HEADLESS HORSEMAN OF THE APOCALYPSE:
COMMAND AND CONTROL OF U.S. STRATEGIC FORCES

VOLUME I

A Dissertation

Presented to the Faculty of the Graduate School

of

Yale University

in Candidacy for the Degree of

Doctor of Philosophy

by

Bruce Gentry Blair

May 1984

ABSTRACT

HEADLESS HORSEMAN OF THE APOCALYPSE:
COMMAND AND CONTROL OF U.S. STRATEGIC FORCES

Bruce G. Blair
Yale University
1984

Mainstream strategic theory and analysis focus narrowly on issues of force structure. This perspective neglects an important dimension of the strategic situation. Crisis stability, deterrence and the strategic balance are affected by command structure performance.

The dissertation traces the development of the U.S. strategic command structure -- the command, control, communications and early warning network used in managing strategic operations. Network performance in the mid 1960s, early 1970s and early 1980s is assessed against two criteria: negative control (prevention of unauthorized, accidental and inadvertant use of strategic weapons); and positive control (preparation and execution of a coordinated strategic attack). The assessment reveals serious deficiencies in both dimensions, deficiencies that carry strong policy implications.

Main conclusions include the following:

1. Due to command vulnerabilities that mainstream analysis seldom considers, U.S. retaliatory capabilities have been far less than generally believed. Since the mid 1960s, Soviet strategic forces have posed a severe threat to U.S. second-strike capabilities.

2. Compared to a Soviet attack strategy that attempts to inflict maximum damage to individual weapons, a strategy based on command structure attack would be far more effective in blunting U.S. retaliation. Command structure vulnerability has vastly exceeded force structure vulnerability during the past twenty years.

3. U.S. command vulnerability undermines crisis stability. It could create intense pressure to initiate nuclear attack in a crisis. Incentives to strike first would be strong on both sides.

4. Command structure vulnerability continues to be the central strategic problem that the United States faces. Marginal dollars in protective investment should be channeled into the command structure rather than the force structure.

5. Projected investments in the strategic command network will not lead to realistic options for limited nuclear war or launch under attack.

PREFACE

I feel very fortunate to have three wise and compassionate advisors on my committee. Without the intellectual guidance, the creative suggestions, the encouragement and other support given to me by Garry Brewer, Martin Shubik, and John Steinbruner, this dissertation would have foundered long ago. My debts to them are legion.

I am grateful to Eric Denardo and Richard Hackman for looking after my welfare when they served as Director of Graduate Studies. John Bassler assisted in the formulation of statistical methods used in the analysis. Bruce Russett enthusiastically supported the research and created numerous opportunities for me to pursue my interest in strategic studies. James Fesler and Kenneth Moore were teachers par excellence and influential figures in my academic preparation for dissertation research. Fellow Yale graduate students Mike Evanisko, Rick Guzzo, Gary Jusela, Chae Pak, and Mike Raskin provided moral support and suggestions, as did numerous colleagues at The Brookings Institution: John Baker, Bob Berman, Dick Betts, Steph Haggard, Bill Mako, John Mearsheimer, Paul Morawski, Ken Oye, and Monica Yin. I especially appreciate the assistance and support of Monica Yin, who gave generously of her time for criticism, editing and art work.

Jan Liss at Brookings and Marie Avitable at Yale provided invaluable administrative guidance as well as encouragement. Patricia O'Brien at Brookings coordinated the secretarial effort. Susan Nichols shouldered the secretarial burden and typed the manuscript with help

from Dallas Mulske and Bob Londis. The final phase of the manuscript's production were handled by Lewis Holliday. I thank Judy Dunn and Bernice Plush for making the working environment at Brookings so pleasant.

I am grateful to Yale University, The Ford Foundation, and The Brookings Institution for financial support that made this research possible. The Brookings Foreign Policy Studies Program headed by John Steinbruner was pivotal in this regard. I owe much to John for this sustained support.

Finally, I wish to thank the many American military officers and government officials, present and former, who consented to be interviewed as part of the project.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

An important set of unanswered questions about the general strategic situation begins with the observation that the performance of command, control, communications and early warning networks is not included in calculations of the strategic balance. Popular calculations are based on weapon system characteristics. They weigh U.S. and Soviet arsenals composed of bombers, submarines and land missiles, but not the physical and procedural arrangements created to operate those forces.

This exclusion raises the question whether standard measures of strategic capabilities are valid. Are they reasonably accurate indicators or do they bear only marginal relationship to actual capabilities? Should decisionmakers rely on such limited calculations to gauge the stability of deterrence, formulate strategic policy, allocate resources or set arms control priorities?

Although the worth of standard measures has not been established and satisfactory answers to the above questions have not been supplied, assessments based on weapon system characteristics strongly influence perceptions of strategic strength. Debate over strategic policy is clearly under the influence, if not the dominance, of such assessments. Witness the preeminence of the model-builder who pits U.S. and Soviet nuclear weapons against each other in formal statistical combat.

Quantitative assessment of this kind, though lacking in consideration of organizational arrangements intended to provide coherent direction of strategic forces, "speaks" with great authority in policy discourse.

The tremendous weight that standard enumeration carries into policy debates is easier to explain than justify. One reason is that the analyses include as well as exclude relevant factors. Prominent among the included factors are several important weapons characteristics: the number of weapons in the respective inventories and their explosive yield, accuracy, range and reliability. Also included are the various delivery systems; impact "footprints" of reentry vehicles; and a host of other variables related to the size and technical configuration of the nuclear forces. As well, a particular class of targets figure prominently in the calculations. Notable characteristics of the usual targets of interest -- strategic bomber bases, missile silos and submarines -- include their number, location uncertainty, and ability to withstand the effects of nuclear explosions.

Another explanation is that the calculations are easily performed. Although the mathematical relationships among the parameters affecting weapons vulnerability are complex, computers and other analytic aids handle the equations with such facility that the computational exercise becomes practically trivial. This ease of computation has swelled the ranks of expert strategic calculators. The number of adherents and the level of their technical comprehension have reached a point where very sophisticated discussions of, for example, missile silo vulnerability to blast effects, are commonplace.

Simplicity also confers the appearance of a sharp analytic cutting edge, which combines with relevance and familiarity to produce persuasive policy prescriptions. Implications for policy are immediately suggested by estimates of the present and future vulnerability of missile silos, for example. Such estimates introduce clear criteria for appraising the force structure, choosing among alternative weapons programs, and setting an agenda for nuclear arms control. And the emergence of a broad national consensus forged under the criteria introduced by such estimates is facilitated.

The absence of alternative measures lends added weight to measures tied to weapon system characteristics and a narrow definition of strategic capability. We settle for these indicators because no convincing set of measures that include other dimensions -- especially, command performance and vulnerability -- has been proposed, and because policy decisions cannot be postponed indefinitely while analysts try to devise better ones. Whether or not pockets of ignorance exist, recommendations must be developed and evaluated.

There is scant comfort to be drawn from these explanations for the imbalance in the present state of strategic analysis. We can account for an imbalance which not only reflects but reinforces the view that strategic capability turns on the size and technical composition of the respective weapons deployments (force structures). But we still have not answered the question whether this view is sound or is misguided. And the field of endeavor, laden with preconceptions and analytic conventions, is complacent. Dissatisfaction with the narrow focus of mainstream analysis occasionally surfaces and users of analysis are occasionally reminded that standard calculations may be prone to serious error. But such misgivings and warnings are offered in a liturgical spirit, and usually relegated to obscure footnotes.

The many key limiting assumptions which underlie much strategic enumeration — particularly, the assumption that weapon system characteristics are the key determinants of strategic strength — require more than a cursory examination and footnote. Though it is not unreasonable to exclude measures of command performance before they are seriously developed, it would be quite unreasonable to accept indefinitely the present imbalance in strategic analysis; to let a computational impasse discourage inquiry into the command implications of nuclear weapons; or to allow the force of analytical habit to prevent the topic of command performance from arriving on the national security agenda. Simple intuition suggests that the omission of command parameters provides scope for miscalculation. It is ipso facto grounds for contesting standard analytic conclusions and imposing a heavy burden of proof on them. And if the scope for miscalculation is as large as one imagines, then much strategic enumeration is not only misleading, but flatly wrong. Command performance quite possibly is not just an important factor, but the key determinant of real strategic capability.

The need to examine the strategic situation with this in mind is pressing. At the moment, strategic programs of unusual magnitude and consequence are being advocated under an extremely narrow definition of strategic capability. Analyses of the effectiveness of Soviet attacks aimed at U.S. force units indicate an incipient threat of Soviet nuclear blackmail and provide a justifying logic for investing nearly $200 billion over the next six years to rectify the situation. The bulk of that sum is earmarked for modernization of the force structure, whose three components all show signs of declining strength. Poseidon missile submarines, the mainstay of one leg of the strategic TRIAD, have aged to a point where forced retirement en masse looms on the horizon. B-52 strategic bombers, the mainstay of another leg, have to contend with increasingly effective Soviet air defenses. And the Minuteman land missile force, the mainstay of the third leg, appears to be severely and imminently threatened by its Soviet counterpart. Calculations indicate that it could be virtually negated as a retaliatory threat by existing Soviet weaponry.

Despite the probable survival of enough weapons to inflict severe punitive damage in retaliation to any postulated Soviet attack, many view current trends with alarm because severe counterforce disparities favoring the Soviet Union are alleged to accompany them. Such asymmetry, should it be allowed to develop, would supposedly create a "window of vulnerability," an opening through which the Soviets could militarily maneuver into a position of exploitable bargaining dominance. A prevalent view is that Minuteman vulnerability alone raises the specter of nuclear blackmail. Unless remedied, this vulnerability would greatly diminish the counterforce potential of U.S. strategic forces, and it is feared that Soviet superiority in this dimension could tip the scales in their favor in the event of superpower hostilities.

The gloomy calculations of the day provide stimulation and justification for a massive infusion of investments in the strategic force structure. But if command performance is really the central question of national security, then heavy reliance on these calculations to gauge the Soviet threat and determine the pattern of future U.S. investment incurs high costs — in misplaced emphasis, unwise resource allocations, and unwarranted confidence. Strategic force units would be bolstered at the expense of the command system, an allocation that could prove wasteful and even counterproductive, no matter what strategy or purpose is driving the investment. It would be ironic if modernization of strategic forces siphoned off attention and resources from command programs to a point where the beefed-up forces could not be directed to any of the purposes at stake (including assured destruction, defined as the ability to destroy the Soviet population and economy in retaliation to attack). No less bizarre would be an investment that produced a force structure effectively geared to nuclear war-fighting (the ascendant goal of current policy and the impetus for most of the programmed investment in strategic systems) but that failed to bring the command structure into close alignment with that purpose. It is clear that deficiencies in command performance could be cause for serious concern regardless of the resilience of the force structure and the strategy to which it is subordinated.

This point seems to have registered with the present administration. Defense Secretary Weinberger drives it home in his FY 83 Annual Report, in which he observes that analysis of the strategic balance has been too narrowly focused in recent years. Although "survivable and enduring command, control and communication's systems are decisive for deterrence and would be critical should deterrence fail," notes Weinberger, criteria used in analysis have nonetheless been "blind to command and control systems." [1] The report further states that command system repair is essential and "perhaps the most urgently needed element" in the administration's overall plan for revitalizing the nation's strategic capabilities. [2] While certain features of that plan belie the Secretary's words (standard analytic criteria continue to drive investment into force modernization, which will consume the lion's share of the total strategic budget), the Reagan administration's profile on the command problem has become very high. It not only aims to spend $18 billion on improvements over the next six years, but also portrays the program as a precondition for force structure modernization. According to one authority, the $160 billion earmarked for new strategic weapons would simply be "a waste of money" unless the proposed investment in command structure development is also made. [3] To help ensure appropriation of the funds, the Pentagon has assigned command, control, and communications (C^3) elements associated with particular weapons a priority equal to the weapons themselves. [4] That equalization is formally stipulated in a recently issued National Security Directive and is reflected in C^3

funding requests attached to major weapons proposals sent to Congress.[5]

These are positive signs that the strategic command problem may have suddenly changed from a nonagendum to an agendum. If the appearance is not deceiving, then this recognition could be decisive, for it creates a demand for a solution and calls forth greater tenacity of purpose in dealing with the problem. If the item is truly on the agenda, and remains there, one could reasonably expect sustained effort to find a satisfactory solution to a long-standing problem.

The command problem, however, has been long-standing for reasons besides simple neglect. The present administration must overcome powerful forces that oppose any fundamental reordering of strategic priorities. Past administrations succumbed to them, and this administration is far from bringing them under control.

The methodological bent of mainstream strategic analysis is only one of these forces. Economic, bureaucratic, technical, political and other forces also array themselves against the policy priorities enunciated by the Reagan administration. Taken together, they constitute a formidable obstacle. Each is briefly discussed next. Later chapters elaborate.

BARRIERS TO COMMAND DEVELOPMENT

Scholastic Barriers

The voluminous, scholarly literature on nuclear strategy, deterrence and related topics has been enormously influential; its doctrines have molded strategic thought into what it is today. Notwithstanding the many virtues of this body of knowledge, it has helped erect major conceptual barriers to command structure development.

Two of these barriers are fundamental assumptions of deterrence theory. First, the theory rests explicitly on the assumption that nuclear weapons are instruments of diplomacy, a means by which to influence an opponent's decisions. The idea that an attacker would strike an opponent's command structure -- decisionmakers and the decisionmaking apparatus -- conflicts with this assumption. Nuclear diplomacy cannot be conducted if opposing decisionmakers and their command systems are destroyed. Why attack command channels if stable deterrence hinges on negotiations with them? Mutual preservation of command systems has thus become a sort of theoretical imperative, which undermines one of the prime justifications for command structure development: command vulnerability to deliberate, direct attack.

The second assumption is that each of two large governments (including their respective strategic organizations) behave as if they were a unitary actor. The perspective of deterrence theory sees decisionmaking power concentrated in the hands of a very few, and sees the course of events as wholly determined by them. Command structure development obviously cannot proceed on the basis of such an assumption. Instead, it requires a perspective that recognizes the diffuse and decentralized nature of the decision process in real organizational settings. The process involves hundreds and thousands of actors, many with delegated powers; standard operating procedures; rules of engagement; and a large number and variety of technical C^3 components performing a wide range of functions at all echelons. The course of events surely can be affected, perhaps determined, by how these elements of the decision process operate.

Economic Barriers

Probably the greatest barrier to command structure development is economic. During the past fifteen years, the United States invested an average of $1 1/2 billion per year (in constant dollars) in strategic command, control, communications and warning intelligence (C^3I). That is not a paltry sum, but still represents a tremendous underinvestment given the rise of a modern Soviet strategic force during the same period.

Reagan's plan has been portrayed as a praiseworthy departure from the historical pattern of underinvestment. It is widely believed to represent a substantial real hike in the C^3I budget. But this belief is mistaken. The actual increase is very modest. It is a mistake, and a disservice, to pretend that current budget proposals will cover the cost of major command modernization. Though estimates are inherently rough, the figure served up by the Reagan administration will not buy a survivable command system, and it represents only a small down payment on an enduring one. The price tag on a survivable, enduring command system far exceeds proposed funding levels.

Political Barriers

Reagan's commitment to command modernization appears to enjoy an unusual degree of political support. Investment in C^3I is the least controversial item in the strategic arms package unveiled last October. No one disputes the fact that the command system has suffered from chronic neglect, or that its repair deserves a high priority. Furthermore, few seem to regard the projected expense of repair as too great an economic burden to bear. No major defense programs would be sacrificed for the sake of command modernization.

Therein lies the catch. Political support is not unqualified. It will evaporate quickly if the endeavor turns out to require investments that are substantially higher than presently forecast. The administration's commitment to a survivable, enduring command system would be put to an especially severe test if the requisite investment threatens funding for major weapons systems such as the B-1.

It seems doubtful that Reagan would himself be prepared to scale down or forego major weapons deployments in order to finance command projects. For good reasons or bad, weapons programs like B-1 and MX are generally deemed to be essential to strategic revitalization, and there is no escaping the fact that political risks would accompany any bold deviation from this entrenched position. Reaction to his scaling down the MX program has given Reagan a preview of the possible coming attractions. MX retrenchment provoked the charge that he has scuttled his campaign promise to close the window of vulnerability at the earliest possible date. Further cuts in weapons investment would certainly intensify the criticism. Reagan could conceivably temper the criticism with reason -- "command improvement more than compensates for weapons cutbacks" -- but probably not. Command analysis is neither sufficiently developed nor sufficiently accepted to sell the idea that money would be better spent on command modernization than force modernization. To many, the proposal would sound like a political maneuver that smacks of strategic window dressing.

Bureaucratic Barriers

Present bureaucratic arrangements are ill-suited to the task of command modernization. Development of a viable strategic command system requires a broad view of the situation, a coherent overall plan, and central direction of the various projects undertaken. Today's management of C^3I programs meets none of these requirements. It lacks focus, unity of purpose, and breadth of vision. And it is anything but centralized.

Decentralized management creates a two-pronged problem. Besides the usual set of problems associated with excessive decentralization -- bureaucratic inefficiency and error in problem definition, coordination of activity, and so forth -- the absence of strong corporate management strengthens the hand of bureaucratic players who would oppose heavy investment in command structure development.

Such opposition is, alas, rather great. It is especially strong within the military services, for several reasons. First, the services attach overriding importance to weapons development and procurement. Along with ammunition, spare parts and maintenance, C^3I ranks low in priority. Second, a substantial number of strategic C^3I programs cut across service lines or extend upward to civilian rungs of the hierarchy; individual services are loath to tap their own budgets to fund these "collective goods." Third, these programs work to centralize control over force operations, and such centralization runs contrary to military traditions. Many within the ranks strongly oppose it. Establishment of a command system that provides for political authorization of a strategic campaign is fully accepted, but not countenanced is a system that permits national policy officials to manage the prosecution of that campaign in a detailed way. Such a system, nonetheless, is what the Reagan administration envisions.

This opposition bodes grief for the administration's strategic policies because it has not been disciplined. The military services exercise enormous power over C^3I programs and budgets, despite the fact that their concerns and priorities lie elsewhere. Absent countervailing leverage, command improvement will be stalled or otherwise fare poorly, as has been the case historically.

This situation is not likely to improve in the near future. Indeed, change for the worse seems probable. The Reagan administration recently revised the Pentagon's Planning, Programming and Budgeting System (PPBS) to give the military services even greater leverage than they already have. Under the new arrangement, which the Pentagon calls "controlled decentralization," it will be harder than ever for C^3I projects to survive the rigors of service review. The evidence is not yet in, but there are early indications that the services are ignoring the command modernization aims set down by national policy officials of the Reagan administration.

Technical Barriers

One of those officials said recently that "we are not prepared in a coherent fashion to spend $18 billion" on strategic command, control and communications.[6] Though the remark brings to mind the management problem discussed above, it was actually referring to technical problems. It is not easy to identify feasible technical solutions to problems such as command vulnerability. For all the amazing sophistication of modern computer, communication and sensor technology, the protection of a command network from the various measures that an aggressor might take against it -- ranging from sabotage to nuclear attack -- is extremely difficult.

The causes of the quandary in which investment planners find themselves are several. First, basic strategic policy has some rough edges that need smoothing out before the command implications can be clearly drawn. For instance, the policy requirement that the United States be prepared to fight a protracted nuclear war implies that the strategic command system must possess endurance; but disagreement exists over how long it must endure. Second, since it is exceedingly difficult to evaluate the overall performance of existing or hypothetical command networks, in any of the relevant dimensions (for example, endurance), it is difficult to decide where and how much to invest in repairs. It is a thoroughly open question whether even extensive repair of C^3I elements would actually aggregate to produce significant improvement in network performance. Third, technical solutions for certain known deficiencies associated with a particular element or collection of elements — for example, command posts, satellites, telephone switchings centers, and so forth — are frequently unknown, and in some instances even the existence of a deficiency may not be known. (To cite the most prominent example, the vulnerability of electronic components to electromagnetic pulse effects produced by nuclear explosions was unknown for many years.)

Psychological Barriers

The gulf between the intrinsic importance of command performance and the importance accorded it over the years leads one to surmise the existence of a deep-seated avoidance of the topic. Perhaps the topic has been left massively underdeveloped out of fear of what deeper examination might reveal.

Serious investigation could conceivably reveal, for example, that command vulnerability will not respond to treatment, regardless of the scale of investment, the efficiency of resource management, or the ingenuity of technicians. Protecting a large, complex strategic organization from the destructiveness inherent in modern nuclear deployments might in the end seem futile.

Final recognition of the inherent vulnerability of command networks would shake confidence in our guiding principles for comprehending and managing the threat of nuclear destruction. These principles of deterrence assume that the strategic decision process will function even under the most adverse conditions. If the assumption is untenable, then a strategy of deterrence cannot be firmly established.

Do we dare entertain the possibility that command vulnerability is an insoluble problem and that the relevance of textbook foundations of nuclear deterrence to the practical questions of national security has been vastly overstated? Today's fresh impulse to expose any and all weaknesses in nuclear control may cause enough anxiety to inhibit that very impulse.

SCOPE AND PURPOSE OF STUDY

In summary, a genuine watershed in the history of modern strategic deployments is coming into existence under an extremely narrow definition of nuclear vulnerability. Despite new effort by the Reagan administration to reorder strategic priorities under a broader definition that encompasses C^3I as well as weapon system characteristics, no dramatic shift in perspective or policy is in prospect. The view that strategic capability turns on the size and composition of the opposing force structures still prevails, and various forces exist to powerfully reinforce it. Under the circumstances, this narrow view will unquestionably continue to dominate strategic debate and largely determine the pattern of future investment in strategic systems -- at a time when strategic policy decisions of great consequence are being made.

It would seem fortuitous if sound strategic policies emerged without benefit of insight into the command implications of nuclear weapons. That much is generally granted. The relevance of command performance to the larger strategic debate and the need for a sensible program of modernization have not been lost on policymakers.

What is lacking is a strong understanding of the topography of the command problem. The Reagan administration has advanced a cogent argument for command modernization, one with strong intuitive appeal, but has evidenced no firm grasp of the technical difficulties or the other impediments to development that exist. Dim comprehension of the issues manifests itself in a general way in the administration's assignment of equal priority to command and force modernization. That instruction is a sign of heightened awareness and better understanding of the significance of command performance, but it is also a symptom of very imprecise calculation of the relative merits of investments in C^3I versus weapons modernization. Administration rhetoric gives the impression that its overall strategic arms package contains just the right mix of force and command ingredients. But the portrayal masks the reality: no recipe exists. Ingredients have simply been combined, or better homogenized, without even the semblance of a formula.

There ought not be any illusions that clarity or consensus on the question of command performance has been achieved. Research on the topic began in earnest only very recently, and it would be unrealistic to impose extravagant expectations on such study efforts any time soon. A good sense of direction, of appropriate and feasible objectives, of the proper balance between command and force structure development, and so forth, are not going to crystallize immediately. Meanwhile, command policies will be conceived under conditions of great uncertainty.

It is hoped that this study will facilitate understanding of the general topic. Its primary aim is to provide an historical assessment of strategic command performance. The study describes, not in exhaustive detail but in considerable depth, the physical and organizational arrangements that exist to provide coherent direction to U.S. strategic forces. It traces the evolution of these arrangements, analyzes their capacities and vulnerabilities, and identifies the implications of command performance.

The implications cannot be fully extended without an appreciation of how the strategic situation appears from the vantage point of mainstream theory and analysis. Chapter 2 therefore presents a "conventional view" of the strategic situation. Key topics include the theory of deterrence; the evolution of national requirements;

statistical combat between U.S. and Soviet forces; and policy prescriptions resulting from standard analyses. The administration's rationale for command modernization is also discussed.

Subsequent chapters are devoted to command analysis and to a critical evaluation of mainstream treatment of the strategic problem. The last chapter makes policy recommendations.

FOOTNOTES

1. Department of Defense Annual Report Fiscal Year 1983 (Department of Defense, 1982), p. II-10.

2. Ibid., p. I-39.

3. "DeLauer Calls New Strategic Plan 'Waste' Without C^3 Improvements," Aerospace Daily, vol. 111 (October 14, 1981), p. 237.

4. DOD Annual Report FY 1983, p. III-77.

5. "Why C^3I Is the Pentagon's Top Priority," Government Executive, vol. 14 (January 1982), p. 14.

6. "DeLauer Calls New Strategic Plan 'Waste' Without C^3 Improvements."

PART I

CHAPTER TWO

MAINSTREAM STRATEGIC THEORY AND POLICY

The equivalent of eight billion tons of TNT resides in the strategic arsenals of the two superpowers. U.S. strategic forces -- missile submarines, manned bombers, and land-based intercontinental ballistic missiles (ICBMs) -- carry about three and one-half billion tons. Soviet forces carry the rest.

The exact amount of potential destructive power that eight billion tons of TNT represent is unknown and practically unknowable, but by everyone's reckoning the detonation of even a small fraction of the deployed weapons on urban/industrial targets would constitute an unprecedented catastrophe. Some idea of the magnitude of the danger can be grasped by comparing current levels of explosive power with the amount released by the bomb that devastated Hiroshima: eight billion tons of TNT is roughly 640,000 times the explosive power of the atomic bomb dropped on Hiroshima in 1945. 68,000 people died, and another 76,000 inhabitants of that city were injured. In today's world of nuclear superabundance, the casualties from an all-out war would undoubtedly dwarf the Hiroshima experience. It has been estimated, and it is generally believed, that only 0.4 billion tons -- 400 megatons in the parlance of nuclear strategists -- exploded on urban/industrial targets in the Soviet Union would destroy two-thirds of that nation's urban population and three-fourths of its industrial capacity. [1] If used against the United States, 400 megatons would probably wreak even greater death and destruction. All this potential ruin resides in a small fraction, one-tenth, of the nuclear megatonnage at the disposal of the leaders of two hostile superpowers.

Scholarly endeavor in the United States between the end of WWII and the early 1960s created a theory -- the theory of nuclear deterrence -- with which to comprehend and manage the dangers implied by these arsenals. Although it has not been subjected to normal scientific test, the theory is coherent, well-developed, and built on a conceptual foundation that has great intellectual acceptance in Western culture. A solid consensus has been forged under the logic of deterrence, whose basic perspective is drawn from the logic-of-choice tradition in economics and the decision sciences. As Steinbruner notes, this tradition, otherwise known as the "rational analysis" tradition, has provided the "clearest, most coherent, most developed conception of the decision process which is available at the moment."[2] It is not surprising that propositions about the prevention of nuclear war were cast from this conceptual mold.

The basic perspective of both rational analysis and deterrence theory sees decisions as investment choices. Decisionmakers act to maximize their values under the constraints faced. Whether advanced as a normative argument or a positive assumption about the nature of human decisionmaking, rationality connotes a procedure whereby alternative courses of action are laid out, relevant costs and benefits of each option are calculated, and the alternative with the highest expected payoff is chosen.

In the strategic context, the decision problem is usually structured (by the objective scientist and presumably actual decisionmakers, too) in such a way that a rationally calculating actor will always choose not to attack the opponent. Each rival faces a choice between two alternatives: attack, or do not attack. As it is usually assumed that neither side can disarm the opponent, choosing to attack risks nuclear retaliation; and, given the inherent destructiveness of nuclear weapons, the expected payoff for preemption would be large and negative. Under the circumstances, electing to launch an attack would be irrational. Both sides are deterred. Nuclear stalemate exists. This despite the possibility that an aggressor might expect to destroy a large fraction of the opponent's forces and substantially weaken the victim's resolve. Unless the probability of retaliation is vanishingly small, the expected costs of preemption will always outweigh the benefits, and hence war will be avoided.

Thus, deterrence theory, in its simplest version, eases the psychological burden of nuclear weapons by turning an apparent liability -- hostile states in possession of awesome destructive power -- into a virtue -- nations sharing a common fate, each averse to unleashing nuclear attacks because such attacks would result in mutual annihilation. All other determining factors in international conflict, whether deleterious or salutary, pale in significance when compared to the influence exerted by a condition of mutual deterrence. During periods of high international tension, when escalating confrontation threatens to elude resolution, this condition acts as a powerful restraint and stabilizing force.

It loomed large during the Cuban missile crisis of 1962, writes Mandelbaum, whose simile likens that episode as well as the history of the nuclear age with two fencers on a tightrope, balancing precariously, "each fearing to thrust decisively because such a thrust would topple them both, attacker and victim, to mutual disaster." [3] Though paradoxical, mutual vulnerability allays fear and even engenders a sense of invulnerability, provided of course that one's faith in rational assumptions is steadfast, and provided that the condition of vulnerability applies to the population and economic infrastructure of nations, and not to their respective deterrent forces.

Mutual deterrence dissolves when one or both sides achieve the strength required to remove the opponent's ability to inflict severe punitive damage in retaliation to attack. In a crisis, the side believing that an unacceptably large fraction of its retaliatory capacity could be suddenly nullified by the opponent's forces might be impelled to strike preemptively. The superior side, as well, might be motivated to undertake the first aggressive actions. Regardless of its original intentions, this side could plausibly imagine a siege mentality — a "use them or lose them" attitude — operating on the weak side, and reason, rightly or wrongly, that it had better seize the initiative and preempt. A condition of two-sided vulnerability would further strengthen incentives for preemptive attack. If strategic forces on both sides are mutually vulnerable, the risk of nuclear war is believed to be unacceptably high. This is the worst of all hypothetical worlds, when they are viewed from the rational decision perspective of deterrence theory.

This view is distinct from orthodox military strategy which usually connotes the art or science of military victory. Strategists governed by orthodox tenets would seek the capacity to neutralize enemy military capabilities, an achievement that would be termed unstable and undesirable by proponents of deterrence. Unlike traditional military strategy, deterrence strategy does not value military forces for their potential role in defeating an adversary. In fact, the application of brute force to forcibly impose one's will on an adversary is alien to the deterrence perspective.

Deterrence theorists value the capacity for violence, particularly nuclear violence, for its implied bargaining power. The capacity to hurt the enemy forms the basis of a coercive diplomacy oriented to influencing behavior rather than overcoming strength. Cast in this role, strategic forces are instruments of threat, coercion and intimidation rather than military victory. [4]

Given the inherent destructiveness of nuclear weapons, the elevation of what T. Schelling calls the "diplomacy of violence" over orthodox military strategy was probably inevitable. Deterrence theory had its detractors; nevertheless a consensus quickly formed around it. There simply was no disputing one obvious fact: nuclear weapons could tear apart the social fabric and economic infrastructure of nations. They could inflict horrible pain on an unprecedented scale. Their potential as terror weapons capable of structuring an opponent's motives and influencing his decisions could have scarcely been disputed. At the same time, their contribution to military victory was not evident. Although nuclear attacks could obviously cause enormous damage to the opponent's military system, the introduction of nuclear weapons into the respective force structures dramatically changed the meaning of and requirements for military victory. Meaningful victory would not be achieved if even a small number of opposing nuclear forces could retaliate against cities. Victory thus requires the capacity to obliterate, in sudden preemptive fashion, all of the enemy's nuclear capabilities. To overcome his strength is to destroy all of it, quickly and decisively. By the early 1960's, assurance that that could be accomplished could no longer be provided, and under the technological conditions of the times, there were reasons to believe that the ability to mount a totally effective first strike would remain out of reach forever. In short, meaningful military victory in the modern nuclear era came to be regarded as unrealizable. This conclusion hastened the eclipse of orthodox military strategy by deterrence thinking.

Although the logic of deterrence rejected policies founded on the principle of military victory and proposed a conception of national security based on the coercive use of the power to hurt, it by no means implied that deliberate nuclear attack would never happen. To be sure, there emerged a strong belief that violence is most successful when held in reserve and made contingent on the adversary's behavior.

Coercive diplomacy is the manipulation of latent violence -- violence that can be withheld or inflicted in the future. But it also believed that the power to hurt and the credibility of threats to do so, may be communicated by some performance of it.

The actual display of this power could involve attacks on opposing military forces, particularly if such attacks were expected to improve the attacker's bargaining position. The strategic counterforce scenarios that have been popularized in recent years, for example, are readily folded into the logic of coercive diplomacy. The outcomes of counterforce exchanges are projected in order to determine whether sharp shifts in relative bargaining power might result. War-winning outcomes are those which result from some "limited" strategic maneuver that allows one side or the other to achieve bargaining dominance. This, however, is not military victory in the orthodox sense. It is manifestly not the same thing as delivering a decisive blow against the opponent's military capabilities.

Vestiges of orthodox military strategy still exist, however. Attacks geared to the objective of damage limitation, for example, continue to be programmed by U.S. nuclear planners who cannot know for sure whether coercive diplomacy might break down.[5] Its failure could lead to sheer violence meant to reduce enemy military capabilities to the extent practicable; the idea of damage limitation is to develop contingency plans designed to limit the amount of damage that could be inflicted by an opponent who resorts to unilateral, "undiplomatic" brute force to achieve his objectives.

Counterforce attacks meant to influence decisions could be difficult to distinguish from attacks geared to damage limitation. Clearly, however, the aims are distinguishable. The former is intended to induce restraint and extort concessions, whereas the latter maximizes damage to opposing military capacity in an effort to minimize vulnerability to enemy attack. The corresponding attack strategies, too, would probably differ in some important respects. For instance, an attack strategy oriented to damage limitation may include enemy command channels as well as individual force deployments among the targets for destruction, whereas a strategy linked to coercive diplomacy would surely not target enemy command channels, the very channels one wants to influence.

POLICY CONCLUSIONS

The basic policy prescription derived from the logic of deterrence is that adequate second-strike capabilities must be provided for, in order to instill absolute certitude in the opponent's mind that nuclear attack would draw severe punitive retaliation. By the same token, the two superpowers have a stake in the maintenance of mutual deterrence; neither side should embark on a course that could severely undermine the other side's ability to retaliate. Military improvements on one side may increase confidence in its retaliatory posture but the opponent's posture might be eroded in the process, resulting in a net loss in overall stability. (In theory, a successful grab for overwhelming strategic superiority would only create a hair-trigger problem that reduces the security of both sides.) Or, if the opponent responds with improvements of its own, the result might be an open-ended arms race that raises the level of nuclear deployments but leaves neither side any more secure.

In the past some effort has been made to improve U.S. strategic systems without creating, in the process, new threats to the opponent's strategic deterrent. However, the state of our own deterrent capability has been the predominant concern and preoccupation of U.S. defense planners. Maintaining a strong and credible threat of retaliation is a sine qua non of national security, and analysts generally agree that it should take precedence over all other strategic policy objectives.

Consensus is not as easily forged, however, when it comes to translating the basic policy conclusion into an actual strategic posture. Abstract theory does not specify what kind and amount of destruction the United States must be able to inflict on the attacker in order to deter him. Nor does it say what particular strategic systems embody these desiderata. These and other derivative policy choices -- for instance, what arms control measures enhance strategic stability -- require analysis which goes beyond the basic logic of deterrence. It is in the nature of these choices that analysis of them is highly subjective and prone to error. And since there is a deeper conflict of values associated with most choices, a politico-bureaucratic bargaining process rather than an analytic problem solving process not infrequently determines the outcome.

At the same time, an analytical approach has proved to be a prime vehicle of consensus. Participants in the problem solving process work with a common data base, common methods, and common problem parameters. They also share a common idiom in which to conduct debate and reconcile differences in the interpretation of results. And so forth. The groundwork for consensus exists by virtue of these facts, and indeed it is often substantially achieved even when it comes to specifying conditions required to establish deterrence, and specifying programs to meet those conditions. Again, analytic judgments do diverge, and not infrequently; and, once delivered to the political arena, they may become sharply polarized and fester there indefinitely. Yet dissection of the issues is ordinarily performed with sufficiently similar tools and surgical procedures that judgments are naturally inclined to converge.

The bases of this consensus in historical context shall be described in the next sections. The topics and the sequence of their discussion correspond to a series of steps readily associated with the rational analysis tradition: (1) establish the kind and amount of destruction needed to deter attack, (2) estimate the damage expected from the opponent's maximum attack, (3) determine whether residual U.S. destructive power satisfies the requirements established at step one, and (4) compare the merits of alternative remedies, if current or projected capabilities fail to satisfy requirements.

REQUIREMENTS: HOW MUCH IS ENOUGH?

The one sacred cow in the retaliation requirements department is known as "assured destruction." Strategists concluded long ago that the United States must be able to visit on an attacker a level of civil destruction which approaches the maximum amount that could be achieved under any circumstances. In specific terms this principle has come to be defined as the ability to destroy in retaliation to attack some 20 to 25 percent of Soviet population and 50 percent of its industrial capacity.[6]

Strategists reason that so stark a threat would dominate the calculations of any adversary, including one with barely any hold on rationality. Surely, the capacity for reprisal on this scale would not be lost on Soviet leaders, and would "swamp all misperceptions arising, for example, from cultural differences, individual idiosyncrasies, and the complexities of internal politics."[7] Such, at any rate, is the rationale for establishing assured destruction as the bedrock of deterrence.

This requirement, however, has not determined actual strategic deployments and targeting assignments. Force planners and political decisionmakers have established additional purposes and roles for the strategic forces, which in turn create demand for a more differentiated targeting policy than that associated with assured destruction, and for a level of strategic deployment that exceeds the level required to achieve the condition of assured destruction alone.

One such role grew out of a political commitment to NATO, coupled with an apparent imbalance of conventional forces in the European theater. To fulfill its pledge to defend Western Europe against an invasion by superior conventional forces of the Warsaw Pact, the United States extended an American nuclear umbrella over NATO in lieu of a full conventional counterweight. The proferring of this nuclear guarantee led to the assignment of some strategic nuclear forces to supplement tactical nuclear deployments committed to this particular mission (NATO defense), and established a requirement for flexible war plans. Attacks by these forces would be intended to serve a specific, limited objective. They need not be, and under the envisioned circumstances are not expected to be, undertaken in conjunction with attacks by forces dedicated to the assured destruction mission. Attack strategy therefore allows for the decoupling of some nuclear forces to defend NATO, while other forces are held in reserve. This strategy is called "flexible response." It was developed in the interest of establishing a firebreak between theater nuclear war and global strategic conflict.

Besides being the linchpin for most thinking and analyses related to NATO and the defense of Western Europe, flexible response at the strategic level has been seized upon as an answer to a paradox that has long plagued the basic strategy of massive retaliation.[8] The paradox is that if strategic deterrence based on the threat of massive retaliation fails, then it would not be rational actually to carry out the threat. In the wake of Soviet attack, even large-scale attack, there would be a continuing necessity to influence the opponent's decision process — in order to deter attacks by his residual forces or otherwise coerce restraint while attempts are made to negotiate a truce — and in view of this necessity, rationally calculating leaders would have nothing substantial to gain and much bargaining leverage to lose by massive retaliation. Moreover, the mass destruction of Soviet urban-industrial targets would be so disproportionate a response to limited strategic attack as to be not credible. Hence, the threat of massive retaliation might not deter low-level strategic threats or attacks — for instance, attacks confined to military facilities located in sparsely populated regions of the country.

The idea behind flexible response, then, is to prevent a situation in which the failure of strategic deterrence would be sudden, categorical, complete and catastrophic, and replace it with a situation in which overall deterrence is strengthened by allowing for failure in stages. The training, disposition and operational plans (for example, limited counterforce) of U.S. strategic forces reflect this policy aim. National policy requires that operational nuclear strategy allow for selective attacks on the Warsaw Pact/Soviet target base, whether those attacks would be undertaken in defense of Western Europe or in response to Soviet strategic attack on the United States. National authorities desire to have options to attack target subsets of their choice, and in electing to respond in a limited fashion they would not wish to relinquish options to execute withheld forces later. Above all, the national leadership does not want to be confronted with a choice between all-out attack and surrender. Even after a large-scale attack on American urban/industrial targets, all-out retaliation may not be judged appropriate. Many argue that some strategic reserve forces should be withheld for an indefinite period, on the theory that a reserve force could provide bargaining leverage even in the aftermath of a strategic exchange that destroys much of the populace and economic resources on both sides. Flexible response is thus seen as an important means of extending deterrence into war itself, and of providing distinguishable firebreaks between levels of intercontinental nuclear warfare.

Although requirements associated with purposes other than assured destruction have been in existence for a long time, their formal roots in U.S. strategic policy have remained somewhat shallow. As far as procurement policy (desiderata for weapons acquisition) is concerned, there has never been a strong, formal commitment to these aims. If a strategic weapons program involved substantial investment, and if it was directed to purposes other than basic deterrence, or assured destruction, it was destined to encounter stiff challenge and probably founder early in the acquisition stage.

This characteristic of strategic policy may seem peculiar in light of longstanding political commitments to the nuclear defense of Western Europe, intellectual acceptance of the idea of flexible response, and existence of war plans that operationalize principles of coercive diplomacy and deterrence extended in time. It is not, however, as peculiar as it seems at first glance. In the first place, procurement decisions made during the late 1950s and early 1960s (before assured destruction became the predominant desideratum of weapons acquisition) resulted in strategic deployments that greatly exceeded the level needed to achieve the condition of assured destruction. There developed a surplus that could be devoted to other purposes such as limited counterforce. Second, the assured destruction algorithm was based on such conservative assumptions that it automatically produced a force structure large enough to satisfy realistic requirements for a wide range of missions, including counterforce as well as assured destruction. (See the discussion below on conservative planning assumptions.) Third, there was never a close relationship between procurement and employment policy (desiderata for weapons assignment, targeting, option packages, and so forth). They were managed quite independently. Civilian policy officials in the executive branch and Congress, together with various American institutions such as the media, tended to bury themselves with the budgetary aspects of strategic policy. Fiscal issues dominated their agenda, limiting their involvement in the formulation of employment policy. In the employment channel, war planners were hardly bound by the criteria applied in weapons acquisition (notably, assured destruction); they devised attack strategy and allocated existing and programmed "surplus" inventories with a broad range of purposes in mind.

During the past ten years, forces to bring the two separate policy channels into closer alignment and to do so under broad policy guidance emphasizing purposes besides assured destruction gained momentum. The

Soviet buildup of strategic arms generated this momentum. Changes in targeting policy partially answered the paradox of the retaliatory threat, but it became apparent that a new procurement algorithm was needed to produce forces that provided for proportionate U.S. retaliatory responses to certain kinds of threats becoming available to Soviet leaders. The assured destruction algorithm was no longer automatically producing the "surplus" forces needed, for example, to respond in kind to a Soviet counterforce attack aimed at U.S. strategic forces including fixed-based missile silos. Although it still provided forces far in excess of realistic requirements for massive retaliation, the technical composition of these "surplus" forces was becoming less and less suited to tasks such as retaliation against time-urgent or hard targets, whose numbers and protection from nuclear attack were growing. In sum, the assured destruction algorithm just wasn't producing the unintended, side benefits it once did. The conditions under which it produced these benefits were unique, and they no longer obtained.

The groundwork for a merger of the two channels under a unified policy based on extended deterrence and counterforce was laid in the early 1970s. Then Secretary of Defense James Schlesinger deserves much of the credit for facilitating this consolidation. He stated the position that the then current attack strategy was too rigid, and too heavily oriented to assured destruction attacks.[9] But his advocacy, which seemed to be concerned with a particular issue of force utilization (the type of issue normally and routinely addressed within the employment channel), transcended the particulars of flexibility and even the general issue of employment policy. A message of much broader and deeper import was conveyed: in modern strategic circumstances there are purposes other than assured destruction at stake, and these purposes ought to be served within the procurement as well as the employment channel.

It is dangerous to ascribe motives and infer beliefs when they are not publicly expressed. But, it does not seem likely that the strategic war plans then in existence were, in and of themselves, the cause of Schlesinger's concern. He may actually have wanted to establish the legitimacy of principles besides assured destruction in order to pave the way for eventual approval, within procurement channels, of programs embodying such principles. He did not seek support for new weapons systems, but that logical consequence of his position eventually did plant itself in the acquisition arena. Widespread intellectual acceptance of the logic of intra-war deterrence has had a profound effect on procurement policy. Today, force and command structure programs designed to serve purposes such as counterforce and protracted war-fighting frequently survive the rigors of budgetary review.

Formal guidance issued during Schlesinger's tenure was consistent with the rhetorical departure from assured destruction. National Security Decision Memorandum (NSDM) -242, signed by President Nixon in January 1974, and associated documents -- Nuclear Weapons Employment Policy (NUWEP) and Policy Guidance for the Employment of Nuclear

Weapons — specify objectives for damage to the Soviet Union in terms of percent destruction of economic, political, and selected military targets.[10] The latter reportedly includes hardened missile silos and command-control facilities.[11] Population is not targeted per se, but the guidance established a requirement for destroying, when escalation cannot be controlled, 70 percent of the Soviet industrial base,[12] which translates into attacks on perhaps 200 major Soviet cities where one-third of the total Soviet population lives. A strategic reserve force was also established. Other features of targeting policy set forth in these documents will be discussed later.

The promulgation of countervailing strategy and recent presidential decision memoranda issued by the Carter administration carried the torch lit by Schlesinger and President Reagan's policy advances it even further down the road. U.S. strategic policy promises to become heavily oriented to nuclear war-fighting in a budgetary as well as an operational sense. The thrust of countervailing strategy and PD-53s, -58s, and -59s, legacies of the Carter administration which remain in effect, is toward concern with controlled attacks on a target list that includes opposing missiles in hardened silos. A fiscal commitment to these goals is implicit in the guidance, and there is reason to expect an even stronger fiscal commitment to them by the Reagan administration.

Although the requirements introduced most recently have not been publicly spelled out in great detail, the broad outlines are generally believed to incorporate the earlier NSDM-242 requirements and plans.

Basically, the United States must be able to absorb the enemy's maximum attack and still possess the capacity to destroy a specified percentage of Soviet economic, political, and military resources. Former Secretary of Defense Harold Brown has determined that U.S. forces must continue to be able to destroy a minimum of 200 major Soviet cities, where two-thirds of the industrial capacity and one-third of its population are concentrated. [13] The assured destruction principle is thus retained, though again Soviet population is not targeted *per se*. [14] Beyond this, he has proposed the following objectives: (1) to cover Soviet hard targets such as missile silos, command bunkers and nuclear weapons storage sites with at least one reliable warhead whose probability of destroying the target is substantial; and (2) to target Soviet general purpose forces, communication-command-control, and war reserve stocks necessary to the conduct of theater campaigns. [15] Furthermore, national leaders must be able to maintain control over this retaliatory capability for weeks or months if necessary. PD-53 requires the national communications system to be capable of riding out a Soviet attack and providing for central and flexible orchestration of U.S. attacks by forces that might be held in reserve for an extended period of time following the initial exchange. [16]

As stressed earlier, many such requirements existed in one form or another in the past, and to some extent were met. But only assured destruction resonated in the procurement channel, and only by happenstance did it produce forces that satisfied requirements for, say, limited counterforce. Now that the pendulum of official and informed public opinion has swung back toward concern for counterforce and nuclear war-fighting, it will likely become much easier to advance programs meant to serve these purposes, in the event that serious deficiencies develop along these dimensions.

Whether or not such deficiencies are in fact developing is one of several basic questions which provide grist for the estimation and assessment process discussed in the next section. This is the process devoted to the systematic and fine-grained analysis of the ability of the United States to satisfy all the requirements — notably, assured destruction, counterforce, and flexible response — set forth in national strategic policy.

Before turning to discuss estimation and assessment, it should be restressed that the resurgence of interest in strategic counterforce does not mean that the primacy of military victory or even damage limitation is being reestablished. The idea of military conquest was repudiated long ago and there are no serious moves afoot to resurrect it. Advocates of U.S. counterforce policies and programs instead argue that Soviet counterforce capabilities have expanded to a point where the opponent's bargaining position might be strengthened by undertaking some limited strategic maneuver. To deny the adversary the additional leverage that might otherwise accrue as a consequence of say, counterforce attack against the U.S. Minuteman force, strategists propose countervailing measures to fortify U.S. coercive diplomacy. Principles of deterrence appear to lend strong support to the general aim if not the specific remedies proposed. Orthodox military strategy based on the idea of military conquest is not driving any of the planned investments.

ESTIMATION AND ASSESSMENT

The procedure generally followed in assessing the adequacy of U.S. strategic deployments is to first calculate the amount of destruction that can be visited on the attacker and then compare this figure with the amount deemed necessary to achieve systematic coverage of the Warsaw Pact/Soviet military-urban-industrial target base.

The amount of destruction that can be visited on the attacker depends in large measure on the effectiveness of the attacker's preemptive attack and defensive operations, which in turn depends in varying degrees on a complex of factors including each side's weapons, organization, plans, geography, communications, intelligence and warning systems, and doctrines and beliefs about the conduct of war.

Sophisticated analyses can be performed on many of these factors. To reduce the estimation problem to manageable proportions, though, analysts focus attention on a limited set of factors — notably, the size and technical composition of targets and attacking weapons. One cannot fail to notice that estimation has become almost synonymous with computer-assisted simulation of interaction between these elements.

Before describing what could be called the statistical combat approach to analysis, and discussing its limitations, the variables considered, and the major conclusions reached, we digress briefly in order to drive home an important point: a major issue of estimation is the level of uncertainty that U.S. planners and political decisionmakers are willing to live with in the interest of nuclear deterrence. As a rule, not very much uncertainty is tolerated. The assured destruction principle itself (requiring a level of destruction that approximates the maximum amount that could be achieved under any circumstances) is a manifestation of risk aversion, as is the insistence that assured destruction be estimated very cautiously -- "crediting only that damage which established knowledge renders both certain and calculable."[17] Only the immediate and direct damage from nuclear attacks on urban-industrial targets is counted; famine, disease, long-term environmental damage, and so forth are excluded.

Similarly, conservative assumptions underlie calculations of the vulnerability of U.S. strategic deployments. For instance, the official yardstick of strategic sufficiency in the 1960s measured the capability of nuclear forces to inflict assured destruction after a <u>greater-than-expected</u> Soviet counterforce attack.[18] A more recent example of the use and consequences of conservative planning concerns the vulnerability of Minuteman silos. Calculations based on conservative assumptions predict that only a small fraction of this force would survive the Soviet's maximum attack in the early to mid 1980s. However, plausible changes in the underlying assumptions -- for instance, assumptions about the operational reliability and accuracy of Soviet ICBMs -- generate results that would presumably dishearten a cautious Soviet planner. For instance, in the hypothetical case of a future Soviet threat consisting of highly accurate, highly reliable, medium-yield MIRVs, "even rather modest shifts in the pertinent assumptions are sufficient to change the apparent advantage from the attacker to the defender if a full first strike on land-based missiles is attempted." [19] In the same vein, former Defense Secretary Brown cites the possibilities of fratricide, missile unreliability, operational degradation in accuracy, and the launch of American missiles before Soviet warheads arrive as reasons why the Soviets cannot be sure that they could destroy 80 to 90 percent of the Minuteman force circa the mid 1980s. [20] In sum, application of the conservative planning principle by both sides produces almost diametrically opposite conclusions. On the one hand, in Brown's words, "we will not have much confidence that more than a small percentage of our silo-based missiles can survive a Soviet preemptive attack." On the other hand, again according to Brown, "the Soviets could not be at all confident of destroying the bulk of our missiles." [21]

Disparate U.S. and Soviet perceptions of the degree of strategic vulnerability that exists on both sides could probably be found in virtually all areas where comparisons are made. Other illustrations of the consequences of risk avoidance in strategic assessment will appear in later discussion. For current purposes, suffice it to say that the conservative planning principle is largely responsible for divergent conclusions. While estimates of the static strategic balance and the effects of marginal changes are usually discussed in terms of underlying numerical and technological realities, the calculations are substantially driven by an entirely subjective matter having to do with attitudes toward risk.

Statistical Combat

Calculators of U.S. retaliatory strength labor under the assumption that the attacker is committed to the destruction of individual elements of the U.S. force structure. Soviet land- and sea-based ballistic missiles are committed to attacks on bomber bases, submarine ports, and individual ICBM silos. Antisubmarine warfare (ASW) forces strive to find and destroy missile submarines patrolling the oceans. And air defense systems attempt to bring down strategic bombers headed toward targets inside Soviet and Eastern Bloc territory.

The effectiveness of the attacker's offensive and defensive operations is estimated for different political and military scenarios. However, calculations are usually based on surprise attack conditions, implausible as that may seem. In all likelihood, Soviet preparations for strategic attack would be detected. But in keeping with the principle of conservative planning, analysts are apt to assume that there is enough scope for a major intelligence blunder that the element of surprise would be present. Attack preparations either go undetected or unheeded. As a result, the alert readiness of U.S. strategic forces remain at the normal, peacetime level, and the damage credited to Soviet attacks is higher than it would be otherwise.[22] This is the cost incurred when "strategic warning" fails.

The penalty for failing to provide "tactical warning" is also severe. This term refers to the process of detecting actual attacks and responding in time to avoid absorbing the full weight of the opponent's strike. If "tactical warning" is not provided, alert forces that depend on it for their survival would be subject to destruction, and the expected damage from Soviet attacks is once again higher than it would be otherwise.

