What Is Hacktivism? 2.0

by metac0m (December 2003)

Hacktivism is the fusion of hacking and activism; politics and technology. More specifically, hacktivism is described as hacking for a political cause. In this context, the term hacker is used in reference to its original meaning. As defined in the New Hacker's Dictionary, a hacker is "a person who enjoys exploring the details of programmable systems and how to stretch their capabilities" and one who is capable of "creatively overcoming or circumventing limitations". (1) Activism is defined as "a policy of taking direct and militant action to achieve a political or social goal". (2) Therefore, a clinical definition of hacktivism is:

> Hacktivism: a policy of hacking, phreaking or creating technology to achieve a political or social goal.(3)

However, both hacking and activism, and thus hacktivism, are loaded words ripe for a variety of interpretation. Therefore it is preferable not to clinically define hacktivism but rather to describe the spirit of hacktivism. Hacktivism is root. It is the use of one's collective or individual ingenuity to circumvent limitations, to hack clever solutions to complex problems using computer and Internet technology. Hacktivism is a continually evolving and open process; its tactics and methodology are not static. In this sense no one owns hacktivism - it has no prophet, no gospel and no canonized literature. Hacktivism is a rhizomic, open-source phenomenon.

In the Beginning...
Since hacktivism is a recombinant initiative comprised of two divergent communities (hackers and activists) it is necessary to understand their respective backgrounds in order to analyze this historic merger and to examine its challenges and future capabilities. "Hacker" was originally a term that encapsulated an individual's deep understanding of computer systems and networks and the ability to invent, modify, and refine such systems. It is a recombinant attitude that promotes problem solving and creative instinct for it does not limit one's options to the possible. Hacking thrives in an environment in which information is freely accessible. The hacker ethic formulated by Steven Levy in his 1984 book "Hackers: Heroes of the Computer Revolution" outlines the hacker tenets:

> 1. Access to computers should be unlimited and total.
> 2. All information should be free.
> 3. Mistrust authority - promote decentralization.
> 4. Hackers should be judged by their hacking not bogus criteria such as degrees, age, race, or position.
> 5. You create art and beauty on a computer.
> 6. Computers can change your life for the better. (4)

The GNU/Linux operating system evolved from this hacker ethic. As fellow hackers from the MIT AI lab were lured into commercial ventures Richard Stallman became increasingly concerned about the decay of the hacker community and the increasing control being exerted over proprietary code. Stallman decided to create a free operating system modeled after the proprietary UNIX system.(5) Linus Torvalds began development on a kernel and released the initial source code for his kernel, named Linux.(6) Together the work of Stallman and Linus form the GNU/Linux operating system. This software is released under the General Public License (GPL), which is known as "copyleft" as opposed to copyright. The GPL allows users to modify and copy the software as long as they make the source freely available to others.(7) There is now a vibrant global, open source community that thrives based on the free flow, and sharing of information.

Hackers abhor censorship. Censorship is often seen as a human rights violation, especially when it is combined with a repressive, governing regime. In addition, hackers mistrust restrictive legislation that encroaches on free access to information and cherished electronic privacy. Thus a natural aversion to repressive governments and predatory, private institutions has developed. In Phrack magazine, Dr. Crash explains that computer technology is being misused not by hackers but by governments and corporations:

> The wonderful device meant to enrich life has become a weapon which dehumanizes people. To the government and large businesses, people are no more than disk space, and the government doesn't use computers to arrange aid for the poor, but to control nuclear death weapons. (8)

This sentiment is not an isolated rant. There is definitely a trend within hacker culture that not only focuses on technical aspects of computing but political aspects as well. In the "Hacker's Manifesto" the ment0r explains:

> We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. (9)

There is an antagonism between government/corporate restrictions and domination of computer technology and hackers who want to ensure free access to information, to circumvent censorship, and to prevent monopoly control of technology.

Activists recognized the benefits of integrating activism and computer/Internet technology relatively quickly. The new open architecture technology of the Internet played a complementary and beneficial role that fit perfectly with existing, decentralized, activist networks. In fact, computerized activism was already taking place before the birth of the WWWeb. Stephan Wray notes that the creation of PeaceNet, a text-based newsgroup service, in 1986 allowed "political activists to communicate with one another across international borders with relative ease and speed." (10) This has allowed activists with little or no technical skills to utilize the benefits of digital communications. The Internet allows for the convergence of meetings, debates, and research in one convenient and fast medium that greatly enhances not only activists' organizational capabilities but also the ability of activists to react to a constantly changing world in a timely manner. In order to educate the public and promote causes and campaigns, activist organizations have utilized the Internet and established an accessible,

updateable, interactive, and international presence that previously would have been difficult if not nearly impossible to maintain.

