COMPUTING AND WAR

by Brian Martin

John Bradley, an established computing professional, in 1972 reached a new stage in his successful career when his employer, the U.S. Air Force, promoted him and transferred him to the Defense Communications Agency. Bradley's new job was to supervise the testing of the prototype for communications between computers in different parts of the country that were parts of the World Wide Military Command and Control System, or Wimex. This system was to provide early warning and communications in case of a Soviet missile attack.

Bradley soon discovered serious problems with Wimex: Its Honeywell computers were out of date and too unreliable. When he tried to raise the issue with his supervisors, they responded by criticizing Bradley himself, getting him transferred and eventually dismissed.[1] This is one of many cases of the suppression of a person who "blows the whistle" on faulty practices, mismanagement or corruption.

The Bradley story epitomizes a number of features of the linkages between computing and war. First, computers in missile early warning systems are but one example of the way in which computing systems have become central to many contemporary weapons systems. Second, the choice of technology for Wimex was a product of particular links between computer companies and military bureaucracies; this reflects the wider processes by which social factors influence the development of computing. Finally, the flaws in Wimex are symptomatic of the vulnerabilities that can plague the use of computing for war.

AUTHOR'S NOTE In writing this article I was helped by advice from Jim Falk and Stewart Russell, by reading a paper by Frank Ferzoco, and by comments from Ian Reinecke, Stephanie Short, and two anonymous referees on a draft

PEACE & CHANGE, Vol 14 No 2, April 1989 203-222

There are numerous ways in which computing and war are interlinked. In this article I outline some of these under a range of categories: hardware and software, the system for production of computing knowledge, ideology, and social institutions. This should give some idea of the ways in which computers and computing are integrated into the systems through which war is prepared for and waged.

Computing, perhaps more than most technological systems, is centrally involved in the war system. Hence, the case study of computing and war provides a useful way to approach the broader issue of the links between technology and war. Even on this wider issue there is little writing that deals with the connections at the levels of knowledge, ideology, and social institutions.

An intellectual appreciation of the linkages between computing and war is a limited objective by itself. The important thing in my opinion is how to intervene in the computing/war system in order to challenge it and replace it with a less lethal alternative. I try in the final section to give some suggestions of how this might be done. The choice of what *should* be done of course depends on each individual's values about desirable futures and about possible and desirable ways of moving toward these futures.

HARDWARE AND SOFTWARE

Even a quick examination of modern war fighting systems shows the central role of computing. High-accuracy missile guidance, for example, could not be achieved without sophisticated computer hardware and software. The cruise missile with its terrain-contour-matching capacity requires an on-board computer that compares observations of elevation, made by sensors, with stored information about the terrain along the flight path, thereby enabling it to travel close to the ground and find its target precisely—if it works.[2]

The computers actually used in weapons systems are only the front-line aspect of the role of computing in the modern

technology of war. The information about enemy terrain that is necessary for the success of cruise missiles is obtained, among other ways, through satellite observations. The processing of these observations depends on computers. Likewise, the development of the cruise missile itself—for example, its engine, radar characteristics, and aerodynamic stability—has relied on computing for design work and testing.

Computing is essential in nearly every phase of contemporary weapons development, as indeed it is for most current technological research and development. For example, the further refinement of nuclear weapons designs requires high-powered computers to simulate the behavior of components and of the explosion itself. New designs are studied first on computer drawing boards rather than by hand in workshops.

More prosaic weapons systems also depend on computing for development and refinement. For example, a computer program can be useful for finding the optimum size and shape for a bullet that will tumble in flight, thereby causing a much more massive injury when it hits a human. So although there are no actual computers inside bullets (yet!), computing has played a vital role in making them what they are.

The activity of military intelligence these days depends heavily on computing. Without its massive bank of computers, the signals picked up by Pine Gap, a U.S. military spy base in central Australia, would be meaningless. One of the ways in which militaries attempt to protect their transmissions from interception is through encoding: scrambling the information using some sort of code. Encoding is then challenged by efforts to decode the other side's code. A computer can be used to do this, because it can automatically test untold possible codes. (The other main way is through spying.) The result has been intense interest in the mathematical subject of cryptology. The U.S. National Security Agency attempted to put controls on the publication of pure mathematics work in cryptology. The National Science Foundation eventually acquiesced to a "voluntary" system.[3]

The success of the U.S. government's Strategic Defense Initiative or "Star Wars" requires enormously sophisticated

software. Whether or not such software can be developed—there have been severe criticisms of the program[4]—it is significant that a highly touted "solution" to the threat of nuclear war should depend so heavily on computing. Not that this is anything new. Strategists have been arguing for years about the merit of relying on computer-based launch-on-warning systems to initiate a second strike in response to a nuclear attack. Military planners seem to have accepted the computer as an essential element in their thinking.

