism: they retain the aspects of collectivism, but combine it with the informality and individualism of computer-grounded activism. This aspect is explored in Milan, 2012.

the individual a total independence of judgment[9], which results in the typical refusal of formal delegation and representation mechanisms. In this respect, internal decision-making is normally characterized by horizontality and the pursuit of consensus. However, the weight activists attribute to action may result in the potential distortion of collective decision-making processes–what a tech activist once called the "dictatorship of action", by which the urgency of taking action may result in decision-making cliques (Milan, 2013). Participation has both an individual and a collective interpretation: on the one hand, it subsumes an emphasis on first-person engagement and individual responsibility towards the community, while on the other it emphasizes communitarianism, collective improvement, and shared ownership. Finally, autonomy is a multifaceted behavioral norm: on the one hand, it indicates the hands-on approach to technology summarized by the DIY imperative, and visible in the activists' faith on the power of users and technical experts. On the other hand, it stands for the values of self-organization and self-determination, both of the group towards society as a whole, and the state in particular, and of the individual within the group.

The ethics of technology encompasses the three notions included in what I have called the internal code of cyberactivists, but adds a few more, namely the principle of openness and the notion of freedom as they apply to online interactions and to technology design. Equality, participation and autonomy merge into the hacker idea of cyberspace as an e-commons belonging to humanity, and to be more precise to the people daily engaging with it, i.e. users and developers. Further, equality refers also to code and bits, as seen for example in principles like net neutrality, which indicates the non-discrimination of traffic on the basis of content. Autonomy as self-determination translates into technology design that "builds in" the right to privacy and to the secrecy of personal communication. Autonomy as self-organization is visible in the rejection of state and business interference in the governance of cyberspace–the hands-off attitude enshrined in Barlow's famous injunction to states to stay out of cyberspace. The notion of autonomy justifies also the adoption of nuisance and trickery as Anonymous-style cyberactivism tactics, which can be interpreted as the reaffirmation of self-determination and independence of the activists from state authorities and the business rule (in other words, the fact that they disregard social norms). Openness refers to the accessibility, malleability and transparency of standards and software, but also of hardware and infrastructure architecture, along the lines first theorized by open source developers. It includes an emphasis on knowledge sharing, collaboration and collective improvement in dealing with technology, as well as to the notion of transparency and access to information similar to what WikiLeaks claims to defend. Finally, activists believe in preserving a number of freedoms in online interactions, including the fundamental freedoms already protected by the 1948 Universal Declaration of Human Rights (freedom of opinion and expression, freedom of association, etc. …), but also freedom of access and the highly contentious freedom (and ability) to embark in (politically-minded) collective action and dissent in cyberspace. Freedom of expression, in particular, entails that access to information is not enough, but individuals and groups must be able to freely produce and disseminate information, relying on, and repurposing if needed, existing knowledge and resources available online. Further, the internet and its applications should be kept free from surveillance by both state authorities and business actors, be it for repression, profiling or marketing purposes.[10] Finally, the notion of freedom speaks to the value of openness: cyberactivists reclaim the right to access, modify, and shape (i.e., 'hack') software and hardware according to their needs and preferences. Table 1 summarizes the ethical values of cyberactivists.

[9] The autonomy of judgment of individuals is however made possible by the pre-existing affinity of political and ethical values. In other words, group members have internalized the ethical code to the extent in which they can make autonomous choices if required by the situation.

[10] Joyce (2012) described the right to "freedom from fear" as it applies to the internet: in other words, "Citizens need to be able to use the internet for political purposes without fear of reprisal."

