ELECTRONIC CIVIL DISOBEDIENCE AND THE WORLD WIDE WEB OF HACKTIVISM

A Mapping of Extraparliamentarian Direct Action Net Politics
(SWITCH / net/work/art)

Stefan Wray

Introduction

In the next century, when cyber-historians look back to the 1990s, they will recognize 1995 as the year of the graphical browser, the year the Internet began to be overshadowed by the Web. But they will probably also view 1998 as an important moment -- in the history of the browser wars. At a minimum, 1998 will be noted for the emergence of two terms that represent similar phenomena: electronic civil disobedience and hacktivism. In that year, a Net based affinity group called the Electronic Disturbance Theater pushed and agitated for new experimentation with electronic civil disobedience actions aimed mostly at the Mexican government. It engaged its FloodNet software and invited participation to an international set of artists, digerati, and political activists to make a "symbolic gesture" in support of Mexico's Zapatistas. While at the same time, in Britain, in Australia, in India, in China, on almost every continent there were reports of hacktivity. In the spring of 1998, a young British hacker known as "JF" accessed about 300 web sites and placed anti-nuclear text and imagery. He entered, changed and added HTML code. At that point it was the biggest political hack of its kind. Since then, and increasingly over the course of the year, there were numerous reports of web sites being accessed and altered with political content.

Taken together we may consider both the more symbolic electronic civil disobedience actions and the more tangible hacktivist events under the rubric of extraparliamentarian direct action Net politics, where extraparliamentarian is taken to mean politics other than electoral or party politics, primarily the grassroots politics of social movement. By no means was 1998 the first year of the browser wars, but it was the year when electronic civil disobedience and hacktivism came to the fore, evidenced by a front page New York Times article on the subject by the end of October. Since then the subject has continued to move through the media sphere. 1

What this paper attempts to do is examine these emerging trends from a slightly wider angled lens. This paper puts forth five portals for consideration: computerized activism, grassroots infowar, electronic civil disobedience, politicized hacking, and resistance to future war. At first they were conceived as five portals into Hacktivism, but perhaps they better serve as five portals for looking at the wider world of extraparliamentarian direct action Net politics, although that phrase is admittedly awkward. Nevertheless, these five portals seem to provide a useful starting point for a more in-depth, yet to come, examination of the convergence of activism, art, and computer-based

communication and media. In addition to starting to define, to frame, and to contextualize contemporary hacktivity, in terms of its roots, its lateral dimension, and its trajectivity, this paper also asks some nascent questions of a political, tactical, technological, ethical, and legal nature and makes some preliminary claims about the likely direction of these various movements.

Computerized Activism

Computerized activism exists at the intersections of politico-social movements and computer-mediated communication. The origins of computerized activism extend back in pre-Web history to the mid 1980s. As an example, the first version of PeaceNet appeared in early 1986. PeaceNet enabled - really for the first time - political activists to communicate with one another across international borders with relative ease and speed. 2 The advent of newsgroup services like PeaceNet, and wider dispersal of other Bulletin Board Systems, email lists, and gopher sites characterizes the cyber-environment within which most early on-line political activists found themselves. This largely text-based environment persisted up until as late as 1994 and 1995, when the first GUI browsers were introduced. Even today, while Web sites augment these earlier forms, email communication remains a central device in the international circulation of struggle and the creation and maintenance of international solidarity networks.3

During the early to mid 1980s the subject of computer-mediated communication (CMC) was taken up by scholars in, for example, psychology and sociology. When communication scholars began to examine CMC, and in particular when they began to assess the juncture of political communication and CMC, a number of academic treatments of "electronic democracy" were written in which politics is positioned narrowly within the confines of electoral or parliamentarian politics. 4 Among the earliest treatments of CMC from among communication scholars who entertain extraparliamentarian or grassroots politics is by Downing in "Computers for Political Change." 5 Not surprisingly, PeaceNet is one of his case studies. For purposes of tracing the origins of more current cross-border email exchange and its role in creating and maintaining international solidarity networks, Downing points to PeaceNet's establishment of international links in 1987. Among early adopters of these means of communication were people in the 1980s anti-nuclear and Central American solidarity movements.

