Articles

Uncertainties in Building a Strategic Defense

C. A. ZRAKET

Building a strategic defense against nuclear ballistic missiles involves complex and uncertain functional, spatial, and temporal relations. Such a defensive system would evolve and grow over decades. It is too complex, dynamic, and interactive to be fully understood initially by design, analysis, and experiments. Uncertainties exist in the formulation of requirements and in the research and design of a defense architecture that can be implemented incrementally and be fully tested to operate reliably. The analysis and measurement of system survivability, performance, and cost-effectiveness are critical to this process. Similar complexities exist for an adversary's system that would suppress or use countermeasures against a missile defense. Problems and opportunities posed by these relations are described, with emphasis on the unique characteristics and vulnerabilities of space-based systems.

THE POLITICAL AND STRATEGIC DESIRABILITY OF A BALLISTIC missile defense (BMD) as envisioned in the U.S. Strategic Defense Initiative (SDI) has been debated widely (*1, 2*). The multifaceted issues of this debate involve (i) the U.S. nuclear deterrent and the question of whether our past and current dependence on devastating retaliation can be sustained politically and militarily over the long term, (ii) the current imbalance in U.S. prompt counterforce capabilities compared to the capabilities of Soviet ballistic missile forces and the perceived U.S. need to correct this imbalance, (iii) the uncertain equilibrium of a defense-dominated world if both sides deploy strategic defenses and the need for international cooperation and arms control in order to make a successful transition to a world less dependent on ballistic missiles for nuclear deterrence, and (iv) the questions of the technical, operational, and economic feasibility of systems that use the new technologies of directed- and kinetic-energy weapons, multispectral sensors, large-scale power sources, space-launch capabilities, and high-performance computers and communications.

The highly advanced and complex nature of the technological systems needed for BMD, especially if they are space-based, favor the United States over the Soviet Union with respect to our technological and economic capabilities. Moreover, such a defense, if it were possible to deploy effectively and thereby create serious uncertainties in Soviet strategic operational planning, could constrain or neutralize the threat of a preemptive or first-strike attack on U.S. nuclear forces and other military targets by Soviet ballistic missiles (*3*). Effective defense could thereby reduce or eliminate U.S. concern about assured retaliation and redress the imbalance in ballistic missile capabilities.

The complexities and uncertainties in developing and deploying a BMD that meets this objective, or a more ambitious one such as widespread population protection, are manifold and diffuse. Similar difficulties would exist for the Soviet Union if they were to develop and deploy a defense-suppression system against a U.S. defense. It is essential to understand these relations if an assessment of the desirability of strategic defense is to affect national policy and the definition of a feasible program.

The most important issues related to building a BMD system are described here, with emphasis on both the problems and the opportunities inherent in a BMD program. The feasibility of building components—sensors and weapons—to the specifications desired is not discussed.

Supersystems and Complexity

Strategic defense is one of those entities known as "supersystems" in the system engineering profession. A supersystem can be defined as an aggregate of systems with hundreds to thousands of nodes interconnected over huge geographic areas. Initial deployment is usually limited and for a particular purpose. As time passes, additional requirements will be imposed and technology will change, thereby necessitating improvements. Thus the supersystem will grow over a period of decades, as shown by the evolution of the U.S. telecommunications, air traffic control, transportation, energy, and air defense supersystems, and the strategic offense supersystem of ballistic and cruise missiles, aircraft, submarines, and their associated command, control, communications, and intelligence (C^3I) (*4*). A supersystem's end state at maturity, if it can ever be said to have reached maturity, is not predictable at the start of full-scale development and least of all during the initial research phase.

No currently available mechanisms for experimenting with supersystem-level concepts and relations exist other than analysis and simulation coupled to experiments that generate test data. These models cannot be completely realistic because of the dynamics of the relations between elements of the supersystem and, in the case of BMD, the lack of empirical data on operations in a nuclear environment.

Ballistic missile defense differs from the kinds of supersystems we have now because it must (i) cope simultaneously with nuclear threats from both offensive and defense-suppression forces, (ii) be highly automated, carrying out all space-based functions automatically except for the real-time enabling and disenabling of strategic operations by the national command and the changes they would make to rules of engagement and procedures embedded in software, and (iii) be credible enough in its projected wartime performance during peacetime operations and testing to ensure that it would never be attacked (*2*).

The author is president and chief executive officer of the MITRE Corporation, Bedford, MA 01730, and a member of the AAAS Committee on Science, Arms Control, and National Security.