Table 1. Overview of the ethical values of cyberactivists

Equality	Participation	Autonomy	Openness	Freedom
• Rejection of hierarchies • Refusal of formal representation or delegation mechanisms • Pursuit of consensus • Independence of judgment of individuals (based on affinity) • 'All bits are equal'	• *At the individual level:* first-person engagement and individual responsibility • *At the group level:* shared ownership, collaboration, communitarianism • Participatory design	• Hands-on approach / DIY • Rule of users and developers • Self-organization • Self-determination • Hands-off approach (no state or business interference) • Privacy by design • Non-interference with a system's functionality ([11])	• E-commons • Openness of (and ability to modify) standards, architecture, software and hardware • Access to information • Knowledge sharing • Collective improvement	• Freedom of opinion and expression • Freedom of information • Ability to embark in collective action and dissent in cyberspace ("freedom from fear") • Freedom to hack software and hardware

Ethics and politics of studying cyberactivism

When I first approached a group of radical techies I wanted to study asking for an interview, the group explained: "in the past, we did not participate in any surveys/interviews etc. It was a decision based on the assumption that social science[s] are too often a police science plus that it is never clear who is going to use this research" (Milan, 2009, p. 68). This quote raises many suggestive points: the skepticism toward the exposure provided by academic research, the issue of relevance of the research not only for theory development but also for the research subjects, and the question of access and its negotiation.

Approaching cyberspace as an object of study is not as straightforward as it might seem at a first sight. To start with, cyberactivists often act underground, and are difficult to reach and reluctant to shed light on their practices, many of which remain surrounded by a great deal of mystery. Secondly, academic practices, grounded on individualism, intellectual ownership and restricted access to knowledge, conflict with the ways activists and activism projects work and with the values they stand for. This clash of organizational cultures and routines can seriously hinder collaboration. Thirdly, studying activism practices in cyberspace implies drawing public attention to projects and tactics that are often secretive, if not crossing the boundaries of illegality. This might invite repression and encourage surveillance, and can harm or jeopardize activist projects. Fourthly, cyberspace practices are often associated with anonymity, which may result in bias and misrepresentations in data collection as well as data analysis. At the same time, the availability of abundant data 'out there' and the unfiltered observation of online behavior (for example, in open list-servs, chat rooms, and forums), might tempt the researcher to go to the field under cover, which might have some serious ethical implications. For these reasons, approaching cyberactivism as an object of study reveals the need to rethink the practices of social research, both methods and epistemological considerations, and to approach critically the ethical standards of our research. This section is divided in two parts. The first focuses on the epistemological and ethical dimensions of research on cyberactivism, asking, 'how do we get to know what we know?' Epistemology is concerned with the study of knowledge,

[11] The hacker principle of non-interference with a system's functionality seems to have partially lost value amongst certain groups, certainly due to the increasing popularity of hacktivism. Even if it remains a fundamental guiding rule for a good portion of cyberactivists, others maintain that it can be sacrificed to the priority of drawing public attention to pressing problems such as online freedom of expression.

and, in my view, it has an essential ethical dimension built to it. The second part discusses the methodological challenges of gaining access to the field and working with cyberactivists.

To begin with, a cyberactivism researcher should adopt the hacker principles of "do not harm" and "leave no damage" as fundamental points of reference. This entails questioning the implications of studying a certain group or practice, and one's personal motivations for doing so. It means reflecting on how the research might impact on activists, and how might the activist community receive it. "Do not harm" commits researchers to a careful selection of objects of study and research questions. It requires care not to expose activist projects to repression by, for example, revealing confidential information, and a commitment to protect the informants' anonymity. If this is valid for any inquiry into social reality, it is particularly relevant in approaching controversial practices like, for example, hacktivism… not last, because it may hinder any future attempt at going to the field.

Studying cyberactivists means trying to bridge, or at least reduce, the gulf created by two profoundly different organizational cultures and routines: academic individualism on the one hand, and activist collectivism on the other. Further, activists often feel exploited by academics.[12] Researchers should acknowledge the material differences existing between themselves and the activists (e.g., the latter are typically volunteers), and negotiate with activists a way to correct this unbalance in power and resources (for example, selecting research questions that are relevant to activists, or even allocating a portion of research funding to support an activist project). This includes also finding ways to share the research results in a way that is acceptable to activists, for instance by publishing the research findings in open access journals. In my experience, the large majority of activists I have worked with posited knowledge sharing as a precondition to participate in the research.