Extremely conservative estimates of force structure vulnerability are based on tactical as well as strategic warning failure. In an earlier era, however, this would not have been so conservative a planning assumption as it is today. Until the mid to late 1960s, confidence in the performance of the early warning network designed to detect missile attacks was justifiably low. The situation seemed to recommend operations that circumvented this problem, keeping reliance on tactical warning at a minimum. Accordingly, some strategic bombers were flown on 24-hour airborne alert between 1958 and 1968.[23] Other efforts reflected this goal. Indeed, the major force structure programs of the 1960s can be understood as an attempt to hedge against the possibility of a tactical warning failure. The idea was to afford strategic units the physical protection they needed to ride out a complete surprise attack, and thereby eliminate reliance on tactical warning for survival of the bulk of the strategic forces. Diversification of the force structure followed, with massive investments in weapons systems that did not require tactical warning to generate their capability. Submarines were deployed at sea, where they could not be readily found and targeted, and land missiles were emplaced in underground silos which were difficult to destroy. Strategic bombers were retained and though these forces still generated their capability in anticipation of nuclear attack, they no longer monopolized the deterrent portfolio. Diversification thus strengthened the threat of retaliation to complete surprise attack.

Because confidence in the performance of early warning systems has grown over the years, the standard assumption is that some advance notification of actual attack would be received. In most analyses, ground alert bombers, for example, have a good chance of surviving a sudden attack. Most calculations are still based on the assumption that "strategic warning" would fail, however. No off-alert forces are brought to alert status before Soviet forces are launched.

The historical picture that emerges from deeper examination of force structure vulnerability under conditions of surprise attack is clear. Regarding bombers and missile submarines, the situation has changed only very marginally during the past fifteen years. While those units maintained at low states of readiness have been and remain highly vulnerable to sudden attack, the alert units continue to be virtually immune to preemptive destruction. The situation is radically different in the case of land missile vulnerability. Although a very high alert rate has been maintained, the technical trend has been running against this component of the force structure.

It is possible to capture this trend using standard equations which combine technical characteristics of land missile targets and attacking weapons to estimate the probability of target destruction. A representative formula selects the target attribute of primary importance to be silo "hardness," expressed in terms of the maximum blast overpressure, in pounds per square inch (p.s.i.), that can be safely tolerated by the structure that houses the missile. It selects the number of attacking weapons, and their yield, accuracy and reliability, as the weapon characteristics of prime import. A standard mathematical relationship between these factors and the probability of target destruction by a single attacking warhead is

$$TKP = OAR \times (1.0 - 0.5^{8.41\,(Y^{2/3})/H^{0.7}\,(CEP)^{2}})$$

Where TKP = Terminal Kill Probability

OAR = Overall Reliability of Attacking Missile

Y = Explosive Yield of Attacking Warhead

H = Silo Hardness in p.s.i.

CEP = Accuracy of Attacking Warhead

For attacks by two warheads with identical attributes, the probability of silo destruction is given by

$$1.0 - (1 - TKP)^2$$

These formulas were used to calculate the results of hypothetical missile attacks on opposing land missile forces during the period between 1962 and 1974 (see Figure 2-1).[24] The graph plots the percentage of each side's ICBM force that would have been destroyed in a large-scale surprise attack. As indicated, the technical trend ran in favor of U.S. forces during the initial period and began to be reversed about 1965. The threat eventually tapered off, reflecting a leveling out of Soviet ICBM deployments (see Figure 2-2) and increased hardness of U.S. missile silos.

Figure 2-1


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
RESULTS OF PREEMPTIVE ATTACK AIMED
AT OPPONENT'S ICBM FORCE
Percent of Soviet Force Destroyed
Percent of U.S. Force Destroyed
62--+-63--+--64-+--65-+-66--+-67--+-68--+-69--+-70--+--71-+--72-+--73-+-74

U.S. AND U.S.S.R. STRATEGIC NUCLEAR DELIVERY VEHICLES:

Historical Changes in Launcher Strength

	1962	1964	1966	1968	1970	1972	1974	1976	1978	1980
U.S.										
Land Missiles	294	834	904	1054	1054	1054	1054	1054	1054	1054
Submarine Missiles	144	416	592	656	656	656	656	656	656	656
Long-range Bombers	600	630	630	545	656	656	656	656	656	656
U.S.S.R.										
Land Missiles	75	190	292	858	1513	1527	1618	1477	1400	1398
Submarine Missiles	some	107	107	121	304	500	720	845	1028	1028
Long-range Bombers	190	175	155	155	140	140	140	135	135	156

Source: International Institute for Strategic Studies, <u>The Military Balance, 1980-81.</u> London: I.I.S.S. 1980) (Also earlier years: annual).

Figure 2-2

The trendline took another sharp upward turn about 1975, however, when the Soviets began to deploy a new generation of land missiles. Three types of ICBMs -- the SS-17, SS-18, and SS-19 -- became operational. Many were designed to carry multiple independently targeted reentry vehicles (MIRVs), and they were credited with higher accuracy than their predecessors.[25]

These improvements produced a large increase in the lethal index of the Soviet missile force, a quantitative measure reflecting the size, yield and accuracy of nuclear inventories. Figure 2-3 shows the pertinent statistics for the beginning of 1975 and 1978.[26] By themselves, "lethality" statistics do not measure the counterforce capabilities of a missile force. Nor do marginal increases in lethality necessarily imply any improvement in counterforce capability. To transform lethality into a meaningful measure of attack capability, a set of targets must be specified, target "hardness" estimates supplied, and the probability of target destruction computed.

This caveat notwithstanding, the elaborated calculations do indicate a definite decline in U.S. land missile survivability. Although there has been a sustained U.S. effort to give missile silos added protection against the effects of nuclear explosions, it has not been enough to offset the numerical and technical advances incorporated in the fourth generation of Soviet missiles. Theoretically, a Soviet ICBM attack in 1978 could have destroyed nearly half of the U.S. Minuteman force.[27] Five years earlier, prior to the introduction of the fourth generation of Soviet ICBMs, only about one-fourth of the Minuteman force was vulnerable to attack (see Figure 2-4).

LETHALITY OF U.S. AND U.S.S.R. STRATEGIC MISSILE FORCES IN 1975 AND 1978[a]

Missile	Explosive Yield of Warhead (Megatons)		C.E.P. Of Reentry Vehicle (Nautical Miles)		Lethality Per Reentry Vehicle (K)[a]		Number of Reentry Vehicles Per Missile		Total Number of Missiles		Total Lethality of Missile Force (K x N)	
United States:	'75	'78	'75	'78	'75	'78	'75	'78	'75	'78	'75	'78
Minuteman III	.17	.17	.2	.15	7.7	13.6	3	3	550	550	12705	22440
Minuteman II	1	1	.3	.3	11.1	11.1	1	1	450	450	4995	4995
Titan	5	7.4	.5	.35	11.7	31	1	1	54	54	632	1674
Poseidon	.04	.04	.3	.25	1.3	1.9	10	10	496	496	6448	9424
Polaris	.2	.2	.5	.5	1.4	1.4	3	3	160	160	672	672
TOTAL											25452	39205
Soviet Union:												
SS-9	25	25	.7	.5	17.4	34.2	1	1	288	183	5011	6259
SS-11, SS-13	1	.5-1.5	1.0	.55-1.5	1	.8-2.1	1	1-3	970	778	970	2187*
SS-17/mod. 1	-	.8	-	.35	-	7.0	-	4	0	70	0	1960
SS-18/mod. 1	-	25	-	.3	-	95.0	-	1	0	40	0	3800

Figure 2-3

Figure 2-3 (continuation)

SS-18/mod. 2	–	2	–	.25	–	25.4	–	8-10	0	55	0	12573
SS-18/mod. 3	–	15	–	.25	–	97.1	–	1	0	30	0	2913
SS-19/mod. 1	–	.6	–	.3	–	7.9	–	6	0	230	0	10902
SS-N-6	1	1.5	1.5	.55	1	4.3	1	1	528	384	528	1651
SS-N-8	1	2.0	1.5	.5	1	6.4	1	1	80	344	80	2202
SS-N-17	–	2.0	–	.3	–	17.6	–	1	0	70	0	1232
SS-N-18	–	.2	–	.3	–	3.8	–	3	0	60	0	684
SS-7, SS-8	5	–	1.5	–	1.3	–	1	–	209	–	270	0
TOTAL											6859	46363

*Sum of 48 SS-13s (1 meg.; 1.1 CEP; 1 RV) + 490 SS-11/mod. 1s (1.5 meg.; 1.25 CEP; 1 RV) + 240 SS-11/mod. 3s (.5 meg.; .55 CEP; 3 RVs).

Notes: [a]Estimates for 1975 and 1978 differ in some cases because of different data sources rather than missile improvements over the three-year period.

[b]K is the yield of a warhead in megatons to the two-thirds power divided by the square of CEP (miss distance in nautical miles).

PRE-EMPTIVE ATTACK AGAINST

OPPONENT'S STRATEGIC FORCES*

	U.S.				U.S.S.R.			
A.	Percent of Delivery Vehicles Destroyed (by Type):							
	Land Missiles	Submarine Missiles	Long-range Bombers	Total	Land Missiles	Submarine Missiles	Long-range Bombers	Total
1973:	24	45	68		56	85	100	
1978:	44	45	77		41-63	85	100	
B.	Warheads Survive:							
1973:	1293	2160	850	4303	667	76	none	743
1978:	1016	2960	904	4880	1666-2238	172	none	1828-2410
C.	Total Yield of Surviving Warheads (equivalent megatons):							
1973:	742	373	579	1694	2106	76	none	2182
1978:	558	400	357	1315	1218-3260	185	none	2503-3445

Figure 2-4

*Notes to Figure 2-4

1973: Assumptions for land missiles are given in Appendix A.

The U.S. strategic bomber force included 397 B-52s and 66 FB-111s. In the analysis it was assumed that 40 percent of the bomber force was on alert, that a Soviet attack destroyed all off-alert bombers and 10 percent of the alert force, and that Soviet bomber defenses destroyed 10 percent of the bombers that survived the initial attack.

Type	Alert	Survive	Warheads	Yield (Total)
B-52 G/H	102	83	498	332
D/F	57	46	184	184
FB-111	26	21	168	63

The entire Soviet bomber force of Tu-95s and Mya-4s was assumed to have been destroyed in a pre-emptive U.S. attack.

The fraction of U.S. missile submarines at sea at any time in 1973 was assumed to have been 55 percent of the total force. The analogous Soviet alert rate was assumed to have been 15 percent of their total force. Those submarines at sea were assumed to have survived.

Type	Missiles At Sea	Warheads	Yield (Total)
U.S. (22 out of 41 subs at sea)			
Polaris A-2	64	64	55
Polaris A-3	112	336	114
Poseidon	176	1760	336
U.S.S.R. (5 out of 34 subs at sea)			
SS-N-6	64	64	64
SS-N-8	12	12	12

1978: Assumptions for land missiles are given in Figure 3.

U.S. Minuteman silos were assumed to be hardened to 1,500 p.s.i., and Titan silos to 300 p.s.i. Modern Soviet land missiles (SS-17, SS-18, SS-19) were assumed to be hardened to 1,500 p.s.i. Older Soviet missiles (SS-9, SS-11, SS-13) were assigned a hardness ranging between 300 and 1,000 p.s.i. This treatment accounts for the ranges that appear under the Soviet columns in Figure 4 above.

Notes to Figure 2-4 (continuation)

In the U.S. attack all Minuteman missiles were expended. The Soviet attack allocated one missile warhead to each of the 1,054 American silos. This hypothetical strategy expended only 25 percent of Soviet land missiles (183 SS-9s, 125 SS-18s including 55 mod two versions with ten warheads each, and 43 SS-19s with six warheads each were expended).

The U.S. bomber force included 335 B-52s and 66 FB-111s. In the analysis 121 bombers, or 30 percent of the total bomber force, were assumed to be alert, and 90 percent of the alert bombers survived the initial attack. Of these, Soviet bomber defenses destroyed 15 percent.

Type	Alert	Survive	Warheads	Yield (Total)
B-52 G/H	77	59	708	236
D/F	24	19	76	76
FB-111	20	15	120	45

As in 1973, all Soviet bombers were assumed to have been destroyed in a pre-emptive U.S. attack.

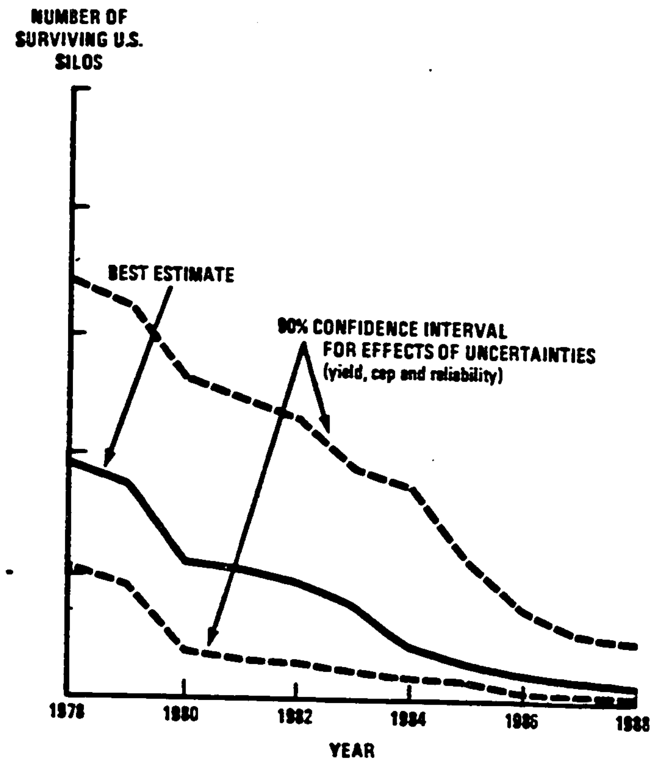
It was assumed that 22 out of 41 American missile submarines were at sea and survivable at any time in 1978. The analogous figure for the Soviet Union was assumed to be 8 out of 56.

	Type	Missiles At Sea	Warheads	Yield (Total)
U.S.				
	Polaris A-3	89	240	82
	Poseidon	272	2720	318
U.S.S.R.				
	SS-N-6	64	64	84
	SS-N-8	56	56	73
	SS-N-17/18	20	52	28

Refinements in Soviet missile accuracy after 1978, coupled with further fractionization (MIRVing) of missile payloads (increasing the number of warheads that can be allocated to each target, thus raising the "kill probability" above that which could be realized if only a single warhead were allocated) moved the Soviets still closer to what many consider to be one of their prime strategic objectives: the capability to destroy virtually the entire U.S. ICBM force. If the standard calculations are to be believed, Soviet strategic missiles will provide this capability in the near future (see Figure 2-5).[28]

With the apparent demise of Minuteman as a viable second-strike force, strategic bombers and missile submarines become the mainstays of U.S. deterrence. Fortunately, they are robust mainstays. The alert portion of both forces appears to be well-protected from sudden attack, and there is no immediate prospect of any serious erosion of either component.

The open ocean is a veritable sanctuary for alert U.S. missile submarines. Once at sea they cannot be readily detected, localized or attacked given the current and foreseeable state of Soviet technology.[29] Soviet antisubmarine warfare forces thus present little danger to U.S. submarines on patrol.[30] Furthermore, by taking advantage of forward bases in Guam, Scotland and (until recently) Spain, the U.S. Navy has managed to sustain a high alert rate. About half of the U.S. force of missile submarines patrol the oceans at any time.[31]



Source: DoD Annual Report Fiscal Year 1980, p. 117.

Figure 2-5

The retaliatory threat carried by these alert units alone is stark. In 1978, after a surprise Soviet attack, they could have delivered some 350 missiles capable of dispensing a combined total of nearly 3,000 warheads.[32] In terms of deliverable explosive power, the amount residing in these weapons was roughly 30,000 times the amount exploded over Hiroshima in 1945.[33] As indicated in Figure 2-4, the level of second-strike destructive power in 1978 was slightly higher than it was in 1973; the expected number of survivable warheads rose substantially (by 38 percent over the five-year period).

Deterioration from age rather than any external threat is the primary source of concern about the future of the missile submarine fleet. All 41 submarines in operation in 1978 were commissioned between 1960 and 1967. Ten of them were recently retired, and the remainder -- 31 Lafayette-class boats (Poseidon) -- will reach the end of their twenty-five year operating cycle at a rate of ten a year beginning in 1988. Hence, all are expected to be retired by 1992.[34]

Analogous problems afflict the strategic bomber force, but they are not as serious. Although the force is mainly comprised of B-52s delivered in the 1956-63 period, most problems associated with age can be corrected through modification and replacement of parts. Many aircraft have underwent structural surgery, and as long as such efforts continue the present fleet should remain structurally sound through the remainder of this century.[35]

The alert bomber force does, however, face significant external threats (unlike the submarine force). In the first place, although alert bombers are poised for a quick getaway in the event of attack, detection and prompt notification of that event are critically important. Aircraft must be aloft well before the arrival of incoming warheads, some of which might be launched on a short time-of-flight trajectory by Soviet submarines positioned near the U.S. coasts. Under the best of circumstances, a surprise attack by Soviet subs would be expected, on the basis of conservative planning assumptions about missile flight times, to destroy some alert bombers.[36] This expectation is reflected in Figure 2-4, which assumes that 10 percent of the alert bomber force would be destroyed on the ground.[37] Standard analyses which calculate the damage more conservatively conclude that upwards of 30 percent could be destroyed, but it would appear that such estimates are overly conservative.[38]

The Soviets actually do not now appear to be pursuing a strategy based on large-scale submarine attacks on bomber bases. If anything, they are withdrawing forces from this mission and concentrating their forces in ocean areas close to home ports, especially Murmansk, where they can be defended against Western ASW forces. Although recent generation submarine missiles launched from the Barents Sea or other waters contiguous to the Soviet Union have enough range to reach the United States, their time of flight would be very long. The prevailing view is that alert bombers would be aloft long before these missiles (as well as Soviet ICBMs with approximately 30-minute flight times) struck U.S. airfields.[39]

The more serious external threat to strategic bombers is the Soviet air defense system. In the 1970s, these defenses could have destroyed perhaps 10-15 percent of the bombers that survived initial attacks on airfields (see Figure 2-4). The technical trend has been running against present-generation penetrating bombers, and it is expected to continue to run against them.

Yet the Soviet deployment of an effective, operational defensive capability is probably a long way off. At present, Soviet terminal defenses -- mainly surface-to-air missiles (SAMs) -- at fixed locations can be easily avoided or suppressed by ICBMs, SLBMs, or SRAMs (short-range attack missiles carried by the penetrating bomber itself). And the Soviet Union lacks an effective interceptor system that enables fighter aircraft to detect and destroy low-flying U.S. bombers. As a result of these deficiencies, U.S. bombers should have at least a 70 percent chance of successful penetration, and that is a conservative estimate. Furthermore, this penetration rate should decrease only marginally during this decade, though some concern exists that new, advanced Soviet defensive capabilities -- in the form of a modern SAM and a "look-down, shoot-down" capability for fighters -- may appear sooner than expected and may pose a formidable threat by the end of this decade. It should also be noted that as Minuteman forces become more vulnerable to preemptive attack, bombers will have to rely less on ICBMs to suppress Soviet air defenses prior to bomber penetration.

Although the future of the present fleet of penetrating bombers — the oldest component of the force structure — is somewhat cloudy, its contribution to deterrence in the current time frame and the recent past is generally thought to be considerable. Even after allowing for surprise attack conditions, significant pre- and postlaunch attrition, and an alert rate that is much lower than it could be (declining, as a result of deliberate policy decisions from about 50 percent in the sixties to 30 percent in the seventies), the amount of destruction that bombers could visit on an attacker would still be immense. Calculations for 1978 (see Figure 2-4) credit the bomber force with a capacity to deliver almost a thousand weapons with a combined yield of 350 megatons, the equivalent of 30,000 Hiroshima bombs.

Adding this amount to the contributions of the other two components, U.S. retaliatory strength, estimated very conservatively, sums to about 1,300 megatons and 5,000 warheads. As indicated in Figure 2-4, there was an overall increase in second-strike warheads and a parallel decrease in cumulative explosive yield over the five-year period (1973-78). The numbers are spread fairly evenly among the three force components, and in absolute terms the figures are very large. If the amount required to achieve the condition of assured destruction is taken to be 400 megatons, then clearly the strategic forces were more than adequate to serve this traditional purpose. Presumably, much of the remainder would have been available for use against military targets. And given the magnitude of this surplus — thousands of weapons and approximately 900 megatons -- the forces could have probably undertaken major operations in the interest of counterforce and related purposes. For this reason, and because assured destruction was provided for as well, it is reasonable to suppose that as of 1978 the U.S. strategic deterrent was robust, stable, and broad, at least under the established technical definition of strategic capability.

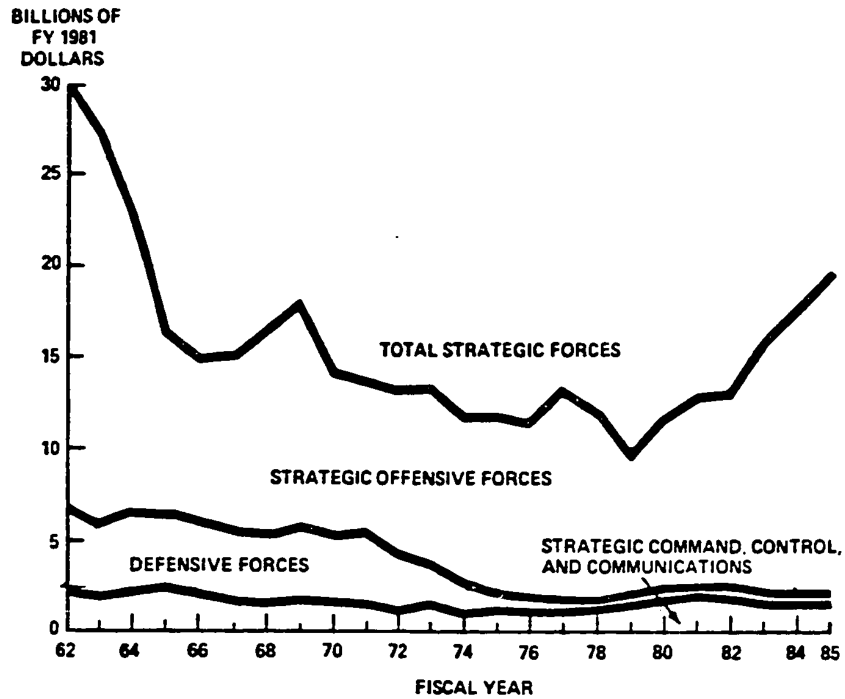
These capabilities have since been declining at a rate that is directly proportional to the increasing vulnerability of the Minuteman force. Although authoritative sources assert that today "Even after riding out a Soviet first strike while on day-to-day alert the United States will be capable of attacking a comprehensive list of military and non-military targets,"[40] the list of destructible military targets, particularly hard targets, is undoubtedly shorter than it was only three years ago. And it is certain to get still shorter unless a concerted effort to bolster the force structure is made.

A force modernization program is in fact underway. And it is not modest. Figure 2-6 projects expenditures for programs pursued by the Carter administration. Summary analysis of its predicted impact on U.S. strategic capabilities is shown in Figure 2-7. As indicated in Figure 2-7, programmed forces were expected to reverse present trends and ensure a situation of rough equivalence with the Soviet Union at least through the end of the decade.

Before describing the main elements of the modernization program proposed by President Reagan, as well as other measures that promise to strengthen U.S. strategic capabilities, we turn to discuss another subject: flexible response.

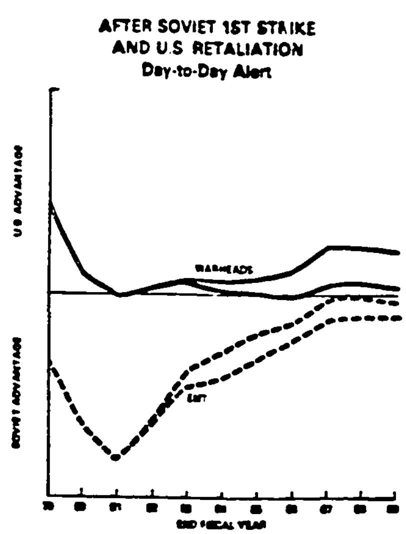
Figure 2-6

STRATEGIC FORCES BUDGET TREND



Source: Department of Defense Annual Report Fiscal Year 1981, p. 71

Figure 2-7



Source: Department of Defense Annual Report Fiscal Year 1981, p. 125

Flexible Statistical Combat

Assessments of the ability of central decisionmakers to execute nuclear forces in a flexible manner fall into several distinct groups: (1) analyses that threat flexibility as a force structure issue; (2) attack plans, especially targeting policy; and (3) studies of the performance of C^3I networks.

1. Flexibility and Survivable Forces: Defining flexibility as a force structure issue reflects the thinking that couples force survivability with the basic national security purposes discussed earlier. In fact, the analytic aims and methods discussed in the previous section and those used to analyze flexibility overlap almost completely. In the latter case, however, greater specificity and political texture are introduced into the scenarios and conclusions. The purposes at stake are not treated as if they were all salient at once. Standard calculations still drive the results, but they are interpreted more in terms of the latitude for politico-military choice and maneuver that they imply.

The basic premise is that in order to have any meaningful choice among politico-military options, forces associated with the options must be able to survive attack. Options are otherwise hollow. The popular variant of limited strategic war which envisions a selective Soviet attack that avoids most large American cities while destroying large segments of the force structure reflects this concern with hollow options. It is argued that if U.S. leaders could not then respond in kind -- because the appropriate forces did not survive in sufficient numbers to execute a proportionate counterforce attack option, then they would capitulate despite their ability to trigger the destruction of Soviet population and industry. Under the circumstances, rational leaders would rule out retaliation based on assured destruction because that would only invite attacks on American cities as well as forfeit all bargaining leverage in the future. By denying U.S. leaders an option that rationally calculating decisionmakers would presumably prefer -- the option to launch an effective counterstrike against Soviet military targets while preserving the threat to Soviet cities -- the Soviets reduce the scope of U.S. flexibility to a point where surrender might be preferred over attacks on industrial centers and other countervalue components of the Soviet target base.

This perspective on flexibility sets up the predominant policy issue as one of ensuring that the force structure is robust. Analyses thus focus narrowly on the size and technical composition of the respective force structures, with a view to assessing whether the Soviets could achieve exploitable dominance by means of selective counterforce attack. The summary calculations in Figure 2-7 can be so interpreted. The results imply that forces programmed by the Carter administration for deployment during the 1980s would have provided the option to mount a selective counterforce attack in response to a Soviet counterforce strike; and, in the wake of such an exchange, a residual force structure as powerful as the opponent's would have equalized bargaining power on both sides. If these calculations are valid, then it would appear that programmed forces were needed to expand the range of effective executive choice and thereby answer, at least partially, the paradox of the retaliatory threat.

Actual war plans and C^3I arrangements are not usually examined under this approach to assessment of the flexibility of the U.S. strategic posture. Hence, the model that generated the results in Figure 2-7 executes hypothetical attack options that only faintly resemble actual target assignments; furthermore, it excludes C^3I operations that would be involved in any attack execution.

The results definitely do not reflect the basis on which the United States actually plans to use its forces. No allowance, for instance, is made for theater nuclear operations to which hundreds of U.S. strategic weapons have been provisionally committed. Similarly, the simulation almost certainly misrepresents the opponent's targeting policy. Such distortion is evident, for instance, in the model's assignment of all Soviet strategic forces to intercontinental operations. Even though many observers believe that a large fraction of Soviet strategic units have always been committed to regional operations, such units are, for purposes of strategic balance calculations, invariably lumped together with other strategic forces. [41]

The usual omission of C^3I parameters is also exemplified by the model. Although an explicit assumption of the simulation is that the initial Soviet attack includes C^3 facilities among its targets, the results reflect none of the plausible adverse consequences of such an attack. [42] In the model, U.S. retaliation is carried out as if it were centrally authorized and fully coordinated. The model also simulates retaliation "in kind," implying accurate characterization of the opponent's initial attack. It also conveys the impression that the residual forces left on each side following a large-scale strategic exchange remain fully responsive (for an indefinite period) to direction by their respective national authorities. And so forth. In other words, the analysis presupposes a sophisticated command system which performs ideally even though the model subjects C^3 to direct enemy attack.

This particular model is representative of a larger class of analyses in that it is set in a "diplomacy of violence" context wherein the risk and consequences of deliberate attacks meant to paralyze an opponent's command structure are downplayed. The use of a notional command structure in strategic enumeration preserves (artificially) this context and the basic deterrence perspective which sees the use of weapons as a means of influencing an opponents behavior rather than incapacitating him.

It is clear that major distortions, omissions, and artifices reduce a typical model's relevance to realistic conditions and call into serious question the validity of its findings. Standard calculations are not very meaningful indicators of the flexibility of the deterrent capabilities of the U.S. strategic posture. Nonetheless, assessments are usually based on these calculations, as though decisionmakers' latitude for choice is essentially determined by force structure conditions.

2. Flexibility and Targeting: Disaggregation of the problem of flexibility also characterizes an approach to analysis that treats the planning assumptions and details of actual strategic war plans as prime concerns. In this view, coercive diplomacy depends for its success on appropriate attack strategy, target priorities, and weapons assignments. War plans should bear relation to the Soviet calculus regarding nuclear war -- threatening his most vital interests, targeting what he values most, exploiting his fears -- in order to provide for maximum influence over his decision process. The plans must also be tailored to provide sensible options for a range of hypothetical circumstances, to allow deterrence to fail in stages, and to facilitate war termination on favorable terms at the earliest possible stage.

Adaptation of targeting policy to changing strategic circumstances and to ongoing assessment of Soviet vulnerabilities and fears has involved the creation of additional option packages as well as some significant changes in target priorities. It is worthwhile to recount some of this history.

The strategic war plan contained a solitary, indivisible option until the early 1960s, when planners created three basic packages: (1) full-scale attack on Soviet/Warsaw Pact military resources, (2) massive attack on enemy cities and industrial centers, and (3) massive simultaneous attack on enemy military and urban-industrial targets. In the event of a conventional, theater nuclear, and/or strategic nuclear attack on the West, U.S. command authorities could have elected to launch the large-scale counterforce attack in retaliation, while withholding forces assigned to countervalue targets.[43] Within limits, different permutations and combinations of target assignments were also possible under this option. Basically, however, they were minor variations on a theme: attacks on a comprehensive list of predesignated military targets. (However, it should be noted that some strategic forces have traditionally been assigned to NATO's general strike plan; these forces, which today include four hundred warheads on Poseidon missile submarines,[44] could be employed in conjunction with other tactical nuclear operations whether or not any options in the strategic war plan were ever exercised).

The next and most recent major revision of targeting doctrine was not undertaken until 1975, when a set of limited attack options were introduced. Figure 2-8 illustrates hypothetically the general nature of these new options. One reason given for the creation of limited strategic options is that the full-scale counterforce package was expected to cause very high collateral damage to the Soviet population and economy. In Schlesinger's words, the option was so massive as to be "virtually indistinguishable from an attack on cities."[45] The revised targeting doctrine was thus motivated in part by a desire to establish more salient nuclear firebreaks and improve the chances of early termination of war. The role of limited options in controlling escalation is well stated in a publication antedating their actual introduction by ten years. According to USAF Basic Doctrine, issued in 1964 under the signature of General C. Lemay, general nuclear war

HYPOTHETICAL STRIKE OPTIONS

Targets[a]	Remote	Urban Collocated	Options[b] A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S[c]
AIRFIELDS																					
Tactical Staging	X					X			X	X			X	X	X	X			X		
Tactical Staging		X													X	X			X		
Strategic Staging	X											X	X	X	X	X			X		
Strategic Staging		X													X	X			X		
DEFENSES																					
Early Warning Radar/ Satellite Tracking (EWR/ST)	X											X	X	X	X	X			X		
EWR/ST		X													X	X			X		
Tallin Air Defense/Galosh ABM		X													X	X			X		
MISSILES																					
IRBM Installations	X					X			X	X			X	X	X	X			X		
IRBM Installations		X													X	X			X		
ICBM Installations	X										X	X	X	X	X	X			X		
ICBM Installations		X													X	X			X		
NAVAL FACILITIES																					
Ports	X											X	X	X	X	X			X		
Ports		X													X	X			X		
STORAGE SITES																					
Nuclear Weapons Depots/Product.	X											X	X	X	X	X			X		
Nuclear Weapons Depots/Product.		X													X	X			X		
PRIMARY CONTROLS																					
C3 Centers	X											X	X	X	X	X			X		
C3 Centers		X													X	X			X		
OTHER MILITARY																					
Troop Concentrations	X								X	X	X		X	X	X	X			X		
Troop Concentrations		X													X	X			X		
URBAN/INDUSTRIAL																					
Electric Power Plants/Dams	X		X		X					X				X		X	X	X	X		
Electric Power Plants/Dams		X														X	X	X	X		
Rail Marshalling Yards	X				X					X				X		X	X	X	X		
Rail Marshalling Yards		X														X	X	X	X		
Key Industrial Plants	X			X	X					X						X	X	X	X		
Key Industrial Plants		X														X	X	X	X		
CITIES		XXX																X	X		
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

NOTES:

[a]Target categories are those presented in Congressional Hearings by the Air Force. The actual number of targets in each category was deleted from the unclassified version of this testimony; however, the order of priority is correct, e.g., more airfields were targeted than defenses.

[b]Options N, P, and Q respectively stand for McNamara's Full-Scale Counterforce, Full-Scale Countervalue, and Full-Scale Counterforce/Countervalue strategies.

[c]An option for Minuteman launch-under-attack was created about 1978. Although characteristics of the option remain secret, it may be speculated that it resembles option K, which represents a large-scale attack against Soviet military targets that are not located near densely populated areas.

Figure 2-8

encompasses three possible types of operations -- countervalue, full-scale counterforce, and limited counterforce. [46] The latter operations:

> ... can vary from a single sortie against one military target to a number of diversified target sorties .... Their objectives are: (1) To demonstrate to the enemy through military action that the United States possesses both the will and the capability to fight at higher levels of intensity to attain the political values at stake, and (2) to convince an enemy that prompt termination of the conflict and negotiations of the issues on reasonable terms are preferable to escalating the war to higher intensity. [47]

Reducing risks of escalation was only one of the objectives of the change of targeting plans. The revision also reflected reassessments of the deterrent effect of different targeting policies. Such policies had been under review since the early 1970s, as part of a wide-ranging study of Soviet threat perceptions. Analysts sought to identify the threats regarded as most grave by the Soviet leadership. By pinning down the Soviet calculus regarding nuclear war, planners hoped to devise a targeting policy which exploits Soviet fears and thereby achieves the optimum deterrent effect. The initial phase of the study effort led to NSDM-242 and NUWEP. Civilian input in the preparation of the latter document, which sets out the attack options, targeting objectives and the damage levels needed to satisfy political guidance contained in NSDM-242 and an associated document (Policy Guidance for the Employment of Nuclear Weapons), was apparently unprecedented. [48]

Additional studies undertaken during the Carter administration centered on such subjects as Soviet views on nuclear war-fighting, Soviet fears of China, the adaptation of targeting to the goal of dismemberment of and regional insurrection within the USSR, and the deterrent effect of targeting Soviet instruments of domestic and external political control -- especially CPSU buildings, command centers used by the political leadership, KGB facilities, and so forth.[49] The conclusions were incorporated in PD-59, signed in 1980, which provided a framework for a strategic war plan containing four basic target groups: (1) nuclear forces, (2) conventional military forces, (3) military and political leadership, and (4) economic and industrial targets. The plan is further divided into the following categories of employment options:

- Major Attack Options

- Selected Attack Options. As an example, to degrade Soviet capabilities to project power in the Middle East-Persian Gulf region, U.S. planners have reportedly developed the nuclear option to strike Soviet military bases and airfields inside the Soviet Union near Iran.[50]

- Regional Nuclear Options. As an example, an RNO might be designed to permit the destruction of the forward elements of an attacking force within a particular area of operations.

- Limited Nuclear Options. These options reportedly permit selective attacks on fixed enemy military or industrial targets. [51]

These options are broken down further to permit central decisionmakers to withhold forces aimed at special classes of targets. Population centers, for example, might be exempted from attacks, as might Soviet national command facilities. Exempting these targets from attack, at least initially, is generally considered to be key to the prevention of escalation. Other withholds, according to Ball, include particular countries included in the strategic war plan. [52] There are many circumstances in which simultaneous attacks on all potential enemy countries -- non-Soviet Warsaw Pact nations, China, Cuba, and Vietnam as well as the Soviet Union proper -- would not be desired. As well, potential targets on allied and neutral territory might be exempted.

Finally, U.S. planners have created special options for preemptive attacks on the enemy target bases, and for launching U.S. forces upon receipt of tactical warning of a Soviet attack. [53]

Although with few exceptions these and earlier options packages have their own unique logic which can be understood without bringing the issue of force vulnerability into the picture, force structure overtones are unmistakenly present in their development. It is no coincidence that the proliferation of options packages paralleled the emergence of a modern Soviet strategic arsenal.

As long as the United States enjoyed a nuclear advantage such that it could destroy, in retaliation to any and all forms of Soviet attack on the West, virtually the entire enemy target list including any unutilized strategic forces, U.S. planners were not apt to make allowances for portions of the force structure to be withheld, even if they envisaged a less than all-out Soviet assault. Furthermore, if unutilized Soviet forces seemed highly vulnerable to U.S. counterattack, as was once the appearance, then U.S. planners had strong reason to expect a comprehensive Soviet attack at the outset. And there was a strong presumption that in spite of the paradox of the retaliatory threat, such an attack would provoke an equivalent response -- that is, all-out retaliation against the entire enemy target list.[54] Prevailing expectations with respect to the likely scale of Soviet attacks and the scale and decisiveness of U.S. retaliation somewhat diminished the perceived importance of limited retaliatory options.

But the paradox of the retaliatory threat and the imminent prospect that Soviet strategic deployments would be able to survive preemptive or retaliatory strikes by U.S. forces carried implications that were not lost on policy officials. As early as 1960, the role of options packages had become salient and well appreciated. The flexibility to withhold portions of the U.S. force was deemed essential to deter the employment of Soviet forces held in reserve, and to counter the bargaining leverage such reserve forces might otherwise confer following an initial exchange.[55] And as the gap between the capabilities of the force structures gradually narrowed, the situation warranted adoption of an increasingly flexible posture. By the mid 1970s, U.S. planners were creating smaller option packages, including some that involved demonstration strikes, and refining others so that, for example, counterforce attacks could be distinguished from an attack on cities.

There will always be some residual doubt about the appropriateness of particular war plans. Scenarios are highly speculative. Gauging the deterrent effect of different strategies is highly subjective. Policies emerge without benefit of any solid empirical foundation, the absence of which results (unavoidably) in the elevation of theory, bald assumption and hand-waving over data, fact and scientific conclusion. By virtue of these limitations, the question whether current war plans effectively foreclose enemy options must remain moot.

Nevertheless, it is generally believed that the proliferation of option packages has been an appropriate reaction to changes in the force balance and that planners can devise options that offer rational responses to the most imaginable of wartime circumstances. In other words, prevailing opinion holds that war plans have not by themselves so severely constricted the range of executive choice that rationally calculating decisionmakers would not have appropriate options at their disposal in wartime.

This does not imply that available weapons inventories adequately flesh out the objectives of the option packages contained in the war plan. To the contrary, the last two administrations have asserted that force structure modernization is now necessary.

As well, C^3I arrangements may not support a flexible strategy, irrespective of the amount of flexibility offered by a modernized force structure and an elaborate, option rich war plan. The last two administrations have determined that the command structure is indeed inadequate and that major improvements are needed to bring it into close alignment with a nuclear strategy of flexible response. Under the Reagan administration, command structure development has been assigned a priority equal to that of strategic force modernization.

3. Flexibility and C^3I Networks: Although U.S. strategic employment doctrine has incorporated plans for flexible and graduated use of strategic nuclear force since the early 1960s, the public record is lacking in authoritative assertions that C^3I networks could continue to function beyond a few hours after the first enemy weapons had landed. As declaratory doctrine and actual operations plans grew increasingly sophisticated, demands on C^3I networks mounted, but until recently the criteria used to evaluate the performance of these networks were derived from the simpler procurement principle of assured destruction. Under this principle, C^3I networks need only meet minimum standards of performance: reliable detection of enemy nuclear attack and rapid dissemination of a short message (the "go code") releasing the entire arsenal in a comprehensive attack. For two decades and more, established war plans have implicitly required that C^3I networks provide for control through a series of exchanges, but formal imposition of requirements that exceed the minimum needed for assured destruction have been resisted. H.D. Benington, then a key official

responsible for command development, exemplified this attitude. In his view, C^3I networks designed to support flexible response would "merely add complexity at the possible expense of reliability." [56] Benington, like his contemporaries of the late 1960s, concluded that "it appears that it is better to keep retaliation pure, simple, and as unsophisticated as possible." [57]

Now that flexible response pervades strategic policy and planning, C^3I networks are being evaluated against a set of more stringent standards. Lt. Gen. H. Dickinson, the chief military architect of strategic C^3I during the Carter administration, is the source of a proposed set of revised criteria which he summarizes as follows:

> To support a credible deterrence posture and war-fighting capability, strategic C^3 systems must provide tactical warning and attack assessment (TW/AA), strategic force control, execution, termination, and Strategic Reserve Force employment for extended periods after absorbing a well-coordinated attack regardless of U.S. force and alert posture. [58]

According to D. Ball, who assessed the performance of present U.S. C^3I systems against a similar set of criteria, the controlled, flexible employment of current U.S. strategic forces is illusory:

> ... it is most unrealistic to expect that there would be a relatively smooth and controlled progression from limited and selective strikes, through major counterforce exchanges, to termination of the conflict at some level short of urban-industrial attacks.... In fact, control of a nuclear exchange would become very difficult to maintain after several tens of strategic nuclear weapons had been used, even where deliberate attacks on command-and-control capabilities were avoided. [59]

Ball's analysis thus confirms an earlier assessment by J. Steinbruner that "regardless of the flexibility embodied in individual strategic forces, the precariousness of command channels probably means that nuclear war would be uncontrollable, as a practical matter, shortly after the first tens of weapons are launched." [60]

Reagan administration officials openly acknowledge that U.S. C^3I systems have not kept pace with evolving strategy and enemy threats to those systems. Recent studies have apparently exposed serious shortcomings, many of which defy ready solution. To D. Latham, current deficiencies underscore what "a very difficult job" it is "to make a system endure and be a war-fighting system in a protracted conflict." [61] It is apparent that, in the official estimation, current U.S. C^3I systems lack "an enduring capability to counter the Soviet capabilities for protracted conflict." [62] Chapter 7 of this report concludes that current C^3I capabilities for flexibility and endurance are indeed extremely limited. Chapter 8 examines the Reagan administration's proposed correctives.

REMEDIES AND SOLUTIONS

Strategic Modernization

The Reagan administration believes that the United States must increase the number, destructiveness, endurance and responsiveness of U.S. strategic forces in order to convince the Soviet leadership that "there can be no circumstance in which it could benefit by beginning a nuclear war at any level or of any duration." [63] At the moment, U.S. defense officials seem fearful that "the Soviets could envision a potential nuclear confrontation in which they would threaten to destroy a very large part of our force in a first strike, while retaining overwhelming nuclear force to deter any retaliation we could carry out." [64] U.S. forces must be sized to deny any such advantage to the opponent; hold at risk those political, military, and economic assets that Soviet leaders value most highly; and allow for terminating a nuclear conflict and "reestablishing deterrence at the lowest possible level of violence." [65]

In October 1981, President Reagan outlined a strategic modernization program that supposedly will prevent Soviet realization of strategic dominance over the United States. To arrest alleged destabilizing trends in the strategic balance, and in particular to offset Soviet advantage in prompt hard target counterforce capability, U.S. strategic power will be revitalized in five major areas:

- Augment and Upgrade Strategic C^3I
- Modernize the Manned Bomber Force
- Deploy New, More Accurate and Powerful SLBMS
- Improve Land-Based Missiles' Accuracy, Power and Survivability
- Strengthen Strategic Defenses

Augment and Upgrade Strategic C^3I: This goal takes precedence over the rest. In his FY 1984 Annual Report, Secretary Weinberger states that the administration has given "highest priority to increasing the ability of our strategic force management systems not only to survive but to remain capable of performing their basic functions throughout a sustained sequence of Soviet attacks." [66]

Dozens of programs are included in the C^3I modernization package. Descriptions of selected key program elements are found in Chapter 8. For present purposes, suffice it to say that the administration believes that its C^3I plan, once implemented, "would deny the Soviets the option of either attempting a decapitation attack, or using protracted war tactics to exploit the limitations of our C^3I system, and would provide the U.S. with a C^3I system compatible with our strategy of deterrence [flexible response]." [67]

Modernize the Manned Bomber Force: [68] At the end of 1983, the number of U.S. strategic bombers in the operational inventory will be about 322 (266 B-52s and 56 FB-111s). Modernization of this force is required to ensure weapon penetration in the face of improving Soviet air defense systems. Some B-52s are thus being refitted to carry air-launched cruise missiles (ALCMs) that can be delivered at long distances from the target. The first squadron of ALCM-equipped B-52G aircraft became operational in 1982. The administration further plans to deploy 100 new B-1B bombers in the mid 1980s, and to begin deployment of 132 advanced "Stealth" bombers in the early 1990s. About 3,200 ALCMs will eventually be deployed on these newer aircraft as well as the older B-52 force, with perhaps a half of the total cruise missile inventory having first-generation characteristics and the remainder having "Stealth" characteristics associated with a second-generation version now under development.

Deploy New, More Accurate and Powerful SLBMs: [69] Construction of Trident submarines to augment, and eventually replace, the aging Poseidon fleet, will continue at a rate of one per year. The first Trident submarine was commissioned in 1981. By the end of 1983, the Navy will have three Trident submarines, each with twenty-four C-4 missiles, in addition to thirty-one Poseidons, each carrying sixteen C-3 or C-4 missiles. Ten Tridents have been authorized through fiscal year 1983, and it is expected that authorization for ten more will be requested in the years ahead.

Beginning in 1989, D-5 missiles will be deployed on Trident submarines. Compared to the C-4 missile which is carried by twelve Poseidons and the first eight Trident submarines, the D-5 is larger, more powerful and accurate. With seventy-five percent more payload and an accuracy approaching 400 feet CEP, the D-5 could be used "to attack any target in the Soviet Union, including their missile silos." [70] This "hard target kill" capability offers, for the first time, the ability to use missile submarines to strike the complete spectrum of targets in the Soviet Union. [71]

Also, starting in 1984, sea-launched cruise missiles (SLCMs) will be deployed on attack submarine and surface ships to strengthen the Strategic Reserve Force. [72]

Improve Land-Based Missiles' Accuracy, Power and Survivability: [73] Between 1986 and 1988, 100 MX missiles will be lowered into existing Minuteman silos. The Minuteman force will be reduced to 900 launchers, and the Titan force will be retired.

MX is twice as accurate as current Minuteman missiles. It can deliver up to ten warheads, compared to three for Minuteman III and one for Minuteman II. These attributes, together with increased explosive yield, give MX the prompt "hard target kill capability necessary to retaliate effectively against the most highly valued and increasingly hard Soviet targets." [74] Administration officials argue that MX would rectify an existing imbalance in prompt hard-target capability which presently is "the most dangerous feature of the current strategic situation." [75] MX forces will put hardened Soviet C^3 facilities at risk, [76] and "break the Soviet monopoly on prompt counter-ICBM capabilities." [77]

Housing MX missiles in Minuteman silos, however, does not enhance force survivability. The administration has therefore proposed to begin engineering design work on a small, single-warhead ICBM popularly known as Midgetman. Full-scale development of Midgetman could begin as early as 1986, with initial deployment in the early 1990s. It may operate in a variety of fixed and mobile modes -- due to its small size -- and yet prove to be accurate enough to destroy very hard targets. Other measures that might enhance ICBM survivability range from superhardening of missile silos to launch-under-attack. Research on the former is under way and holds out some promise. Launch-under-attack is in one sense a policy option that is already available. The president may simply decide to execute the strategic forces before the full weight of enemy attack is absorbed, thereby permitting more forces, particularly ICBMs, to escape destruction. In principle, that decision -- not to ride out the attack -- already rests with national authorities. But implementation of such a decision is not, practically speaking, easily performed. Technical and procedural adjustments are required to achieve high confidence in our ability to exercise this policy option (see Chapter 7).

Strengthen Strategic Defenses: The administration seeks to close large gaps in coverage in the North American air defense network; replace obsolete air defense interceptor aircraft; pursue a vigorous research effort in the area of ballistic missile defense; and continue development of an operational antisatellite system.

Strategic Arms Control

The strategic modernization program outlined above could be fully implemented under either the provisions of the unratified SALT II agreements, to which both parties have adhered by informal understanding, or the provisions proposed by the United States at the ongoing START negotiations. At the same time, the U.S. proposal at START calls for drastic reductions in the Soviet weapons that sparked the latest drive to modernize the American arsenal.

Those Soviet weapons that are the focus of U.S. concern are the SS-18s and SS-19s, which presently confer a large Soviet advantage in prompt hard target kill capability. The Soviets have 308 SS-18s, which can carry ten warheads each, and 330 SS-19s, which carry six warheads each. Using less than half of these weapons, the Soviets theoretically could knock out the Minuteman force in a first strike. 2500 Soviet residual weapons, capable of hard target attack, would be available for other uses. This residual capability alone vastly exceeds the hard target attack capability of all 1,000 Minuteman missiles.

The American proposal would reduce SS-18 and SS-19 launchers to 110 and 100, respectively, in exchange for reductions of 425 Minuteman launchers (to 575 from the present level of 1,000). Although the Soviets theoretically could still knock out the downsized U.S. Minuteman forces, the size of their residual SS-18/19 force following a 2:1 attack would be much smaller (500 instead of 2500). Furthermore, that force would pale in comparison with the survivable, prompt hard target attack capability in the U.S. arsenal after the president's modernization program has been implemented.

By all indications, the Soviet Union will not accede to the U.S. demand for deep cuts in their heavy land-based missile force. Despite signs of American willingness to accept a higher subceiling on SS-18/19 missiles, the positions of the protagonists seem too far apart for marginal compromises to bring them together. At present, U.S. policymakers surely do not expect arms negotiations to succeed in removing what they perceive to be the major source of instability in the strategic situation. To the contrary, they generally see strategic modernization of U.S. forces as the only promising remedy.

SUMMARY

As the two superpowers amassed weapons of mass destruction and mated them with survivable delivery vehicles, orthodox views of military conquest became anachronistic. Increasingly remote were the prospects of overcoming enemy military strength by brute force. Increasingly probable was a war in which both sides would suffer massive damage and casualties.

Untenable notions about military victory in the nuclear age were supplanted by a conception of the strategic problem which linked nuclear weapons with mutual deterrence. It became almost axiomatic that nuclear attack would not be initiated by rational decisionmakers as long as both sides possessed enough survivable forces to virtually annihilate an aggressor nation's economy and cities.

Rational deterrence theory nonetheless spawned limited war scenarios in which strategic weapons are brandished if not actually used to achieve exploitable bargaining dominance. Standard calculations which pit nuclear forces against each other in statistical combat to produce measures of counterforce effectiveness and postexchange residual capabilities are commonly used to gauge enemy potential to achieve such dominance. According to these calculations, the U.S. Minuteman force is highly vulnerable to Soviet attack and the U.S. force structure as a whole compares unfavorably with the Soviet force structure in terms of counterforce capability. This alleged imbalance supposedly confers an exploitable advantage on the Soviet Union. To close this "window of vulnerability," the United States Government has embarked on a course of strategic modernization that emphasizes weapons for prompt hard target attack and command networks for control of those weapons during a protracted conflict.

FOOTNOTES

1. Alain C. Enthoven and K. Wayne Smith, How Much Is Enough? Shaping the Defense Program, 1961-1969 (New York: Harper and Row, 1971), p. 207.

2. John D. Steinbruner, "Beyond Rational Deterrence: The Struggle for New Conceptions," World Politics, vol. 28 (January 1976), p. 225.

3. Michael Mandelbaum, The Nuclear Question (Cambridge: Cambridge University Press, 1979), p. 218.

4. The most thorough development of this basic theme is Thomas C. Schelling's Arms and Influence (New Haven: Yale University Press, 1966).

5. "U.S. strategic forces are not procured for a damage limiting mission. However, should a nuclear war occur, our forces may be utilized to limit damage to the United States to the extent practicable in addition to being used to destroy resources which contribute to the postwar power, influence and recovery capability of the enemy." Statement by then Secretary of Defense Harold Brown, U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 1, p. 554.

6. Enthoven and Smith, How Much Is Enough? p. 207.

7. Steinbruner, "Beyond Rational Deterrence," p. 227.

8. Ibid., pp. 231-34.

9. Schlesinger testimony, and articles.

10. See Desmond Ball, "Counterforce Targeting: How New? How Viable?" Arms Control Today, vol. 11 (February 1981), pp. 1-9; and U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 1, p. 556.

11. Ball, "Counterforce Targeting," p. 2.

12. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1978, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 2, p. 212.

