WHEN POLITICS AND TECHNOLOGY SPEAK THE SAME LANGUAGE:

Stewardship in Cyberspace According to Cyberactivists

STEFANIA MILAN

Citizen Lab, Munk School of Global Affairs, University of Toronto

MARCH, 2012

CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

Canada Centre for Global Security Studies

MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO

> —Hackers 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, as manifested by these young technophilic denizens of the Information Age, may in fact *be* new, and 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.[1]

This quote by cyberpunk novelist Bruce Sterling dates back to 1993, but it could have been written yesterday. Over the last few years, cyberactivists, hackers, radical techies, and hacktivists have become a disruptive social force that can no longer be ignored. As active citizens of cyberspace and self-appointed "guardians" of the Internet, cyberactivists claim to embody a "shift in social values" away from the commercialization and enclosure of cyberspace. But what does it mean to be a "steward of cyberspace" as a cyberactivist? What is the role of cyberactivists in supporting cyberspace as a commons? In this paper I explore stewardship in cyberspace from the cyberactivist point of view. 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. Examples of cyberactivism include electronic disturbance tactics and online civil disobedience, self-organization and autonomous creation of infrastructure, software and hardware hacking, and hacktivism.[2]

I see cyberspace 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: first, it is a "gym" in which to practise political participation and digital citizenry, where alternative and often contradictory views about society are articulated and shared. Second, it is a platform for collective action, like a public square would be: a site to articulate, organize, and bring forward social struggles, a site where cyber-specific forms of collective action can take place. But far from being only a set of tools, cyberspace has become a site of struggle in its own right, because it has partially lost its original character as an e-commons and is threatened by increasing commercialization, tightening state control, and restrictive legislation.

Here I examine forms and practices of cyberactivism seen through the lenses of cyberactivists' perception(s) and vision(s) of cyberspace. The assumption is that perceptions of what is or is not

1 Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam, 1993). Available at http://cyber.eserver.org/sterling/crackdwn.txt.

2 Cyberactivism means different things to different people. Sandor Vegh 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). (Sandor Vegh, "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, 2003), 72-73. Here I adopt a restrictive notion of cyberactivism focusing on infrastructure-related activism and ignoring, for example, organizing and networking. In addition, the focus is on collective actors such as networks of hackers or Internet activists—individuals, such as bloggers writing in their own capacity, will not be considered. Generally speaking, cyberactivists are part of the organized civil society. By organized civil society I mean the realm of nonstate and nonbusiness actors, organized in formal (nongovernmental organizations) or informal (social movements, networked collective action) groupings and networks.

a legitimate practice in cyberspace, as well as the expectations concerning what cyberspace should look like, guide online behaviour, and thus shape a certain understanding of rights and duties in cyberspace. First I present a timeline of cyberactivism and explore activists' values and their perceptions of cyberspace. Then, I reflect on the state of things in contemporary cyberactivism. Finally, I bring my observations on cyberactivists' online behaviour and perceptions of cyberspace to bear with the notion of stewardship in cyberspace.

A BRIEF HISTORY OF INFRASTRUCTURE ACTIVISM IN CYBERSPACE

Activism targeting or exploiting cyberspace infrastructure has taken many forms, from self-organization for the creation of alternatives to electronic disturbance to hacktivism. Generally speaking, we can boil down these practices into two categories: subversion and disruption of the existing order in cyberspace, and self-organization for the creation of autonomous spaces. 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 commons that should be freely and equally enjoyed by all netizens—with the exclusion of those who are believed to actively work against these principles.

HACKERS AND OPEN SOURCE

Not surprisingly, the idea of an e-commons emerged 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, emerged in the 1970s around the Massachusetts Institute of Technology. Hackers were intrinsically apolitical, and operated under a set of tacit values that later became known as "hacker ethics." These principles included freedom of speech, access to information, world improvement, and non-interference with the system's functionality. (These values are encapsulated in their injunctions to "leave no damage" and "leave things as you found them [or better]"). Around the same time, software developers and user communities started advocating and practising 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 or free software movement. Hackers and open-source advocates shared a hands-on attitude to computing; however, hackers emphasized a "do not harm" approach whereas open-source advocates championed collective improvement and selfless collaboration.