Throughout the process, the researcher has to exercise recurrent reflexivity, critically questioning her identity and role as an observer immerged in a complex social world, torn between the scientific observation of social change and social change as it happens. In other words, studying activism, and cyberactivism in particular, implies a process of continuous redefinition of the self by the researcher, as activists regularly challenge identity, motivations, and standpoints of their interlocutors. The researcher has to learn to accept this very personal exposure as a legitimate part of the conversation. Reflexivity could the shape of "iterative cycles of dialog, action and reflection" (Ryan and Jeffreys, 2008, p. 4), involving both activists and researchers, and oriented to mutual learning.

A further ethical question one might ask is "what knowledge should be produced and for whom (Croteau et al., 2005). Observers claimed that there is a growing "artificial divide between the practice of social change and the study of such efforts" (Ibid., p. xiii). In this respect, the approach that I call "engaged research" represents a good compromise between a research exclusively oriented to theory development and the practice of action research (which in turn seeks to enact solutions to the problems brought forward by social actors).[13] I take "engaged research" to mean an inquiry into the social world which, without departing from systematic, evidence-based, social science research, is designed to make a

[12] According to my experience, the suspicion toward academics derives from three main problems. First, activists are under the impression that academics take advantage of activists merely to further their careers. Many activists I interviewed lamented that collaboration often ends abruptly once the researcher has collected enough data. Secondly, researchers seem to fail to recognize that activism is 'work': activists are not necessarily waiting for an opportunity to talk with researchers, and they may have better things to do. This is particularly true in the case of those activists who do not depend on, and may not even be interested in, public recognition. Thirdly, the researcher may eventually assume a position from which she *speaks for* the activists, and might end up being identified as the authority in the field–often at the expenses (and to the disappointment) of the activists on the ground.

[13] For an overview see Greenwood and Levin, 2005. The process of collaborative research is also called "co-generative inquiry".

difference for disempowered communities and people beyond the academic community.[14]

Faced with these challenges, how can a researcher create a respectful research relationship with her informants, one able to originate 'thick' reliable data? What follows illustrates some methodological 'tricks' that I have extensively tested in the field. They include allowing time for building a trusted relationship and a sustained dialogue, designing research questions that matter *also* to activists, learning new sociability skills to adapt to the activists' social environment, and respecting group dynamics.

A researcher can bridge the gulf between researchers and activists in two ways: by becoming a trustworthy interlocutor, and by designing a research that is acceptable to (and respectful of) the research subjects. Building a research relationship based on clarity, mutual respect and trust takes time, and requires frequent exchanges and lengthy negotiations. However, this phase of mutual learning has the benefit of considerably improving data collection. Including research questions that relate closely to the problems experienced by activists encourages them to accept the research as legitimate and engage with it. Further, the researcher should adjust her way of relating to respondents to the ways "in which social practices are defined and experienced" (Hine, 2005, p. 1). In the case of cyberactivists, this might mean to privilege online interactions over face-to-face exchanges, and might force the researcher to familiarize herself with the conventions and behaviors typical of cyberactivists. Using an email account from a nonprofit provider and encrypting emails might signal familiarity with, and respect for, the activists' values.

The individualism vs. collectivism divide has some methodological implications, too. In the absence of spokespersons, the researcher might have to address the group (and not the individual) as the unity of analysis. As one of my earlier interview partners noted, grassroots tech groups "are collective enterprises," and addressing individuals within the group means "breaking down the collective dimension" of the project (Hintz and Milan, 2010, p. 840). This, however, comes at the cost of extending considerably the time frame for data collection.

Finally, it is essential to question the amount and quality of data that is gathered and released to the public, in order to reduce the potential harm for the activists and their projects. This means, for instance, to look critically at what connections are exposed, what tactics are revealed, and to carefully weigh the costs and benefits of going public with certain findings.