13. Department of Defense Annual Report Fiscal Year 1979 (Department of Defense, 1978), p. 55; Department of Defense Annual Report Fiscal Year 1980 (Department of Defense, 1979), p. 77; and Department of Defense Annual Report Fiscal Year 1981 (Department of Defense, 1980), pp. 65, 79.

14. Department of Defense Annual Report Fiscal Year 1982 (Department of Defense, 1981), p. 42.

15. Department of Defense Annual Report Fiscal Year 1980 (Department of Defense, 1979), pp. 77-78.

16. "In support of national security policy, the nation's telecommunications must provide for: (1) connectivity between the National Command Authority and Strategic and other appropriate forces to support flexible execution of retaliatory strikes during and after

an enemy nuclear attack; and (2) responsive support for operational control of the armed forces, even during a protracted nuclear conflict." Presidential Directive/NSC-53 (The White House, November 15, 1979), p. 1.

17. Steinbruner, "Beyond Rational Deterrence," p. 227.

18. Enthoven and Smith, How Much Is Enough? pp. 178-79, 208.

19. John D. Steinbruner and Thomas M. Garwin, "Strategic Vulnerability: The Balance Between Prudence and Paranoia," International Security, vol. 1, no. 1 (Summer 1976), p. 168.

20. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 1, p. 539.

21. Department of Defense Annual Report Fiscal Year 1979 (Department of Defense, 1978), p. 106.

22. Perhaps the least defensible use of the assumption of strategic warning failure concerns standard calculations of bomber prelaunch vulnerability. In most analyses, ground alert bombers come under heavy attack by as many as 20 Soviet missile submarines positioned in U.S. coastal waters, a massive departure from peacetime patrol practices which goes undetected or unheeded. U.S. intelligence could hardly fail to detect deployments of this magnitude, and U.S. decisionmakers could hardly fail to respond with measures -- for instance, increasing alert bomber readiness, bringing off-alert bombers to alert, dispersing aircraft to inland bases, and so forth -- to

reduce the force's vulnerability. Yet, conservative planners base their calculations on the assumption that no such steps would be taken.

23. Declassified Posture Statement.

24. Appendix A provides assumptions.

25. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 1, p. 584.

26. The lethal index, or *K*, or U.S. missile forces are shown for comparison. It should be noted that *K* is more sensitive to accuracy than weapon yield. U.S. warheads, even though usually smaller in yield than Soviet warheads, have had greater nominal lethality because of their better accuracy. Soviet deployment of fourth-generation ICBMs erased this edge.

27. Assumes force characteristics shown in Figure 2-3. Minuteman silos were assigned a hardness of 1,500 p.s.i. By comparison, U.S. ICBMs launched in a preemptive attack could have destroyed between 40 and 60 percent of the Soviet land missile force, depending on Soviet silo resistance to blast overpressure. Assumes force characteristics shown in Figure 2-3. SS-17, -18, and -19 ICBMs were assigned a silo hardness of 1,000-1,500 p.s.i. in the calculations. SS-9, -11, and -13 ICBMs were assigned a hardness of 300-1,000 p.s.i.

28. The United States is not standing still in this regard, and will theoretically pose an analogous threat within ten years.

29. While there is consensus on this point, that is, that today and in the decade ahead the Soviets could not conduct an effective campaign of open-ocean ASW, there is concern in some quarters that communication antennas trailed by U.S. missile submarines could become more susceptible to detection by nonacoustic sensors such as spaceborne radar. The chances of detection would still be remote, but it is generally believed that even sporadic detections could furnish Soviet ASW forces with useful information about U.S. patrol patterns. Soviet ASW capabilities are assessed by Bruce G. Blair, "Arms Control Implications of Anti-Submarine Warfare (ASW) Programs," Evaluation of Fiscal Year 1979 Arms Control Impact Statements, Report for Committee on International Relations, U.S. House of Representatives (Washington, D.C.: GPO, 1978), pp. 103-119.

30. The United States is dramatically "ahead" in ASW capability. Dated assessments that seem valid today conclude that the ability of the United States to mount a totally effective, preemptive strike against Soviet SSBNs does not exist and "is not practically achievable" and indeed that there is "no realistic prospect of being able to destroy in a sudden attack a major part of the deployed Soviet force of missile-launching submarines, certainly not before they could launch their missiles in retaliation." U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, 95th Congress, 1st Session

(Washington, D.C.: GPO, 1977), Part 10, p. 6756; and U.S. Congress, Senate, Committee on Appropriations, DOD Appropriations for Fiscal Year 1975, 93rd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 1, p. 45. At the same time, it is stated that the United States does have "a good capability to destroy enemy submarines in a protracted war at sea." Ibid. And there are clear indications that the Soviets worry a good deal about the survivability of their subs. The deployment of Delta-class SSBNs armed with long-range missiles (4,800 n.m.) reflects this concern. Since Delta submarines can strike the United States from home waters (for example, the Barents Sea), Soviet naval forces can better defend these missile submarines against Western ASW forces. By the middle of 1978, the Soviets had several hundred single-warhead missiles and sixty MIRVed missiles operational in Delta submarines, and had demonstrated some capability to protect those forces at sea. Soviet Yankee class submarines armed with relatively short-range missiles (1,500 n.m.) still had to contend with an impressive array of Western ASW elements, however. These subs must transit a dangerous course to reach launch stations off U.S. coasts. For further discussion of U.S. ASW capabilities against Soviet SSBNs, see Blair, "Arms Control Implications of Anti-Submarine Warfare (ASW) Programs."

31. Blair, "Arms Control Implications of Anti-Submarine Warfare (ASW) Programs," p. 104. By comparison, 85 percent of the Soviet missile submarine fleet is anchored in port under normal conditions.

32. Assuming perfect missile reliability.

33. The amount residing in the relatively secure portion of the Soviet submarine deterrent was smaller by comparison, but still large by absolute standards. Assuming that 15 percent of the Soviet force operated at sea at any time, some 700 missiles and 800 warheads were vulnerable to surprise attacks aimed at coastal ports. Discounting Western ASW capabilities entirely, the remaining force of Delta- and Yankee-class subs could have delivered 140 missiles and 172 warheads in retaliation, for a combined yield equivalent to 15,000 Hiroshima bombs.

34. See Lawrence J. Korb, "The FY 1981-1985 Defense Program: Issues and Trends," AEI Foreign Policy and Defense Review, vol. 2, no. 2, pp. 40-41.

35. For a graphical projection of B-52 G/H, D, and FB-111A aircraft life expectancy, see U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 1872, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 3, Book 1, p. 629.

36. Surprise attack in the other direction would be expected to destroy virtually all Soviet long-range bombers, because they are evidently maintained at a very low state of readiness. See Joseph J. Kruzel, "Military Alerts and Diplomatic Signals," in The Limits of Military Interventions, Ellen P. Stern, ed. (Beverly Hills: Sage Publications, 1977), p. 88. U.S. Poseidon submarines are apparently assigned Soviet bomber bases as targets. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1978, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 2, p. 186.

37. This estimate is in accord with former Defense Secretary Brown's statement that virtually all alert B-52s can take off before the arrival of Soviet weapons. U.S. Congress, House, Committee on Armed Services, Review of the State of U.S. Strategic Forces, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), p. 195. See also U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1977 Authorization for Military Procurement, Research and Development, 94th Congress, 2nd Session (Washington, D.C: GPO, 1976), Part 5, pp. 2937, 3029.

38. Such calculations typically assume that Soviet missile submarines would be launched on a "depressed trajectory" which cuts flight time by 50 percent and thereby reduces the chances of bomber survival. The assumption is extremely conservative, in view of the fact that the Soviets have never tested any sub-launch missile in a depressed trajectory profile.

39. Some potential Soviet submarine launch stations in the polar regions, however, were not adequately covered by U.S. tactical warning systems during the 1970s.

40. Department of Defense Annual Report Fiscal Year 1981 (Department of Defense, 1980), p. 126.

41. Soviet weapons usually included in strategic calculations but generally believed to have a regional or theater mission are the entire bomber force, SS-11 and -17 ICBMs in MRBM/IRBM fields, and most Yankee-class SSBNs. The wartime role of the SS-11 is considered in U.S. Congress, Senate, Committee on Armed Services, Department of

Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C: GPO, 1978), Part 9, p. 6554.

42. "A meaningful ... way to assess the deterrent capability of our strategic posture is to examine how our forces might perform in response to a hypothetical Soviet attack on them and on command, control, and communications (C^3) facilities associated with the operational control and employment of these forces .... This assessment does not ... reflect the uncertainties resulting from the attacks on our C^3 systems." Department of Defense Annual Report Fiscal Year 1981 (Department of Defense, 1980), pp. 123-24.

43. See U.S. Congress, House, Committee on Armed Services, Authorizing Appropriations for Aircraft, Missiles and Naval Vessels, 88th Congress, 1st Session (Washington, D.C: GPO, 1963), Report 62, March 6, 1963, p. 16.

44. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1979, 95th Congress, 2nd Session (Washington, D.C: GPO, 1978), Part 2, pp. 848-49.

45. U.S. Congress, Senate, Subcommittee on Arms Control, International Law and Organization, U.S.-USSR Strategic Policies (Washington, D.C.: GPO, March 4, 1974).

46. USAF Basic Doctrine (Department of the Air Force, August 1964), p. 3-1.

47. Ibid.

48. Ball, "Counterforce Targeting," p. 2.

49. Ibid., p. 7.

50. Ibid., pp. 6-7.

51. Ibid., p. 6.

52. Ibid.

53. Ibid.

54. The odds for comprehensive retaliation were regarded as overwhelmingly high. A report in 1963 by the House Armed Services Committee contains a representative view: "In talking about global nuclear war, the Soviet leaders always say that they would strike at the entire complex of our military power including Government and production centers, meaning our cities. If they were to do so, we would, of course, have no alternative but to retaliate in kind." U.S. Congress, House, Committee on Armed Services, Authorizing Appropriations for Aircraft, Missiles and Naval Vessels, p. 16.

55. Ibid.

56. "Can Vulnerability Menace Command and Control?" Armed Forces Management, vol. 15 (July 1969), p. 41.

57. Ibid., pp. 41-42.

58. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), Part 7, p. 493.

59. Desmond Ball, "Can Nuclear War Be Controlled?" Adelphi Papers, no. 169 (London: International Institute for Strategic Studies, 1981), pp. 35-36.

60. John D. Steinbruner, "National Security and the Concept of Strategic Stability," Journal of Conflict Resolution, vol. 22 (September 1978), p. 421.

61. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 5, pp. 4, 24.

62. Richard D. DeLauer, The FX 1984 DoD Program for Research, Development, and Acquisition (Department of Defense, 1982), p. V-1.

63. Department of Defense Annual Report Fiscal Year 1984 (Department of Defense, 1983), p.51.

64. Ibid., p. 53.

65. Ibid., p. 52.

66. Ibid., p. 54.

67. DeLauer, The FX 1984 DoD Program for Research, Development, and Acquisition, p. V-5.

68. Congressional Budget Office, Modernizing U.S. Strategic Offensive Forces: The Administration's Program and Alternatives (Washington, D.C.: GPO, 1983), pp. 7-8.

69. Congressional Budget Office, Modernizing U.S. Strategic Offensive Forces, pp. 9-11.

70. "Background Statement From White House on MX Missile and B-1 Bomber," New York Times (October 3, 1981).

71. DeLauer, The FX 1984 DoD Program for Research, Development, and Acquisition, p. V-7.

72. Ibid.; and "Background Statement from White House."

73. Congressional Budget Office, Modernizing U.S. Strategic Offensive Forces, pp. 2-7.

74. DeLauer, The FX 1984 DoD Program for Research, Development, and Acquisition, p. V-8.

75. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 5968, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 2, p. 62.

76. Ibid.

77. "Background Statement from White House."

CHAPTER THREE

ORGANIZATIONAL DIMENSIONS OF STRATEGIC PROGRAMS AND OPERATIONS

The framework of rational analysis seems to provide considerable leverage on the strategic problem. It offers an apparently sound conceptualization — the logic of mutual deterrence — as well as a methodological fulcrum for moving strategic logic onto a concrete defense platform. Both crisis decisionmaking and strategic budget/program planning are placed under a descriptive and normative decision framework with three distinguishing characteristics. First, decisionmaking is subjectively rational, in the nontrivial sense that decisionmakers have a set of objectives in mind and some reasons for choosing one particular policy alternative over another. Put differently, decisionmaking is disciplined by a logical approach to maximizing values: specify objectives (pin down the nature of relevant costs and benefits), judge (calculate) the expected payoffs of alternative courses of action, and select the alternative with the highest payoff. Second, the decision process is characterized as objectively rational in that it would not be trivial for someone who understands the decision problem to identify significantly better alternatives than those actually being considered. (Decisionmakers are credited with the ability to develop appropriate — objectively rational -- investment strategies, contingency plans, and so forth.) Third, implicit in this logic-of-choice characterization of the decision process is the image of an individual or close-knit group actively involved in steering the ship of state. Thanks to a well-oiled rudder that is well connected to the steering wheel, executive control is firm and positive. Suborganizations involved, for instance, in procuring or operating strategic forces, respond quickly and smoothly to the manipulations of a central steersman.

A critique of the rational analysis model begins with the observation that organizations with responsibilities for strategic programs comprise a multitude of people and activities. These organizations are simply too large and cumbersome for a single person or committee to steer them in any detailed way. Centralized coordination by means of exhaustive instruction from a central steersman would obviously be a monumental and futile undertaking.

It is apparent, moreover, that <u>most</u> of the people and activities connected with strategic programs are but loosely and indirectly connected to the steering wheel. Behavior is substantially driven by decentralized forces: a diffuse authority structure; restricted and disaggregated streams of information; and specialized sets of low-order decision rules (standard operating procedures, rules of thumb, precooked plans, and so forth). In short, the decision process is highly disaggregated.

Significant decentralization is unavoidable, and it is not without virtues. Overcentralization would otherwise exist to hamper, for instance, the preparation of a coherent defense budget, or the management of crisis diplomacy. In the latter instance, extreme centralization would force national officials to devote an excessive amount of time and effort to force management, at the expense of addressing the political problems that caused the crisis in the first place. Decentralization alleviates overburden at the center by shifting a considerable amount of decisionmaking power and responsibility to the periphery. Overburden at the periphery and, for that matter, at all levels of command, is further alleviated by built-in decision rules that automatically trigger preprogrammed organizational responses when certain predefined conditions appear.

The existence of significant decentralization in strategic organizations is not a radically new appreciation, but it carries an important general implication that the central steersman image of strategic decisionmaking does not come to grips with: ample scope exists for discontinuity between national policy intentions and actions taken at subordinate echelons.

This fact is particularly relevant to command structure development. As discussed earlier, the Reagan administration aims to create a command system that allows for central, flexible direction of strategic forces during a protracted nuclear conflict. Such a system is the operational linchpin for a nuclear war-fighting and bargaining strategy, which is the logical answer to the paradox of the threat of massive retaliation. However, the aim of current policy may be unrealistic, for two basic reasons. First, existing institutions involved in the design and funding of command modernization programs are notoriously maladroit in handling central systems, because the institutions themselves are decentralized. Also, these institutions are not natural allies or proponents of centralization. Second, the basic policy aim naively overestimates the potential responsiveness of combat organizations to central command. Only so much flexibility and centralization can be accommodated (or would be tolerated) by the organizations that actually operate the strategic forces. The aspirations of the Reagan program appear to lie far beyond those limits.

These are topics worthy of further discussion. Implicit in the discussion below is a critique of the rational analysis framework. Our principal aim, however, is to illuminate the problems of command structure development so that they might be more effectively tackled.

MANAGEMENT OF PROGRAMS AND BUDGETS: INSTITUTIONAL LAISSEZ-FAIRE

Throughout the post WWII era, a diffuse decision process has determined the physical and organizational characteristics of C^3I networks. System configuration has been largely shaped by and for suborganizations, without much concern for overall integration and centralization. Decentralization was literally wired into the communications network, leaving national officials without the physical means they would need to bring strategic operations under firm central control. And the entire multibillion dollar investment, which in the words of one observer was made "without even the semblance of a conceptual rationale," [1] resulted in a C^3I infrastructure — called the World Wide Military Command and Control System [2] — that stubbornly resists attempts at rewiring it to strengthen the interfaces between central decisionmakers and subordinate echelons.

Prior to 1958, progress toward integration and centralization of C^3I elements was effectively blocked by legislative barriers. The National Security Act of 1947, and the Amendment of 1949, decreed that the military departments would be administered as individual executive entities by their respective Secretaries. Authority vested in the Secretary of Defense was quite limited by comparison. His mandate was to provide general direction and guidance to the military departments. The pertinent legislation thus sanctioned, indeed tacitly approved, a buildup of separate C^3I networks in each military department. The departments proceeded to do just that, and the result, seen from a defense-wide perspective, was a hodgepodge of fragmented C^3I subsystems.

The Defense Reorganization Act of 1958 relaxed the restrictive covenants of earlier legislation. The Office of the Secretary of Defense (OSD) was empowered, for instance, to place C^3I programs under its purview. Yet the chaotic adhocracy that characterized earlier management practices continued to operate. Although the Act gave Assistant Defense Secretaries considerable authority over the military departments and their respective C^3I programs, OSD organized itself so ineffectively that it all but surrendered its management perogatives in this particular sphere of defense activity.[3] With management responsibilities divided up among four assistant secretaries, the Director of Defense Research and Engineering, and numerous OSD staff offices, the _laissez-faire_ practices of the military departments were mimicked at the OSD level. In a report critical of this arrangement it was written that:

> ... communications was not considered as a system requiring integrated and unified consideration and a corporate management.... These fragmented and overlapping responsibilities resulted in inefficient and ineffective communications management throughout the Department.[4]

Under the 1958 Act, the Secretaries of the military departments, though no longer included in the chain of combat command, retained primary responsibility for the C^3I networks used by combat commanders. The departments would engineer, install, man and operate these networks in support of the newly created unified and specified commands.

These combat commands were supported at the expense of national command system development, owing in part to ineffectual management at the OSD level, and even the C^3I needs of the unified/specified commands were ministered with prejudice. The military departments opposed, for instance, interservice consolidation of C^3I channels within each of the unified commands, even though the basic idea of a unified command is to fuse forces from two or more branches to permit joint operations within a particular geographical region. This opposition, attributed to service parochialism,[5] meant that communications channels would remain separate (with the military departments providing C^3I support for their affiliated forces exclusively, within each unified command), to the detriment of force coordination.

The unified, specified, and subordinate combat commanders also lacked a strong voice in the development of the C^3I networks upon which they relied. The priority, direction, and technical aspects of C^3I development were largely determined by the military departments, not the senior combat commanders, whose recommendations were neither earnestly solicited nor readily endorsed. The combat commanders were so far removed from the locus of budgetary decision as to be disenfranchised. Their proposals for correcting C^3I deficiencies competed with every other defense program for attention and resources, and they generally fared poorly by comparison.

Two noteworthy but feeble efforts to promote integration and centralization of C^3I networks were made in the early 1960s. The first effort led to the creation of the Defense Communications Agency (DCA). Formed in 1960 to institute a common worldwide military communications system, DCA assumed responsibility for a newly designated network called the Defense Communications System (DCS). This network was intended to provide long haul, point-to-point communications: (1) from the national command level to the unified/specified commanders; (2) from the unified/specified commanders to their respective component (as well as other subordinate) commanders; and (3) between/among the various unified/specified commanders. Many of these same DCS channels were included in the National Military Command System (NMCS), to which DCA provided technical support. DCA's responsibilities extended to other critical NMCS elements besides communications channels: the primary and alternate national military command centers; national emergency command post aircraft; and telecommunications and computer processing equipment at various joint "war rooms" in the Pentagon.

DCA's grant of authority, particularly budget authority, was wholly incommensurate to its sweeping mandate. Powerless, this key defense agency quickly became a client of the military departments and, to a lesser extent, the combat commanders.

The fatal weakness in the agency's charter was its stipulation that the Secretaries of the military departments would have statutory control over the Defense Communications System. The departments funded the procurement of equipment. They funded and constructed the facilities. They supplied the manpower for engineering and installing equipment. The departments maintained and operated all of the resources "on loan" to the Defense Communications Agency. [6]

DCA was further weakened by its relationship with the Joint Chief's of Staff (JCS). The agency reported directly to the JCS; as a consequence, communications requirements forwarded by the unified/specified commanders for JCS validation dominated the agency's agenda. Also, agency involvement in the development of "tactical" communications and "tactical" intelligence systems was forbidden. DCA could not, therefore, facilitate progress toward centralization and integration of key tactical systems, including some that provided early warning data and some that linked nuclear weapons commanders to higher authority.

In sum, bureaucratic conditions compromised the independence of the agency, virtually guaranteeing that DCA would perpetuate, not solve, the command problems that motivated its creation. The situation was impossible because the military departments owed allegiance to their affiliated forces within the combat commands; the military departments controlled DCA's purse strings; the combat commanders set communications requirements; DCA reported to the JCS; and "tactical" communications/intelligence systems were excluded from DCA oversight.

The other noteworthy but feeble effort to promote centralization of C^3I networks consisted of a formal DOD Directive issued in 1963. Instead of empowering DCA, or expanding its own role and competence in the supervision of C^3I programs, OSD issued a directive stressing the importance of meeting national as well as subordinate C^3I requirements. DOD Directive 5100.30 amounted to little more than advice and exhortation. It emphasized that tactical networks, for example, ought to be made responsive to the needs of national decisionmakers. But it stopped short of compelling compliance. The authority of the military departments and combat commanders was not eroded. And since OSD offered them no incentive to alter their priorities, the logic and pattern of investment in command structure development were not affected. The parochial interests of the individual departments and combat commanders continued to take precedence over national interests.

This subordination of programs in the national interest is illustrated by a latent bureaucratic skirmish that never quite developed because of DCA's statutory impotence.[7] By about 1967, it was becoming increasingly apparent that DCA's AUTOVON network was potentially a more survivable means of telephone communications with Strategic Air Command (SAC) forces than the main system providing this service at the time. SAC operated its own dedicated land line system, called the Primary Alerting System (PAS), which ran underground by cable from the east coast to California (via SAC Headquarters and North American Air Defense Headquarters). A complementary cable running underground from Massachusetts to Florida was also being laid.[8] PAS was meant to provide a hardened telephone link among major SAC command facilities and forces. By comparison and contrast, AUTOVON interconnected virtually all U.S. military bases as well as the national command center by means of commercial microwave and land lines. Furthermore, AUTOVON consisted of multiple independent channels and switch points for rerouting transmissions over surviving circuits, and was therefore potentially a robust network. With some effort -- for example, modest design modifications and improved automation of the circuit-switching process -- the latent redundancy inherent in the network's configuration probably could have been developed to a point where AUTOVON compared very favorably to PAS in terms of survivability. PAS, however, was a SAC-dedicated channel and SAC was the sole proprietor. DCA, which key SAC personnel viewed with considerable disdain,[9] was not a welcome partner in any prospective joint venture to improve strategic communications. SAC evaded the issue and all the bureaucratic entanglements that a partnership with DCA may have entailed simply by enjoining DCA from any involvement in the development of voice communications for SAC combat operations. DCA was in no position to contest such matters, and so the idea of developing AUTOVON for SAC force operations was dropped. SAC continued to rely completely on PAS for strategic voice communications, in spite of diminishing confidence in its survivability. [10]

The management chaos that plagued C^3I programs during the decade of the sixties was responsible in no small measure for numerous worrisome conditions and operational misfortunes. For instance, by the end of the 1960s:

- There were 33 DOD telecommunications centers on the island of Oahu alone. [11] CINCPAC and the Army, Navy and Air Force Pacific Commanders each maintained a separate telecommunications center within a few miles of each other in the Honolulu area. [12] Worldwide, there existed at least 55 sites at which two or more military branches maintained independent telecommunications centers. [13] Within the Pentagon itself, the Army and Air Force each operated three centers, and the Navy operated two. [14] Due to technical incompatibility, as a rule neither the telecommunications nor the automatic data processing systems in operations around the world could bridge traditional service boundaries.

- There had been numerous recorded instances of communications breakdown during crises. Communications malfunction has been singled out as the primary cause of the mishandling of several international incidents including the attack on the USS Liberty (1967), the seizure of the USS Pueblo (1968), and the shootdown of a U.S. E-121 aircraft (1969) by North Korea. Autopsies of these incidents pointed up how difficult it was for messages originated at the national level to find their way into the main arteries of military communications networks. Many messages were misrouted, misinterpreted, and even misplaced. Most of them arrived too late, or never reached their intended destinations. Similar problems beset attempts at communications from the bottom to the top of the command hierarchy. [15]

- There were very serious deficiencies in the Minimum Essential Emergency Communications Network (MEECN), described as "a last-ditch communications network which the President would use to pass emergency action orders to the military forces during and after a nuclear attack." [16] MEECN was a nominal system that was not well integrated, and many elements assigned to it were becoming less rather than more compatible as the services continued to develop and deploy elements without regard for their mutual compatibility. DDR&E, the office with primary responsibility for resolving problems of design incompatibility, was unable to do so. Particularly, service problems arose because very long frequency (VLF) radio equipment, the key component of MEECN, was under separate development by the Navy and Air Force, and could not be coordinated. [17]

The impulse to reform management practices once again surfaced in the early 1970s. Concern, particularly on the part of then Deputy Secretary of Defense David Packard, about the lack of institutional focus led first to the creation in 1970 of the Office of Assistant to the Secretary of Defense for Telecommunications. The office was elevated in January 1972 to the level of Assistant Secretary of Defense, in a move to further unify OSD activities in this field. A WWMCCS Council was formed with a view to lending prestige and authority to the Assistant Secretary,[18] and accelerating work on important strategic projects, such as new national command post aircraft and strategic satellite communications. Packard also directed DCA to coordinate MEECN engineering and integration work, hoping this would steer the divergent research and development programs in the Navy and Air Force onto parallel technological paths.[19] Finally, Packard attempted to rectify a decade of misplaced emphasis within the combat commands and military departments by designating the national military command system as the priority component of WWMCCS.[20] In Packard's words:

> ...instead of the local commanders now having as their first priority to design their command system to meet the requirements of their mission, they first have to have a design to meet the requirements of the national command system and second, to meet the requirements of their mission.[21]

DOD Directive 5100.30, reissued in 1971, not only elevated the priority of the national command system, but also downgraded the importance of the unified/specified commanders in the chain of command for execution of the strategic war plan.[22] The JCS was assigned responsibility for ensuring compliance with the provisions of this mandate.

The fatal weakness in this effort to bring about corporate management of C^3I programs was that budget authority was still not adequately provided for. In fact, as the disconnect between the national command system and the military command networks landed on the defense agenda, and as more centralized, coherent arrangements for supervising C^3I projects began to coalesce, real program and budget control in the defense department was being further decentralized. Packard himself was partially responsible for loosening OSD's reins on specific programs and budgets, and for creating a modus operandi (called participatory management) that inhibited initiative at the OSD level. As a result of management practices instituted during Laird's tenure, OSD mainly exercised negative control over specific programs. It did set overall defense budget ceilings; "fenced" some program categories — for instance, certain surveillance programs; reviewed programs requested by the services; and reserved the right to cancel programs or veto Program Objective Memorandums (POMs) submitted annually by the services. But it played a passive or reactive role in the setting of internal budget priorities, and seldom created or pushed ideas of its own.

OSD authority was especially weak in an area — namely, telecommunications — where OSD activism was especially disliked by the uniformed services. A congressional subcommittee report published in

1975 describes the circumstances in which OSD's Telecommunications Office (Schlesinger downgraded the Assistant Secretary position to the level of Director of Telecommunications and Command Control Systems, or DTACCS, in 1974) found itself:

> [The subcommittee views] the responsibility of the Telecommunications Office as the management of all telecommunication resources of the Department so as to provide the maximum communications capability at minimum costs from the viewpoint of the overall mission of the Department of Defense, while insuring adequate support for each of the military departments in carrying out their individual defense missions. In attempting to carry out that responsibility, however, the Telecommunications Office almost inevitably comes into conflict with the military services which either own or lease all of the Department's communication resources. Each of the services has established an independent communications system designed to satisfy its peculiar requirements in carrying out its defense mission. Because of that identity of their communications systems with defense missions, the services tend to regard any action of the Telecommunications Office which would result in reduction or alteration of those systems as an interference with their responsiveness to their mission responsibilities. Accordingly, the proposals of the Telecommunications Office ... have been strenuously resisted by the armed services ... [and] the Telecommunications Office has not had sufficient authority to overcome such resistance....[23]

Richard H. Schriver, who was head of DTACCS in 1976, candidly acknowledged his lack of direct budget authority, though he gives the impression that his veto power conferred substantial indirect control:

> The fiscal control is not direct. I think it is important to understand that the way we function is primarily through a veto power in order to have the services fund projects that may not be totally in

> the service interests but are in the JCS and OSD interests.[24]

Schriver suggested that, for instance, this leverage enabled OSD to persuade the Air Force to spend an additional $63 million on the DSCS satellite program (a DCA managed program that supports the national command system) in FY 1977.[25] However, this was the only FY 1977 telecommunications item, in a consolidated budget of approximately $4 billion, that had not been originally requested by the services.[26] OSD initiated few proposals and infrequently exercised, or threatened to exercise, its right of veto. This form of leverage was applied in a few exceptional cases, such as the E-4 national command aircraft. It was seldom brought to bear when smaller, though often important, items were at stake. For instance, over the period 1976-78, the head of WWMCCS engineering at DCA recommended acquisition of ten different types of C^3 equipment for the purpose of improving U.S. capabilities for "rapid reaction command control."[27] They were intended to provide national officials with better means of managing tactical engagements involving conventional forces, particularly forces deployed to areas where they normally do not operate.[28] The items, such as transportable satellite earth terminals, were relatively inexpensive. But the services declined requests to fund them, and senior OSD officials did not apply pressure in support of the WWMCCS engineer's proposals.[29]

The participatory management arrangement instituted by Laird and institutionalized by his successors was not the only reason for OSD's deferential, passive role. In the area of strategic command development, OSD did not wish to undertake any ambitious new programs. Few if any OSD officials took issue with the official position that "the ability to execute the nuclear force in the large general war case was adequately provided for by programmed systems",[30] a conclusion that fostered complacency at the OSD level and averted a clash between OSD and the services over budget priorities. A different conclusion would have generated demands on the services to divert resources from weapons programs which they powerfully supported to C^3I programs which they generally eyed with disfavor.

Furthermore, OSD officials apparently believed that the protection of individual weapons deserved a higher priority than the protection of the C^3I systems that stand behind the forces. Thomas Reed, for example, who as DTACCS during the mid 1970s was responsible for basic OSD policy in the area to which his title refers, defended a proposal to construct a "soft" (vulnerable) system for communicating with submarines on the grounds that not only would it increase the stealth of subs (by eliminating the need for subs to trail antennas near the ocean's surface), but also that its vulnerability would not matter since missile <u>submarine</u> vulnerability is what really counts in the final analysis. When asked whether he favored a transmission grid that could survive a direct nuclear attack, Reed replied:

> ...it is not clear to me we ought to try to build a surface survivable anything in this era ... because

> the submarines are what really provide the stability in case of some worldwide difficulties.[31]

The statement adduced is consonant with traditional perspective on strategic stability. The overriding importance of force structure protection was also invoked by the Navy in justifying a "soft" communications system (known as Seafarer).[32] The rationale seemed to run as follows: since Seafarer enhances the survivability of U.S. missile submarines, it increases the number of nuclear weapons available for use in a second strike and hence strengthens deterrence; and, since bolstering deterrence lessens the risk of Soviet preemptive attack, there is that much less cause for concern about the vulnerability of Seafarer itself. However dubious this line of reasoning may seem, it was nothing more or less than an articulation of conventional wisdom, a wisdom that conveniently works to contain expenditures on C^3I. The services would be the last to challenge conventional wisdom; C^3I and weapons spigots draw from the same economic reservoir, and the services value weapons above all else.

Formal DOD planning guidance perpetuated the imbalance in command and force structure development. Even the WWMCCS Council, the high level oversight group which presided over all military C^3 programs, could not sanction C^3 improvements that might detract from weapons survivability or flexibility. In this vein, the former Acting Secretary of the WWMCCS Council outlined the following rule of thumb which his group observed:

> ...let me emphasize that the basic policy of the WWMCCS Council, as expressed in DOD planning guidance, is that command, control, and communications, or C^3, should not constrain the flexibility or survivability of the weapons systems themselves.[33]

The issues of command vulnerability and C^3I program management resurfaced after President Carter took office. The administration rejected the previous administration's contention that execution of U.S. nuclear forces in the wake of a massive Soviet first strike was "adequately provided for" by programmed systems. There were reasons to believe that that was not so under any responsible definition of adequacy, and there were no illusions that programmed systems would provide for a command structure of the sort needed to support a strategy of flexible response.

The policy turnabout resulted in part from a series of studies that exposed many serious C^3I vulnerabilities and operational deficiencies, and in part from the Carter administration's move to raise standards of command performance. With the pendulum of concern swinging away from assured destruction and toward flexible response, the administration saw need for greater endurance, survivability, flexibility and centralization in C^3I networks. PDs-53, -58 and -59 reflected this shift in emphasis. Key combat CINCS, notably the SAC Commander, General Ellis, shared this assessment and strongly backed the administration's effort to repair and modernize the command system.

The institutional means of translating such desires into tangible accomplishment, however, remained inadequate throughout the Carter term. Attempts at overhauling C^3I management and acquisition practices did not succeed in wresting resource control from the military departments, leaving OSD and the combat CINCS without sufficient leverage on C^3I budgets and programs.

The most noteworthy and the earliest (1977) of these attempts began with the commissioning of a Defense Science Board Task Force to reevaluate the process by which OSD and the military departments design and procure command systems. Completed in the summer of 1978, the Task Force report confirmed what everyone already knew: "The nation is failing to deploy command and control systems commensurate with the nature of likely future warfare, with modern weapons systems, or with our available technological and industrial base." [34] Fundamental improvements were needed to allow U.S. forces to respond appropriately under the careful control of national authorities, at all levels of conflict, and to avoid unnecessary escalation, the Task Force concluded. [35]

To remedy the situation, the Task Force made a provocative recommendation that ultimately failed to win acceptance due to powerful opposition from the military departments. It called for the creation of a new agency with statutory authority "to manage the design and acquisition of command and control systems ... which cut across Service boundaries or are of major concern to OSD, JCS or the National Command Authority." [36] Beyond the transfer of statutory authority to this agency, the Task Force recommended that the combat CINCs be provided with sufficient funds and manpower to modernize their command systems, within the guidelines established by the new agency, to meet the needs of their respective commands.[37] Moreover, the combat CINCs' capabilities for evaluating their command systems should be strengthened, the report said.

These recommendations were watered down as they passed through successive stages of bureaucratic review. Instead of creating a new agency, the Defense Communications Agency would be expanded and assigned the new responsibilities. Then it was determined that DCA's statutory authority should extend only to interservice systems, strictly defined, which excluded key elements of the strategic network — for instance, E-4 airborne command posts, TACAMO submarine communications relay aircraft, and strategic early warning networks such as PAVE/PAWS and BMEWS radar systems. Ultimately, no statutory control at all passed to DCA. The JCS and the services unanimously and effectively opposed it on the grounds that "Service prioritization of command and control systems among other programs in PPBS would be lost if statutory control of them was given to an agency."[38] In other words, the proposed restructuring not only directly threatened service control over C^3I expenditures, but also indirectly threatened their control over the allocation of resources to other programs including weapons systems. From the services' standpoint, this was clearly an intolerable proposition. The Task Force, on the other hand, had found no other solution.

During the transition period following the inauguration of President Reagan, several senior officials who had been deeply involved in command system development reflected on the circumstances in which they found themselves. The usual complaints were voiced. H.L. Van Trees, Acting ASDC^3I, noted the perennial OSD struggles: identifying the things that need to be done; getting the services to put the needed C^3 programs in their budgets; and making sure that funds for C^3 programs are not moved to support some other program.[39] He advocated the establishment of stronger resource management control within OSD. General Ellis, who would soon retire from his post as CINCSAC, also recommended further centralization of budget authority. He would place a C^3I advocate at the Deputy Secretary level (a notch higher than usual) to ensure OSD budget control.[40] Ellis also lamented the fact that although a high level JCS office had finally been created for the purpose of facilitating CINC input to C^3I policy channels, the JCS office in question lacked the budget and program authority needed to implement CINC recommendations. Lt. General H. Dickinson, the then Director of this JCS office (C^3 Systems), summed up the situation as follows: "In general, the development, and programming and procurement process throughout the Government is not designed to handle C^3-system problems."[41]

The situation has not improved under the Reagan administration. The previous administration's office of ASDC^3I, which lacked sufficient countervailing leverage vis-á-vis the services, according to the present Undersecretary for Research,[42] was replaced by an office of even lower rank (Deputy Undersecretary for C^3I). The $ASDC^3I$ position was only recently reinstated. At the same time, the Pentagon's latest PPBS revision featuring "controlled decentralization" further consolidates the military services' tight control of the C^3I budget. In short, nothing has really changed. Control of programs and budgets continues to be unfocused and heavily decentralized. Investments continue to be driven by diffuse service interests. OSD still functions within the participatory management framework built by Laird, and therefore lacks the power to bring C^3I programs under strong central direction. And the prospects of sorely needed reforms of the sort recommended by the Task Force are as remote as ever. Absent such reform, Reagan's promise to create a command system that allows for central, flexible direction of strategic forces during a protracted conflict will surely remain unfulfilled.

This is not to say that resource control is the key to bringing the command system into alignment with current nuclear strategy, which assumes a highly centralized, rational decision process with national leaders providing coherent direction to strategic forces over a long period of time. As discussed next, the direction of strategic forces is not, and cannot be, nearly as central, rational or precise as we generally think.

MANAGEMENT OF FORCE OPERATIONS: ILLUSION OF CENTRAL CONTROL

The image of a unitary actor steering the ship of government is also incongruous with the way strategic forces are operated. Although the past 25 years have witnessed a gradual increase in centralization, force operations, like C^3I programs and budgets, are still managed without very much direction from central authorities. In both cases, activities are better understood as products of a diffuse, decentralized decision process.

The extent to which low-order decision rules and standard operating procedures (SOPs) regulate the peacetime activities of the strategic forces is quite apparent. At this moment the alert bomber crews, submarine commanders, land missile launch crews, and all warning and C^3 units that support these force components are enacting standard routines which account for practically all of their behavior. Routines determine the location, disposition, readiness and behavior of the units assigned to the strategic mission. Routines focus the attention of active units so as to simplify the complexity of their environment; channel energy so as to simplify their operations on the environment; provide them with built-in solutions to the ordinary problems they encounter; and coordinate a diversified, far-flung force structure with a minimum amount of interaction between units required. Programmatic activity stabilizes a large scale and potentially dangerous operation, and does so without constant or even frequent direct supervision by high level policy officials (civilian and military authorities).

The programmatic decision process which accounts for such stability operates on simple principles.[43] It requires, first of all, a focused receptor to pick up an environmental input and deliver it to an information channel. Next, the input is compared with a desirable range of values for that variable, and if it falls outside this interval, minor adjustments (a programmed response) are made until the input, whose value and value changes are routinely monitored, falls within tolerances. When these adjustments succeed, the system can be said to have adapted to environmental disturbances. Gain adjustments to radio receivers used by strategic units to monitor communications from external sources illustrate a simple version of this adaptive process. Such adjustments are made when environmental forces -- especially changing atmospheric conditions — perceptibly reduce the strength of radio signals.

If gain adjustments fail to restore adequate reception -- in abstract terms, if the monitored input remains outside of a defined interval after a simple programmed response is made -- then other different programmed responses will be triggered sequentially until reception is restored or the repertory of responses exhausted. Examples are frequency switching, reorientation of antennas, and activation of back-up receivers. Such a repertory of behavior patterns, each of which operates in a characteristic way upon receipt of perceptual inputs, increases the adaptive capacity of the system. As long as the environment is fairly stable — in other words, the pertinent variables and their values do not undergo radical change --

an entity consisting of nothing more than a set of built-in decision rules, which apply to only a small domain of environmental conditions and which are capable of invoking only a limited range of responses, can possess high adaptive capacity. Such capacity can exist even in a rich environment, where the pertinent variables and combinations of variables are numerous. The capacity for ultrastability in a rich environment is gradually acquired through evolutionary changes in rule structure. As a rich but stable environment reveals its variety, and as established action sequences prove to be inappropriate enough that system instability results, unsuccessful decision rules and programmed responses are slightly modified or they are dropped from the organization's repertory. This learning process based on trial and error appears to have a better chance of restoring system equilibrium through elimination of inappropriate rules/responses, or through slight modification of existing routines, than it does through attempts at elaboration or overhaul of organizational structure. Such attempts, which may be based on rational analyses, are seldom made in any case.

Programmed activity is so much a part of peacetime strategic operations that the behavior of the forces requires no further explanation. One need not introduce central decisionmakers' (or anyone else's) goals or rational calculations, for example, to explain the activity. In fact, general policy goals may be rationalizations of the extant repertory of organizational behavior patterns rather than the other way around. Goals are tied more closely to past activities than has been realized, and frequently are better understood as summaries of previous actions. Much of the organization's work does not seem to be directed toward goal attainment, nor influenced by rational analysis. Instead, it can be understood more readily as actions with a primitive orderliness, this orderliness being enhanced retrospectively when individuals review what has come to pass as a result of the actions.

This view -- that organization is an agent of simplification, not maximization, and that it seeks stability, not goals -- is strengthened if one recognizes that the organization's operating routines, and the particular environmental conditions that evoke them, are not generally known, let alone devised, at high levels. This view is further strengthened if one recognizes that national purpose or strategy has not greatly influenced the development of the information channels that provide the highly specific information which triggers operating routines. A decentralized bureaucracy dominated by service interests has created, or better, let evolve, a collection of information channels individually tailored to the limited sets of procedures performed by relatively low level actors. As discussed above (institutional laissez-faire), the development of a national military command system geared to central control was retarded as a consequence.

This is not to say that there is no connection whatever between rationality and operating routines. Connections may exist in many instances and, moreover, at times operational policy is considered and set at a high level. Nevertheless, for those cases where policy is addressed in a serious way at high levels, the steering wheel is still but loosely connected to the rudder. Policy statements of high officials usually contain a modicum of operational guidance, leaving a myriad of details to be worked out by people and suborganizations not under the watchful supervision of key policymakers. Some suborganization interprets the policy, generates the criteria for choice, performs the analysis and adjusts operational procedures. Furthermore, although policymakers may have influenced the original pattern of operations, the pattern has probably since been transformed, through a process of pragmatic experimentalism, without the benefit of further review or guidance. In time, the original rational bases of many operating procedures are lost sight of and new rationalizations are invented to explain them.

An observer of strategic organizations has proposed that negative control is the prevailing "goal" of the command system during peacetime.[44] Under normal circumstances, strategic forces are exercised in such a way as to minimize the risk of accidental or unauthorized launch of nuclear weapons. Early warning networks, similarly, tend to err on the safe side of miscalculation. In sum, negative control, embodied in a myriad of rules, SOPs and other routine command practices, normally drives the behavior of strategic organizations. In peacetime it takes precedence over other objectives.

Those other objectives can be grouped under the general heading of positive control, defined as the authorization and effective coordination of attack preparations and/or actual strikes. The tense circumstances in which positive control would become a high if not predominant priority are especially apt to evoke the image of a central authority taking personal charge of the diplomatic and military components of American policy. The decision process that governs crisis or wartime behavior, however, is essentially no different from the process that governs peacetime operations. It is still a diffuse, programmatic process.

It has to be. A central authority simply cannot be aware of all that is relevant. Even if the information channels could provide the authority with all the data needed to make rational decisions, no individual or small group could assimilate it. (We must restress the fact that such channels have not been adequately developed in any case.)

Conditional rules -- do A if event 1 occurs, B if event 2 occurs, and so forth -- exist to prevent the overload of the information and decisionmaking capacity of national authorities and, as well, subordinate commanders. Rules devoted to positive control are pervasive. They incorporate the possibility of using information -- "2 occurred" -- and significant flexibility has been achieved by combining them with information channels to take account of varying circumstances.

Positive control, like negative control, can thus be viewed as an epiphenomenal outcome. Neither is simply a matter of organizational compliance with orders issued by an authority, but rather a coincidence of programmed behavior and policy objectives. Control is achieved when diffuse organizational reactions accomplish something that coincides with a salient national purpose.

This view implies that positive control probably depends less for its success on C^3I networks that give central authorities access to large amounts of information and allow them to issue detailed operating instructions to the forces, than it does on careful attention in peacetime to the self-organizing properties of large organizations: the conditional rules and the information channels needed to implement the rules. Subjecting the programmed repertory of organizations and the supporting information channels to intensive scrutiny and periodic modification is an attempt at preordination which complements and simplifies efforts by authorities to direct force operations during crises or war.

The formulation of conditional rules to achieve positive control has many drawbacks as well as advantages, beginning with the fact that serious attempts at preordination require unusual exertion on the part of national policy officials. This entails civilian participation in activities traditionally dominated by military planners, many of whom look askance at the involvement, regarding it as intrusion by civilian interlopers.

Legend has it that when General C. LeMay was CINCSAC, he alone knew the exact manner in which the nuclear forces under his command would fight.[45] The role of the national authority in positive control was basically confined to providing political authorization to unleash the forces. An authorization message would have been sent without detailed knowledge of either SAC's contingency plans or the strategy SAC would actually implement upon receipt. Furthermore, SAC did not integrate its contingency plans with the plans of the other services until the early 1960s. As late as 1960, when then Secretary of Defense Gates established (despite strong protests from one of the service chiefs) a Joint Strategic Target Planning Staff under the direction of the CINCSAC, there was no formal mechanism for coordinating long-range nuclear strike plans developed by SAC and the Navy,[46] much less a mechanism for immersing civilian interlopers in the planning process.

Today, civilian access to the military's contingency plans is much freer. On occasion, national policy officials even participate in the formulation of preprogrammed options. Without exception, however, the detailed planning is delegated. And delegated again. Timing, targeting, execution procedures (including procedures for authenticating messages) and so forth are revised by subordinates in suborganizations to create rule structure far more complex than the printed menu of options would suggest. As a result, authorities, and particularly national authorities, cannot fully comprehend many aspects of the policies they inspire: the extent to which rule structure limits the kinds of responses that authorities may call forth; the exact character of a programmed response; the complexity of the organizational reactions triggered and what can go wrong during implementation; and so forth. Authorities may not realize, for example, that even without damage to the command network, current organizational arrangements do not permit them significant personal control over the implementation of any given option. National authorities could trigger the implementation process, but they could not, for example, impose some important conditions on the firing of weapons assigned to the chosen option. Suppose that authorities wanted to impose the condition that no weapons will be fired until most of the commanders sent orders to fire have acknowledged receipt of the order. Or that no weapons will be fired until <u>all</u> commanders sent orders to fire have copied the correct targeting instructions and aimed their weapons accordingly. Or that commanders who find themselves unable immediately to launch some of their weapons (those not deliberately withheld) will withhold those weapons until further notice. These conditions could <u>not</u> be imposed. No provisions exist to do so. And an attempt by central decisionmakers to impose them in an <u>ad hoc</u> way would only invite confusion.

These are <u>minor</u> conditions that pertain to the implementation of a <u>prepackaged</u> attack option. It is easy to imagine the consequences of any abrupt attempt to assert positive control in a way that requires <u>major</u> changes in organizational structure. An attempt at improvisation would massively disrupt established routine and thereby create disorder and confusion. Improvisation courts organizational paralysis. As former CINCSAC General Power once put it, "You cannot coordinate a plan after you have been told to go to war. It all has to be part of a well-thought-out, well-worked-out plan. And there is one basic law you must follow: Do not change it at the last minute." [47]

The rigidity of a given rule or option, which may be too complex to understand yet not complex enough to incorporate adequate controls on implementation, does not mean that rule structure cannot take account of varying circumstances. A collection of rigid rules/options can, in principle, be responsive to a large variety of possible events. A "well-thought-out" plan anticipates the range of likely events, and contains rules to take account of them. Furthermore, if unexpected events occur, organizational learning and adaptation are theoretical possibilities in some circumstances.

The situation contrasts sharply with the situation in peacetime, however, even though the programmatic nature of the process by means of which the strategic forces are controlled is the same in all settings. While the strategic forces operate according to built-in decision rules in periods of international calm, high alert, and wartime, we can confidently judge the appropriateness of these rules/responses for a peacetime environment only. The consequences of routines enacted in peacetime are at least susceptible to direct observation, and perceptibly adverse consequences caused by inappropriate routines often induce, albeit over an extended period of time, appropriate changes in organizational structure. By contrast, the consequences of routines enacted under crisis or wartime circumstances can only be hypothesized; neither the environmental conditions nor the organizational responses to these conditions can be directly observed.

These are environments in which we have had little or no experience. Consequently, organizational structure has not "profited" from any evolutionary learning process of the kind discussed above. Let me appeal to this fact for partial justification of the presumption that the established repertory of preprogrammed responses is likely to be inappropriate. Additional justification of this presumption is that in the absence of experience and a strong empirical foundation, no rational analysis can predict events well enough to achieve full flexibility in the formation of rules. Finally, in a major crisis or war the environment changes so fast and time is so compressed that there would be less chance for an evolutionary learning process to run its course, even without damage to the command network. Organizational structure is likely to be so inappropriate that substantial rule modification would be warranted, yet environmental change over time is likely to be so dramatic that adaptation through feedback and evolutionary learning would have little chance of success. The resulting disruption would be even greater in the event nuclear attack damages the C^3I network, and the chances of recovery diminished still further.

Even if the established repertory of strategic organizations proved to be appropriate, C^3I vulnerabilities could render the fact academic. By its very nature, information is needed to implement conditional rules. Degradation of information channels could in effect eliminate the most appropriate rule or rules from the repertory. The greater the degradation of information channels, the greater the degradation of control. (Positive <u>and</u> negative, though the latter's priority would be relatively low in the event of actual Soviet attack.)

Massive degradation of control is, alas, almost inevitable given current C^3I deficiencies. This appears to be the case regardless of Soviet attack strategy. For instance, a Soviet counterforce attack designed to maximize damage to the U.S. force structure would cause sufficient collateral damage to the command network to make war uncontrollable, regardless of what calculations U.S. political leaders might make at the time and irrespective of the existence of retaliatory options created for this very contingency. Such an attack would trigger diffuse organizational reactions which, in conjunction with damage to C^3I networks, almost guarantee a quick departure from any rationally preferred course of action (see Chapter 7).[48]

Insights into the performance of strategic organizations under various conditions can be gleaned from simulation and exercise data. And these insights often suggest appropriate changes in both rule structure and physical C^3I arrangements. However, war games and exercises are relevant to only a narrowly defined set of plausible situations, and even then they only partially illuminate the diffuse activities of the forces, the possible consequences of triggering them, and the physical and procedural modifications needed to improve performance. The learning process is artificial, in that modifications stem from dissatisfaction with the performance of units thrust into a world of make-believe. The appropriateness of existing structure, and of modifications to it, is no less hard to judge than the representativeness of the fictional environment in which performance evaluation is conducted.

It is nonetheless of great interest that strategic units often give poor performances even in fictitious situations.[49] Although the circumstances contrived for exercise purposes may only faintly resemble those encountered in the event of actual mobilization or war, at least they feature greater variety and more rapid change than are characteristic in peacetime. For this reason, organizational performance under simulated test conditions is informative. The inappropriateness of extant repertory and the inability of organizations to adapt well to a variegated, fast-changing environment that is artificial surely say something about how well organizations can be expected to perform in a variegated, fast-changing environment that is real.

Exercises and tests are constant reminders of the fact that the consequences of triggering the organizational routines devoted to positive control cannot be foreseen with high confidence. Whenever large, complex organizations are involved, there is always a significant risk that declaratory policy at the national level and action policy at the military level will diverge. At the conclusion of actions, national officials' aims as originally defined may not have been even approximately accomplished.

The historical record of efforts to bring American policy under central direction during nuclear crises lends support to this general argument. In the Cuban missile crisis of 1962, for instance, the U.S. Navy's aggressive pursuit of its ASW mission in the North Atlantic, though consistent with the general political construction that national officials set on the course of events, diverged from the formulated intention of policy officials. This bold campaign, undertaken as a normal operational measure in support of the blockade, reduced if not removed the nuclear threat posed by Soviet cruise missile submarines. Its success greatly bolstered U.S. defenses against nuclear attack, and may have been a decisive factor in the event of nuclear war with the Soviet Union. But neutralizing this particular component of Soviet nuclear capability was never an explicit aim of national policy officials. To be sure, the Navy's actions seem to have followed the general political signals of U.S. national policymakers whose actions and pronouncements painted the gloomiest of prospects. Nuclear war with the Soviet Union was hanging over the entire incident. The danger was real, and aggressive preparations for war seemed warranted and consistent with the tenor of the confrontation. Nevertheless, the Navy's ASW campaign not only escaped the attention of the president and his advisors until well into the crisis but also:

> ... constituted extremely strong strategic coercion and violated the spirit of the Executive Committee policy. It is not unreasonable to suppose that American ASW activity in the North Atlantic was in fact the strongest message perceived in Moscow in the course of the crisis, and if that is true, then the efforts to bring American policy under central direction must be said to have failed.[50]

National authorities are increasingly moved to try to bring military operations under their direct supervision. Since the Cuban Missile Crisis, when political leaders attempted to give specific instructions directly to local commanders of destroyers stationed along the quarantine line, direct civilian supervision from Washington of crisis military operations in various parts of the world have been attempted on numerous occasions. Such attempts have met with unusual success, especially since the advent of the communications satellite. The evacuation of Lebanon and Saigon, the "tree-cutting" operation along the Korean DMZ, the Mayaguez rescue, and the abortive mission to rescue American hostages held in Tehran can be cited as examples. While it cannot be said that remote control over these special operations approached perfection (witness the delay in termination of bombing raids on Cambodia during Mayaguez; U.S. military forces conducted those raids more than 30 minutes after the president ordered their cessation following the release of the Mayaguez crew),[51] national officials managed to exercise considerable control, thanks to the ever-expanding capacity, speed and reach of satellite communications.