CYBERSPACE FOR CIVIL SOCIETY

The first social experiments using 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), the precursor of the modern Internet which allowed users to exchange messages and files through 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 large, well-resourced 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 social change 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. Founders "had the Internet vision of global communications unfettered by commercial barriers."[3] In 1990 nonprofit Internet providers joined forces in the Association for Progressive Communications 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."[4]

HERE COMES THE INTERNET

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."[5] The 1994 Zapatista uprising served as a source of inspiration for Western activists: exploiting the ontological qualities of the Internet, such as its ability to reach out to the most remote nodes, insurgents managed to transform a local struggle in the remote Mexican state of Chiapas into the first "information guerrilla movement."[6] The Internet allowed the nascent social movement to speak for itself and control information vital to its survival, and served as the backbone for the creation of supportive transnational networks able to amplify its messages. In 1996 the Zapatistas called for "mak[ing] a network of communication among all our struggles and resistances."[7] 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 piece of software called "Active" (developed by the activist community in Sydney, Australia, and released as free software), users could publish texts and pictures online without editorial filter or registration. In this respect, activists consider Indymedia "the mother of all blogs."[8] In 2002, three years after its foundation, there were already eighty-nine IMCs across six continents. For almost a decade Indymedia served the communication needs of social movements across the world. Similar do-it-yourself projects appeared that put self-organization, free

3 Brian Murphy, "The Founding of APC: Coincidences and Logical Steps in Global Civil Society Networking." Association for Progressive Communications (APC) *Annual Report 2000*, 28-30, http://www.apc.org/about/history/coincidences-and-logical-steps-in-networking.

4 "The APC Vision," About APC, http://www.apc.org/en/about.

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

6 Maria Elena Martinez-Torres, "Civil Society, the Internet, and the Zapatistas," *Peace Review* 13, no. 3 (2001): 347-355.

7 Marion Hamm, "Indymedia—Concatenations of Physical and Virtual Spaces," January 2005. Available at http://republicart.net/disc/publicum/hamm04_en.htm.

8 Milan "The Way Is the Goal," 89.

speech, and the cooperation of countless individuals at the centre of social change.

HANDS OFF THE INTERNET

In 1996 US cyber-libertarian activist John Perry Barlow launched the "declaration of independence of cyberspace." The declaration reads: "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."[9] 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 individual developers, civil society-based creators of information technology, and small businesses. 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—self-regulation of those who create and use the infrastructure is the only legitimate form of regulation in cyberspace, and should be based on the prerogative "First, do no harm."[10]

THE DAWN OF HACKTIVISM

In the 1990s protest extended to cyberspace, as new forms of expressing dissent emerged that took advantage of the low cost and flexibility of network-mediated communication. In 1995 the first netstrike, "a networked version of a peaceful sit-in" according to its promoters, targeted the French government in opposition to its nuclear experiments in the Mururoa Atoll, Polynesia. In mid-1990s, the US tactical media collective known as 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.[11] Online direct action such as virtual sit-ins, "digital storms," and denial-of-service attacks aimed at making a website temporarily unavailable were seen as the virtual equivalent of blocking a company's headquarters. However, according to the CAE electronic disturbance was a cell-based form of direct action, as opposed to a mass movement—a hit-and-run media intervention exploiting decentralization, one of the features of contemporary societies. In 1996, the Texas-based "computer underground group" known as Cult of the Dead Cow coined the term *hacktivism* to indicate the politically motivated use of technical expertise like coding—in other words, hacktivists seek to fix society through software and online action. Thanks to the controversial actions of online collectives such as Anonymous, the concept is very popular nowadays. However, different groups associate different objectives and tactics under its umbrella, not all of which are compatible. For example, hacktivism's disruptive nature crashes with the freedom-of-information and no-damage

9 John Perry Barlow, "A Declaration of the Independence of Cyberspace," 8 February 1996, available at https://projects.eff.org/~barlow/Declaration-Final.html.

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

11 Critical Art Ensemble, *The Electronic Disturbance* (New York: Autonomedia, 1993) and *Electronic Civil Disobedience* (New York: Autonomedia, 1996). Available at http://www.critical-art.net/books.html.

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. In addition, the most disruptive forms of cyberactivism such as sabotage cross the boundaries of acceptable practices in liberal democracies. In this respect they do nothing but contribute to a backlash against cyberactivism.

