Title
SDI: Two Views of Professional Responsibility

Journal
Institute on Global Conflict and Cooperation, 75(10)

ISSN
0034-6748

Authors
Cohen, Danny
Lorge Pamas, David

Publication Date
1987

IGCC

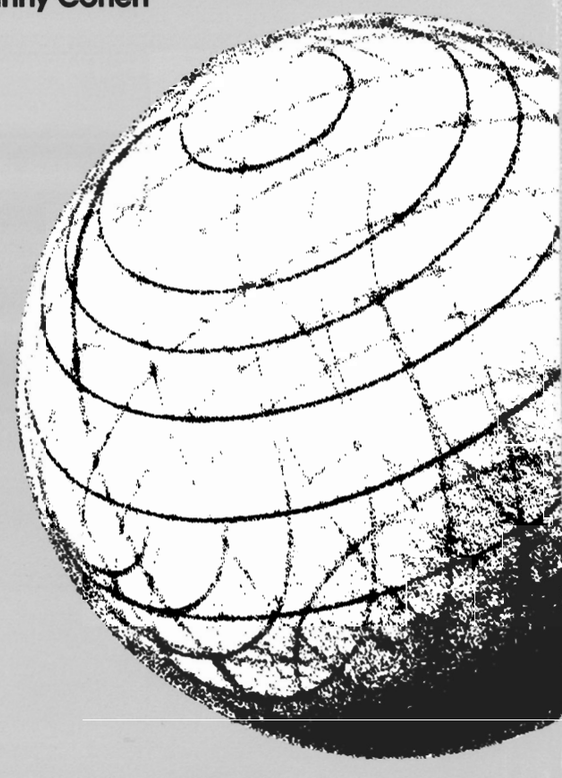
University of California
Institute on Global Conflict
and Cooperation

IGCC Policy Paper No. **5**

SDI:
TWO VIEWS OF PROFESSIONAL RESPONSIBILITY

David Lorge Parnas

Danny Cohen



8687-484

University of California
Institute on Global Conflict
and Cooperation

The Institute on Global Conflict and Cooperation is an interdisciplinary Multicampus Research Unit of the University of California, established by the Regents in June 1983. The mission of IGCC is to promote research and teaching on international conflict and cooperation, with particular emphasis on threats and avoidance of nuclear war. The IGCC Central Office is located at the University of California, San Diego.

Director: Herbert F. York
Associate Directors: G. Allen Greb and James M. Skelly

Address Inquiries to:
Publications Director
Institute on Global Conflict and Cooperation
Mail Code Q-068
University of California, San Diego
La Jolla, CA 92093

IGCC TITLES

Research Paper Series

No. 1. Lawrence Badash, Elizabeth Hodes, and Adolph Tiddens
Nuclear Fission: Reaction to the Discovery in 1939
53 pp, 1985

No. 2. Michael D. Intriligator and Dagobert L. Brito
Arms Control: Problems and Prospects
12 pp, 1987

No. 3. G. Allen Greb
Science Advice to Presidents: From Test Bans to the Strategic Defense Initiative
21 pp, 1987

Policy Paper Series

No. 1. George A. Keyworth II
Security and Stability: The Role for Strategic Defense
12 pp, 1985

No. 2. Gerald R. Ford
The Vladivostok Negotiations and Other Events
13 pp, 1986

No. 4. Johan Galtung
United States Foreign Policy: As Manifest Theology
20 pp, 1987

No. 5. David Lorge Parnas
Danny Cohen
SDI: Two Views of Professional Responsibility
28 pp, 1987

Other Titles

Neil Joeck and Herbert F. York
Countdown on the Comprehensive Test Ban
(Joint publication with the Ploughshares Fund, Inc.)
23 pp, 1986

James M. Skelly, ed.
Sociological Perspectives on Global Conflict and Cooperation: A Research Agenda
36 pp, 1986

Gregg Herken, ed.
Historical Perspectives on Global Conflict and Cooperation
34 pp, 1987

Seymour Feshbach and Robert D. Singer, eds.
Psychological Research on International Conflict and Nuclear Arms Issues: Possible Directions
50 pp, 1987

Walter Kohn, Frank Newman, and Roger Revelle, eds.
Perspectives on the Crisis of UNESCO
71 pp, 1987

problem, rather than a problem that is typical to all major defense systems.

In his rebuttal, Prof. Parnas also mentions the SAFEGUARD project. There are as many opinions about the reasons for discontinuing SAFEGUARD as there are people who were involved. For Prof. Parnas to claim that it was due to the ineffectiveness of the system is unsubstantiated, and therefore irresponsible. In fact a very large portion of the software developed for SAFEGUARD is still in continuous use in several other defense systems.

Prof. Parnas tells us that "the public might also be interested in knowing that in the last few years I [Parnas] have repeatedly challenged software people to name software products that functioned adequately when first given to users for actual (not test) use." Apollo, Voyager, and the flight control of the shuttle are just a few of the answers to his challenge. One wonders why it is that Prof. Parnas does not consider these examples.

University of California
Institute on Global Conflict
and Cooperation

IGCC Policy Paper No. **5**

SDI:
TWO VIEWS OF PROFESSIONAL RESPONSIBILITY

David Lorge Parnas
Danny Cohen

RESPONSE

David L. Parnas

It is unfortunate that Dr. Cohen has chosen to attack the critics of SDI rather than their arguments. It is more unfortunate that he has chosen to base his arguments on false assumptions about their positions. The following six statements are intended to set the record straight.