By the late 1980s and the very beginning of the 1990s, the significance of cross-border, international, email communication began to be realized. The international role of email communication, coupled to varying degrees with the use of the Fax machine, was highlighted in both the struggles of pro-democracy Chinese students and in broader trans-national movements that lead to the dissolution of the Soviet Union. Shortly thereafter, we began to see scholarly work on this subject. Harasim’s "Global Networks: Computers and International Communication" began to theorize about the role of international email communication in linking together the world. 6

Computerized activism remained marginal to political and social movements until the explosion of the Internet in the early to mid 1990s and more so until the arrival of the graphical browser in 1994 and 1995. Now, in the post-Web Internet phase there is widespread use of these media forms by a plethora of grassroots groups and other political actors in countries all over the world. 7

A common thread or understanding that runs through various types of politically based computer-mediated communication, from early BBS systems, to email listservs, and to sophisticated Web sites with fancy bells and whistles, seems to be an overarching dominant paradigm that privileges discourse, dialogue, discussion and open and free access. This observation becomes important when looking more at electronic civil disobedience and politicized hacking, because it is with this dominant paradigm of the Habermasian Web that these later forms conflict and cause friction.

So the first portal of Computerized Activism is important for understanding the roots of today's extraparliamentarian, more direct action focused, political CMC. It is the portal that has been with us the longest, and the portal within which most political actors on the Net feel the most comfortable. Computerized activism, defined more purely as the use of the Internet infrastructure as a means for activists to communicate with one another, across international borders or not, is less threatening to power than the other types of uses we see emerging in which the Internet infrastructure is not only a means toward or a site for communication, but the Internet infrastructure itself becomes an object or site for action. This transgression, or paradigmatic shift in thinking, of moving away from believing the Internet solely as communication device to Internet as communication device and site for action is dealt with incrementally in the next four sections.

Grassroots Infowar

Grassroots infowar is an intensification of computerized activism. Infowar here refers to a war of words, a propaganda war. Grassroots infowar is the first step, the first move away from the Internet as just a site for communication and the beginning of the transformation from word to deed. Grassroots infowar actors emerge fully cognizant they are on a global stage, telepresent across borders, in many locations simultaneously. There exists a sense of immediacy and interconnectivity at a global level. More than a mere sharing of information and dialogue, there is a desire to push words towards action. Internet media forms become vehicles for inciting action as opposed to simply describing or reporting.

In the early 1990s, following the U.S. directed "smart" bombardment of Iraq and following the dissolution of the Soviet Union and the subsequent uselessness of Cold War rhetoric as a rationalization for foreign intervention, the U.S. military-intelligence community, along with its allies in financial-corporate sectors, needed to craft a new military doctrine. Their answer was Information Warfare and the threat of info-terrorism. State-side scholars at RAND, a think tank in Santa Monica, California, that often does the military's "thinking", set about devising new theoretical constructs that would lay the

basis for their version of Information Warfare. In 1993, under the RAND banner, Ronfeldt and Arquilla wrote Cyberwar is Coming! This work sets out the distinctions between netwar and cyberwar and is cited by nearly every subsequent treatment of Information Warfare theory.8 Where netwar refers more to the war of words, the propaganda war that exists on the Internet itself, cyberwar refers to cybernetic warfare, war dependent on computers and communications systems, the war of C4I - Command, Control, Communication, Computers, and Information.

Not long after RAND's theoretical intervention, pragmatic cases of netwar appeared. Among the most celebrated is the case of Mexico's Zapatistas and the international community of supporters that quickly brought that struggle on to the Internet. With the global pro-Zapatista Internet experience there began to be a rethinking or an interrogation of RAND's theoretical constructs, albeit from a more radical grassroots perspective. Some of this recasting has been brought forth in pieces by Harry Cleaver, a professor at the University of Texas at Austin and key person behind the Chiapas95 project, an email-based news and information distribution service. Probably Cleaver's most well known work in this regard is "The Zapatistas and the Electronic Fabric of Struggle." 9

Despite some radical interventions and attempts to reframe dominant forms of military and intelligence Information Warfare theory, most of the material, not surprisingly, is produced by the likes of RAND, the National Defense University, the Department of Defense, the US Air Force, or private sector initiatives. The meme of Information Warfare seems to have spread and been promulgated largely through network security paranoics and others keen on guarding digital property. But there are signs that Information Warfare is spreading to other areas. This year Information Wafare hit the international digital arts community by being the main subject of the annual Ars Electronic Festival in Linz, Austria.9