Defense Architectures and Survivability

The functions of a BMD might include defense of intercontinental ballistic missile (ICBM) silos, defense of other military targets such as C^3I, light area defense of urban areas or military and industrial facilities, or heavy area defense of all U.S. targets. The architecture that has been adopted in SDI to achieve these functions is the multilayered defense (*5*). In this concept, boost-phase intercept would represent the first line of defense. The boosters of attacking missiles, which are much more vulnerable than the warheads propelled into space by the boosters, would be destroyed in the first few minutes of flight. For example, they would be destroyed by space-based kinetic-energy interceptors (high-impulse rockets with terminal guidance and nominal ranges of about 2000 km) in low earth orbit or by directed-energy weapons that are space-based (chemical lasers) or with surface-based components (x-ray lasers) that are launched into space on warning of attack. These "pop-up" weapons would require basing near the attacker's territory, for example, in submarines; they probably would not have time to destroy attacking missiles except during the midcourse phase.

An alternative, designed to reduce some of the vulnerabilities of space-based weapons to antisatellite systems, involves placing a number of hardened relay mirrors in geosynchronous orbit. These large, segmented mirrors would relay the energy from ground-based, short-wavelength, high-power lasers (high-energy, free-electron lasers with adaptive optics) to a larger number of mission-fighting mirrors orbiting at lower altitudes. Each fighting mirror satellite within range of an attacking missile would acquire its target, align the mirror, and send the laser beam from the relay mirror onto the target long enough to destroy it.

In the post-boost phase, the targets of these defense weapons would be the post-boost vehicle (PBV) that dispenses warheads and decoys over a period of a few minutes. In the midcourse phase, which lasts about 20 to 25 minutes, the defense would attempt to track and to discriminate the thousands of attacking warheads from the hundreds of thousands of accompanying decoys, and to destroy the warheads with both space-based and ground-based extended-range kinetic-energy interceptors or directed-energy weapons.

Space-based optical and radar sensors coupled to interactive discrimination elements (neutral particle beams to sense neutron emission or lasers for thermal tagging of targets) would provide surveillance and discrimination data in the midcourse and boost phases. Extremely high frequency (EHF) or laser satellite communications would be used for space-to-space links, and EHF and superhigh-frequency communications for space-to-ground links. Battle management satellites and ground-based command centers would be used to coordinate and control operations.

In the terminal phase, which lasts less than 2 minutes, surface-to-air high-acceleration kinetic-energy interceptors would engage warheads in late midcourse and between their moments of reentry into the atmosphere—where the decoys slow down and burn up—and the points of detonation on ground targets. Airborne optical and ground-based radar sensors would provide surveillance data in this phase. The interceptors and sensors would be organized into defense elements, each defending an area of several hundred kilometers in radius. Research on terminal BMD systems by the United States has been conducted for many years, and such systems are in advanced stages of development. In a multilayered defense, the boost and post-boost phases are critical to overall performance, especially if population defense is the objective, because they would destroy boosters and PBVs before large numbers of warheads and decoys are released, thereby simplifying the task of discrimination and destruction of the remaining individual warheads.

For a light area defense, tens to hundreds of interceptor satellites in low earth orbit could be deployed in conjunction with tens of ground-based defense elements spread over the United States. For a heavy area defense, up to a few thousand satellites could be deployed in low earth orbit in conjunction with hundreds of ground-based defense elements. A few thousand interceptor satellites might be needed in a heavy area defense for both redundancy and survivability to ensure that enough satellites would be available at the right place and time to engage a large attack. In the near term, kinetic-energy weapons are the most feasible form of ground- and space-based interceptors. As the ballistic missile threat evolves, directed-energy weapons might be required, for example, against missiles with fast-burn boosters. Passive and active surveillance and tracking sensors, communications links, and information-processing capabilities in space, in the air, and on the ground would provide battle management and C^3I.

Foremost in a BMD supersystem would be its capability to withstand countermeasures and operate effectively. Countermeasures can take three forms: (i) active measures that deceive defenses with many kinds and number of decoys, thrust-equipped replicas of warheads, and electronic jamming and spoofing of sensors, and that suppress defenses with various antisatellite (ASAT) weapons (*6*) such as ground-based lasers and direct-ascent nuclear-tipped interceptors, or orbital ASATs with directed-energy and kinetic kill weapons; (ii) passive measures that circumvent the defense such as offensive ballistic missile forces with fast-burn boosters that release warheads and decoys before kinetic-energy interceptors have time to get to the boosters to destroy them, the clustering of launches to saturate space defenses, the use of depressed trajectories to avoid space defenses, and the use of maneuvering reentry vehicles to avoid terminal defenses; and (iii) threatening measures such as greatly increased ballistic missile and air-breathing offensive forces to saturate and destroy defenses.

