THE HACKER

2

The Mythology of
Terrorism on the Net

The "wired world" is often presented and perceived as a world without borders. To some extent this idea is true, particularly when one is analyzing how the Internet is used by various military organizations and multinational corporations; however, in a general sense, the Internet is not a world without borders. It does not exist in a vacuum. For example, when an individual logs onto the Net, h/er perception of the electronic experience is partly shaped and framed by the socialization practices of that person's native country, and hence the experience has national and/or ethnic qualities. The mythologies of the Net that perhaps might seem most relevant to an individual are also partly determined

by geography, class, and cultural identity. The development of the mythologies through which the meaning of the Net is constructed, or more accurately, imposed, typically arise out of national interests. To sum up, the Net is culturally and politically bordered, and its meaning is constructed under the authority of capital's variables of separation. For this reason CAE feels bound to make the following qualification: As CAE proceeds to discuss the mythology of terrorism on the Net, please remember that the position developed here comes from the perspective of those facing the political struggles against the rampant forces of authoritarianism in the U.S. Consequently, some of our comments may not be applicable to the European or world situation in general. It can also be said with a degree of certainty that a number of elements in this discussion will not be applicable to third world countries where terrorism still is considered to have limited revolutionary significance. On the other hand, CAE does hope that this essay will contribute to a comparative study of perceptions of the meaning and function of terrorism on the Net.

It was an experience that CAE had in London that drew the group to this topic of terrorism and the Internet. In the fall of 1994, the collective was speaking at the *Terminal Futures* conference held at the Institute for Contemporary Art, London. The topic was "electronic civil disobedience." During the question-and-answer period at the end of the talk, an audience member said that what we were suggesting was not a civil tactic of political contestation at all; rather, the tactic that we had suggested was "pure terrorism." CAE found this comment to be very curious because we could not understand

who, or more to the point, what this audience member thought was being terrorized. How can terror happen in virtual space, that is, in a space with no people—only information? Have we reached a point in civilization where we are capable of terrorizing digital abstractions? How was it that this intelligent person had come to believe that electronic blockage equaled terror? This is an unusual puzzle that CAE would like to take the first steps toward solving.

Let us begin by briefly describing terrorism as a political action. Terrorism is a strategic form of contestation, in which the resistant faction attacks the designated oppressor by using tactics of near-random violence against its citizenry. The resistant faction seeks two consequences through such actions: First, to create a panic that will sweep through the population. The panic originates when members of the public have a perpetual apprehension of their own mortality, due to what is perceived to be a consistent state of violence. If this panic can be maintained for a long enough period of time, the public will eventually demand negotiations to end this socio-psychological state of discomfort.

Second, this strategy is used in the hope that the oppressor will show its true face—one of extreme authority. That is, the oppressor will exert extreme control over its population in a militaristic manner. Two crucial events occur when the symbolic order of domination collapses and the material order of the military takes over. First, from the point of view of the citizens, "basic" freedoms are sharply curtailed; if this condition is maintained for long enough, terrorists believe that the citizens will eventually shift blame for their apparent lack of au-

tonomy from the terrorist organization to the state. Second, resistant factions tend to believe that the state will not be able to maintain the financial drain on its resources caused by constant use of military force. Unlike the deployment of spectacle, deployment of the military is exceedingly expensive, and there is no return on the investment other than temporary moments of social order. Due to financial constraints, the oppressor is eventually forced to come to the bargaining table. Terrorism then is not a revolutionary strategy, but one designed to force negotiation over policy.

The essence of terrorism is twofold. First, there is a public perception that terrorist violence is uncontrollable. Second, terrorism requires organic bodies to house the terror. But since terrorist violence cannot occur on a very large scale (since it is cellular in nature), a third component is required—an apparatus that can and will spread the spectacle of fear in a manner that blankets the given territory. We know this apparatus as "the media." The terrorist's violence allows he/r to appropriate this apparatus, and use it to deploy the type of fear that s/he sees as most advantageous. This final component is what leads us to understand that terrorism, as a necessary radical strategy in the first world, is an anachronism. The control of spectacular space is no longer the key to understanding or maintaining domination. Instead, it is the control of virtual space (and/or control of the Net apparatus) that is the new locus of power. For information economies, the Net, along with various intranets, are the apparatus of command and control. Since the division of labor has reached a plateau of unforeseen complexity, the most costly disaster that can happen in these economies is a communication gap;

this would cause the specialized segments of the division of labor to fall out of synch. Those who are electronically literate and dedicated to resisting both state authority and the hegemony of pancapitalism can use this development to great advantage. Through simple tactics of trespass and blockage, these resisters can force the state, military, and corporate authorities to come to the negotiating table. Placing the public in a state of fear is no longer necessary, nor is it essential to inflict violence on people in order to incite political change. And oddly enough, not even private property needs to be attacked or destroyed. All that is needed to accomplish what terrorism rarely does— policy negotiation—is to deny access to data conduits and bodies of data.

