The Heritage Foundation Backgrounder

No. 707 | The Heritage Foundation 214 Massachusetts Avenue N.E. Washington, D.C. 20002-4999 (202) 546-4400

May 12, 1989

MEETING THE CHALLENGE OF SDI BATTLE MANAGEMENT

INTRODUCTION

The Strategic Defense Initiative (SDI) raises many hopes: that nuclear war can be deterred without having to threaten devastating nuclear retaliation; that the United States actually can be defended from Soviet attack; and that the nightmare of nuclear war may fade.

For SDI to work, however, a deployed strategic defense system has to have a reliable network of communication links and computers to ensure that all parts of the system work together and that military commanders can contact the system during all phases of a battle.

This network, called a battle management system, would be responsible for such important tasks as coordinating the activities of sensors and weapons and providing communications between SDI hardware and its military commanders.

Incorrect Assertions. Critics of SDI have claimed that it is not feasible to design a complex SDI battle management system that will function properly against a massive ballistic missile attack launched by the Soviet Union against the U.S. Studies and press reports have argued this case, including a May 1988 report by the Office of Technology Assessment (OTA). This research arm of Congress found that there was a "significant probability" that a strategic defense system would suffer a "catastrophic failure" because of problems with the computer software of the battle management system. The OTA report concludes that the battle management system computer software requirements are so large and complex that the system would be unreliable.

The study also maintains that the communications links essential to effective battle management could be disrupted easily by Soviet electronic jamming.[1]

These assertions are incorrect. For one thing, critics fail to consider the security that can be given to the communications system by diversifying the means of communication. For another, the critics assume that the battle management system will depend on a single unified software package housed in the computers of a ground-based SDI command center. In fact, the battle management function may well be performed by many small computers with compartmentalized software packages dispersed in space on orbiting satellites and in numerous command centers on earth.

Maintaining Secure Communications. By increasing the number of computers and compartmentalizing the software into individual packages, an SDI battle management system will be decentralized, making it less vulnerable to catastrophic failure than a centralized system based on a single powerful computer system run by a unified software package. The reason: if one small part of the decentralized battle management system fails, the rest of the system will not fail with it because other computer systems will not be affected and thus can still send commands to weapons and sensors, maintaining open and secure lines of communication and coordinating and controlling the system in battle.

While the challenges involved in developing the battle management system for an overall strategic defense system are considerable, they are far from insurmountable. There are several steps that can address each of the ostensibly insuperable problems of developing a reliable SDI battle management system. These steps include:

♦ ♦ Decentralizing the SDI battle management system.

A highly centralized SDI battle management system based on a unified software package in a centralized computer system would be imprudent. The battle management system instead should be dispersed in a large number of ground-based and space-based computers with individual software packages. By decentralizing the battle management functions of SDI, the computer software can be less complex. This means that devising computer programs for SDI can be divided into smaller, more manageable problems. This will simplify vastly the task of designing computer software programs for SDI.

♦ ♦ Diversifying the battle management system's communications.

SDI must have secure lines of communication between weapons and military commanders. A highly centralized, interconnected communication system would be prone to catastrophic failure, like series lights on a Christmas tree, if one part went out or were destroyed. The alternative is a decentralized communication system. SDI's battle management system could be designed to use a number of different technologies, including lasers or

1 U.S. Congress, Office of Technology Assessment, *SDI: Technology, Survivability, and Software*, OTA-ISC-353 (Washington, D.C.: Government Printing Office, May 1988), pp. 4-5.

radio frequency transmitters, to increase the different kinds of communication channels and to diversify entire battle management system communications. This would make it much more difficult for the Soviets to find a single, inexpensive way to interrupt or jam the communications system with electronic devices.

♦ ♦ Tasking staff to make critical battle management decisions.

The system should be designed so critical battle management decisions, such as instructing the SDI system to initiate battle, would be made by men and women rather than machines. This would prevent the system from going into operation without a direct authorization from a military commander.

♦ ♦ Testing the battle management system through simulations of an actual attack.

Among the most important goals in designing SDI's battle management system is to demonstrate its reliability. Otherwise U.S. leaders could not be sure that SDI would work in war. This should be done by conducting exhaustive and realistic tests using computers to simulate different kinds of nuclear attacks on the U.S. Since a computer will not know whether a simulation is real or not, it will have to treat each simulation as the real thing, thereby giving SDI commanders an opportunity to test the reliability of SDI's computer software under realistic conditions.