Theorizing about grassroots or bottom-up Information Warfare doesn't nearly get as much attention as the dominant models and as a consequence there is not much written on the subject. 11 The case of the global pro-Zapatista networks of solidarity and resistance offers a point of departure for further examination of grassroots infowar. One feature of Zapatista experience over the course of the last 5 years is that it has been a war of words, as opposed to a prolonged military conflict. This is not to say there isn't a strong Mexican military presence in the state of Chiapas. Quite the contrary is true. But fighting technically ended on January 12, 1994 and since then there has been a ceasefire and numerous attempts at negotiation.12 What scholars, activists, and journalists, on both the left and the right, have said is that the Zapatistas owe their survival at this point largely to a war of words. This war of words, in part, is the propaganda war that has been successfully unleashed by Zapatista leaders like Subcommandante Marcos as well as non-Zapatista supporters throughout Mexico and the world. Such propaganda and rhetoric has, of course, been transmitted through more traditional mass communication means, like through the newspaper La Jornada. 13 But quite a substantial component of this war of words has taken place on the Internet.

Since January 1, 1994 there has been an explosion of the Zapatista Internet presence in the forms of email Cc: lists, newsgroups, discussion lists, and web sites.14

A primary distinction, then, between earlier forms of computerized activism and forms of grassroots infowar is in the degree of intensity. Coupled with that is the degree to which the participants are noticed and seen as a force. Given the Zapatistas relatively high profile in Mexican society over the course of the last five years, and given the fact that they are technically a belligerent force negotiating with a government, the Internet activity surrounding them takes on a different significance than, say, for example, the Internet activity of the Sierra Club, Amnesty International, or other similar ventures.

An important difference is that in grassroots infowar comes the desire to incite action and the ability to do so at a global scale. At the end of 1997, news of the Acteal massacre in Chiapas, in which 45 indigenous people were killed, quickly spread through global pro-Zapatista Internet networks. Within a matter of days there were protests and actions at Mexican consulates and embassies all over the world.15 This incident, too, is now seen as a turning point in the stance by some toward the Internet infrastructure. While prior to this moment, there had been few if any incident reports of pro-Zapatista hacktivity, following there has been a shift, the beginning of the move toward accepting the Internet infrastructure as both a channel for communication and a site for action.

Electronic Civil Disobedience

Acting in the tradition of non-violent direct action and civil disobedience, proponents of Electronic Civil Disobedience are borrowing the tactics of trespass and blockade from these earlier social movements and are experimentally applying them to the Internet. A typical civil disobedience tactic has been for a group of people to physically blockade, with their bodies, the entranceways of an opponent's office or building or to physically occupy an opponent's office -- to have a sit-in. Electronic Civil Disobedience, as a form of mass decentered electronic direct action, utilizes virtual blockades and virtual sit-ins. Unlike the participant in a traditional civil disobedience action, an ECD actor can participate in virtual blockades and sit-ins from home, from work, from the university, or from other points of access to the Net. [16]

The phrase "Electronic Civil Disobedience" was coined by a group of artists and theorists called the Critical Art Ensemble. In 1994 they published their first book that dealt with this subject, "The Electronic Disturbance," followed two years later by "Electronic Civil Disobedience and Other Unpopular Ideas."16 Both of these works are devoted to a theoretical exploration of how to move protests from the streets onto the Internet. They examine the tactics of street protest, on-the-ground disruptions and disturbance of urban infrastructure and they hypothesize how such practices can be applied to the Internet infrastructure.17

Before 1998, Electronic Civil Disobedience remained largely as theoretical musings. But after the 1997 Acteal Massacre in Chiapas, there was a shift toward a more hybrid position that views the Internet infrastructure as both a means for communication and a site for direct action. This shift distinguishes more sharply the third portal of Electronic Civil Disobedience from the first and second portals.

Electronic Civil Disobedience is the first transgression, making Politicized Hacking the second transgression and Resistance to Future War the third. Each succeeding transgression moves the stance toward the Internet infrastructure further away from the public sphere model and casts it more as conflicted territory bordering on a war zone. Where the former more discursive model is perhaps a manifestation of Habermas's Paris Salon, the later may have roots in the Boston Tea Party. 18

The realization and legitimization of the Internet infrastructure as a site for word and deed opens up new possibilities for Net politics, especially for those already predisposed to extraparliamentarian and direct action social movement tactics. In early 1998 a small group calling themselves the Electronic Disturbance Theater had been watching other people experimenting with early forms of virtual sit-ins. The group then created software called FloodNet and on a number of occasions has invited mass participation in its virtual sit-ins against the Mexican government. 19

EDT members Carmin Karasic and Brett Stalbaum created FloodNet to direct a "symbolic gesture" against an opponent's web site. FloodNet is a Web-based Java applet that repeatedly sends browser reload commands.20 In theory, when enough EDT participants are simultaneously pointing the FloodNet URL toward an opponent site, a critical mass prevents further entry. Actually, this has been rarely attained. Given this, perhaps FloodNet's power lies more in the simulated threat.