These episodes, however, are special cases. It would be a sweeping generalization to say that strategic operations of the sort associated with U.S.-Soviet nuclear confrontation could be brought under the same degree of central direction. Mayaguez-type operations and strategic nuclear operations are vastly different in terms of scale, diversity of weapons systems, geographical dispersion, objectives, risks and stakes involved. They are thus vastly different in terms of tractability.

The cases may not be dissimilar in at least one important respect: central direction runs contrary to strong military traditions. Direct civilian supervision conflicts with what could be called institutional ethos, and this tension was in evidence during the Cuban crisis when political leaders communicated instructions directly to U.S. ship commanders. Allison characterizes this encroachment on the military chain of command and on the autonomy of local commanders as "unique in naval history and, indeed, unparalleled in modern relations between American political leaders and military organizations." [52] The establishment of a direct command channel between the White House and local commanders, made possible by advances in the technology of communications, created "enormous pain and serious friction," according to Allison. [53] Similarly, a stormy exchange took place when Secretary McNamara demanded of Admiral Anderson — then Chief of Naval Operations — precise information on the Navy's procedures for intercepting Soviet ships which might attempt to pass through the blockade. According to Allison's account, Anderson did not comply. [54] He refused to provide information requested by his civilian superior.

There is a wealth of anecdotal evidence to suggest that something like institutional ethos exists as a source of tension and that it may affect the way in which national policy and military operations actually interact. A story in a trade journal offers one such illustration. The story relates the tale about former Defense Secretary Rumsfeld's monitoring, from the national military command center, the 1976 evacuation of Americans from Lebanon, and how "some military officers" wince at the part of the tale where Rumsfeld maintains direct, instant voice contact with the boatswain's mate in charge of the land craft which transported evacuees to a waiting Navy ship. [55] Another story related to the author by a former, senior official in OSD concerns the Navy's role in the evacuation of Saigon.

It seems that the ranking Navy officers near the scene transported themselves from ships in direct communication with Washington to ships without that capability in order to gain local autonomy in directing the evacuation. This same official summed up the attitude of many Navy officers toward a 1972 OSD Directive (5100.30) removing the shore-based unified commanders from the chain of command for execution of the strategic war plan: "they believe strategic communication runs to and stops at the shore." In other words, national authorities should exercise only a rudimentary form of positive control — initial communication of nuclear authorization to unified commanders — and both the traditional chain of command and the operational autonomy of local ship commanders (in this case, missile submarine commanders) ought to be preserved.

The prevailing ethos is clearly at odds with the idea of central management. It works to restrict direct communication between national officials and on-scene commanders; to inhibit full disclosure of in-progress operations; to promote conformity with preprogrammed operational measures in support of prearranged contingency plans; to discourage national authorities from changing plans "at the last minute"; and to encourage aggressive pursuit of established missions by military commanders.

This assessment carries no pejorative connotations. It is not meant to insinuate that commanders are overzealous or cavalier toward their civilian superiors, and certainly not that anyone intentionally undermines national policy. Nor does the assessment imply that resistance to centralization necessarily detracts from either military effectiveness or the achievement of broader national policy objectives.[56] To the contrary, a strong argument can be made that positive control depends heavily on standard operating practices. Improvisation on the part of central authorities invites massive disruption of established routine, especially in the case of large-scale operations, and may increase rather than reduce the potential for discontinuity between national policy intentions and force behavior.[57]

The main point of this discussion of institutional ethos is simply that it appears to be another significant force that promotes decentralization of crisis operations. The corollary is that it opposes developments that would enlarge the role of civilian authorities in controlling those operations. This is one of the principal reasons why the services and combat commanders do not design their command systems to be optimally responsive to national authorities, but instead design them with a view to meeting the narrower requirements of their own missions. As discussed earlier in this chapter, OSD has not succeeded in its repeated attempts at balancing these priorities. As shall be noted in a later chapter, at least one senior OSD official has concluded that this imbalance in command system development has been extreme, to a point where even the most rudimentary form of positive control — initial communication of presidential authorization to retaliate — might not be possible in the event of Soviet preemptive attack on the U.S. command system.

SUMMARY AND IMPLICATIONS

The secondary applications of rational logic — proportionate retaliation and intra-war strategic bargaining — advanced as an answer to the paradox of the threat of massive retaliation, appear to entail drastic alteration of the existing structure of strategic organizations. The activities of these organizations, which range from C^3I procurement to war planning to force operations, are not regulated either by axioms of deterrence or by means of specific instructions from national policymakers. To the contrary, the behavior patterns of the organizations bear scant relation to national purpose, intention or deterrence strategy. Attempts at developing a command structure that allows for central, flexible direction of strategic force operations will be frustrated — by military traditions that oppose centralization; by a decentralized budget process that assigns relatively low priority to command modernization and an even lower priority to command programs designed to meet national command requirements rather than the narrower requirements of subordinate missions and strategies; and by the fact that U.S. strategic organizations, being highly decentralized and heavily structured by low-order rules, presently operate according to fundamentally different principles of control.

Unusual effort on the part of national policy officials would be required to bring strategic activities into closer alignment with national purposes and strategy, and that effort would be most productively spent not during but before some outbreak of hostilities.

The amount of positive control that central leaders could potentially exercise once hostilities begin depends in large part upon the degree of their involvement in contingency planning and other preprogrammed actions. With time in the missile age measured in minutes and hours, operation plans must be worked out in detail and in advance. It is plain that, for example, to have a choice of striking or not striking certain targets, the target list must at least be divided up into preplanned option packages to which specific forces have already been assigned and readied. Provided such preparations have been made, national authorities could cue the forces to release the entire arsenal in a comprehensive attack, or cue forces to release portions of it as deemed necessary under the circumstances. But in any event, programmed crisis and wartime operating procedures had better be understood and approved by central leaders prior to the eruption of hostilities, as there would be minimal scope for review and ad hoc changes.

The amount of positive control that can be achieved also depends in part on the configuration and performance of information channels associated with the implementation of a strategy or set of operating procedures. Whether national authorities are in or out of a particular programmed decision loop, the destruction of information channels that carry information input to the actors that are in the loop would obviously degrade their ability to perform their procedures. These channels just as obviously need protection from attack.

The services, however, habitually constrain the C^3I budget, at the expense of improved C^3I networks, in favor of weapons investments. National policy officials would have to take extraordinary, unpopular steps to break this habit. Service control over C^3I resource allocation probably would have to be stripped, with statutory control transferred to a "neutral" office or agency.

There is no doubt that such a move would be necessary if we aspire to expand the role of national authorities to include them in more of the decision loops. The greater the responsibility of central leaders to filter information about the environment and issue instructions as to what strategy the forces should follow (the operating procedures followed by central leaders would produce decision cues that trigger the implementation of corresponding rules at subordinate echelons), and the greater the complexity of national strategy, then the greater the need for developed, robust C^3I networks that tie into the national command system. But unusual effort once again would be required to effect such development. Repeated attempts at establishing the national military command system as the priority component of WWMCCS have utterly failed.

Central leaders are not inclined to devote the effort needed to make all these difficult adjustments, and even if made, tight positive control would be far from assured. Significant decentralization of operating procedure and information channels cannot be entirely avoided. Significant vulnerability of decision centers and communications links to nuclear attack cannot be completely eliminated.

Pertinent details of existing structure will inevitably escape observation, even when carefully scrutinized. The exact nature and degree of organizational constraint on executive decisionmaking cannot be fully determined. The consequences of triggering the diffuse organizational reactions associated with mobilization or attack cannot be precisely anticipated or calculated. In sum, there is an irreducible risk of discontinuity between national purpose and force operations.

At the moment, there are reasons to believe that the scope for such divergence is sufficiently large that the paradox of the retaliatory threat has not been operationally answered. The answers, we argue in greater detail later, provided by carefully calibrated retaliation and strategic bargaining are more academic than operational.

Questions can also be raised about the ability of central leaders to manage crisis operations. Would diffuse organizational reactions to information input from political leaders and the external environment produce outcomes that coincide with the intentions of national policy officials? Many have come to believe that even without damage to the command system, positive control of crisis operations could break down and that the more serious threat of war lies in that possibility rather than in the possibility of an outright breakdown of deterrence. Steinbruner, for example, concludes that "the most serious threat of war under current circumstances probably lies in the possibility that organizationally and technically complex military operations might override coherent policy decisions and produce a war that was not intended."[58]

Finally, the primary application of rational logic — deterrence based on the threat of assured destruction — is a matter of some doubt. Positive control in this context simply means that operating procedures geared to prompt nuclear retaliatory attacks on a massive scale would be triggered and successfully performed once assured destruction becomes the salient objective of national security. While we are reminded that it would not be rational to actually carry out a strategy of massive retaliation, the capacity to do so is considered to be the essence of nuclear deterrence.

With so much policy attention focused recently on secondary questions of intra-war nuclear deterrence and bargaining, one might suppose that all problems related to the elementary requirement of assured destruction have been solved. We do indeed have some grounds for believing that positive control arrangements required to implement massive retaliation are adequate. Senior defense officials assure us that the conditions necessary to satisfy this requirement exist. Repeated assurances along this line have been heard since the missile age dawned.

Whether or not the degree of confidence expressed over the years by national officials has actually been warranted depends in part on command performance. Calculators of U.S. second-strike capabilities, however, have usually skirted the question of command performance. Historical assessment of basic U.S. deterrence strategy has been based almost entirely on calculations of the vulnerability of individual weapons deployments. The next several chapters demonstrate that these calculations, and the conclusions drawn from them, appear to be erroneous and misleading.

FOOTNOTES

1. William J. Broad, "Philosophers at the Pentagon," Science, vol. 210 (October 24, 1980), p. 412.

2. DOD Directive 5100.30 (December 2, 1971) defines WWMCCS as the system that "provides the means for operational direction and technical administrative support involved in the function of command and control of U.S. Military Forces." WWMCCS thus encompasses virtually all C^3 assets within the military.

3. See U.S. Congress, House, Committee on Armed Services, Review of Department of Defense Worldwide Communications Phase I, 92nd Congress, 1st Session, Report May 10, 1971 (Washington, D.C.: GPO, 1971), pp. 1-42. (Hereafter Phase I Report, May 10, 1971.)

4. Ibid., p. 20.

5. "While many of the Subcommittee witnesses expressed reservations about the wisdom of consolidation, their objections were not based on any operational degradation of the military communications system. On close analysis, their vague objections appear to be based more on jurisdictional rather than operational grounds. They are reluctant to share their communication facilities with the other services." U.S. Congress, House, Committee on Armed Services, Review of Department of Defense Worldwide Communications Phase III, 93rd Congress, 2nd Session, Report February 7, 1975 (Washington, D.C.: GPO, 1975), p. 8. (Hereafter Phase III Report, February 7, 1975.) See also U.S. Congress, House, Committee on Armed Services, Review of Department

of Defense Worldwide Communications Phase II, 92nd Congress, 2nd Session, Report October 12, 1972 (Washington, D.C.: GPO, 1972). (Hereafter Phase II Report, October 12, 1972.)

6. Phase I Report (May 10, 1971), pp. 18-20; 22-26.

7. This illustration is based on a telephone interview with C.L.B., formerly with AT&T.

8. "Closer Military-Industry Relationship Seen Helping Command and Control," Aerospace Daily, vol. 106 (November 7, 1980), p. 33.

9. C.L.B. interview: "SAC regarded DCA as a glorified AT&T."

10. PAS cables were laid in sections about 50 miles long, and joined together at these intervals by manned maintenance facilities. A single break in the cable or the destruction of a single manned site would have disastrous effect on overall PAS performance. Two or three strategically aimed weapons probably would knock it out completely. When PAS was originally designed, it was projected to be relatively survivable because it was presumed that, given Soviet missile numbers and accuracy, Soviet planners would not be willing to commit the forces needed to destroy PAS. The system was thus designed to sustain only collateral damage. By the mid to late 1960s, however, Soviet missile accuracy and deliverable warheads had increased to a point where direct nuclear attack on PAS could no longer be discounted.

11. Phase II Report (October 12, 1972), p. 16,498.

12. Ibid.

13. Phase III Report (February 7, 1975), p. 6.

14. In addition, the Pentagon housed a communications center for the Defense Intelligence Agency and the National Military Command Center, for a grand total of ten centers within the Pentagon alone. Phase II Report (October 12, 1972), p. 16,498.

15. See Phase I Report (May 10, 1971), pp. 6-17.

16. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 9, p. 1,165.

17. "Internetting to Enhance Survivability of Strategic Command and Control" and "Can Vulnerability Menace Command and Control?" Armed Forces Management, vol. 15 (July 1969), pp. 40-43; Lt. General Lee M. Paschall, "WWMCCS -- Nerve Center of U.S. C^3," Air Force Magazine, vol. 58 (July 1975), p. 55; U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1970, 91st Congress, 1st Session (Washington, D.C.: GPO, 1969), Part 4, pp. 861-62 and Part 3, p. 1,125; U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1972 Authorization for Military Procurement, Research and Development, 92nd Congress, 1st Session (Washington, D.C.: GPO, 1971), Part 4, p. 2,759-61; U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 4, pp. 2,628-29; U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 6, p. 1,705 and Part 9, pp. 1,165-66.

18. Members included the Deputy Secretary of Defense, the JCS Chairman, and two Assistant Secretaries (for Intelligence and for Telecommunications).

19. See references in footnote 17 of this chapter.

20. Department of Defense Directive 5100.30 (December 2, 1971).

21. Congressional Record (October 29, 1971), p. 38,381.

22. Further discussion of this restructuring can be found elsewhere in this manuscript.

23. Phase III Report (February 7, 1975), p. 5.

24. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1977, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 6, p. 33.

25. Ibid.

26. Ibid., pp. 3, 33.

27. DOD Directive 5100.79 (November 21, 1975) established, within DCA, an engineering office to design a command network according to IBM Corporation studies and plans for WWMCCS through 1985. IBM's WWMCCS architecture placed primary emphasis on the need to handle Mayaguez-type contingencies and hence on investment in rapidly deployable C^3 assets.

28. The idea was to be able to operate anywhere in the world in the manner of the "tree-cutting" operation in the Korean demilitarized zone, when the national military command center in Washington, the CINCPAC in Hawaii, and the Commander UN Forces in Korea were able to set up a conference and maintain continuous control of the operation.

U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1977), Part 10, pp. 6,793-96.

29. Interview with Mr. Babbitt, WWMCCS Engineer.

30. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 10, p. 6,795. This "official position" was actually that of the WWMCCS architecture developed by the IBM Corporation, and ultimately the conclusion was rejected by the Carter administration.

31. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 3689, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), Part 4, p. 4,024.

32. Admittedly, program justifications serve rhetorical and political purposes and as such do not necessarily indicate any deep-seated view on strategic stability or anything else. In fact, until 1975 the Navy insisted that a "hard" survivable communications system (then called Sanguine) was essential: "The whole idea behind Sanguine is to produce a means of communicating with our missile-launching nuclear submarines which is so sure and so survivable under any conditions including nuclear attack that any enemy would be most hesitant to attack us knowing our retaliatory capability is assured. In other words, having Sanguine as one of our defense systems will, hopefully, prevent a nuclear attack on the United States." Statement

of Rear Admiral J. L. Boyers, Director of Naval Telecommunications, in U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1975 Authorization for Military Procurement, Research and Development, 93rd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 6, p. 3,207.

33. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1977 Authorization for Military Procurement, Research and Development, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 12, p. 6,802.

34. Defense Science Board Task Force, Command and Control System Management (Washington, D.C.: Office of the Under Secretary of Defense, Research and Engineering, July 1978), p. 1.

35. Ibid., pp. 5-6.

36. Ibid., p. 2.

37. Ibid., p. 2.

38. Gerald P. Dinneen, "C^2 Systems Management," Signal, vol. 34 (September 1979), p. 16.

39. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, 97th Congress, 1st Session (Washington, D.C.: GPO, 1981), Part 7, p. 4,225.

40. Ibid., p. 4226. At this hearing Ellis says, "Strategic C^3I has not received cohesive management attention nor the funding support commensurate with the job it has been asked to do. This deficiency is a direct threat to the effective employment of our strategic forces. ... My thought is that we establish at the Secretary of Defense level

an office reporting directly to him in which all of the responsibilities reside." Ibid., pp. 3792, 3803.

41. Ibid., pp. 4,226-27.

42. Gerald P. Dinneen, Carter's ASDC^{3}I, "wasn't given the leverage he should have had to get the Services to do the job the way he wanted to do it," says DeLauer. "Why C^{3}I Is the Pentagon's Top Priority," Government Executive, vol. 14 (January 1982), p. 14.

43. For a thorough treatment of programmatic decision processes, see John D. Steinbruner, The Cybernetic Theory of Decision (Princeton: Princeton University Press, 1974). Other particularly relevant sources include Graham T. Allison, Essence of Decision (Boston: Little, Brown and Company, 1971); Richard Cyert and James March, A Behavioral Theory of the Firm (Englewood Cliffs, N.J.: Prentice-Hall, 1963); Richard R. Nelson, "Issues and Suggestions for the Study of Industrial Organization in a Regime of Rapid Technical Change," in Policy Issues and Research Opportunities in Industrial Organization, Victor R. Fuchs, ed. (New York: Columbia University Press, 1972); Karl Weick, The Social Psychology of Organizing (Redding, Mass.: Addison-Wesley, 1969); John D. Steinbruner, "Beyond Rational Deterrence: The Struggle for New Conceptions," World Politics, vol. 28 (January 1976), pp. 223-45.

44. John D. Steinbruner, "Nuclear Decapitation," Foreign Policy, vol. 45 (Winter 1981-82), p. 23.

45. David Alan Rosenberg, "'A Smoking Radiating Ruin at the End of Two Hours': Documents on American Plans for Nuclear War with the Soviet Union, 1954-55," International Security, vol. 6 (Winter 1981-82), p. 25.

46. Alain C. Enthoven and K. Wayne Smith, How Much Is Enough? Shaping the Defense Program 1961-1969 (New York: Harper and Row, 1971), pp. 3, 171.

47. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1961, 86th Congress, 2nd Session (Washington, D.C.: GPO, 1960), Part 7, p. 88.

48. See Chapter 7.

49. JCS Polo Hat and SAC "Global Shield" exercises invariably reveal major lapses in organizational performance of strategic operations.

50. John D. Steinbruner, "An Assessment of Nuclear Crises," in The Dangers of Nuclear War, Franklyn Griffiths and John C. Polanyi, Editors (Toronto: University of Toronto Press, 1979), pp. 38-39.

51. John D. Steinbruner, "National Security and the Concept of Strategic Stability," Journal of Conflict Resolution, vol. 22 (September 1978), p. 424.

52. Graham T. Allison, Essence of Decision (Boston: Little, Brown and Company, 1971), p. 127.

53. Ibid., p. 128.

54. Ibid., pp. 131-32.

55. Armed Forces Journal International

56. Although the Navy's ASW campaign deviated from the policy intentions of national officials, this aggressive, decentralized action produced unintended consequences (it delivered a stronger coercive message to Moscow than national officials ever intended) that converged on the ultimate policy objective of getting the Soviets to accept U.S. terms for resolving the crisis.

57. To the extent that effective improvisation is possible in a fast-changing environment, it is probably something best left to local commanders. Attempts at centralized improvisation perhaps only serve to undermine the ability of local commanders to respond with the necessary speed and flexibility to change in the local situation. An instructive case study and theoretical discussion is Dan Horowitz, "Flexible Responsiveness and Military Strategy: The Case of the Israeli Army," Policy Sciences, vol. 1 (1970), pp. 191-205.

58. John D. Steinbruner, "National Security and the Concept of Strategic Stability," Journal of Conflict Resolution, vol. 22 (September 1978), p. 412.

CHAPTER FOUR

COMMAND PERFORMANCE AND MASSIVE RETALIATION IN THE MID 1960s

> If you are going to attack a nation, you have to attack its control centers.
>
> — General Power (CINCSAC) 1960

To the student schooled in rational deterrence theory, the choice of preserving or destroying the opponent's command structure appears to be the most critical, the most difficult, and the most controversial. T. Schelling, a leading developer of the theory of deterrence, states:

> Here is a point where the distinction between the straightforward application of brute force to block enemy capabilities and the exploitation of potential violence to influence his behavior is a sharp one.[1]

It is a distinction with a dilemma. On one hand, a command structure attack seems inconsistent with the idea of exploiting nuclear force for political effect. The diplomacy of violence cannot be practiced if decisionmakers on either side instructed their forces to follow a strategy that would leave the opponent's decisionmaking and bargaining apparatus fractured, or that would severely degrade the enemy's ability to retain central control over surviving forces. The primary purpose of nuclear weapons might well be defeated by such a strategy. On the other hand, a strategy based on destruction of key

C^3I elements might offer the most attractive solution to the problem of limiting damage from enemy attacks. If so, and if the judgment is made that nuclear war probably cannot be avoided, then attack on the opponent's command structure could be a plausibly rational defensive act. The choice of strategy, then, depends on "whether the enemy's command structure is more vital to the efficient waging of war or the effective restraint and stoppage of war, and which of the two processes is more important to us." [2]

It is an open question whether or not Soviet attack strategy is geared to the destruction of U.S. control centers and communications channels. Soviet strategy may have evolved much like its American counterpart, becoming increasingly oriented to selective attacks with options to withhold forces aimed at population and command centers. Or it may have evolved differently, or just more slowly in the same direction. Whatever its course, however, there is no doubt that throughout the historical sequence Soviet strategists have treated command structure attack with utmost seriousness. This appreciation is evident in extensive Soviet efforts to protect their own command structure from nuclear attack. [3] It is also evident in their doctrinal writings, which strongly suggest that Soviets, in wartime, intend to exploit weaknesses in U.S. C^3I. Examples of authoritative and apparently representative Soviet views on the subject include the following:

> 1. The targets for destruction will now include...in the first instance the economies of the belligerents...the strategic offensive nuclear weapons...the system of governmental and military control and the main communications centers. [4]

2. The first nuclear strike can immediately lead to the disorganization of the government, military control, and the whole rear area of a country.[5]

Others go so far as to suggest that disruption of C^3I networks could lead to the defeat of the opponent:

> Under conditions of a nuclear war, the system for controlling forces and weapons, especially strategic weapons, acquires exceptionally great significance. A disruption of the control over a country and its troops in a theater of military operations can seriously affect the course of events, and in difficult circumstances, can even lead to defeat in a war. Thus areas deserving special attention are the following: knowing the coordinates of stationary operations control centers and the extent of their ability to survive, the presence of mobile command posts and automatic information processing centers; the communications lines' level of development and, first of all, that of underground and underwater cable, radio-delay, ionospheric and tropospheric communication lines; field communication networks and duplicate communication lines; communication centers and the extent of their facilities, dispersion and vulnerability.[6]

Besides divulging a keen awareness of the potential decisiveness of command structure attacks, Soviet military literature reveals an appreciation of the significance of rather esoteric nuclear effects such as atmospheric ionization and electromagnetic pulse:

> ... a nuclear explosion in the 50 MT range of force at an altitude of 80 km can lead to a complete loss of ordinary ionospheric radio communications over an area radius of 4,000 km....[7]
>
> A considerable threat to the intercontinental ballistic missiles are powerful nuclear explosions set off at great altitudes, because the impulses of electromagnetic energy created by such explosions

> can put out of commission not only the on-board missile equipment, but also the ground electronic equipment of the launch complexes.[8]

A widening audience of U.S. analysts and senior policy officials have lately become cognizant of this apparent Soviet determination to suppress the U.S. command structure in wartime. F. Ermarth characterizes Soviet strategy as oriented to damage limitation objectives, and the means by which it would be achieved include preemption and command structure attack:

> ..their operational perspective on the factors that drive war outcomes places a high premium on seizing the initiative and imposing the maximum disruptive effects on the enemy's forces and war plans. By going first, and especially disrupting command and control, the highest likelihood of limiting damage and coming out of the war with intact forces and a surviving nation is achieved, virtually independent of the force balance.[9]

Many senior U.S. military and civilian officials share this view of Soviet strategy. Several recent statements by high ranking officials can be cited as examples:

1. [The Soviets] believe that by neutralizing part of our command, control, and communications by electronic countermeasures and striking part by direct firepower, they will disrupt our control effectiveness...That this doctrine is being implemented is demonstrated...almost daily.[10]

2. ..the Soviets, as a matter of doctrine, treat destruction or disruption of our C3 systems as an integral part of their force planning and execution...The range of exploitation is wide, ranging from physical destruction to electronic disruption and deception. In other words, C3 systems are targets just like aircraft, airfields, and supply centers.[11]

3. At the moment it is possible that he does think he can attack our Minuteman forces, ...take out our NCA, ...destroy a major part of our population and industry, and suffer no retaliation in turn because he had knocked out our communications.[12]

4. [We can see] increasing numbers and capabilities of Soviet systems to attack our strategic C3 or reduce their effectiveness.[13]

Former Defense Secretary Harold Brown also stressed in a speech that Soviet strategic forces are aimed at U.S. command and warning elements.[14] In all likelihood, he says, these elements have always been targeted. For instance, according to Brown, in the past the Soviets "almost surely targeted" 200 SS-9 ICBMs against 100 underground launch centers that directly control the U.S. Minuteman force.[15] If so, it suggests that Soviet planners came to believe that, at least as far as this particular force component was concerned, the control system rather than the individual missile emplacements constituted the target of greatest opportunity. Might it not also suggest that Soviet planners determined that C^3I was America's primary nuclear vulnerability, and concluded that attacks on it would have a far better chance of parrying retaliation than would attacks on the individual weapons themselves?

If damage limitation has been set forth as the main objective of the Soviet nuclear war plan, if operational strategy has been grounded in the belief that attacks on C^3I networks serve this purpose better than an attack designed to maximize damage to individual force deployments, and if C^3I networks have in fact constituted the weakest component of the U.S. strategic posture, then popular accounts of trends in U.S.-Soviet strategic capabilities distort historical realities. Inasmuch as these accounts usually either rest explicitly on standard calculations of force structure vulnerability, or emphasize the same set of variables that such calculations include, they shed light on an aspect of strategic history that may be tangential, while neglecting a dimension of perhaps far greater significance. They may overstate and perhaps greatly exaggerate the amount of damage that the United States could have inflicted on an aggressor at any particular period in the historical sequence.

A reconsideration of strategic history begins in this chapter. We shall evaluate the performance of the strategic command structure in the early to mid 1960s, and then turn to succeeding periods in the next three chapters. Chapters 4, 5 (early 1970s) and 6 (late 1970s) assume a deliberate Soviet attack designed to cause maximum damage to the U.S. command structure. Since assured destruction was the benchmark of strategic sufficiency throughout this period, the implications of U.S. command vulnerability for flexible war-fighting and strategic bargaining are not developed. In Chapter 7, however, we turn to consider the scenario in which the Soviets pursue a limited counterforce strategy in a bid for intra-war bargaining dominance over the United States. The later analysis will assume that the Soviets forgo deliberate assault on the U.S. command structure; instead, they mount an attack designed to cause the maximum damage to the U.S. force structure. Collateral damage suffered by the command structure will be assessed with a view to gauging C^3I capacities for proportionate retaliation and the authoritative control of residual forces held in reserve during a protracted war.

To provide context and a basis for comparison, assessments based on enumeration which exclude measures of command performance are woven into our discussions. However, in most areas, strict comparisons cannot be made for want of a common unit of measurement. C^3I networks generally do not yield to quantitative technique, and when they do, they yield only partially. This is not to say that weaknesses and vulnerabilities cannot be sufficiently appreciated that meaningful comparisons with force structure vulnerabilities are precluded. It is to say that because of the nature of the evidence the comparisons are more difficult and require a more intuitive interpretation.

GOLDEN AGE REVISITED: MID 1960s

Although it was generally believed that until the mid 1960s, at least, the United States possessed overwhelming nuclear superiority over the Soviet Union, senior U.S. defense officials realized as early as 1961 that vital segments of the command network lacked adequate protection from missile attack. Enthoven and Smith give us a glimpse of the problems that were identified shortly after Robert S. McNamara became Secretary of Defense in 1961:

> Perhaps the most critical vulnerability problem ... lay in the U.S. high-level command structure, which was located in a comparatively small number of points on or near Strategic Air Command (SAC) bases or major cities, all of which were themselves prime targets for enemy attack. Most of the facilities were soft, and most of the communications links

> were vulnerable. A well-designed Soviet attack ... would have deprived our forces of their authorized commands to proceed to targets.[16]

It is noteworthy that by the end of 1961 government officials had debunked the mythical missile gap which had theretofore projected Soviet missile superiority. Along the narrow dimensions used to assess the strategic balance, the overwhelming superiority of the United States had been reaffirmed. However, as the above quote underscores, this sanguine reassessment neglected a critical dimension of the American strategic posture.

At McNamara's behest, measures designed to reduce the vulnerability of command centers and their communications were briskly implemented. Enthoven and Smith document the key parts of the program:

> Several national command centers were established, including some maintained continuously in the air. New procedures, equipment, and safeguards were introduced to make certain that only authorized national authorities could release nuclear weapons. Steps were taken to improve the survivability and reliability of communications systems, and all such systems were merged into a new National Military Command System.[17]

The authors describe McNamara's program as "extensive." This overstates the actual scope of the program. The revolutionary implications of the missile age had scarcely been worked through in relation to the command structure at all levels. Testifying before Congress in 1963, by which time the main steps in the initiatives cited above had been made, McNamara acknowledged that, "there is still substantial vulnerability in our command and control system."[18] He mentioned in particular the vulnerability of SAC and national level communications systems. He did not cite, but surely he anticipated, serious problems in the area of missile submarine communications.

In that same appearance, McNamara reported that the DOD "had hardly begun to study, thoroughly, the command and control system, particularly the communications system, on which our control of our strategic retaliatory forces during a nuclear attack will depend." [19] This was 1963. The United States had already deployed a large strategic missile force. Several hundred land missiles were operational, and several hundred more were under construction. Polaris missile submarines had been introduced in November 1960. By 1963, operational submarine launchers numbered about 200, and would double by 1965. If strategic force management was poorly understood, as McNamara suggested, then it seems fair to say that the rapid and large-scale deployment of raw strategic power held the highest priority during the early 1960s. The command and control implications of the strategic buildup were only slowly dawning.

Minuteman Vulnerability

Initial deployments of Soviet ICBMs did not put silo-based Minuteman missiles at risk. According to the standard calculations which measure the expected damage from nuclear blast effects, the strategic rocket force of the Soviet Union, even if fully committed, could have destroyed only a small fraction of the Minuteman force. At least two conditions deemed necessary to destroy a large fraction of the force were absent: (1) approximate numerical parity, permitting the Soviets to assign at least one weapon to each aimpoint, and (2) pinpoint missile accuracy, needed to ensure that each intended target lay within the lethal radius of each assigned weapon's likely point of impact. The absence of these conditions was apparently responsible for repeated assurances by U.S. officials that the Minuteman force was invulnerable to attack.

Recalling Figure 2-1, as late a 1966 a preemptive attack involving the entire Soviet land missile force would have destroyed only about ten percent of the numerically superior American force.[20] Figure 4-1 gives the assumptions that underlie this estimate, which is not very sensitive to changes in these assumptions. For example, if under the principle of conservative planning the reliability of Soviet missiles is raised from 75 percent to 90 percent, the expected damage increases from 10 percent to 12 percent of the U.S. force. Similarly, more conservative assumptions about Soviet missile accuracy only marginally change the results. Under all plausible conditions, a Soviet attack aimed at missile silos would have been ineffective and self-disarming. Thus, to the extent that American confidence in its land missile deterrent rested on standard calculations of force structure vulnerability, a high degree of confidence in this component was warranted.

Such confidence however, may have been unwarranted. There was at least one other dimension to the problem, a dimension that standard calculations excluded. Before we can begin to reach even tentative

U. S. AND SOVIET LAND MISSILES: 1966

Country	Missiles Deployed	Type	Yield[1] (Y)	Accuracy[2] (CEP)	Hardness[3] (H)	Reliability[4] (OAR)
U.S.	54	Titan II	5 MT	0.7 n.m.	300 p.s.i.	0.75
	800	Minuteman I	1 MT	0.7 n.m.	300 p.s.i.	0.75
	80	Minuteman II	1 MT	0.3 n.m.	300 p.s.i.	0.75
U.S.S.R.	150	SS-7	5 MT	1.5 n.m.	5 p.s.i.	0.75
	70	SS-8	5 MT	1.5 n.m.	100 p.s.i.	0.75
	110	SS-9	25 MT	0.7 n.m.	100-300 p.s.i.	0.75
	10	SS-11	1 MT	1.0 n.m.	300 p.s.i.	0.75

[1] Yield expressed in megatons.

[2] CEP is the median miss distance in nautical miles; 50 percent of the missiles are expected to fall within a circle whose radius is the CEP, and 50 percent are expected to fall outside.

[3] Hardness is the amount of overpressure, in pounds per square inch, that a missile silo can withstand.

[4] OAR is the product of the individual probabilities that the missile will not malfunction during each stage of countdown, launch, and flight.

Figure 4-1

conclusions about the retaliatory capability residing in the Minuteman force in 1966, the performance of the manned underground facilities, which maintained remote launch control over the silo-based missiles, must be estimated.[21] As we shall see, an interesting comparison emerges between the results calculated for an attack aimed at these launch control centers (LCCs) and an attack aimed at the missile silos (LFs).

The key physical aspects of this particular control problem concern the number of attacking Soviet missiles in 1966, their capability to disable individual LCCs, and the amount of redundancy existing in the Minuteman launch control system. First, the Soviet ICBM force, though numerically insufficient to attack a substantial fraction of the deployed LFs, was large enough to attack all of the deployed LCCs. The Soviets could have aimed at least one high-yield SS-9 missile at each of the 88 operational LCCs.[22]

Second, the estimated yield and accuracy of SS-9 missiles were sufficient to generate powerful blast overpressure in the vicinity of LCCs, threatening destruction of most of them. The probability of LCC survival depended on its hardness, which may have been as low as 250 pounds per square inch (p.s.i.) of blast overpressure. If that were the case, an LCC would have had only about an 11 percent chance of surviving an attack by an SS-9 missile with perfect reliability.[23]

The most severe vulnerability problem lay in the communications associated with LCCs. The communications linking them to higher authority were far more susceptible to damage from nuclear weapons effects than was the LCC structure itself. PAS, the primary medium of strategic communications, employed a voice link akin to an ordinary telephone that was vulnerable to very modest overpressure (approximately 20 p.s.i.) despite its subsurface deployment (see Chapter 3). SACCS, a teletype connection, depended on surface, terrestrial land lines that were vulnerable to overpressure in the 5 p.s.i. range. Back-up channels consisted of radio systems of which only one was designed to withstand nuclear attack. This system, the least vulnerable to blast effects, featured underground, "pop-up" antennas intended to receive high frequency (HF) radio transmissions. But the antennas associated with HF communications were not heavily protected. Once deployed above ground, their vulnerability to blast effects would have been acute, and even while retained in their underground sheaths, they were not expected to withstand overpressures that exceed 50 p.s.i. In addition to blast effects, SS-9 surface detonations would have generated fields of electric and magnetic energy powerful enough to disable any communications equipment exposed to them.

The third aspect of the situation is that the launch of Minuteman forces required the active participation of LCCs. A back-up airborne launch system would soon become operational, but at the time no such redundancy existed.

Back-up LCCs provided a considerable though limited amount of launch redundancy. Not every LCC was interconnected with every missile in the force. Instead, the forces were organized into missile squadrons composed of 50 LFs and five LCCs.[24] Squadrons were completely independent of each other; it was physically impossible for LCCs in one squadron to fire any missiles belonging to a different squadron. However, within a given squadron, arrangements were such that any two functioning centers could fire all 50 missiles. A single LCC could also fire them, but the countdown to lift-off would have been extended by half an hour, perhaps longer. To avoid this delay, two LCCs had to perform the launch procedures.

The destruction or disablement of all five LCCs within a squadron would have removed the launch capability for that unit and effectively incapacitated 50 missiles. Calculations of the expected damage to LCCs thus provide a reasonable basis for estimating the unusable portion of the Minuteman force following the initial Soviet strike. The conversion is straightforward: minus 50 missiles for every squadron deprived of launch control.

Estimates of the unusable portion of the Minuteman force do not tell the whole story, however. Partial damage to a squadron also degrades performance. Apart from launch delays caused by the event discussed above (destruction of four LCCs), there are conditions that cause problems of intra-squadron coordination among two or more surviving LCCs, and the attendant lowering of unit performance can be substantial.

Coordination problems stem from degraded intra-squadron communications, and complex interactions among the rules and operating procedures that govern the actions of LCCs. As argued at a somewhat high level of abstraction in Chapter 3, the consequences of enacting such preprogrammed routines cannot be fully anticipated, and this general proposition is borne out when an attempt is made to predict the results of LCC operations under conditions of partial damage. Despite the fact that LCC operators are instructed to follow a well-defined set of procedures, and may do so to the letter, remarkably little is known about the outcomes that the programmatic decision process is capable of generating under the broad range of conditions that may apply. Aided by a computer model that simulates the decision process, we have been able to "observe" at least some of the unfolding interactions that appear to have adverse effects on performance.

Before describing several illustrative interactions and their consequences, we turn to summarize calculations of the unusable portion of the Minuteman force. Disablement of entire squadrons is estimated on the basis of expected damage from two distinct sources: blast overpressure and electromagnetic pulse. Since degradations resulting from problems of intra-squadron coordination are excluded from the calculations, the results should be interpreted as the minimum expected damage from a dedicated Soviet attack on LCCs. The amount of damage attributable to blast will be estimated first.[25]

Damage From Blast Overpressure: The results of the analysis, summarized in Figures 4-2 to 4-10 depend on assumptions about target hardness, Soviet missile accuracy and reliability, and Soviet attack strategy. But in practically every case the estimated damage from blast effects alone exceeds that which an all-out Soviet attack on missile silos inflicts. In most cases the difference is rather great.

Contrary to then-prevailing opinion, the size and accuracy of the Soviet missile force did not preclude a major threat to Minuteman. Figure 4-2 shows this clearly. If these two are taken to be the only pertinent parameters, then in 1966 an SS-9 missile attack aimed at LCCs rather than individual silos may have virtually disarmed the Minuteman force.

There are of course other relevant parameters that must be taken into account. Missile reliability and reprogramming capabilities, for example, are shown in Figure 4-2 to be important determinants of the effectiveness of a Soviet attack on LCCs.

Closer examination of the Soviet missile force would probably conclude that the capability for extensive reprogramming was lacking in 1966, and that SS-9 missile reliability was far from perfect. Nevertheless, conservative planning assumptions would probably credit the SS-9 with an overall reliability in the 0.80 to 0.85 range, in which case a significant risk ($\geq$ 10 percent probability) existed that one-half to two-thirds of the Minuteman force would have been incapacitated, even without any reprogramming of the attacking forces. (According to the standard calculations, a comparable threat based on silo attacks did not develop until quite recently). Presumably, a risk-averse American planner would also have found cause for worry if missile reliability were much lower but reprogramming capabilities could not be ruled out. Even if reliability were only 0.70, a highly significant risk ($\geq$ 20 percent) existed that reprogramming of the attack would have resulted in the loss of launch control over three-fifths to three-quarters of the Minuteman force.

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS

Soviet Missile Reliability	-----------Land Missile Force Incapacitated----------- (Percent of Minuteman)			
		Reprogrammed Attack		
	Expected	Risk≥20%	Risk≥10%	Risk≥5%
.70	47-71	59-77	65-82	71-82
.75	59-77	65-82	71-88	77-94
.80	65-77	77-88	77-94	82-94
.85	71-82	82-94	88-94	88-100
.90	82-88	88-94	94-100	94-100
.95	88-94	94-100	100	100
1.00	100	100	100	100
		Non-Reprogrammed Attack		
.70	18	29	35	35
.75	24	35	41	47
.80	35	47	53	53
.85	47	59	65	71
.90	59	71	77	82
.95	77	88	88	94
1.00	94	100	100	100

Figure 4-2

The reasoning behind these estimates is that the Minuteman force was at least as vulnerable as the LCCs that controlled it, and the LCCs were at least as vulnerable as the LCC communications that linked them to higher authority. For Figure 4-2, the destruction of that link at a given LCC was assumed to occur if blast overpressure exceeded 50 p.s.i., the estimated tolerance of the hardest communications system. Figures 4-3 and 4-4 show the results when this threshold is raised to 100 and 150 p.s.i., respectively.

Structural damage rendering LCCs inoperable (not just communications) is associated with blast overpressures in the 250-1,000 p.s.i. range. An attack strategy designed to dig out the LCC structures themselves while still attempting to maximize the number of squadrons destroyed would have forced Soviet planners to allocate at least ten missiles per Minuteman squadron (at least two per LCC). Calculations summarized in Figures 4-5 to 4-10 assume such a strategy which, owing to limited SS-9 resources, precludes attacks on many squadrons in order to double up on other squadrons. The results assume that there was no attack reprogramming.

The upshot of all this is that a command structure attack offered, at least on paper, a not remote chance of disabling the bulk of the Minuteman force; and, the expected damage exceeded by a wide margin the damage that could have been expected from an attack on LFs, at one-third the cost in terms of Soviet missiles expended. Although in most of the cases considered, the odds against disarming the Minuteman force using blast effects against LCCs were overwhelming, the Soviet SS-9

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS

Soviet Missile Reliability	-----------Land Missile Force Incapacitated------------ (Percent of Minuteman)			
		Reprogrammed Attack		
Reliability	Expected	Risk≥20%	Risk≥10%	Risk≥5%
.70	47-65	53-71	59-77	65-77
.75	53-71	65-77	65-82	71-88
.80	59-71	71-82	77-88	77-88
.85	65-77	77-88	82-88	88-94
.90	77-82	82-88	88-94	94
.95	82-88	88-94	94	94-100
1.00	94	100	100	100
		Non-Reprogrammed Attack		
.70	18	24	29	29
.75	24	29	35	41
.80	29	41	47	47
.85	41	53	59	59
.90	53	65	71	77
.95	71	82	82	88
1.00	94	100	100	100

Figure 4-3

SOVIET SS-9 ATTACK AGAINST MINUTEMAN LAUNCH CONTROL CENTERS

Soviet Missile Reliability	------------Land Missile Force Incapacitated------------ (Percent of Minuteman)			
	Reprogrammed Attack			
	Expected	Risk≥20%	Risk≥10%	Risk≥5%
.70	41-53	47-65	53-65	59-71
.75	47-59	53-71	59-77	65-82
.80	53-65	59-71	65-77	71-82
.85	59-65	65-77	71-82	77-88
.90	65-71	77-82	77-82	82-88
.95	71-77	82	88	88-94
1.00	77	88	88-94	94
	Non-Reprogrammed Attack			
.70	12	18	24	29
.75	18	29	29	35
.80	24	35	41	47
.85	35	47	53	53
.90	47	59	65	65
.95	59	71	77	82
1.00	77	88	88	94

Figure 4-4

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[a,d,f]

Soviet Missile	--------Land Missile Force Incapacitated-------- (Percent of Minuteman)[h]					Land Missile Force Degraded (Percent of Minuteman)[h]
Reliability	Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%	Expected
.75	33	44	44	50	56	22
.80	39	50	50	56	56	17
.85	44	50	56	56	61	22
.90	50	56	61	51	61	11
.95	56	61	61	61	61	6

Figure 4-5

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[b,d,f]

Soviet Missile Reliability	Land Missile Force Incapacitated (Percent of Minuteman)[h]					Land Missile Force Degraded (Percent of Minuteman)[h]
	Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%	Expected
.75	22	28	33	33	39	28
.80	22	28	33	39	44	28
.85	28	39	39	44	50	22
.90	33	39	44	50	56	22
.95	33	44	50	50	56	22

Figure 4-6

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[a,c,f]

Soviet Missile Reliability	-------Land Missile Force Incapacitated------- (Percent of Minuteman)[h]					Land Missile Force Degraded (Percent of Minuteman)[h]
	Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%	Expected
.75	17	22	28	28	33	33
.80	17	28	28	33	39	39
.85	28	33	39	44	50	39
.90	33	44	50	50	61	39
.95	44	56	61	67	72	39

Figure 4-7

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[a,d,g]

Soviet Missile Reliability	Land Missile Force Incapacitated (Percent of Minuteman)[h]					Land Missile Force Degraded (Percent of Minuteman)[h]
	Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%	Expected
.75	11	17	22	22	28	22
.80	17	22	28	28	33	22
.85	17	28	33	33	39	28
.90	22	28	33	39	44	28
.95	28	39	39	44	50	22

Figure 4-8

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[a,e,g]

Soviet Missile Reliability	-------Land Missile Force Incapacitated------- (Percent of Minuteman)[h]					Land Missile Force Degraded (Percent of Minuteman)[h]
	Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%	Expected
.75	17	22	28	28	33	17
.80	22	28	28	33	33	17
.85	22	28	33	33	39	11
.90	28	33	33	39	39	11
.95	28	33	39	39	39	11

Figure 4-9

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[b,e,g]

Soviet Missile Reliability	--------Land Missile Force Incapacitated-------- (Percent of Minuteman)[h]					Land Missile Force Degraded (Percent of Minuteman)[h]
	Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%	Expected
.75	6	11	17	17	22	17
.80	11	17	17	22	28	17
.85	11	17	17	22	28	17
.90	11	17	22	22	28	17
.95	17	22	22	28	33	17

Figure 4-10

NOTES TO FIGURES

[a]SS-9 missile accuracy assumed to be 0.7 nautical miles.

[b]SS-9 missile accuracy assumed to be 0.9 nautical miles.

[c]Attack Strategy A: one-on-one attack against eighteen Minuteman squadrons. No reprogramming.

[d]Attack Strategy B: two-on-one attack against eleven Minuteman squadrons. Seven squadrons not attacked. No reprogramming.

[e]Attack Strategy C: three-on-one attack against seven Minuteman squadrons. Eleven squadrons not attacked. No reprogramming.

[f]Launch control center hardness assumed to be 250 pounds per square inch.

[g]Launch control center hardness assumed to be 1,000 pounds per square inch.

[h]Percent of the Minuteman force of 880 missiles

force could have substantially reduced U.S. land missile strength and there was an outside chance that the damage would have been very great indeed.

Damage From Electromagnetic Pulse: The standard analytic conclusion that Minuteman was an invulnerable force also completely discounted possible damage from a nuclear weapons effect known as electromagnetic pulse (EMP).[26] Originating with the interaction of released gamma rays and air, EMP is a brief but intense energy wave that can induce tremendous voltage and current surges in cables, antennas, power and telephone lines, buildings, aircraft, and so forth. These "collectors" can then deliver the power surge to electronic components, causing temporary or permanent damage to electrical systems.

For a high-yield nuclear explosion above the earth's atmosphere, released gamma rays travel long distances before colliding with air. As a result, the pulse covers a large area of the earth. Figure 4-11 depicts the area of exposure for a single high-yield explosion 60 miles above the United States. A 20,000-50,000 volt pulse blankets all LFs and LCCs located within the six operational Minuteman fields.[27]

For ground or near-surface bursts, which electrify both the air and the ground, the pulse would be at least an order of magnitude greater than the peak pulse observed at the surface from a high-altitude explosion.[28] But, a pulse this strong would radiate only about five miles. Outside this region, pulse strength dissipates rapidly with increasing distance from the burst point.

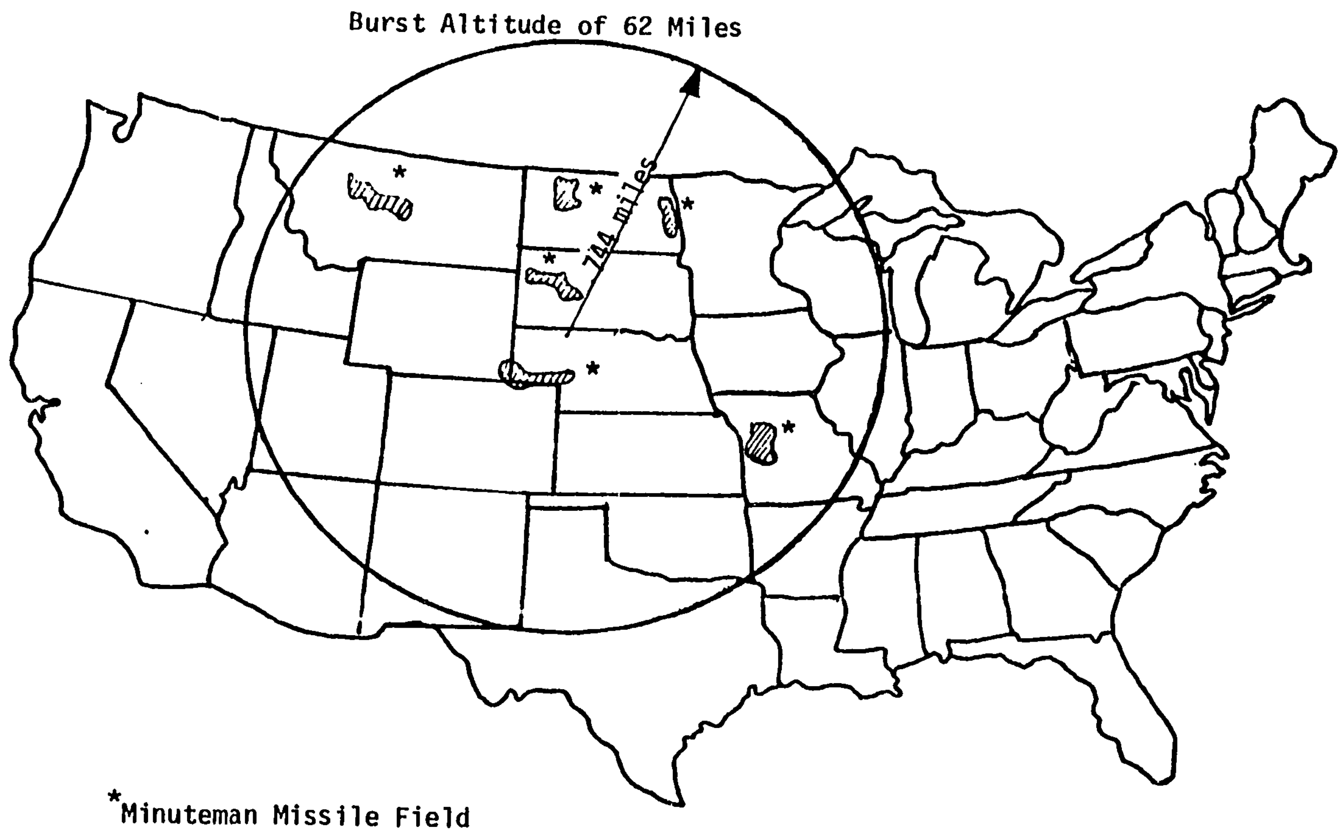

Burst Altitude of 62 Miles
744 miles
*Minuteman Missile Field

Figure 4-11

Given Soviet missile accuracy in 1966, it is quite certain that Minuteman LCCs (and some nearby LFs) would have been exposed to strong electromagnetic fields. By contrast, each SS-9 explosion would not necessarily have exposed a launch control center to high blast overpressure. Missiles landing well within seven-tenths of a mile from their targets would have subjected the centers to extreme overpressure. But missiles landing, say, two miles from their targets would not have. In short, blast overpressure and electromagnetic pulse are separate and independent threats to the LCCs. A burst near the surface generates both phenomena, either of which might damage the target. Compounding the problem, any exoatmospheric explosion(s) could have blanketed the entire area in which LCCs and LFs were deployed.

Their vulnerability to EMP attack cannot be measured precisely, but it appears to have been appreciable in 1966. Regarding missiles and their support equipment inside their LFs, DOD testimony reveals that:

> ..in the early 1970s, we began an extensive EMP assessment of Minuteman silos to determine their hardness to high altitude and ground burst EMP. We found that, although there was some EMP hardness inherent in existing Minuteman silos, additional EMP hardening was required to provide greater assurance that Minuteman silos were not vulnerable to EMP. [29]

Launch control centers, as well, appeared to be vulnerable to EMP, for several reasons. First, each LCC is a large, distributed and redundant electrical system with numerous cables, transmission lines, and antennas to collect the energy from electromagnetic fields. Voltage and current surges could have entered an LCC along numerous paths. Second, the disabling of a single critical element — the main computer or the communications receivers — can render an LCC inoperable even though other critical components suffered no damage. Third, in 1966 the LCCs lacked any special protection against EMP. Lastly, recent theoretical and experimental studies of the vulnerability of electrical systems similar to those found at LCCs suggest that the latter were prone to damage or serious disruption from a typical high-intensity pulse.

