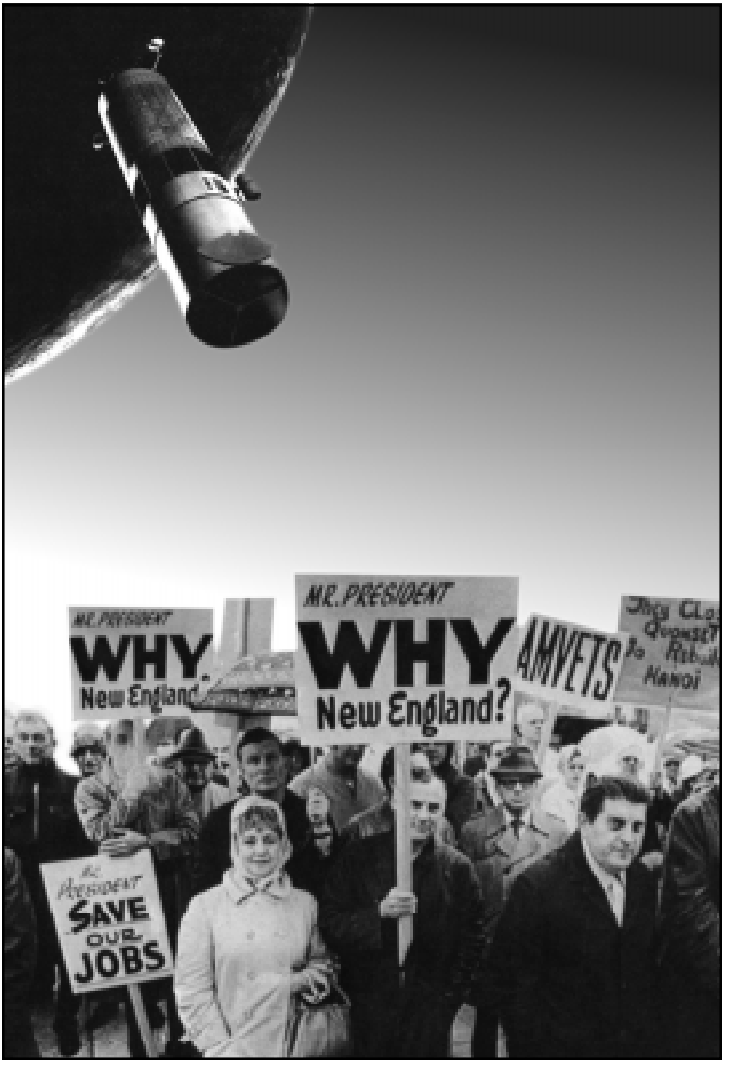
MR. PRESIDENT
WHY
New England
MR. PRESIDENT
WHY
New England?
AMVETS
SAVE
OUR
JOBS

1

Electronic Civil Disobedience*

One essential characteristic that sets late capitalism apart from other political and economic forms is its mode of representing power: What was once a sedentary concrete mass has now become a nomadic electronic flow. Before computerized information management, the heart of institutional command and control was easy to locate. In fact, the conspicuous appearance of the halls of power was used by regimes to maintain their hegemony. Castles, palaces, government bureaucracies, corporate home offices, and other architec-

*"Electronic Civil Disobedience" was originally written as part of a window installation for the *Anti-work Show* at Printed Matter at Dia in the Spring of 1994. It was then reprinted by Threadwaxing Space in *Crash: Nostalgia for the Absence of Cyberspace*. The version presented here is the original form with only a few modifications. The addendums were written the following summer before the article was presented at the *Terminal Futures* conference at the Institute of Contemporary Art in London.

tural structures stood looming in city centers, daring malcontents and underground forces to challenge their fortifications. These structures, bespeaking an impregnable and everlasting solidity, could stop or demoralize contestational movements before they started. Indeed, the prominence of this spectacle was a double-edged sword; once the opposition became desperate enough (due to material privation or to symbolic collapse of a given regime's legitimacy), its revolutionary force had no problem finding and confronting the powerholders. If the fortifications were breached, the regime would most likely collapse. Within this broad historical context emerged the general strategy for civil disobedience.