On September 9, 1998, EDT exhibited its SWARM project21 at the Ars Electronic Festival on Information Warfare, where it launched a three-pronged FloodNet disturbance against web sites of the Mexican presidency, the Frankfurt Stock Exchange, and the Pentagon, to demonstrate international support for the Zapatistas, against the Mexican government, against the U.S. military, and against a symbol of international capital.22

But within several hours of activating project SWARM, FloodNet was disabled. On web browsers Java coffee cups streamed quickly across the bottom of the screen and FloodNet froze. Participants began to send email with word of trouble. Later that day a Wired writer learned from a Department of Defense spokesperson that the DOD had taken some steps against FloodNet. At the same time, an EDT co-founder received email that the Defense Information Systems Agency had complained about his ECD web site content.23

Globally, 20,000 connected to the FloodNet browser on September 9 and 10. This action reverberated through European media. It was later picked up by Wired, ZDTV, Defense News, and National Public Radio, among others. On

October 31, EDT made the front page of the New York Times. The story continued to unfold. More interest from the media sphere. On November 22, EDT called for FloodNet against the School of the Americas.24 As part of EDT's grande finale for the 1998 season, the group plans to release a public version of FloodNet at 12:01 a.m. on January 1, 1999.

Politicized Hacking

Again mentioning Mexico, in addition to the Electronic Civil Disobedience style action directed at the surface, at the web site entranceway, there have also been in 1998 actually hacks into Mexican government web sites where political messages have been added to those sites. 25 This particular tactic of accessing and altering web sites seems to have been the popular tactic for this year. Probably one of the most well known examples of this is the story of the young British hacker named "JF" who hacked into around 300 web sites world wide and placed anti-nuclear imagery and text. This method has been tried by a number of groups. October issues of the Ottawa Citizen and the New York Times did a decent job of capturing a number of these examples as they described this new trend. 26

One main distinction between most Politicized Hacking and the type of Electronic Civil Disobedience just mentioned is that while ECD actors don’t hide their names, operating freely and above board, most political hacks are done by people who wish to remain anonymous. It is also likely political hacks are done by individuals rather than by specific groups.

One of the reasons for the anonymity and secrecy is that the stakes are higher. Where proponents of forms of electronic civil disobedience actions are perhaps in an ambiguous area of law, certain types of political hacks, used to varying degrees of success, are unquestionably illegal. Few will question the legality of actually entering into an opponent's computer and adding or changing HTML code.

This distinction speaks to a different style of organization. Because of the more secret, private, low key, and anonymous nature of the politicized hacks, this type of activity expresses a different kind of politics. It is not the politics of mobilization, nor the politics that requires mass participation. This is said not to pass judgement, but to illuminate that there are several important forms of direct action Net politics already being shaped.

As touched on already, depending on the conception of politics, politicized hacking is either a recent phenomena or one that can be traced back to hacking's origins. For the purposes of creating a portal to look into this world of extraparliamentarian direct action Net politics, it may be useful to consider both perspectives. There is clearly something political about early hackers' desires to make information free. It probably would be useful to examine the history of early to mid 1980s hacking to look for more political origins of today's hacktivism. The computerized activism of the mid to late 1980s existed alongside the first generation of hackers. There may have been cross-over then.