The suppression of space-based BMD elements by an attacker can be done with dedicated ASAT weapons as noted in (i) above or by using some of the interceptor weapons in the attacker's own BMD system. Conversely, a nation being attacked could use its BMD both to destroy attacking warheads and to defend itself against the attacker's ASAT and BMD weapons. A situation with two such opposing defense systems in space and their ability to react rapidly could result in serious instabilities during crises without arms control measures to inhibit incentives for first attacks. In general, the dynamics of an offense and defense mix on both sides will make planning for offensive operations vastly more complex than today's situation with essentially offensive forces only (*7*).

If arms reduction treaties are adopted that greatly limit the offense in numbers and kinds of weapons, BMD would be effective against threatening measures. To overcome active and passive countermeasures, BMD could be designed to counter the defense-suppression capabilities of the attacker, including those from the attacker's own BMD system. The age-old preferred strategy of the offense is to blast or burn a hole in the defense and drive through it. To counter this strategy, the space-based elements in a light or a heavy area defense could allocate a portion of their interceptors and C^3I assets (directed-energy or kinetic kill weapons) to defend themselves against the attacker's ASAT weapons or defense interceptors. They could also defend themselves through electronic jamming and spoofing of the attacker's assets.

Space-based BMD elements could also use passive survivability measures such as shielding and hardening of satellites, proliferation of many small satellites instead of fewer larger ones, and real-time orbit maneuverability of all space assets. Ground-based BMD elements such as surface-to-air missile batteries and large ground-based lasers would require an air defense against bombers and cruise

missiles as well as use of their assets to defend themselves against attacking ballistic missiles. All of these measures would increase the survivability but also the costs of BMD. It is uncertain what these costs would be and whether they would be offset by the costs to the offense for the defense-suppression and saturation measures it used.

One reason for these costs to the offense is that an attacker's defense-suppression system would require sophisticated surveillance, communications, and weapons capabilities similar to those that a BMD would have. If the BMD is proliferated, as it almost surely would be, the attacker must mount a large, timed onslaught without tipping off the defense. This, in turn, must be closely tied to the offensive attack because a hole blasted in a space-based BMD above one's territory lasts only until a new set of defense satellites arrives on the scene; the attacker's job would then have to be repeated. If the attacker gives an inadvertent tip-off, orbits of the defense satellites can be changed. Thus the job of targeting or retargeting hundreds of ASAT weapons in real time would require a highly sophisticated surveillance, tracking, and communications system that is subject to various countermeasures by BMD. Additional costs to the offense would be incurred for passive countermeasures such as the use of fast-burn boosters that would require the development and deployment of a new ICBM force whose PBVs might still be vulnerable to attack if the missiles have multiple warheads.

This situation would shift the uncertainties from the unique vulnerabilities and costs of space-based BMD to the mutual vulnerabilities and costs of BMD versus suppression and saturation of BMD. A typical measures-countermeasures development competition could ensue; the country having the necessary economic resources and the best technological capabilities could develop the capability to deter the other side's deployments.

Design Choices for Space-Based Defense

Choices arise when formulating a space-based BMD architecture consisting of hundreds to a few thousand weapons satellites that are to destroy both boosters and then warheads during the midcourse phase. The generic choices are, first, a centralized architecture where a designated space-based or ground-based battle management element collects track and discrimination data on threatening objects from sensor satellites and allocates and assigns weapons to them. This architecture would be highly efficient in resource allocation but would lack survivability.

A second choice would involve a system that divides the tasks among separate sensor, battle management, and weapons satellites in a hierarchical fashion. Battle groups formed from these satellites could be designated beforehand or they could be reconfigured dynamically to engage separate sets of targets and thereby match the needs of the operational situation. Each battle group could use preferential self-defense against a selected group of targets. The hierarchical configuration might be less efficient in weapons allocation than the centralized one, but more robust and flexible. In this configuration, sensor and battle management satellites would be in mid- to geosynchronous orbit principally for survivability and coverage, while weapons satellites would be in low earth orbit because of range limitations.

A third choice would involve semiautonomous satellites in low earth orbit, each with its own integrated sensing, battle management, and weapons capabilities, designed to operate in a fully distributed fashion. Coordination would be achieved by rules of engagement established beforehand and by adaptive control and communications networks between satellites and to and from ground-command facilities. This configuration would be the most robust and flexible if these control and communications networks were highly reliable and if satellites with complex, integrated capabilities could be developed with high levels of performance and reliability.

The nature of the surveillance and battle management capabilities in each of the three configurations would be different. For example, sensor satellites in the first two configurations might use linear-scanning arrays of infrared detectors for surveillance and active radars for tracking, whereas sensors in the semiautonomous satellites might utilize laser ranging for tracking and fixed mosaic arrays for continuous coverage because each sensor would be responsible for covering limited, preplanned areas in a push-broom fashion. Communications and battle management software would be highly distributed in the semiautonomous configuration and more centralized in the other two configurations.