This strategy was unusual because the contestational groups decided they did not need to act violently toward those who occupied the bunkers of power, and chose instead to use various tactics to disrupt the institutions to such an extent that the occupants became disempowered. Although the smiley face of moral force was the pretext for using this approach, it was economic disruption and symbolic disturbance that made the overall strategy effective. Today acts of civil disobedience (CD) are generally intended to hasten institutional reform rather than bring about national collapse, since this style of resistance allows the possibility for negotiation. For this reason, modern first-world governments tend to be more tolerant of these acts, since they do not necessarily threaten the continued existence of a nation or its ruling class. While civil disobedience does not go unpunished, it is generally not met with extreme violence from the state, nor are participants in CD ordinarily labeled as revolutionaries and treated as political prisoners when arrested. (There have of course been some notable excep-

tions to this policy in the first world, such as the persecution of American civil rights activists in the deep South).

Although CD is still effective as originally conceived (particularly at local levels), its efficacy fades with each passing decade. This decline is due primarily to the increasing ability of power to evade the provocations of CD participants. Even though the monuments of power still stand, visibly present in stable locations, the agency that maintains power is neither visible nor stable. Power no longer permanently resides in these monuments, and command and control now move about as desired. If mechanisms of control are challenged in one spatial location, they simply move to another location. As a result, CD groups are prevented from establishing a theater of operations by which they can actually disrupt a given institution. Blocking the entrances to a building, or some other resistant action in physical space, can prevent reoccupation (the flow of personnel), but this is of little consequence so long as information-capital continues to flow.

These outdated methods of resistance must be refined, and new methods of disruption invented that attack power (non)centers on the electronic level. The strategy and tactics of CD can still be useful beyond local actions, but only if they are used to block the flow of information rather than the flow of personnel. Unfortunately, the left is its own worst enemy in developing ways to revise CD models. This situation is particularly ironic, since the left has always prided itself on using history in critical analysis. Now, rather than acknowledge the present shift in historical forces when constructing strategies for political activism, members of the left continue to act as if they still live in the

age of early capital. This is particularly strange because contestational theory always stresses the importance of dramatic shifts in political economy (early capital to late capital, industrial economy to service economy, production culture to consumption culture, etc). Indeed, the left's lapse of insight on this matter indicates that the schism between theory and practice is as bad as (or worse than) it has ever been.

This particular form of cultural lag prevents activists from devising new strategies for reasons that are difficult to pinpoint. At least one factor responsible is the continued presence of the remnants of the 60s New Left within the ranks of activist groups. Preoccupied as they are with the means used to achieve past victories (primarily the contribution that the New Left made to the withdrawal of American troops from Viet Nam), members of these groups see no need to invent new approaches. Nostalgia for 60s activism endlessly replays the past as the present, and unfortunately this nostalgia has also infected a new generation of activists who have no living memory of the 60s. Out of this sentimentality has arisen the belief that the "take to the streets" strategy worked then, and will work now on current issues. Meanwhile, as wealth and education continue to be increasingly distributed in favor of the wealthy, as the security state continues to invade private life, as the AIDS crisis still meets with government inaction, and as the homeless population continues to expand, CAE is willing to go out on a limb and say that perhaps an error in judgment has occurred. This claim is not intended to undermine what has been accomplished on local levels; it is intended only to point out that contemporary activism has had very little effect on military/corporate policy.

CAE has said it before, and we will say it again: as far as power is concerned, the streets are dead capital! Nothing of value to the power elite can be found on the streets, nor does this class need control of the streets to efficiently run and maintain state institutions. For CD to have any meaningful effect, the resisters must appropriate something of value to the state. Once they have an object of value, the resisters have a platform from which they may bargain for (or perhaps demand) change.

At one time the control of the street *was* a valued item. In 19th century Paris the streets were the conduits for the mobility of power, whether it was economic or military in nature. If the streets were blocked, and key political fortresses were occupied, the state became inert, and in some cases collapsed under its own weight. This method of resistance was still useful up through the 60s, but since the end of the 19th century it has yielded diminishing returns, and has drifted from being a radical practice to a liberal one. This strategy is grounded in the necessity of centralizing capital within cities; as capital has become increasingly decentralized, breaking through national boundaries and abandoning the cities, street action has become increasingly useless. Since cities have been abandoned by business and left to rot in a state of bankruptcy, and have become plagued by crime and disease, it seems reasonable to assume that they are no longer useful in the expansion of power. If they were of use, surely they would be continually renewed and defended.

Dangers do lie in this often tautological line of argument. Is the city of no value because it is not maintained, or is it not maintained because it is of no value? This error in logic

is inescapable, since the question of who or what is in control cannot be answered. Power itself cannot be seen; only its representation appears. What lies behind the representation is lost. The location and nature of cynical power is purely a matter of speculation. Macro power is known only as a series of abstractions such as "straight white males," "the ruling class," or best of all, "the powers that be." Macro power is experienced only by its effects, and never as a cause. Consequently, certain indicators must be used to determine what is of value to power, or to find the (non)location of power. The assumption here is that key indicators of power-value are the extent to which a location or a commodity is defended, and the extent to which trespassers are punished. The greater the intensity of defense and punishment, the greater the power-value. These indicators have been derived from experience, but they cannot be given theoretical justification, since a second principle will eventually have to be used to explain a first principle.

