by Paul Abrahams, acm president

president's letter

The Strategic Defense Initiative

On March 23, 1983, President Ronald Reagan unveiled his hopes and plans for the Strategic Defense Initiative (SDI) popularly known as Star Wars. At once it was apparent that computer systems would be at the heart of any realization of SDI. Major advances in software engineering, artificial intelligence, parallel processing and real-time systems would be necessary for SDI to achieve its goals. Since then the computer science community has been riven by controversy over whether SDI is feasible or even desirable.

Earlier this year the American Mathematical Society (AMS) adopted a resolution on SDI stating that "many scientists consider SDI (commonly referred to as Star Wars) incapable of achieving its stated goals and dangerously destabilizing." The resolution went on to say that "the AMS will lend no support to the Star Wars program."

SDI has so far been more of an issue for individuals within ACM than for ACM as an organization. However, Peter Neumann, the chairman of the ACM Committee on Computers and Public Policy, has been running an informal study group to consider the issue. Neumann is also the moderator of ACM's on-line Forum on Risks to the Public in Computers and Related Systems.

The ACM Code of Ethics provides reason for individual ACM members to be concerned about SDI. Item EC3.1, pertaining to Ethical Considerations, states:

"An ACM member shall accept only those assignments for which there is reasonable expectation of meeting requirements or specifications, and shall perform his assignments in a professional manner."

Canon 5 states:

"An ACM member should use his special knowledge and skills for the advancement of human welfare."

The first ethical consideration under Canon 5 is:

"An ACM member should consider the health, privacy, and general welfare of the public in the performance of his work."

If SDI has no prospect of meeting its requirements or threatens to harm the health and general welfare of the public by inducing nuclear catastrophe, then working on SDI creates ethical problems for many of us.

What in fact are the requirements for SDI? The decision to proceed with SDI research was justified politically by the rationale put forth by President Reagan in his 1983 speech. In that speech he said:

"But what if free people could live secure in the knowledge that their security did not rest upon the threat of instant U.S. retaliation to deter a Soviet attack; that we could intercept and destroy strategic ballistic missiles before they reached our own soil or that of our allies?"

He went on to say:

"I call upon the scientific community . . . to give us the means of rendering these nuclear weapons impotent and obsolete."

These are the requirements for SDI. The key phrase in the first statement is "secure in the knowledge"; it implies that a strategic defense must be absolutely trustworthy. The key word in the second statement is "impotent"; an impotent weapon is necessarily obsolete.

One of the most superficially compelling arguments for the feasibility of SDI is that technological optimism has historically often been justified. The argument goes something like this: "Every major scientific and technological advance was preceded by a time when the wisest heads claimed that it couldn't be done. The pessimists were wrong. We built flying machines, made talking pictures, split the atom, cured polio, sent men to the moon, and built computers that you can hold in your hand. SDI can achieve its goals." Yes, optimists are sometimes right, but they are not always right. Moreover, there are two logical fallacies in the argument that technological optimism applies to SDI.

First, there is no objective test to determine the success of SDI. In all the examples that people cite to prove that the pessimists are wrong in matters of scientific progress, Nature is the opponent. Nature does not change its strategy; nations do. In all these other examples of scientific and technological accomplishment, there has been an objective test to know when the problem is solved. The success of SDI is inherently not testable.

Let us assume that all the problems of software, physics, and engineering associated with SDI can in fact be resolved. Let's assume that we can build any system we wish to, as the optimists would have us do. The unanswerable question still remains: how do we know when we are done? By what means can we state with assurance that we have indeed met President Reagan's

stated requirement of rendering nuclear weapons impotent—that is, incapable of rendering us harm—no matter how and in what numbers they are delivered, how they are defended, and what the opponent knows of our defenses?

Second, the technological optimism argument is symmetrical. It applies as well to the offense as to the defense, and to the Soviet Union as well as to the United States. Suppose that an effective defense against ballistic missiles has apparently been constructed. Suppose further that this defense has not been constructed by the United States, but instead by the Soviet Union. How many advocates of SDI would be prepared, at that point, to say, "OK. You can hit us, but we can't hit you. We give up. Mr. Gorbachev, the world is yours!"