Combinations of these choices could be configured in hybrid architectures. The choices outlined here require definition in detail to establish reliable cost estimates for defense architectures. Reliable estimates are not available yet because of the early state of the research in all elements of the defense and the lack of engineering and deployment information on Soviet forces and countermeasures.

Defense Effectiveness

The attempt to measure overall BMD effectiveness presents some dilemmas. For example, let us compare the effectiveness of two specific defense architectures each with its own configuration of sensors, weapons, and battle managers. While the number of leakers (enemy warheads penetrating the defense) is, in principle, a perfectly plausible and useful measure of defense effectiveness, practical use of this measure is not easy. Calculations of number of leakers need assumptions on the kill probability of the defense weapons and on the discrimination effectiveness of the sensors, both of which vary over wide values because of the early state of research and the resulting uncertainties about their future performance. Under such circumstances, any absolute statement about architecture performance, even the relative system performance between two architectures, is difficult to make unless one architecture is clearly dominant over a wide range of assumed values.

Also, we should not directly compare two different architectures against the same threat. A defense architecture would, to some degree, affect the Soviet response and ultimately determine important details of the threat as well as the weapons and tactics to be used against the defense itself. Therefore, holding an attack scenario constant for two alternate defenses is misleading.

With respect to any architecture, it is useful to distinguish between good system design with respect to feasibility and survivability and good use of a system with respect to concepts of operation, rules of engagement, and decision structure. A feasible design may fail because it is not operated effectively and wisely.

All of the foregoing concerns about effectiveness also apply to cost. For example, placing hundreds to thousands of satellites in orbit would be prohibitively expensive if accomplished with current techniques. It now costs a few thousand dollars per pound to put satellites in orbit. How much and when the weight of space-based sensors and weapons and how much the cost to launch them can be reduced by new technologies are unknown (*8*). The timing of the solutions to high space launch costs and high satellite weights is a critical constraint to the start and pace of deployment of a space-based BMD system. In this respect, kinetic-energy weapons are more amenable to earlier deployment than directed-energy weapons.

Cost-effectiveness of BMD is now being approached only in a

general sense. Cost-effectiveness at the margin is usually accepted as the most valid approach, but the value of the target set being protected by BMD must also be taken into account in any cost comparisons between defense and offense. In any case, until the knowledge base covering threats, architectures, weapons, sensors, computers and communications, software, and space transport and power costs expands considerably over the next decade, cost-effectiveness analysis for BMD will remain in its present undetermined state.

Defense Requirements

The classical approach of research, development, and ultimately system acquisition works well for items that are similar to things we know how to build (a faster interceptor aircraft, a wider bandwidth, jam-resistant radio link, a more sensitive radar). It does not work at all well for new things (the first atomic bomb, the first semiautomated air defense system, the first ICBM). For new supersystems, particularly those in the early research stages, early commitment to a set of detailed requirements is premature. For example, not enough is known about the critical technologies (sensors, lasers, and C^3I) that make up SDI to proceed confidently to deployment now. Incorrect choices could be made and time and money wasted.

A BMD program needs some operational objectives to remain coherent and relevant to national policy. A program aimed only at protecting U.S. ICBMs in hard silos or protecting the North Atlantic Treaty Organization (NATO) forces against short-range tactical ballistic missiles would be very different from a program aimed at defending all U.S. targets. A program aimed at providing the earliest possible protection against a Soviet surprise deployment (breakout) of a ground-based system would be different from one aimed at achieving a near-leakproof defense early in the next century. At this top level, a coherent statement of requirements is absolutely necessary: why we want the defense and what it is to defend. These requirements influence the nature of the research program and the pace and extent of development and deployment.

A prime objective of SDI could be to obviate the ICBM as a first-strike or preemptive weapon. Such a requirement places great emphasis on architectures with extensive space-based elements for sensors, battle management and C^3I, and weapons. Whether any such architecture is a politically, operationally, technically, or economically viable option for strategic defense is the critical issue today. The major complexities in formulating the design for and testing the utility and desirability of such an architecture show the need for a coherent set of top-level requirements.

To help formulate requirements, defense analysts use scenario generation to simulate the future operationally and politically. The first kind of scenario generation, one that tests the utility of an architecture, is the "one-shot" type that calls for groups of enemy missiles of type A with characteristics of type B to be launched from location C at U.S. target set D and that would probably achieve damage level E. This kind of scenario is relatively easy to deal with. Difficulties here usually arise from the lack of engineering data on sensors and weapons and the uncertainties about the performance to be assumed for threats.

The second kind of scenario generation, an iterative process that tests the desirability of an architecture, is much more important, and more difficult to do well. Here we must handle questions on whether or when arms reduction might succeed, how and why international crises might develop, how to deal with our allies in developing and deploying strategic defense systems, the impact on our current nuclear deterrent and on NATO and its flexible-response strategy, how the defense we select will interact with our offense, how and when to deal with the transitions to new supersystem capabilities, and when and what countermeasures to a defense might develop in the Soviet Union. We must also avoid the fallacy that the more elements considered in such a scenario, the more accurate it is. In fact, this complexity introduces more incoherency.