THE ROLE OF BATTLE MANAGEMENT IN STRATEGIC DEFENSE

SDI's battle management system obviously is a key component of the overall SDI system. It would be responsible for providing critical information to sensors and weapons, communications between SDI's various components, and the means for human commanders to manage the overall system.

The battle management system would do a number of specific things. First, it would collect data generated by heat-seeking and other kinds of sensors that detect a launch of an enemy missile. These sensors would track missiles and warheads flying through space. Second, when enemy missiles came within range of SDI's weapons systems, either ground-based missile interceptors or small rockets placed on satellites in orbit, the battle management system would provide these weapons with the information they need to intercept their targets. Third, after the first round of SDI weapons were aimed and fired, the battle management system would compile information obtained from sensors such as the Boost Surveillance and Tracking System (BSTS) as to whether the targeted missile had indeed been destroyed.

Detecting Decoys. Fourth, the battle management system would collect data from the sensors tracking the missile or its remaining stages through space to determine which missiles were real and which were decoys and thereby avoid wasting shots in later stages of the defense. An enemy could, for example, load up a missile with a number of harmless "dummy" warheads, which could confuse the battle management system or overload it

with more tracking tasks than it could handle. Finally, the system would relay to commanders an assessment of which enemy missiles survived and which had been destroyed so that they could decide how to continue the battle.

To be effective, the battle management system has to function very rapidly and reliably. In the critical "boost-phase" period, for example, when enemy missiles are taking off, there are only four or five minutes in which to destroy them. After this, the missile's easily-detectable, heat-emitting plume disappears. The rest of the enemy attack could take less than 40 minutes. There would be little time for fixing problems in the system once it was in use.

The battle management system also must assess the course of the battle and communicate information critical to making the entire strategic defense system work, such as how many enemy missiles or reentry vehicles evaded the first round of attacks by SDI weapons. For this reason, reliable communications are a critical element of a flexible and responsive defense system.

COMPONENTS OF AN SDI BATTLE MANAGEMENT SYSTEM

SDI's battle management system would contain two components. The first would be an array of computers that controlled the various elements of the overall SDI system, along with human commanders. Each of these computers would contain software to direct the computer to make decisions during battle, including directing sensors to track certain target missiles, targeting weapons against specific enemy missiles, and timing the release of the weapons.

The exact location of these computers would depend on the kind of SDI system deployed. In one possible system, called "Brilliant Pebbles," many of the computers would be housed within the interceptor satellites themselves. "Brilliant Pebbles" is a new strategic defense concept, involving the deployment of thousands of small and relatively cheap satellite interceptors that contain no explosive warhead and destroy enemy missiles shortly after takeoff by smashing into them.

Complex Minicomputers. The tiny projectiles have been dubbed "brilliant" because they operate on their own without much central guidance. The computers for "Brilliant Pebbles" would be small and light, capable of performing complex computations in hostile environments, even in the radioactive environment caused by exploding enemy missile warheads. The software directing these computers would tell them such things as the locations of both weapons and targets, when to release SDI weapons, and where to direct the weapons based on information received from sensors and human commanders.

The second component of the SDI battle management system is an integrated communications system to allow the various components of the overall SDI system to "talk" with each other, with human commanders of SDI, and with systems embedded in U.S. missiles. This communications

system would provide SDI heat-seeking and other sensors and weapons (such as interceptor satellites and ground-based missiles) with the information required for proper coordination of the overall system. The communication system must work in a hostile environment, and it must not be easily disrupted either by enemy electronic jamming or by interference caused by nuclear explosions. Laser and radio frequency transmitters are being explored as the means for providing secure communications. The SDI communications system also is likely to employ a number of different channels to ensure security and reliability. Brilliant Pebbles, for example, is expected to use two separate channels on two different kinds of transmitters – based possibly on laser and radio frequency technology.

IS IT POSSIBLE TO DESIGN A RELIABLE SDI BATTLE MANAGEMENT SYSTEM?

The main criticism of the SDI battle management system contends that the required computer software would be too long and complex to work reliably. The trouble is that these criticisms by Congress's Office of Technology Assessment (OTA) and others are not based on an evaluation of any specific battle management system; such a system, after all, does not exist. The criticisms, rather, are of a general nature, based on an analysis of existing computer software capabilities and trying to imagine how these capabilities might fare under the most rigorous requirements of a strategic defense system.

