Marshall Massengill

English 101: Section 112

Emily Wicker

May 9, 2006

Project 2: Final Draft

Hackers

Hackers are often called cyberterrorists or high tech bank robbers by the mass media however disrupting telecommunications networks and stealing credit card numbers is not one of the cornerstones of hacker culture. Hacker culture is formed around one of the most basic human instincts, curiosity. This desire to explore and create has lead to great advances in the way people communicate and share ideas, such as the birth of the Internet. Scholars agree that the Internet has changed the way the world works and most agree that the Internet's purpose has become the widespread dispersion of information. With the spread of the Internet and cheap consumer electronics that have the ability to access the Internet, how has this hacker culture influenced the rest of the world through technology and the ideas of the hacker ethos?

In the course of this review I will dissect and compare essays from authors who attempt to analyze the hacker ethos, compare hacker culture to democratic societies, and examine the Internet's role in the organizing of grassroots-movements. The first part of this review is an analysis of what the hacker ethic is and how the different authors each approach the subject. Continuing on, I will review how each of the authors shows how the methods and technology developed by the hacker community have changed popular culture on an individual level. Lastly, I will compare how each of the authors views the hacker culture in a larger group sense, and in particular I will analyze how each of the authors views cyberactivism. In concluding this review I will explain my own thoughts on the subjects at hand and provide some personal experience that I have had with the hacker community.

The hacker ethic

Hackers used to be stereotyped as nerdy teenagers who would sit at home in their parent's basements and tie up the phone lines for hours on end just so they could be connected to similar teenagers in other parts of the world. However, these same hackers have now taken jobs at some of the largest global corporations and are spreading the hacker ethos. At the heart of what defines a hacker is the basic human desire to create, explore, and control. Bryan Warnick, the author of "Technological metaphors and moral education: The hacker ethic and the computational experience", writes "The experience of the computer epitomizes the technological theme of achieving control" (Warnick, 2004, p. 273). Warnick is stating that one of the reasons why hackers are so drawn to computers is the thrill of having control over something. This sentiment is echoed by Olga Skordodumova in her article called "Hackers as information space phenomenon." Skordodumova describes a hacker as a "user performing actions directed at an unauthorized software or data usage" (Skordodumova, 2004, p. 107). Skordodumova is claiming that a hacker is someone who comes up with new uses for data or software. In other words, a hacker is someone who invents. Thus far the characteristics of a hacker seem to be a want to control and create. This leaves the human instinct of curiosity.

Hackers have a desire to control and create and it is much easier to control and create when full, unrestricted access is available. Warnick makes a point of explaining the Open Source movement. In summary, most software is based around the idea that a company keeps the source code, the code that makes up the program, closed to the eyes of the public. This is in stark contrast to the fundamental principal behind the Open Source movement, a movement that many proclaimed hackers are a part of. This desire for information and resources is really just an echo of the human instinct of curiosity. Warnick does a superb job of pointing this out by stating that "hackers tend to see themselves as combating any closed system that would prefer to keep secrets" (Warnick, 2004, p. 272). This might explain the typical anti-corporate-software-company mentality that is so prevalent within the hacker community, as it is both an issue of curiosity and control.

The other authors also address the issue of control in regards to the hacker ethic. Hyung-jin Woo, Yeora Kim, and Joseph Dominick are the authors of “Hackers: Militants or merry pranksters? A content analysis of defaced web pages,” an article that takes a look at what motivates hackers. Although they claim that hackers enjoy exerting control over systems in a manner that is not always productive and is often destructive in nature, they do state that to be a hacker a person must want to get a thrill from problem solving. Therefore Woo, Kim, and Dominick are under the impression that control, at least in regards to the hacker ethic, comes from the ability to destroy something. In comparison, Kirsty Best, the author of “The hacker's challenge: Active access to information, visceral democracy, and discursive practice”, believes that control, in regards to the hacker ethic, comes from the ability and the want to create and inform. In her article, Best uses a quote from the editor of “2600: The Hacker Quarterly”: who states that anyone who engages in criminal acts “ceases being a hacker and commences being a criminal” (CNN, 2001). These two ideas are on opposite sides of the spectrum in how hackers exert their control over systems; however they both show the common theme of hackers wanting to have control, which is also one of the most basic human cravings.