Applied Hacktivism

Hacktivism is the fusion of the evolution of computer activism with the politicization of the hackers. The evolutionary progress of both communities has put them in a position where they can compliment each other because they face the same techno-political opposition: the repressive use of laws and technologies by private corporations and governments to increasingly monitor and control the Internet. The emergence of techno-politics has emboldened each community and provides a conduit for electronic activism. Oxblood Ruffin of the cDc explains:

> Hacktivism forges conscience with technology and girds us against the disagreeable nature of conflict. It allows us to mount better arguments, rally unseen allies, and take on any tyranny. (11)

The actualization of politicized hacking has taken a variety of forms ranging from electronic civil disobedience to circumventing limitations through technology development and implementation. However, there is major objection to and contestation of the motivation and methodology of activities that are often described as hacktivism. As with the hacker/cracker dichotomy many distinguish between hacktivism and "cracktivism". The former is used to describe politically motivated hacking that is constructive and the latter disruptive. Cracking is defined as "the act of breaking into a computer system" (12) and when such acts are carried out for an explicit political purpose they are often described as hacktivism. But hacktivism is fluid and its focus and expression has evolved over time. To avoid "definition confusion", it is better to analyze specific situations contextually and examine the goals, methods, results. Events often described as hacktivism have been classified as: cracking (including defacement and denial of service), virtual sit-ins, and technology development.

Unauthorized access, defacement and DoS comprise "cracktivism" and should be examined with particular scrutiny since instances of unauthorized access and network disruption are prominently featured in the current sensationalized media climate. Such attacks are often labeled by the media as "hacktivism" despite there being a clear lack of political significance and little if any creative, technological proficiency involved in the attack. Moreover, they are labeled as such despite the fact that the perpetrators themselves, along with the hacktivist community, rarely describe such events as hacktivism. In 1998 there were several targeted events in which computer intrusion and defacement was used to protest injustice.

- Milw0rm broke into computer systems at India's Bhabha Atomic Research Centre, Bombay (BARC) in a protest against nuclear weapons tests. (http://www.wired.com/news/technology/0,1282,12717,00.html)
- LoU members Bronc Buster and Zyklon disabled firewalls in order to allow China's Internet users uncensored access to the Internet. (http://www.wired.com/news/print/0,1294,16545,00.html)
- X-Ploit defaced the websites of Mexico's Finance Ministry and Health Ministry to protest the government of President Ernesto Zedillo and to show solidarity with the Zapatista rebellion. (http://thehacktivist.com/archive/news/1998/MexicanHackers-Reuters-1998.pdf)
- Kaotik Team defaced 45 Indonesian Websites to include messages calling for full autonomy for East Timor. (http://thehacktivist.com/archive/news/1998/E-Guerrilas-OttawaCitizen-1998.pdf)

Defacement, despite being the most commonly cited hacktivist tactic in the media, is not considered hacktivism just because of some vague message that, when interpreted as political, suddenly makes a defacement hacktivism instead of just another defacement. Hacktivism must have a level of intentionally that the overwhelming majority of defacements don't have. A defacement itself is not hacktivism. Kevin Poulsen distinguishes between vandalism and hacktivism:

> Vandalism is malicious destruction or damage, not artful and subversive tampering. The proof for protest is in the quality of the work, the clarity of the message, and the motives behind it. (13)

When random websites are defaced – websites that have no connection to the supposed issue of protest – it is not hacktivism. Defacements began to drastically increase in 2000 dues to general lax security and the dissemination of exploits for Microsoft IIS server, most notably the Unicode Directory Traversal Vulnerability which allowed defacements to be conducted through a web browser – as easily as you would visit a URL (14). This resulted in a focus on apolitical high profile defacements leaving defacement as a method to attract attention to a political cause and as a mechanism of protest overshadowed and spent.

Although some politically motivated defacements do continue to take place they are considered an anachronism by many hacktivists and fail to affect political change or even draw attention to a political cause. Unlike the defacements of 1998, contemporary "political" defacements are often the result of ongoing feuds between defacement groups. Embedded within a nationalist discourse, the taunts between opposing defacers are interpreted as politically motivated "cyberwars" and enflamed by sensationalist media reporting. In a widely cited example that occurred in 2001, a "cyberwar" erupted after a U.S. spy plane was shot down in China. However, as Attrition.org discovered, it was more a case of "self-fulfilling prophecy" – defacers who had not shown any political motivations suddenly became political only after the media interpreted their defacements as political. Instead of being a "cyberwar", Attrition.org describes the event as "the collective dick-waving of a bunch of script-kidiots fueled by so-called journalists generating media hype - the former trying to feed their egos and the latter to feed their hit counts." (15)