The shape of any effective U.S. defense will affect to a large degree the design of and tactics for the use of Soviet offensive weapons. How the Soviets would respond to a defense we have not even decided to build is hard to predict. Their response could include arms reduction proposals, more offensive weapons, different offensive weapons, a spread of direct and indirect suppression systems on U.S. defenses themselves, or a combination of all these measures.

In scenario generation, the offensive-defensive balance will continuously change. Also, this kind of process becomes quite lengthy and time-consuming because each defense concept usually leads to several plausible enemy responses. As the cycles are repeated, the directions of the branches increase geometrically. However, scenario generation of both kinds must be done. The second kind is difficult to do convincingly because of the diffuse reasons for political actions and military strategies. However, unless a full range of responses is considered, there can be no assurance against correcting the vulnerabilities of the defense. Also, we can never be sure why we may have prevented a war or why nuclear deterrence is working as a result of our particular strategic posture. In the end it becomes a matter of political and military judgment. This is especially true when the matter of BMD and offensive arms reduction is considered.

BMD and Arms Reduction

As noted, the feasibility of BMD depends on offensive arms reduction, which would simplify the job of the defense. In this context the critical issue for BMD is whether it will meet U.S. objectives for deterring Soviet military actions and also for maintaining stability in our strategic relations. In addition, can it help to defend Western Europe? The efficacy of BMD on these objectives cannot be determined in the near term because it depends on the results of ongoing SDI research and on arms reduction negotiations. However, both sides must have BMD for strategic relations to remain stable since BMD affects both the first- and second-strike capabilities of nuclear forces and their wartime capabilities. Also, if major offensive force reductions were agreed to by the United States and the Soviet Union, BMD could provide insurance for both sides against a surprise breakout of offensive weapons.

Nevertheless, it is questionable whether U.S. nuclear deterrence that depended primarily or only on BMD would be as reliable, at least for many decades, as the current nuclear deterrent provided by the triad of nuclear forces—ICBMs, bombers, and submarines. Also, BMD on both sides might undermine the strategy of selective strikes that is central to NATO's doctrine of flexible response and extended deterrence, since a large retaliatory strike by NATO would be required to overcome Soviet BMD. Finally, the explicit ASAT capabilities of BMD when both sides have a mix of offensive and defensive forces make it difficult to transition to a defense-dominant world. Such a situation would require a high degree of cooperation in arms control.

It is unlikely that the Soviet Union would agree to major offensive arms reductions without some control or regulation of the pace and breadth of SDI research, testing, and deployment. Without such control, the United States would have the advantage of its superior technical and economic resources. From a U.S. perspective, a valid SDI research program is necessary to provide the basis of an offensive arms reduction agreement and to deter Soviet breakout of a ground-based BMD. What is at stake for the United States then in

an arms reduction negotiation, in addition to preserving its current nuclear deterrent, is the pace of development and testing in SDI and the desirability of an agreement to restrict testing in a way that would prevent rapid deployment of a BMD system.

Battle Management, Networks, and Computability in Space-Based BMD

The development, assembling, and operation of hundreds to thousands of highly automated and netted sensors, weapons, and battle managers would pose the most daunting of challenges in building an area defense. Battle management/command, control, communications, and intelligence (BM/C^{3}I) is the system element that relates all the parts of the defense to one another. The design of BM/C^{3}I is embodied in commanders, operators, and procedures and embedded in computers, communications, and sensors, and their associated software throughout the system.

This BM/C^{3}I system must be designed to operate in time periods that include system deployment and in peacetime and wartime operations. For deployment that may encompass decades, BM/C^{3}I must manage the transitions as defense-in-depth is deployed while maintaining the effectiveness and survivability of the defense system. It must manage and control transport deployment and logistics, perform reliability and readiness testing, and establish and enforce standoff ranges for space assets that may be threatened by antisatellite weapons. For wartime operations, BM/C^{3}I must be designed to survive and manage the defense of the defense system, manage the battle and continuously track targets and discriminate decoys, assign and control weapons, perform kill assessment, manage power use, coordinate elements of the defense, provide communications and software security and antijam protection, delegate command, manage preferential defense strategies, and interact with the nation's offense to ensure coordinated operations.

The cost of the BM/C^{3}I infrastructure compared to sensors and weapons would be small, but BM/C^{3}I must work. Therefore, it must be made as simple as possible by reducing the interactions needed between defense elements. For example, the quantity of system components—sensors, weapons, and battle managers—could be increased in redundant ways to simplify resource allocation and control and to increase reliability through preplanned assignments of components to threat corridors and the use of dynamic reconstitution strategies when the BMD is attacked.