Opportunity for Error. The conclusions of the critics rest on several assumptions. First, critics assume that the computer software required for a strategic defense system and its battle management functions will be very large and exceedingly complex. Estimates of the amount of computer software needed have ranged as high as 100 million lines of computer code.[2] A line of computer code is a rough measurement of computer software complexity. It refers to a single command to the computer to perform some operation. The U.S. long distance telephone system, by comparison, requires 50 million lines of computer code. Were the estimate correct for the SDI battle management computer system, it would require the largest and most complex body of software ever devised. The larger and more complex a computer system, the greater the opportunity for errors. The critics thus argue that dependable software for the SDI battle management system is unattainable. The OTA study concludes that:

> The nature of software and experience with large, complex software systems indicate that there may always be irresolvable questions about how dependable BMD [ballistic missile defense] software would be and about the confidence the United States could place in dependability

2 M. Mitchell Waldrop, "Resolving the Star Wars Software Dilemma," *Science*, May 9, 1986, p. 710.

> estimates. Existing large software systems, such as the long-distance telephone system, have become highly dependable only after extensive operational use and modification. In OTA's judgement, there would be a significant probability (i.e., one large enough to take seriously) that the first (and presumably only) time the BMD system were used in a real war, it would suffer a catastrophic failure.[3]

The OTA statement of a "significant probability" of failure was a professional statistician's usage of the term, and should not be interpreted to mean the same thing as the likelihood of failure. Press reports of the OTA study misinterpreted this. OTA clearly did not say that SDI would fail.[4] It is fair to say though that, because of this and other alleged problems with an SDI battle management system, many critics of SDI believe that the battle management system would be likely to fail.[5] They believe that deploying strategic defenses is not practical because of this inevitable unreliability.

Disrupting Communications. A second assumption of the critics is that the SDI communications system could be disrupted easily and thus could fail. Secure, reliable communications, of course, would be essential to the operation of SDI's battle management system. Battle management computers process information provided them by the communications system. If the computers did not receive this information, the battle management computers could not perform their missions, and important battle actions, such as the interception of targeted enemy missiles, would not be performed. This has led critics to assert that disrupting the communications of such space-based elements as weapons and sensors placed on orbiting satellites would be an easy, cost-effective way to neutralize the strategic defense system.

A third assumption of the critics is that a centralized, computer-controlled battle management system could initiate battle erroneously, with catastrophic results. They argue that the time available to begin the engagement of enemy missiles after takeoff is very short, perhaps four or five minutes. The need for rapid reaction by the defense in this so-called boost phase has led some experts to speculate that the decision to open fire must be made by a computer, rather than a human. This raises the possibility that the country could go to war because of computer error. It is argued further that the erroneous triggering of the SDI system would be similar to an accidental launch of nuclear missiles.

---

3 Office of Technology Assessment, *op.cit.*; catastrophic failure is arbitrarily defined by OTA as a decline of 90 percent or more in system performance.

4 Kim R. Holmes, "The Strategic Defense Initiative: Myth and Reality," Heritage Foundation *Backgrounder* No. 664, July 26, 1988, p. 2.

5 David L. Parnas, "Software Aspects of Strategic Defense Systems," *American Scientist*, September-October, 1985, p. 435; Herbert Lin, "The Development of Software for Ballistic-Missile Defense," *Scientific American*, December 1985, p. 53.

Finally, critics assume that the only way to prove the reliability of an SDI battle management system is to operate it in battle under realistic war conditions. They assert that peacetime testing on computers cannot anticipate the wide variety of stressful situations that could confront such a large, complex system. They maintain that reliability certainly could be achieved only by the use of the system over an extended period of time. They point out that a strategic defense system might have to deal with large numbers of enemy missile launches, an environment disrupted by numerous nuclear explosions, and unforeseen enemy countermeasures such as deploying in space decoys simulating warheads. Because these conditions have never been experienced, the critics do not believe that realistic simulations can be devised.

FEASIBILITY OF AN EFFECTIVE SDI BATTLE MANAGEMENT SYSTEM

To evaluate these criticisms properly, it is important to look at some of the key variables or alternatives in developing an SDI battle management system. The critics, for the most part, fail to take them into account. The most important of these variables is the possibility of decentralizing the SDI battle management system.