The contemporary conception of hacktivism seems to concern itself more with overtly political hacking. It is such a recent development that journalists have only barely begun to discover it, while scholars have had little time to consider it. There are numerous web sites devoted to hacking, but very few are devoted to Hacktivism per se. Although, one web site devoted to Hacktivism was created in the fall of 1998 by a group called The Cult of the Dead Cow. 27

An important fact to realize and emphasize is that hacktivism, current forms of politicized hacking, is very much in its infancy. It is too early to draw definitive conclusions or to make strong predictions as to the direction it will take. Perhaps we can point to certain trajectories and make some logical projections. But we need to remember that at this point there is no consensus or agreement. Maybe the entire notion of hacktivism confuses and challenges sets of values and hacker codes of ethics. Quite possibly there is some re-thinking happening and we might begin to see a new set of ethical codes for hacking.28

Resistance to Future War

Some call the 1990-1991 Gulf War the first Information War because of the heavy military reliance on information and communication technology. The Gulf War was a pinnacle of achievement for the weapons industry, a chance to battle test sophisticated hardware that had been developed and manufactured under the Reagan and Bush presidencies. The weapons systems were dependent, as were all communications, on a major telecommunications infrastructure involving satellite, radar, radio, and telephone. The "smart" bombs were just the most mentioned of the sophisticated weaponry that was showcased during the made-for-CNN war.

Although significantly under-reported by mainstream U.S. media, there was sizeable domestic opposition to the Gulf War, both prior to and especially during the first days of U.S. bombing of Iraq. In San Francisco, the first three days of the Gulf War are referred to as the Three Days of Rage. During that period, demonstrators filled, occupied, and controlled the streets and in some cases bridges and highways in the greater San Francisco Bay Area. Similar disruptions happened up and down the west coast and all across the country. There was widespread grassroots resistance to the U.S. bombardment of Iraq in January 1991.29

One part of that history is the role of information and communication technology, not just for the military forces, but also for the grassroots resistance. If the Gulf War is indicative of a paradigmatic shift toward the practice of Information Warfare, then it's also useful to look at the way in which ICT enabled resistance to the war effort. Some people within the opposition to the 1990-1991 Gulf War used email to communicate and they learned about resistance in other cities through Bulletin Board Systems and newsgroups. Others without computer access used fax and telephone. But many people had no connection to computers and received nothing by fax,

instead they came out into the streets because of seeing posters or by hearing announcements on TV or on radio, or through word of mouth. It is safe to say that the Internet played only a marginal role in spreading news and moving people into action. The opposition to the war also watched CNN just like everyone else.

But that was the end of 1990 and the very beginning of 1991, 8 years ago at the time of this writing, and in a pre-Web phase and even pre-Internet phase. Yes, by then the PC revolution had exploded and more and more people were buying modems, but the Gulf War is clearly positioned in the pre-boom days of the Internet in the United States. An interesting question is what would happen today, or moreover, what might happen tomorrow or in the near future, if presented with a similar set of circumstances. What if, for example, a Gulf War-like scenario emerged at the end of the year 2000 and the beginning of 2001? Suppose the United States decided to engage in what became an unpopular war, what might hacktivism look like in a condition of more generalized resistance? Or said another way, what might generalized resistance look like with the condition of hacktivism?

The above is what is meant to be asked by suggesting that Resistance to Future War is the fifth portal into direct action Net politics. Where might this all lead? Until now, incidents of hacktivity have been sporadic and basically unconnected. Hacktivist events have been singular and not connected to a set of simultaneous occurrences. Perhaps the Electronic Disturbance Theater's work demonstrates the possibility of waging a campaign on the Internet, and sustaining a presence over a period of time. But the group's one goal of a SWARM has yet to be achieved. Maybe it is useful to think of the SWARM metaphor in the consideration of Resistance to Future War.

Perhaps a SWARM is a convergence of generalized resistance, referring to a situation in which there are not just isolated cases, or several pockets of opposition, but when there is across-the-board resistance occurring at a number of different levels and happening in cities and towns all across the country, all at the same time. Such was the case during moments of domestic Gulf War resistance. There was a simultaneous outpouring of people into the streets who engaged in quite a range of activity, both legal and illegal. A multitude of tactics were being used at the same time but without any central command or directing orders from above. Incidents of such upsurge are rare, but they undoubtedly will occur again. What will hacktivism look like then? What of it when hacktivism moves from isolated incidents to a convergence of allied forces? Is this when hacktivism ceases to be and becomes cyberspacial resistance? While it may be too early to make accurate predictions, it seems true that the force or power of hacktivism has yet to be fully recognized or tested. Yet before getting lost in futuristic science fiction, consider some critiques.

Emerging Critiques of Direct Action Net Politics

There is no consensus among social and political activists regarding electronic civil disobedience, political hacking, hacktivism, or more generally

extraparliamentarian direct action Net politics. It may in fact be too early to judge or to make definitive claims about these new tactics, but some critiques have co-developed along with the development of these new methods. They point to some basic questions over the effectiveness and appropriateness of these forms of electronic action.