RADICAL TECH ACTIVISM AND ALTERNATIVE ISPS

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."[12] Networking infrastructure became an object of contention in its own right. Radical tech activism was born, with the aim of creating autonomous cyber-infrastructure independent from the state and the market. Projects aimed at providing like-minded citizens with public access to the Internet as a tool for individual and collective empowerment in the information society. At first, when Internet connections in private homes were still rare, activists offered public access points such as Internet cafés, often in occupied buildings. But in particular they became noncommercial Internet service providers (ISPs), offering e-mail accounts and mailing-lists, web space and blogging platforms, encryption systems and etherpad services – at no cost and with a committment to privacy protection. Self-organized servers like Autistici/Inventati in Italy, Riseup in the United States, and Resist in Canada, continue to be very popular today. Riseup, for example, hosts some 50,000 e-mail accounts and over 1 million people subscribe to the mailing lists hosted on its servers. Both groups operate on a voluntary basis and through collective organizing principles and are commited to fighting online surveillance. They are connected to grassroots social movements: in Europe, in particular, they emerged in the milieu of the squatted social centres, with strong links to the more radical and antagonist scene. Nowadays, most groups exist only in cyberspace but occasionally, they step out. A German collective, for example, once transformed a countryside barn in a remote north German village into a high-tech media hub that provided thousands of environmental activists with a sophisticated communication infrastructure to report on a protest against nuclear waste shipments.

THE RENAISSANCE OF HACKTIVISM

Since 2008, hacktivism has become more popular and widespread as the disruptive actions of online communities like Anonymous and LulzSec have come under the spotlight. Anonymous is an online community whose self-identified members engage in disruptive activities, trickery, and nuisance campaigns in support of freedom of speech online. It originated in online chat rooms focused on politically incorrect pranks but mutated later into a politically engaged collective, maintaining an orientation to the "lulz" – a neologism indicating the fun associated with pranks. Membership is informal and fluctuating: among its members are techno-savvy activists but also digital natives and netizens who believe in the potential of the Internet for collective action. Hacktivists take action against companies, governments, and individuals in retaliation for behaviours that are considered a threat to activist values, such as openness and the uncensored Internet. Anonymous activists often define themselves as the

12 Milan "The Way Is the Goal," 88-89.

"guardians of the Internet." They have mobilized against anti-digital piracy legislation and campaigns, and in support of the whistle-blower site WikiLeaks by attacking (i.e., temporarily taking down) the websites of companies and security agencies guilty of taking action to enclose the Internet. Partially owing to cyber-libertarian thought, hacktivists see cyberspace as a secluded free space where the rules and norms of real life do not apply. At the same time, cyberspace functions as a cultural laboratory, and a place to have fun following one's own rules, regardless of whether having fun means politically incorrect or law-breaking behaviours.

PROTECTING PRIVACY, FREEDOMS AND AUTONOMY IN CYBERSPACE

As cyberspace becomes increasingly centralized in a handful of companies, hackers and radical techies try to create ways to move freely in cyberspace, for example, by creating alternatives to commercial social-networking services and encryption tools. As we speak, activists across the Western world organize to offer alternatives to corporate social-networking sites. Crabgrass, which originated within Riseup, is based on open-source software and targets the needs of bottom-up grassroots organizing; Diaspora is a distributed social-networking service based on the federation-of-servers model; the open-source and distributed microblogging service Thimbl uses existing software like SSH and xinetd/finger. Briar is a trust-based secure news and discussion platform for journalists and activists in authoritarian regimes; it allows users to create invitation-only discussion groups and aims at "creating spaces for disagreement. Instead of having only one space where we all agree, we should have as many spaces as necessary to encounter and disagree."[13] Other projects include Lorea from Andalusia, Spain, and Social Swarm and Secushare in Germany. They seek to put users back in control of their data, and implement privacy protection and collective and user-based ownership. To respond to security and surveillance threats, hackers created hands-on fixes such as Tor, an "onion routing" encryption system designed to protect users' anonymity in online interactions. Similarly, Freedombox aims at protecting individual privacy and anonymity by implementing end-user encryption. Meanwhile, following a call for the Hacker Space Program in summer 2011, a group of hackers proposed to build a distributed satellite communications ground station network that would provide fast, cheap. and secure Internet.

THE REALITY CHECK ON CONTEMPORARY CYBERACTIVISM

What is the state of things in contemporary cyberactivism and why do cyberactivists deserve our attention? First, cyberactivism and hacktivism in particular are increasingly popular and attract mostly digital native generations across social classes and geographies. What we have seen in action with Anonymous and LulzSec is a manifestation of a wave of movement activity that is virtual, distributed, and individualized. Hacktivism is no longer just a marginal struggle by a bunch of geeks, nor the terrain of skilled hackers in dark basements. What were, back in the 1990s, sporadic cell-based cyber performances are now tactics practised on a regular basis by decentralized networks of individuals seeking to intervene regularly in real-world struggles. The extraordinary visibility hacktivism acquired with the WikiLeaks case encouraged

13 Michael Rogers (from Briar) at Unlike Us Conference #2, Amsterdam, 10 March 2012.

more young people who do not care about the consequences to join the struggle. Certainly the popularity of cyberactivism is linked to the dramatic increase in the number of people with access to technology and technical expertise. But it is also due to the perception that activism that originates and lives in cyberspace is possible and worthwhile: compared to other activism tactics such as campaigning or street demonstrations, cyber disruption and electronic disturbance have an intense and real-time impact with only a limited deployment of resources.