If the traditional location for deploying power has been abandoned, where has power moved? If we assume that the flow of capital is still crucial to the present system, then there is a trail to follow. (Un)common sense tells us that we can follow the money to find power; however, since money has no point of origin but is part of a circular or spiraling flow, the best we can expect to find is the flow itself. Capital rarely takes a hard form; like power, it exists as an abstraction. An abstract form will probably be found in an abstract place, or to be more specific, in cyberspace. Cyberspace may be defined as a virtual informational landscape that is accessed through the phone system. (For the purposes of this essay, the association between cyberspace and VR

proper should be ignored). The degree of access to the information located in cyberspace suggests how institutions are configured in real space. In complex society, the division of labor has become so differentiated that the organizational speed necessary to keep the many segments synchronized can only be achieved by using electronic communication networks. In turn, the controlled deployment of information and access to it becomes a central clue in solving the puzzle of social organization. When access to information is denied, the organizational properties of the institution from which it is withheld become unstable, and—should this condition be maintained for too long—the institution will eventually collapse because of a communication gap. The various segments will have no idea if they are working at cross purposes against each other or if they are working in unison against competing institutions. Blocking information access is the best means to disrupt any institution, whether it is military, corporate, or governmental. When such action is successfully carried out, all segments of the institution are damaged.

The problem with CD as it is now understood is that it has no effect on the core of organization; instead, it tends to concentrate on one localized sedentary structure. In the case of national or multinational institutions, such actions are no more disruptive than a fly biting an elephant. Back when power was centralized in sedentary locations, this strategy made sense, but it is vain now that power is decentralized. To dominate strategic sites in physical space was once the key source of power, but now domination rests on the ability of an institution to move where resistance is absent, in conjunction with the ability to temporarily appropriate a given physical space as needed. For an oppo-

sitional force to conquer key points in physical space in no way threatens an institution. Let us assume that a group of dissidents managed to occupy the White House. It might prove embarrassing for the administration in power and for the Secret Service, but in no way would this occupation actually disrupt the efficient functioning of executive power. The presidential office would simply move to another location. The physical space of the White House is only a hollow representation of presidential authority; it is not essential to it.

In measuring power-value by the extent to which actions are punished and sites are defended, it is readily apparent that cyberspace ranks high on the scale. Defense systems in cyberspace are as well-developed as they can be. The Secret Service (previously an agency whose job was to protect individuals connected with the office of the President and to investigate counterfeiting rackets) has become increasingly swept up in its role as cyberpolice. At the same time, private corporations have developed their own electronic police forces, which function in two ways: First, they act as security forces, installing information surveillance and defense systems, and second, they act as a posse of bounty hunters to physically capture any person who breaks through the security systems. These forces, like the legal system, do not distinguish between actions in cyberspace on the basis of intent. Whether private information sources are accessed simply to examine the system, or whether the purpose is to steal or damage the source, these forces always assume that unauthorized access is an act of extreme hostility, and should receive maximum punishment. In spite of all this security, cyberspace is far from secure. It has expanded and mutated at such a rapid rate that security systems are unable

to reconfigure and deploy themselves with equal speed. At present, the gate is still open for information resistance, but it is closing.

Who is attempting to hold the gate open? This is perhaps one of the saddest chapters in the history of resistance in the US. Right now the finest political activists are children. Teen hackers work out of their parents' homes and college dormitories to breach corporate and governmental security systems. Their intentions are vague. Some seem to know that their actions are political in nature. As Dr. Crash has said: "Whether you know it or not, if you are a hacker you are a revolutionary." The question is, a revolutionary for what cause? After poring through issues of *Phrack* and surfing the internet, one can find no cause mentioned other than the first step: free access to information. How this information would be applied is never discussed. The problem of letting children act as the avant-garde of activism is that they have not yet developed a critical sensibility that would guide them beyond their first political encounter. Ironically enough, they do have the intelligence to realize where political action must begin if it is to be effective—a realization that seems to have eluded leftist sophisticates. Another problem is the youthful sense of immortality. According to Bruce Sterling, their youthful fearlessness tends to get them arrested. A number of these young activists—the Atlanta Three, for example—have served time in what has to be recognized as political imprisonment. With only the charge of trespass against them, jailing these individuals seems a little extreme; however, when considering the value of order and private property in cyberspace, extreme punishment for the smallest of crimes should be expected.