1. Responsible opponents to SDI do not oppose the goal attributed to SDIO by Dr. Cohen, "free us from the danger of nuclear holocaust," or that stated by President Reagan, "make nuclear weapons impotent and obsolete." Many SDI opponents have campaigned for similar goals for decades. The arguments made against SDI are based on the inability of technology to accomplish those goals, not their undesirability.
2. No responsible professional would claim that professionals are not mortals—even on "their turf." We claim no infallibility but give the public information and opinions to the best of our ability. In contrast, several supporters of SDI have stated that their information and expertise is available only to the government, not the public.
3. No critic of SDI has ever suggested that a BMD [Ballistic Missile Defense] system is now being deployed. However, SDIO's official charter calls upon SDIO to undertake "a comprehensive program to develop key technologies . . . move the United States towards its ultimate goal of a thoroughly reliable defense." The SDIO charter, and its progress reports, makes it clear that the program is a development program, not a research program as Dr. Cohen suggests. Dr. Cohen knows that SDI is officially classified as advanced development. (6.3).
4. At no point before or during the initial meeting of the SDIO Panel on Computing in Support of Battle Management, which later renamed itself the "Eastport Group," did I believe I have a solution, present a solution, or have a proposal rejected. In public debates, Dr. Cohen has been asked to describe the solution he claims I presented, but was unable to do so.

   I was asked to inform the panel about the work I have done on weapon delivery software; I presume that it was this work that led to my invitation to join the panel. Unaware that my information would be perceived as a proposal, and unaware that the panel had rejected it, I did not feel the anger attributed to me by Dr. Cohen. Even today, I do not consider comments about the broad applicability of my work to be pejorative.

employed by some contractors. Unfortunately, this is true for every profession and every field of human activity. Obviously, this should be fought against. Prof. Parnas's error is the consequent conclusion that because such people are involved in SDI, the program cannot succeed ("the blind led by those with their eyes shut"). In fact, most good activities accomplished by human beings (from medicine and welfare to space flights) are accomplished within and despite this truth; this should not be used to conclude that we cannot do anything useful until the earth is populated only by good and smart people.

Somehow it happened that words like "responsible," "concerned," and "conscious" are monopolized by the opponents of the SDI program. One may get the feeling that Soviet nuclear warheads, like the California condor, should be preserved and never be shot at.

Are we more safe with our security in the heads of our adversaries or in our own hands? Those who preach about the dangers of miscalculation, misunderstanding, overreaction, and the danger of accidental nuclear war—neglect all these arguments when it comes to our ability to *defend* ourselves rather than our "ability" to *deter* our enemies.

The question we *should* be asking is, "If we have *any* reason to believe that we might have it in our power to prevent 'The Day After' from happening, what kind of people are we if we don't have the patience, the commitment—the *humanity* to do so?"

The president has pointed out that the purpose of the SDI program is not to build a fully capable anti-ballistic system now, but rather to conduct research to support an informed decision by *another* president and *another* Congress sometime in the future—perhaps not before the turn of the century.

Our approach to solving this family of problems must be to attack it with a family of solutions. Since it seems unlikely that there exists any single solution to this thicket of problems, our objective must be to find that combination of answers that offers the greatest synergism and the highest leverage in the sum of its individual approaches.

SUMMARY

Professionals have the right and the obligation to guide the public in their areas of expertise. They also have the obligation to alert the public to the fact that their speculations are not more profound than those by laymen. They should present their knowledge and learned results, and not neglect to describe their limitations.

Professionals, more than laymen, have the responsibility of not letting their *opinions* (e.g., about desirability) drive their *judgment* (e.g., about feasibility), and *not* follow the queen's practice in *Alice in Wonderland,* "Sentence First—Verdict Afterwards," as many have demonstrated.

SDI: ONE VIEW OF PROFESSIONAL RESPONSIBILITY*

David Lorge Parnas

INTRODUCTION

In May of 1985 I was asked by the Strategic Defense Initiative Organization, the group within the Office of the U.S. Secretary of Defense that is responsible for the "Star Wars" program, to serve on a $1,000(US)/day advisory panel, the SDIO Panel on Computing in Support of Battle Management. The panel was to make recommendations about a research and development program to solve the computational problems inherent in space-based defense systems.

Like President Reagan, I consider the use of nuclear weapons as a deterrent to be dangerous and immoral. If there is a way to make nuclear weapons impotent and obsolete and end the fear of nuclear weapons, there is nothing I would rather work on. However, two months later I had resigned from the panel. I have since become an active opponent of the SDI. The purpose of this article is to explain why I am opposed to the program. I begin by stating my personal views on defense work and professional responsibility.

MY VIEW OF PROFESSIONAL RESPONSIBILITY

My decision to resign from the panel was consistent with long-held views about the individual responsibility of a professional. I believe that professionals have responsibilities that go beyond an obligation to satisfy the short-term demands of their immediate employer.

As a professional:

1. I am responsible for my own actions and cannot rely on any external authority to make my decisions for me,

2. I cannot ignore ethical and moral issues. I must devote some of my energy to deciding whether the task that I have been given is of benefit to society,

3. I must make sure that I am solving the real problem, not simply providing short-term satisfaction to my supervisor.

 This paper originally appeared in *Abacus* 4 (Winter 1987): 46-52, as "SDI: A Violation of Professional Responsibility." Dr. Parnas addressed the issues raised in this paper in a presentation to the IGCC Faculty Seminar on International Security, University of California, San Diego, February 19, 1987.