Whereas most current social science is research *about* (social groups, processes, events), engaged researchers aim to make research *with* (i.e., in collaboration with) these subjects. Research *with* requires a commitment from both sides to collaborate and come to terms with the mutual differences. It involves a long-term time frame, recurrent cycles of reflection and negotiation, and constant adjustments along the way. In short, research *with*, in my view the most rewarding way of researching cyberactivism, is about developing fair relationships and an understanding of the research process as a, possibly equitable, collaboration. This also means—as banal as it may sound—to recognize that activism is 'work.'

In conclusion

In this paper, I set off with the task to illuminate the complex relationship between ethics and cyberactivism, looking at both the articulated ethical codes of cyberactivists, and the ethical challenges facing any researcher approaching cyberactivism as a field of study.

[14] To know more, see the special feature of the *International Journal of Communication* on the epistemology of engaged research that I edited in 2010 (Milan 2010b). The five articles offer useful case studies on the practice of engaged research.

Cyberactivists might often seem contradictory (and behave accordingly). However, cyberactivism politics embodies a strong ethical dimension that cannot be dismissed, precisely because it points to a "shift in social values" that has the potential to speak truth to power. Their contribution in envisioning a freer and more equal cyberspace is crucial to our society, in an age in which the world wide web, and the knowledge it hosts, bends more and more towards commercialization, privatization, and exclusion. The activist values of self-determination, equality, openness, communitarianism, and unfiltered freedom of expression may sound unrealistic. I argue that they should be considered in their guise of "guiding stars", that is to say principles that should inspire and orient human action, without we necessarily try to achieve them.[15]

Further, cyberactivism may lack accountability, but it expresses agency. In contemporary societies characterized by disaffection towards representative democracy and declining civic engagement, some expressions of cyberactivism may be interpreted as a quest for participation and an exercise of direct democracy. As such, cyberactivism has the potential of fostering individual and collective empowerment and participation. Some of its forms, such as self-organization and hit-and-run cyber disturbance actions, should be tolerated if not enabled. They can be seen as manifestations of an emerging grassroots social force pushing the boundaries of liberal democracies and questioning the relationship between individuals and the state as well as the role of the state as the guardian of individual freedoms. Rather than enemies of liberal democracy, cyberactivists are the carriers of grassroots demands concerning the present and future of our society–a society that, to quote Sterling, "*lays more and more value on the possession, assimilation and retailing of information as a basic commodity of daily life.*"

I advocate for a critical approach in addressing cyberspace as a field of study, one that takes the hacker imperatives to "leave no damage" and "do not harm" as essential benchmarks. There is an ethical dimension of research into cyberspace activism that is crucial also for the advancement of social theory. While acknowledging cyberactivists as carriers of alternative narratives of cyberspace, we should engage with the ethics of studying cyberspace activism, respecting as much as possible the cyberactivists' values and the boundaries they might impose on us, even when they are difficult to understand. Researchers should adopt the activists' preferences in matter of researching their own activities, not only in view of obtaining unrestricted access and avoiding bias and deliberate distortions of data, but also in view of making research that matters to the groups being researched and, possibly, to society as a whole.

[15] This metaphor was mentioned by an Indymedia activist in an interview with Arne Hintz (2009).

References

Barlow, John Perry (1996). "A Declaration of the Independence of Cyberspace," 8 February.

Carter, Adam (2012). "From Anonymous to shuttered websites, the evolution of online protest", CBC News, 15 March.

Cerf, Vinton (2004). "First, Do No Harm," in Internet Governance: A Grand Collaboration (ed. Don MacLean) (New York: United Nations ICT Task Force), 13-15.

Coleman, Gabriella (2010). "What It's Like to Participate in Anonymous' Actions", *The Atlantic,* 10 December.

Critical Art Ensemble (1993). The Electronic Disturbance (New York: Autonomedia, 1993).

Critical Art Ensemble (1996). Electronic Civil Disobedience (New York: Autonomedia).