In an emerging discourse on several email listservs, that is too complicated to treat fairly in such a short piece as this one, there have been periodic criticisms raised both generally and specifically about aspects of the above mentioned tactics.30 By no means can this piece attempt to describe and comment on all criticisms being raised about hacktivism et al, but it can at least address several of the criticism raised that seem most important. As already stated there are critiques aimed at the effectiveness and the appropriateness of cyber-protests. In terms of effectiveness, three closely related types of questions have appeared regarding political, tactical, and technical effectiveness. Concerning appropriateness there are ethical questions, that may be also considered as political questions, and of course there are legal questions. Some of the legal concerns raise issues of enforceability and prosecuteability.

Political and tactical effectiveness are closely intertwined. Are these methods of computerized activism effective? The answer to which is, that it depends on how effectiveness is defined. What is effective? If the desired goal of hacktivism is to draw attention to particular issues by engaging in actions that are unusual and will attract some degree of media coverage, then effectiveness can be seen as being high. If, however, effectiveness is measured in terms of assessing the actions ability to be a catalyst for fomenting a more profound mobilization of people, then probably these new techniques are not effective. This distinction then, perhaps, is important. Hacktivism is not likely to be an organizing tool and the end result of hacktivity is not likely to be an increase in the ranks of the disaffected. Rather hacktivism appears to be a means to augment or supplement existing organizing efforts, a way to make some noise and focus attention.

Technical critiques of hacktivism at the level of computer code are another way of addressing the efficacy of these new methods. Undoubtedly there will be disagreement as to how effective a particular technique is or isn't. But it seems that if new methods are created in an environment of experimentation, then valid critiques will be taken into consideration and used to redesign or alter plans and strategies. However, there are some technical critiques that are actually much more ideologically based than it would first seem. For example there is a certain tendency to reify bandwidth and from that viewpoint any action that clogs or diminishes bandwidth is considered negative. So then, technical critiques can be value-laden with particular stances toward the Internet infrastructure.

Despite the current levels of political, tactical, and technical questions that are being raised about hacktivism et al, it seems to be an area that is in a period of expansion, rather than contraction. And it generally seems that this critique and questioning is healthy and useful for the refinement of the practice.

As just mentioned, some technical critiques are bound together with ideological pre-dispositions and are therefore also political questions, and perhaps even ethical questions of appropriateness. To judge blocking a web site, or clogging the pipelines leading up to a web site, is to take an ethical position. If the judgement goes against such activity, such an ethical position is likely to be derived from an ethical code that values free and open access to information. But there are alternative sets of values that justifies, for example, the blocking of access to web sites. These differences in beliefs over the nature of the Internet infrastructure are among people who are basically on the same side when it comes to most political questions. Some of these differences will probably be worked out as the subject and practice matures, while there may remain clear divisions.

Last but not least, the more prosecutorial minded are apt to pass judgement on the appropriateness or inappropriateness of certain forms of hacktivism based on where the actions stand with respect to the law. While it is true that some forms of hacktivity are fairly easy to see as being outside the bounds of law - such as entering into systems to destroy data - there are other forms that are more ambiguous and hover much closer to the boundary between the legal and the illegal. Coupled with this ambiguity are other factors that tend to cloud the enforceability or prosecuteability of particular hacktivist offenses. Jurisdictional factors are key here. The nature of cyberspace is extraterritorial. People can easily act across geographic political borders, as those borders do not show themselves in the terrain. Law enforcement is still bound to particular geographic zones. So there is a conflict between the new capabilities of political actors and the old system to which the law is still attached. This is already beginning to change and legal frameworks, at the international level, will be mapped on to cyberspace.

This section does not do justice to the full range of critiques that can be identified and described, and further exploration of the subject of direct action Net politics should make sure such a deeper analysis is taken. The intention here has been more so to develop a greater understanding of these new forms of electronic action and to only mention a few overarching critiques so as to not give the impression that this is moving forward without resistance. Quite the contrary is true. It seems that hacktivity has met and will meet resistance from many quarters. It doesn't seem as if opposition to hacktivist ideas and practices falls along particular ideological lines either.