Some have held that a professional is a "team player" and would not "blow the whistle" on his colleagues and employer. I disagree. As the Challenger incident demonstrates, such action is sometimes necessary. One's obligations as a professional precede other obligations. One must not enter into contracts that conflict with one's professional obligations.

MY VIEWS ON DEFENSE WORK

Many opponents of SDI oppose all military development. I am not one of them. I have been a consultant to the Department of Defense and other components of the defense industry since 1971. I am considered an expert on the organization of large software systems and I lead the U.S. Navy's Software Cost Reduction project at the Naval Research Laboratory. Although I have friends who argue that "people of conscience" should not work on weapons, I maintain that it is vital that people with a strong sense of social responsibility continue to work within the military industrial complex. I do not want to see that power completely in the hands of people who are not conscious of social responsibility.

My own views on military work are close to those of Albert Einstein. Einstein, who called himself a militant pacifist, at one time held the view that scientists should refuse to contribute to arms development. Later in his life he concluded that to hold to a "no arms" policy would be to place the world at the mercy of its worst enemies. Each country has a right to be protected from those who use force, or the threat of force, to impose their will on others. Force can morally be used only against those persons who are themselves using force. Weapons development should be limited to weapons that are suitable for that use. Neither the present arms spiral nor nuclear weapons are consistent with Einstein's principles. One of our greatest scientists, he knew that international security requires progress in political education, not weapons technology.[1]

WHAT IS SDI?

SDI, popularly known as "Star Wars," was initiated by a 1983 presidential speech calling on scientists to free us from the fear of nuclear weapons. President Reagan directed the Pentagon to search for a way to make nuclear strategic missiles impotent and obsolete. In response, SDIO has embarked upon a project to develop a network of satellites carrying sensors, weapons, and computers to detect ICBMs and intercept them before they can do much damage. In addition to sponsoring work on the basic technologies of sensors and weapons, SDI has funded a number of Phase I "architecture studies," each of which proposes a basic design for the system. The best of these have been selected and the contractors are now proceeding to "Phase II," a more detailed design.

THE RELIABILITY ISSUE

Many of the critics repeat the argument that the expected SDI system will not be reliable due mainly to the impossibility of complete full-scale realistic testing.

This is a very important point. It is interesting that the same media that criticize SDIO on this point also criticize SDIO for its attempts to conduct simulations, experiments, and validation efforts through its future National Test Bed.

It would be more responsible not to raise the issue in a vacuum, but instead in the context of defense systems in general.

None of our major defense systems has ever been fully tested in realistic conditions—and, thank God, neither was any of our adversaries'. Many remind us that we test our ICBMs only on east to west flights (from California to Kwajalein) and have no *proof* of their ability to navigate over the pole. Luckily the same holds true for the Soviet, too (except that they fly from west to east).

We have never conducted a realistic full-scale test of our strategic forces, of NORAD, or of our strategic Attack Warning system, and I hope that we never will. Thinking about these issues does not make one feel good about defense systems in general. Does it? Does this imply that we should not develop *any* major defense system because by definition it can never be fully tested in realistic conditions? Obviously not.

We have never tested a nuclear warhead on an ICBM, but for the sake of knocking SDI the critics trust these untested ICBMs as the cornerstone of our security.

Pointing to these issues as faults unique to the SDI system is misleading and not necessarily of high professional responsibility. It implies to the general public that the government is about to replace defense systems that were fully tested under the most realistic conditions (and hence are of the utmost reliability and stability) by an unreliable system.

Those who raise the important issue of reliability should have the professional responsibility to raise it in the proper context.

The "technical" debate about the doability/trustworthiness/etc., is reminiscent of the debates in the 1950s and the 1960s about the doability/trustworthiness/etc., of the ICBMs. Many of the "responsible" professionals of those days argued about the undoability of inertial navigation. Then, as now, opinions led many who wrapped themselves in their professional credentials and claimed to "know" that it was technically impossible.

SOME KEY QUESTIONS

I believe that Prof. Parnas managed to find incompetent people who work for the Defense Department and for SDIO (like the person who argued in favor of 100,000 errors). I also believe that there are dishonest people

ABOUT ANOTHER DEFENSE SYSTEM

Gregory Fossedal has pointed out that the current criticism of SDI resembles British arguments against air-defense measures before World War II:

> In the 1930s, opponents of a British defense against German attack argued that a few firebombs could result in a "total holocaust" of London, as one member of Parliament put it. "The bomber will always get through," said Prime Minister Stanley Baldwin. Hence, they argued any defense was useless.
>
> Winston Churchill, then a discredited backbencher, saw the folly of this reasoning and decided, given that no defense is ever perfect, to see what kinds of defenses could be built. "Science is always able to provide something" he wrote in a memo in 1935.
>
> The key he said was not scientific at all, but political. "General tactical considerations, and what is technically feasible act and react upon one another. Thus, the scientists should be told what facilities the air force would like to have, and airplane design be made to fit into and implement a definite scheme of warfare."
>
> Thanks to Mr. Churchill's efforts, private scientists were able to design and build defenses—despite furious objection from Air Ministry bureaucracy. By seeing the strategic error of demanding perfection of defense, Mr. Churchill knew that the opinion of scientists who opposed him wasn't so much wrong as it was irrelevant. In fact British air defense concentrated on rapidly deploying what was available, knowing that more exotic technologies, such as radar, would come along later.[1]

Those who found the idea of air defense impossible had the professional responsibility and the right not to work on the project, just as those who preferred to pursue it had the professional responsibility and the right to work toward that goal.

Each group should respect the rights of the other. Unfortunately, this courtesy is not always followed.