Second, while cyberactivism may lack accountability, it expresses agency. In contemporary societies characterized by disaffection towards representative democracy and declining citizen participation and civic engagement, some expressions of cyberactivism may be interpreted as a quest for participation in society and an exercise of direct democracy. As such, cyberactivism has the potential of fostering personal and collective empowerment, participation, and self-determination. Hence some 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 and 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 societies.

CYBERACTIVISM AND STEWARDSHIP IN CYBERSPACE

Politically motivated cyberactivism relies on the use of information and communication technologies as tools for social change. Cyberactivists adopt different tactics and embody distinct visions of what cyberspace should look like. These distinct visions, however, boil down to a few aspects: decentralization, free speech, access, openness, cooperation, and transparency. Relationships in cyberspace should be as much as possible regulated by values other than money; they should put the user and his or her self-determination and agency at the centre, and be characterized by the respect for privacy, anonymity, and individual freedoms. In the eyes of cyberactivists, cyberspace is an arena for practising civic participation and exercising political agency, and a sphere of political and infrastructural autonomy to be defended from states and corporations. So, is cyberactivists' cyberspace compatible at all with the notion of stewardship? There are two possible answers to this question.

No, cyberactivism is not compatible with stewardship if stewardship equals corporate and state rule as the only sovereign power in cyberspace and the exclusive arbiter of online interactions and resource management. So far the connivance of corporations with the capitalist state has brought innovation and infrastructure development, but also surveillance and control. In such a scenario, all that is left to cyberactivists is resistance and sabotage. According to one of the Crabgrass developers, "the main problem in the political economy of information capitalism is surveillance. Can the rule of law be brought to bear on the internet? There is a concerted effort at the global level to create internet citizens by attaching real identities to bits. But as hackers we know this is not possible as identity cannot be enforced on bits. It will take a police state apparatus to enforce this technical fiction."[14] One of the crucial nodes for cyberactivists is the question of legitimacy and accountability of state and corporate rule in cyberspace. As Barlow puts it, "governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions."[15] This might be an extremist position, but the bad news is that governments and corporations can no longer simply ignore cyberactivists and their actions.

The second possible answer is more optimistic. Yes, cyberactivism is compatible with stewardship, if stewardship entails acknowledging the different souls inhabiting cyberspace and respecting if not protecting their values and diversity. After all, cyberactivists consider themselves the custodians of Internet freedoms. They do not reject the idea of stewardship as such. It all comes down to who the steward is, and what the values are that guide him or her. Effective and tolerable stewardship in cyberspace would necessarily have to go through a process of learning about and understanding the reciprocal differences in agendas, values, and priorities. I envision a division-of-labour model whereby different groups perform different stewardship functions in only partially overlapping circles of action. More specifically, the role of cyberactivists in sustaining and supporting cyberspace as a commons is to be found in their ability to embody high ideals of Internet freedoms and online collaboration, free from profit-oriented and control mechanisms. In this respect, cyberactivists can help to raise awareness and stand as a reminder of the ideals of participation and equality in cyberspace for which we should all strive.

14 Elijah Sparrow at Unlike Us Conference #2, Amsterdam, 10 March 2012.

15 Barlow, "A Declaration of the Independence of Cyberspace."

Stefania Milan studied communication sciences at the University of Padova, Italy, and holds a PhD in Political and Social Sciences from the European University Institute. Her research interests include digital technologies and participation, social movements, radical internet activism, and the interplay between technologies and society. She enjoys experimenting with digital, participatory and action-oriented research methods, and seeks to find ways of bridging research with policy and action. Stefania taught communications governance, digital technologies, and digital research methods at the University of Lucerne, Switzerland, and at the Central European University, Hungary. She has worked extensively in international media outlets and has been involved in media activism projects.

At the Citizen Lab, under the supervision of Professor Ron Deibert, Dr. Milan will investigate bottom-up infrastructure development. She will analyze how political and cultural values of activists and developers affect technology development and how it shapes power in cyberspace.