Conclusion

Several things seem to be clear at this point. The first is that hacktivism, as defined across the full spectrum from relatively harmless computerized activism to potentially dangerous resistance to future war, is a phenomena that is on the rise. Second, as just eluded to, hacktivism represents a spectrum of possibilities that exists in some combination of word and deed. On the one end of the spectrum is pure word. On the other end of the spectrum is pure deed. Computerized activism hovers closer to pure word, while the successive portals moves closer toward pure deed. Third, along with

this tendency towards transgression, towards giving value to actions that move beyond words and that sees the Internet infrastructure also as a site for action, there comes with this a critique and resistance. Despite this critique hacktivism is likely to continue to spread, but perhaps modified to accommodate some of the criticism. Fourth, with its continued spread, modified by critique or not, hacktivism is also likely to continue to gain attention. While media coverage may eventually drop off if or when hacktivism becomes more commonplace, at this point the way in which hacktivism is being represented is still new enough to warrant media attention for the foreseeable near future.

What remains unclear about hacktivism emerges when we start to ask questions like: what does this mean and where is this going? While we can claim with a fair degree of certainty that hacktivism is on the rise, there is little way to tell where it will lead to and the significance or lack there of that it will or might obtain. Moreover, there are aspects of hacktivism that still need to be explored. For example, the entire issue of extraterritoriality, of the Internet not being bound to any particular geographic region and the difficulties that poses for law enforcement, is one area that deserves further attention.

One reason why it is difficult to get a firm grip on hacktivism's direction, in addition to simply saying that it is too early to tell, is that hacktivism will evolve in response to changing global economic and political conditions. As it is hard to predict trends and directions in the global economy, it too, then, becomes hard to predict events that will be linked to those meta shifts.

Nevertheless, some people are trying to understand and make sense out of where hacktivism could go, although they might not be doing so using the particular word 'hacktivism' to describe this activity. Governments and corporations are keenly concerned, for example, about network security. To get some indications about the forecast for hacktivism in the 21st century it may be very useful to examine what these sorts of institutions are saying and how they are preparing to defend themselves.

It could very well be that governments might impose severe regimes that successfully curtail hacktivism. If so, 1998 might be seen at some point as the glory days, when hacktivist experiments were able to go largely unchallenged, because the mechanisms of the state had not yet been in place to deal with the new phenomena. Or it could be that hacktivism is able to successfully remain several steps out in front of law enforcement efforts, or that too many people become involved that enforceability remains problematic. Again, it is difficult to know any of this.

Finally, while we can speak with some clarity about facets of hacktivism and also point to aspects of it that remain ambiguous and unforeseen, there is an overarching concern that comes from this discussion that deserves more attention. Specifically arising out of the consideration of the fifth portal, Resistance to Future War, what are the long term consequences posed for governments and states if individuals, non-state actors, can engage in forms of cyberspacial resistance across traditional geo-political borders? This is an

important question raised by this discussion and one that demands more attention to answer properly. But it seems clear already that we are at the onset of a new way of thinking about, participating in, and resisting war, and that today's nascent hacktivity is part of the trajectory towards that new way.

Footnotes

1. Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web," New York Times, 31 October 1998, sec. A1; Same in Carmin Karasic scrapbook (http://custwww.xensei.com/users/carmin/scrapbook/nyt103198/31hack.html)
2. John D. H Downing, "Computers for Political Change: PeaceNet and Public Data Access," Journal of Communication 39, no. 3 (Summer 1989): 154-62.
3. Harry Cleaver, "The Zapatistas and the International Circulation of Struggle: Lessons Suggested and Problems Raised," Harry Cleaver homepage 1998 (http://www.eco.utexas.edu/faculty/Cleaver/lessons.html)
4. Kenneth L. Hacker, "Missing links in the evolution of electronic democratization," Media, Culture & Society 18, (1996): 213-32; Lewis A. Friedland, "Electronic democracy and the new citizenship," Media, Culture & Society 18, (1996): 185-212; John Street, "Remote Control? Politics, Technology and 'Electronic Democracy'," European Journal of Communication 12, no. 1 (1997): 27-42.
5. John D. H Downing, "Computers for Political Change: PeaceNet and Public Data Access," Journal of Communication 39, no. 3 (Summer 1989): 154-62.
6. Linda M. Harasim, ed., Global Networks: Computers and International Communication (Cambridge, Mass.: MIT Press 1993)
7. There are many protest web sites. Trying a search on keywords "protest" and "web site" and there will be thousands of hits.
8. John Arquilla and David Ronfeldt, "Cyberwar is Coming!," Comparative Strategy 12 (April-June 1993): 141-65.; (http://gopher.well.sf.ca.us:70/0/Military/cyberwar)
9. Cleaver, Harry "The Zapatistas and The Electronic Fabric of Struggle," Harry Cleaver homepage 1995 (http://www.eco.utexas.edu/faculty/Cleaver/zaps.html)
10. Gerfried Stocker and Christine Schopf, eds. InfoWar (Wien, Austria: Springer 1998); Ars Electronica Festival 1998 (http://www.aec.at/infowar)
11. Stefan Wray, "Towards Bottom-Up Information Warfare: Theory and Practice: Version 1.0," Electronic Civil Disobedience Archive 1998 (http://www.nyu.edu/projects/wray/BottomUp.html) 12. Stefan Wray, "The Drug War and Information Warfare in Mexico," Masters Thesis, University of Texas at Austin, Electronic Civil Disobedience Archive 1997 (http://www.nyu.edu/projects/wray/masters.html)
13. La Jornada (http://serpiente.dgsca.unam.mx/jornada/index.html)
14. Harry Cleaver, "Zapatistas in Cyberspace: An Accion Zapatista Report," Harry Cleaver homepage 1998 (http://www.eco.utexas.edu/faculty/Cleaver/zapsincyber.html)
15. No specific reference to this fact. But it is a matter of record.