Applying the maximum punishment for a minimal offense must be justified in some way. Either the system of punishment must be kept hidden from the public, or the offense must be perceived by the public as a horrific disruption of the social order. Currently, the situation in regard to crime and cyberspace seems neutral, as there is no solid commitment by the state to either path. The arrest and punishment of hackers does not make headlines, and yet the law and order alarm has started to ring. Operation Sundevil, a thorough sweep of hacker operations in 1990 by the Secret Service and corporate posses, received minimal attention from the media. It was well publicized amongst the groups affected by such activities, but it was hardly the material needed for a "60 Minutes" investigation or even a Phil Donahue show. Whether this lack of publicity was intentional or not on the part of the Secret Service is difficult to say. Certainly corporations do not like to call attention to their posses, nor does the Secret Service want to advertise its Gestapo tactics of confiscating the property of citizens not charged with any crime, and neither of the two want to encourage hacker behavior by openly revealing the power that can be gained through "criminal" access to cyberspace. From the point of view of the state, it makes strategic sense to limit the various threats of punishment to the technocracy, until electronic dissidents can be presented to the public as the incarnation of evil bent on the destruction of civilization. However, it is difficult for the state to designate a techno-child as the villain of the week along the lines of Noriega, Saddam Hussein, Khadafy, Khomeny, or anyone involved with drugs from users to cartel leaders. To go public will require something more than just a charge of trespass; it will have to be something that the public can really panic about.

Hollywood has begun to make some suggestions in films such as *Die Hard II* and *Sneakers*. In *Die Hard II*, for example, terrorist hackers appropriate airport computers and use them to hold planes hostage, and even crash one. Fortunately these scenarios are still perceived by the public as science fiction, but it is precisely this kind of imaging which will eventually be used to suspend individual rights, not just to catch computer criminals, but to capture political dissidents as well. Legal agencies are just as able to persecute and prosecute political factions when what they *could* do arouses fear in others.

Herein lies the distinction between computer criminality and electronic civil disobedience. While the computer criminal seeks profit from actions that damage an individual, the person involved in electronic resistance only attacks institutions. Under the rubric of electronic resistance, 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. The authoritarian goal is to prevent this distinction from being perceived; all electronic resistance must fall under the totalizing sign of criminality. Conflating electronic civil disobedience (ECD) with criminal acts makes it possible to seal off cyberspace from resistant political activity. Attacks in cyberspace will carry penalties equivalent to those merited by violent attacks in physical space. Some leftist legal agencies, such as the Electronic Frontier Foundation, have already realized that basic freedoms (of speech, assembly, and press) are denied in cyberspace and are acting accordingly, but they have yet to start work on legitimizing the distinction between political and criminal action. The same legal

penalties that apply to CD should also apply to ECD. However, state and corporate agencies should be expected to offer maximum resistance to legal activities aimed at legitimizing ECD. If these authoritarian structures are unwilling to grant basic rights in cyberspace to individuals, it seems safe to assume that a pseudo-legitimized resistance will not be tolerated either.

The strategy and tactics of ECD should not be a mystery to any activists. They are the same as traditional CD. ECD is a nonviolent activity by its very nature, since the oppositional forces never physically confront one another. As in CD, the primary tactics in ECD are trespass and blockage. Exits, entrances, conduits, and other key spaces must be occupied by the contestational force in order to bring pressure on legitimized institutions engaged in unethical or criminal actions. Blocking information conduits is analogous to blocking physical locations; however, electronic blockage can cause financial stress that physical blockage cannot, and it can be used beyond the local level. ECD is CD reinvigorated. What CD once was, ECD is now.

Activists must remember that ECD can easily be abused. The sites for disturbance must be carefully selected. Just as an activist group would not block access to a hospital emergency room, electronic activists must avoid blocking access to an electronic site that may have similar humanitarian functions. For example, let us assume that a profiteering pharmaceutical company is targeted. Care will have to be taken not to block the data controlling the manufacture and distribution of life-saving medications (no matter how bad the extortion profits might be from the drugs). Rather, once the company is targeted, activists

would be wiser to select research or consumption-pattern data bases as sites for occupation. Having the R&D or marketing division shut down is one of the most expensive setbacks that a company can suffer. The blockage of this data will give the resistant group a foundation from which to bargain without hurting those who are in need of the medications. Further, if terms are not met, or if there is an attempt to recapture the data, ethical behavior requires that data must not be destroyed or damaged. Finally, no matter how tempting it might be, do not electronically attack individuals (electronic assassination) in the company—not CEOs, not managers, not workers. Don't erase or occupy their bank accounts or destroy their credit. Stick to attacks on the institutions. Attacking individuals only satisfies an urge for revenge without having any effect on corporate or government policy.