Croteau, David, William Hoynes, and Charlotte Ryan, eds. (2005). Rhyming Hope and History: Activists, Academics, and Social Movement Scholarship. (University of Minnesota Press: Minneapolis).

Day, Richard (2005). Gramsci is Dead: Anarchist Currents in the Newest Social Movements (Pluto Press: London).

Delio, Michelle (2004). "Hacktivism and How It Got Here", *Wired*, 14 July.

Gorenstein Massa, Felipe (2010). Out of Bounds: The Anonymous Online Community's Transition to Collective Action. (Unpublished manuscript, Boston College).

Greenwood, Davydd J. and Morten Levin (2005). "Reform of the social sciences and of universities through action research", in The Sage Handbook of Qualitative Research. (eds. Denzin N. K. and Y. S. Lincoln) (Sage: Thousand Oaks, CA), 43–64.

Hackett Robert A. e William K. Carroll (2006). Remaking media. The struggle to democratize public communication (Routledge: London and New York).

Hamm, Marion (2005). "Indymedia—Concatenations of Physical and Virtual Spaces," January 2005.

Hine, Christine, ed. (2005). Virtual methods. Issues in social research on the Internet. (Berg: Oxford and New York).

Hintz, Arne (2009). Civil Society Media and Global Governance: Intervening into the World Summit on the Information Society. (Lit: Münster).

Hintz, Arne and Stefania Milan (2010). "Social Science is Police Science: Researching Grass-Roots Activism". *International Journal of Communication* 4 (2010), Feature: 837–844.

Leach, Darcy (2009). "An elusive 'we': Anti-dogmatism, democratic practice, and the contradictory identity of the German Autonomen", *American Behavioural Scientist*, 59: 1042-1068.

Levy, Steven (1984). Hackers: Heroes of the Computer Revolution. (New York: Dell/Doubleday).

Löblich, Maria and Manuel Wendelin (2012). "Civil Society Participation in Internet Politics on the National Level and beyond. A Case Study on Germany", *New Media and Society* (online pre-print)

Joyce, Mary C. (2012). "The four freedoms of the internet", *Meta-Activism Blog*.

Jordan. Tim and Paul A. Taylor (2004). Hacktivism and Cyberwars: Rebels with a Cause? (London: Routledge).

Murphy, Brian (2000). "The Founding of APC: Coincidences and Logical Steps in Global Civil Society Networking." Association for Progressive Communications Annual Report 2000, 28-30.

Martinez-Torres, Maria Elena (2001). "Civil Society, the Internet, and the Zapatistas," *Peace Review* 13, 3: 347- 355.

Meikle, Grahan (2002). Future active: Media activism and the Internet. Future Active: Media Activism and the Internet (Routledge: New York).

Milan, Stefania (2009). Stealing the fire. A study of emancipatory practices in the field of communication. PhD dissertation, European University Institute.

Milan, Stefania (2010a). "The Way Is the Goal: Interview with Maqui, Indymedia London / IMC-UK Network Activist," *International Journal of E-Politics*, 1, no. 1, (2010): 89.

Milan, Stefania (2010b). "Toward an Epistemology of Engaged Research", *International Journal of Communication* 4 (2010), Feature: 856-858.

Milan, Stefania (forthcoming, 2012). "WikiLeaks, Anonymous, and the Exercise of Individuality: Protesting in the Cloud", in Beyond WikiLeaks: Implications for the Future of Communications, Journalism & Society (eds. Benedetta Brevini, Arne Hintz and Patrick McCourdy) (Palgrave Macmillan: Basingstoke, UK).

Milan, Stefania (forthcoming, 2013). Wiring Social Movements. Emancipatory Practices for Autonomous Communication Infrastructure. (Palgrave Macmillan: Basingstoke, UK).

Padovani, Claudia and Andrew Calabrese (forthcoming, 2012). Communication Rights and Global Justice: Reflections on the Short History of a Social Movement. (Hampton Press: Cresskill, NJ).