16. Stefan Wray, "On Electronic Civil Disobedience," Peace Review 11, no. 1, (1999), forthcoming; Electronic Civil Disobedience archive 1998 (http://www.nyu.edu/projects/wray/oecd.html)
17. Critical Art Ensemble, The Electronic Disturbance (Brooklyn, NY: Autonomedia 1994); Critical Art Ensemble, Electronic Civil Disobedience and Other Unpopular Ideas (Brooklyn, NY: Autonomedia 1996); Critical Art Ensemble homepage (http://mailer.fsu.edu/~sbarnes/)
18. Stefan Wray, "Paris Salon or Boston Tea Party? Recasting Electronic Democracy, A View from Amsterdam," Electronic Civil Disobedience archive 1998 (http://www.nyu.edu/projects/wray/teaparty.html)
19. Electronic Disturbance Theater homepage (http://www.thng.net/~rdom/ecd/ecd.html)
20. Brett Stalbaum, "The Zapatista Tactical FloodNet," Electronic Civil Disobedience Web Page 1998 (http://www.nyu.edu/projects/wray/ZapTactFlood.html)
21. Ricardo Dominguez, "SWARM: An ECD Project for Ars Electronica Festival '98," Ricardo Dominguez homepage 1998 (http://www.thing.net/~rdom/)
22. Electronic Disturbance Theater, "Chronology of SWARM," (http://www.nyu.edu/projects/wray/CHRON.html)
23. "Email Message From DISA to NYU Computer Security," Electronic Civil Disobedience homepage (http://www.nyu.edu/projects/wray/memo.html)
24. Electronic Disturbance Theater's call for Electronic Civil Disobedience on November 22, 1998 (http://www.thing.net/~rdom/ecd/November22.html); (http://www.thing.net/~rdom/ecd/block.html)
25. "Mexico rebel supporters hack government home page," Reuters, 4 February 1998; Same in Electronic Civil Disobedience homepage (http://www.nyu.edu/projects/wray/real.html)
26. Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web," New York Times, 31 October 1998, sec. A1; Same in Carmin Karasic scrapbook (http://custwww.xensei.com/users/carmin/scrapbook/nyt103198/31hack.html); Bob Paquin, "E-Guerrillas in the mist," The Ottawa Citizen, 26 October 1998 (http://www.ottawacitizen.com/hightech/981026/1964496.html)
27. Hacktivism web page (http://www.hacktivism.org); Cult of the Dead Cow homepage (http://www.cultdeadcow.com/)
28. While it is possible to point to certain early hacker ethical codes that, for example, privilege free and open access to all, there is not a monolithic hacker's perspective. Nevertheless, some whom call themselves hackers have criticized the FloodNet project because one of the things they allege it does is block bandwidth. This view can be said to be a digitally correct position.
29. The author knows about grassroots resistance to the 1990/1991 Gulf War because he was involved in anti-war organizing and action in the San Francisco Bay Area during this period.
30.Some of these listservs include: nyfma@tao.ca, damn-org@tao.ca, media-l@tao.ca, accion-zapatista@mcfeeley.cc.utexas.edu