---

[1]From Gregory Fossedal, "A Common Thread Linking Star Wars," *Washington Times,* 23 December 1986.

MY EARLY DOUBTS

As a scientist, I wondered whether technology offered us a way to meet these goals. My own research has centered on computer software and I have used military software in some of my research. My experience with computer-controlled weapon systems led me to wonder whether any such system could meet the requirements set forth by President Reagan.

I also had doubts about conflict of interest. I have a project within the U.S. Navy that could benefit from SDI funding. I suggested to the panel organizer that this conflict might disqualify me. He assured me that if I did not have such a conflict, they would not want me on the panel. He pointed out that the other panelists, employees of defense contractors and university professors dependent on DoD funds for their research, had similar conflicts. Readers should think about such conflicts the next time they hear of a panel of "distinguished experts."

MY WORK FOR THE PANEL

The first meeting increased my doubts. In spite of the high rate of pay, the meeting was poorly prepared; presentations were at a disturbingly unprofessional level. Technical terms were used without definition; numbers were used without supporting evidence. The participants appeared predisposed to discuss many of the interesting, but tractable, technical problems in space-based missile defense while ignoring the basic problems and "big picture." Everyone seemed to have a pet project of their own that they thought should be funded.

At the end of the meeting we were asked to prepare position papers describing research problems that must be solved in order to build an effective and trustworthy shield against nuclear missiles. I spent the weeks after the meeting writing up those problems and trying to convince myself that SDIO-supported research could solve those problems. I failed! I could not convince myself that it would be possible to build a system that we could trust or that it would be useful to build a system that we did not trust.

WHY TRUSTWORTHINESS IS ESSENTIAL TO PRESIDENT REAGAN'S GOALS

If the U.S. does not trust SDI it will not abandon deterrence and nuclear missiles. Even if the U.S. did not trust its shield, the USSR could not assume that SDI would be completely ineffective. Seeing both a "shield" and missiles, it would feel impelled to improve its offensive forces in an effort to

compensate for SDI. The U.S., not trusting its defense, would feel a need to build still more nuclear missiles to compensate for the increased Soviet strength. The arms race would speed up. Further, because NATO would be wasting an immense amount of effort on a system it couldn't trust, we would see a weakening of our relative strength. Instead of the safer world that President Reagan envisions, we would have a far more dangerous situation. Thus, the issue of our trust in the system is critical. Unless the shield is trustworthy, it will not benefit any country.

THE ROLE OF COMPUTERS IN "STAR WARS"

SDI discussions often ignore computers, focusing on new developments in sensors and weapons. However, the sensors will produce vast amounts of raw data that computers must process and analyze. Computers must detect missile firings, determine the source of the attack, and compute the attacking trajectories. Computers must discriminate between threatening warheads and decoys designed to confuse our defensive system. Computers will aim and fire the weapons. All the weapons and sensors will be useless if the computers do not function properly. Software is the glue that holds such systems together. If the software is not trustworthy, the system is not trustworthy.

THE LIMITS OF SOFTWARE TECHNOLOGY

Computer specialists know that software is always the most troublesome component in systems that depend on computer control. Traditional engineering products can be verified by a combination of mathematical analysis, case analysis, and prolonged testing of the complete product under realistic operating conditions. Without such validation, we cannot trust the product. None of these validation methods works well for software. Mathematical proofs verify only abstractions of small programs in restricted languages. Testing and case analysis sufficient to ensure trustworthiness take too much time. As E.W. Dijkstra has said, "Testing can show the presence of bugs, never their absence."

The lack of validation methods explains why we cannot expect a real program to work properly the first time it is really used. This is confirmed by practical experience. We can build adequately reliable software systems, but they become reliable only after extensive use in the field. Although responsible developers perform many tests, including simulations, before releasing their software, serious problems always remain when the first customers use the product. The test designers overlook the same problems as the software designers overlook. No experienced person trusts a software system before it has seen extensive use under actual operating conditions.

The American public is exposed time and again to "experts" claiming that the SDI system cannot be accomplished because of technical difficulties. This is not the first time that experts predicted that certain things are impossible.

For example, in 1937, Prof. Hans Bethe published a short article in which he mathematically proved that "The Maximum Energy Obtained from the Cyclotron" (*Physical Review*, Vol. 52) is about 10 MV for protons, a limit that has already been exceeded by many orders of magnitude.

Incidentally, his theoretically proven limit had been exceeded even before the article was published. It was not that his mathematics was wrong—he just did not realize all the possible ways of accomplishing it.

Bethe's limited vision erred in two ways: (1) The cyclotron itself was developed, by additional invention and development, to the "synchrocyclotron" with energies in excess of 200 MeV for protons; and (2) a wholly new device, the "synchrotron," was invented *to accomplish the same purpose*, that is capable of at least 2,000,000 times the "limit" Bethe "proved" in accelerating protons.

When professionals make claims about impossibilities, they have the responsibility to clarify whether their claims apply only to the methods that they examine or to all possible methods, including those that they do not envision.

The public, guided by the professionals, has the right to know the difference. It is unfortunate that the critics of SDI do not fulfill this part of their obligation as well.

Those who claimed that "you cannot hit a bullet with a bullet" (i.e., hit a reentry vehicle with a missile) never revisited the issue (at least not in public) after repeated experiments proved the possibility of doing just that.