It can be argued that there is nothing particularly sinister in the massive use of computing in technological warfare, because computing is penetrating virtually all aspects of contemporary technology. Although computers are used in war, they are also used in all sorts of other areas, such as growing wheat or making toys. An analogy might be made to the vital role of steel in weapons systems. Does this mean that the steel industry and steel technology are inherently warlike? Is the use of Fortran to write a weapons design program any more damning of Fortran than the use of English to write a memo in the army is damning of English?

In some cases there appears to be a direct influence of the military on computer architecture and languages. For example, a reason for the preference for hierarchical structures in computer architecture seems to have been the ease with which these structures could accommodate the problems posed by the military in the 1950s, whereas the early preference for large mainframes in part reflected military interest in number-crunching problems such as missile trajectories. The U.S. Department of Defense has spent enormous sums developing its own computer language, ADA.

Even if the influence of military priorities on computing development could be further elaborated, the existence of this influence would not go very far in saying that computers are *inherently* militaristic. But perhaps that is not really the issue anyway. Rather than focusing on the physical presence of computers in weapons and weapons design, it may be better to ask how it is that computer workers are mobilized to further military aims.

KNOWLEDGE PRODUCTION SYSTEMS

Modern scientific knowledge is not something that simply "springs to mind" through the inspiration of a few geniuses who spend their time contemplating the universe. Most scientific knowledge is now created through regularized systems that are quite similar to other systems of industrial production.[5] The workers who produce scientific knowledge are scientists. Although many of these workers believe that *they* are in control of what they produce and how, this is true only in a limited sense. The funding, employment, key problems, and choices for development are all heavily dominated by large organizations, especially the state and large corporations. The military is one of these large organizations—a part of the state—that has a strong influence on the scientific knowledge production system.[6]

The military provides a great deal of funding for computing research. This helps to push that research in certain directions. Many of the early developments in computing after World War II—including some of the first electronic computers—were the direct result of military interest in problems such as calculating ballistic missile trajectories. Military funding influences the direction and pace of developments, although not all the actual uses of those developments. Military-funded research on the "electronic battlefield" may turn out to have some spinoffs for civilian applications, but much of it will be useful only to the military for military purposes.

Computing researchers may have their own agendas. They may accept military money for Star Wars research on the grounds that Star Wars can't work anyway and they will simply grab some of the money and use it for their own projects. This justification misses an important impact of the military's funding for research. Although a large fraction of military research funding may be "diverted" into civilian or (more likely) useless areas, the military nevertheless creates for itself a valuable reservoir of research results to examine and from which to pick and choose. If some esoteric bit of research surprisingly turns out to have some practical application, the military will obtain a preview and an early option.

A second point is that military funding maintains a reserve of skilled researchers doing work that is at least peripherally related to military priorities. This reserve of scientific workers is valuable in case of a major conflict or crisis, because many will offer their services to work on a project of national urgency. Without regular funding, a reserve army of appropriately skilled scientific workers would be much less likely to be on hand.

The availability of employment by the military is a related influence on the computing knowledge production system. Some researchers are reluctant to take a public antiwar stand because it may jeopardize future job prospects in military research groups or in bodies that must maintain good relations with the military, such as some government departments. The influence via employment can be seen as an extension of the more general military influence via funding for computing research.

The influence of the military on computing research extends more widely than direct funding and employment. Because of military funding, certain areas of immediate or indirect interest to the military gain added prominence, such as the need to develop very large high-reliability and high-security computing networks. These same areas have civilian applications too, so researchers concerned with these applications may pursue them without a thought to the military applications. The point is that the areas of special interest to the military come to seem somewhat more important as *scientific* problems partly because of the added funding and research activity stimulated by military interest. Areas that have no likely military spinoffs do not obtain this fillip.