It has been suggested that viruses and worms are used by hacktivists to promote political messages. The only well documented event occurred in 1989 when a political worm known as WANK targeted the HEPnet and the NASA SPAN networks to protest the development of nuclear weapons (16). There have been few politically motivated viruses and worms since WANK. The few which have been identified as political include:

- Mawanella : A virus that appeared in 2001 describing the burning down of two mosques and one hundred Muslim-owned shops in Mawanella. (http://www.sophos.com/virusinfo/articles/mawanella.html)
- Injustice: A worm that appeared in 2001 protesting the killing of 12 year old Palestinian child Mohammad Al-Durra.

(http://www.sophos.com/virusinfo/articles/injusti.html)

- Vote-A: A 2001 worm that calls for a vote on whether America should go to war. (http://www.sophos.com/virusinfo/analyses/w32vote-a.html)
- Yaha-E: A 2002 worm that attempts a denial of service attack on a Pakistani government's website. (http://www.sophos.com/virusinfo/articles/yahae3.html)

It is important to note that the anti-virus form Symantec current has a growing database of over 65000 viruses and worms of which few contain any content that could be interpreted as political. However, the self-serving interests of security firms have led them into exaggerating the existence of political viruses and worms. For example, the text of the Yaha-E worm is simply several lines of misspelled taunts directed at a rival defacement group – a message that is hardly political. The fact is that viruses and worms are infrequently associated with political purposes. The development and use viruses or worms is not broadly accepted within the hacktivist community – in fact most oppose it.

Electronic Civil Disobedience (ECD) is a legitimate form of non-violent, direct action utilized in order to bring pressure on institutions engaged in unethical or criminal actions. Within the electronic environment, ECD aims to disrupt the operation of information and capital flows of carefully selected target sites without causing serious damage. Currently based on, but not limited to, the tactical use of blockade and trespass, ECD acts as a mechanism through which "the value system of the state (to which information is of higher value than the individual) is inverted, placing information back in the service of people rather than using it to benefit institutions." (17) The actualization of ECD in this regard has been an attempt to blockade electronic targets through mass participation. Stefan Wray explains:

> 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. 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. 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. (18)

It should be noted that a Mexican organization, Ame La Paz, while supportive of the concept issued a statement critical of the EDT's action:

> We also think your Electronic Civil Disobedience on April is a brilliant, intelligent and well-planned proposal, but it is unnecessary and dangerous. (19)

Ame La Paz stated that not only had the EDT failed to consult with Mexican organizations they also did not consult with the Zapatistas. Furthermore, Ame La Paz suggested that such actions may lead to increasing confrontation and the escalation of hostilities in cyberspace. There have been other such critiques of electronic civil disobedience from within the activist community. (20)

The etoy story of 1999/2000 is a tale starring the European art collective etoy.com and Internet toy giant eToys.com. etoy is a dynamic artwork that "uses the corporate structure to maximize cultural value" in order to explore the problems of globalization. (21) After etoy turned down an offer by eToys to buy the domain name etoy.com, eToys sought and won a temporary court injunction denying etoy the use of the domain etoy.com despite the fact that etoy.com had been registered before the eToys Corporation had even existed. The reasoning was that etoy.com was confusingly similar to etoys.com Not content to quit, supporters of etoy, most notably RTMark began a campaign, a toy war, designed not only to diminish the value of eToys stock to create a precedent that "would force e-commerce companies in the future to think twice about censorship for financial profit." (22)

A Virtual Sit-In was organized to span the prime shopping days of Dec. 15-25 and publicity campaigns targeted eToys investment boards all of which had an impact on the stock price of eToys. In fact the stock began to drop the day the protests began. eToys eventually drop their claim and etoy regained control of the etoy.com domain with eToys picking up the legal costs. (23)

Another major ECD action, one which introduced the concept of synchronized electronic and street based protest, was initiated by the electrohippies collective to coincide with the 1999 street demonstrations in Seattle, Washington against the meeting of the World Trade Organization. They argue that by coordinating street and Internet based protest the interests of the public are furthered. The web, they argue, is not separate from the street:

> Therefore, we must find mechanisms for lobbying and protest in cyberspace to complement those normally used in real life. Without public pressure cyberspace will have no moral or normative controls to control the excesses of politicians, groups or corporations who would seek to dominate that public space. (24)

The action was conducted "To provide a mechanism for ordinary people, who cannot get to Seattle, to register a protest that may have the impact equivalent to actually being there in person" (25) by slowing or blocking access to the WTO's servers.