This model, although it seems so easy to grasp, is still science fiction. No alliance exists between hackers and specific political organizations. In spite of the fact that each would benefit through interaction and cooperation, the alienating structure of a complex division of labor keeps these two social segments separated more successfully than could the best police force. Hacking requires a continuous technical education in order to keep skills up to date and razor sharp. This educational need has two consequences: First, it is time-consuming, leaving little or no leisure time for collecting information about specific political causes, building critical perspective, or designating contestational sites. Without such information, hacker politics will continue to be extraordinarily vague. Second, continuous reeducation keeps hackers tied into their own hermetically-sealed classroom. Little interaction occurs with others

outside this technocratic subclass. Traditional political activists do not fare any better. Left behind in the dust of history, this political subgroup knows what to do and what to target, but has no effective means to carry out its desires. Political activists, as knowledgeable as they might be about their causes, are too often stuck in assembly meetings debating which monument to dead capital they should strike next. Here are two groups motivated to accomplish similar anti-authoritarian ends, but which cannot seem to find a point of intersection. While the former group lives on-line, the latter group lives in the street, and both are unknowingly being defeated by a communication gap for which neither is responsible. The schism between knowledge and technical skill has to be closed, to eliminate the prejudices held by each side (hacker intolerance for the technologically impaired, and activist intolerance for those who are not politically correct).

The hacker/activist schism is not the only difficulty that keeps the idea of ECD in the realm of science fiction. The problem of how to organize potential alliances is also significant. Leftist activism has traditionally been based on principles of democracy—that is, on a belief in the necessity of inclusion. They believe that with no other bargaining power besides sheer number, the populist mass must be organized so that its collective will can be asserted. The weaknesses of this strategy are rather obvious. The first weakness is the belief in a collective will itself. Since the populist mass is divided by so many sociological variables—race/ethnicity, gender, sexual preference, class, education, occupation, language, etc.—it is readily apparent that viewing "the people" as a monolith of consensus is absurd. What fulfills the needs of one group can be repressive or

oppressive to another. Centralized organizations attempting to flex their political muscles through the power of numbers find themselves in a peculiar position: Either the group size is relatively large, but it cannot move en masse, or the group advocates an ideological position useful only to a limited sociological set, thereby shrinking their number. In addition, in order for the most simple organization to exist, there must also be bureaucracy. Bureaucracy requires leadership, and hence hierarchy. Leadership structures are generally benevolent in these situations, since the leadership is often based on talent and motivation rather than on ascriptive characteristics, and it fluctuates among the membership; however, bureaucratic structure, regardless of how relentlessly it strains toward justice, still erodes the possibility of community (in its proper sense). Within such an organizational pattern, individuals are forced to trust an impersonal process over which they have no real control.

The use of democratic principles of centralization, when analyzed on a global scale, becomes even more depressing. As yet, no democratic organization exists that comes even remotely close to constructing a multinational resistance. Since power has gone global, avoiding attack is merely a matter of moving operations to a location where resistance is absent. Further, in regard to the condition of pluralism, national interest becomes a variable—a policy that is useful within one national situation becomes repressive or oppressive in another. Collective democratic action may be weakly effective on the local (micro) level, but it becomes next to useless on a macro scale; the complexity of the division of labor prevents consensus, and there is no apparatus through which *to organize*.

The option of realizing hacker fantasies of a new avant-garde, in which a technocratic class of resistors acts on behalf of "the people," seems every bit as suspect, although it is not as fantastic as thinking that the people of the world will unite. A technocratic avant-garde is theoretically possible, since an apparatus is in place for such a development. However, since the technocracy consists overwhelmingly of young white first-world males, one has to wonder just what issues would be addressed. That dreaded question of "who speaks for whom?" looms large whenever the idea of avant-gardism is shuffled about.