Computing workers are not always passive pawns in taking up military work. Many of them actively pursue military-related projects and attempt to sell their ideas to the military. This is the role of the scientist as "military hustler."[7] The computing professionals and the military have become mutually dependent. The computing workers depend on the military for funding, status, and direction while the military depends on the

expertise of computing workers to keep its systems running and to develop new ones.

The influence of military funding and potential applications on computing research is no different from similar influences of corporations, the state, and professional bodies. Corporations that want to reduce the uncertainty entailed in having human workers will promote and apply computing developments that eliminate some of these workers while maintaining the need for corporate management structures.[8] The upshot is that computing research in areas in which there are no powerful vested interests providing funds or offering large payoffs is largely neglected. Indeed, it is hard for computing researchers to even conceive of what these areas might be, because the current research priorities are seen as natural rather than as an outgrowth of wider patterns of funding and application.

It may sound as if all computing workers are totally channeled into military-supporting or at least military-indifferent areas, but there are at least some researchers who consciously set out to tackle projects of immediate significance for nonmilitary purposes, and many others who end up doing this simply because their intellectual interests take them along different paths. Most of these directions are filtered out at the stage of development. A good idea relevant to the military is likely to be given a heavy dose of funds for development and demonstration, even though military funders are sometimes poor judges of what will serve their own interests, narrowly defined. A good idea irrelevant to the military but relevant to a food manufacturer, for example, may receive some funding, though food manufacturers do not have research establishments as richly endowed as do militaries. Finally, a good idea irrelevant for war, profit, or bureaucratic control is unlikely to receive any large-scale funding at all.

The computing knowledge production system as a whole is not unified and centrally organized. There are all sorts of small idiosyncratic research projects as well as large, directed research teams. The sources of funding and inspiration are

diverse. In this system the military does have a considerable influence on overall directions, by provision of funding and employment, by influencing what are seen as the key research problems, and by selectively taking up specific types of developments that do occur. Computing is not a simple tool of the military; nevertheless, much of it is attuned to military priorities.

IDEOLOGY

As well as the physical occurrence of computers in military hardware and the role of computing in the design and development of weapons systems and other parts of the military role in society, computing plays a certain ideological role for and in the military. A social judgment made on the basis of a social scientific study often is seen to have greater credibility if it has popped out of a computer. By building values or even conclusions into a computer program or a computer-designed piece of equipment, these values or conclusions attain for most observers greater objectivity: the results are perceived as emanating from a machine process that somehow transcends the motives and failings of its creators.

This process is most apparent in an area such as the "limits to growth"—predictions of global catastrophe due to population growth, resource use, and so on—in which the outcome of a simple model, obvious after a bit of reflection given the assumptions made, is anointed with the blessing of science via a computer program. The military also makes use of computer-related credibility, but seldom in so direct a manner. The U.S. radar warning system against nuclear attack relies on computers, nuclear targeting is organized through a computer system, and command and control systems are heavily dependent on computers. These and other military systems are painted as more reliable because they are automated: the ever-ready radar and computer system provides protection against a sudden Soviet attack.

Yet the role of computing in these systems does not have a high profile so far as the public is concerned; in addition, the ideological role of computers is often ambivalent. Just as the limits to growth studies were attacked by the demonstration of flaws in the model—such as that changing a few parameters would lead to different results[9]—the ideological uses of military computing are vulnerable to criticism. The computer failures of the early warning system are symptomatic. In addition, many people feel uncomfortable depending on automated systems, hence the continual pressure to maintain manned systems.

It is probably *within* the military that the ideological uses of computing are greatest. One important function of computing is the separation, provided by automated weapons systems, between the war makers and those attacked. Computers are a vital part of technological weapons systems that remove military personnel from the blood and agony of war fighting. High-altitude bombing, the electronic battlefield, crewless vehicles, and a host of other techniques have increasingly removed soldiers, not to mention officers, from the formal scene of the fighting. (The contrary process brought about by nuclear weapons and intercontinental ballistic missiles is one of bringing everyone, including civilians, onto the front lines of a future conflict.) This separation makes it possible, at least for some, to wreak devastation with less of the moral revulsion that results from seeing the consequences of one's action directly.