- 1998 Mexico: Protest against the Mexican government's escalating war against the Zapatistas and other indigenous people in Chiapas. (http://www.thing.net/~rdom/ecd/April10.html, http://www.wired.com/news/politics/0,1283,14931,00.html)
- 1999 WTO: Protest against the policies of the World Trade organization in conjunction with massive street protests in Seattle. (http://news.bbc.co.uk/1/hi/uk/543752.stm)
- 99/00 etoy: Protest against censorship for financial profit after the usurping of the etoy domain name. (http://www.heise.de/tp/english/inhalt/te/5843/1.html)
- 2000 Worldbank: Protest against World Bank policies in conjunction with street based protests in

Prague. (http://www.villagevoice.com/issues/0042/ferguson.php)

- 2001 FTAA: Protest against the proposed FTAA agreement in conjunction with street based protests in Quebec City. (http://news.zdnet.co.uk/internet/0,39020369,2085755,00.htm)
- 2002 WEF: Protest against corporate globalization and the World Economic Forum. (http://security.itworld.com/4339/020201wefdown/page_1.html)

The virtual sit-in, or client-side DDOS, differs from server-side DDOS since "client-side distributed actions require the efforts of real people, taking part in their thousands simultaneously" while the latter requires the cracking of computers to use as zombies in an automated DDOS attack. Attrition.org's Brian Martin explains server-side DDOS:

> Prior to launching this form of DDoS flood, the attacker must first compromise various hosts on different networks. The more networks and machines used as launch points, the more potent the attack. Once each host had been broken into, they would install a DDoS client program on the machine that would sit ready to attack. Once the network of compromised servers was configured with the new client program, the attacker could send a quick command from the DDoS server software triggering each machine to launch an attack. (26)

Others within the hacker/hacktivist fervently oppose the tactic of the virtual sit-in suggesting that there is no difference between a virtual sit-in and a DDOS attack. In a response to the electrohippies, Oxblood Ruffin of cDc/Hacktivismo explains:

> Denial of Service, is Denial of Service, is Denial of Service, period. The only difference between a program like Stacheldraht [a DDoS application written by The Mixter] and the client side javascript program written by the Electrohippies is the difference between blowing something up and being pecked to death by a duck. (27)

Hacktivism is not strictly the importation of activist techniques into the digital realm. Rather it is the expression of hacker skills in the form of electronic direct action. It acknowledges that neither the tactics nor the objectives of hacktivism are static. Rather, they must continually evolve in order to be effective. Thus a distinction is made between hackers engaged in activism and activists attempting utilize the technical aspects of hacking to mimic and rationalize traditional forms of activism. This sentiment is summed up by Oxblood Ruffin of cDc/Hacktivismo:

> Hacktivism is about using more eloquent arguments - whether of code or words - to construct a more perfect system. One does not become a hacktivist merely by inserting an "h" in front of the word activist or by looking backward to paradigms associated with industrial organization. (28)

Disruption (whether by computer break-ins, defacement or denial of service), in this regard, is not viable option. In fact it is condemned. Oxblood explains:

> Many on-line activists claim to be hacktivists, but their tactics are often at odds with what we consider hacktivism to be. From the cDc's perspective, creation is good; destruction is bad. Hackers should promote the free flow of information, and causing anything to disrupt, prevent, or retard that flow is improper. For instance, cDc does not consider Web defacements or Denial of Service (DoS) attacks to be legitimate hacktivist actions. The former is nothing more than hi-tech vandalism, and the latter, an assault on free speech. (29)

Instead, it is argued that the focus of hacktivism should be shifted from electronic disruption to problem solution. Oxblood Ruffin explains:

> Hacktivism is an open-source implosion. It takes the best of hacking culture, and the imperatives of the quantum community, and fuses a solution. (30)

Hacktivismo chooses to re-define hacktivism as "using technology to advance human rights through electronic media."(31) Re-focusing on the initial hacker ethic, hacktivists seek creative solutions that circumvent limitations in code. If, as Lawrence Lessig suggests, "code is law" (32) then code itself is the primary location of struggle. Despite being heralded as a democratizing technology by virtue of its decentralized, open-architecture design the Internet is increasingly coming under pressure by institutions, governments and corporations that seek to own and control it. The increasing penetration of draconian cyberlaw – including anti-(cyber)terrorism provisions as well as intellectual property law – combined with technological measures that restrict freedom of speech and expression online threaten the Internet both as a communications medium and as a means of activism.