The most powerful weapon against authoritarianism has been delivered into the hands of the left, and yet we are letting it slip away. This is what truly worried CAE about the audience member's comments at the London ICA. The inherent civility of electronic disobedience is being deliberately and officially misconstrued under the signs of that which it is clearly not—terrorism, or more modestly, criminality. Most of the resistance on the Net confines itself either to offering alternative information services or to organizing around issues of autonomy, such as free speech. To be sure, these issues are important, but they are also secondary. However, the most important issue is not being discussed, and that is the demand for the right for people to use cyberspace as a location for political objection. Currently in the U.S., the punishment for trespass or for blockage in cyberspace is jail on the first offense. We must demand that a distinction be made between trespass with political intent and trespass

with criminal intent. For civil disobedience in physical space the penalty in the U.S., if one is arrested at all, is usually a $25 fine and a night in jail with one's fellow demonstrators. The state can be generous here, since such tactics are purely symbolic in the age of nomadic capital. Such generosity is not shown when the political action could actually accomplish something. This is a situation that must be changed.

But let us return to our original enigma, why an intelligent person would believe that civil disobedience is actually terrorism, when it is clear that electronic resistance has no relationship to terrorism in any tactical sense—no one dies, no one is under any threat. Further, it seems clear that the myth of electronic terrorism originates in the security state and in the U.S., at any rate, is deployed by state agencies such as the FBI and the Secret Service as well as by spectacular institutions such as Hollywood. How are people being duped by such obvious ploys? CAE's belief is that the prevalence of this myth reflects a subtle yet major shift in the validation of reality. The problem stems not so much from the efficiency of the state propaganda machine, but from a condition which is much more fundamental—an inclination to accept the idea of virtual terror.

The origins of this predisposition in the realm of the social are difficult to pinpoint, but probably began with the realization that power can be grounded in information. The first complex manifestation of this form of power is the bureaucracy—a very ancient form indeed. From the earliest days of the bureaucracy, official records

began to take on the status of official reality. What has changed since the days of papyrus and scrolls is that the organization of information has become amazingly efficient, since the invention of computers with their massive space-saving memories combined with accurate systems for immense storage and high-velocity retrieval. Combine these powers with computer networking capabilities, which transform information into a nomadic phenomenon, and the dominance of information reality becomes unstoppable. Information management is now generally perceived as a science of tremendous precision. And with the understanding of this activity as a science comes an authority and a legitimacy that cannot be disputed; after all, science is, for better or for worse, the master system of knowledge in secular society.

Let us return to the idea of the record. From an existential point of view, the record, optimized by the electronic information apparatus, has taken the form of horrific excess. Each one of us has files that rest at the state's fingertips. Education files, medical files, employment files, financial files, communication files, travel files, and for some, criminal files. Each strand in the trajectory of each person's life is recorded and maintained. The total collection of records on an individual is h/er or her data body—a state-and-corporate-controlled *doppelgänger*. What is most unfortunate about this development is that the data body not only claims to have ontological privilege, but actually does have it. What your data body says about you is more real than what you say about yourself. The data body is the body by which you are judged in society, and the body

that dictates your status in the social world. What we are witnessing at this point in time is the triumph of representation over being. The electronic file has conquered self-aware consciousness.

Herein lies a substantial clue as to why some people fear the disruption of cyberspace. While the organic body may not be in danger, the electronic body could be threatened. Should the electronic body be disrupted, immobilized, or (heaven forbid) deleted, one's existence in the realm of the social could be drastically effected. One could become a social "ghost," so to speak—seen and heard, but not recognized as real. The validation of one's existence could disappear in the flick of a keystroke. Once a population has accepted the notion that representation justifies one's being in the world, then simulacra begin to have direct material effects on the motivations and perceptions of people, allowing the security state and other keepers of information to exert maximum control over the general population. No doubt the erasure of social existence is a threat that strikes terror into people's hearts. This is, in part, why CAE believes it has been so easy to deploy the sign of terrorism on the Net. This is also partly why CAE members were accused of terrorism when we suggested using tactics of civil disobedience on the Net. Once we moved CD out of the realm of the physical, where disruption is localized and avoidable for those who accept their data body as their superior, we were suggesting their erasure as a consequence of political objection. What is frightening to CAE about this scenario is that electronic erasure is perceived as equivalent to being killed in a bomb

explosion. Now the perception exists that the absence of electronic recognition equals death.

With such considerations in mind, those who plan to continue the fight against authoritarianism, and who support maximum individual autonomy, have two important projects to complete. First, organic being in the world must be reestablished as the locus of reality, placing the virtual back in its proper place as simulacra. Only in such a situation can virtual environments serve utopian functions. If the virtual functions and is perceived as a superior form of being, it becomes a monstrous mechanism of control for the class that regulates access to it and mobility within it. The continuing calls for consolidation, fencing, and privatization of the Internet are indicators that resistance is behind in this battle. Second, steps must be taken to separate political action in cyberspace from the signs of criminality and terrorism. The current state strategy seems to be to label as criminal anything that does not optimize the spread of pancapitalism and the enrichment of the elite. If we lose the right to protest in cyberspace in the era of information capital, we have lost the greater part of our individual sovereignty. We must demand more than the right to speak; we must demand the right to *act* in the "wired world" on behalf of our own consciences and out of good-will for all.