Needless to say, the psychic separation from killing is often incomplete. There are many military personnel who recoil from destruction even at a distance. But as systems become more automated and the decisions about the unleashing of powerful weapons are placed in fewer hands, the scope for moral revulsion to inhibit war making is reduced. (This is not the place to examine the much greater sensitivity to personal spilling of blood in many contemporary societies—cruel tortures and brutal executions are no longer seen as valid public spectacles, as they were in the Middle Ages, for

example—paralleled by a massive increase in the capacity for remote killing.)

Another use of computing within the military comes through the use of battle simulations and other techniques for developing strategy and tactics. As in all mathematical and computer modeling, the results from such exercises in war gaming reflect the assumptions that are built into the model. Putting a military or political problem through a mathematical or computer translation process helps to hide the assumptions and to make the results seem more objective. In this way the military is able to prepare for war in a manner that masks the one-sided assumptions about "aggression," "freedom," "defense" and so forth. And again, war gaming provides an enhanced ability, for those planning for war in intricate detail, for psychic separation from its consequences.

SOCIAL INSTITUTIONS[10]

So far I have described how computers and computing are heavily implicated in the technology of war, how the computing knowledge production system is linked to the special interests of the military, and how computing can be ideologically linked to war. Another way to analyze the connections between computing and war is in terms of the social institutions underlying both computing and the war system, including the state, bureaucracy, the military, and patriarchy.

The state comprises a range of social structures including national government, government bureaucracies, regional and local government, the legal system, the military, the police, and government-owned industry. The state, as that social institution that is built on a monopoly over what is claimed to be the legitimate use of violence within a territory, is central to the war system. Modern wars—violent confrontations between professional military forces—are fought between states and not directly between classes, sexes, or ethnic groups (though there is much violence involving these groups). Civil wars are violent conflicts between groups contending for state power.

The development of computing for war has come largely through state sponsorship, especially through direct employment of computer specialists and through military funding of computing research and development. Most academic researchers are tied to the state through state funding for higher education, though the link to war is usually indirect here.

The symbiosis between the state and science was hinted at in World War I, forged in World War II, and cemented in the decades since. Computing was born into this system of science-state mutual reinforcement between source and the state. It is hard to imagine a development of computing completely cut off from service to the state. The only major driving force behind computing development independent of the state is corporate capitalism, which in relevant areas is closely tied to state priorities anyway.[11] The state provides most of the funding for contemporary universities, and funds targeted for military-related research are a significant feature of this funding.[12]

A second social institution involved in the war system is bureaucracy, which is a way of organizing the work of people using hierarchy and a complex division of labor. All major state organizations are organized as bureaucracies, and indeed the military is a model bureaucracy. The relevance of bureaucracy to modern war is that it makes it possible to mobilize large numbers of people and large amounts of resources for the service of the state and in particular for military purposes. Without bureaucracy, the routine extraction of an economic surplus for the state (for example through taxes) would not be easy, and the formulation of policy from the top and the organization of many people's work to implement that policy would be very difficult.

The many transformations of war making in the past few hundred years can be summed up by the word *bureaucratization.* Rather than being based, for example, on the ad hoc recruitment of small numbers of fighters for particular conflicts that had little impact on the general population as in feudal times, the present, historically unique war system is based on large standing armies of professional soldiers, on regular

economic transfers to military purposes, on hierarchical command structures, on close links with social and technological systems for "civilian production," and on mass patriotism to mobilize populations to support war efforts. Most of these features of contemporary war systems depend strongly on the bureaucratic mode of organization.

Although the early development of computing was heavily constrained by military and corporate imperatives, the rapid expansion of computing meant that at least in some areas, and perhaps especially in the 1960s, computing was a craft activity. Some individuals could be involved in many aspects: operating, key punching, programming, and running jobs. In other words, the division of labor was relatively simple, and selected people could advance in the field based on their performances without the barriers of credentials or formal positions. At the same time, there has always been a competing influence toward increasing bureaucracy. Work is stratified by the classifications of operators, data inputters, coders, programmers, and systems analysts. Formal training is increasingly expected of new entrants to the area.[13]

The bureaucratization of computing makes it easier to control by those at the top, namely managers, and this makes computing more amenable to the military. A group of independent craft workers is harder to dragoon into the service of a particular interest group than is a bureaucratized workforce, which can be manipulated from the top. Computing is now little different than any of a large number of bureaucratized areas, including manufacturing, energy production, and scientific research. What this means is that computing operations and computing research can readily be meshed with other bureaucratized operations, one of which is military operations.

