The Hacker's Ethics

The Cyberpunk Project

The idea of a "hacker ethic" is perhaps best formulated in Steven Levy's 1984 book, *Hackers: Heroes of the Computer Revolution*. Levy came up with six tenets :

1. Access to computers - and anything which might teach you omething about the way the world works - should be unlimited and total. Always yield to the Hands-On imperative !
2. All information should be free.
3. Mistrust authority - promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degress, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

Phrack, recognized as the "official" p/hacker newsletter, expanded on this creed with a rationale that can be summarized in three principles. 1) First, hackers reject the notion that "businesses" are the only groups entitled to access and use of modern technology. 2) Second, hacking is a major weapon in the fight against encroaching computer technology. 3) Finally, the high cost of equipment is beyond the means of most hackers, which results in the perception that hacking and phreaking are the only recourse to spreading computer literacy to the masses :

> "Hacking. It is a full time hobby, taking countless hours per week to learn, experiment, and execute the art of penetrating multi-user computers : why do hackers spend a good portion of their time hacking ? Some might say it is scientific curiosity, others that it is for mental stimulation. But the true roots of hacker motives run much deeper than that. In this file I will describe the underlying motives of the aware hackers, make known the connections between Hacking, Phreaking, Carding, and Anarchy, and make known the "techno-revolution" which is laying seeds in the mind of every hacker... If you need a tutorial on how to perform any of the above stated methods [of hacking], please read a [*Phrack*] file on it. And whatever you do, continue the fight. Whether you know it or not, if you are a hacker, you are a revolutionary. Don't worry, you're on the right side." (Doctor Crash, 1986)

Although hackers freely acknowledge that their activities may be occasionally illegal, considerable emphasis is placed on limiting violations only to those required to obtain access and learn a system, and they display hostility toward those who transgress beyond these limits. Most experienced computer underground members are suspicious of young novices who are often entranced with what they perceive to be the "romance" of hacking. Elite hackers complain continuously that novices are at an increased risk of apprehension and also can "trash" accounts on which experienced hackers have gained and hidden their access.

In sum, the hacker style reflects well-defined goals, communication networks, values, and an ethos of resistance to authority. Because hacking requires a broader range of knowledge than does phreaking, and because such knowledge can be acquired only through experience, hackers tend to be both older and more knowledgeable than phreaks. In addition, despite some overlap, the goals of the two are somewhat dissimilar. As a

consequence, each group constitutes a separate analytic category.

This is from Richard Stallman, who found his way to the M.I.T. AI Lab in 1971, toward the tail end of the big sixties hacking burst there. He is perhaps best known for having written the mother of all freeware programs, a text-editor known as Emacs.

> "I don't know if there actually is a hacker's ethic as such, but there sure was an M.I.T. Artificial Intelligence Lab ethic. This was that bureaucracy should not be allowed to get in the way of doing anything useful. Rules did not matter - results mattered. Rules, in the form of computer security or locks on doors, were held in total, absolute disrespect. We would be proud of how quickly we would sweep away whatever little piece of bureaucracy was getting in the way, how little time it forced you to waste. Anyone who dared to lock a terminal in his office, say because he was a professor and thought he was more important than other people, would likely find his door left open the next morning. I would just climb over the ceiling or under the floor, move the terminal out, or leave the door open with a note saying what a big inconvenience it is to have to go under the floor, "so please do not inconvenience people by locking the door any longer". Even now, there is a big wrench at the AI Lab entitled "the seventh-floor master key", to be used in case anyone dares to lock up one of the more fancy terminals."