Prof. Parnas stated that "To do that, satellite clocks will have to be accurately synchronized. None of this can be done when the network's components and communication links are unreliable." This is a typical classic mistake of predicting future technical capabilities based on what one knows today, and approaching problems with "how would I do it," a mistake that professionals are expected to avoid. Even laymen, having access only to public unclassified information, can find out that satellites already keep time within a few nanoseconds (with drift of about 3μsec per year) using today's technology. Laboratory systems have already improved this by an order of magnitude. I dare not predict what would be possible beyond the mid-1990s. This simple example shows that being a professional in one field is not an expert-license for all domains.

intensive-care unit in a hospital, for example, and not addressing the special properties and problems of the SDI system.

We, the rest of the panel, could understand his anger with our response, but were surprised by his convenient recollection of the event as one in which "Everyone seemed to have a pet project of their own."

Prof. Parnas is correct in reporting that the Eastport panel did not react with "serious and scientific discussion of the technical problems that I [Prof. Parnas] raised." The Eastport panel, like many others, found the issues that Prof. Parnas raised in the minipapers that followed his resignation letter to be *irrelevant.* For example, one of them is, "Can automatic programming solve the SDI software problem?" In it Prof. Parnas observes that "claims that have been made for automatic programming systems are greatly exaggerated." This would be relevant if SDIO (or even just the Eastport panel) had advocated the inverse, that automatic programming will solve the SDI software problem.

The Eastport panel was, in fact, astonished at the irrelevance of nearly all the topics of these minipapers, and concluded that he had used the occasion to voice all his pet opinions.

Since the subject of this publication is *professional responsibility,* it is not the right forum for arguing against the points that Prof. Parnas raises.

THE DICHOTOMY

A few months ago a reporter called me about SDI. When I identified myself as a supporter of the program he said, "This means that you believe that it is possible."

This typical comment is due to the existing dangerous dichotomy in the country about SDI. There are those who find it desirable, and therefore worth the effort of finding out how to pursue it, and there are those who find it undesirable and therefore "know" that it is impossible, and that no research has the potential to further our knowledge on the subject.

Here is where professionals enter the picture. The general public and the media feel helpless confronting the technical issues, and are looking up to the professionals to provide guidance.

Professionals have the right and the obligation to guide the public. However, they also have the responsibility to alert the public when they step out of their area of expertise. For example, when a dentist (or a physicist, or a "responsible computer professional") discusses what the Soviet Union would do in response to the SDI, the public has the right to know that this is speculation rather than professional opinion.

WHY SOFTWARE FOR SDI IS ESPECIALLY DIFFICULT

SDI is far more difficult than any software system we have ever attempted. Some of the reasons are listed below. A more complete discussion can be found in "Software Aspects of Strategic Defense Systems."[2]

SDI software must be based on assumptions about target and decoy characteristics; those characteristics are controlled by the attacker. We cannot rely upon our information about them. The dependence of any program on those assumptions is a rich source of effective countermeasures. Espionage could render the whole multi-billion-dollar system worthless without our knowledge. It could show an attacker how to exploit the inevitable differences between the computer model on which the program is based and the real world.

The techniques used to provide high reliability in other systems are hard to apply for SDI. In space, the redundancy required for high reliability is unusually expensive. The dependence of SDI on communicating computers in satellites makes it unusually vulnerable. High reliability can be achieved only if failures of individual components are statistically independent; for a system subject to coordinated attacks, that is not the case.

Overloading the system will always be a potent countermeasure because any computer system will have a limited capacity and even crude decoys would consume computer capacity. An overloaded system must either ignore some of the objects it should track, or fail completely. For SDI, either is catastrophic.

Satellites will be in fixed orbits that will not allow the same one to both track a missile from its launch and destroy it. Responsibility for tracking a missile will transfer from one satellite to another. Because of noise caused by the battle and enemy interference, a satellite will require data from other satellites to assist in tracking and discrimination. The result is a distributed real-time data base. For the shield to be effective, the data will have to be kept up-to-date and consistent in real-time. To do that, satellite clocks will have to be accurately synchronized. None of this can be done when the network's components and communication links are unreliable; unreliability must be expected during a real battle in which an enemy would attack the network. Damaged stations are likely to inject inaccurate or false data into the data base.

Realistic testing of the integrated hardware and software is impossible. Thorough testing would require "practice" nuclear wars including attacks that partially damage the satellites. Our experience tells us that many potential problems would not be revealed by lesser measures such as component testing, simulations, or small-scale field tests.

Unlike other weapon systems, there will be no opportunity to modify

the software during or after its first battle. It must work the first time.

These properties are inherent in the problem, not a particular system design. As we will see below, they cannot be evaded by proposing a new system structure.

MY DECISION TO ACT

After reaching the conclusions described above, I solicited comments from other scientists and found none that disagreed with my technical conclusions. Instead, they told me that the program should be continued, not because it would free us from the fear of nuclear weapons, but because the research money would advance the state of computer science. I disagree with that statement, but I also consider it irrelevant. Taking money allocated for developing a shield against nuclear missiles, while knowing that such a shield was impossible seemed, to me, to constitute fraud. I did not want to participate and submitted my resignation. I felt it would be unprofessional to resign without explanation and submitted my position papers to support my letter. I sent copies to a number of government officials and friends but did not send them to the press until they had been sent to reporters by others. They have since been widely published.[2]

SDIO'S REACTION

The SDIO's reaction to my resignation transformed my stand on SDI from a passive refusal to participate, to an active opposition. Neither SDIO nor the other panelists reacted with a serious and scientific discussion of the technical problems that I raised.

The first reaction came from one of the panel organizers. He asked me to reconsider, but not because he disagreed with my technical conclusions. He accepted my view that an effective shield was unlikely, but argued that the money was going to be spent and I should help to see it well spent. There was no further reaction from SDIO until a *New York Times* reporter called. Then, the only reaction that I received was a telephone call demanding to know who had sent the material to the *Times*.