High frequency antennas, for example, can "collect many thousands of amperes and exhibit voltages well in excess of their normal voltages." [30] Another study determined that the surges induced in antennas and transmission lines could exceed one million volts and ten thousand amperes. [31] These values are only suggestive of the magnitude of the problem. Appendix C analyzes, in a more rigorous way, the vulnerability of the computers at launch control centers. The analysis assumes a high-yield burst above the atmosphere, and calculates the voltage surge at the ends of a hypothetical buried cable connecting a hypothetical missile silo and an LCC computer. In the analysis, the computer contains integrated circuits having a voltage damage threshold on the order of ten volts for a pulse duration of approximately one-millionth of a second. Since the voltage surge at the ends of the buried cable varies with the direction of arrival of the incoming electromagnetic pulse, calculations for many different angles were performed. The estimated voltage surge for the worst-case angle of arrival exceeds the damage threshold for integrated circuits by two orders of magnitude. For all cases considered, the average peak value of the surge exceeded the damage threshold by a factor of 40. These estimates may not be valid even as a first approximation of LCC vulnerability. But there is no doubt that, as a study sponsored by the Defense Nuclear Agency puts it, "old cable systems remain a focal point of EMP concern." [32]

The method used earlier to calculate SS-9 damage to the Minuteman force can accommodate probabilistic representations of EMP threat. Various levels of threat, ranging from zero to 90 percent probability that a single pulse would disable an LCC actually exposed to it, were combined with expected blast damage to estimate the compound damage to the Minuteman force from an SS-9 attack in 1966. Figure 4-12 summarizes one set of calculations. The results are far from worst-case because the LCCs are credited with a blast hardness of 250 p.s.i., and the attacker is not credited with any reprogramming capability. The underlying assumptions are identical to those that apply in Figure 4-7 above, though of course the earlier treatment ignored electromagnetic pulse effects. Figure 4-12 adds this dimension. It might be useful to recapitulate the key assumptions: (1) the Soviets target 88 SS-9 missiles at 88 Minuteman launch control centers, (2) SS-9 accuracy is seven-tenths of a mile, (3) LCCs can withstand up to 250 p.s.i. of blast overpressure, (4) each LCC receives a pulse of electromagnetic energy in addition to some overpressure, (5) the damage from blast and electromagnetic pulse are uncorrelated. Figure 4-13

SOVIET SS-9 ATTACK AGAINST MINUTEMAN LAUNCH CONTROL CENTERS[a]

Soviet Missile Reliability	EMP "Kill" Probability[b]	Land Missile Force Incapacitated (Percent of Minuteman)[c]				
		Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%
.75	0	18	24	29	29	35
.75	.10	18	24	29	35	47
.75	.20	24	29	35	41	53
.75	.30	29	35	41	47	59
.75	.40	35	47	53	53	65
.75	.50	41	53	59	65	71
.75	.60	53	65	71	77	82
.75	.70	65	71	77	82	94
.75	.80	77	82	88	94	100
.75	.90	88	100	100	100	100
.85	0	29	35	41	47	53
.85	.10	29	41	47	53	59
.85	.20	35	47	53	59	71
.85	.30	41	53	59	65	71
.85	.40	47	59	65	71	82
.85	.50	59	65	71	77	88
.85	.60	65	71	77	82	94
.85	.70	77	82	88	94	100
.85	.80	82	88	94	100	100
.85	.90	94	100	100	100	100

Figure 4-12

SOVIET SS-9 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[d]

Soviet Missile Reliability	EMP "Kill" Probability[e]	Land Missile Force Incapacitated (Percent of Minuteman)[f] Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%
.75	0	18	24	29	29	35
.75	.10	24	29	35	41	53
.75	.20	35	41	47	53	65
.75	.30	47	53	59	65	77
.75	.40	59	65	71	77	88
.75	.50	71	82	88	88	100
.75	.60	82	88	94	100	100
.75	.70	88	100	100	100	100
.75	.80	100	100	100	100	100
.75	.90	100	100	100	100	100
.85	0	29	35	41	47	53
.85	.10	35	47	53	59	71
.85	.20	47	59	65	65	77
.85	.30	59	65	71	77	88
.85	.40	65	77	82	88	94
.85	.50	77	88	94	94	100
.85	.60	88	94	100	100	100
.85	.70	94	100	100	100	100
.85	.80	100	100	100	100	100
.85	.90	100	100	100	100	100

Figure 4-13

NOTES TO FIGURES 4-12 THROUGH 4-13

[a]Blast and electromagnetic pulse damage from surface bursts only.

[b]The probability that a surface burst would disable an LCC by EMP effects alone.

[c]Percent of the Minuteman force of 880 missiles.

[d]Blast and electromagnetic pulse damage from surface bursts and a single exo-atmospheric burst.

[e]The probability that a surface burst, by itself, would disable an LCC by EMP effects alone; and, the equal probability that an exo-atmospheric burst would disable an LCC by EMP effects alone. Assumes independent but equal "kill" probabilities for each pulse.

[f]Same as (c) above.

shows the expected damage when it is further assumed that the Soviets explode a single high-yield warhead above the atmosphere, generating another pulse which simultaneously strikes all 88 launch control centers.

The results require little interpretation. They indicate that unless the LCCs were not very susceptible to damage from EMP effects, a Soviet attack in 1966 offered a good chance of reducing the effective retaliatory capacity of American land missiles to low levels. They do not establish the actual vulnerability of exposed LCCs, but they at least raise that as an important question. It is a hard question, much more so than the question of vulnerability to blast effects. But the very fact that damage from electromagnetic pulse cannot be assessed with analytical precision or high confidence is a story unto itself. It casts fundamental doubt on the standard approach to analysis of strategic vulnerability.

Other Problems Affecting LCC Performance: Many problems of both a technical and organizational nature are not reflected in the above computations. Technical problems that probably would have been encountered include, in particular, severe degradation of communications reception at surviving LCCs. Restoration of communications would have been difficult and slow in the event that telephone and the other unprotected communications system broke down under attack (a virtual certainty).

The erection of an antenna intended to receive HF transmissions would have been attempted with fingers crossed (an explosive charge wired to LCC controls was supposed to propel the antenna out of its underground sheath into position), and if successfully deployed the LCC once again becomes dependent upon an exposed and easily destructible antenna. Furthermore, high frequency communications are unreliable in a nuclear environment. While high frequency radio confers the benefits of long-distance communications, the adverse effects of nuclear explosions on wave propagation are pronounced at that wavelength. A nuclear burst can produce sufficient atmospheric ionization to cause signal blackout, and with some direct effort, for instance a high altitude detonation, "blackout may persist for many hours over regions thousands of miles in diameter." [33] The Defense Nuclear Agency reported to Congress in 1976 that it had restudied the data from atmospheric nuclear tests conducted in 1962, and had "reconfirmed that high frequency band radio is grossly degraded in a nuclear environment." [34] While it is uncertain whether nuclear explosions would have blacked out the frequency range within which the only semisurvivable means of receiving instructions from higher authority operated in 1966, disruption of communications reception at surviving launch control centers was virtually certain.

Other adverse effects on squadron performance could have resulted from interactions among human, technical and procedural factors. To illustrate one possible adverse consequence of established organizational procedure, suppose that the post attack condition of a

Minuteman squadron was as follows: (1) three LCCs destroyed, (2) one LCC damaged, and (3) one LCC undamaged. Let an undamaged LCC be defined as one which remains internally functional and which maintains normal control over squadron LFs and normal contact with higher authorities. A damaged LCC is defined as one which remains interconnected by underground cable to squadron LFs, but which lacks a communications link to higher authority as well as to the undamaged LCC in its squadron.

Under these hypothetical circumstances preestablished operating procedures would have prevented retaliation, even though missile silos escaped damage altogether, the missile squadron had a normally functioning LCC, and a line of communications existed between higher authorities and the undamaged LCC. The inability to launch missiles is due to procedures which govern actions by the damaged, isolated LCC. This center and the undamaged center work at cross-purposes. The latter, upon receipt of valid war commands from higher authority, send arm, target and fire commands to Minuteman LFs. But the damaged center, though it cannot receive emergency action messages from higher authority, does not remain passive while the companion LCC initiates the launch sequence. It cancels the arm, target and fire commands transmitted by the functional center. As it is able to monitor squadron missile status, the damaged LCC detects what appears to be an attempt by another LCC to fire squadron missiles without authorization. It could have, and if it adhered to preestablished safeguard procedures it would have, successfully prevented the countdown. [35]

In the above example, it is assumed that the undamaged LCC validated the execution message and initiated the launch sequence. However, the decision to treat the message as authentic normally required confirmation from another squadron LCC; and, in the absence of such information (as in the situation outlined above), the undamaged LCC would not necessarily have exercised its conditional grant of authority to initiate the launch sequence on its own. To have done so, the LCC must have satisfied itself that the message was apparently authentic, and then exhausted every possible means of obtaining confirmation from an outside source (including sources besides LCCs). At what point, if ever, does the LCC decide that it has availed itself of every possible means of obtaining confirmation, that the effort is futile, and that the proper course of action is the launch of the squadron's weapons? The rules of authentication were (and still are) ambiguous enough that the final LCC decision could have gone either way. We would venture to guess that under many imaginable circumstances an LCC would have never abandoned the effort to make outside contact, in which case there would not have been any arm, target or launch commands for the other surviving (but isolated) LCC to cancel. Thus, it is plausible that even if four LCCs had been destroyed, removing the capability to prevent the successful launch of the squadron's missiles by the fifth LCC, no weapons would have been fired. This despite the receipt of an authentic execution message by the surviving LCC. Furthermore, it is conceivable that under established procedure no missiles would have been launched even if two or three LCCs survived attack and all received an apparently authentic execution message.

LCC performance may have also been degraded by the destruction of feedback mechanisms which facilitate correction of errors committed during the launch sequence. Intra-squadron computer and voice communication links provided the primary means of error correction, and if damaged the chances of recovering from mistakes in time to avoid, for example, execution of the wrong attack plan (or execution of the right plan at the wrong time) would have been diminished.[36]

Outcomes like those discussed above may not be foreseen in advance of actual conflict, but they would come as no great surprise to analysts who view strategic organizations as operating in accordance with a programmatic decision process that has benefited little from experiential learning. Although standard models of strategic conflict exclude both operational detail and human error in control systems, such factors do exist and their effects on performance can be rather great, as the illustrations above attest.

Soviet capability to degrade performance appears to capitalize on an inherent tension between two priorities that substantially drove the behavior of Minuteman squadrons. Much of the established procedure within the squadron (and any other strategic unit, we argue) was devoted to <u>negative control</u>, that is, the prevention of unauthorized launches. On the other hand, much of the established routine was devoted to <u>positive control</u>, that is, attack authorization and coordination. These were competing priorities, and LCC vulnerability intensified the trade-off. As we have seen, operating procedures devoted to the two priorities could interact in ways that precluded a salvo launch by a squadron that suffered only partial damage. In this instance procedures devoted to negative control are predominant, and the interaction results in failure to execute an authorized launch. The intra-squadron coordination required to implement the attack cannot be achieved. Positive control breaks down. Degradation results, for instance, when a sole surviving LCC with an authentic execution message in hand persistently but unsuccessfully seeks confirmation of the message's authenticity from an outside source.

This last example can be modified to illustrate the opposite result: degradation of negative control. Suppose that a sole surviving LCC received an invalid execution message, but the LCC could not determine this unless communications with another unit could be established. If the LCC failed to make contact, and hence failed to discover that the message was not authentic, yet proceeded to launch squadron missiles, as was allowed by established procedure, then we have a clear case of a breakdown of negative control.

A complete, unmitigated breakdown of negative control would have occurred if isolated LCCs launched their forces on their own accord, without receiving an execution message at all. In that event, the destruction of all LCC communications links to higher authority would not negate squadron retaliation (as the previous calculations assumed). The physical capability to execute the squadron's missiles would have still existed (in 1966), as long as at least one LCC survived the attack, and the possibility that surviving LCCs would have engaged in unauthorized strategic operations cannot be categorically ruled out.

Negative control is clearly a relevant criterion for assessing the performance of strategic organizations but it is also a complicating factor in any evaluation. For current purposes, suffice it to state that the two priorities — positive and negative control — are embodied in rules and procedures which substantially drive the behavior of strategic units; that the two priorities are intertwined; that an unresolved trade-off exists between them; and that command system vulnerability intensifies this fundamental tension.

Further degradation of overall command performance would have been incurred in both dimensions in the event Soviet forces had attacked other parts of the command structure besides LCCs. Primary targets may have included national command centers, high level military headquarters, early warning sensors and assessment centers, and/or the communications channels by means of which execution messages would have been disseminated to the bomber and submarine forces as well as Minuteman LCCs. These C^3I elements constituted a relatively small set of potential targets, and none were more vulnerable than those used to manage missile submarine operations in 1966.

Missile Submarine Vulnerability

In 1966, the Soviets had no proven, effective capability to detect, localize or attack U.S. missile submarines deployed at sea. But the strategic weapon system least vulnerable to enemy attack was at the same time the least manageable. There is strong evidence that with some concentrated effort the Soviets could have detached the submarine fleet from central command channels, and moreover that the force would have faced a protracted period of isolation.

Organizational arrangements, as well as physical configuration, created this vulnerable state. Organizationally, the chain of command for execution of the strategic war plan ran from the national command authorities to the unified (and specified) commanders, and then to the executing missile submarines (and bomber and land missile forces under the jurisdiction of CINCSAC, the specified commander). This arrangement meant that, for instance, "one would call CINCPAC who would then pass the order on down to the forces."[37] But this also implies that successful attacks on CINCPAC (Commander-in-Chief Pacific) and CINCLANT (Commander-in-Chief Atlantic) would have removed a vital link in the command hierarchy and isolated Pacific- and Atlantic-based missile submarines under these respective unified commands.

The primary command centers of the unified commanders were fixed, ground-based facilities located in Honolulu and Norfolk. They could not have withstood attacks directed against them. Located nearby were fixed, emergency alternate command centers that were either unhardened or only partially protected. One of the best protected command posts, CINCPAC's alternate facility in the Kunia tunnel, probably was vulnerable in any practical sense to direct attack.

This vulnerability was partially mitigated by the deployment of an EC-135A airborne command post to satisfy a CINCPAC requirement established in 1965.[38] This aircraft would be maintained on ground alert and launched upon receipt of tactical attack early warning, or earlier if circumstances warranted. Its weaknesses included: 1) lack of EMP protection; 2) reliance on an unreliable tactical early warning network for prelaunch survival; and 3) limited range and endurance. EC-135A aircraft also possessed an extremely limited communications suite. It is very doubtful that it could have established direct contact with either alert missile submarines or CONUS-based higher authorities.

The primary communications channels connecting national authorities with missile submarines employed vulnerable land lines, undersea cables, and fixed coastal radio stations. Emergency action messages sent from the NCA to CINCLANT would have been routed via land line, and via land line and undersea cable to CINCPAC. (Prior to 1964, when the transpacific cable was laid, communications with CINCPAC relied on HF radio to span the Pacific.) The unified commanders would have then passed the message to dispersed shore-based radio stations for transmission to alert submarines. The destruction of CINCPAC and CINCLANT headquarters would have therefore incidentally destroyed two critical communications as well as command modes.

The radio stations and transmitters were of course more numerous and widely scattered than the facilities in Honolulu and Norfolk that coordinated their use. Radio stations at 60 or more shore locations worldwide were dedicated to the fleet broadcast system, and radio transceiver capabilities on hundreds of surface ships augmented this system.

Although even conventional explosives could have destroyed any given shore-based station, [39] including any one of the handful of very low frequency (VLF) transmitters that were key to submarine communications, [40] many contended that the large number of assets on land and at sea ensured adequate post attack communications. Representative of this view, which prevailed in the early 1960s, is the following statement submitted to Congress in 1960 by Navy Admiral Raborn:

> Practically all military and civilian shore communications stations in all countries of the world are vulnerable to nuclear attack.... Hardening such facilities for protection against thermonuclear bombs would be a tremendously expensive undertaking. POLARIS communications reliability will not be governed by the vulnerability of any single shore radio station. It is a fact that a large amount of dispersed U.S. Navy communications equipment and stations exist today in the United States, at sea in every Navy ship, and in friendly countries which would survive an attack due to sheer numbers. Any or all of these facilities can and will be commanded quickly to act as communication stations for POLARIS as the need arises. The sheer multiplicity of radio stations will almost assure with certainty an adequate number of surviving stations capable of communicating with the POLARIS submarine. [41]

Former Secretary McNamara echoed this appraisal in an appearance before a committee of Congress in 1963:

> (MR. FORD) What about your very low frequency communications with POLARIS submarines? Are these transmitting stations secure?

> (SECRETARY MCNAMARA) I am told (by Admiral Anderson, then Chief of Naval Operations) that they are probably secure, but that, to the extent they might be destroyed, the redundancy in our total naval communications system is such that beyond any reasonable doubt we could communicate with the POLARIS submarine.[42]

This was wishful thinking. In the first place, these assessments did not come to grips with the full range of physical threats to missile submarine communications. Besides being vulnerable to the blast effects of nuclear and conventional explosives, radio stations were susceptible to electronic countermeasures, especially jamming. The U.S. Navy's radio broadcast system possessed negligible antijam capabilities. Soviet jammers, until and unless suppressed by Western forces, probably could have substantially reduced the effective range of radio transmissions from shore and ships at sea. Among the key stations subject to such interference were the VLF shore stations, some of which could not radiate enough power to overcome even modest amounts of jamming, and all of which lacked the special antijam equipment needed to achieve maximum effectiveness from available power.[43]

Other physical threats that were not sufficiently weighted in the official assessments include EMP effects. There was some risk that high altitude bursts would have caused widespread damage not only to shore stations, but ships as well. Finally, messages broadcast over low frequency (LF) and VLF were susceptible to distortion from nuclear effects on the ionosphere, and HF radio communications may have been blacked out for very long periods.[44] HF blackout would have severely degraded Navy communications, because most shore stations and all ships relied on HF radios for long-distance communications.

The official conclusion also had not come to grips with the fact that successful propagation of messages through a partially damaged and loosely coupled network requires a well worked out plan to coordinate the actions of units included in the network. Recent experience indicates that organizational rather than technological factors impose the sharpest constraints on performance. When the Navy finally began in 1979 to seriously investigate various schemes for using ships at sea to relay messages to missile submarines, it found that sheer numbers alone do not ensure reliable strategic communications. Recent testimony by Admiral Kaufman, former Director of Navy Command, Control and Communications, is instructive:

> The Navy is currently refining the means for using ships to relay communications to submarines with High Frequency radio equipment already in the fleet. Exercises conducted in the Atlantic this January further tested a concept we call Mobile HF. Under this concept, ships monitor selected frequencies and relay them over several frequencies according to predetermined schedules to avoid interfering with each other. This results in a chain reaction effect in the High Frequency spectrum with many messages, on many frequencies, from many sources leading to a high probability these messages will be received by a submarine. Preliminary results from the January tests are encouraging, but a complete analysis must await the return from sea of the submarines involved in the exercise.[45]

Since the preplanning required to organize a functional network involving ships and other general purpose communications stations had not even been initiated by the mid 1960s, it is safe to assert that the official assessment of the role and contribution of such assets to post attack communications with missile submarines was overly optimistic.

The official conclusion was vulnerable on one last score. Redundancy was not really a distinguishing feature of the total naval communications system. Many transmitters were geographically collocated, and those that were not in close physical proximity were functionally tied into common command centers or communications facilities. The existence of critical nodes and the considerable amount of interdependence among the shore-based elements suggest that communications redundancy was minimal. And as far as command redundancy was concerned, practically none existed at all. It is likely that the destruction of the unified command centers would have produced so severe a concussion to the command structure that it would not have been possible for central decisionmakers to exercise positive control over the missile submarine force.

How authority over submarine operations would have devolved and what problems of negative control may have arose in the event enemy attacks ruptured the command system are once again matters of speculation. We at least know that submarine crews, like LCCs, possessed the physical capacity to launch nuclear weapons on their own.[46] They did not depend on higher authorities for an enabling code, without which weapons could not be unlocked and fired.

But unlike LCCs, submarine crews may have operated under formal guidance that permitted the firing of missiles without the personal command of higher authorities. Under some circumstances, the exact contours of which remain cloaked in secrecy, a conditional grant of launch authority evidently extended down to the lowest rung of the submarine command hierarchy. That nuclear launch authority may have been delegated to the local submarine commanders is suggested by the following colloquy in congressional hearing held in 1963:

> (MR. FLOOD) What I have in mind is a Buck Rogers situation where you have 18 of your POLARIS on station waiting for the signal to fire. Somehow, somewhere, in some way the enemy has cut your communications with the 18. You don't know about it and the submarines don't know about it. You give the order with the red button and nothing happens.
>
> (Discussion with Admiral Galantin Deleted)
>
> Then the situation I pose is most unlikely within the rule of reason?
>
> (ADMIRAL GALANTIN) That is right.
>
> (MR. FLOOD) Then there is a point and time under certain circumstances in which the ship commander is authorized to open up?
>
> (ADMIRAL GALANTIN) Yes sir.
>
> (MR. FLOOD) There never has been the need to exercise that right? The need has never occurred.
>
> (ADMIRAL GALANTIN) That is right. [47]

This hoary testimony may be quite misleading. However, we can be reasonably sure that military commanders at relatively low echelons in the missile submarine command hierarchy operated with the knowledge that their links with higher authority were tenuous indeed, and that retaliation might have to be executed without the personal command of their civilian or military superiors.

Bomber Vulnerability and Additional LCC Vulnerabilities

By 1966 SAC had made considerably more progress than the Navy had made toward establishing a viable command channel for controlling its strategic forces. SAC operated a ground network with an airborne backup that provided a degree of genuine redundancy and survivability. Under the principle of conservative planning, Soviet calculations may have estimated that the overall system, in spite of its many deficiencies, was sufficiently robust that execution messages could have been delivered to large segments of SAC's forces with high probability. But by the same token, U.S. planners had cause for serious concern about its performance in a nuclear environment.

Cautious planners on both sides could have quickly concluded that even small-scale attacks would neutralize the ground network. Individual ground-based command centers and communications lines had little chance of surviving the blast effects of direct nuclear attack, and too little redundancy (except for LCC redundancy) existed to offset this vulnerability. And there was a critical node in the network. As mentioned earlier, authorization of nuclear strikes would have been passed from the NCA to the specified commander, who in turn would have relayed the message (after translating it into SAC message formats) to the executing forces. Thus, the destruction of SAC Headquarters in Omaha would have severely degraded the performance of the ground segment. And destruction was likely if the headquarters had been directly attacked. This nodal command center was underground but "not in any secure way," as Former Secretary McNamara once put it. [48]

Assuming that SAC Headquarters survived, the "go-code" authorizing strategic attack would have been simultaneously transmitted over several ground-based media to subordinate units. These media included the Primary Alerting System (PAS); a teletype channel known as the SAC Automated Command and Control System (SACCS); and leased commercial land line communications, particularly AUTOVON/AUTODIN. All these media except for PAS utilized surface terrestrial lines and were liable to suffer severe degradation even from collateral damage. PAS featured modest protection from blast effects, and thus may have withstood collateral effects. All systems lacked protection from EMP effects.

These lines went to the three Numbered Air Force Headquarters in the United States, Minuteman and Titan LCCs, wing command posts at primary SAC bomber bases, and other units at home and abroad. With the exception of LCCs, none were built to withstand nuclear attack.

The "soft" Numbered Air Force Headquarters located at Barksdale AFB, Louisiana, March AFB, California, and Westover AFB, Massachusetts, played a particularly important role in the exercise of positive control over SAC bombers in flight. Collocated with these bases as well as SAC Headquarters itself were HF radio antennas used for long-range radio communications with bombers which had launched and were en route to their targets.[49] This HF system was called "Short Order," and it was an integral part of an operation known as "positive control launch." Upon receipt of early warning of actual Soviet attack (tactical warning), or upon receipt of intelligence data indicating that Soviet attack was imminent (strategic warning), standard operating procedure called for bombers to launch (if not already airborne), fly to designated points outside enemy territory, loiter for a period of time, and then automatically return to their home bases unless they received an execution message. [50] "Short Order" was the primary means of delivering that message. But it was not able to withstand direct attack, was vulnerable to HF blackout, and was partially susceptible to enemy jamming.

A collection of ground radio stations (called "Green Pine" sites) located on an arc between Alaska's Aleutian Islands and Iceland augmented "Short Order." [51] Beyond the Green Pine arc, HF signals transmitted from stations in the United States were unreliable even in peacetime. The signals were also susceptible to interference from enemy jamming, and in a nuclear environment "Short Order" may have been blacked out completely. If an execution message could have been delivered to Green Pine sites, they in turn could have relayed it via ultra high frequency (UHF) radio to bombers en route to their positive control orbits. Assuming these back-up sites were not destroyed by Soviet attacks, they could have communicated to any bomber within line-of-sight range (approximately 200 miles) without risk of serious disruption from jamming or nuclear effects. Once the bombers had traversed the arc and flown out of UHF range, however, further communications would have become quite problematical. [52]

The central postattack problem, though, was reaching Green Pine sites in the first instance. In peacetime, SAC Headquarters and/or Numbered Air Force Headquarters could have sent the execution message over land lines and/or HF radio. But neither the communications media nor the originating command centers were survivable. Postattack communications with Green Pine sites would have been no less difficult than wartime communications with the bombers themselves.

Although the ground segment of SAC's command network would have disintegrated under attack and therefore could not have been employed to trigger retaliation by either bombers or ICBMs, it nonetheless served some important control functions, especially during the critical period between the launch and impact of enemy weapons. One of its prime purposes was rapid dissemination of orders from CINCSAC to launch ground alert bombers under the positive control policy outlined above. Getting bombers off the ground and a safe distance away from their home bases within minutes after detection of incoming warheads was essential to bomber survival. Given that tactical warning time could have been as short as fifteen minutes (detection to impact at northernmost CONUS bases), or shorter still if the performance of the Ballistic Missile Early Warning System (BMEWS) proved to be less than its theoretical optimum,[53] and given that bomber crews on day-to-day alert required about fifteen minutes from the time they received notice of the attack until the time they put a safe distance between themselves and their home base,[54] SAC could not afford even short delays in the implementation of a positive control launch.

CINCSAC was in the best position to expedite this procedure. Attack indications picked up by BMEWS sensors would have been sent to North American Air Defense (NORAD) Command Headquarters in Colorado, and promptly relayed from there to SAC Headquarters. A message directing a positive control launch would have originated in Omaha and traveled over PAS to wing command posts and other SAC units. Wing command posts at bomber bases would have then sounded a klaxon alarm, cueing the alert crews to scramble to their aircraft, and transmitted the message by radio to the aircraft, triggering the launch of the bomber force on a flight to predesignated points outside Soviet territory.

Another important function of the ground segment was generation of the airborne command system prior to the impact of incoming weapons. SAC maintained EC-135 command aircraft on 15-minute ground alert at its Numbered Air Force Headquarters and kept one EC-135, called "Looking Glass," on 24-hour airborne alert in the vicinity of Omaha. [55] "Looking Glass" served as the alternate command post for SAC Headquarters. SAC also deployed EC-135s with radio-relay missions to Lockbourne AFB, Ohio and Ellsworth AFB, South Dakota where they were maintained on 15-minute ground alert. [56] Upon detection of Soviet missile launches, EC-135 aircraft on ground alert would have been flushed into the air by means of the same communications channels used to launch the bomber force. Under established procedures for a positive control launch, EC-135s would have occupied predesignated airborne stations inside U.S. territory, forming a network similar to the present-day net depicted in Chapter 5 (Figure 5-6).

The Post Attack Command Control System (PACCS) employed UHF radio for line-of-sight communications with LCCs, wing command posts at bomber bases (from which alert bombers would have already been launched), and outbound bombers within UHF range. For long-range communications, HF radio was the primary (and sole) means. HF was the only direct link from PACCS aircraft to remote Green Pine sites and far-flung strategic bombers in flight, and there was substantial reliance on HF for communications between PACCS aircraft. (Note that the network depicted in Chapter 5 is rather compact and allows for UHF interconnection between all aircraft that are adjacent to each other. This tight UHF serial linkage resulted from a PACCS restructuring in 1970, when command aircraft at numbered air force headquarters were relocated to bases in the Midwest. In 1966, when key command aircraft were stationed in Massachusetts, California and Texas, PACCS was widely dispersed and consequently reliance on HF radio for intra-PACCS communications was much greater.)

Reliance on airborne HF radio systems for long-distance communications was a major liability. As discussed earlier, the adverse effects of nuclear explosions on radio signal propagation are severe at that wavelength. Furthermore, the transmitting power of airborne radios could not match the strength of a ground-based transmitter and hence could not perform as effectively if stressed by enemy jammers. Consequently, even without direct damage to PACCS, reliable communications with strategic bombers that were beyond UHF range (400 n.m.) could not be safely assumed by cautious U.S. planners, at least not for a nuclear environment. Nor could completely reliable communications among PACCS aircraft themselves be taken for granted. And for that matter, communications from PACCS to LCCs may have been quite difficult. Although EC-135s operated within UHF range of many Minuteman complexes, the best protected receive antenna at LCCs operated at the HF bandwidth, a much less reliable frequency compared to UHF.

In addition, PACCS aircraft were not immune to direct damage. There was some risk that alert aircraft would have been destroyed on the ground, perhaps as a result of sluggish tactical warning of ICBM attack, or perhaps as a consequence of undetected attacks by submarine missiles launched from waters contiguous to coastal EC-135 bases. Soviet _Golf_- and _Hotel_-class missile submarines which periodically patrolled the Eastern Atlantic in 1966 posed a potential threat to the command aircraft based in Massachusetts, for example. Sensors designed to detect submarine-launched ballistic missiles did not become operational until 1968.[57]

EMP effects produced by high altitude nuclear explosions probably posed a greater threat to PACCS, however. Aircraft exposure to EMP was virtually certain, and the resulting currents flowing through the plane could have reached very high levels. This problem is analyzed further in Chapter 5. Suffice it to say here that under conservative planning assumptions PACCS aircraft would have suffered significant damage from EMP effects.

In sum, Soviet attacks aimed at SAC's command structure would have greatly undermined positive control over bombers and ICBMs. SAC could have used the "soft" ground network to flush ground alert bombers and PACCs aircraft prior to the impact of incoming weapons (provided that tactical warning information arrived in time), but it relied on an airborne command network to deliver execution messages to the strategic forces in the wake of enemy attacks; and, the post attack capability of this network was questionable.

Failure of primary ground and airborne communications would have left SAC with one last-ditch means of strategic communications: the Emergency Rocket Communications System (ERCS). This system was comprised of Blue Scout sounding rockets deployed in a "soft" configuration on the Wallops Island just off the Virginia coast.[58] Prior to launch, an execution message could have been recorded on a tape device inside a missile. After launch, the message was to be transmitted over UHF by the missile's communications package. The idea was to exploit the altitude, range and velocity of a missile so that a message could be quickly disseminated over a large area using a radio frequency that nuclear explosions would only mildly and momentarily disturb. In principle, any SAC unit within line of sight of any portion of the missile's trajectory could have received the message. In practice, ERCS was a troubled system. It was not well integrated into any nuclear command hierarchy and technically it was a thin reed to lean on. Its reliability, transmitter power and survivability were such that cautious planners would not have counted on it at all.

Design improvements and better protection for ERCS deployments were in fact in store. Minuteman missiles would be equipped with communications packages and operationally deployed in silos in Missouri in 1967. [59]

All these deficiencies in SAC's command structure could only have aggravated the problem of negative control, especially in the case of LCCs. Isolation of bombers from higher authorities did not present quite as serious a problem. Established procedure required them to turn back in the event authorization to attack was not received. This guidance was unambiguous. Yet, it is likely that bombers, like LCCs and submarines, lacked physical safeguards against unauthorized retaliation. If safeguards were consistent across all three force components, then strategic bombers did not need to receive enabling codes from higher authority before weapons could be unlocked and armed. The public record, however, does not sustain any firm conclusions about negative control over bombers in the 1960s.

National Command Vulnerabilities

In 1966, national command authorities (NCA) had access to four primary command posts from which strategic operations could have been managed. Components of the National Military Command System (NMCS), they are listed below in ascending order of vulnerability to attack:

1. National Military Command Center (NMCC) located inside the Pentagon.

2. Alternate National Military Command Center (ANMCC) located near Fort Richie, Maryland, about 75 miles from Washington.
3. National Emergency Command Post Afloat (NECPA), a U.S. Navy cruiser deployed in the Eastern Atlantic near the coast.
4. National Emergency Airborne Command Post (NEACP), an EC-135 aircraft maintained on 15-minute ground alert at Andrews AFB, Maryland, just outside Washington.[60]

The NMCC, a soft facility connected to the White House Situation Room, obviously had no chance of surviving a nuclear attack directed against it. It could have been destroyed with no more than about 20 minutes advance notice if attacked by Soviet ICBMs. If attacked by submarine missiles, it may have been destroyed without warning.

The ANMCC had been in operation since 1953, a time when the Soviet nuclear threat consisted of atomic weapons delivered by bombers.[61] The underground facility has recently been rated as "moderately hard,"[62] which probably means that in the mid 1960s the structure itself stood a good chance of surviving missile submarine attack and a reasonably good chance of surviving ICBM attack. Backward extrapolation of information would also suggest that a small number of people manned the facility around the clock (with additional personnel on standby), and that constant communications between it and the NMCC were maintained.[63] Up-to-date data bases were kept by means of reports submitted by the NMCC, NORAD and other major commands.

Communications associated with both the ANMCC and the NMCC consisted of land line telephone and teletype systems interconnecting the facilities with the unified and specified commands among others.[64] A radio communications uplink to NEACP was also provided by the ANMCC.[65] Not surprisingly, all these links were exposed and vulnerable to attack. Former Secretary McNamara, testifying in 1963, stated that NMCC and ANMCC communications were "vulnerable in any practical sense."[66] Thus, survival of the ANMCC structure itself was a necessary but not sufficient condition for NCA direction of strategic forces. Its associated communications, too, must have survived.

The ANMCC was expected to survive longer, but not much longer, than the NMCC. The difference would probably have been measured in minutes or tens of minutes. Still, these were critical minutes during which time a transfer of control from the ground to NEACP could have been attempted. If tactical warning had been received and a decision to retaliate had been reached by the president, the ANMCC and associated communications may have survived long enough to convey the decision to NEACP. If the president or a successor were located at the ANMCC during the attack, he would have had more time to decide whether to order retaliation. If the president were aboard NEACP, the ANMCC may have survived long enough to relay early warning and other information being fed to the ANMCC from NORAD, SAC and other major commands. Without support from the ANMCC, the NEACP probably could not have obtained timely information about a Soviet nuclear attack. In all likelihood, NEACP would have depended upon PACCs aircraft for information about the attack, with SAC Headquarters relaying early warning information from NORAD to "Looking Glass," and "Looking Glass" relaying that information to NEACP via the PACCs network. Basically, the ANMCC performed a transition function. It was the primary and perhaps the sole means by which transfer of national control from the ground network to the airborne network could have been affected in an orderly and timely fashion.

The NECPA ship deployed in the Eastern Atlantic was less vulnerable to attack by virtue of its mobility. In 1966, however, the command ship was restricted to waters within troposcatter communications range of a single shore facility in Delaware.[67] This restriction probably put the NECPA at greater risk. More importantly, the shore facility could easily have been lost in the event of Soviet attack.

NEACP, the national command aircraft, had a better chance of surviving nuclear attack than any of the other national command posts did. McNamara had decided in 1961 to station EC-135 aircraft at Andrews AFB. Three were deployed in 1962.[68] One of the three stood on ground alert.

National officials had the option to board NEACP in time of crisis, but ground-based facilities were much more suitable locations to manage a crisis. They provided ample space for advisors; unlimited endurance; immediate and direct access to main communications and intelligence networks; greater capacity to handle larger amounts of data; and so forth. NEACP was ill-suited in all these respects.

Nevertheless, this option existed and if it were exercised well in advance of Soviet attack the chances of NCA survival would have been much improved.

NEACP survival was by no means assured, however, as Soviet planners were not lacking in strategies to attack aircraft in flight. One such strategy would have been based on EMP attack. A single high altitude explosion would have blanketed a large area of airspace and NEACP was almost certain to be within it. The aircraft's flight pattern was in fact likely to have been confined to a small area, where approximate coordinates probably could have been predicted with fair accuracy. Two requirements and a condition combined to impose sharp constraint on NEACP's flexibility. The first requirement was to maintain continuous communications with the ANMCC during the pre- and transattack period, so long as that were possible. The second requirement was to establish communications with adjacent aircraft in the PACCS network. The relevant condition was the limited communications range of the EC-135 aircraft model then in service. Until EC-135J aircraft replaced older models in 1968, NEACP's communications range allowed it to tie into only "one or two sole points on the ground."[69] This constraint and the requirement to be interconnected with PACCS aircraft narrowed the scope of NEACP's operational flexibility.

If national authorities chose to remain on the ground during a crisis, as seems likely, NEACP could have been launched and maintained on airborne alert for up to 10 hours (unrefueled). In the event of a sudden attack on Washington area command posts, NEACP's primary responsibility, if no execution message had been issued prior to the NCA's demise, would have been to contact a constitutionally defined successor and inject any orders from the new NCA into the PACCS network for dissemination to the nuclear forces. There was some chance that the initial attack would have been detected in time to permit the NCA to escape in helicopters, in which case it may have been possible to coordinate a rendezvous with NEACP at one of the many airstrips in the Washington area. [70]

An alternative posture would have NEACP on maximum ground alert, standing by to receive national officials and take off minutes before incoming ICBMs arrived. A helicopter flight from downtown Washington to Andrews would have taken perhaps eight minutes, and additional minutes would have elapsed before and after this flight. But BMEWS was expected to provide fifteen to twenty minutes warning (detection to impact), which may have been just enough time to permit the successful launch of NEACP with national officials on board. Also, during a period of tension, NEACP could have been relocated to any of several airstrips in the vicinity of Washington in order to confound Soviet intelligence and targeting. National authorities may have been able to rendezvous with NEACP and take off with more time to spare because of NEACP's covert deployment to a secret location. [71]

A ground alert posture nevertheless increased the risk of its destruction. A no-warning attack by missile submarines was not outside the realm of possibilities. BMEWS malfunction, NCA indecision, and a host of other causes of fatal delay -- fatal for both the NCA and the NEACP -- can also be imagined. Whether the added risk of a ground alert posture would actually have been taken, for the sake of keeping NEACP accessible to national authorities, is of course a moot question.

Under normal peacetime conditions, protection of the NCA would have been much more difficult. In the unlikely event of a "bolt-out-of-the-blue" surprise attack, national authorities would not have been in the best position either to escape the attack or ride it out. NEACP's chances of survival were doubtless better, if BMEWS performed at its theoretical optimum and if the aircraft had standing orders to launch without the NCA upon receipt of tactical warning. Still, the margin of error would have been narrow for an aircraft maintained on 15-minute ground alert. Under the best of circumstances (for a surprise attack) NEACP had only a few minutes to spare.

In sum, under the technical conditions of the mid 1960s, it was not possible to fully protect either the elected president or his successors from sudden attack, not even during an extreme national emergency when precautions to reduce vulnerability could have been taken. Protection of the communications required to exercise national control over strategic operations was even more difficult.

This situation once again raises questions about predelegation of authority and possible attendant problems of negative control. The issue of predelegation is succinctly stated in a report prepared by the Library of Congress:

> The realities of command and control in the nuclear age would seem to increase the necessity for prior

> delegation under certain carefully defined conditions. For example, in the event that the president were disabled in a surprise attack and his lawful successor were not immediately accessible, a contingency plan, containing a delegation of authority to order the use of nuclear weapons under certain conditions, would seem to be a logical and prudent precaution -- perhaps necessary to national survival.[72]

The president's right to delegate his authority to use nuclear weapons is unquestioned; however, it is open to question whether or not any president has ever done so. The report just cited states:

> Under existing law, the president alone has the basic authority to order the use of nuclear weapons. This authority, inherent in his constitutional role as Commander-in-Chief, may be delegated to subordinate officers in the chain of command virtually without limitation. Whether the president has, in fact, delegated the authority to use nuclear weapons under certain circumstances has not been ascertained.[73]

It has since been disclosed and officially confirmed that in one instance, at least, presidential authority has been delegated to a military command. In his prepared statement presented to a congressional subcommittee in 1976, a former senior military officer informed them that the NORAD Commander possessed such authority:

> ... I know of no instance where any U.S. or NATO field commander has been delegated authority to use U.S. nuclear weapons without express approval of the President of the United States, with one exception ... the North American Air Defense Commander, who has been delegated such authority only under severe restrictions and specific conditions of attack.[74]

Although the "specific conditions of attack" were not defined, the severe restrictions consisted mainly of a requirement that the NORAD Commander persist in trying to reach civilian authority until the last possible moment.[75] This requirement is reminiscent of procedures followed by isolated LCCs, which must have made every effort to get independent confirmation of the authenticity of an execution message in its possession. The situations are vastly different, however. The NORAD commander, unlike LCCs, could have initiated nuclear operations without ever having received an emergency action message from higher authority. LCCs must at least have possessed a message. Regarding missile submarines, the idea that communications silence might be broken in order to request authorization to release nuclear weapons or to confirm the authenticity of an execution message, was probably anathema. It was almost certainly proscribed.

The possibility that others besides the NORAD Commander operated under some formal guidance permitting them to initiate nuclear strikes without the personal command of the NCA is strongly suggested by the following colloquy. It took place during congressional hearings held in 1960. General Power, then CINCSAC, seems to be saying that he possessed conditional authority to unleash SAC's nuclear arsenal. While it is not very specific nor necessarily indicative of arrangements in the mid 1960s, the testimony seems germane:

> (MR. MAHON) You cannot tell where the President might be. He might be, at the time of a surprise attack, in South America, in Russia, in India, or he might be in some other place. Since you are the man who is charged with the responsibility of commanding the Strategic Air Command and launching

> our retaliatory force, has a system been worked out that would enable you to get going with your intercontinental ballistic missiles or your intermediate-range ballistic missiles of your airplanes?
>
> (GENERAL POWER) Yes, there is a very adequate system. But again, you have to go through and verify that you are actually under attack.
>
> In other words, no one is going to make that hasty a decision. It would not be right to do it. You might start a war accidentally, and you cannot afford to do that. Mind you, we are talking about a matter of minutes. Let us say you see, at its apogee, a missile coming over. This gives you 15 minutes' warning. You will not have to be particularly bright when those 15 minutes have passed to know if they are real missiles; they will be going off in this country. Therefore, we are talking about a very short time period.[76]

Predelegation of basic authority to order the use of nuclear weapons facilitates the exercise of positive control in the event of NCA incapacitation and hence weakens, presumably, motivation to attack the NCA in the first instance. Nevertheless, the destruction of the highest level of the command hierarchy would probably result in a considerable loss of attack coordination, an important aspect of positive control. Predelegation of basic authority does not remove all incentive to neutralize the NCA.

This assertion does not really contradict previous observations on the decentralized nature of attack coordination. Coordination does require detailed advance preparation of operational units, a process which unavoidably decentralizes many significant aspects of control. And the appropriateness of diffuse, preprogrammed rules and procedures does set an upper bound on the amount of coordination that is theoretically attainable. But central authority must be exercised in order for the theoretical optimum to be achieved.

Strategic planners labor under the assumption that central authorities would at least be able to designate an attack pattern and the exact time at which implementation of that attack would be set in motion. The target assignments and firing schedules of the established war plans are predicated on this major assumption, that is, that all strategic deployments would be operating under a common attack reference time and attack option. Strategic operations could not otherwise be integrated to achieve systematic and efficient coverage of the enemy target base.

Actors at the national level are in the best position to provide these simple but basic instructions. Their inability to do so would leave SAC units and SSBN units without a common frame of reference. As a consequence, some of the benefits of integration would be lost. By extension, the inability of the unified/specified commanders to provide such instructions to the forces under their respective jurisdictions would result in further degradation. And so forth. Coordination would clearly be minimal in the event individual strategic units were completely isolated from each other as well as higher authority. While extensive predelegation of basic authority to launch weapons would ensure retaliation, it would not by itself assure systematic coverage of the enemy target base.

It is possible that what has been called institutional ethos would act as an "invisible hand" which concerts the expectations and behavior of isolated units, resulting in far greater force coordination than random chance would ever suggest. By virtue of role playing in war games and exercises, indoctrination, familiarization with extant attack options, and even informal interaction within professional military circles, key actors may come to share assumptions about the course of action each is apt to pursue. We would venture to guess that in 1966, the standard "massive counterforce" option would have been seized upon by a large number of units and that attacks would have generally conformed to that plan in spite of the fact that such intentions and behaviors could not have been overtly communicated.

It is of course possible that contingency plans not only predelegated basic authority, but also specified rules for choosing an attack plan and execution time. Such instructions would have resolved much of the uncertainty that would have otherwise undermined positive control. At the same time, there are reasons to believe that specific instructions would not be endorsed by national policy officials. Resistance to elaborate qualification would be politically motivated: unambiguous instructions evade the effective power of the president.[77]

THE STRATEGIC SITUATION: 1966

The concerns raised in this chapter fell outside the scope of the established conception of the strategic problem, whose narrow compass directed attention to such issues as the emergent SS-9 ICBM threat to Minuteman silos. Most analyses focused narrowly on questions of force structure vulnerability, and the issues that came into prominence appeared to be few, understandable, and resolvable.

These appearances dissolve under a broader definition of strategic capability; and appropriately so, for while the narrower, simpler definition generated valuable technical comprehension of certain aspects of the situation, it excluded a dimension of central importance. As a consequence of this omission, the Soviet threat was misestimated and the policy conclusions derived from these miscalculations were unsound. Such, at any rate, is the upshot of this chapter.

U.S. Second-Strike Capabilities and the Overall Strategic Balance

Force structure and command structure analyses generate divergent assessments of the strategic balance. If the standard calculations are to be believed, a preemptive surprise attack by the Soviet Union would have been ineffective and self-disarming if directed against U.S. strategic forces. For this reason, and because a preemptive counterforce attack in the other direction could have destroyed a large fraction of the opponent's forces, the United States was generally believed to possess overwhelming strategic superiority. But analysis of the U.S. arrangements for exercising positive control over retaliatory forces alters this judgment. An attack strategy with a much higher expected payoff in terms of blunting U.S. retaliation would have been based on destruction of key command and communications nodes. The main objective would have been the isolation of strategic forces from central authorities, causing (1) loss of force coordination; (2) loss of ability to issue or receive execution orders; and (3) breakdown of the physical capability to launch ICBMs. Conservative planning assumptions leave little doubt, from both a U.S. and Soviet standpoint, that this strategy would have been far more effective than a strategy based on maximum attack on alert U.S. forces. And to conservative U.S. planners, this strategy ought to have been seen as a very serious threat. The strategy put U.S. capabilities for assured destruction at considerable risk.

In short, command structure analysis refutes the idea that during most of the sixties the balance of strategic power greatly favored the United States. These were not the halcyon days of American nuclear preponderance. It is hard to regard them so when the strategic organizations responsible for war conduct were liable to disintegrate under the weight of enemy attacks.

Crisis Stability

The above thoughts are not to suggest that the Soviet Union had an opportunity to strike with impunity. The destructive power of the U.S. force structure was immense, and conservative Soviet planners undoubtedly expected a fairly large fraction of it to be expended in the wake of a Soviet attack. In spite of the tenuous command and communications channels that stood behind the threat of retaliation carried by U.S. forces, Soviet confidence in their ability to paralyze the U.S. command structure and thereby remove the threat should not have been very high. The U.S. strategic posture surely acted as a powerful deterrent to attack.

Nevertheless, the situation during this historical period was less stable than was commonly believed. Standard calculations did not impart an adequate appreciation of Soviet incentives to strike quickly and preemptively against U.S. C^3I assets. The creaky condition of the command structure at least did not discourage the Soviets from taking the first aggressive actions in a crisis.

Nor did it reduce incentives for early utilization of U.S. forces. The difference between the effectiveness of an attack executed while the command structure was still coherent and an attack executed after absorbing the full weight of the opponent's strike would have been stark. In the second case, retaliation would have been much slower to develop, and the magnitude and coordination of the attack would have been markedly reduced. There was also a distinct possibility of unauthorized strikes by isolated forces. It is not unreasonable to suppose that national policy officials would have preferred to authorize attacks early, if they sensed a growing loss of control and if further delay risked a loss of influence over the attack option finally implemented.

Force Components and Strategic Stability

Most analysts equate the vulnerability of each force component to its contribution to strategic stability. Alert missile submarines were estimated to be invulnerable to attack, and hence their deployment was viewed as a stabilizing factor. Silo-based ICBms were determined to be somewhat more vulnerable, and in light of the technical trend running against them which was fully appreciated, ICBMs ranked below submarines as well as bombers. They were the least stable component of the force structure. Bombers occupied an intermediate position in this rank order. Alert bomber deployments were less stabilizing than submarine deployments were, but more so than ICBM deployments.

A reversal of this order results when the components are differentiated with respect to the viability of their C^3 systems. In 1966, missile submarines were the least manageable component, both before and after a Soviet attack, especially an attack aimed at the U.S. command network. Prestrike and postattack control of ICBMs were good by comparison, and better than bombers, too. Bombers compared favorably to missile submarines, thus retaining their intermediate position in this rank order.

ICBMS and Command Stability: In 1966, a command network with modest redundancy connected land missile complexes with central decisionmakers. No individual ground element -- communications link or command node -- could have been expected to survive a direct nuclear attack. However, the ground segment provided a timely, reliable and two-way interconnection in peacetime and in the prestrike phase of conflict; and, the airborne segment, though dependent upon the prestrike performance of the ground network (including early warning facilities) had some chance of establishing a line of communications to many of SAC's dispersed strategic forces. During peacetime and periods of high international tension, the ground structure kept the ICBM force in harness, under firm authoritative direction. Direct and instantaneous transmission of directives was possible, and each element in the chain of ICBM command could acknowledge receipt of such messages almost instantly. Direct land line communications also enabled SAC Headquarters to monitor ICBM alert status on a near real-time basis. Thus if, for instance, a certain missile aimed at a high priority target went off alert for maintenance, SAC could and did authorize coverage of that target by another missile. Once completed, SAC received immediate notification of the retargeting, as did higher authorities including the NMCC and ANMCC.

Land lines lessened, and basically eliminated, reliance on radio communications. When radios were employed, security did not prohibit two-way communications. Security precautions in general were not stringent and encumbering. Also, transmitters and receive antennas were confined within the continental United States, where atmospheric conditions play less havoc on signal propagation than is the case at higher latitudes. Problems of signal propagation yielded to simple instructions to change frequencies, and this was often coordinated over the telephone. The launch control centers did not move, and as a result the orientation of antennas with respect to ground-based transmitters remained constant and optimal. The relatively close proximity of radio transmitters and receivers made communications less susceptible to deliberate interference from jamming, and unless land lines were attacked as well, the resulting degradation of command would not have been serious. Fixed locations, access to supplies, and the availability of maintenance personnel facilitated, under normal circumstances, the repair of land line and radio communications systems. Interested parties could be quickly notified of a problem affecting any portion of the communications system, and work to correct serious malfunctions could proceed on a priority basis. Under combat conditions, the prompt restoration of ground-based communications would have been unlikely, but the prospects would have been far worse if the system terminated at imprecisely known, inaccessible locations.

After a large nuclear attack on the American command structure, control of ICBMs depended heavily on the functioning of SAC's airborne command network, which in many respects did not measure up to very high standards. Individual aircraft lacked adequate protection from EMP effects. Communications range, particularly in a nuclear environment, was too limited. Aircraft were subject to inherent limits on endurance (10 hours unrefueled maximum). BMEWs warning time was barely enough to ensure their prelaunch survival. The survival and smooth interaction of a network of such aircraft was questionable.

Still, PACCs did provide a redundant link to ICBMs which was far more survivable and coherent than the ground- and ship-based network used to control missile submarines. The destruction of SAC

Headquarters and other subordinate SAC command units on the ground would not have isolated SAC forces as readily as attacks on the unified commands would have isolated missile submarines from higher authority. Continuity of command over SSBNs would have probably been lost in the event that the Navy's ground elements had been attacked.

Missile Submarines and Command Stability: Although this component was on balance worse than bombers and ICBMs in terms of both pre- and postattack control, it possessed one particularly important advantage over ICBMs: the invulnerability of its communications gear, launch mechanisms and crew. As discussed earlier, the Soviets could have targeted every LCC in the Minuteman force. Missile submarines were virtually immune to analogous attempts at decapitation. The favorable comparisons end there, however.