Another key social institution in the war system is the military itself. The military is a central institution of the state, embodying and enforcing its monopoly on "legitimate" violence. Military forces in industrialized countries are increasingly reflecting the division of labor and the specialization of function that characterizes industrial society generally. Armies are not made up of masses of troops for fighting on the front

lines. Rather, military forces are built around sophisticated weapons systems that require a host of "civilian" support workers: mechanics, electricians, machinists, engineers, and so forth. Professional and technical workers are just as essential to contemporary technological warfare as are the official troops. Computer workers are part of this. Those who design, operate, program, or maintain military computers are just as crucial as the front-line fighters. Even the computing necessary to keep track of equipment or provide paychecks is vital to the functioning of the military.

Patriarchy is the collective domination of men over women that operates through a variety of channels including the family, the state, corporations, professions, and the law. Men control most of the key positions in governments, corporations, trade unions, and other powerful social institutions. The question is, how deeply implicated is patriarchy in the war system? Certainly the military is an intensely masculine area in which characteristically masculine attributes of aggressiveness, competition, and inhibition of emotions are encouraged while the feminine values of caring, nurturance, and expressiveness are stamped out. (There are some contradictions: soldiers are drilled into obedience, normally considered a feminine attribute.)

Computing is also a male-dominated area, and one that draws on characteristically masculine attributes. The commonality of patriarchy to the military and computing makes easier a meshing of their goals. Whether patriarchy provides a tight or a loose bond between computing and war is something that has not been examined.[14]

What is the significance of these connections between computing and war via the social institutions of the state, bureaucracy, the military, and patriarchy? Basically these are institutions that are structured in a way that makes them convenient for serving the purposes of war, whether by extracting resources from the economy for military hardware or by providing a gender orientation that facilitates the expression of aggression and domination. If computing is structured in a way that makes it congruent with many of these

same institutions—which is what I have been arguing—then computing is linked to war through the patterns of its social and conceptual organization. This means that the links between computing and war go deeper than the presence of computers in military satellites or the funding of computing research by the military. Rather, features of computing work such as hierarchy, the division of labor, and male domination are keys to the role of computing in the war system.

STRATEGIES

So far I have emphasized the way computing is linked to the war system and not given much attention to the frictions between them. The heavy use of computing in high-technology weapons systems brings vulnerabilities as well as strengths. The failures of ballistic missile early warning systems show not only the failures of humanly constructed computer systems, but also the ideological weakness for the military of depending for defense on the aura of invincible technology. As practical military technology, many sophisticated computer systems remain poorly tested. The complicated flight dynamics programmed into ballistic missiles are misleading so long as actual flight tests over planned ranges—specifically over the North Pole—remain untested. The concern over the electromagnetic pulse—the pulse of electromagnetic energy following a very massive and very high-altitude nuclear explosion that could disable electronic systems over a whole continent—shows that technological sophistication can have hidden vulnerabilities.

Here I do not wish to dwell on the technological shortcomings of computer systems used in war, but to outline some of the strategies for intervening in the computing/war nexus. Doing this will also throw some light on the value of the different ways, presented in earlier sections, of looking at the relation between computing and war. Given the presence of a significant, active, professional concern about computing used in war, it is appropriate to examine strategies for computing workers too.

An obvious and fruitful channel is for computer experts to speak out against the military machine and especially the uses of computing within it. Speaking out simply as a member of the public adds to the general strength of the antiwar movement; when a person speaks out specifically as a computing expert, this has several added impacts. Most important, it undercuts any appearance of professional unanimity on the use of computing in war. Governments rely heavily on claims that they and their experts know best how to promote national security. When specialists speak out critically on military policy, this punctures the government's claimed monopoly on expertise and helps open wider public debate. This happened when some academic cryptologists attacked on technical grounds the National Security Agency's attempt to monopolize the field. Challenging the promilitary experts can help expose the value judgments involved in ostensibly technical decision making.

Speaking out also challenges those computing experts who do work for or otherwise serve the military. Some of them will find it harder to justify to themselves that they just carry out neutral research whose use is decided by policymakers and that there is nothing they can do to oppose the situation anyway. Another impact that professionals can make is to refuse to accept funding for military-related research or other activity. This withdraws expertise from the military and, more important, helps undermine the legitimacy of military research.[15] The valuable activities of Computer Professionals for Social Responsibility as part of the peace movement mostly fall in this category of speaking out and refusing to participate in military research. The importance of this should not be underestimated, especially because professionals in general are very slow to take public stands on social issues.