The hacker ethic is comprised of two different principals; curiosity to know how something works and the ability to control a system through creation or destruction. While these principals might seem like basic human wants, they are the basis of the hacker ethic because hackers give in to their overwhelming passions of curiosity and control. Hacking, at its core, is not about stealing credit card numbers or cybervandalism. It is about control and an unquenchable thirst for knowledge.

Hacking individualism

On an individual level the hacker ethic can be compressed into a simple fascination to manipulate life and the things that people use in life everyday. Warnick explains that hacking is about art and expression: “THE HACK turns the computer from a mere corporate tool into an instrument of artistic creation and expression” (Warnick, 2004, p. 272). Not only does the computer become a form of artistic creation and expression, but thinking about computers in such a way opens the door into a world where hackers become the heroes. Warnick explains that one of the most popular films in the past few years has been The Matrix, a film in which the hero is a hacker character who sets out on a journey to free an entire group of people from the control of a closed system (Warnick, 2004, p. 272). Warnick explains that this is a common expression of the hacker world-view and that many people have adopted it (Warnick, 2004, p. 273). Likewise, Woo, Kim, and Dominick, show evidence in their article that points toward the fact that most web page defacement hacks are motivated individually as pranks, "About 70% of the defacements could be classified as pranks" (Woo, Kim, and Dominick, 2004, p. 63). Woo, Kim, and Dominick continue in saying that one of the reasons for web page defacement is ego and thus a hacker will disrupt a web site's operation with little regard for what a web site does or stands for. In summary, most hackers are motivated by the thrill of being able to say that they defaced a web site, in other words: bragging rights (Woo, Kim, and Dominick, 2004, p. 64 – 65).

In agreement, Best also points out that "hacking as a form of individual democracy predates overtly political group formation" (Best, 2004, p. 264). This makes sense when one thinks about democracy in terms of a free and open society and voting in terms of a free and open election process. Free and open are terms that the hacker community uses to refer to the Open Source movement and how hackers prefer their software and systems to be. The thoughts that drive many hackers to yearn for free information and open access to information are often very controversial thoughts. Some hackers take the idea of free and open information very seriously in regards to democracy and policy making.

Hacktivism

The most common form of hacking, in terms of large groups, is hacktivism. Hacktivism is the result of hacking culture's influence on activism or when technology meets politics. Best writes that "Hackers involved in the open software movement fundamentally believe that active access to information creates better software" (Best, 2004, p. 269). At the heart of democracy is the spread of information and thought. The first Amendment of the United States constitution contains provisions for free speech and freedom of the press. This translates directly into the heart of the hacker ethos. In his article “The Internet and the Seattle WTO protests,” Mathew Eagleton-Pierce describes how the protests for the World Trade Organization talks in Seattle were organized in cyberspace, despite actually being carried out in the real world (Eagleton-Pierce, 2001, p. 332). In her article entitled “Passage to cyberactivism: How dynamics of activism change,” Laura Illia writes that “following the introduction of communication technologies (CT), information technologies (IT), and the Internet, the environment within which organizations and activists deal with each other changed” (Illia, 2002, p. 327). Illia is writing about how the Internet and the technologies developed by the hacker community have changed the landscape of protests and activism. In particular the ability to communicate with more people across wider borders has changed the way protests happen and how large they are. Hacktivism can play a role not only in protesting the government and its actions but also in helping the government to secure the national infrastructure as Mark Milone suggests in his article titled “Hacktivism: Securing the national infrastructure.” Milone suggests that “Hacktivists can aid in the defense of the National Infrastructure by testing critical systems, identifying potential weaknesses, monitoring suspicious activity in cyberspace and, possibly, aiding in retaliatory attacks on hostile governments” (Milone, 2003, p. 90). Milone is suggesting that hackers who wish to help out their country could do so via the use of their special talents.