Most critics assume that battle management software will be written for a centralized computer system. In such a system, a central computer would gather information from all of the system's sensors and tightly coordinate the firing of many different types of weapons in space and on earth. This computer would be placed on the ground but linked with supporting computers on orbiting satellites in space. Early studies of strategic defense did assume that centralized battle management would be best, since it would maximize the efficiency of the weapons by preventing two weapons from shooting at the same target. In actual operation, a highly centralized system would be rigid and prone to failure if it suffered damage in battle or contained software errors.

Preferred by the Pentagon. Development of SDI, however, no longer is confined to the assumption that the battle management system must be centralized. "Brilliant Pebbles," for example, uses very decentralized computers housed in thousands of small, cheap, and fully autonomous space-based interceptors in low-earth orbit.[6]

6 The capabilities of Brilliant Pebbles include the following: a surveillance and tracking system capable of converting data on enemy missiles into video images (called a wide-field-of-view video imaging system); an on-board computer as powerful as a CRAY-1 computer, one of the most capable computers in the world; a radar capable of making actual images of enemy missiles for purposes of surveillance and tracking; and a communications system to receive instructions from commanders on the ground. Department of Defense, Strategic Defense Initiative Organization, *1989 Report to the Congress on the Strategic Defense Initiative* (Washington, D.C.: SDIO, March 1989), p. 5.3-3.

The decentralized approach to SDI battle management, in fact, long has been preferred by the Pentagon managers at the SDI program. The idea of a decentralized battle management system goes back to a 1985 study by the Pentagon-sponsored Eastport Study Group.[7] This study concluded that a widely distributed, hierarchical battle management system would be more reliable than a centralized system.

Hierarchical Structure. The system envisioned by the Eastport Study and subsequently adopted by the Pentagon's Strategic Defense Initiative Organization (SDIO) is arranged, much like a U.S. military command structure, with many small, independent battle groups. Each group would report to a higher unit in the system, much as a private reports to a sergeant. Each battle group would consist of a group of sensors and weapons responsible for the defense of a certain area, which could be a pre-designated sector in space or some zone of air space over U.S. or allied territory. The battle group would process sensor data, track missiles, missiles stages, or warheads, aim and fire its weapons, and determine afterwards which targets had been destroyed. It would not require a continuous stream of detailed instructions from a central battle management computer because it would be concerned only with the battle in its own sector. Thus, it would only need to report a summary of its own activities to the next higher unit in the system.

While Brilliant Pebbles is just one example of what could be a host of options for developing a decentralized SDI system, the fact that it is an option receiving close scrutiny by SDI researchers and scientists demonstrates that the centralized battle management system attacked by critics is not the only option.

A Decentralized System

Many problems associated with the complexity of SDI's battle management software can be overcome by designing a decentralized battle management system. A decentralized battle management system promises to simplify the task of uniting computer software for an SDI battle management system. Reducing the amount of coordination needed in the system, and hence the chances of failure, would mean that the complexity of the battle management software, too, could be reduced. This is because software would have to be written for smaller, more numerous computers, instead of a huge, highly centralized one requiring an enormous degree of coordination. The Brilliant Pebbles concept, for example, would grant essentially complete autonomy to the individually deployed interceptors by housing all the necessary computing and communications capabilities on board the interceptor satellite.

To be sure, a decentralized battle management system would reduce efficiency by permitting two different interceptor satellites to shoot at the same target. Yet according to a preliminary analysis by the Eastport Study

7 Eastport Study Group, "Report to the Director, Strategic Defense Initiative Organization," Washington, D.C., 1985.

Group, even with a completely decentralized strategic defense system, with no coordination of the individual weapons, only 20 percent more weapons would be needed to make the decentralized system as effective as one that was perfectly coordinated in a centralized system.[8]

A decentralized battle management system would ease the growing pains of a SDI system deployed in phases. A SDI system of necessity will be deployed in phases over many years. This requires a battle management system that is flexible and adaptable. Some SDI critics believe that, as a battle management computer software is modified and expanded over the years, its complexity will become unmanageable. However, a decentralized system would facilitate the introduction of new weapons, sensors, and other changes. This is because new weapons and sensors could be phased in, one system at a time, and not, as with a centralized system, all at once. The largely autonomous individual elements of a decentralized system could be widely varied, reflecting different technologies over time and tied together by a common communications network.