Although speaking out is important, it also has limitations that can be seen by examining the computing knowledge production system and the social institutions linked to both war and computing. Although *some* computing workers may speak out, the provision of funds, careers, and status by computing research will ensure that a sizable fraction of

researchers continue to carry out military work. The idea that mass withdrawal might by itself bring war to a halt—"What if they had a war and all the computing workers pulled the plug?"—ignores the reality of deep linkages that help tie many computing workers to the military. The bureaucratic and patriarchal nature of computing work, as well as the role of funding, are difficult to challenge by a straightforward appeal to alternative values.

Another strategy is to promote the sort of computing that would be appropriate for a peaceful and equitable world and so shift energy and legitimacy from war work to peace work. This is analogous to the initiative in the antinuclear power movement to promote renewable and decentralized energy alternatives. Instead of simply opposing the military, computer workers can develop positive alternatives that provide employment and useful products. This strategy of "peaceful conversion" of military computing work to civilian work and of "computing for peace" strikes deeply at the linkages between computing and war. It is an immediate challenge to the usual knowledge production system. To provide a challenge to the bureaucratization and male domination of computing, the "computing for peace" needs to be organized in a more egalitarian and participative way. This has been the orientation of a few initiatives, perhaps the most notable of which has been the community memory project in San Francisco associated with the *Journal of Community Communications.* The aim here was to provide a network of computer terminals with a system that would allow individuals to add and extract information (announcements, offers, and so on) on an equal basis without subjecting themselves to some sort of hierarchical control.[16]

The problems with this project are likely to be the familiar ones. The development of "alternative computing" lacks the financial and institutional support given to mainstream computing for its support of government and corporate purposes. Without the protection of regular funding and secure jobs, the alternative schemes depend heavily on voluntary efforts. Only

a few people have the commitment to pursue such efforts in the face of indifference or hostility from established institutions. A bigger problem is that even should a successful scheme be developed, there is no easy way to "sell" it for wider use. This problem is the reverse of the military's procedure of funding lots of research in the hope that some of it bears fruit and can be easily picked off for massive funding, development, and application. The alternative computing efforts are few, and when they do produce a promising seed, it often falls on barren ground.

In spite of the major difficulties, the aim of alternative computing is vitally important. Unlike some other professions, computing still contains a high number of enthusiastic amateurs who "work" in the area not for career reasons but because they are excited about what they are doing. Many of these enthusiasts could readily turn their attention to computing that would equalize rather than hoard knowledge and that would serve the needs of the powerless rather than the powerful members of society. What is required is much more attention to practical projects that satisfy these sorts of criteria and are engaging for computing buffs.

The final strategy I examine here is related to the idea, What if they had a war and all the computing workers pulled the plug?, which I dismissed earlier. The tight integration of computers and computing research into contemporary military systems, while making weapons more deadly and expanding the capacity for surveillance and monitoring, also opens a major vulnerability. Computing experts as a professional group are both a strategic asset for the military and a strategic threat should they become unreliable. If even a small fraction of computing workers in the military decided to sabotage computing systems—from tampering with circuits to subtly altering programs—major military weapons systems could be brought to a standstill.

Internal resistance to directives has always plagued militaries. For example, some bombing pilots in the Vietnam war simply ran their sorties and dropped the bombs in the most

harmless place possible. I have read about members of U.S. crews assigned to intercontinental ballistic missiles who have pledged to each other not to fire weapons in retaliation. The successes of most of the major social revolutions in the past several centuries—for example in France in 1789, in Russia in 1917, and in Iran in 1979—have depended on the internal collapse of the military of the previous regime rather than its conquest by brute force.[17] This vulnerability to revolt remains. Now that militaries have become so highly technological, the role of technical experts in withdrawing support could establish a new pattern for military failure or collapse.

How can this vulnerability of militaries to sabotage or to withdrawal of technical support be linked to peace movement strategies? I think the major connection is via social defense—also called civilian defense, civilian-based defense and nonviolent defense—which can be defined as nonviolent community resistance to aggression as an alternative to military defense. Social defense is based on methods such as petitions, demonstrations, strikes, boycotts, sit-ins, and setting up alternative institutions. It aims to obstruct the opponent and also to win converts by defending a just cause with only nonviolent means.[18] There are some promising precedents for social defense, such as the resistance of the Czechs to the 1968 Soviet invasion and the resistance of the Norwegians to the Nazis in 1941-1945.