After the story broke, the statements made to the press seemed, to me, to be designed to mislead, rather than inform, the public. Examples are given below. When I observed that SDIO was engaged in "damage control," rather than a serious consideration of my arguments, I felt that I should inform the public and its representatives of my own view. I want the public to understand that no trustworthy shield will result from the SDIO-sponsored work. I want them to understand that technology offers no magic that will

The SDI is working now on *research and development* of the technology, not on *deploying* it. The answers to all questions about the performance of the SDI system depend on what the mission of the system would be, on what the future threat would be, and how (and if) we will deploy the system.

One may wonder about spending funds on developing the technology if these basic questions cannot be answered first. However, the only way to answer these questions intelligently is by starting from the knowledge about what the technology can do—knowledge that we do not yet have, about technology still under development.

The same situation is not unique to SDI. When scientists develop new wings for supersonic fighters it is too early to ask about their effect on the performance of the entire air defense system, before these wings are integrated into complete aircraft (such as the F-16) and before decisions are made about the deployment of these aircraft.

The SDIO realizes that it does not have all the answers yet, and even not all the questions. Therefore, it conducts its research in a variety of directions, and exposes every step to reviews and critique.

THE EASTPORT PANEL

In 1985, SDIO convened the Eastport panel to "devise an appropriate computational/communications response to the [strategic defense battle management] problem and make recommendations for a research and technology development program to implement the response."

The Eastport panel was not asked to be a "team player" and to rubber stamp everything that was presented to it—and it did not behave as such. The report of the panel criticized some aspects of the work performed for SDI in no uncertain terms (or "quite harsh" as Prof. Parnas said).

The panel met several times during 1985, for presentations and discussions, and its members performed related work between meetings. As the work progressed the panel chartered its way (rather than asking SDIO to direct its path), and chose the next steps of action.

Prof. Parnas was the only member that reached his conclusions before the second meeting. This is not the place to argue them. Having arrived at these conclusions, Prof. Parnas took the only possible action, and resigned from the panel.

In his description of the first meeting, Prof. Parnas recalls, "Everyone seemed to have a pet project of their own that they thought should be funded." This is true only about Prof. Parnas himself! In this first meeting he already *knew* the "solution," the right direction for SDIO to pursue. When he presented that pet of his to the rest of the panel, his general-purpose approach was immediately criticized as being equally applicable to an

SDI:
ANOTHER VIEW ON PROFESSIONAL RESPONSIBILITY*

Danny Cohen

INTRODUCTION

In March of 1983 President Reagan announced his goal to free us from the danger of nuclear holocaust. Within minutes the country was already polarized between supporters (who found the idea desirable) and opponents (who found the idea to be undesirable and contrived reasons why it would be technically impossible to attain).

Many professional organizations, such as physicists, physicians, and "responsible" computer scientists aligned themselves against the SDI.

Professionals have the responsibility to provide professional judgment and guidance. Is this responsibility restricted only to their domain of expertise, or does it apply to all areas of life?

It is my opinion that when professionals step off their turf, they cease to be "professionals" and become mortals, like the rest of us.

WHAT IS SDI?

The SDI (also known as "Star Wars") is a research program directed eventually to freeing us from the fear of nuclear disaster. The SDI is not building a "shield" as some depict it. It was not "sold" to the public as an umbrella that will be in use momentarily.

In January 1985, the Administration described the program as follows:

> [SDI's] purpose is to identify ways to exploit recent advances in ballistic missile defense technologies that have potential for strengthening deterrence—and therefore increasing our security and that of our Allies. The program is designed to answer a number of fundamental scientific and engineering questions that must be addressed before the promise of these new technologies can be fully assessed. The SDI research program will provide to a future President and a future Congress the technical knowledge necessary to support a decision in the early 1990s on whether to develop and deploy such advanced defensive systems.

eliminate the fear of nuclear weapons. I feel that to be part of my personal professional responsibility as a scientist and an educator.

Democracy can only work if the public is accurately informed. Most of the statements made by SDIO supporters seem designed to mislead the public. For example, one SDIO scientist told the press that there could be 100,000 errors in the software and it would still work properly. Strictly speaking this statement is true. If one picks one's errors very carefully, they won't matter much. However, a single error caused the complete failure of a Venus probe many years ago. I find it hard to believe that the SDIO spokesman was not aware of that.

Another panelist repeatedly told the press that there was no fundamental law of computer science that said the problem could not be solved. Again, strictly speaking, the statement is true but it does not counter my arguments. I did not say that a correct program was impossible; I said that it was impossible that we would trust the program. It is not impossible that such a program would work the first time it was used; it is also not impossible that 10,000 monkeys would reproduce the works of Shakespeare if allowed to type for 5 years. Both are highly unlikely. However, we could tell when the monkeys have succeeded; there is no way that we could verify that the SDI software was adequate.

Another form of disinformation was the statement that I, and other SDI critics, were demanding perfection. Nowhere have I demanded perfection. To trust the software we merely need to know that the software is free of catastrophic flaws, flaws that could cause massive failure or that could be exploited by a sophisticated enemy. That is certainly easier to achieve than perfection, but there is no way to know when we have achieved it.

A common characteristic of all these statements is that they argue with statements other than the ones that I published in my papers. In fact, in some cases SDIO officials dispute statements made by earlier panels or by other SDIO officials rather than debate the points that I made.