Simpler Testing

A decentralized battle management system would make testing the computer software easier. Properly testing the software of a centralized battle management system would present enormous difficulties. Errors in so complex a system, for example, could be very difficult to locate during testing by computers. In contrast, a decentralized approach would simplify testing greatly. A highly decentralized system, such as Brilliant Pebbles, would divide the computer programs needed to run the battle management system into small packages. These would be easier to test and to correct. If it could be demonstrated that the individual elements of a decentralized system worked, then it would be much more likely that the entire system also would function properly. A decentralized approach would enable SDI commanders to avoid the risks associated with a centralized computer system, in which one small problem in a part of the system could cripple whole operation.

Less Computer Software. A decentralized battle management system would reduce the volume of computer software required. With a decentralized battle management system, the Strategic Defense Initiative Organization estimates that 20 million to 40 million lines of code would be needed for the software for a strategic defense system. Of that, battle management software would require an estimated four million to six million lines of code.[9] The Marshall Institute calculates no functional package, such as that required for intercepting warheads after they reenter the atmosphere, would have more than 100,000 lines of code and that several would use no

8 *Ibid.*

9 U.S. Congress, Hearings before the Defense Subcommittee of the House Committee on Appropriations, *Department of Defense Appropriations for 1988, Part 6* (Washington, D.C.: Government Printing Office, 1987), p. 1098.

more 10,000 lines of code. They also estimate that well under two million lines of code would be needed for that phase of space-based defense in which enemy missiles are destroyed in the first minutes after takeoff (called the boost-phase).[10] This compares with the over 100 million lines of code that SDI critics charge will be required for the system.

A volume of software similar to that required for a decentralized battle management system, some four million to six million lines of code, is used in other military systems. Private estimates are that the Brilliant Pebbles system will require just 700,000 lines of computer code overall, with between 100,000 and 200,000 lines of code to run the computers housed in the interceptors.[11]

Perfect the First Time. To put the numbers associated with computer code in perspective, the *Aegis* defense system, a naval anti-aircraft missile system designed to track hundreds of targets, uses about sixteen million lines of code. Computer systems at the Cheyenne Mountain Air Force Station, home of the North American Aerospace Defense Command (NORAD), use over 46 million lines of code.[12] An experiment called "Delta 180" conducted by SDIO in September 1986 involved tracking a rocket in space, maneuvering to intercept that rocket, and then destroying it by colliding with it. This successful experiment required about one million lines of computer code. The software was written in six months and worked perfectly the first time it was used.[13]

As these examples show, large, complex computer systems have been built and are currently operational. While the software requirements for a strategic defense system are not yet fully determined, the software required by even some of the higher estimates is not significantly larger than that required in proved military systems. Writing the software for a strategic defense system's battle management component is clearly achievable.

More Reliable Communications

A decentralized battle management system will limit the impact of disrupted communications. Secure, reliable communications are essential to the operation of a strategic defense system. Disrupting these communications, however, will not be as easy as SDI critics assume.

There would be only local effect from interruptions of communications with the space-based elements of an SDI system with a decentralized battle management system. The disruption, for example, of effective communications with a small number of the interceptors in the Brilliant Pebbles system would have a limited impact on the capability of the overall SDI system. Only a few of the interceptors out of the thousands deployed would be rendered inoperable. This decentralized approach to battle

10 George C. Marshall Institute, *Report of the Technical Panel on Missile Defense in the 1990s* (Washington, D.C.: George C. Marshall Institute, 1987), p. 2.
11 Interview with the staff of the George C. Marshall Institute, March 31, 1989.
12 Brian J. Hogan, "About Star Wars: What's for Real," *Design News*, September 5, 1988, p. 77.
13 Marshall Institute, *op.cit.*, p. 12.

management could be expected to yield a highly dependable system, not easily disabled by enemy action.

Diversifying the battle management's communications system would make the disruption of communications more difficult. A variety of communications methods are being considered for use in SDI, including radio, millimeter wave, and lasers. Each has different advantages and disadvantages. Using a combination of different types of communications systems would make electronic jamming by an enemy very difficult. Brilliant Pebbles, for example, would use two independent communications channels. One channel would use an orbiting satellite to link up communications, while the other channel would link deployed interceptors directly with each other.[14] Meanwhile, the harmful, destructive effects of electronic interference caused by nuclear explosions, called electromagnetic pulse (EMP), would be handled by designing satellites resistant to the abrupt electrical surges associated with EMP.[15]

Man in Control of Machines

The SDI system will be controlled by humans, not computers. Critics charge that, because of the need for rapid reaction against enemy missile launches, the SDI system would have to be activated by computers. Yet the Pentagon has no intention of removing the decision to activate the SDI system from human control. The entire system is being designed in accordance with what is called a "man-in-the-loop requirement," meaning that a human commander would be in charge of SDI operations at all times. A human commander would need to authorize the system to open fire. He or she also would be able to override the battle management computers to shut the system down.