Terminating the program

The current state of research in regards to the hacker ethic is well documented and lines up quite well with my own experiences in the hacker community. Hackers are driven by curiosity, the want to create, and the need for control. The hacker ethic has had a large impact on how people view technology on an individual and personal level. From high school students who put simple after-market computer chips in their sports cars to soccer moms constantly changing their background to be pictures of their kids. It does not end there though; Ipods and Apple's iTunes software have led people to demand greater control over when and how they listen to their music. Corporate society has picked up on this desire for control too; hackers were the first to put video games on cell phones, but now everyone has at least three with the purchase of the cheapest cell phones. This outlook on control from the hacker community has most definitely breached the firewall of society. The basis of the hacker ethos is really just an amplified portion of what the human psyche craves most. Furthermore the hacker ethic is the sum of the birth of the Internet and the birth of personal computers, because technology has become so invasive and has become such a large part of everyone's life. Hackers are merely the people who understand the technology and have the ability to control it and customize it in ways that can benefit their own personal uses.

Hacktivism is the result of many people understanding the technology and using it for the purposes of helping out their own groups. This can be seen in the writings from Best, Woo, Kim, Dominick, Warnick, and Milone. Unlike Milone, I do not think true hackers are motivated to help countries or causes that are not for open information or freedom of ideas. This can be seen in places such as China where the hackers in the country are actually fighting extremely hard to find ways around the "Great Firewall of China," the filtration of information into the self-proclaimed communist country. Along with hacktivists in the country, hacktivist organizations such as the Cult of the Dead Cow (http://www.cultdeadcow.com) are also fighting hard to take down any sort of blockage that impedes the free flow of information into China. A possible method of testing to see if hacktivists are motivated by the free flow of information or by a certain political stance, might be to round up all the hacktivist projects in existence on the Internet and compare the purpose of each project. This is not a simple task and coming up with guidelines for evaluating the purpose of each project would be the hardest part of the task by far.

Hackers are not evil miscreants out to destroy corporations or run up charges on credit cards that do not belong to them. Hackers are just curious and want to play with technology. Hackers simply want to control systems so that they can play with them. Hackers crave unrestricted access to information so they can learn more about the technologies they want to control. Some hackers are motivated by the joy of creating a program that only they can use and appreciate while other hackers are motivated to help spread the ideas of free software. In the end, it is still curiosity and an infatuation with control that are the driving factors behind the hacker ethic.

Sources:

Warnick, B. R. (2004). Technological metaphors and moral education: the hacker ethic and the computational experience. *Studies in Philosophy & Education*, *23*(4), 265-281.

Skorodumova, O. (2004). Hackers as information space phenomenon. *Social Sciences*, *35*(4), 105-113.

Woo, H., Kim, Y., & Dominick J. (2004). Hackers: militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology*, *6*(1), 63-82.

Best, K. (2003). The hacker's challenge: active access to information, visceral democracy and discursive practice. *Social Semiotics*, *13*(3), 263-282.

CNN, Q&a with emmanuel goldstein of 2600: the hacker's quarterly. (2001). Retrieved Mar. 02, 2006, from CNN In-Depth Specials - Hackers - Q&A with Emmanuel Goldstein of 2600: The Hacker's Quarterly Web site: http://www.cnn.com/TECH/specials/hackers/qandas/goldstein.html.

Eagleton-Pierce, M. (2001). The Internet and the Seattle WTO protests. *Peace Review*, *13*(3), 331-337.

Illia, L. (2003). Passage to cyberactivism: how dynamics of activism change. *Journal of Public Affairs (Wiley)*, *3*(4), 326-337.

Milone, M. (2003). Hacktivism: securing the national infrastructure. *Knowledge, Technology & Policy*, *16*(1), 75-104.