Some hackers have been challenging restrictions to free speech and fair use rights in the courts. 2600 Magazine has been taken to court several times over such issues, most notably the DeCSS case. In Nov. 1999 Masters of Reverse Engineering (MoRE) released DeCSS, a program that allowed users to make copies of copy-protected DVD's. MoRE member Jon Johansen claimed they had released the code so that users could play DVD's on the Linux operating system. 2600 Magazine was sued by the MPAA for publishing the DeCSS source code. (33) Although 2600 decided not to appeal a ruling against them in the U.S. (34) Jon Johansen won his court case in Norway and has since released an open source utility that dumps the contents of a Quicktime stream drawing attention to fair use rights. (35)

Increasingly, activists and hacktivists are being criminalized and labeled as terrorists. Users, activists, and hackers alike face censorship and surveillance on the Internet. Thus hacktivists have begun to develop technologies aimed at empowering Internet users and activists with security and privacy enhancing tools. There are numerous ongoing hacktivist projects to develop technologies that would enable activists, citizens and civil society networks to secure themselves against, or work around, Internet censorship and surveillance. The scope of these technologies ranges from small, simple scripts and programs to highly developed peer-to-peer network protocols, and stegonography tools. The new collaborative hacktivist community Hackforge.net aims to bring together hackers and activists in an open source collaborative software development environment in

order to facilitate the continued development of hacktivist technologies.

Oscillating between creation and confrontation hacktivism is returning to its hacker roots. True to the hacker definition of "circumventing limitations" hacktivists have always focused on technology development, with a particular focus on ensuring freedom of speech on the Internet, although this aspect has often been ignored by the media and academics. Hacktivism is not simple pranksterism, nor is it malicious or destructive. It is not synonymous with defacements and DoS attacks. Hacktivism is a form of electronic direct action in which creative and critical thinking is fused with programming skill and code creating a new mechanism to achieve social and political change. Hacktivists are committed to securing the Internet as a platform of free speech and expression. This ensures that the Internet remains a medium for activism and an environment that facilitates the free flow of information.

What is Hacktivism? 1.0 can be found at:
http://www.thehacktivist.com/hacktivism1.php

Notes:

1. http://www.hack.gr/jargon/html/H/hacker.html

2. http://dictionary.reference.com/search?q=activism

3. This definition appeared on the CULT OF THE DEAD COW's now defunct website http://www.hacktivism.org which is archived here: http://web.archive.org/web/19981203083935/http://www.hacktivism.org/

4. http://mosaic.echonyc.com/~steven/hackers.html

5. http://www.gnu.org/gnu/thegnuproject.html

6. http://www.li.org/linuxhistory.php

7. http://www.gnu.org/copyleft/gpl.html

8. http://www.phrack.org/phrack/6/P06-03

9. http://www.phrack.org/phrack/14/P14-03

10. http://thehacktivist.com/archive/edt/wwwhack.html

11. http://www.hack.gr/jargon/html/C/cracking.html

12. http://www.securityfocus.com/bid/1806/info/

13. http://www.techtv.com/cybercrime/print/0,23102,2000216,00.html

14. http://www.attrition.org/mirror/attrition/defacements-graphs.html

15. http://www.attrition.org/security/commentary/cn-us-war.html

16. http://www.cert.org/advisories/CA-1989-04.html

17. http://www.critical-art.net/books/ecd/ecd2.pdf

18. http://thehacktivist.com/archive/edt/wwwhack.html

19. http://www.thing.net/~rdom/ecd/amelapaz.html

20. http://www.thing.net/~rdom/ecd/harrycontrib.html
http://www.nettime.org/Lists-Archives/nettime-l-9808/msg00028.html

21. http://www.etoy.com

22. http://www.rtmark.com/etoymain.html

23. http://www.wired.com/news/politics/0,1283,33111,00.html
http://www.wired.com/news/politics/0,1283,32936,00.html
http://www.rtmark.com/etoy.html

24. http://www.gn.apc.org/pmhp/ehippies/files/op1.htm

25. http://www.gn.apc.org/pmhp/ehippies/archive/wtoir.htm

26. http://www.attrition.org/~jericho/works/security/dos.html

27. http://www.cultdeadcow.com/details.php3?listing_id=410

28. http://www.cultdeadcow.com/details.php3?listing_id=410

29. http://hacktivismo.com/news/modules.php?name=Content&pa=showpage&pid=10

30. http://www.cultdeadcow.com/cDc_files/cDc-0361.html

31. http://hacktivismo.com/news/modules.php?name=Content&pa=showpage&pid=10

32. http://code-is-law.org/

33. http://www.theregister.co.uk/content/archive/23633.html

34. http://www.2600.com/news/view/article/1233

35. http://www.theregister.co.uk/content/4/34141.html