The timing or synchronization of all satellite elements in hierarchical or semiautonomous space-based networks would be critical to maintaining coherence of overall operations and to providing dynamic control capabilities. For example, within each element or node, an epoch must be defined within which tasks must be carried out, such as tracking and weapons assignment, that are to be repeated each epoch and coordinated with other satellites that share these tasks. A master clock in each node would maintain this function, and each master clock would be synchronized with all other clocks. Information to be transmitted between nodes could then be time-tagged so that each node could operate asynchronously. Complex dynamic network-adaptation algorithms and high capacity would be needed to maintain coherent operations as nodes were disabled. Deadlock in communications between nodes must be prevented. Such capabilities have never before been attempted for networks with hundreds to thousands of nodes and with such severe timing and coordination requirements when they are being attacked (*9*). Network architectures and protocols of this level of complexity have not yet been designed or developed (*9*).

With respect to information processing, a computer system on the ground is easier to build, maintain, upgrade, evolve, and test than one in space. Also, requirements for radiation hardening, fault tolerance, and self-testing of equipment can be much less severe on the ground. In space, processing equipment would require at least a 100-fold improvement over the current state of the art in size, speed, weight, power, hardening, and reliability to achieve the needed performance. Space-based sensors would require at least 100-fold improvements in hardening, resolution, and signal processing than the state of the art today. Full-scale development of these processors and sensors would take about a decade or more.

Computation in the supersystem could be distributed in many ways: by defense layer (boost, midcourse, and terminal), by battle group, and by function (target tracking, weapons allocation, system maintenance, and network control). Partitioning or distributing computation in these ways or others would assist in designing, implementing, and verifying software if interfaces between elements were defined precisely and methodology of design was rigorous.

Because elements of a defense system would be fully distributed in the most survivable architecture, exact or optimum solutions for some functions such as stereotracking (use of two or more sensors) and weapons assignment would result in combinational explosion (the need to consider excessively many trials before choosing the best solution). For example, if there are n objects to be considered, associations in sensor correlation (two sensors) scale as n^2, but assignment of weapons to targets can scale as $n!$. Considerable progress has been made in the development of simplified, heuristic algorithms that approach optimum performance in these areas with greatly reduced computation. Other areas of system operations such as situation assessment and kill assessment would require similar simplified algorithms. The use of highly parallel computers rather than sequential processors may further reduce computation times, but computing power by itself would not resolve the uncertainties in data from many remote sources.

Essential to the overall reliability of BM/C^{3}I is whether we know in detail the operational tasks to be performed; how they can be done with simplified algorithms; when valid engineering data on performance of sensors, weapons, and threat objects would be available; and how BM/C^{3}I could be designed to achieve fault tolerance. Fault tolerance, through redundancy and applications integrity in design, would be needed at all levels of the defense system from integrated circuits to processors, fully functioning nodes, and network control.

Software

The feasibility of designing and building reliable software for BMD has been discussed widely (*10*). Reliability in software has three components: (i) trustworthiness—known, predictable effectiveness and freedom from catastrophic flaws, (ii) fault tolerance—ability to continue to function coherently when parts of the system are damaged or destroyed, and (iii) information security—ability to prevent spoofing and exploitation through use of trusted computer programs and coding and authentication techniques in computers and communications.

To assess the feasibility of creating and maintaining reliable software, one should distinguish between the uncertainties and flaws in (i) the operational design for the defense system and the associated engineering data on the performance of sensors, weapons, target missiles, and decoys; (ii) the design of the conceptual structures—data sets, algorithms, relations among databases, and functions—that compose the abstract software entity; and (iii) the implementation of these structures with programming and machine languages within space and speed constraints. Brooks (*11*) termed (ii) the essential task for the software and (iii) the accidental task.

Software is inherently complex and changeable. Software engineering in the past has dealt with the accidental task through use of higher order languages, time-sharing, unified programming environments and, more recently, object-oriented programming, expert systems, program verification techniques, and high-performance work stations. The accidental task of generating millions of lines of software code may cause small errors whose operational impact on the defense system may be large because of the discontinuous and highly discrete nature of software. Rigorous design and testing are needed to prevent such errors and to correct them when they occur.

The more important and more difficult uncertainties and flaws occur in the operational design and in the software structures. For example, algorithms to track targets may not work because the engineering data on sensors or on targets and decoys may not be complete or accurate. Also, the unique vulnerability of space elements may cause saturation of the defense in ways not contemplated beforehand. The defense might then not respond effectively in dynamically reallocating assets to overcome the saturation. The interactive nature of a defense system with an informed enemy makes the prediction of all such possibilities difficult. Similarly, serious design errors may occur in software structures. The solution is to build the operational design and the software in operationally useful increments, evaluating each step along the way.