The question of resistance then becomes threefold: First, how can the notion of an avant-garde be recombined with notions of pluralism? Second, what are the strategies and tactics needed to fight a decentralized power that is constantly in a state of flux? Finally, how are the units of resistance to be organized? Without question, no certain answers are available, but CAE would like to offer the following proposals. The use of power through number—from labor unions to activist organizations—is bankrupt, because such a strategy requires consensus within the resisting party and the existence of a centralized present enemy. However, in spite of the lack of consensus on what to do, most organizations do share a common goal—that is, resistance to authoritarian power. Yet even in terms of goals there is no consensus about the practical basis of authoritarian power. The perception of authoritarianism shifts depending on the coordinates from which a given sociological group chooses to resist authoritarian discourse and practice. How then can this situation be redefined in constructive terms? An anti-authoritarian predisposition becomes useful only when the idea of the democratic

monolith is surrendered. To fight a decentralized power requires the use of a decentralized means. Let each group resist from the coordinates that it perceives to be the most fruitful. This means that leftist political action must reorganize itself in terms of anarchist cells, an arrangement that allows resistance to originate from many different points, instead of focusing on one (perhaps biased) point of attack. Within such a micro structure, individuals can reach a meaningful consensus based on trust in the other individuals (real community) in the cell, rather than one based on trust in a bureaucratic process. Each cell can construct its own identity, and can do so without the loss of individual identity; each individual within the cell maintains at all times a multidimensional persona that cannot be reduced to the sign of a particular practice.

How can a small group (four to ten people) have any type of political effect? This is the most difficult question, but the answer lies in the construction of the cell. The cell must be organic; that is, it must consist of interrelated parts working together to form a whole that is greater than the sum of the parts. To be effective, the schism between knowledge and technical ability in the cell must be closed. A shared political perspective should be the glue that binds the parts, rather than interdependence through need. Avoid consensus through similarity of skills, since in order for the cell to be useful, different skills must be represented. Activist, theorist, artist, hacker, and even a lawyer would be a good combination of talents—knowledge and practice should mix. With the cell in place, ECD is now a viable option, and as explained earlier in the essay, with ECD, demands will at least be recognized. Another advantage is that the cell has the option of pooling financial resources,

so the minimal equipment needed for ECD can be purchased. The problem of potential legal fees is an argument for centralization—cells may not have a long lifespan. Admittedly, the toxic illegality of electronic political action is one of the key variables that relegates this narrative to the realm of science fiction.

For more radical cells ECD is only the first step. Electronic violence, such as data hostages and system crashes, are also an option. Are such strategies and tactics a misguided nihilism? CAE thinks not. Since revolution is not a viable option, the negation of negation is the only realistic course of action. After two centuries of revolution and near-revolution, one historical lesson continually appears—authoritarian structure cannot be smashed; it can only be resisted. Every time we have opened our eyes after wandering the shining path of a glorious revolution, we find that the bureaucracy is still standing. We find Coca-Cola gone and Pepsi-Cola in its place—looks different, tastes the same. This is why there is no need to fear that we will one day wake up and find civilization destroyed by mad anarchists. This mythic fiction is one that originates in the security state to instill in the public a fear of effective action.

Do centralized programs still have a role in this resistance? Centralized organizations have three functions. The first is to distribute information. Consciousness raising and spectacle production should be carried out by centralized counter-bureaucracies. Cash and labor pools are needed in order to research, construct, design, and distribute information contrary to the aims of the state. The second function is for recruitment and training. It cannot be emphasized

enough that there must be more bases for training technologically literate people. To rely only on the chance that enough people will have the right inclination and aptitude to become technically-literate resisters means that there will be a shortage of resistant technocrats to fill the cellular ranks, and that the sociological base for the technocratic resistance will not be broad enough. (If technical education continues to be distributed as it is today, the attack on authority will be horribly skewed in favor of a select group of issues). Finally, centralized organizations can act as consultants on the off chance that an authoritarian institution has decided to reform itself in some way. This can happen in a realistic sense, not because of an corporate-military ideological shift, but because it would be cheaper to reform than to continue the battle. The authoritarian fetish for efficiency is an ally that cannot be underestimated.

All that centralized organizations must do—in a negative sense—is to stay out of direct action. Leave confrontation to the cells. Infiltrating cellular activity is very difficult, unlike infiltrating centralized structures. (This is not to say that cellular activities are difficult to monitor, although the degree of difficulty does rise as more cells proliferate). If the cells are working in double blind activities in a large enough number, and are effective in and of themselves, authority can be challenged. The fundamental strategy for resistance remains the same—appropriate authoritarian means and turn them against themselves. However, for this strategy to take on meaning, resistance—like power—must withdraw from the street. Cyberspace as a location and apparatus for resistance has yet to be realized. Now is the time to bring a new model of resistant practice into action.