No Threat to Earth. Even with human control of the SDI system, there is still the question of what would happen if the defense were activated by accident. Would there be catastrophic destruction to the earth or the start of World War III, as might happen if nuclear missiles were fired accidentally?

These fears are unjustified. The weapons that would be employed by a strategic defense pose little or no threat to human beings on earth. Interceptor missiles launched from space, which lacked the heat shielding needed to enter the atmosphere, simply would burn up if accidentally launched toward the earth. Brilliant Pebbles interceptors, which would destroy their targets by the force of collision, have no explosive warheads at all. Even laser weapons in space would be incapable of penetrating the atmosphere with enough energy to do much damage on earth.

Computer Simulations

The reliability of SDI's battle management system can be effectively tested through the use of computer simulations. Critics charge that there is no sure

14 Lt. General James A. Abrahamson, "End of Tour Report," February 9, 1989, p. 1-1.
15 Marshall Institute, *op.cit.*, p. 15.

way short of a real-world attack to test the reliability of a SDI battle management system. This is untrue. The Pentagon plans to test SDI battle management systems with highly realistic computer simulations whose accuracy has been verified by physical experiments. Simulations of various types of missile attacks on the U.S. are especially well suited to testing computer software, since a program cannot tell if the inputs it is receiving are coming from a real attack or a device designed to imitate one. A computer program's reaction to a wide variety of situations, likely and unlikely, can be tested. Other means of testing include deliberately inserting errors into a program to evaluate its ability to respond and to correct the error. The basic design philosophy can be described as "build a little, test a little, learn a lot."[16]

Double Standard. SDI critics apply a double standard to SDI battle management systems. The standards of reliability applied by critics to the SDI battle management system, if applied to U.S. offensive strategic forces, would find those forces unreliable. Strategic defenses should not be held to a higher standard than is used for evaluating the reliability of nuclear weapons.

The U.S. has never launched a full-scale nuclear assault just to make sure the weapons work. Yet these same nuclear systems are the foundation of the country's defense posture and are considered credible and worth maintaining. They are not believed to be perfect; they are simply the best possible with the resources available. Uncertainty is a part of life, and military planning is no exception to this rule. There is no way to be absolutely certain that any military plan or system, including the nation's offensive nuclear forces, would not fail, at least in part, the first time it was used in an actual war.

CONCLUSION

The SDI battle management system is responsible for such important tasks as coordinating sensors and weapons, providing communications between various SDI components, and providing the means for human commanders to manage the overall SDI system. Any shortcomings in battle management ultimately would have an impact on the ability of the overall SDI system to protect the nation against ballistic missile attack.

Critics' Failure. Since battle management will be a key element in any strategic defense system, opponents of SDI have focused their criticisms on the design and reliability of the battle management system. Some of the concerns raised by the critics, such as the need for high quality battle management software, pose important technical questions, while others such as setting unrealistic reliability standards not applied to other weapon systems already deployed, seem politically motivated.

16 U.S. Congress, Hearings before the Defense Subcommittee of the House Committee on Appropriations, *Department of Defense Appropriations for 1988* (Washington, D.C.: Government Printing Office, 1988), p. 696.

In either case, critics of SDI have failed to make a convincing case that the technical problems associated with building an effective, reliable battle management system for SDI are insurmountable.

Toward An Effective System. To ensure that an SDI system will work reliably, the Pentagon should decentralize its battle management system, diversify the communications system, and test all systems with highly realistic computer simulations.

While designing and deploying a reliable battle management system will not be easy, it is within the nation's grasp. Concerns raised by the critics about the feasibility of an effective battle management system should not hinder research and development in this area. Steps can and are being taken to address these concerns. The requirements for designing an effective and reliable battle management system do not pose an insurmountable obstacle to the deployment of an effective strategic defense system.

Prepared for The Heritage Foundation by
Robert J. Jarrell, Jr.
a Washington, D.C.-based independent
defense consultant