A number of techniques would be available for this task: (i) partitioning the overall job into well-defined parts with rigorously defined interfaces, (ii) using already proven software routines when available, (iii) using common software as much as possible throughout the system, (iv) rapid prototyping to iteratively establish and test operational and software requirements and designs, (v) developing an evolutionary approach in building the system in increments that are well tested and understood, (vi) using rigorous design methodologies and the best designers available, and (vii) continuous testing and exercising of the operational system during peacetime operations.

The task of providing reliable software for BMD, and for that matter a defense-suppression system, is formidable compared to past efforts in air defense, strategic C^3I, and air traffic control (*2*). In these cases, real-time software has operated successfully for decades. However, no system with the complexity of space-based BMD has been built before. Compromises and delays in operational design and deployment would have to be made. Much more research and a lengthy development effort are needed in dealing with the operational design and implementation of a specific BMD architecture before a conclusive judgment can be made about the reliability of software for this space-based system.

System Testability

A BMD system can and would be tested at every single phase from research through deployment. Broadly, testing would be at four levels, all of which are necessary to fielding a reliable system:

1) Research—to achieve understanding of the processes involved.

2) Component and subsystem test—to convince the designers and the decision-makers of the validity or lack of validity of a given approach to a subsystem or component.

3) System-level simulation and test—to get the operational bugs out of the system and to measure system performance against the specifications and operational objectives. This level extends from computer and network simulations to combinations of simulations and prototype weapons, sensors, communications, and software that would be tested on the ground and in space.

4) Deployed-hardware and software testing (full-scale testing of a deployed system with target missiles)—to test system operations and crew training in as realistic an environment as possible.

System-level tests, especially in space, are the current point of contention between the United States and the Soviet Union with respect to an SDI arms control agreement. Such system tests might include, for example, multiple, rapid firings of space-based kinetic kill vehicles against target missiles to assess multiple intercept capabilities and the quality of tracking, guidance, and kill mechanisms under realistic timing conditions.

An area of major uncertainty in defense system performance involves the use of nuclear weapons against the defense. Nuclear weapon effects produced by low-altitude nuclear bursts are moderately well known. At the close-in regimes (less than a kilometer or so), overpressures are also high and objects are destroyed. The effects of high-altitude nuclear burst many tens to hundreds of kilometers away from targets are quite different, however. The effect radii on electronics and sensors, for example, are much greater than the direct-destruction radii.

The last high-altitude nuclear test was in 1962, but many measurements of phenomena not made in 1962 could affect systems deployed in 1995 or 2010. Since the present nuclear test ban treaty prohibits above-the-ground tests, there would be a special burden on defense system designers and nuclear weapon effects experts to invent as realistic a series of tests as possible, by using a combination of underground tests and simulations, in order to assess the impact of nuclear effects on defense system performance, especially space-based sensors and weapons. The use of nuclear weapons against the defense by the offense would require the offense to also assess the impact of these nuclear effects on offensive timing and performance.

Information is lacking on the effects of multiple bursts as opposed to single, high-altitude detonations. This information is important because the heating of the upper atmosphere by an initial burst would create different conditions for a subsequent burst that could produce new backgrounds against which sensors would have to operate.

Conclusions and Observations

The current formulation of objectives for BMD that are being used to guide U.S. development and deployment programs include a capability to (i) cause serious uncertainties in Soviet strategic operational planning and thereby deter the first-strike use of their ICBMs, (ii) limit damage and deny military objectives of a nuclear ballistic missile attack, especially a limited one, and (iii) provide for assured survival of the population.

Systems to achieve the first two objectives may be technically feasible, but their cost-effectiveness, reliability, and survivability are highly uncertain. For the foreseeable future, the third objective probably is not feasible unless major reductions and changes are made in offensive forces. It is possible but unlikely that new technological breakthroughs will change the situation. The known technological possibilities have already been discounted in most assessments. However, the SDI research program is only a few years old, and significant innovation is still taking place in such areas as the efficiency of free-electron lasers, the brightness of chemical lasers, the accuracy of high-acceleration kinetic-energy weapons and the weight reduction of their payloads, precision optics and cooling for sensors, fault-tolerant communications, software engineering, space launch capabilities, and the acquisition of knowledge on the phenomenology of ballistic missiles during flight (*12*).

Any supersystem, especially ballistic missile defense, must evolve and grow over decades; hence a 20- to 30-year perspective should be taken in assessing policy options. This characteristic can be a strength rather than a weakness if development and deployment are

planned accordingly and a commitment is made to a long-term, phased program.