During peacetime, as a security precaution no one except for the submarine crew itself knew the exact location of missile submarines on patrol.[78] (The submarine commander drew up his 68-day patrol plans after leaving port.)[79] Once deployed, radio silence was strictly observed. A sub never engaged in two-way communications with higher authorities, except when it could not perform its primary mission, lest intercepted signals and direction finding compromise location. Ordinarily, then, higher authorities could not monitor the status of the submarine.

Missile submarines could receive communications during routine patrols but not without some difficulty. One reason for this was that the primary means of communications -- fixed VLF shore stations --

frequently encountered adverse atmospheric conditions. Submarine reception was especially variable in the North Atlantic and the Mediterranean. Reception also depended on the trailing antenna's orientation with respect to shore-based transmitters. Fluctuations could result from changes in a submarine's heading. [80] On the technical side, it should be noted that the signal processing equipment in missile submarines left room for substantial improvement, and that underpowered shore-based back-up transmitters aggravated the problem. In general, as one official put it, missile subs monitor radio signals with the precision of an electrocardio machine, and circumstances varying from changes in signal pulse strength to interference from fishing nets may require "urgent excursion to shallow depths to regain communications." [81]

Given the total dependence on radio, routine maintenance or mechanical difficulties reduced the responsiveness of submarines, while similar problems had slight effect on the responsiveness of SAC forces. This was true for malfunctions at both ends of the communications channel. At the transmitting end, equipment downtime interrupted the flow of information from higher authorities. At the other end, problems such as the loss of towed buoys (they sometimes snapped) interrupted reception. And communications malfunctions at the receiving end had to be repaired without outside assistance or supplies, which in practice meant that some repair work had to await the return to port.

During peacetime, many missile submarines at sea were exempt from a national requirement to maintain 24-hour communications reception. Submarines in transit, for example, followed "modified" alert procedures which called for periodic, not continuous, reception of messages broadcast from shore.[82] These submarines often operated at depths and speed that were not conducive to signal reception using trailing antennas at or near the ocean's surface. Only periodically would a missile submarine in transit slow down, float a wire antenna and monitor broadcasts from shore.

An intense international crisis would have tended to magnify such command and communications problems. For instance, the surging of port-bound missile submarines to protect them from Soviet preemptive attack and to bring them within striking range of Soviet targets would have substantially increased the number of submarines in transit. As a result, a large number of submarines would not have been in the best position to receive messages from higher authorities on a continuous basis, nor would these authorities have known the location and status of an unusually high number of missile submarines. In the absence of two-way communications, central decisionmakers could not have determined which submarines had arrived on station; which were prepared to fire; which had received the latest emergency action and intelligence information; which were experiencing problems with communications; or which were engaged in tactical interaction with Soviet ASW forces, the chances of which were likely to be considerably higher than normal under conditions of increased levels of military activities on both sides. In the event of detection, harassment, or attack, the submarine commander's main responsibility was to elude Soviet forces, using force if necessary. All the while, a missile submarine could not have informed higher authorities of the incident, nor awaited instructions on course of action. Indeed, the trailing of communications wire or buoy antennas would have been impractical while the submarine undertook evasive action, which took precedence over the national requirement for missile submarines to maintain continuous reception. Interruption of reception was both necessary and permissable under such circumstances. [83]

By all indications, arrangements for post attack control were in disarray. The ground segment provided a precarious link, and an embryonic airborne segment had not yet achieved significant operational capability. [84] The Navy had not deployed anything that satisfied even minimal requirements for post attack control of the undersea deterrent. With small but concentrated effort the Soviets could have isolated the entire force from higher authorities.

This state of affairs was not acknowledged at the time. The official assessment of the situation was in fact reassuring. Many claimed that the "sheer multiplicity" of survivable radio stations at sea and on land compensated for the vulnerability of primary shore-based elements. This confidence was unwarranted, however. Data from recent Navy experiments relevant to realistic wartime conditions have demonstrated that it is no simple matter to sustain a chain reaction which successfully relays messages through an ancillary network to submarines. Preplanning, practice and tuning of organizational procedure are prerequisites, and none of this had been done during the sixties. Furthermore, several episodes of crisis management during the late 1960s raised serious doubts about the performance of undamaged naval communications networks. These episodes were empirical embarrassment to the theories expounded just a few years earlier. In hindsight, it is apparent that the official position was mere bald assertion. What potential redundancy that did exist in the "total naval communications system" could not have been brought to development spontaneously, as the need arose in wartime.

Strategic Bombers and Command Stability: Strategic bombers on ground alert were like ICBMs in terms of command stability, while bombers on airborne alert were more like missile submarines. The bomber's contribution to command stability therefore ranked somewhere between the other components.

In peacetime, bombers stationed at primary SAC bases remained under the firm control of higher military authorities. SAC knew their exact location at all times, and monitored their readiness by means of SACCS reports submitted by local wing command posts. [85] Established procedures allowed bomber readiness to be stepped up in a timely and orderly fashion, though not without some degradation of control during and after major transitions such as the dispersal of bombers from primary to secondary bases. (Such dispersion reduced the vulnerability of the force). PAS provided a direct, reliable link to send alert messages out and accept returning acknowledgements. (But SACCS and PAS did not extend to many of the dispersal bases.)

A very substantial degradation of control would have accompanied a positive control launch. Bombers would have no longer been directly plugged into land line communications networks, and their ability to receive instructions would have steadily decreased as they put more and more distance between themselves and SAC radio stations. At some point in their flight toward the Soviet Union, all communications with the force would have been lost.[86] At the same time, the risks of tactical interaction with opposing forces would have increased as bombers flew farther away from home bases, and the bomber force's opportunities to engage in two-way communications with higher authorities without compromising its position and survival prospects would have diminished. At some point, presumably, restrictions on the freedom of bombers to acknowledge receipt of the "go-code" would have been severe.

Preemptive Soviet attacks on fixed command centers and communications channels would of course have compounded these problems. In all likelihood, the PACCS network would have assumed primary responsibility for the control of strategic bomber operations but it would have been hard-pressed indeed to fulfill this responsibility. PACCS itself was not invulnerable to attack and even an intact network would have reached only a fraction of the far-flung bomber force via radio communications. The chances of reaching them by means of emergency communications rockets were even more remote.

Negative Control

Our analysis of command structure performance may not have answered very many questions about the negative side of the control problem, but questions have at least been raised. Standard analyses completely ignore the topic.

Insight into the problem of negative control begins with an appreciation of its close relationship to the problem of positive control. Physical and organizational arrangements serve both priorities, but a physical condition — namely, vulnerability to attack — creates a trade-off between them which probably cannot be resolved without altering the American form of government.

Since under the technical conditions of the mid 1960s full protection of both the president and the physical means by which he would have exercised positive control could not be provided, absolute negative control could not have been achieved without risking neutralization of the entire strategic arsenal by a sudden attack on Washington and the NCA. To prevent this from happening, or better to dispel any Soviet notion that it could happen, strategic organizations possessed the physical capability and very likely some form of conditional authority to employ nuclear weapons without the personal command of the president or his successors as defined by the Constitution.

Despite unusual secrecy, open and credible sources give some general idea of the circumstances in which such attacks would have been launched. Past testimony, cited earlier, indicates that in the early

1960s strategic operations might have been undertaken under conditions ranging from communications blackout to verification of nuclear explosions within U.S. territory.

This testimony suggests that procedures for executing forces without the personal participation and approval of national officials had been spelled out clearly. As a matter of principle, precise guidance would seem necessary to ensure proper and smooth devolution. Ambiguous definitions of the actors, the permissable actions, the circumstances involved, and so forth would have invited confusion.

However, another, more important principle was at stake: the authority of the president. Unambiguous definitions would have eroded the effective power of the president, and the farther such definitions had been developed, the more troublesome their political implications would have become. Consequently, the unified and specified commanders probably operated under significant ambiguity of authority. [87] Carrying the logic a step farther, if the vulnerability of the unified and specified commanders was significant, then strategic units at even lower echelons of the command hierarchy would have operated under similar assumptions, that is, strategic operations might have to be undertaken without the personal command of either the president <u>or</u> their immediate military superiors. Relative to the national command system, the vulnerability of the unified/specified commands was less by virtue of greater numbers, dispersion, mobility and readiness. But even so the commanders at this level had not been provided protection comparable to that afforded subordinate units, especially commanders of individual bomber, submarine and ICBM units. It seems reasonable to suppose, therefore, that ambiguity of authority permeated the military command hierarchy from top to bottom. Formal, unambiguous guidance at the bottom would have so thoroughly compromised the effective power of national leaders that we must expect ambiguity to have prevailed.

A condition of ambiguous authority is not without paradox, however. It does avoid troublesome political implications. And it may preserve the effective power of the president during communications outages of significant duration. But at some point clear definitions and precise guidance may preserve it better. Actors presumably do not have an unlimited tolerance of uncertainty. We cannot realistically expect ambiguity of authority to be endured with aplomb for an indefinite period.

How might the uncertainty be resolved in the absence of formal guidance? What has been called institutional ethos would arguably have the most systematic effect on behavior. Although it is a very difficult thing to get a handle on, there is reason to suppose that it can exert powerful influence on the way in which national policy and military operations interact during crises. It may well be the key determinant of the behavior of American forces in wartime circumstances where ambiguity of authority is salient. We would expect subordinate actors to eventually assert control and pursue a course of action leading to less than fully coordinated execution of strategic forces.

Reliance on Tactical Warning

Analysis of organizational performance brings a key feature of the strategic situation into high relief: the command structure that stood behind the triad of force components could not have absorbed the full weight of a Soviet nuclear attack without timely advance warning and fast reaction. This point is stressed because mainstream strategic analysis downplays the contribution of early warning to strategic capabilities.

To be sure, standard calculations of bomber vulnerability include assumptions about tactical warning. Nonetheless, calculations of the overall strategic strength of the United States leave a wrongful impression of the significance of early warning. The impression is that it became less important once the United States shifted from total reliance on bombers to reliance on a diversified portfolio, two components (ICBMs and missile submarines) of which seemed capable of riding out an all-out, surprise attack. In reality, tactical warning became indispensable because the United States failed to develop a strategic command network that could survive sudden attack without it. With the exception of "Looking Glass," no hedges against intelligence failure and early warning malfunction had been provided, as far as the command system was concerned. Instead, the United States staked its capacity for the control of nuclear retaliation on a system which employed ground alert aircraft and generated its capacity in anticipation of Soviet nuclear attack.

The highest echelon of the command hierarchy was not exceptional in this respect. In 1966, the national command post with the best chance of escaping attack unscathed was an EC-135 aircraft normally maintained on 15-minute ground alert near Washington. Survival of a national command entity was thus predicated, at least for many scenarios, on reliable and timely detection of incoming nuclear weapons. Without sufficient advance warning from BMEWS radar, the national command aircraft as well as all PACCS aircraft except for "Looking Glass" could have been caught on the ground and destroyed. The vulnerability of the two ground- and one ship-based national command posts meant that prompt notification of attack and immediate reaction by these command aircraft were essential for exercising even a rudimentary form of national positive control.

Policy Implications in Retrospect

The wisdom of U.S. strategic policy during the mid 1960s is called into question by the foregoing assessment. If the strategic situation in 1966 has been portrayed accurately, nuclear explosive energy was being deployed much faster than it was being harnessed for the national purposes it was intended to serve. The capacity of the United States to manufacture and deploy weapons outstripped its capacity to impose the organizational and physical controls needed to bring them and the threat of retaliation they carried under firm positive control in wartime.

To rectify this imbalance, the rate of strategic deployments should have been slowed, and marginal dollars in protective investment should have been channeled into the command structure. Missile submarines were the worst offenders in terms of command stability; their deployment should have been sharply curtailed, pending development of more viable arrangements for their control. Other areas of underinvestment doubtless included tactical warning, the performance of which largely determined whether then existing command channels would have been capable of triggering retaliation. And improvements in tactical warning notwithstanding, expenditures that reduced dependence of command channels on early warning would have represented a prudent investment.

That the strategic policy actually pursued at the time incurred high costs — in unwarranted confidence, misplaced emphasis, and unwise resource allocations -- is a judgment that enjoys the benefits of hindsight. In fairness to the consensus responsible for that policy, it must be recorded that many of the problems identified earlier as potentially severe threats to the strategic command network could not have been well appreciated at the time. For example, EMP damage caused by nuclear bursts in the exoatmosphere was a scientific surprise that yielded only slowly to scientific explanation. That no part of the command structure had been deliberately designed to withstand EMP exposure was an unavoidable accident of history. Similarly, the performance of strategic organizations turned on those small procedural details discussed in general terms in Chapter 3 and illustrated in this chapter. They defied comprehension because of the complexity of their interaction. Full comprehension of the consequences of the programmatic decision process in strategic organizations was in fact beyond reach. It still is.

Regardless of the store of available knowledge, a sharp shift in strategic priorities could not have been effected. The policy commitment to large-scale deployments of ICBMs and missile submarines, made at the expense of C^3I, could not have been replaced by a commitment to a program reflecting balanced priorities unless the machinery to manage such a program existed or could have been instituted quickly. As discussed in Chapter 3, the machinery did not exist. Management of C^3I programs was decentralized, diffuse, fragmented. And the prospects of bringing the relevant programs under any headstrong, corporate direction must have been too remote to warrant the attempt. In any case, the amount of time required to institute the necessary machinery probably would have been measured in years.

In spite of this institutional intractability, some significant C^3I programs were initiated during the early 1960s and several came to fruition during the decade. It would be remiss not to acknowledge that quite innovative solutions to certain problems were found and applied. Though it was not treated as a prime concern, the strategic command problem certainly was not shrugged off as one of minor significance.

The extenuating and mitigating circumstances that can be invoked in defense of a rather ill-conceived policy during the initial period of strategic deployments cannot be carried over to succeeding periods, however. In hindsight, it is clear that the United States had embarked on a fixed course. Too few paused to review what had come to pass. There was a further general retreat into the abstract and mechanistic world of standard strategic enumeration, a world where it was almost axiomatic that strategic capabilities turned on the size and technical composition of the respective force structures, even though that same view of the world had created a policy that left glaring deficiencies in the means by which strategic forces would be managed in wartime. Instead of correcting these deficiencies as well as the basic policy responsible for them, analysts anchored themselves even more firmly to the established conception of the strategic problem.

For the next fifteen years, standard calculations of force structure vulnerability would pose the questions, drive the analyses, and set the priorities. These calculations, we argue, became a substitute for more comprehensive thought and an anesthetic for analysts and decisionmakers who refused to confront the real problem -- namely, the inherent vulnerability of command networks -- posed by an opponent arming itself with thousands of strategic nuclear weapons.

Deterrence theory abetted this myopic embrace of statistical models of combat between opposing force structures. The perspective of deterrence theory saw nuclear weapons as instruments of pre- and intra-war diplomacy, a means by which to influence the opponent's decisions.

The idea that an attacker would strike an opponent's command structure -- the decisionmakers and decisionmaking apparatus -- ran against the grain of this perspective. Intellectual acceptance of the "diplomacy of violence" perspective, coupled with a tendency among Western strategists to attribute like attitudes and beliefs about war conduct to Soviet planners ("mirror-imaging"), made preservation of C^3I a sort of theoretical imperative. But such transference of Western reasoning rides roughshod over the preponderance of evidence suggesting that Soviet attack strategy has always been based on destruction of U.S. strategic command channels. And it begs the basic question whether preemptive attack on C^3I is ever a plausibly rational act. The theoretical imperative is really just bald presumption, a presumption that underlies the popular idea that a nuclear war might be won by militarily maneuvering oneself into a position of bargaining dominance. This idea, in turn, popularized statistical models of limited nuclear exchanges between opposing force structures.

For whatever reasons, the fact remains that U.S. strategic policy has only recently incorporated a broader conception of the strategic problem, a conception that is unrealized in practical terms. Those aspects of the strategic situation that were discussed in the preceding section are not peculiar to the particular period of history covered in this chapter. They were aspects of the situation in the 1970s, and 1980s, as well. The next chapter examines the general state of affairs in the early 1970s.

FOOTNOTES

1. Thomas C. Schelling, Arms and Influence (New Haven: Yale University Press, 1966), p. 214.

2. Ibid., pp. 212-13.

3. John D. Steinbruner, "Nuclear Decapitation," Foreign Policy, vol. 45 (Summer 1981-82), p. 19; and Desmond Ball, "Can Nuclear War Be Controlled?" Adelphi Papers, no. 169 (London: International Institute for Strategic Studies, 1981), pp. 44-45.

4. V.D. Sokolovskiy, Soviet Military Strength, Harriet Fast Scott, trans. and ed. (New York: Crane, Russak, 1975), p. 242.

5. Quoted in Joseph Douglas, Jr. and Amoretta Hoeber, Soviet Strategy for Nuclear War (Stanford: Hoover Institution Press, 1979), p. 36.

6. Ibid., p. 78.

7. Ibid.

8. Ibid., pp. 49-50.

9. Fritz W. Ermarth, "Contrasts in American and Soviet Strategic Thought," International Security, vol. 3, no. 2 (Fall 1978).

10. Statement of Gerald Dinneen, ASC^3I, U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1978, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 3, p. 639.

11. Statement of General A.D. Slay, Commander, Air Force Systems Command, U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th

Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 5, pp. 3799-800.

12. Statement of (Ret.) Admiral D.J. Murphy, Deputy Under Secretary of Defense for Policy, U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6439.

13. Statement of (Ret.) Admiral D.J. Murphy, U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 4, p. 483.

14. Harold Brown, "Our National Security Position," Speech delivered before the Council on Foreign Affairs, September 13, 1978, Vital Speeches, vol. 45 (October 15, 1978), p. 27.

15. Richard Burt, "Brown Says Soviets Long Sought Way to Knock Out U.S. Missiles," New York Times (May 31, 1979), p. A4.

16. Alain C. Enthoven and K. Wayne Smith, How Much Is Enough? Shaping the Defense Program 1961-1969 (New York: Harper and Row, 1971), pp. 166-67.

17. Ibid., p. 169.

18. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1964, 88th Congress, 1st Session (Washington, D.C.: GPO, 1963), Part 1, p. 407.

19. Ibid.

20. The theoretical "kill probability" of an SS-7 or SS-8 missile was 10 percent. Given the availability of 220 missiles of these two types, in 1966 the Soviets could have expected to destroy 22 American silos in a preemptive attack. In addition, the SS-9 missile force with a "kill probability" of 64 percent, and the SS-11 missile force with a "kill probability" of 8 percent, could have attacked 120 missile silos and destroyed 71 of them. Thus, the Soviet land missile force threatened only 10 percent of the American land missile force (93 silos out of 934 deployed).

21. A considerable distance -- at least three miles -- separates unmanned missile silos from manned launch control centers. Hardened underground cables, and in some instances radio links, connect launch control centers to missile silos.

22. Under the Minuteman program, ten LFs were deployed for every LCC deployed. 1,000 LFs and 100 LCCs were eventually constructed.

23. The estimated probability of LCC survival against nuclear blast effects ws approximately 15, 20, 24, 29 and 33 percent for a one-on-one attack by missiles with corresponding reliabilities of 95, 90, 85, 80 and 75 percent. Some estimates of LCC hardness range as high as 1,000 p.s.i., however, in which case an LCC had at least a fifty-fifty chance of survival.

24. Basic LCC configuration and operations have not changed much since their initial deployment. For recent descriptions that would be valid for the mid ʹ60s period (note: discussions of airborne launch control do not apply), see U.S. Congress, Senate, Committee on Armed

Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, pp. 6465-67; U.S. Congress, Senate, Committee on Armed Services, Military Posture and H.R. 10929, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 3, Book 1, p. 342; U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 10, pp. 6845-47.

25. Sample calculations of the derivation of results are given in Appendix B.

26. For further references and discussion of EMP, see Appendix C, this text; see, also, Samuel Glasstone and Philip J. Dolan, The Effects of Nuclear Weapons (Department of Defense and Department of Energy, 1977), chapter 11, pp. 514-540.

27. According to one source, a "typical high-level EMP pulse could have an intensity of 100,000 volts per meter," DNA EMP Awareness Course Notes (Chicago: I.I.T. Research Institute, September 1973), DNA 2772T, p. 1. Another source assigns a value of 100,000 volts per meter to a "representative" pulse, defined as a pulse that is above average in strength but is significantly less than worst-case. J.H. Marable, J.K. Baird, and D.B. Nelson, "Effects of Electromagnetic Pulse on a Power System," ORNL-4836 (Oak Ridge, Tenn.: Oak Ridge National Laboratory, December 1972), p. 12. Glasstone and Dolan state that the strength of the EMP would be 50 percent of the maximum peak field over most of the exposed area. Thus, if the expected maximum is 100,000

v/m, then most of the circled area in Figure 4-11 would receive 50,000 v/m. Glasstone and Dolan put the figure at "tens of kilovolts per meter." Glasstone and Dolan, The Effects of Nuclear Weapons, pp. 537-38. EMP studies generally assume, as a yardstick, that the Soviets detonate a one-megaton weapon at about 300,000 feet to produce a peak EMP field of 50,000 v/m. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 12604, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 2, p. 10781; and U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, 92nd Congress, 2nd Session (Washington, D.C.: GPO 1972), Part 3, p. 1945.

28. See Glasstone and Dolan, The Effects of Nuclear Weapons, pp. 517-19.

29. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6538.

30. DNA EMP Awareness Course Notes, p. 263. "EMP energy collection tends to be maximized within the HF band."

31. J.H. Marable, R. Barnes and D.B. Nelson, "Power System EMP Protection," ORNL-4958 (Oak Ridge, Tenn.: Oak Ridge National Laboratory, May 1975), p. 2.

32. DNA EMP Awareness Course Notes, p. 124.

33. Glasstone and Dolan, The Effects of Nuclear Weapons, p. 485.

34. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1977 Authorization for Military Procurement, Research and Development, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 6, p. 3906.

35. Senate Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, p. 6845, passim.

36. A specific example would be dialing in the wrong attack option into the LCC computer for transmission to LFs. See ibid., p. 6846, passim.

37. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1977, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 6, p. 47. Statement by Lt. General Paschall, DCA. Admiral Burke, questioned as to where Polaris submarines would get their firing orders in the event of general nuclear war, testified in 1961 that "Any submarine would get them from the unified commander." U.S. Congress, House, Committee on Armed Services, Military Posture Briefings, 87th Congress, 1st Session (Washington, D.C.: GPO, 1961), p. 967.

38. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1966, 89th Congress, 1st Session (Washington, D.C.: GPO, 1965), Part 2, p. 372.

39. Such facilities are "only as hard as a handgrenade or a single conventional weapon." U.S. Congress, Committee on Armed Services, Military Posture and H.R. 5068, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 3, Book 2, p. 1878.

40. VLF has always been the primary mode of communication to missile submarines. Using a high-powered transmitter, VLF signals propagate thousands of miles and still penetrate seawater down to about 30 feet. Reception permits (or better, requires, since VLF is the only operational means of underwater reception) a submarine to position an antenna within a few feet of the surface.

The propagation characteristics of VLF inspired the construction of strategically located VLF transmitters for use by the unified commanders, and the equipping of submarines with towed buoy and buoyant wire antennas for underwater reception (receive only). Construction was initiated in the late 1950s, with stations already in existence providing an interim capability until the better situated and higher powered transmitters became operational. Sites planned, operational or under construction during the mid 1960s were located at Cutler, Maine; Jim Creek, Washington; North West Cape, Australia; Hawaii; United Kingdom; Japan; and Balboa, Canal Zone. See U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1964, 88th Congress, 1st Session (Washington, D.C.: GPO, 1963), Part 5, pp. 819-20; "Navy Emphasis Swings Toward Strategic Command and Control," Armed Forces Management, vol. 15 (July 1969), pp. 62-64; "Navy: A Theory of Evolution," Armed Forces Management, vol. 16 (July 1970), pp.

4-42. The Cutler and North West Cape (later renamed Harold E. Holt) stations normally served virtually the entire globe, with remaining VLF sites providing backup. If the two main sites and back-up sites were lost, operational procedure required subs to monitor LF broadcasts (approximately 20 stations), and then HF broadcasts (30 stations) if all else had failed.

41. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1961, 86th Congress, 2nd Session (Washington, D.C.: GPO, 1960), Part 5, p. 359.

42. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1964, 88th Congress, 1st Session (Washington, D.C.: 1963), Part 1, p. 407.

43. The lack of antijam features in fixed VLF is noted by the then Deputy Assistant Chief of Naval Operations, in "Navy: A Theory of Evolution," p. 41. Mention of ongoing efforts to obtain adequate VLF antijam capability is found in U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1969, 90th Congress, 2nd Session (Washington, D.C.: GPO, 1968), p. 2150. The program name for these efforts is Verdin. Initial operational capability of Verdin was not achieved until the late 1970s. Power upgrading of the fixed VLF network was still underway as late as 1972. Senate Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, Part 5, p. 2834.

44. Interference with signals transmitted in these frequency regimes may last for hours. See Glasstone and Dolan, The Effects of Nuclear Weapons, pp. 482-486; Captain Michael A. King and Paul B. Fleming, "An Overview of the Effects of Nuclear Weapons on Communications Capabilities," Signal, vol. 34 (January 1980); and MX Missile Basing (Washington, D.C.: Office of Technology Assessment, September 1981), pp. 298-99.

45. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 3403.

46. This capacity is authoritatively confirmed in testimony given as early as 1960 and as late as 1976. See U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1961, 86th Congress, 2nd Session (Washington, D.C.: GPO, 1960), Part 5, p. 367; and U.S. Congress, House, Committee on International Relations, First Use of Nuclear Weapons: Preserving Responsible Control, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), p. 94.

47. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1964, 88th Congress, 1st Session (Washington, D.C.: GPO, 1963), Part 5, p. 817.

48. U.S. Congress, Senate, Committee on Armed Services, Military Procurement Authorization for Fiscal Year 1964, 88th Congress, 1st Session (Washington, D.C.: GPO, 1963), p. 56.

49. Development of Strategic Air Command 1946-1976 (Headquarters Strategic Air Command, March 21, 1976), p. 84. System characteristics described in Department of Defense Annual Report July 1959 to June 1960 (Washington, D.C.: GPO, 1961), p. 323-23.

50. Development of Strategic Air Command 1946-1976, p. 84.

51. Kenneth J. Stein, "Realtime Data Aid SAC Mission," Aviation Week and Space Technology, vol. 104 (May 10, 1976), p. 49. Authoritative references to the Greenpine network are few and far between. The closest thing to official acknowledgement of the existence of this network during the mid to late 1960s is the mention of "forward area UHF sites, which have as their purpose to communicate with the B-52 bombers." U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1970, 91st Congress, 1st Session (Washington, D.C.: GPO, 1969), Part 3, p. 1125.

52. A fairly recent assessment applies equally to earlier circumstances: "After the aircraft have passed beyond line of sight of our ground-based radios, we presently rely on high frequency communications to pass execution or recall orders to the bombers.... However, the high frequency radio has an availability of about 90 percent under benign conditions; worse than that over polar or aural [sic.] regions and can have extended outages under conditions of nuclear perturbation of the ionosphere." U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1977, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 6, pp. 82, 85.

53. "The BMEW's warning time is about 15 minutes, about half the transit time of an ICBM." U.S. Congress, Senate, Committee on Armed Services, Military Procurement Authorization, Fiscal Year 1966, 89th Congress, 1st Session (Washington, D.C.: GPO, 1965), p. 1158. An experimental complex of over-the-horizon, forward-scatter radars, designed to provide an additional ten minutes of warning, had been installed in Asia and Europe in December 1965, but the system did not become operational until 1968 (see discussion in Chapter 5).

54. "... we also have some 900 bombers, well dispersed, half of them on 15-minute alert and backed up by an improved warning system." U.S. Congress, Senate, Committee on Armed Services, Military Procurement Authorization, Fiscal Year 1966, p. 950.

55. Locations of EC-135 deployments are identified in Development of Strategic Air Command 1946-1976, pp. 84, 93, 102. The alert status of 15 minutes is author's estimate. For a Soviet view of the U.S. airborne command system, see Colonel V. Lebeder, "Control From the Air," Voyennay M, 6 (1967), pp. 79-84.

56. Development of Strategic Air Command 1946-1976, p. 123.

57. See Chapter 5.

58. Interview with Air Force Lt. Col.

59. See Chapter 5.

60. Entities enumerated in Library of Congress, United States Defense Policies in 1963, 88th Congress, 2nd Session (Washington, D.C.: GPO, 1964), House Document 335, p. 32. See also J.H. Wagner, "NMCS: The Command Backup to Counterforce," Armed Forces Management, vol. 9 (July 1963), pp. 23-25.

61. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6447.

62. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 5068, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 1, p. 1055.

63. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 12564, 93rd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 4, p. 3605; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6409.

64. Emergency voice communications traveled through the Joint Chiefs of Staff Alerting Network (JCSAN), and emergency teletype communications were transmitted through the Emergency Message Automatic Transmission System (EMATS). Wagner, "NMCS: The Command Backup to Counterfore," p. 24. See also U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 10929, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 3, Book 1, p. 308.

65. "NEACP obtains needed information and reports from the ANMCC via radio and ground communications links." U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1976, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), Part 1, p. 850.

66. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1964, 88th Congress, 1st Session (Washington, D.C.: GPO, 1963), Part 1, p. 407.

67. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1968, 90th Congress, 1st Session (Washington, D.C.: GPO, 1967), Part 5, p. 237-38; "Electronic Systems," DMS Market Intelligence Report (DMS Inc., September 1969), NMCS, p. 5.

68. Senate Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, Part 3, p. 1462.

69. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1968, 90th Congress, 1st Session (Washington, D.C.: GPO, 1967), Part 5, p. 238.

70. For recent discussions of this procedure, see U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 187.

71. Such an operation appears to be included in recent contingency plans. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1976, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), Part 2, p. 66.

72. Congressional Research Service, Library of Congress, Authority to Order the Use of Nuclear Weapons, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), pp. 3-4.

73. Ibid., p. 1.

74. House Committee on International Relations, First Use of Nuclear Weapons: Preserving Responsible Control, p. 55.

75. Ibid., p. 79.

76. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1961, 86th Congress, 2nd Session (Washington, D.C.: GPO, 1960), Part 7, p. 69.

77. John D. Steinbruner, "National Security and the Concept of Strategic Stability," Journal of Conflict Resolution, vol. 22 (September 1978), p. 419.

78. Senate Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, p. 6631.

79. Ibid.

80. A recent report notes that reliability problems have historically plagued the towed buoy antenna, and as a result SSBN commanding officers have generally employed the buoyant wire antenna which is bidirectional and thus cannot receive signals throughout a full 360 degrees. General Accounting Office, The Navy's Strategic Communications Systems -- Need for Management Attention and Decisionmaking, Unclassified Version, PSAD-79-48A (May 2, 1979), pp. 17, 37.

81. Senate Committee on Armed Services, Fiscal Year 1977 Authorization for Military Procurement, Research and Development, Part 12, p. 6821.

82. General Accounting Office, The Navy's Strategic Communications Systems, pp. 2-3.

83. Senate Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, p. 6734.

84. See discussion of "TACAMO" communications aircraft in Chapter 5.

85. SAC Automated Command and Control System (465 L). SACCs provided CINCSAC and the NMCC with an automated system for monitoring the status of all SAC forces. Terminals were located at SAC Headquarters, the three Numbered Air Force Headquarters, and all SAC bomber bases and missile LCCs within CONUS. SACCs became fully operational in 1965. It uses unprotected land lines to interconnect the terminals.

86. Senate Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, p. 6816.

87. The following passage develops a pertinent argument that also has historical relevance:

> A responsible president, for example, would presumably never determine in advance that a failure of communication between the White House and SAC lasting more than five minutes would automatically confer on the SAC commander full authority to take any military action deemed necessary. Such a rule would remove the president from the chain of command under so many imaginable circumstances, that even if it were to be stated in an apparently authoritative manner a judicious SAC commander would hardly believe it. Under many of these circumstances, a president with

> communications restored would clearly be expected to reassert control and would not appreciate aggressive, extensive exercising of power during the interim. An attempt at elaborate qualification could produce more credible rules of procedure; but it is precisely because increased credibility would increase the real effort on presidential power that the political implications would also become more difficult. As a consequence of this dilemma we must expect that modern strategic forces operate with the knowledge that there are conditions under which strategic operations might have to be undertaken despite ambiguous authority to do so.

Steinbruner, "National Security and the Concept of Strategic Stability," p. 419.

CHAPTER FIVE

COMMAND PERFORMANCE AND MASSIVE RETALIATION IN THE EARLY 1970s

> ...even if the Soviets attempt to match us in number of strategic missiles we shall continue to have, as far into the future as we can now discern, a very substantial qualitative lead and a distinct superiority in the numbers of deliverable weapons and the overall combat effectiveness of our strategic offensive forces.
>
> — Annual Defense Report for FY 1970 [1]

THE CONVENTIONAL VIEW: EARLY 1970s

The second half of the 1960s witnessed a dramatic surge in the number of Soviet strategic force deployments. But confidence in U.S. strategic capabilities remained high. In their annual reports, Defense Secretaries testified to the reliability and survivability of U.S. strategic forces, and asserted without reservation that the threat of retaliation carried by these forces could not be removed by preemptive attack. [2] Even extremely conservative assessments of second-strike capabilities during the early 1970s struck reassuring notes. P. Nitze, for example, applied worst-case assumptions and used a measure of capability (strategic vehicle "throw-weight") which biases calculations in favor of the Soviet Union, and still concluded that the United States enjoyed a margin of superiority. [3]

The conventions of strategic thought and analysis which produced these assurances also guided strategic force planning and formal arms negotiations. In the area of planning, primary emphasis was placed on measures that protected the offensive force structure from attack and bolstered its capability to penetrate enemy defenses. The emergent SS-9 ICBM threat in particular stimulated efforts to protect Minuteman missiles with extra layers of defense, both passive (silo hardening) and active (antiballistic missile, or ABM, deployments). Penetration of enemy defenses was enhanced by equipping the ICBM and SLBM forces with MIRVed payloads.

Conceptual and analytic conventions applied to force planning also spilled over into the SALT arena, where ABM defenses and SS-9 deployments became focal issues. The initial impetus to engage the Soviets in formal arms negotiations arose from small-scale Soviet ABM deployments which U.S. observers feared might lead to a nationwide system capable of shielding Soviet population and industry from counterattack by U.S. strategic missiles. Credible nationwide ABM defenses which removed the threat of U.S. retaliation to attack would be profoundly destabilizing, and so the U.S. delegation sought to constrain ABM deployments, even though large-scale ABM defense of Minuteman would have to be abandoned as a consequence.

Although the ABM treaty precluded any major effort to deploy active systems to defend Minuteman silos against SS-9 attacks, the aim of protecting Minuteman was pursued in negotiations devoted to offensive arms limitations. In fact, this goal was paramount. U.S.

negotiators were unyielding in their insistence upon an SS-9 sublimit of about 300 deployments, a sublimit which became the sine qua non of any comprehensive agreement to limit offensive systems. The sublimit was also a bone of contention until the eleventh hour of the two-year-long negotiations. J. Newhouse chronicles the drama of events surrounding the issue:

> As SALT recessed briefly for Christmas (December 1971), the Soviets were still balking at the sublimit, the Americans still pushing, but without much hope. A failure to get the sublimit was among the gloomiest of prospects. Signing a SALT agreement bereft of this, his highest priority, could have cost Nixon the support of the American military and perhaps other parts of the government as well. No one can say whether he'd have taken the risk. [4]

A DIVERGENT ASSESSMENT

Against this background, it was unusual for someone in D. Packard's position to be immersed in the management of strategic C^3I programs. While he was the Under Secretary of Defense from 1969 to 1972, Packard personally reviewed strategic C^3I capabilities, became a forceful advocate of C^3I modernization, and played an instrumental role in raising the priority of the airborne segment of the command system. Packard had come to believe that command and control was "the single most serious question that needed resolution within the Defense Department" [5] and that "the greatest requirement we have, the greatest shortage, was for improvement in our airborne command and control system." [6] He adjudged the program deserving the highest priority within DOD as a whole to be the development of a survivable airborne command post to replace the EC-135 aircraft used in NEACP and "Looking Glass" operations.[7]

The priority he assigned to the E-4 program reflected a deeper concern of his: the United States might not be able to respond at all to a Soviet nuclear attack because of weaknesses in post attack control over the strategic forces.[8] Variations on the theme of command vulnerability also filled pages of congressional hearings on defense supplemental requests submitted just after Packard's resignation. Then Secretary Laird, for example, citing serious deficiencies in strategic C^3 survivability and reliability, told Congress that C^3I was the "most vulnerable single element in our strategic deterrent," and that repair was a matter of extreme urgency.[9]

The particular command organization in existence in the early 1970s seemed almost designed to collapse under the weight of attack. Figure 5-1 lists and evaluates the primary ground-based command nodes and communications links relied on in 1971-72. As indicated, virtually all of the elements lacked adequate protection from one or more nuclear weapons effects. What's more, mutual dependence among the elements was such that the destruction of only a few critical nodes would have severely degraded the entire ground network. The airborne back-up network, though not as vulnerable as the ground network, was certainly far more vulnerable than the force structure. Also, the effectiveness of the airborne network depended critically on the performance of the ground-based network during the early phases of conflict.

STRATEGIC COMMAND STRUCTURE: ATTRIBUTES OF THE GROUND C^3 SEGMENT

	Vulnerabilities*											
	Total Number			EMP Effects			Blast Effects			Atmospheric Change Effects		
	L	M	H	L	M	H	L	M	H	L	M	H
Command Centers:												
National Military Command Center (NMCC)	x				x?				x			
Alternate NMCC	x				x?			x				
CINCSAC HQS	x				x?				x			
Numbered Air Force HQS	x				x?				x			
CINCLANT/CINCPAC HQS and Alternates	x				x?				x			
SAC Wing Command Posts		x			x?				x			
Launch Control Centers			x		x?			x				
North American Air Defense (NORAD) HQS	x				x?			x				
Communications:												
Land Lines and Switching Centers			x		x?				x			
Transoceanic Cables	x			x					x			
Navy Main Shore Terminals for Communications World-Wide	x				x?				x			
Navy LF/VLF Stations	x				x?				x		x	
Navy HF Stations		x			x?				x			x
SAC LF/VLF Stations	x				x?				x	x		
SAC HF Stations		x			x?				x			x
SAC UHF Green Pine Sites	x				x?				x	x		
SAC UHF Emergency Communications Rockets	x				x?			x			x	
DoD Satellite Control Centers	x				x?				x	x		
	L	M	H	L	M	H	L	M	H	L	M	H

*L = Low Vulnerability
M = Medium Vulnerability
H = High Vulnerability

Figure 5-1

One of Packard's last official acts was to issue a directive (DOD Directive 5100.30, December 1971), one of the aims of which was to reduce C^3I vulnerability through elimination of some critical nodes in the command structure. For instance it modified the chain of command for execution of the strategic war plan so that in principle national authorities could direct strategic units in the absence of the unified and specified commanders. The aim was not to eliminate intervening command nodes, but rather to create alternate paths that bypass such nodes in the event of their destruction. Some physical and organizational restructuring along the lines set forth in the directive occurred, but not until sometime after the time period covered in this chapter. The command network existing in the early 1970s included these critical command nodes and that fact would partially explain Packard's grim assessment of the situation.

Another patent deficiency in the strategic command structure had attracted Packard's attention. It concerned the MEECN network which was supposed to provide a last-ditch means by which the president could pass execution messages to the strategic forces during and after a nuclear attack. In reality, this "network" was merely a collection of ground and airborne communications elements that appeared to be the least susceptible to direct attack, jamming, or other adversities. These elements were mainly LF/VLF radio systems[10] being operated or developed to meet special mission requirements of the unified and specified commanders, not the requirements of the NCA. MEECN thus consisted of a very restricted set of subnetworks, which for technical reasons were not generally "interoperable." Basic incompatibilities existed between SAC and Navy VLF subnetworks, for example. An execution message that found its way into one of the Navy's VLF MEECN channels would not have been propagated outside this channel. SAC forces would not have received it.

To bring the purpose and the performance of the MEECN network into closer alignment, Packard expanded the scope of MEECN to include consideration of elements besides LF/VLF, and the Defense Communications Agency (DCA) and the Joint Chiefs of Staff were assigned responsibility for the program. During the early 1970s, however, MEECN remained a nominal system. After compiling a data base and identifying elements "that could be internetted to provide an initial survivable system (emphasis added),"[11] DCA forwarded, in December 1971, an initial set of recommendations to the Joint Chiefs of Staff and the Secretary of Defense.[12] Congressional testimony by the official responsible for the program best summarizes its status in 1972:

> ...we have made substantive progress in learning more about the network as it is, in defining some of its deficiencies, laying out a program that is aimed at improving some of these deficiencies, and in turn we have made some progress in laying out longer range program objectives and efforts.[13]

These remarks were made exactly ten years after McNamara's testimony, cited earlier, that the Defense Department had hardly begun to study the communications system on which U.S. retaliatory capabilities depended. The command-control implications of the missile age were scarcely any clearer in 1972 than they were a decade earlier.

Packard had also become concerned about the vulnerability of the command structure to EMP effects. This threat had not been confronted squarely even though theoretical breakthroughs achieved during the mid 1960s had given rise to some rather dire speculation. [14] Senator Goldwater recalls that toward the mid 1960s, during Senate hearings:

> ...the theory was discussed right here in this room that a (deleted) megaton device detonated (deleted) miles above Kansas City would destroy all of our communications ability for most of the United States. And it was generally conceded that that was true. And at that time I know that they started hardening the entire communications system. [15]

The speculation recounted by Senator Goldwater actually did <u>not</u> stimulate significant effort to harden communications. Contrary to his impression, protective investment went into individual offensive and defensive weapons. Between 1965 and 1972, research on command structure vulnerability to this esoteric phenomenon languished, and it was still languishing long after the force structure had been hardened.

A modest research effort to assess the EMP-vulnerability of general purpose communication systems had been started about 1969. [16] The research conducted through 1972 had produced results that many considered to be inconclusive. According to the director of DCA, tests run on some of the relays and switches of the AUTOVON system, for example, "did not prove conclusively that there would be damage to the system." [17] In another test conducted about 1970, DCA in effect wrapped an electronic cocoon around an entire AUTODIN switching center to simulate EMP attack. Temporary disablement lasting less than a minute resulted, but the findings once again suggested that the center would recover. Regarding such fleeting transients, the DCA spokesman remarked: "we just are not going to worry about it any more." [18]

Other observers questioned the validity of such findings, noting that the switch point, the building itself, is not the problem (though later tests of the switch point itself did uncover considerable vulnerability [19]). Conclusive results could only be obtained from tests of the total circuit consisting of the switch point and the hundred of miles of EMP "collectors" (the wires) that converge on the switch. [20] Furthermore, some observers challenged the position that there was no cause for concern unless test results proved conclusively that a problem existed. This position conflicted with the principle of conservative planning.

J. Northrop, Former Deputy Director of the Defense Nuclear Agency (DNA), viewed the situation from the perspective of a conservative planner. Testifying in 1972, he shed some light on the status of EMP research and the divisions of opinion that had affected progress to date:

> We have gone through a period of some years now in which our major strategic systems have indeed been hardened against this electromagnetic pulse threat. This is the Poseidon and the Minuteman, and our strategic defense systems Sprint and Spartan.
>
> Now, the one issue that we identified last year in our testimony that we were beginning to address, however, was the effect of the electromagnetic pulse on communications systems.... Programs to harden this system to the other nuclear effects of radiation blast, blackout, and fallout are available and present no unknowns in their solution. The EMP research has not progressed to

> the same status. This supplemental fund request is intended to provide the initial effort to evaluate the effects of threat level, high altitude EMP on elements of the C^3 systems, and will be the first step toward providing a C^3 system with balanced hardness....
>
> When we presented Dr. Foster and the staff last year the proposal that there should be, frankly, a major escalation in the funding level to attack this problem, it was basically a problem of whether we could prove the problem existed, whereas from our point of view the question was could we prove it did not exist.
>
> In our initial studies it was hoped that we could identify that the problem would not be a continuing one -- that is that the problem would go away. I think what has happened here is the final recognition that the problem appears to continue to be a potential hazard that must be addressed, and that our initial studies were not successful in making it go away.[21]

Among the studies that failed to make the hazard go away were laboratory tests that exposed small electronic components to a simulated EMP environment. Former Secretary Laird reported in 1972 that, "these (tests) are now far enough along to cause grave concern about the effects on all our electronics systems unless special protective measures are taken and verified."[22]

Regarding the ground segment of the command structure, virtually no significant measures would be taken to protect deployed elements, for several reasons. First, the cost of replacing old systems with systems designed to operate in EMP environments would have been prohibitive. That idea was never seriously proposed; it would have meant tearing out most of the then existing network and putting in an entirely new one. Second, protection of networks already in use could not be provided without a detailed assessment of the vulnerabilities peculiar to each, and in most cases such diagnoses were impractical. The types of experiments that a thorough assessment fairly well demanded entailed either atmospheric nuclear testing or the simulation of EMP fields over large areas. The former was banned by treaty. The latter was technologically infeasible. Many therefore concluded that the necessary level of technical comprehension of the vulnerabilities of operational networks was forever beyond reach. In this vein, the Defense Science Board concluded: "The effects of EMP on the enormously complex leased telephone circuits are not (and in our opinion, cannot be) understood well enough to assess with reasonable confidence the extent of their vulnerability to EMP." [23] Third, it is possible that the likely conclusions of a thorough assessment would have aided the opponent more than they would have the United States; some may have found in this risk a reason not to undertake the assessment. Fourth, it was generally believed that correctives would have carried a high price tag. It has been estimated, for example, that full protective shielding for certain types of facilities would cost over $100,000 per facility, [24] an expense the services would not want to bear. Lastly, and most importantly, direct attack using blast effects against existing ground facilities could have wreaked havoc in any case. Protection against EMP effects would not have removed that threat, and hence extensive EMP hardening generally appeared to be a rather dubious investment. Exceptions to the general rule included blast resistant Minuteman installations (LFs and LCCs). [25] Also, although massive reinvestment in EMP protection was never seriously entertained, EMP design protection would be built into certain programmed C^3I elements. This future investment would mitigate EMP vulnerability, but only slightly since critical systems such as the terrestrial communications linking the various elements would not be hardened against EMP effects.

It was apparently the vulnerability of the ground segment to direct attack -- the realization that its preservation or destruction had become a Soviet wartime prerogative -- which led Packard to examine carefully the airborne segment, it being the only alternative means of providing coherent direction to the strategic forces in the wake of Soviet nuclear attack. Examination of this channel impressed upon him the need for a major program to upgrade its capabilities. The command aircraft then deployed, and the network they constituted, inspired so little confidence that Packard embarked on a personal crusade to hasten the replacement of EC-135 aircraft with advanced E-4 airborne command posts. An unmistakable sense of urgency surrounded congressional hearings and other public discussions of airborne capability in general, and NEACP capability in particular. The EMP problem once again figured prominently in the discourse, and as we shall see, in the case of the airborne segment the problem was addressed in a serious way. Protection of national command aircraft against EMP was assigned high priority, and the attempt actually to provide the protection was more or less successful. Within the time frame covered in this chapter, however, the entire airborne network was exposed to nuclear attack using EMP effects and would continue to be exposed for many years to come.

A host of other reasons were given to justify replacement of EC-135 aircraft. The E-4 would provide additional space for national policy officials; extend the endurance of NEACP from 10 hours to 16 hours (unrefueled) or from 24 hours to 72 (refueled); expand the capacity to store and process data; increase the range and effectiveness of communications; and so forth. The overarching justification was simply that the United States had clearly staked its ability to control retaliation on an airborne system, and EC-135 aircraft just seemed pitifully outmoded.

The time had come to deploy a command aircraft that would have a reasonably good chance of actually carrying this burden. In the words of then Secretary Laird:

> The Advanced Airborne Command Post is an urgent program if we are to retain a credible and realistic deterrent in the future.... Our current airborne command system is severely deficient in survivability and capacity and cannot fulfill our essential needs in the event of nuclear attack on our country. It lacks the survivable secure communications needed for control and execution of the forces.[26]

Central Command Vulnerabilities: Reliance on Airborne Systems Grows

Simple extrapolation of the baseline conditions described in the previous chapter would give a reasonably good idea of conditions existing in the early 1970s. The situation was not static during this period (1966-73), though, and it is useful to review some of the changes that took place.

Circumstances in the early 1970s were in part the result of two prior internal decisions, both of which increased reliance on the airborne network to control U.S. strategic forces under post attack conditions. One of these decisions was made by the U.S. Navy in 1970. Discounting the national interests at stake, Navy officials terminated the NECPA program, which had been expanded during the late 1960s to include two ships and several shore-based troposcatter stations along the Eastern seaboard.[27] The decision, for which the Navy invoked fiscal austerity as justification, irritated many OSD officials concerned with NCA survivability. They took particular umbrage at the fact that they were not consulted in advance, and that the Navy scrapped NECPA while retaining all of its own command ships.[28] Nevertheless, the decision was allowed to stand. Under the decentralized budgetary procedures followed at the time, reversing the decision would have involved high level intervention and bureaucratic infighting that OSD officials did not care to instigate.

The second decision had to do with protective investment in fixed, ground-based command facilities. About the mid 1960s, McNamara advanced the principle of complementarity: neither a survivable airborne command post nor a survivable ground-based command post would by itself adequately serve the purpose of post attack C^3.[29] Contending that positive control required both types of arrangements, McNamara recommended construction of a deep underground center for SAC to back up its Omaha headquarters and complement its PACCS network.[30] Under the same principle, provision of like facilities for use by national officials would have been advisable, and it is likely that plans to build a subterranean shelter for the NCA were drawn up.

Had such plans gone forward, construction would have probably been completed by the early 1970s. The installation almost certainly would have become obsolete soon thereafter, but for awhile conservative Soviet planners probably would have concluded that the facilities could not be destroyed with high confidence. The plans were disapproved or shelved, though, leaving the NCA and other high level commanders without highly survivable command centers on the ground. The ANMCC provided some degree of protection, but not enough to warrant much confidence that the NCA would survive if located there. Under the principle of conservative planning, the ability of the ANMCC to survive attack appeared to be rather doubtful in 1966. By 1972, the considered technical judgment was not equivocal: "the facilities up near Ft. Richie could not withstand a determined missile attack."[31] A senior military officer best sizes up the situation as Packard and other members of the newly formed WWMCCS Council viewed it at the time:

> One of the items [Packard] considered lacking most was the capability of the National Command Authorities to control our strategic forces in a wartime or national emergency situation.[32]
>
> [Council] members were concerned about the eroding survivability of the underground command post [near Ft. Richie]. We could find ourselves in a position where it was impossible to guarantee the survivability of the National Command Authority.[33]

The obsolescence of the ANMCC was preordained by the Soviet commitment to deploy a large force of modern ICBMs by the end of the decade of the sixties. Its decline as a viable means of effecting an early and orderly transition from ground to airborne control of strategic force was also foreshadowed, but by a separate development: Soviet deployment of a new generation of missile submarines. By 1970, Yankee class submarines were operating on a regular basis in an area of the Atlantic Ocean within striking range of Washington and the ANMCC.[34] According to Defense Secretary Laird, testifying in 1972, these submarines, which were armed with more reliable, accurate and longer range missiles than their predecessors carried, rendered "Washington area" command-control facilities "rather vulnerable."[35] They added a new dimension to the vulnerability problem because of the short flight times of missiles launched at relatively close range, and because reliable, timely detection of submarine missile launches was problematic. These conditions heightened the risk that ground-based national command facilities such as the ANMCC would be destroyed or isolated before command and control could be transferred from ground centers to NEACP.

Yankee submarine deployments also created a new threat to NEACP itself. Since NEACP was routinely maintained on ground alert at Andrews AFB near Washington, a central question of NCA survival in the early 1970s was whether or not NEACP would be able to escape destruction by missiles launched from Yankee submarines deployed in the Western Atlantic. According to the Air Force, there was some chance that NEACP would be destroyed: "An SLBM 'launch without warning' attack could destroy NEACP aircraft at Andrews AFB when Red submarines are in close proximity to U.S. shores."[36] But, as the Air Force hastened to mention, there are circumstances in which NEACP might survive. Calculations of the prelaunch survivability of NEACP as well as other aircraft in the PACCS network are sensitive to a range of assumptions, particularly assumptions about the capabilities of tactical warning systems in operation then. We turn next to assess these capabilities.

SLBM Early Warning Capabilities: Prior to mid 1972, the United States was without any submarine missile detection system worthy of the name. The only operational system for detecting missiles launched from waters contiguous to the east and west Coasts of the United States consisted of seven height-finder radars deployed along the coasts and the Gulf of Mexico, augmented by a somewhat more advanced radar maintained on standby status at a station on the east coast. The basic group of seven sites employed antiquated "dish" radars originally designed and operated for defense against enemy aircraft.[37] Their range was inherently restricted by line of sight. For instance, a missile launched from 1,200 nautical miles at sea on a westerly trajectory would have reached an altitude of 200 miles before a radar could possibly have detected it. While the total flight time over this distance (1,200 nautical miles) would have been approximately fourteen minutes, the boost phase of flight during the climb to altitude, which the radar could not see, would have accounted for a large percentage of the fourteen minute total. More significantly, the radars could not generate sufficient power to achieve the maximum theoretical range allowed by earth curvature so that even a missile within line of sight could have escaped detection for a long time. The effective range of the radars was no greater than about 750 nautical miles, [38] and perhaps considerably less. That translates into a maximum warning time of about ten minutes.