People's Global Action (2006). Call for a meeting to defend our autonomous servers. Interpersonal communication.

Ryan, Charlotte and Karen Jeffreys (2008). The Practice of Collaborative Theorizing. Unpublished manuscript.

Stein, Laura, Dorothy Kidd, and Clemencia Rodriguez (2009). Making our media. Volume Two: National and Global Movements for Democratic Communication, (Hampton Press: Cresskill, NJ).

Sterling, Bruce (1993). The Hacker Crackdown: Law and Disorder on the Electronic Frontier (New York: Bantam).

Stone, Brad and Michael Riley (2011). "Hacker vs. Hacker", BloombergBusinessWeek Magazine, 10 March.

Vegh, Sandor (2003). "Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank," in Cyberactivism: Online Activism in Theory and Practice (eds. Martha McCaughey & Michael D. Ayers) (New York: Routledge), 72-73.

Wong, Wendy and Andrew Brown (2012). Nobody from Everywhere: IR and the Politics of Wikileaks and Anonymous. Paper for the BSIA conference, University of Waterloo, 17 April

Directory of the groups cited in this paper

Anonymous. Online community whose self-identified members engaged in disturbance action in cyberspace and beyond (most notably, DDoS attacks).

Association for Progressive Communications **(APC).** Founded in 1990, it is an international NGO committed to empower and support the civil society through ICTs. It is also a network of over 50 civil society organizations, most of which in developing countries. Many members work also as nonprofit ISPs.

Autistici/Inventati **(A/I).** Italian nonprofit internet service provider linked to the radical social movement scene.

Chaos Computer Club **(CCC)**. Based in Germany, it is probably the biggest hacker organization. Promoter of the hacker ethic, and concerned with transparency in government and freedom of information. It organizes annually the Chaos Communication Congress, in Berlin. /

Crabgrass**.** Web application designed for social networking, group collaboration and network organizing. It is a Riseup production.

Critical Art Ensemble **(CAE).** Tactical media collective operating at the intersection of between art, critical theory, technology, and political activism. Active since 1987.

Cult of the Dead Cow (now **Hacktivismo**). Texas-based underground computer group. Credited with having invented the term "hacktivism".

Diaspora**.** Distributed social networking service. It aims at putting the user back in control of his or her data.

European Counter Network (**ECN**, also known as **Isole nella Rete**). The oldest provider of the European radical social movement scene. Inspired to antifascist values, it started in the 1990s as a BBS service. It launched NGVision, the first video sharing platform for the publication of video footage from street demonstrations.

FidoNet**.** Worldwide independent computer network used in the 1990s for communication between BBSs.

GreenNet **(GN).** Founded in 1986, London-based GreenNet is a ethical ISP dedicated to the environmental activism community. Member of the APC. http://www.gn.apc.org

Independent Media Centre **(IMC**, or **Indymedia).** The first IMC was established in 1999 in Seattle in occasion of the summit of the World Trade Organization, in order to provide activists with a platform to report directly from the streets. It is now a global network of independent information.

Lulz Security (or **LulzSec).** Group of hackers responsible of some renowned cybersecurity attacks against Sony and the website of the CIA. Its members were arrested in 2012.

May First/People Link**.** New York-based member-run progressive ISP. The motto reads "Growing networks to build a just world". It provided the communication infrastructure to the Social Forum of the Americas.

PeaceNet and EcoNet (now The Institute for Global Communications). Emerged from some of the first experiments of connectivity for civil society groups, it now only web hosting services to nonprofit groups, individuals, and small companies.

Riseup**.** Based in the United States, it is one of the biggest alternative ISPs. It provides online communication tools such as webhosting, email accounts but also VPN, chat, and etherpad services to social change activists.

Resist!ca Set up in 2000, it is a Vancouver-based anarchist server offering email accounts and mailing lists to anti-capitalist activists.

Tor. Free software designed to protect users from network surveillance (and traffic analysis in particular). Based on the onion routing system.