It is daunting to deal with the technical and operational complexities in light and heavy area defense, especially the survivability and performance of space-based configurations. The placing of hundreds to thousands of interconnected nodes of at least three different kinds (sensors, battle managers, and weapons, or combinations of them) in space at altitudes from low earth orbit to geosynchronous orbit or higher would pose sensing, discrimination, distributed-network-control, computational, and software reliability problems more complex than anything we have faced before. To build and operate a fully reliable BMD in space under benign conditions would be an unprecedented achievement. Under wartime countermeasures, it would be highly unpredictable. An attacker's defense-suppression system, however, would face similar uncertainties and countermeasures.

The current SDI research program addresses the technical uncertainties in missile defense through use of a national test network coupled to component research programs in sensors, weapons, and BM/C^3I. But proven system solutions with operational usefulness are still a long way off, perhaps up to 10 to 20 years (*13*). Therefore, the most prudent course for the United States is to continue a vigorous research program within the 1972 Antiballistic Missile Treaty and to maintain today's nuclear deterrent. This course would maintain the technological momentum and commitment to a BMD program without taking any irrevocable or premature political or strategic actions. The treaty also prevents the Soviet Union from deploying a ground-based BMD system that uses, for example, phased-array radars and advanced surface-to-air missiles that they have already developed. In conjunction with the research program, the results of arms reduction negotiations on strategic offensive systems could make some forms of BMD more feasible and thereby lead to achievable defense objectives.

REFERENCES AND NOTES

1. For example, J. S. Nye, Jr., *Foreign Aff.* **65**, 1 (fall 1986).
2. C. A. Zraket, *Daedalus* (spring 1985), p. 109.
3. S. M. Meyer, *Survival* **27** (no. 5), 277 (November-December 1985); "The U.S. SDI and Soviet defense policy: Near-term impact and responses," discussion paper for the Aspen Arms Control Workshop, Aspen, CO, August 1986 (Massachusetts Institute of Technology, Cambridge, 29 July 1986). In these papers, Meyer reports, from a Soviet perspective, how an SDI effectiveness of about 40 to 60% in destruction of attacking warheads would threaten Soviet strategic objectives and create serious uncertainties for Soviet operational planning of preemptive strikes and damage limitation.
4. C. A. Zraket, *Science* **224**, 1306 (1984); ———, R. R. Everett, H. D. Benington, *Ann. Hist. Comput.* **5** (no. 4), 330 (October 1983).
5. Office of Technology Assessment, U.S. Congress, *Strategic Defenses* (Princeton University Press, Princeton, NJ, 1986), pp. 141–260. The report discusses in detail examples of the SDI ballistic missile defense architectures and technologies outlined in this article, including the characteristics of sensors and weapons.
6. M. M. May, *Science* **232**, 336 (1986). May discusses the threats to military satellites and some protective measures.
7. T. Jarvis, in *Managing Nuclear Operations*, A. Carter, J. Steinbruner, C. A. Zraket, Eds. (Brookings Institution, Washington, DC, January 1987), pp. 661–678.
8. G. Field and D. Spergel, *Science* **231**, 1387 (1986); *ibid.* **234**, 1060 (1986); M. I. Hoffert and G. Miller, *ibid.*, p. 1057. Field and Spergel discuss the cost-exchange ratio (CER), cost of destroying a missile divided by the cost of the missile, for space-based, infrared laser systems and conclude that most likely the CER would be greater than one. Hoffert and Miller argue that other approaches such as short-wavelength excimer lasers coupled to greatly reduced space launch and satellite production costs could result in CERs of less than one. Field and Spergel replied that their model of satellite production costs is more accurate and that the weight of significant subsystems (power supply and pointing, acquisition, and tracking) of the excimer laser were underestimated by Hoffert and Miller.
9. For example, R. Binder *et al.*, special issue on Packet Radio Networks, *Proc. Inst. Electr. Eng.* (January 1987), p. 74; N. Shacham and J. Westcott, *ibid.*, p. 83.
10. For example, *Eastport Study Group—A Report to the Director, Strategic Defense Initiative Organization* (Eastport Study Group, Marina del Rey, CA, 1985); D. L. Parnas, *Am. Sci.* **73**, 432 (September-October 1985).
11. F. P. Brooks, Jr., in *No Silver Bullet—Essence and Accidents of Software Engineering*, H. J. Kugler, Ed. (Elsevier, New York, 1986), pp. 1069–1076.
12. L. Marquet, "SDI progress and prospects," paper presented at the Annual Meeting of the American Physical Society, San Francisco, 30 January 1987 (available from SDI Organization, Pentagon, Washington, DC).
13. For example, H. Brown, *Foreign Aff.* **64**, 435 (America and the World 1985).

14. This article is based in part on a brief, informal memorandum written for the American Physical Society as background for their 1986 study of directed-energy weapons. I thank my colleague T. Jarvis for extensive help and his review of this article.