Some warning time, furthermore, would be consumed by activities that intervened between initial sensor detection and aircrew reaction. Data flowed from the radar sites to NORAD Headquarters, which in turn sent notification to the ANMCC/NMCC and the unified/specified commanders, who in turn notified aircrews through local command posts.

Even if these intermediate steps took no time at all -- that is, aircrews are alerted the instant incoming missiles are detected by radar -- aircraft on ground alert at coastal locations still had virtually no chance of escape under surprise attack conditions and the odds were not very much better for aircraft on high alert in a crisis. In sum, the radar detection network did not supply the margin of safety needed to ensure command aircraft survival.

The successful launch of an early warning satellite on March 1, 1972, led quickly to a dramatic improvement in submarine missile detection. [39] This satellite was similar to one launched in 1971 and "parked" over the Indian Ocean at an altitude of 22,300 miles, where its sensors monitored Soviet ICBM missile launches in the Eastern Hemisphere. Because of the high altitude, geographic coverage of the

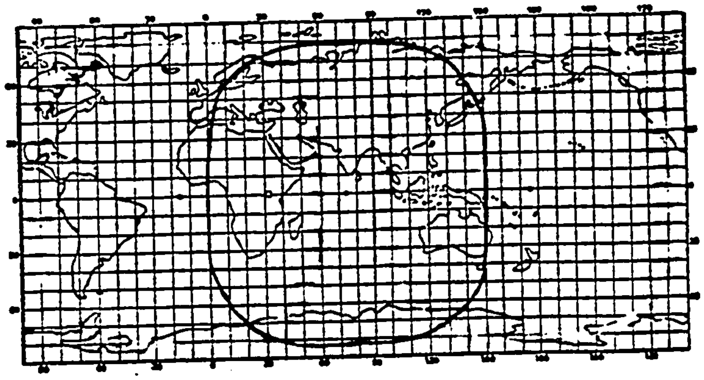
Eastern Hemisphere was extensive. Because of its geosynchronous orbit, the satellite was stationary with the earth. The area below was always the same. As Figure 5-2 shows, almost all of the Soviet Union, China and other potential missile launch and test areas came within view. This satellite thus complemented BMEWs as well as a foreign-based over-the-horizon (OTH) radar network that had become operational in 1968. [40]

The satellite launched in 1972 was positioned in a stationary orbit over Panama to monitor areas of the Atlantic, Pacific and Caribbean in which Yankee subs patrolled. (Figure 5-2 demarcates the area within continuous line of sight of the satellite.) It, like the satellite over the Indian Ocean, reportedly carried both thermal infrared and visible light detectors. [41] The infrared devices could sense the radiated energy of the hot plume of a submarine missile during its relatively slow climb to altitude. A missile may have been detectable within only a few tens of seconds after breakwater, depending on cloud conditions and several other factors discussed below. Upon initial detection, operators on the ground presumably would have switched on the visible light sensors in order to verify the suspected launch and track the flight path.

These early warning satellites have been credited with the capability to provide 30 minutes of advance warning of ICBM impact (compared to 25 minutes for OTH and 15-20 minutes for BMEWS) [42] and a manifold improvement in tactical warning in the event of missile submarine attack. Performance, however, was subject to a variety of technical and organizational constraints.

Early Warning Satellite Positioned Over Indian Ocean

(Maximum Coverage)*



Early Warning Satellite Positioned Over Panama

(Maximum Coverage)*

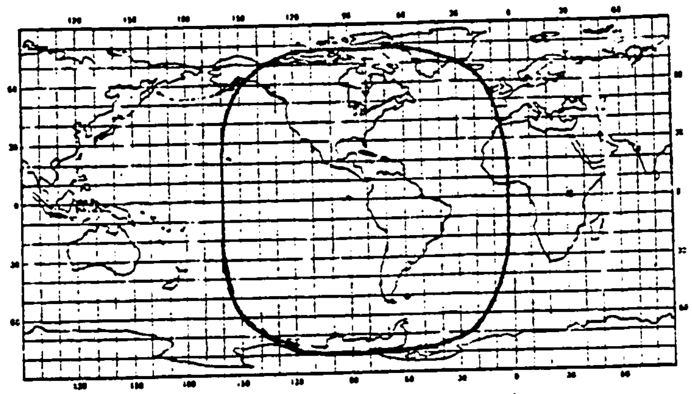
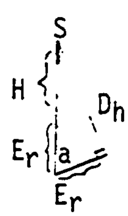


Figure 5-2



*Note: Line-of-sight limits coverage. Referring to diagram below, the distance to the horizon (D_h) for a satellite (S) at a given altitude (H) is equal to:

$$D_h = \sqrt{(E_r + H)^2 - (E_r)^2}$$

where E_r is the earth's radius (or @ 3,964 miles). Since $\sin a = D_h/(H+E_r)$, we can compute angle a in degrees using a table of trigonometric functions. In this example, H = 22,300; D_h = 25,963; sin a = .9885; and a = 81 degrees (as projected on above maps). Ground distance from center of circle to edges = a(69), or 5,589 miles.

Deeper examination of the technical details uncovers a range of deficiencies. For example, sun glint and glare from clouds and ocean surface occasionally triggered false alarms and created blind spots that degraded coverage in certain areas. [43] The time of these occurrences and the affected area were fairly predictable, as they tended to be correlated with seasonal changes. But solar outages are not desirable even if they are regular. The problem was not substantially alleviated until the launch of a companion satellite in 1973. The coverage of the two satellites extensively overlapped, but they were spaced far enough apart that blind spots normally would not coincide. If one satellite experienced solar or other problems, the other satellite could scan the trouble area from a different position and look angle. Yet false alarms continued to plague satellite surveillance. [44]

Unpredictable computer malfunctions and communications outages plagued satellite receiving stations on the ground. [45] Readout stations associated with ICBM and SLBM launch detection were sited near Woomera, Australia and at Buckley Airfield, Colorado, respectively. [46] Problems with the communications and data processing equipment at those locations evidently caused intermittent breakdowns in service as well as false alarms.

Another technical limitation concerns the instantaneous field of view of the satellite sensors. Figure 5-2 demarcates the total surface area within line-of-sight range of a particular satellite, not the specific area actually under surveillance at any given instant in time.

Only a minute fraction of the total area of possible surveillance, and only a small fraction of the area from which Soviet submarine missiles could strike U.S. territory, were being monitored at any moment in time. In other words, a satellite positioned over Panama could not have monitored both oceans simultaneously, nor could it have simultaneously monitored all possible launch points within any given body of water. For instance, a Yankee submarine SS-N-6 missile with a range of 1,300 nautical miles could have hit Washington from an area of the Atlantic roughly one million miles square. The satellite over Panama probably had less than one percent of this area in view at any instant in time.[47] Full coverage of the area required the satellite sensor to methodically scan portions of the surface, bringing a part of the ocean into view as another left it. There was some chance of a delay in detection, and probably some chance that an event of short duration would have been missed completely. Furthermore, repeated scans were required to in order to minimize the risk of false alarms.

The basic physical limitation imposed on range by earth curvature also proved to be a significant constraint on detection capability once the Soviets deployed Delta submarines armed with very long-range SS-N-8 missiles. SS-N-8 missiles were tested toward the end of 1972 and deployed operationally soon afterwards. With a range in excess of 4,300 nautical miles, the missile was easily capable of flying undetected over U.S. coastal radar,[48] and it could have been launched from points in the Pacific, North Sea, and Arctic regions that were beyond the line-of-sight range of early warning satellites in geosynchronous orbit.[49] Some parts of these regions were behind BMEWS and hence outside its area of coverage. A senior military officer testified in 1973 that the SS-N-8 posed a new threat to the U.S. strategic forces including land-based warning systems, command and control centers, and SAC bomber bases,[50] a view reinforced by the then Deputy Secretary of Defense who reportedly asserted in 1973 that, "all points in the continental United States are now subject to SLBM attack without warning."[51]

A final technical consideration is that the warning elements themselves were enormously exposed to nuclear attack. All the radar sites used in early warning were extremely vulnerable, and the communications that fed radar sensor data to NORAD Headquarters — the focal point of and critical node within the radar network — were not survivable. A granite mountain protected the underground operations center itself, but not the communications entering it, and even the underground center was unlikely to survive an attack directed against it. Regarding satellite early warning, the two readout stations were the least survivable components of the system.[52] The amount of protection afforded these facilities was practically nil. Finally, all of the long-haul terrestrial and undersea communications lines linking ground radar sensors and satellite readout stations with NORAD, SAC and national authorities were enormously exposed to direct attack using blast effects. They also were vulnerable to indirect attack using electromagnetic pulse effects.

These vulnerabilities undermined but did not necessarily preclude advance warning of an in-progress attack. Unless sabotaged in advance, major attack on the warning system would almost certainly have been detected by that same system. Furthermore, the inexplicable loss of particular warning sensors may have been interpreted as an indication, albeit ambiguous, that an attack was underway.[53] In short, prestrike alerting of aircraft on ground alert was not necessarily jeopardized by the vulnerability of the warning system. For purposes of estimating the prelaunch survivability of NEACP and other airborne command posts, this technical constraint on the performance of the warning system will be ignored.

Organizational arrangements for the dissemination of satellite warning data improved upon the scheme devised for BMEWS and the SLBM radar detection network. Data from the radar sensors were funneled into NORAD Headquarters before spreading out to other users. By contrast, operators at satellite readout sites transmitted data directly to SAC Headquarters, the NMCC and ANMCC as well as NORAD.[54] The Joint Chiefs of Staff had also included the unified commanders (for example CINCLANT, CINCPAC) among the units designated as users of satellite data,[55] but these commanders evidently received information via NORAD rather than directly from the readout stations.

Despite this attempt at streamlining the warning process, the network remained complex in that data still flowed through numerous communications channels and command nodes before reaching final destination points. The process continued to be organizationally elaborate in other respects. Optimal performance required, for example, a working relationship between the Navy and NORAD. The Navy's role: track Soviet submarines and report their location to NORAD. For operations involving sensors with limited range, field of view, and so forth, current information on known or suspected submarine locations would have been valuable both for purposes of sensor operation and data interpretation.

Such organizational details together with the technical constraints sketched earlier suggest that simplifying assumptions like "90 seconds elapse between missile breakwater and klaxon alarm at airbases" can be quite misleading. Such assumptions underlie most strategic analyses, for instance calculations of the prelaunch survivability of U.S. strategic bombers on ground alert.[56] We, too, resort to simplifying assumptions about tactical warning in order to assess the prelaunch vulnerability of NEACP. Our calculations and conclusions probably are optimistic.

In spite of the tendency to gloss over many aspects of tactical warning operations for the sake of quick and dirty calculation of the threat, few fail to appreciate the distinct possibility that overlooked or slighted details could have grave implications for wartime performance. For all the technological marvel of modern early warning satellites, conservative planners usually eschew, on principle, heavy reliance on any form of tactical warning. The opportunities for technical and organizational error are too numerous, and the allowable margin of error is just too slim. Provision of tactical warning clearly should not be a precondition for the success of strategic operations. Such, at any rate, is the basic position of a school of thought which has numerous adherents. Dependency on tactical warning for the generation of the retaliatory capability of the strategic bomber force thus became widely regarded as a major liability, while missile submarines and ICBMs won praise for being able to ride out attacks without prior warning.

This principle was not applied to command structure development. Tactical warning became indispensable. As well, strategic warning became increasingly important. The prelaunch survivability of NEACP and other command aircraft within striking range of Soviet missile submarines depended as much on anticipation of imminent Soviet attack and on knowledge of the movements of Soviet submarine deployments as it did on the performance of tactical warning networks. Even if systems dedicated to attack detection performed at their theoretical optimum, aircraft at normal alert readiness could not have coped with surprise attacks; normal aircraft reaction times were too slow. Prelaunch survival therefore depended on anticipation of possible enemy attack and correspondingly increased vigilance and alert readiness. Similarly, movements of submarines that brought them closer to U.S. air bases warranted precautionary U.S. responses, for instance an increase in the readiness of aircraft on ground alert, to compensate for the reduction in flight time of the submarine missiles.

This dynamic is partially captured by the calculations presented below. The calculations serve illustrative purposes only, and may not be completely relevant to realistic conditions, as it is hard to know what changes in the disposition of command aircraft were likely to be triggered by strategic warning indications, changes in submarine patrol patterns, and so forth. It is quite possible that the alert status of command aircraft was not geared, for example, to the disposition of Soviet missile submarines. The public record strongly suggests a preoccupation with the Soviet submarine threat to U.S. strategic bombers on ground alert. Because of the small scale of enemy deployments during peacetime, it was apparently concluded that they did not constitute a serious threat even when submarines moved from their usual patrol areas to positions near to U.S. coasts. Under this definition of the threat, however, the implications for the security of command aircraft would not be noticed.

Prelaunch Vulnerability of NEACP and Other Strategic Command Aircraft: Early 1970s: In one respect the calculations below are conservative. The analysis rests on the assumption that a significant risk existed if the probability of successful attack on ground alert aircraft exceeded ten percent. In other respects the estimates are optimistic because they are based on unusually favorable conditions that existed but for a brief time during the early 1970s. The conditions obtained in 1972. Before 1972, the prelaunch vulnerability of command aircraft including NEACP was almost certainly much greater. For one thing, warning satellites for detection of submarine attack had not yet been orbited. For another, key Post Attack Command Control System (PACCS) aircraft were deployed near the coast. (SAC did not begin to transfer command aircraft at Westover AFB, Massachusetts, for example, to inland bases until the middle of 1970). After 1972, SS-N-8 missiles launched from certain ocean areas may have avoided both radar and satellite detection.

Other assumptions used in the analysis work to inflate the chances of aircraft survival. First, submarine missile launches are detected without fail. Second, aircraft receive orders to take off only two minutes after missile breakwater. This is not only an optimistic view of the technical capabilities of the early warning system and the communications channels between sensors and the forces, but is also an optimistic view of the human decisionmaking process that leads to the issuance of takeoff instructions. Under normal circumstances, when negative control is the predominant priority of strategic organizations, the tendency to hesitate before ordering the launch of the airborne command network probably would be strong and hence slower reaction times would be expected. Even under crisis conditions, when the importance of positive control is paramount, activities devoted to attack verification and threat assessment would almost certainly have consumed several minutes more than our calculations assume. Third, blast is the only effect that can cause aircraft damage. Vulnerability to EMP attack is excluded, even though a strategy based partially on high altitude EMP attack could have been employed to reduce effective warning time (EMP instantly radiates 700 miles from the burst point) and exploit the vulnerability of aircraft that are exposed while still on the ground (currents induced in aircraft caught on the ground are estimated to be several times higher than those induced in flight). Similarly, we do not consider the possible effects of EMP damage to the ground-based communications circuits that carry sensor data to command centers and takeoff instructions to ground alert aircraft. (A threat postulated in recent years which could just have easily been proposed in the early 1970s imagines a submarine missile launched at close range and detonated at high altitude during the upward portion of the missile's trajectory, causing EMP pulses that disrupt ground-based C^3I channels only a few minutes after missile breakwater. The concern is that this precursor EMP attack would delay the launch of ground alert command aircraft long enough to permit follow-up Soviet SLBMs and perhaps ICBMs to inflict blast damage on those aircraft.)

Notwithstanding these optimistic assumptions, ground alert aircraft were acutely vulnerable to surprise attack. Enemy submarine missiles launched against EC-135 aircraft on day-to-day alert would have caught the aircraft on the ground and destroyed them by nuclear blast effects.

This acute prelaunch vulnerability stemmed from the simple fact that the flight time of attacking missiles was shorter than the reaction time of aircraft. Flight times are shown in Figure 5-3. The slope of the dotted line relates flight time to range. For instance, the elapsed time between SS-N-6 missiles breakwater and weapon impact over distances of 500 and 1,000 nautical miles would have been eleven

SUBMARINE LAUNCHED BALLISTIC MISSILE TRAJECTORIES

(Non-rotating Earth)

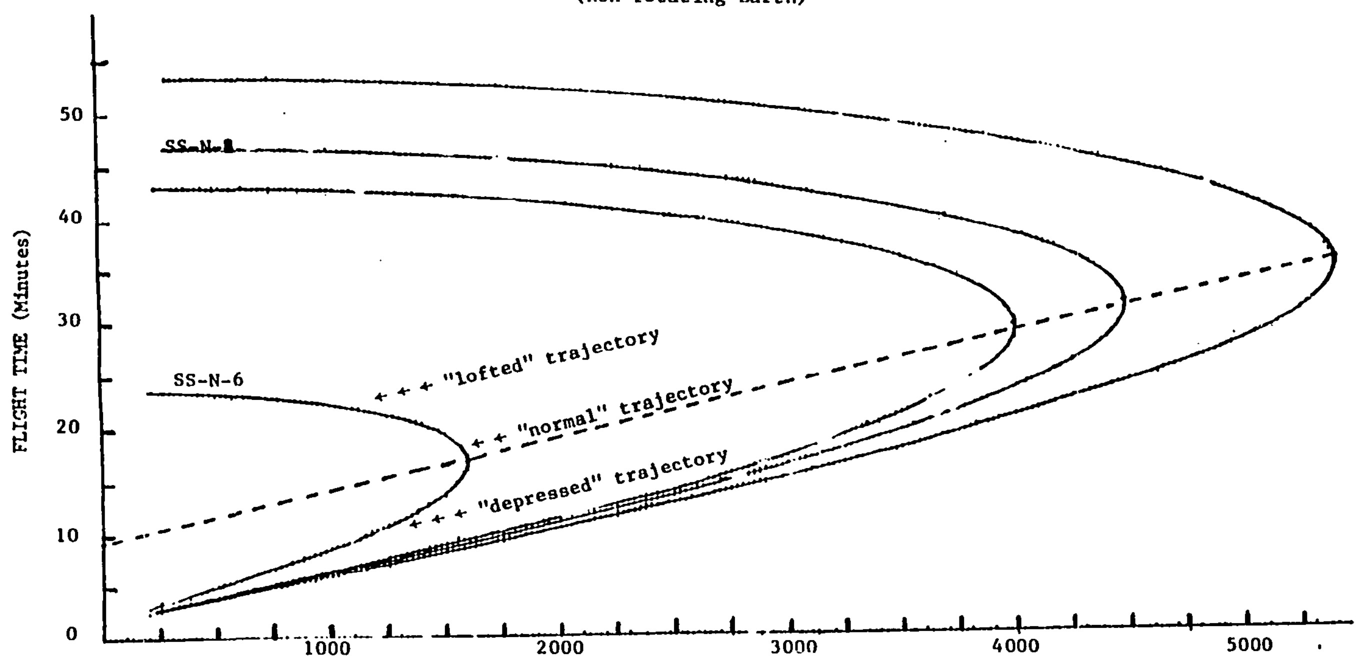


Figure 5-3

and fourteen minutes, respectively. Even the longer flight time is shorter than the normal reaction time (the time between missile breakwater and aircraft brake release) of ground alert command aircraft.

How much shorter is not a datum of public record, as actual reaction times of aircraft are classified. Available evidence does indicate, however, that the reaction time of aircraft maintained at a normal state of readiness was about fifteen minutes, allowing for warning delay, crew scramble, engine start-up, taxi and other pre-takeoff procedures. Pertinent testimony reveals, for example, that EC-135 engine start-up takes about three minutes and that an aircraft can be airborne about six minutes after start-up.[57] An additional six minutes, for a total of fifteen minutes, would have plausibly been lost to warning delay and crew scramble. (It seems certain that no less than two minutes would have elapsed between missile breakwater and the receipt of tactical attack warning at the airbases, and that crews would have taken several minutes to scramble from their alert facilities to their aircraft.) The resulting estimate — fifteen minutes — corresponds to estimates given for alert EC-135s operated by the Commander-in-Chief of Europe, Pacific and Atlantic Commands. A senior military official reported that the primary alert EC-135 in each of these commands was on fifteen minute alert.[58] (We remind the reader that CINCLANT did not deploy an airborne command post until 1973.)

The actual flight time of Soviet SS-N-6 missiles is also uncertain, owing in large measure to uncertainty about the location of enemy submarines at the time of launch. But in all circumstances in which submarine missiles were within firing range of the target, the flight time would have been sufficiently short that destruction of the target would have been virtually assured. Even if an SS-N-6 missile were fired at maximum range, or 1,600 nautical miles from the target, an aircraft on 15-minute alert could not have put enough distance between itself and its airbase (the assumed aimpoint) to survive the blast effects of the exploding weapon. As Figure 5-3 indicates, the flight time of the attacking missile would have been no more than seventeen minutes (and perhaps as little as sixteen minutes if the missile flew a direct east-to-west trajectory, exploiting the earth's rotation which "moves" the target closer to the missile during the period of missile flight). Aircraft brake release for takeoff occurs, in this example, only two minutes before the incoming weapon explodes, and during the brief period between takeoff and weapon detonation the aircraft would have flown a distance of only 42,000 feet from the runway (see Figure 5-4). This would not have been a safe distance away, because the lethal radius of a Soviet SS-N-6 missile was itself 42,000 feet. (This estimate is based on an assumed weapon yield of one megaton and aircraft hardness of two p.s.i. of blast pressure.) Thus, aircraft destruction was virtually certain unless the attacking missile proved to be unreliable.

DISTANCE FLOWN BY EC-135 AIRCRAFT

AS A FUNCTION OF TIME AFTER BRAKE RELEASE

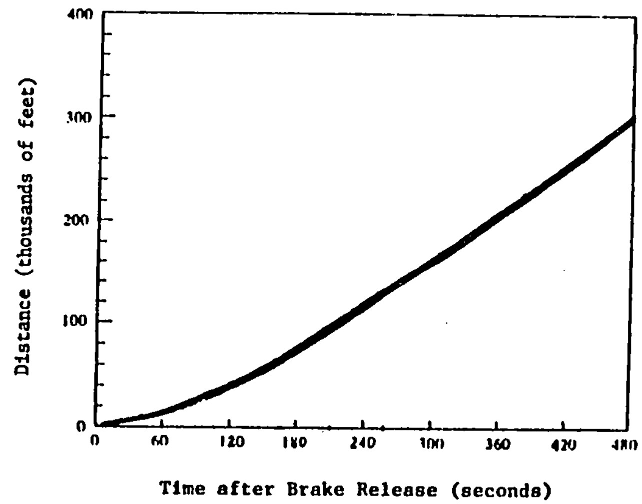


Figure 5-4

Source: Author's estimates based on unclassified data and Alton H. Quanbeck and Archie L. Wood, Modernizing the Strategic Bomber Force (Washington, D.C.: The Brookings Institution, 1976), p. 48.

Formal calculation of the probability of safe escape can be performed using the equation given below: [59]

$P_s = 1 - r_m (R_L/R_U)^2$ where:

P_s = probability of safe escape

r_m = missile reliability

R_L = lethal radius of weapon

R_U = distance between aircraft and aimpoint at moment of detonation

Assuming missile reliability to be 85 percent, the chance of safe escape for an aircraft whose reaction time and fly-out speed places it 42,000 feet from the aimpoint at the moment of weapon detonation equals: $1 - .85 (42{,}000/42{,}000)^2$, or 15 percent. The firing of two or more missiles, if optimally spaced around the aimpoint, would further reduce an aircraft's chance of safe escape. In the hypothetical example given above, the probability of safe escape for aircraft under attack by two weapons is $(.15)^2$, or 2 percent.

Figure 5-5 maps the patrol areas in the Atlantic from which Soviet "Yankee-class" submarines armed with one-megaton weapons posed a threat to the various EC-135 elements of the PACCS network. [60] Theoretically, the firing of a single reliable SS-N-6 missile from any of the Atlantic zones -- marked A, A-B, and A-B-C -- would have destroyed the national command aircraft stationed at Andrews Air Force Base under normal day-to-day alert conditions. In 1972, NEACP alone was within firing range

SOVIET SUBMARINE THREAT ZONES

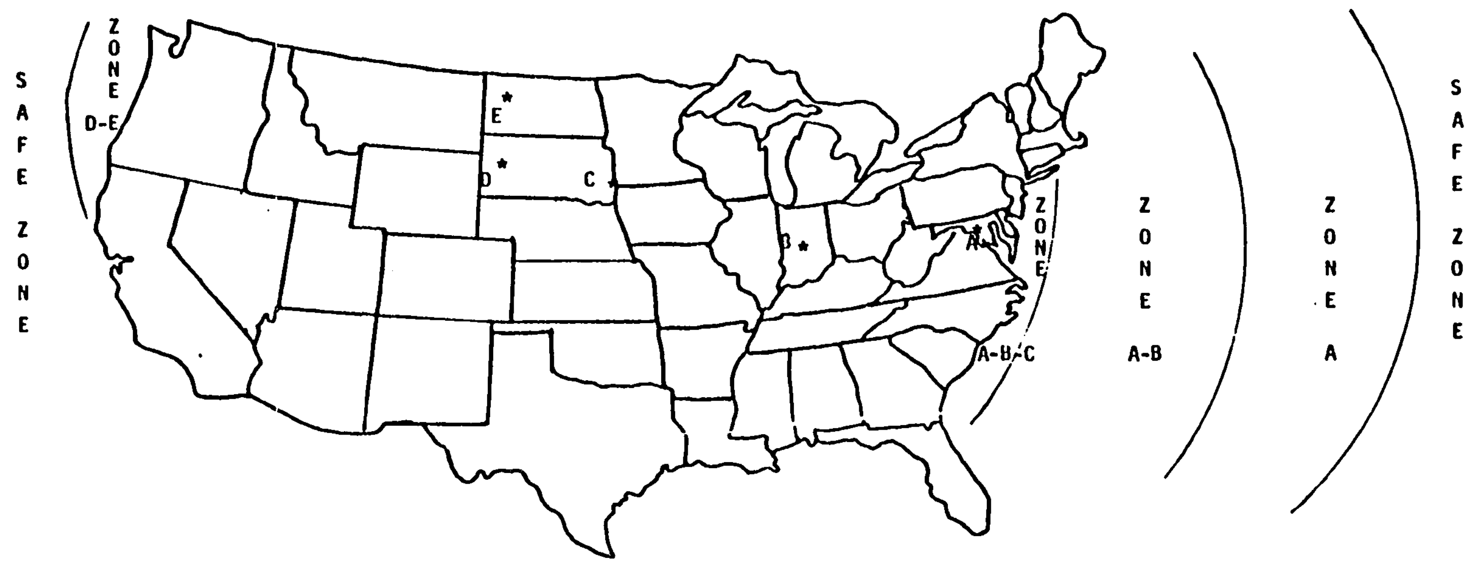


Figure 5-5

of a Soviet submarine stationed in zone A (CINCLANT's airborne command post came under the same threat when it was deployed in 1973 at Langley Air Force Base, Virginia), but enemy submarines could move progressively closer to the U.S. shoreline to bring other elements of the PACCS network within range. From zone A-B, a submarine firing two reliable missiles would have destroyed PACCS aircraft on ground alert in Indiana as well as NEACP. From zone A-B-C, a submarine posed an equivalent threat to PACCS aircraft stationed at Offutt AFB, Nebraska. Finally, a submarine on patrol in zone A-B-C together with one in zone D-E could have destroyed all ground alert elements of PACCS as well as NEACP under conditions of surprise attack.

The significance of this theoretical vulnerability is debatable. Many observers totally reject surprise attack scenarios on the grounds that signs of enemy preparation for attack would appear prior to the actual attack; that such indications would be correctly read; and that strategic organizations would react in time to avoid the worst consequences of sudden attack without warning. In this view, command vulnerability to surprise attack, however acute, does not merit serious concern as long as strategic organizations are prepared to take steps -- for instance, dispersal of PACCS aircraft, reduction of aircraft reaction times, and institution of airborne alert -- designed to complicate enemy targeting, provide more escape time for aircraft on ground alert and otherwise serve to protect the command structure. Emergency measures would presumably be taken in a crisis and would presumably work to thwart enemy exploitation of peacetime vulnerabilities.

To conservative U.S. planners, however, the scope for intelligence failure, political indecision, sluggish organizational response, and so forth is sufficiently large that surprise attack is not implausible. Extreme prelaunch vulnerability of PACCS aircraft on normal ground alert is therefore a pertinent fact and in light of the key role these aircraft play in postattack strategic control it is an extremely important fact.

Opinion can also split over the related issue of the effectiveness of programmed crisis responses. Whether implementation of emergency protective measures would have substantially reduced PACCS aircraft vulnerability depends on a complex of factors, many of which were excluded from earlier calculations. Pertinent considerations include the sabotage threat, the effects of electromagnetic pulse and the ability to sustain airborne alert operations throughout the course of a prolonged crisis.

What can be shown using the analytic approach applied earlier is that while the prelaunch vulnerability of aircraft placed on a higher-than-normal ground alert during a crisis would not have been acute, as it was under normal readiness conditions, it would have still been significant. Depending on the disposition of enemy submarine deployments and U.S. PACCS aircraft, particularly NEACP, high confidence in the prelaunch survivability of EC-135s would not have been warranted under many circumstances.

Consider a hypothetical situation in which a preplanned organizational response to crisis would have reduced NEACP's reaction time from fifteen to seven minutes. SS-N-6 missiles subsequently launched from a distance of, say, 500 nautical miles, would have arrived about four minutes after NEACP brake release, allowing NEACP to put 123,000 feet between itself and the runway before weapon detonation. But the risk of NEACP destruction in this case is still significant: ten percent (calculated as follows -- .85 $[42,000/123,00])^2$. In the event of attack by four missiles, the estimated risk is 40 percent.

To achieve a very high level of confidence (over 90 percent) in NEACP's survival against a large attacking force (for example, four enemy missiles) with short flight times (for example, eleven minutes), the reaction time of the aircraft had to be reduced to four minutes or less because seven minutes were needed to fly a safe distance away from the barraged area (an area centered on the airbase, assuming optimally spaced and timed detonations). In other words, to be highly survivable the aircraft had to be positioned at the end of the runway, engines running and ready for immediate takeoff upon receipt of tactical warning.

Beyond the practical difficulties of maintaining this level of readiness during a prolonged crisis, there would have been virtually no margin for error or delay in the processing of tactical warning information. Nearly perfect performance was required in the postulated circumstances; but, it would not have been prudent to expect flawless performance.

Deployment of Soviet submarine missiles capable of flying on depressed trajectories would have further diminished the benefits that emergency measures such as increased alert readiness were intended to provide. The following chart shows the reduction in SS-N-6 flight time that might have been achieved if depressed trajectories could have been flown.

Flight Times (Nonrotating Earth)

Range (Nautical Miles)	Normal Trajectory (minutes)	Depressed Trajectory (minutes)	Time Reduction (minutes)
500	11.50	5.00	-6.50
750	12.75	7.00	-5.75
1000	14.00	8.50	-5.50
1250	15.25	11.00	-4.25
1500	16.50	14.00	-2.50

The implications of such short flight times for aircraft survival can be illustrated by comparing the prelaunch vulnerability of NEACP to attack by normal and depressed trajectory missiles. For example, we estimated that NEACP's probability of survival against four missiles fired at a range of 500 miles would have been 90 percent if the aircraft reaction time were four minutes. This estimate assumed normal missile trajectories. If depressed trajectories are postulated, however, NEACP's prospects of survival are greatly diminished. A <u>single</u> SS-N-6 missile fired on a depressed trajectory from a distance of 500 nautical miles would have had an 85 percent chance of destroying

NEACP; from a distance of 750 miles, the probability of NEACP destruction would have been 25 percent. Conversely, NEACP's probability of survival ranged between 15 and 75 percent for a single missile launched from a distance of 500 to 750 miles. In the event of attack by four missiles, the probability of survival declines to between nil and 20 percent.

Soviet forces did not actually pose the threat implied by the above calculations. Soviet missiles evidently had not been flight tested in depressed trajectories, and testing almost certainly would have been conducted before weapons designed to operate in that mode were fielded. The calculations simply illustrate that certain tactics may have been devised, if necessary, to at least partially offset the additional margin of safety that increased alert readiness is supposed to provide. (It is also worth noting that standard calculations of force vulnerability, and in particular bomber vulnerability, usually include depressed trajectory missile attacks among the cases considered.)

The main conclusion of these illustrative calculations is that the very small-scale deployment of Soviet missile submarines in 1972 was not insignificant. From the standpoint of alert bomber survivability, the Soviet missile submarine threat was a token one. *Yankee* submarines nonetheless put command aircraft at considerable risk. If genuine strategic surprise were achieved, neither NEACP nor any of the other major elements of the airborne command network would have been successfully launched prior to the impact of incoming submarine missiles. If genuine strategic surprise was not achieved and aircraft alert readiness was higher than normal, as seems likely in many crisis circumstances, then the prelaunch vulnerability of command aircraft would not have been acute. But the successful launch of NEACP prior to the arrival of incoming submarine-launched weapons would have been questionable under certain plausible circumstances even if tactical warning systems performed flawlessly. And given the extreme sensitivity of aircraft vulnerability to tactical warning performance, significant risk was inherent in the situation. These risks applied to all PACCS aircraft, not just NEACP.

The above illustrations suggest, however, that a military command -- namely, SAC -- stood a better chance of surviving a dedicated attack on the command structure than key national entities did. SAC enjoyed greater geographic insulation from enemy submarines on patrol; operated an alternate command post on round-the-clock airborne alert; and normally maintained additional command aircraft on ground alert. By contrast, geography did not favor the prelaunch survivability of national command aircraft; for various reasons the maximum precaution against sudden attack -- continuous airborne alert -- could not be taken; and redundancy in the form of back-up alert aircraft other than the primary was not normally provided.

Postlaunch Configuration and Capabilities of NEACP and PACCS: 1972: The PACCS/NEACP airborne network was restructured in 1970. EC-135 command aircraft located at the three Numbered Air Force Headquarters at bases in Louisiana, Massachusetts and California were transferred to bases in the Midwest. These reassignments reduced the vulnerability of ground alert aircraft to missile submarine attack and provided for a more compact network which could be serially interconnected by UHF line-of-sight radio communications. Back-up systems for communicating beyond line-of-sight range included HF and newly deployed LF radio, neither of which propagated as well as UHF radio in a nuclear-disturbed atmosphere.

Once launched, the airborne network extended from the seat of national government to the far west Minuteman missile complexes. Figure 5-6 shows a hypothetical network consisting of eight airborne stations.[61] Line-of-sight communications to ground missile units constrain the orbits of four aircraft — "Looking Glass" and three airborne launch control centers. "Looking Glass" is also restricted to a flight pattern that allows continuous line-of-sight radio communications with SAC Headquarters in Nebraska. The easternmost orbit, occupied by NEACP, is assumed to be confined to a region within line-of-sight communications range of ground entry points and national command posts in the Washington area. Additional constraint is imposed on these five orbits, as well as the remaining three orbits occupied by a radio relay aircraft and two auxiliary command aircraft, to reflect the loss of flexibility that results when line-of-sight communications between all adjacent aircraft must be continuously maintained.

An attack strategy based on EMP effects probably offered the best chance of damaging aircraft in the network. In the event of a high altitude burst above the center of the country, exposure to EMP was

HYPOTHETICAL POST ATTACK AIRBORNE NETWORK

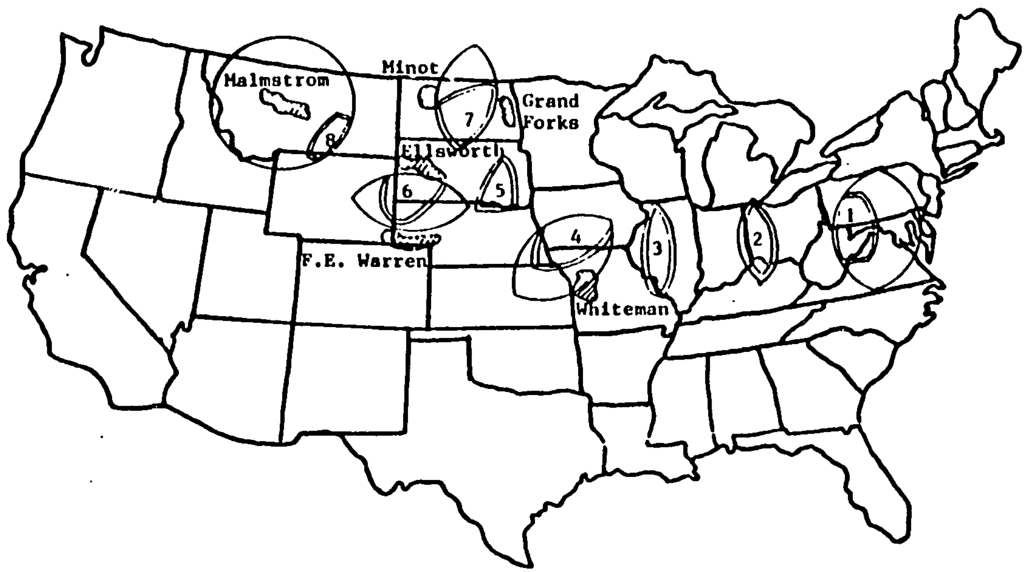


Figure 5-6

——— Orbital constraints imposed by air-to-ground communications (200 miles)

═══ Orbital constraints imposed by air-to-air communications (400 miles)

Function/Orbits (and Home Base): 1 - NEACP (Andrews AFB, Va.); 2 - Relay Aircraft (Grisson AFB, Ind.); 3 - East Aux. (Offutt AFB, Neb.); 4 - "Looking Glass" and ALCC/ERCS for Whiteman Missile Complex (Offutt AFB, Neb.); 5 - West Aux. (Ellsworth AFB, S.D.); 6 - ALCC for F.E. Warren and Ellsworth Missile Complexes (Ellsworth AFB, S.D.); 7 - ALCC for Grand Forks and Minot Missile Complexes (Minot AFB, N.D.); 8 - ALCC for Malmstrom Missile Complex (Minot AFB, N.D.)

virtually certain, and the loss of only one or two aircraft in the serial linkage could have been very costly. This will become clearer when we turn to discuss the specific functions performed by the constituent parts of the network.

This potential problem was not lost on defense officials at the time. That the entire airborne command network might be vulnerable to EMP was a possibility that began to worry many during the early 1970s. Although the performance of aircraft exposed to EMP fields had not been assessed with scientific precision, the theoretical refinements of the mid 1960s strongly suggested that aircraft vulnerability would be high unless special protective measures were taken. Analysts realized that EC-135 aircraft (and EC-130 TACAMO aircraft discussed later) in the then current fleet not only lacked such protection,[62] but that they also were being equipped with modern electronic devices (transistors, semiconductors) which actually were more susceptible to damage than the older systems (vacuum tubes) were. Periodic modernization of avionics and communications equipment was exacerbating an already significant problem.

These predictions would be validated later. Analyses and test simulations would show that EMP could induce very large currents on the exterior and interior of aircraft exposed to a full-threat (50,000 volt) pulse. Figure 5-7 provides estimates of exterior currents for an aircraft.[63] While these values have been taken from a study of the B-1 strategic bomber and therefore may not be representative of actual values for NEACP and other aircraft in the airborne command fleet, they

Aircraft Exterior Currents From

Exposure to Maximum Expected EMP

Configuration	Peak Current (Amperes)
Cockpit	
Airborne	5,600
Ground	12,700
Air Refuel	26,700
Fuselage, center	
Airborne	8,850
Ground	25,000
Fuselage at wing	22,600

Figure 5-7

probably do not overestimate current levels for EC-135 (and EC-130 TACAMO aircraft). Given the configuration of most airborne command posts and radio relay aircraft -- for instance, their use of a trailing wire antenna several miles long -- the values applicable to them would probably be even higher than those shown.

Past experience indicates that basic fuselage construction allows about one-tenth of the exterior current to flow on the inside of an airframe.[64] Thus, interior current flow might range between 560 and 2,670 amperes. In the case of the B-1, hardening plans called for extra shielding to reduce these currents to less than 10 amperes. In addition, internal communications and avionics equipment would have been protected against current surges on the order of 10 amperes.[65] In the case of the unprotected EC-135 and EC-130 aircraft deployed in the early 1970s, one could reasonably expect hundreds or thousands of amperes to flow inside, coupling into sensitive equipment with damage thresholds far below the expected level of exposure.

Unless this diagnosis severely distorts the realities of the EMP problem, NEACP and the rest of the airborne command network were never the robust deterrent linchpin that they were cracked up to be. Throughout the period covered in this chapter and the last, there was significant risk that a few high altitude explosions would have adversely affected the performance of the airborne network.

By the early 1970s, this threat loomed large indeed, since by that time NCA authorization of retaliation hinged on the performance of NEACP. In Packard's opinion, so much was riding on outmoded aircraft that a crash program to modernize the airborne network deserved the highest priority within the Defense Department. He advocated acceleration of the schedule to develop and deploy the E-4, a militarized jumbo jet hardened against EMP, partially on the grounds that the high EMP-vulnerability of then operational aircraft should be eliminated as soon as possible. The Air Force responded to Packard's personal intervention with a proposal to deploy E-4 aircraft on an accelerated schedule and Secretary Laird pursued his Deputy's recommendation by directing the Air Force Secretary to immediately initiate the E-4 program. [66]

As part of the supplemental budget request for fiscal year 1973, submitted in recognition of the need to accelerate the E-4 program, funds were also sought for "an EMP simulator of sufficient size to test adequately avionics in full-size aircraft at close to the EMP threat level." [67] According to the Air Force project officer, the simulator would be available by 1975 "to test the total configuration at the 50 kilovolts per meter level that we expect to exist based on the threat. This will give us the design assurance at the time of initial operating capability that the [E-4] does in truth have the protection against EMP that our current systems [EC-135s, EC-130s] do not have." [68]

A barrage attack using blast effects also could have been attempted, and with some chance of success. This concern surfaced in the early 1970s and became part of the rationale for deployment of an E-4 fleet to replace the EC-135 fleet. A pertinent argument developed during testimony on behalf of the E-4:

> The improved operational capability of the E-4B (747) ... permits use of random flight patterns and evasive flight profiles without concern of loss of communications connectivity with the strategic forces, thereby compounding an enemy's intelligence and targeting problem.[69]

Although the Soviets did not have any known capability to conduct real-time surveillance of PACCS aircraft in flight, we can be reasonably sure that Soviet planners could have studied details of the network -- home bases, missions, communications capabilities, and so forth, and deduced a fair amount of information about probable flight patterns in wartime.[70]

A surprise barrage attack aimed at "Looking Glass" operating on routine alert in peacetime may have had an even better chance of success. Peacetime practices were not as covert, and Soviet planners doubtless had the benefit of accumulated intelligence gathered over the course of many years. They knew the home base of operations. They could easily have discovered that much of the operation proceeded like clockwork. The schedule for takeoffs and landings, for instance, was fixed, repetitive and predictable. Using "ferret" satellites or other collectors of signal intelligence, interception of routine communications between "Looking Glass" and SAC Headquarters probably was possible.[71] Such intelligence may have eventually revealed additional significant details about the normal area of operations and the flight profile within this region. In short, Soviet planners surely knew approximately where to direct a barrage attack.

For purposes of illustration, let us suppose that Soviet planners determined that "Looking Glass" normally stayed within line-of-sight radio communications range of both SAC Headquarters and Minuteman units in Missouri. Figure 5-8 bounds the area of operations that would allow for such simultaneous links from an aircraft flying at an altitude of about 32,000 feet. UHF radio communications from spots outside this perimeter would not have been as effective since those spots lie over the horizon from SAC Headquarters, or Minuteman units, or both. The constrained area measures 49,000 square miles. For obvious reasons the air space above some 9,000 square miles -- the space within and immediately around the Minuteman sites, are excluded from the orbit.

The probability that a barrage attack of varying intensity would destroy "Looking Glass" is shown in Figure 5-9. These estimates assume an altitude of 32,000 feet for both the target and the explosions; aircraft hardness of one or two p.s.i.; missile reliability of 80 percent; and the commitment of ten to fifty SS-9 ICBMs.[72] Under these assumptions, the risk of destruction is significant. To a conservative planner, it is very significant if a large-scale barrage (30 or more missiles) is postulated. Actually, the risk would be much greater if our calculations included airborne hazards associated with attacks on ground targets in the vicinity of airborne orbits. Turbulence and particulate matter may have destroyed or severely degraded some command aircraft and/or their communications equipment such as trailing wire antennas.

PRACTICAL OPERATING REGION FOR SAC AIRBORNE COMMAND POST*

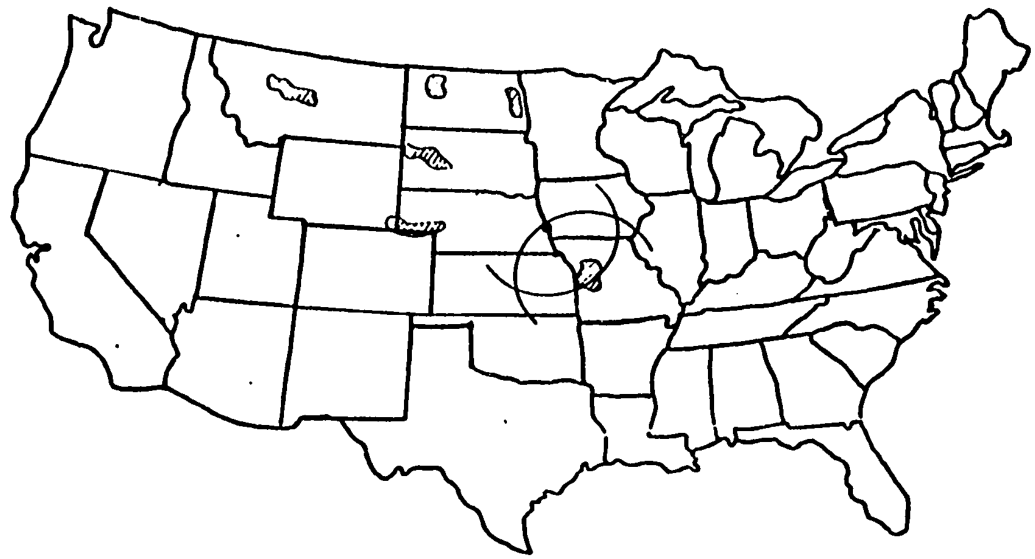


Figure 5-8

*The region is define by the intersection of two circles, one centered on Omaha and the other centered on the Minuteman complex in Missouri. The radius of each circle is 200 miles, which was noted to be about the range limit of line-of-sight communications for aircraft at altitude (six miles). The intersection of the circles = (2/3)pi(r^2) - (r^2 3)/2 .

SS-9 BARRAGE ATTACK AGAINST

SAC AIRBORNE COMMAND POST

Soviet Missile Reliability	Aircraft Hardness (PSI)	Probability of Destroying Aircraft — Missiles Targeted: 10	20	30	40	50
.80	1	.11	.21	.32	.43	.53
.80	2	.05	.10	.15	.21	.26

Figure 5-9

Although this set of calculations is meant to serve illustrative purposes, we hasten to note that the underlying assumptions are not arbitrary. The results depend mainly on the parameters of the aircraft's orbit, and the parameters used in the analysis can be justified on the grounds that they appear to define an optimal area of operations. If "Looking Glass" were to maintain continuous, direct radio communications with SAC Headquarters, it could monitor the disposition of SAC forces until the ground facility came under attack. Under preattack conditions, the ground facility could also have relayed early warning, execution or other emergency messages sent via land lines from NORAD and the NCA. In the event of enemy attack SAC Headquarters could have immediately notified "Looking Glass," or delegated CINCSAC authority to it, or both. And so forth.

It would have also been prudent for "Looking Glass" to operate within line-of-sight range of Minuteman units in Missouri. This practice would have facilitated direct, timely and survivable communications to part of the ICBM force as well as to ERCS missiles which also were deployed there (see discussion below). Through ERCS, "Looking Glass" had some chance of reaching the rest of SAC's forces, including far-flung manned bombers. A requirement to operate within communications range of ERCS would seem further warranted in light of the limited airborne endurance of "Looking Glass," and the fact that an attack could occur any time during a normal eight-hour shift. Without aerial refueling, the aircraft would have had enough fuel to fly for only about two hours if an attack occurred at the end of its regular duty shift.

"Looking Glass" (and other PACCS aircraft) could use ground entry points to tie directly into SAC's primary alerting system, however. This capability did expand its freedom of movement beyond the limits defined above. The greater the number of ground entry points, the more freely the aircraft could roam, at least in peacetime. The exact number and location of these interfaces are not publicly known, but there were not very many.[73] Furthermore, the sudden destruction of ground communications channels was an ever-present danger, and hence "Looking Glass" could not stray too far from an orbit that would allow for direct radio contact with ground units. "Looking Glass" also could not have roamed too freely if it hoped to be in a position to link up quickly with other PACCS aircraft over the radio frequency (UHF) that offered the greatest immunity to disruption from jamming and nuclear effects on the atmosphere. The functions of these other aircraft are discussed next.

A. <u>SAC Auxiliary Command Posts and Communications Relay Aircraft</u>: The workload of "Looking Glass" was potentially so great that in 1962 SAC deployed auxiliary command aircraft to provide assistance in wartime.[74] An inventory of nine such aircraft existed in 1972, two of which were kept on ground alert at all times. One of them was stationed at Ellsworth AFB, South Dakota. Once launched, this West Auxiliary Airborne Command post would have positioned itself between "Looking Glass" and missile launching aircraft to the west. The second auxiliary, called East Auxiliary Airborne Command Post, was based on ground alert at SAC Headquarters. Time permitting, CINCSAC and the JSTPS would have boarded and assumed a flight position between "Looking Glass" and the East Communications Relay Aircraft. [75] The SAC airborne battle staff and the workload would have thus been spread over three aircraft ("Looking Glass" and the two auxiliaries) interconnected serially by UHF line-of-sight radio communications. But even so the workload was considered to be too great to handle. Using manual methods of data processing, battle staffs were "saturated with incoming information during exercises." [76] It was concluded that battle staffs could not process incoming data while at the same time supporting "nuclear war decisionmaking." [77]

Communications equipment aboard these three EC-135C model aircraft consisted of UHF radio for line-of-sight transmissions, and HF and LF radio for longer range communications. Assuming an intact, eight-station PACCS network, UHF links provided access to all Minuteman LCCs. "Looking Glass" could communicate directly to LCCs in Missouri complexes via air-to-ground UHF radio, and indirectly to LCCs at other Minuteman complexes via air-to-air UHF links running through the West Auxiliary aircraft and missile launching aircraft. In the other direction, communications from NEACP were relayed to "Looking Glass" by the East Communications Relay Aircraft and the East Auxiliary aircraft. All four aircraft in this chain used UHF air-to-air radio as the primary means of interconnection.

"Looking Glass" and its two auxiliary aircraft were tasked with responsibility for controlling outbound bombers (launched on tactical warning) as well as the ICBM force. Communications with far-flung bombers were still problematical, however, because reliance on HF radio was still very great.

Since 1966, SAC twice had tried and failed significantly to enhance long range communications with bombers. The first effort was made as part of a major teletype communications program called Survivable Low Frequency Communications Program (SLFCS). In 1968, SAC deployed two SLFCS radio transmitters on the ground and configured LCCs, bomber base wing command posts, and Green Pine facilities to receive SLFCS transmissions. SAC command post aircraft and NEACP were equipped with SLFCS transceivers used in conjunction with a trailing wire antenna which extended about two miles from the tail of the plane.[78] The idea behind both the ground and air segments of SLFCS was to exploit the superior propagation characteristics of the low frequency radio bandwidth in order to increase the reliability of communications, especially with LCCs and forward area Green Pine sites, in a nuclear environment.[79] Low frequency signals are not nearly as prone to blackout from nuclear explosions as HF signals are. At the former wavelength, signals can be propagated along the surface of the earth (a "ground wave"), whereas long distance HF transmissions propagate by repeated reflections between the earth and the upper atmosphere (a "sky wave"). Ionization of the upper atmosphere caused by nuclear explosions can black out HF communications, but it would not blackout a low frequency ground wave. Glasstone and Dolan note: "Ionization from nuclear explosions will not generally degrade the performance of LF systems which normally depend only on the ground wave."[80] Another important propagation characteristic of SLFCS is the ability of low frequency signals to penetrate the earth to considerable depths. This is of course irrelevant to the question of bomber communications, but it was exploited to improve communications to LCCs. The burial of SLFCS antennas at LCCs greatly increased the resistance of LCC communications to blast effects.[81]

The ground portion of SLFCS worked well, but it was extremely vulnerable to direct attack. The two large, fixed transmitters in Nebraska and California could not withstand attack, and all the ground receiving stations with the possible exception of LCCs were unlikely to survive direct attack.