The study of the potential of social defense is in its infancy. To my knowledge there has been no systematic study of the ways in which computing workers could act to frustrate an invasion or military takeover, although even a brief examination of the area suggests the enormous scope for such action.[19] Social defense, because it is participative and indeed requires the support of most people in order to succeed, provides a challenge to the major social institutions linked into the war system. Developing computing for social defense is one way to help promote a stronger social defense and also to orient computing away from its war linkages.

NOTES

1 Rhonda Brown and Paul Matteucci, "The High Cost of Whistle-blowing," *Inquiry*, 4 (September 1, 1981):14-19

2. For a basic account see Daniel L Slotnick and Joan K. Slotnick, *Computers. Their Structure, Use, and Influence* (Englewood Cliffs, N J.· Prentice-Hall, 1979), chap. 7, or Owen Greene, *Europe's Folly. The Facts and Arguments about Cruise* (London Campaign for Nuclear Disarmament, 1983), pp. 12-19.

3 James Bamford, *The Puzzle Palace* (Boston: Houghton Mifflin, 1982), chap. 9; Susan Landau, "Primes, Codes and the National Security Agency," *Notices of the American Mathematical Society*, 30 (January 1983) 7-10.

4 David Lorge Parnas, "Software Aspects of Strategic Defense Systems," *American Scientist* 73 (September-October 1985):432-440; see more generally, Alan Borning, "Computer-system Reliability and Nuclear War," *Communications of the ACM* 30 (February 1987) 112-131

5 Hilary Rose and Steven Rose, eds , *The Political Economy of Science* and *The Radicalisation of Science* (London: Macmillan, 1976)

6 See the many examples in Robin Clarke, *The Science of War and Peace* (London Jonathan Cape, 1971)

7 Bruno Vitale, "Scientists as Military Hustlers," in *Issues in Radical Science* (London Free Association Books, 1985), pp. 73-87

8 Harry Braverman, *Labor and Monopoly Capital* (New York· Monthly Review Press, 1974).

9 H S D. Cole, Christopher Freeman, Marie Jahoda and K L R Pavitt, *Thinking about the Future. A Critique of The Limits to Growth* (London: Chatto & Windus, 1973)

10 This analysis is developed in Brian Martin, *Uprooting War* (London Freedom Press, 1984), chap. 10.

11 Seymour Melman, *Pentagon Capitalism* (New York McGraw-Hill, 1970).

12 See, for example, the articles in *Science for the People*, vol. 20, number 1 (January-February 1988).

13 Joan A Greenbaum, *In the Name of Efficiency· Management Theory and Shopfloor Practice in Data-processing Work* (Philadelphia: Temple University Press, 1979); Philip Kraft, *Programmers and Managers. the Routinization of Computer Programming in the United States* (New York: Springer Verlag, 1977)

14 For one view in relation to science generally, see Brian Easlea, *Fathering the Unthinkable: Masculinity, Science and the Nuclear Arms Race* (London: Pluto Press, 1983)

15 Steve Nadis, "After the Boycott: How Scientists are Stopping SDI," *Science for the People* 20 (January-February 1988) 21-26

16 See *Journal of Community Communications* and Tom Athanasiou, "Hightech Alternativism," in *Making Waves: The Politics of Communications* (London· Free Association Books, 1985), pp. 37-51.

17 Katherine Chorley, *Armies and the Art of Revolution* (London Faber and Faber, 1943).

18 See, for example, Anders Boserup and Andrew Mack, *War Without Weapons* (London Frances Pinter, 1974), Adam Roberts, ed., *The Strategy of Civilian Defense*

(London Faber and Faber, 1967), Gene Sharp, *Making Europe Unconquerable* (Cambridge, Mass.: Ballinger, 1985)

19 An initial effort is given in Jacki Quilty, Lynne Dickins, Phil Anderson, and Brian Martin, *Capital Defence. Social Defence for Canberra* (Canberra, Australia Canberra Peacemakers [GPO Box 1875, Canberra ACT 2601, Australia], 1986)