Addendum: The New Avant-Garde

CAE fears that some of our readers might be getting a bit squeamish about the use of the term "avant-garde" in the above essay. After all, an avalanche of literature from very fine postmodern critics has for the past two decades consistently told us that the avant-garde is dead and has been placed in a suitable resting plot in the Modernist cemetery alongside its siblings, originality and the author. In the case of the avant-garde, however, perhaps a magic elixir exists that can reanimate this corpse. The notion has decayed quite a bit, so one would not expect this zombie to look as it once did, but it may still have a place in the world of the living.

The avant-garde today cannot be the mythic entity it once was. No longer can we believe that artists, revolutionaries, and visionaries are able to step outside of culture to catch a glimpse of the necessities of history as well as the future. Nor would it be realistic to think that a party of individuals of enlightened social consciousness (beyond ideology) has arrived to lead the people into a glorious tomorrow. However, a less appealing (in the utopian sense) form of the avant-garde does exist. To simplify the matter, let us assume that within the present social context, there are individuals who object to various authoritarian institutions, and each has allied h/erself with other individuals based on identification solidarity (race/ethnicity, sexual orientation, class, gender, religion, political beliefs, etc.) to form groups/organizations to combat the mechanisms and institutions that are deemed oppressive, repressive, exploitive, and so on. From a theoretical perspective, each of these alliances has a contestational role to play that should be respected and appreciated; however, in terms of

practice, there is no basis to view them all as equals. Unquestionably, some groups will have greater resource power than others; that is, some will have greater access to wealth, prestige, hardware, education, and technical skills. Typically, the greater the resources, the greater the effect the group can have. However, the configuration of access in conjunction with the groups' placement along political, numerical, and spatial/geographic continuums will also greatly alter the effectiveness of the group. (A full catalogue of possibilities cannot be listed within the parameters of this discussion). For example, a large, very visible group that is on the radical fringe, which works to change national policy, and which has reasonably good access to resources will also receive stiff counter-resistance from the state, thereby neutralizing its potential power. The rapid destruction of the Black Panther Party by the FBI is an example of this vulnerability. A relatively large liberal group with strong resources that acts locally will receive less counter-resistance. (Hence the misguided belief that if everyone acts locally for reform, policy will change globally and peacefully. Unfortunately local action does not affect global or national policies, since the sum of local issues does not equal national issues). For example, an alliance of various green groups in North Florida has been very successful at keeping oil companies off the Gulf coast line and protecting the local national forests and preserves from logging companies and land speculators; however, such success is by no means representative of the national or international situation in regard to the Green movement.

Then what kind of group configuration *will* gain the most far-ranging results, in terms of disturbing the political/cultural landscape? This is the question that CAE tried to

answer in this essay. To repeat: cellular constructions aimed at information disruption in cyberspace. The problem is access. The education and technical skills needed are not widely distributed, and moreover are monopolized (though not through individual intentionality) by a very specific group (young white men). Education activists should be and in many cases are working as hard as possible to correct this problem of access, even though it does seem almost insurmountable. At the same time, contestational forces cannot wait to act until this access problem is corrected. Only in theory can we live by what ought to be; in practice we must work in terms of what is. Those who are trained and ready now need to start building the model of electronic resistance. Those who are ready and willing to begin to form the models of electronic resistance in the new frontier of cyberspace are the ones CAE views as a new avant-garde.

The technocratic avant-garde offers one slim hope of effective resistance on a national and international scale; and, in its favor, in terms of efficiency, and unlike its Modernist predecessors, the intelligentsia, this group does not have to organize "the people." Much like the problems of resource access, this necessity or desire has always bothered the forces of democracy. Avant-gardism is grounded in the dangerous notion that there exists an elite class possessing enlightened consciousness. The fear that one tyrant will simply be replaced by another is what makes avant-gardism so suspect among egalitarians, who in turn always return to more inclusive local strategies. While CAE does not want to discourage or disparage the many possible configurations of (democratic) resistance, the only groups that will successfully confront power are those that locate

the arena of contestation in cyberspace, and hence an elite force seems to be the best possibility. The increased success of local and regional resistant configurations, in part, depends upon the success of the avant-garde in the causal domain of the virtual. As for "enlightened consciousness," CAE believes blind groping is a more accurate description. Avant-gardism is a gamble, and the odds are not good, but at present, it's the only game in town.