No, technological optimism would surely be invoked. Using good old American know-how and enterprise, we would find a way to penetrate the Soviet defense system and restore the potency of our weapons. But if we have faith that we could penetrate a Soviet version of SDI, how can we then turn around and claim the Soviets would be unable to penetrate an SDI system that we might build?

There are other ways of delivering nuclear weapons besides via ICBM's. These include sea-launched cruise missiles (SLCM's, or "slickums" to those in the trade), low-level bombers, and even emplaced bombs smuggled into the country. The strategic defense, it seems, is a Maginot Line; an enemy may simply choose to go around it rather than through it.

Some advocates of SDI have defended it by arguing that an absolute defense is unnecessary, and that it is sufficient to create uncertainty as to whether or not the system can be penetrated. According to this argument, an opponent will not attack unless success is certain. The biggest trouble with this defense of SDI is that it contradicts the assumptions by which SDI was justified. SDI advocates have been making this argument to technically sophisticated audiences, but no one in a conspicuous political position, certainly not President Reagan, has been willing to state openly that certain and perfect defense is neither necessary nor possible.

Pursuing SDI is a major public policy decision. Yet more modest goals for SDI have never been publicly stated and justified. An agreed-upon set of more modest goals probably does not exist. Even with more modest goals, there are strong technical reasons for doubting the feasibility of SDI. These doubts concern both the software and the physics involved. No one claims it will be easy. Even President Reagan in his 1983 speech recognized it as a formidable technical task, one that might not be accomplished before the end of the century.

David Parnas was a member of the SDI Organization (SDIO) Panel on Computing in Support of Battle Management. In a collection of eight essays, published in *American Scientist* and also in the December, 1985 issue of *Communications*, he explained why he believes that systems of the sort being considered by the SDIO can never be trustworthy. He argued the difficulties with SDI software are inherent in the nature of software and the task to be performed. They are not just accidents resulting from the current state of research in software engineering and program verification.

There are competent and distinguished computer scientists who dispute these conclusions, notably Richard Lipton of Princeton University. It is difficult for an outsider to fully evaluate the debate because it entails technically sophisticated and specialized arguments about what might or might not be achieved in an unknown future. Even Lipton and his colleagues have not attempted to argue that SDI can provide the kind of absolute defense that President Reagan set as a goal—one that would render nuclear weapons impotent.

In a similar vein, the American Physical Society commissioned a study group to examine the science and technology of directed energy weapons. In its May, 1987 report, this distinguished group found "significant gaps in the scientific and engineering understanding of many issues associated with the development of these technologies," and estimated that "a decade or more of intensive research would be required to provide the technical knowledge needed for an informed decision about the potential effectiveness and survivability of directed energy weapon systems."

The Reagan Administration's commitment to SDI and its evident desire to establish a constituency for it by creating a network of SDI contractors has had painful implications for some computer science researchers. Although there is no way to prove a cause and effect relationship, the Defense Advanced Research Projects Agency (DARPA) budget has been shrinking over the last three years while the SDIO budget has been growing. Since DARPA has historically been a bulwark of support for computer science research, the result has been increasing pressure on researchers to take SDIO money. This pressure has created an ethical dilemma for researchers who doubt the value of SDI, and has a lot to do with the resolution adopted by AMS. I expect that computer professionals in industry will experience similar pressures if they have not already.

I must emphasize that these are my personal views and not an official statement of ACM policy. I am concerned about these issues as an ACM member, a computing professional, and a human being hoping to survive for a few more years on this earth. I believe that SDI is a mistake because no system is capable of meeting the requirements stated for SDI. The software cannot be reliably constructed, the system risks catastrophe whether or not it works, the SDI effort will consume immense resources that are badly needed elsewhere, and the SDI effort creates severe ethical conflicts for computer professionals.