THE "90%" DISTRACTION

One of the most prevalent arguments in support of SDI suggests that if there are 3 layers, each 90% effective, the overall "leakage" would be less than 1% because the effectiveness multiplies. This argument is accepted by many people who do not have scientific training. However,

1. there is no basis for the 90% figure; an SDI official told me it was picked for purpose of illustration,
2. the argument assumes that the performance of each layer is independent of the others when it is clear that there are many links,

3. it is not valid to rate the effectiveness of such systems by a single "percentage." Such statistics are only useful for describing a random process. Any space battle would be a battle between two skilled opponents. A simple "percentage" figure is no more valid for such systems than it is as a way of rating chess players. The performance of defensive systems depends on the opponent's tactics. Many defensive systems have been completely defeated by a sophisticated opponent who found an effective counter-measure.

THE "LOOSE COORDINATION" DISTRACTION

The most sophisticated response was made by the remaining members of SDIO's Panel on Computing in Support of Battle Management, which named itself the Eastport group, in December. This group of SDI proponents wrote that the system structures proposed by the best Phase I contractors, those being elaborated in Phase II, would not work because the software could not be built or tested. They said that these "architectures" called for excessively tight coordination between the "battle stations," i.e., excessive communication, and they proposed that new Phase I studies be started. However, they disputed my conclusions, arguing that the software difficulties could be overcome using "loose coordination."[4]

The Eastport Report neither defines its terms nor describes the structure that it had in mind. Parts of the report imply that "loose coordination" can be achieved by reducing the communication between the stations. Later sections of the report discuss the need for extensive communication in the battle station network, contradicting some statements in the earlier section. However, the essence of their argument is that SDI could be trustworthy if each battle station functioned autonomously, i.e., without depending on help from others.

The Eastport group's argument is based on four unstated assumptions:

1. Battle stations do not need data from other satellites to perform their basic functions.
2. An individual battle station is a small software project that will not run into the software difficulties described above.
3. The only interaction between the stations is by explicit communication. This assumption is needed to conclude that test results about a single station allow one to infer the behavior of the complete system.
4. A collection of communicating systems differs in fundamental ways from a single system.

it." "The money will be spent, all you can do is make good use of it." "The system will be built, you cannot change that." "Your resignation will not stop the program."

It is true my decision not to toss trash on the ground will not eliminate litter. However, if we are to eliminate litter, I must decide not to toss trash on the ground. We all make a difference.

Similarly, my decision not to participate in SDI will not stop this misguided program. However, if everyone who knows that the program will not lead to a trustworthy shield against nuclear weapons refuses to participate, there will be no program. Every individual's decision is important.

It is not necessary for computer scientists to take a political position, they need only be true to their professional responsibilities. If the public were aware of the technical facts, if they knew how unlikely it is that such a shield would be effective, public support would evaporate. We do not need to tell the public not to build SDI. We only need to help them to understand why it won't be an effective and trustworthy shield.

References

1. Albert Einstein, Sigmund Freud, "Warum Krieg," Diogenes Verlag, Zuerich, 1972.

2. Parnas, D. L. "Software Aspects of Strategic Defense Systems," *American Scientist*, September-October 1985, pp. 432-440. Also published in German in *Kursbuch 83, Krieg und Frieden—Streit um SDI*, by Kursbuch/Rotbuch Verlag, March 1986, and in Dutch in *Informatie*, Nr. 3, March 1986, pp. 175-186.

3. Parnas, D. L. "On the Criteria to be Used in Decomposing Systems into Modules," Comm. ACM 15, 12, December 1972, pp. 1053-1058.

4. Eastport Group "Summer Study 1985," A Report to the Director—Strategic Defense Initiative Organization, December 1985.

5. "Wer Kuscht, hat Keine Chance," *Der Spiegel*, Nr. 47, 18 November 1985.

in research funding in significant amounts can be received only on the basis of defense-related appropriations."

SHOULD WE PURSUE SDI FOR REASONS OTHER THAN THE PRESIDENT'S?

I consider such rationalizations to be both unprofessional and dangerous. SDI endangers the safety of the world. By working on SDI, these scientists allow themselves to be counted among those who believe that the program can succeed. If they are truly professionals, they must make it very clear that an effective shield is unlikely and a trustworthy one impossible. The issue of more money for high technology should be debated without the smokescreen of SDI. I can think of no research that is so important that it justifies pretending that an ABM system can bring security to populations. Good research stands on its own merits; poor research must masquerade as something else.

I believe in research; I believe that technology can improve our world in many ways. I also agree with Professor Makowski of the Technion who wrote, "Overfunded research is like heroin, it leads to addiction, weakens the mind, and leads to prostitution." Many research fields in the U.S. are now clearly overfunded, largely because of DoD agencies. I believe we are witnessing the proof of Professor Makowski's statement.

MY ADVICE TO OTHERS ABOUT PARTICIPATION IN DEFENSE PROJECTS

I believe it quite appropriate for a professional to devote his energies to making the people of his land more secure. In contrast, it is not professional to accept employment doing things that do not advance the legitimate defense interests of that country. If the project would not be effective, or if, in his opinion, it goes beyond the legitimate defense needs of the country, a professional should not participate. Too many do not ask such questions. They ask only how they can get another contract.

It is a truism that if each of us lives as if what we do does matter, the world will be a far better place than it now is. The cause of many serious problems in our world is that many of us act as if our actions do not matter. Our streets are littered, our environment polluted, and children are neglected because we underestimate our individual responsibility.

The arguments given to me for continuation of the SDI program are examples of such thinking. "The government has decided, we cannot change

All of these assumptions are false!