Addendum II:
A Note on Absence, Terror, and Nomadic Resistance

In *The Electronic Disturbance*, CAE argued that a major change in the representation of power had occurred over the past twenty years. Power once represented itself as a visible sedentary force through various types of spectacle (media, architecture, etc.), but it has instead retreated into cyberspace where it can nomadically wander the globe, always absent to counterforces, always present whenever and wherever opportunity knocks. In "Electronic Civil Disobedience," CAE notes that for every strategy there is a counterstrategy. Since cyberspace is accessible to all of the technocratic class, the resistant within this class can also use nomadic strategies and tactics. Indeed, the primary concern among the military/corporate cyber police (Computer Emergency Response Team, the Secret Service, and the FBI's National Computer Crime Squad) is that nomadic strategy and tactics are being employed at this very moment by contestational groups and individuals (in the words of authority, "criminal" groups). The cyberpolice and their elite masters are living under the sign of virtual catastrophe (that is, anticipating the electronic disaster that *could* happen) in much the same way that the op-

pressed have lived under the signs of virtual war (the war that we are forever preparing for but never comes) and virtual surveillance (the knowledge that we may be watched by the eye of authority).

The current wave of paranoia began in early 1994 with the discovery of "sniffer" programs. Apparently some adept crackers are collecting passwords for unknown purposes. The reaction of the cyberpolice was predictable: They are convinced that this could only be done for criminal intent. Of prime concern is the development of the tactic of data hostaging, where criminals hold precious research data for ransom. Motivations for such an activity are construed solely as criminal. (This is typical of US policy—criminalize alternative political action, arrest the guilty, and then claim with a clear conscience that the US has no political prisoners). CERT, the FBI, and the SS seem convinced that teen crackers have matured and are evolving past information curiosity into information criminality. But something else of greater interest is beginning to occur. The terror of nomadic power is being exposed. The global elite are having to look into the mirror and see their strategies turned against them—terror reflecting back on itself. The threat is a virtual one. There could be cells of crackers hovering unseen, yet poised for a coordinated attack on the net—not to attack a particular institution, but to attack the net itself (which is to say, the world). A coordinated attack on the routers could bring down the whole electronic power apparatus. The vulnerability of the cyber apparatus is known, and now the sign of virtual catastrophe tortures those who created it. As James C. Settle, founder and head of the FBI's National Computer Crime Squad, has said: "I don't think the stuff we are *seeing* is the stuff we need to be worried

about. What that activity we do see is indicative of, however, is that we have a really big problem.... Something is cooking but no one really knows what." The motto of the sight machine reverberates out of Settle's rhetoric: "If I can see it, it's already dead." At the same time, the opposite—what Settle calls "the dark side"—is out there, planning and scheming. Nomadic power has created its own nemesis—its own image. This brings up the possibility that as a tactic for exposing the nature of nomadic power, ECD is already outdated without having ever been tried. No real "illegal" action needs to be taken. From the point of view of traditional terrorism, action that can reveal the cruelty of nomadic power need only exist in hyperreality, that is, as activities that merely indicate a possibility of electronic disaster. From this moment forward, strategies of the hyperreal will have to be downgraded into the real, meaning the technocratic class (those with the skill to mount a powerful resistance) will have to *act* on behalf of liberation from electronic control under the nomadic elite. The reason: They are not going to have a choice. Since the individuals in this class are the agents of vulnerability within the realm of cyberspace, repression in this class will be formidable. Since "the dark side" has no image, the police state will have no problem inscribing it with its own paranoid projections, thus doubling the amounts of repression, and pushing the situation into a McCarthyist frenzy. To be sure, each technocrat will be paid well to sell h/er sovereignty, but CAE finds it hard to believe that all will live happily under the microscope of repression and accusation. There will always be a healthy contingent who will want to die free rather than live constrained and controlled in a golden prison.

A second problem for nomadic power, as it finds itself suddenly caught in the predicament of sedentary visibility and geographic space, is that not only could an attack on cyberspace bring about the collapse of the apparatus of power, but the possibility also exists for attacking particular domains. This means that ECD could be used effectively. Even though nomadic power has avoided the possibility of a theater of operations emerging contrary to its needs and goals in physical space, once a resistant group enters cyberspace, elite domains can be found and placed under siege.

Whether or not the barbarian hordes—the true nomads of cyberspace—are ready to sweep through the orderly domains of electronic civilization remains to be seen. (If the hordes do their jobs well, they never *will* be seen. The domains will not report them, as they cannot expose their own insecurity, in much the same way a failing bank will not make its debts public). The hordes do have one advantage: They are without a domain, completely deterritorialized, and invisible. In the realm of the invisible what's real and what's hyperreal? Not even the police state knows for sure.