1. The data from other satellites is essential for accurate tracking and for discriminating between warheads and decoys in the presence of noise.
2. Each battle station has to perform all the functions of the whole system. The original arguments apply to it. Each one is unlikely to work, impossible to test in actual operating conditions, and, consequently, impossible to trust. Far easier projects have failed.
3. Battle stations interact through weapons and sensors as well as through their shared targets. The weapons might affect the data produced by the sensors. For example, destruction of a single warhead or decoy might produce noise that makes tracking of other objects impossible. If we got a single station working perfectly in isolation, it might fail completely when operating near others. The failure of one station might cause others to fail because of overload. Only a real battle would give us confidence that such interactions would not occur.
4. A collection of communicating programs is mathematically equivalent to a single program. In practice, distribution makes the problem harder, not easier.

Restricting the communication between the satellites does not solve the problem. There is still no way to know the effectiveness of the system and it would not be trusted. Further, the restrictions on communication are likely to reduce the effectiveness of the system. I assume that this is why none of the Phase I contractors chose such an approach.

The first claim is appealing and reminiscent of arguments made in the 60s and 70s about modular programming.[3] Unfortunately, experience has shown that modular programming is an effective technique for making errors easier to correct, not for eliminating errors. Modular programming does not solve the problems described earlier in this paper. None of those arguments were based on an assumption of tight coupling; some of the arguments do assume that there will be data passed from one satellite to another. The Eastport Report, like earlier reports, supports that assumption.

The Eastport group is correct when it says that designs calling for extensive data communication between the battle stations are unlikely to work. However, the Phase I contractors were also right when they assumed that without such communication the system could not be effective.

THE ULTIMATE RESPONSE: REDEFINING THE PROBLEM

The issue of SDI software was debated in March 1986 at an IEEE Computer Conference. While two of us argued that SDI could not be trusted, the two SDI supporters argued that that did not matter. Rather than argue the computer science issues, they tried to use strategic arguments to say that a shield need not be considered trustworthy. One of them argued, most eloquently, that the president's "impotent and obsolete" terminology was technical nonsense. He suggested that we ignore what "the president's speechwriters" had to say and look at what was actually feasible. Others argue that increased uncertainty is a good thing—quite a contrast to President Reagan's promise of increased security.

In fact, the ultimate response of the computer scientists working on SDI is to redefine the problem in such a way that there is a trivial solution and improvement is always possible. Such a problem is the ideal project for government sponsorship. The contractor can always show both progress and the need for further work. Contracts will be renewed indefinitely!

Those working on the project often disparage statements made by the president and his most vocal supporters, stating that SDIO scientists and officials are not responsible for such statements. However, the general public remains unaware of their position and believe that the president's goals are the goals of those who are doing the scientific work.

IS SDIO-SPONSORED WORK OF GOOD QUALITY?

Although the Eastport panel was unequivocally supportive of continuing SDI, its criticisms of the Phase I studies were quite harsh. They assert that those studies, costing US$1,000,000 each, overlooked elementary problems that were discussed in earlier studies. If the Eastport group is correct, the SDIO contractors and the SDIO evaluators must be considered incompetent. If the Eastport group's criticisms were unjustified, or if their alternative is unworkable, their competence must be questioned.

Although I do not have access to much of the SDIO-sponsored work in my field, I have had a chance to study some of it. What I have seen makes big promises, but is of low quality. Because it has bypassed the usual scientific review processes, it overstates its accomplishments and makes no real scientific contribution.

DO THOSE WHO TAKE SDIO FUNDS REALLY DISAGREE WITH ME?

I have discussed my views with many who work on SDIO-funded projects. Few of them disagree with my technical conclusions. In fact, since

the story became public, two SDIO contractors and two DoD agencies have sought my advice. My position on this subject has not made them doubt my competence. Those who accept SDIO money give a variety of excuses. "The money is going to be spent anyway, shouldn't we use it well?" "We can use the money to solve other problems." "The money will be good for computer science." I have also discussed the problems with scientists at the Los Alamos and Sandia National Laboratories. Here, too, I found no substantive disagreement with my analysis. Instead, I was told that the project offered lots of challenging problems for physicists.

In November I read an interview with a leading German supporter of Star Wars. He made it clear that he thought of SDI as a way of injecting funds into high technology and not as a military project. He even said that he would probably be opposed to participation in any deployment should it come to pass.[5]

THE BLIND LED BY THOSE WITH THEIR EYES SHUT

My years as a consultant in the defense field have shown me that unprofessional behavior is common. When consulting, I often find people doing something foolish. Knowing that the person involved is quite competent, I may say something like "You know that's not the right way to do that." "Of course" is the response, "but this is what the customer asked for." "Is your customer a computer scientist? Does he know what he is asking?" ask I. "No" is the simple reply. "Why don't you tell him?" elicits the response, "At XYZ Corporation, we don't tell our customers that what they want is wrong. We get contracts."

That may be a businesslike attitude but it is not a professional one. It misleads the government into wasting taxpayers' money.

THE ROLE OF ACADEMIC INSTITUTIONS

Traditionally, universities provide tenure and academic freedom so that faculty members can speak out on issues such as these. Many have done just that. Unfortunately, at U.S. universities there are institutional pressures in favor of accepting research funds from any source. A researcher's ability to attract funds is taken as a measure of his ability.

The president of a major university in the U.S. recently explained his acceptance of a DoD institute on campus by saying, "As a practical matter, it is important to realize that the Department of Defense is a major administrator of research funds. In fact, the department has more research funds at its disposal than any other organization in the country . . . increases