The airborne portion of SLFCS was basically immune to attack, but it did not work well. Various technical problems ranging from insufficient transmitter power to inefficient antenna design to antenna reel-out jams plagued the airborne SLFCS systems. It was not reliable and only marginally effective. Even in a benign environment the airborne command posts could not have reliably reached the Green Pine sites for relay of messages to bombers. Their capability to reach much closer units such as other EC-135C command post aircraft in PACCS and Minuteman LCCs, which were equipped for reception of low frequency transmissions in 1968, was also questionable. In a benign environment, the equipment reliability and signal range of SLFCS was such that NEACP probably could have reached "Looking Glass," which in turn probably could have reached LCCs at all six Minuteman wings. But the overall probability of getting a message through this NEACP - Looking Glass -

LCC nexus using SLFCS was almost certainly no better than 50 percent under favorable conditions and worse in a nuclear environment.

Early recognition of airborne SLFCS deficiencies and the growing vulnerability of Green Pine facilities led to a program to develop a long range VLF system that would allow airborne command posts to communicate directly to bombers. Initiated in 1967, the Special Purpose Communications (SPC) program defined a one-way, antijam (seven words per minute) system that employed a very long trailing wire antenna for transmission to bombers and tankers equipped with VLF receivers and short antennas.[82] In 1969, a spokesman for the Air Force promoted the project on the grounds that an operational VLF capability "might be the difference between success and failure in getting the message through (to bombers)."[83] By 1971, plans to equip bombers and tankers with receivers and EC-135 aircraft with transceivers were shelved, as a result of fiscal belt tightening that occurred at the turn of the decade. Development of transceive VLF capabilities for command post aircraft proceeded independently under the E-4 program.

As a result of cutbacks in the SPC program, the systems available in the early 1970s for purposes of long-range communications from command post aircraft to strategic bombers included HF radio, which was unreliable in a nuclear or heavy jamming environment; SLFCS, which lacked sufficient range and depended on fixed ground-based receivers (Green Pine); and Minuteman ERCS, a last-ditch MEECN element that had become fully operational in 1967.[84] SAC would rely on these tenuous channels for the duration of the decade, while pursuing a solution based on satellite communications. (See discussion of AFSATCOM program in next chapter.)

B. Missile Launching Aircraft and ERCS: About 1963, McNamara initiated the development of a system for launching Minuteman missiles by airborne remote control. [85] Successful tests of an EC-135 ALCC were completed in early 1967, and the Airborne Launch Control System (ALCS) was declared operational. [86]

Besides "Looking Glass," which may have doubled as an ALCC as well as a command post, SAC possessed nine dedicated missile launching aircraft in 1972. Three of them, along with air crews and missile launch control personnel, were stationed on ground alert at all times. An ALCC based at Ellsworth AFB, South Dakota, had responsibility for 150 Minuteman ICBMs at Ellsworth and 200 missiles at F.E. Warren AFB, Wyoming. One of two ALCCs based at Minot AFB, North Dakota, had responsibility for 200 missiles at Malmstrom AFB, Montana. The other had responsibility for 150 missiles at Minot and 150 missiles at Grand Forks AFB, North Dakota. [87]

ALCC aircraft backed up the underground LCCs and could gain control over a missile or group of missiles if the missile(s) had become isolated from all five LCCs in a squadron. [88] Missile launch facilities (LFs) normally received a continuous, computer-automated stream of signals from the LCCs. Cessation of these signals, due to the destruction of all five LCCs or the severance of LF-LCC communications links, would have spontaneously activated a radio receiver, at each isolated LF, to monitor computer-coded transmissions from any ALCC flying in the vicinity. ALCCs could transmit all of the launch sequence commands -- target, arm, and launch commands -- that an LCC could. Unlike LCCs, however, ALCCs could not monitor missile status before, during or after the transmission or commands. A radio uplink from the LF to the ALCC did not exist. [89]

Several LFs at Whiteman AFB, Missouri, housed missiles equipped with a tape recorder and a UHF radio package instead of a warhead. Minuteman ERCS systems had been successfully tested in 1966 and declared fully operational in late 1967, [90] replacing earlier ERCS variants such as Blue Scout sounding rockets. "Looking Glass" possessed the capability to transmit voice messages to the missiles prior to launching them, [91] though airborne launch control was once again contingent upon the loss of LCC control (not to mention the survival of ERCS LFs and associated communications, both of which were at least as vulnerable to nuclear weapons effects as standard Minuteman LFs housing nuclear-armed missiles). [92] Functional ERCS missiles could record an execution message sent by "Looking Glass" (or LCCs), play it back to permit launch crews to check its completeness and accuracy, and broadcast the message during a flight along either a northwest or northeast trajectory. [93] These trajectories would have positioned the ERCS missiles to broadcast, for no more than thirty minutes (the flight time of a Minuteman missile), SIOP execution messages to Minuteman and Titan LCCs, wing command posts at bomber bases, strategic bombers in flight, and any other SAC unit that was tuned to the proper UHF frequency and located within range of the transmitter. [94] Range was of course subject to the physical constraints imposed by earth curvature. It was also limited by the transmitting power of the ERCS communications package and by the effects of atmospheric scintillation on the UHF signals transmitted from ERCS during its flight through space. As discussed later (Chapter 6), nuclear explosions in the upper atmosphere could black-out UHF transmissions from space vehicles such as satellites and ERCS missiles.

It is likely that Navy strategic units such as TACAMO aircraft (see discussion below) also listened for ERCS transmissions. The prevailing expectation, however, was that the unified commanders (that is, CINCLANT, CINCPAC) would pass execution orders down to the TACAMO and the missile submarine fleets. There is reason to suppose, therefore, that TACAMO was less than fully integrated — procedurally if not technically — into the ERCS channel. If they had been, SAC would have been in a position to execute strategic forces under the jurisdiction of non-SAC commanders. [95]

Within SAC itself, procedural arrangements were such that under certain plausible conditions the attempt to launch either ERCS or nuclear armed missiles by means of ALCC aircraft would have failed. A Soviet attack aimed at underground LCCs may have set up the following situation: communications at the LCCs are temporarily disrupted, or destroyed, while at the same time the LCCs remain interconnected with missiles in their squadron. The isolation of LCCs from higher authorities and ALCCs but not from missiles in the squadron would have created internal procedural contradictions that would have prevented execution. The LCCs could not receive execution messages, and the ALCCs could not exert remote control over the missiles because as long as even a single underground LCC continued to be connected to the squadron LFs, airborne access to the LFs was blocked. There was a procedure whereby surviving LCCs deliberately relinquished control of the LFs (accomplished by turning off all LCC computers), to permit control to transfer to an ALCC, but the procedure required coordination between the LCCs and the ALCC; and, coordination required communications, which in the postulated circumstances do not exist. Furthermore, this procedure would not have applied unless an execution message had already been received and acted upon by an underground LCC. Its purpose was to enable an ALCC to send a second launch vote to LFs in squadrons which contained only one surviving LCC. (The launch vote from this LCC would have begun the delayed launch countdown; a second vote from an ALCC would have eliminated the delay, resulting in immediate lift-off.)

The priority of negative control explains the absence of a procedure whereby LCCs would turn off their computers in the event of a loss of communications at LCCs. To have done so would have facilitated positive control in that ALCCs could have then assumed control and launched the forces. But negative control would have been degraded. An unauthorized launch command sent by an LCC that did not shut down its computer would have escaped notice by those that did.

Degradation of positive control would have been severe under the circumstances described above. Established procedure would have precluded the launch of nuclear-armed ICBMs and ERCS, disabling perhaps the last remaining means of controlling the strategic forces. This particular predicament would not have arisen if at least one LCC with operative communications with higher authorities had existed, or if all five LCCs had been destroyed, allowing for assumption of control by ALCC aircraft. Yet some degradation of positive control would have still been incurred, especially upon destruction of all five LCCs. ALCCs, like LCCs, could have executed the launch sequence — target, arm, and launch; but, unlike LCCs, they could not have confirmed that the proper commands had been received and processed at the isolated LFs. As DOD spokesmen put it, airborne missile crews launch "in the blind, without knowledge of missile availability or control over missile targeting."[96] ALCC aircraft could not have determined, for example, whether a nuclear detonation in the region had interfered with the radio signals carrying target instructions to the missiles. If the radio command did not reach the missiles in proper code, it is possible that the ALCC launch command which followed would have hurled the wrong number of missiles at the wrong targets at the wrong time. Being unable to monitor missile status, ALCC crews could not have taken stock of the error, if it was noticed at all. Many other unintended departures from the authorized attack plan may have occurred as a result of this technical shortcoming. For instance, coded launch signals may have failed to register at numerous LFs housing missiles that were supposed to be launched, and the resulting need to retransmit the signals may not have been apparent to ALCC crews.

Delay in the execution of the retaliatory forces is another form of degradation of positive control. Some delay was inevitable, given the fact that ALCC aircraft and/or ERCS missiles would have been used to relay execution messages to surviving LCCs, fire missiles at isolated LFs, or both. The length of time involved would have depended on a complex of factors such as aircraft locations and readiness. For instance, an hour or more could easily have elapsed between the time that PACCS aircraft were flushed into the air and the time that they were positioned to establish a fully coherent UHF line of communications.[97] By this time, ERCS deployments themselves could have been attacked and perhaps destroyed by Soviet ICBMs. The loss of ERCS would have spelled isolation for large segments of the bomber and submarine forces.

Prelaunch Survivability and Postlaunch Capabilities of Navy Command Aircraft and TACAMO Communications Relay Aircraft: 1972: Despite reassurances from Navy personnel who portrayed the Navy's ground-based radio broadcast network, coupled with ship-borne radio communications, as a reliable means of post attack control over missile submarines, McNamara became convinced of the need to fortify communications links from the NCA to those forces. In 1965, he established a requirement for placing an alert EC-135 airborne command post at the disposal of CINCPAC. That aircraft was stationed in Hawaii. McNamara's concern also motivated the establishment of the

Special Communications Project Office within the Navy. Created in 1967, this office was given responsibility for developing programs to satisfy an "urgent need" to ensure "effective communications at all times from the National Command Authorities and Commanders in Chief to the deployed FBM (fleet ballistic missile) forces....during and after heavy nuclear and electronic jamming attack." [98]

Soon thereafter, two special projects came to fruition. In the late 1960s, after McNamara's departure from government, the Navy's airborne VLF radio relay program — called TACAMO — became operational. [99] TACAMO provided the most survivable communications link to missile submarines. The second project was called "Pilgrim." The Navy configured Pacific-based missile submarines and TACAMO aircraft to receive messages broadcast over navigation radios operated by the U.S. Coast Guard. [100] Several such radios, so-called Loran-C stations located in the Western Pacific, were given the capability to rebroadcast execution messages by superimposing information onto the navigation signals emitted at the VLF range of the radio spectrum. [101] The Navy thus added a few more radio stations to its missile submarine communications network, stations which transmitted on a frequency that is superior to LF and HF in terms of range, jam resistance, and vulnerability to ionization effects produced by nuclear explosions. This expansion, however, was of minor significance. Enlargement and modernization of the Soviet strategic arsenal rendered "Pilgrim" insecure before it was even put in operation. By 1972, the United States could not rely on fixed communications stations to trigger submarine retaliation.

We had come to depend almost totally upon airborne command posts and TACAMO communications relay aircraft for post attack control over the submarine force. A spokesman for the Navy's Special Communications Project Office, which had overall responsibility for the TACAMO program, described the TACAMO aircraft as "the only operational survivable element that the Navy has today [March 9, 1972] and most likely will have until the latter part of the 1970s." [102] While it testifies to the questionable effectiveness of other available systems -- notably, shore- and ship-based radio communications -- the statement warrants strong qualification. TACAMO by no means ensured a secure, reliable link between higher authorities and missile submarines.

TACAMO featured propeller driven (280 knots per hour cruise speed and 4530 mile range), [103] unrefuelable EC-130 aircraft outfitted with VLF transmitters and long trailing wire antennas. The sole purpose of the fleet was to relay strategic war orders to missile submarines. In accordance with the Joint Strategic Objectives Plan, EC-130s operated in the Pacific and Atlantic areas.

The TACAMO fleet consisted of twelve aircraft when it became operational in 1969. Four of these were assigned to the Pacific; eight supported submarines deployed in the Atlantic. [104] For various reasons, the fleet never did satisfy formal requirements for maintaining one aircraft on continuous airborne alert in each sector. About fourteen actively operational aircraft — seven in each ocean — are needed to achieve this objective. [105] Training and periodic rework raises the total number of needed inventory to eighteen. In 1972, a fleet of only twelve aircraft was authorized, and only nine of those were available for duty. [106] One aircraft had crashed in January of that year, and two were in normal periodic rework or modification. Consequently, the Navy was forced to cut back the Pacific contingent in order to sustain operations in the Atlantic. Airborne alert in the Pacific was intermittent; it probably was maintained at about the rate realized in 1980, or about 25 percent of the time. [107] Although the airborne alert rate in the Atlantic was much higher, continuous airborne alert was not achieved until late 1973. [108] In both ocean areas, the Navy evidently had been striving to maintain back-up TACAMO aircraft on 30-minute ground alert. [109]

The technical sophistication of TACAMO communications left much to be desired. Aircraft transmitters radiated only a few tens of kilowatts of peak power, and efficient use of this power was difficult to achieve because of design and operational problems associated with the trailing wire antenna. [110] Consequently, TACAMO's effective range probably did not exceed several hundred miles under the best of circumstances, and hence only a fraction of the alert submarines could be reached at any given time. Communications performance would have been even poorer during a heavy electronic attack. [111] Nuclear effects may also have degraded TACAMO signal propagation, a point made by a DOD official who said that TACAMO aircraft "have insufficient communication range in a nuclear environment." [112] Under either of these adverse conditions, the aircraft may have been unable to communicate successfully with alert submarines unless they were in close proximity to each other. If close proximity were required, as seems likely, then TACAMO aircraft probably would have run out of fuel long before the time needed to deliver an execution message to all alert submarines, particularly those stationed in the Mediterranean. [113] In all likelihood, only a small fraction of alert submarines could have been served by TACAMO aircraft during the aircraft's time on station. Furthermore, neither TACAMO nor higher authority could verify successful message delivery because missile submarines normally would not and could not acknowledge receipt of messages.

No one really had good reason to believe that TACAMO would work. TACAMO was declared operational in the late 1960s even though the Chief of Naval Operations stated that its operational effectiveness had not been established. [114] It was not until 1976 that the Navy began a scientific assessment of the effectiveness of TACAMO in relaying messages to missile submarines. [115]

Range constraint discouraged the basing of alert TACAMO aircraft in the continental United States. Aircraft were normally forward-based at locations such as Wake Island, Guam, Bermuda and Western Europe. As a result, TACAMO aircraft were more susceptible to detection and more exposed to attack than were CONUS-based PACCS aircraft, for example, which served Minuteman and strategic bomber units. TACAMO aircraft placed on ground alert at forward bases were especially vulnerable. An authoritative assessment of one facet of the vulnerability problem existing in the late 1970s probably would be valid for the period of the early 1970s: "A ground-alert TACAMO within range of submarine launched ballistic missiles (SLBMs) is clearly vulnerable to destruction."[116] The high prelaunch vulnerability of ground alert TACAMO probably stemmed in part from their apparent inaccessibility to timely tactical early warning data.

Aircraft on airborne alert obviously would have been much less vulnerable to direct attack using nuclear blast effects. Air mobility, however, did not mitigate vulnerability to EMP attack. TACAMO aircraft were enormously exposed to such attacks, and severe damage from EMP attack may have occurred since TACAMO had not been afforded any protection against it.[117]

Forward deployment also entailed some risk that TACAMO aircraft would be detected and tactically engaged by opposing forces. The rather overt character of normal TACAMO operations compounded this risk in that enemy planners had a better chance of monitoring the disposition of airborne units and devising tactics for engaging them in the event of war.

TACAMO did take certain precautions to counter enemy pursuits of this sort. For instance, TACAMO aircraft, like the submarines they served, maintained virtual communications silence during airborne patrols.[118] This restriction reduced the chance of detection using direction finding or other methods. An attendant disadvantage of this procedure, however, made restrictive communications a double-edged sword. With increased stealth came greater uncertainty about the status of TACAMO. The absence of routine two-way communications between TACAMO and other units left higher authorities (and submarine commanders) not knowing whether TACAMO was fulfilling its role. Neither the status of alert submarines nor the condition of the most survivable communications link to those forces could have been ascertained by central authorities.

Compounding the uncertainty about submarine responsiveness to central command was the continuing problem of communications with submarines in transit. TACAMO deployments did not ameliorate this problem. Submarines that were not on high alert in their patrol areas still only periodically positioned themselves to copy radio transmissions. Nearly fifty percent, or half, of the missile submarines at sea were normally operating in such a reception mode.[119]

Tenuous communications channels from central authorities to TACAMO aircraft further reduced confidence in TACAMO effectiveness. In peacetime, TACAMO could reliably receive messages from many sources, including LF and HF shore stations scattered around the globe. Certain land-based LF and HF transmitters were dedicated to the TACAMO mission.[120] The main uplink to TACAMO aircraft on airborne alert in the Atlantic area, for instance, evidently consisted of HF transmitters at various locations that were keyed at CINCLANT Fleet Headquarters in Norfolk.[121] But in wartime, the reliability of communications would have been drastically reduced in the event of Soviet command structure attack. Soviet attacks on vulnerable land-based transmitters, and/or their nodal keying facilities, which cautious planners would have expected to occur, would have severely degraded communications from higher authorities to TACAMO aircraft. Once these links were severed, TACAMO units probably would have been isolated from central authorities.

TACAMO isolation was probable because CONUS-based command aircraft such as NEACP and "Looking Glass" lacked the communications capabilities needed to reliably span the great distances that separated them from TACAMO units (and from CINCPAC's command aircraft). Deficiencies of major proportions plagued all three of the interconnecting circuits: HF radio, LF radio, and ERCS-borne UHF radio.

HF radio could not be counted on to perform well in a nuclear environment because of its susceptibility to blackout. There is also considerable doubt as to the use of common HF frequencies between TACAMO and other key command aircraft such as "Looking Glass." TACAMO normally monitored HF transmissions from Navy sources and it seems unlikely that they would have switched channels to listen for SAC broadcasts unless required to do so by the JCS's MEECN plan. In the early 1970s, the JCS did not include HF radio in the MEECN plan and hence intercommand compatibility of HF communications probably did not exist.

The effectiveness of SLFCS, which constituted a major portion of the MEECN, was also questionable. Technical incompatibilities, cited earlier, evidently reduced the potential for TACAMO reception of LF transmissions from SAC aircraft, despite JCS demands for complete interoperability among MEECN components. Furthermore, CONUS-based

EC-135 command aircraft used SLFCS equipment that could not effectively or reliably broadcast messages over very long distances. Had it been available back then, even an E-4 command aircraft equipped with today's modern LF/VLF communications suite would have had great difficulty reaching forward-deployed TACAMO units. Recent testimony indicates, for instance, that LF/VLF systems designed for the E-4 would permit NEACP to reach "Looking Glass" in an adverse environment and Pacific-based TACAMO in a benign environment.[122] If such ranges approach the limit of feasible E-4 capabilities, then the obsolete LF communications suites carried by CONUS-based command aircraft during the early 1970s clearly lacked the range needed to reach TACAMO units. These older suites employed far less efficient antennas and could generate only one-tenth of the transmitter power of an E-4 system (20 kilowatts versus 200). As a consequence, the chances were slim at best that the SLFCS suites aboard NEACP, "Looking Glass," or any other CONUS-based EC-135 aircraft could have successfully transmitted messages to any forward deployed TACAMO unit or to CINCPAC's airborne command post. NEACP had the best chance of reaching Atlantic-based TACAMO aircraft, since its assigned airborne orbit would have been the closest to TACAMO's operational area on the Atlantic side. However, NEACP's ground station was the closest to enemy missile submarines and its prelaunch vulnerability was correspondingly greater than other command aircraft. Thus, the command aircraft that had the best shot at communications with TACAMO was the least survivable.

The question whether ERCS would have filled the communications void that would have otherwise left TACAMO aircraft (along with forward-deployed bombers) isolated from higher authority is difficult to answer. The available store of pertinent unclassified information on the strengths and weaknesses of this rather exotic system is meager and inconclusive.

Optimists see many virtues in the ERCS system. Three are notable. First, ERCS missiles were deployed in protective shelters that could withstand large blast overpressures. Second, ERCS missiles could have been proliferated in sufficient numbers to reasonably ensure the survival of at least two missiles (one for each trajectory). Third, ERCs transmitted on UHF, a frequency that, compared to HF and LF/VLF, was relatively unaffected by the secondary effects of nuclear explosions.

But the weaknesses of this system were just as numerous. Some were earlier identified — complicated launch operations and susceptibility to signal distortion caused by atmospheric scintillation. In addition, nuclear fireballs in the direct path of line drawn between an ERCS missile and the receiving unit would have blacked out the signal. (This presented a severe operational problem for ERCS-to-Minuteman LCC communications but only a minor problem for ERCS-to-TACAMO/Bomber communications. In the former case, multiple fireballs in the Minuteman fields were expected.) More significantly, the vulnerability of ERCS silos to blast effects would have been much greater than standard calculations would suggest if Soviet intelligence methods had revealed which specific silos housed the ERCS missiles. Even if only the particular flights within which ERCS missiles were deployed had been identified, the survivability of this crucial communication system would have been jeopardized.

Other real or apparent deficiencies -- for instance, vulnerability of ERCS launch facility electronics to electromagnetic effects -- together with those listed above raise real doubt about the efficacy of the ERCS communications link to TACAMO aircraft. Conservative U.S. planners could not have counted on ERCS to perform this vital function.

STRATEGIC SITUATION: 1972

By 1972, the perspective that sees strategic capability turning on the size and technical composition of force deployments was beginning to yield to a broader conceptualization that encompasses organizational performance as well as weapon characteristics. A cadre of analysts and senior defense officials led by David Packard had come to believe that the exclusion of either dimension from strategic assessment provides considerable scope for miscalculation, and distortion of defense priorities. Packard and others also concluded that past conceptual and material underinvestment in the C^3I area had indeed weakened U.S. security. They harbored serious doubts as to the ability of central authorities to survive enemy attack and to direct U.S. strategic forces to coherent national purposes in the wake of nuclear attacks on the U.S. command structure.

The command implications of large-scale nuclear weapon deployments, nevertheless, were only dimly illuminated during this period. The strategic agenda of the Nixon administration continued to treat the number, technical characteristics, and economics of nuclear weapons and delivery systems as the central questions of national security. The elaborate physical and procedural arrangements for managing those forces were overshadowed by force structure issues and by arms limitation talks designed to constrain the respective force structures of the two sides. This imbalance in strategic analysis and policy attention produced gross misunderstanding of the actual strategic balance. Many other aspects of the strategic situation were inadequately appreciated.

U.S. Second-Strike Capabilities and the Overall Strategic Balance

Popular calculations based on weapon characteristics indicated a robust U.S. strategic posture and a significant advantage in overall strength. Calculations showed that although the overwhelming superiority supposedly enjoyed in earlier years had evaporated as a result of the vast Soviet arms buildup of the late 1960s and early 1970s, the United States still maintained a dominant position. Furthermore, only the most conservative of projections had the Soviets drawing even with or overtaking the United States in the near-term future. The Soviets were lagging behind in important areas of strategic development, particularly in missile accuracy and fractionalization. Even if these leads were lost overnight, the United

States was credited with awesome second-strike capacity for nuclear reprisal. By all accounts, the raw destructive power required to inflict swift and severe punitive retaliation to nuclear attack positively resided in the U.S. force structure and nothing the Soviets could plausibly devise could change that stark reality. For the foreseeable future, the force structure requirement of deterrence would be easily met.

Popular calculations, however, obscured the fact that Soviet attack on the U.S. command structure threatened to destroy central positive control over strategic forces. U.S. retaliation could have been blunted, if not blocked.

The most formidable problem in this regard was preserving national control in the wake of a surprise attack. The consequences of intelligence failure or inadequate response to indications of impending attack would have been extremely adverse. With the deployment of Yankee-class Soviet submarines, the United States became exposed to nuclear strikes that could have virtually decimated the most survivable portion of the U.S. command system: the fleet of ground alert C^3 aircraft. NEACP was especially vulnerable to submarine missile attack. This vulnerability not only raised the specter of NCA decapitation, a decisive outcome if retaliation required the personal authorization of the president, but also threatened one of the two key communications links to Atlantic-based TACAMO aircraft. Most other C^3 aircraft were practically as vulnerable as NEACP. Consequently, central control over quite a large number of second-strike forces could have been lost.

Estimated conservatively, the weapons still under central control after a surprise Soviet attack would have ranged between zero and 30 percent of the total number in the alert inventory.

Fewer than half the total number in the inventory, we estimate, would have been responsive to central authorities even if the U.S. command system had been fully generated in anticipation of the attack. Advance strategic warning followed by command mobilization would have greatly enhanced the survivability of the airborne command system but survivability was not by itself a sufficient condition to guarantee delivery of execution messages to the forces. Direct radio communications links between the airborne C^3 elements and the forces were too tenuous and the performance of ERCS was too uncertain to warrant high confidence in the ability of central authorities to issue instructions to a large fraction of the forces, particularly submarines (via TACAMO relay) and far-flung strategic bombers (that is, bombers outside the line-of-sight UHF range of C^3 aircraft).

In short, standard estimates of U.S. second-strike capabilities were wildly misleading. The number of survivable U.S. weapons exceeded the number of controllable second-strike weapons by a factor of two or more. The Soviet threat, in other words, was much greater than generally believed.

Crisis Stability

Crossing the nuclear threshold on the basis of calculations showing that command structure attack might succeed would have defied reason so long as Soviet leaders could still summon hope that general war with the United States could be avoided. Conservative Soviet planners could not have confidently predicted that Soviet strikes would cripple the U.S. command structure and thereby parry nuclear retaliation. Although such an outcome seemed to lie well within the bounds of plausibility, the consequences of attack were sufficiently unpredictable that the influence of this consideration on Soviet crisis decisionmaking ought to have been very marginal.

The ways in which command structure attack risked failure were numerous. For instance, missile submarines, which presumably would have played a central role in the strategy, did not lend themselves especially well to coordinated attacks on time-urgent targets. Cautious Soviet planners surely discounted, and heavily, their effectiveness. And even if high performance was expected of these forces, quite modest changes in assumptions about, for example, the reaction times and hardness of U.S. C^3 aircraft on crisis alert, would have drastically reduced attack effectiveness. The advantage could have easily shifted from the attacker to the defender. Furthermore, Soviet planners could not confidently predict the effects of electromagnetic pulse on U.S. C^3I equipment; the extent and duration of radio communications degradation caused by nuclear explosions in the atmosphere; the inherent range constraints and other limitations of

U.S. communications systems; and so forth. In short, attack on U.S. command structure was a gamble. Given the stakes involved, rationally calculating leaders would have exhausted all diplomatic means of crisis resolution and finally abandoned all hope for staving off general war before they would have resorted to strategic attack.

Having said this, the fact remains that U.S. command vulnerability and little else was responsible for creating a situation in which Soviet nuclear attack could have been a plausibly rational act, albeit an act of last resort. Command vulnerability was the main potential source of instability in a nuclear confrontation, and it represented a potential catalyst for intentional escalation on the part of <u>both</u> sides.

On the American side, command vulnerability was the only factor that could have seriously undermined confidence in U.S. second-strike capabilities. The uncertainties cited above as cause for Soviet doubt about the effectiveness of an attack aimed at U.S. C^3I were, under the principal of conservative planning, cause for U.S. decisionmakers to harbor fears that such an attack might actually succeed in neutralizing the American strategic arsenal. Pressures to release the forces would have mounted as hope for diplomatic resolution of the crisis waned. With diplomacy on the verge of collapse, incentives for preemption may have grown strong on both sides, despite mutual expectations that opposing forces would survive. Once diplomacy collapsed, leading to Soviet preemptive attack, pressure to unleash U.S. forces immediately upon receipt of attack detection surely would have been overwhelming.

In this respect, launch-on-warning existed long before Minuteman vulnerability pushed this dangerous tactic into the spotlight of policy debate.

Negative Control

For the period between 1966 and 1973, the unclassified literature is virtually devoid of information on safeguards against the accidental or unauthorized use of strategic weapons. It is hard to know whether negative control became more stringent or more relaxed, if it changed at all.

However, there is no gainsaying the fact that tension between positive and negative control increased. A new threat to the National Military Command System (NMCS) was emerging in the form of Soviet missile submarine deployments in the Western Atlantic. All elements of the NMCS, fixed and mobile, became increasingly vulnerable to sudden destruction, and that circumstance intensified the conflict between the two control priorities. To maintain the same degree of positive control in the face of new submarine missile threats, a relaxation of negative control would have been necessary. And vice-versa. Bolstering one meant weakening the other.

More extensive predelegation of nuclear release authority, for instance, would have reinforced positive control at the expense of negative control. This measure, if adopted, would have reduced the risk of command decapitation but increased the risk of unauthorized strikes by U.S. strategic forces. Alternative measures whose adoption would have reinforced positive control — especially, measures designed to permit higher states of command readiness to be achieved on shorter notice, and plans to mobilize strategic forces for war at a lower crisis threshold — were also bound to erode negative control. Shortened decision time; earlier and more aggressive preparations to defend against attacks; more frequent and intense encounters with opposing forces in unfamiliar circumstances, and related conditions would have run risks of miscalculation, overreaction, spontaneous escalation and accidental war. In short, steps taken to bolster positive control and deterrence would have increased the risk of producing a war that was not intended.

As noted earlier, the unclassified literature does not suggest that negative control practices were actually modified as a result of new Soviet threats to the U.S. command structure. We merely assert that the increased vulnerability raised the level of tension between the conflicting principles. The trade-off between positive and negative control became a salient feature of the strategic situation.

Ironically, the final step in the positive control process — namely, delivery of execution orders — takes care of the negative control problem. Positive control vulnerabilities created pressures to take that final step upon receipt of missile attack warning (if not before). The strategic situation thus alleviated problems of accidental/unauthorized attack because it worked to force an intentional national decision to authorize retaliation before Soviet weapons arrived.

Force Components and Strategic Stability

In the mid 1960s, an inverse relationship existed between the vulnerability of a given force component and the vulnerability of its C^3I system. Missile submarines were hard to locate and attack but easy to isolate from higher command authorities. Land missiles were more easily located and attacked but less easily isolated. Bombers ranked between the other two components in both dimensions.

This inverse relationship was even more pronounced in the early 1970s. Missile submarines still found sanctuary at sea, while bombers and land missiles, especially the latter, found themselves more exposed to attack than at any previous period. At the same time, investments in command structure had been disproportionately channeled into SAC, and as a consequence land missiles and bombers proved clearly superior to submarines in a key dimension. Although the deployment of TACAMO aircraft was arguably an impressive step toward the creation of survivable submarine communications, genuine strides toward survivable communications, as well as survivable command-control, were made by SAC. This progress derived mainly from the reorganization of the PACCS network; deployment of airborne launch control centers; construction of hardened, underground low frequency antennas at Minuteman launch control centers; and deployment of the Emergency Rocket Communications System at a strategically located missile complex in Missouri. These systems, though insufficiently robust by absolute standards, provided a degree of control over land missiles and bombers that far surpassed that which could be exercised over submarines. Command channels serving the submarine force were distinctly inferior.

Reliance on Tactical Warning

By 1973, the U.S. command structure was tremendously dependent upon early tactical warning of in-progress strategic nuclear attacks. With prompt notification that attacks, particularly submarine missile attacks, were underway, NEACP and other essential command aircraft maintained on ground alert at known, fixed locations at least stood some chance of escape. That chance was rather slight in the case of surprise attack, because the flight time of submarine missiles launched from U.S. coastal waters was generally shorter than the reaction time of command post aircraft on normal ground alert. Prompt tactical warning of surprise attack was thus insufficient by itself to ensure aircraft survival. But reliable, timely warning was still essential; in crisis and peacetime circumstances alike, tactical warning was indispensable. Without it, targeted aircraft on ground alert stood virtually no chance of safe escape. And without those aircraft, the efficacy of the airborne command system was doubtful. The two aircraft -- "Looking Glass" and a solitary TACAMO aircraft -- that were kept constantly aloft on airborne alert and thus were not dependent upon tactical warning, lacked the capability to bring U.S. retaliatory forces under effective positive control.

Policy Implications in Retrospect

Without exception, the strategic issues of perceived importance during the early 1970s concerned nuclear weapons and delivery systems: the accretion of Soviet strategic forces; the growing vulnerability of land-based missiles, particularly Minuteman; the emergence of a Soviet missile submarine threat to ground alert strategic bombers; the advent and deployment of MIRVs on U.S. Minuteman and Poseidon missiles; and the imposition of SALT ceilings and sublimits on offensive and defensive strategic deployments.

This emphasis was misplaced. In view of the continuing acute vulnerability of the U.S. strategic command structure, the size and technical composition of the U.S. and Soviet force structures scarcely deserved the attention they received. The efficacy of the command structure, not the vulnerability of Minuteman, ought to have been the focal issue.

Packard and others recognized the extreme imbalance in the state of strategic analysis and policy but effective agents of change they were not. The distorted priorities that troubled these officials stemmed from a deep-rooted perception of the strategic problem. This perception together with entrenched institutional biases thwarted major departures from established policy. Packard and his coterie could not bring about the far-reaching conceptual and institutional change necessary to produce a sensible agenda. Cognizant of their limited influence, Packard could express only cautious optimism on the occasion of his resignation: his direction "in itself won't necessarily change anything but it will focus attention on the problem." [123]

Even the attention span proved short, however. The command problem did not receive the attention it deserved until the late 1970s. In fact, the 1970s was a decade of preoccupation with force structure issues and refinement of the arcane science of force structure vulnerability. As a consequence, the condition of the command structure deteriorated, a process that culminated toward the end of the decade in a crisis of confidence in U.S. command performance. It suddenly dawned on the defense community that the price of past neglect was a deficient tactical warning system; a national command system that was enormously exposed to sudden decapitation; a communications network that could effectively, reliably reach only a fraction of deployed retaliatory forces; vulnerabilities that created a powerful incentive to launch-on-warning; and a situation that promised to get worse before it would get better.

It is ironic that the idea of flexible response extended in time was promoted during the period between Packard's resignation and the late 1970s. The command system was fraught with deficiencies that cast fundamental doubt on our operational capabilities to accomplish far simpler aims such as assured destruction, yet the fantasy of controlled, protracted strategic conflict captured the imagination of many strategists and assumed prominence in strategic policy. New demands would be imposed on a command system that hardly inspired confidence in its ability to meet minimum essential requirements.

It is also ironic that the tactic of launch-on-warning became topical only after the demise of Minuteman survivability was perceived to be imminent. Due to command vulnerability, strong incentives to use this tactic had existed for a long time.

FOOTNOTES

1. The 1970 Defense Budget and Defense Program for Fiscal Years 1970-74 (Department of Defense, 1969), p. 46.

2. See ibid., p. 47; Fiscal Years 1972-76 Defense Program and the 1972 Defense Budget (Department of Defense, 1971), p. 63; Annual Defense Department Report FY 1973 (Department of Defense, 1972), p. 67.

3. See Paul Nitze, "Assuring Strategic Stability in an Era of Detente," Foreign Affairs, vol. 54 (January 1976), pp. 207-232.

4. John Newhouse, Cold Dawn: The Story of SALT (New York: Holt, Rinehart and Winston, 1973), p. 238.

5. U.S. Congress, Senate, Committee on Appropriations, DOD Appropriations for Fiscal 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 4, p. 987.

6. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 2, p. 17.

7. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 3, p. 1463.

8. Attributed to Packard by Orr Kelly, "Ready for Doomsday," Washington Evening Star-News (February 28, 1973), p. A1.

9. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, op. cit., Part 2, p. 18; U.S. Congress, Senate, Committee on Appropriations, DOD Appropriations for Fiscal Year 1973, op. cit., Part 4, p. 510.

10. U.S. Congress, House, Committee on Armed Services, Military Posture and An Act (S. 3293), 90th Congress, 2nd Session (Washington, D.C.: GPO, 1968), p. 8684-85.

11. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 9, p. 1166.

12. Ibid.

13. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, op. cit., Part 3, p. 2028.

14. Seminal theoretical development is associated with the work of W. J. Karzas and Richard Latter, for example, "Detection of the Electromagnetic Radiation from Nuclear Explosions in Space," Physical Review, vol. 137 (March 8, 1965), pp. B1369-78.

15. U.S. Congress, Senate, Committee on Armed Services, Military Construction Authorization Fiscal Year 1977, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), p. 551.

16. The main study effort sought to produce by 1979 a data base for high altitude EMP vulnerability of the principal elements — notably, leased land-line telephone (AUTOVON) and teletype (AUTODIN) switches, military satellite ground terminals — of the Defense

Communications System. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, op. cit., Part 9, p. 1151. For a description of AUTOVON, AUTODIN, and related networks, see U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1976 and July-September 1976 Transition Period Authorization for Military Procurement, Research and Development, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), Part 1, pp. 152-53.

17. U.S. Congress, House, Committee on Armed Services, Research, Development, Test, and Evaluation Program for Fiscal Year 1971, 91st Congress, 2nd Session (Washington, D.C.: GPO, 1970), p. 8453.

18. Ibid.

19. EMP tests of an Autovon switching center conducted in 1975 reportedly caused extensive damage. William J. Broad, "Nuclear Pulse (II): Ensuring Delivery of the Doomsday Signal," Science (June 5, 1981), p. 1116.

20. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 12604, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 2, p. 10763.

21. Ibid., pp. 10746, 10751, 10762.

22. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, op. cit., p. 18.

23. U.S. Congress, Senate, Committee on Armed Services, Military Construction Authorization Fiscal Year 1977, op. cit., p. 574.

24. Interview with C.S., DCA.

25. EMP hardness fixes were incorporated into Minuteman silos beginning in 1972, with completion expected by late 1979. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6538. These fixes included the installation of a sensor to detect an oncoming and set critical circuits to a passive mode during the pulse. Surge arrestors were installed to isolate all lines that penetrated the silo. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1977 Authorization for Military Procurement, Research and Development, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 11, pp. 6485-86. Some LCC EMP hardening was also provided. U.S. Congress, Senate, Committee on Armed Services, Military Construction Authorization Fiscal Year 1977, op. cit., p. 574.

26. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 2, p. 7. One cannot fail to notice contrasts between this testimony and the milder words of Laird's Annual Report: "Our current airborne command and control system is deficient in that it lacks capacity for added communications and data processing equipment. We need to improve the survivability of the system, and to provide the more secure communications needed for control and execution of the forces." Annual Defense Department Report FY 1973, op. cit., p. 73.

27. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1968, 90th Congress, 1st Session (Washington, D.C.: GPO, 1967), Part 5, pp. 237-38; U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1970, 91st Congress, 1st Session (Washington, D.C.: GPO, 1969), Part 3, p. 668; "Electronic Systems," DMS Market Intelligence Report (September 1969), NMCS, p. 5; U.S. Congress, House, Committee on Armed Services, Research, Development, Test, and Evaluation Program for Fiscal Year 1971, 91st Congress, 2nd Session (Washington, D.C.: GPO, 1970), Part 2, p. 8058.

28. Interview, especially with R.T. Navy continued to operate its Fleet Command Ships (Little Rock and Oklahoma) as well as its AG Command Ships.

29. U.S. Congress, Senate, Committee on Armed Services, Military Procurement Authorization Fiscal Year 1964, 88th Congress, 1st Session (Washington, D.C.: GPO, 1963), p. 55.

30. Ibid., pp. 55-56.

31. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 3, p. 1973.

32. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, op. cit., Part 3, p. 1943.

33. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1973, op. cit., Part 4, p. 988.

34. Richard T. Ackley, "The Wartime Role of Soviet SSBNs," U.S. Naval Institute Proceedings, vol. 104 (June 1978), p. 36. According to Ackley, Yankee subs were patrolling the Pacific within range of CONUS by 1971.

35. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 12604, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 2, p. 10718.

36. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, op. cit., Part 3, p. 1975.

37. See "Sea-Launched Ballistic Missile Warning Net Development Set," Missiles and Rockets (January 24, 1966), pp. 16-17; Major General Otis C. Moore, "No Hiding Place in Space," Air Force Magazine (August 1974), p. 45; "Electronic Systems," DMS Market Intelligence Report (December 1968), 474N (SLBM), p. 2; Annual Defense Department Report FY 1973 (Department of Defense, February 1972), p. 75. The more advanced radar located in New Jersey to augment the basic group would be deactivated in 1974 for environmental reasons while an even more advanced OTH phased-array radar located in Florida would be activated about the same time to provide extensive coverage of the Caribbean area. Jane's Weapon Systems, AN/FPS-49 (2509.153) and AN/FPS-85 (2546.153), p. 539; Phillip J. Klass, "FPS-85 Radar Expands to Cover

SLBMs," Aviation Week and Space Technology, vol. 98 (February 19, 1973), pp. 61-66; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Appropriations for Fiscal Year 1975,vol. 93, no. 2 (Washington, D.C.: GPO, 1974), Part 1, p. 516.

38. Estimate based on Strategic Command, Control, and Communications: Alternative Approaches for Modernization (Washington, D.C.: Congressional Budget Office, October 1981), p. 10.

39. "Additional Warning Satellites Expected," Aviation Week and Space Technology (May 14, 1973), p. 17; Annual Defense Department Report FY 1973, op. cit., p. 75; Annual Defense Department Report (Department of Defense, March 1973), p. 63; Bruce G. Blair and Garry D. Brewer, "Verifying SALT Agreements," in Verification and SALT: The Challenge of Strategic Deception, William C. Potter, ed. (Boulder: Westview Press, 1980), p. 28.

40. The so-called forward-scatter radars, code-named 440L, transmitted high frequency radio waves across the Soviet land mass from foreign-based transmitters. Distant receivers detected a missile during its vertical boost through the ionosphere by measuring the resulting disturbance in the received radio signal and relaying data to NORAD. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1973, op. cit., Part 4, p. 649. An experimental system was installed in late 1965, successfully tested in 1966, further developed and expanded during 1967, and completed early 1968. U.S. Congress, Senate, Committee on Appropriations, Military Procurement Authorization for Fiscal Year

1967, 89th Congress, 2nd Session (Washington, D.C.: GPO, 1966), p. 601; U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1968, op. cit., Part 5, p. 601; Jane's Weapon Systems, Ground Radar (1948.153), p. 535; The 1970 Defense Budget and Defense Program for Fiscal Years 1970-74 (Department of Defense, January 1969), p. 64 (also, subsequent Defense Department Annual Reports); and Edgar Ulsamer, "Strategic Warning, Cornerstone of Deterrence," Air Force Magazine (May 1974), pp. 42-43.

41. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1975, 93rd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 4, p. 591.

42. U.S. Congress, Senate, Committee on Appropriations, Military Procurement Authorization, 89th Congress, 1st Session (Washington, D.C.: GPO, 1965), p. 1158.

43. Barry Miller, "U.S. Moves to Upgrade Missile Warning," Aviation Week and Space Technology, vol. 101 (December 2, 1974), pp. 17-18; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Appropriations for Fiscal Year 1975, op. cit., Part 1, pp. 116, 516.

44. A congressional report disclosed that this is a "continuing problem." As late as 1980, it was still the case that there were many satellite infrared indications of missile attack that have to be evaluated but prove not to be associated with a threatening missile launch. U.S. Congress, Senate, Committee on Armed Services, Recent False Alerts from the Nation's Missile Attack Warning System, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), p. 4.

45. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, op. cit., Part 6, pp. 1688, 1691.

46. Miller, "U.S. Moves to Upgrade Missile Warning," p. 16.

47. Estimate based on Miller's article which reports that the sensor contained 2,000 infrared elements, each capable of subtending an angle corresponding to about two square miles of surface area. Miller, "U.S. Moves to Upgrade Missile Warning," p. 18.

48. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1975, op. cit., Part 4, p. 936, and Part 7, pp. 1328-30.

49. John W. Finney, "Pentagon Seeks Funds for Radars," New York Times (December 4, 1973), p. A9; U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1975, op. cit., Part 7, p. 116; U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1975, op. cit., Part 4, p. 936.

50. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, op. cit., Part 6, p. 1691.

51. Finney, "Pentagon Seeks Funds for Radars," p. A9.

52. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1975, op. cit., Part 4, p. 935.

53. The minute BMEWs go out, a former CINCSAC once speculated, "I am liable to launch the ground alert force." U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1961, 86th Congress, 2nd Session (Washington, D.C.: GPO, 1960), Part 7, p. 76.

54. It is easy to infer from numerous sources that NORAD was a critical node for relaying all sensor data except for early warning satellite data. Apparent corroboration of this point is found in U.S. Congress, Senate, Committee on Armed Services, Recent False Alerts from the Nation's Missile Attack Warning System, op. cit., p. 3. This report notes that satellites and PAVE PAWS radars are the only two systems that feed data directly to major command centers besides NORAD. (Note: PAVE PAWS radars were not deployed until the late 1970s.)

55. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1975, op. cit., Part 4, p. 591.

56. See, for example, Alton H. Quanbeck and Archie L. Wood, Modernizing the Strategic Bomber Force (Washington, D.C.: The Brookings Institution, 1976), especially pp. 46-47.

57. U.S. Congress, House, Committee on Armed Services, Research, Development, Test, and Evaluation for Fiscal Year 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 3, p. 11054.

58. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, op. cit., Part 5, p. 1655. This testimony indicates that each command maintained those aircraft with the primary and secondary on 15- and 60-minute ground alert, respectively.

59. See Quanbeck and Wood, Modernizing the Strategic Bomber Forces, esp. Appendices.

60. PACCS refers to a network that comprises NEACP and SAC EC-135 aircraft as shown in Figure 5-6 below. Formally, PACCS excludes NEACP and the EC-135 aircraft assigned to the unified commanders. Except for "Looking Glass," discussed below, all the orbits shown in Figure 5-6 would have been occupied by EC-135 aircraft normally maintained on ground alert. See U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, op. cit., Part 5, p. 1655.

61. The existence of eight airborne stations is acknowledged in U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1976 and July-September 1976 Transition Period Authorization for Military Procurement, Research and Development, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), Part 6, p. 2751. The total number of aircraft supporting PACCS was 32 (three national command aircraft, five "Looking Glass" aircraft, nine SAC auxiliary command aircraft, nine airborne launch control aircraft and six SAC communications relay aircraft). U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, op. cit., Part 2, p. 28.

62. "The electronic and command and control equipment in the EC-135 were not designed to operate in a nuclear environment — that is, to be resistant to nuclear effects, especially electromagnetic pulse (EMP)." U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, op. cit., Part 2, p. 38.

63. L.W. Ricketts, J.E. Bridges and J. Miletta, EMP Radiation and Protective Techniques (New York: John Wiley, 1976), p. 291.

64. Ibid., pp. 291-92.

65. Ibid.

66. The history of the E-4 program, beginning in 1964, is traced in U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, op. cit., Part 3, pp. 1461-64. Packard has been given full credit for reversing past failures in having the E-4 program assigned sufficient priority for it to compete with other service priorities. See U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1973, op. cit., Part 4, pp. 986-88.

67. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, op. cit., Part 2, p. 8.

68. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, op. cit., Part 3, p. 1945.

69. U.S. Congress.

70. Operators of TACAMO, the airborne submarine communications system described below, actually filed flight plans with the proper civil aviation authorities, according to one official interviewed for this study.

71. It appears that since 1967, Soviet electronic reconnaissance satellites — ferret satellites — as well as certain communications satellites have played a role in monitoring the airborne program. It is certain, at least, that Soviet ferret satellites routinely passed over the airborne orbit shown in Figure 5-8. The "ground tracks" of

ferret satellites -- specifically, those with an inclination of 74 degrees, a period of 95 minutes, and a circularized altitude of about 340 miles -- transversed the aircrafts' operating region twice daily. The Soviets did not allow the orbit to drift away from the region during successive passes, implying strong interest in that specific region.

72. These estimates have been scaled to account for the attenuating effects of altitude on blast overpressure. For instance, the overpressure generated by an SS-9 against a target 13 miles away varies from 3 p.s.i. for a target altitude of one mile, to 1 p.s.i. for a target altitude of six miles. Against a target 9 miles away, overpressure varies from 6 p.s.i. to 2 p.s.i. for target altitudes of 1 and 5 miles, respectively.

Since the lethal radius of a single SS-9 burst is 13 miles against an aircraft flying at 32,000 feet and hardened to withstand 1 p.s.i., the probability of destroying the aircraft which could be anywhere within a 40,000 square mile expanse is 1.54 percent (.0154). The lethal radius against an aircraft hardened to 2 p.s.i. is 9 miles; the probability of destruction is .79 percent (.0079).

73. Congressional testimony recently disclosed the existence of fourteen ground entry points that the NEACP and SAC command post aircraft can use to tie into terrestrial communications channels. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization For Appropriations, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 1, p. 390. See also Figure 6-3b.

74. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1977, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 6, p. 10.

75. JSTPS deployment in a command aircraft is corroborated in U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, op. cit., Part 2, p. 47.

76. U.S. Congress, House, Committee on Armed Services, Research, Development, Test, and Evaluation Program for Fiscal Year 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 3, p. 10929.

77. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 4, p. 500.

78. Department of Defense Annual Report for Fiscal Year 1968, op. cit., pp. 397-98; U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1973, op. cit., Part 4, p. 985; U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1968, op. cit., Part 5, p. 568; U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1970, 91st Congress, 1st Session (Washington, D.C.: GPO, 1969), Part 4, pp. 862-63.

79. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1970, op. cit., Part 3, p. 1125.

80. Glasstone and Dolan, op. cit., p. 484.

81. See Chapter 6 for an assessment of LCC vulnerability in the late 1970s.

82. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1970, op. cit., Part 4, pp. 861-64.

83. Ibid., p. 864.

84. ERCS is discussed below.

85. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 13456, 89th Congress, 2nd Session (Washington, D.C.: GPO, 1966), p. 7352.

86. Department of Defense Annual Report Fiscal Year 1967 (Washington, D.C.: GPO, 1969), p. 364; U.S. Congress, Senate, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 3, p. 1462. Deployment of ground receivers at LFs probably extended past 1967; U.S. Congress, Senate, Committee on Appropriations, DOD Appropriations for Fiscal Year 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 4, p. 985.

87. Interview with USAF Lt. Col.

88. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations For Fiscal Year 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO 1980), Part 4, p. 917.

89. Ibid., p. 918.

90. Department of Defense Annual Report Fiscal Year 1967, op. cit., p. 364; Department of Defense Annual Report Fiscal Year 1968 (Washington, D.C.: GPO, 1968), p. 397. ERCS missiles have never been

fired from their operational silos and other tests of operational ERCS components have been restrictive in order to prevent enemy identification of ERCS silos. See footnote 93 of this chapter.

91. "'Looking Glass' Capabilities Improved," Aviation Week and Space Technology, vol. 104 (May 10, 1976), p. 57.

92. Interview with USAF Lt. Col.; U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 10, p. 6845.

93. The first tests of the prelaunch message playback capabilities of operational Whiteman systems were not conducted until 1976, according to a defense official interviewed. The tests revealed complete failures of the playback mechanisms associated with certain silos.

94. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 4, p. 480; General Russell E. Dougherty, "SAC Command Control," Signal (March 1975), p. 49.

95. Minuteman and B-52 forces are the only components identified in testimony as potential receivers of ERCS signals. U.S. Congress, House, Committee on Armed Services, Research, Development, Test and Evaluation Program for Fiscal Year 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 3, p. 11009. In principle, however, MEECN included ERCS and under the MEECN concept ERCS

transmissions would be used by strategic forces of all services. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations For Fiscal Year 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 4, p. 481. Recent hearings disclose that the signal from ERCS rockets flying over open ocean areas in both the Atlantic and Pacific may be received by TACAMO or by submarines directly. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 3346. This testimony notes that submarines must have antennas at the surface to receive ERCS signals.

96. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations For Fiscal Year 1981, op. cit., Part 4, p. 918; U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 5068, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 1, p. 1039; U.S. Congress, House, Armed Services Committee, Military Posture and H.R. 10929, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 3, Book 1, p. 343.

97. Interview with USAF General Officer, 1979.

98. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), Part 5, p. 2844.

99. Ibid., p. 2847. Also, see U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1975 Authorization for Military Procurement, Research and Development, 93rd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 6, p. 3225.

100. Ibid., p. 2846.

101. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 7, pp. 775-77.

102. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, op. cit., Part 5, p. 2836.

103. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 10929, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 2, p. 625.

104. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, op. cit., Part 6, p. 603.

105. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 142.

106. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1974, op. cit., Part 6, p. 603.

107. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), Part 7, p. 554.

108. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, 97th Congress, 1st Session (Washington, D.C.: GPO, 1980), Part 7, p. 4048.

109. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1976, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), Part 5, p. 903.

110. The peak power of shore-based VLF transmitters provides a suggestive comparison. The transmitter at Cutler, Maine, for example, radiated over 1,000 kilowatts, or roughly 20 times more power than operational TACAMO systems and 5 times more than a 200 kw. TACAMO transmitter under test and development. It is also important to note that antenna verticality determines signal range and seawater penetration, and achieving proper verticality using long antennas trailed from a moving platform represented no small feat. The Cutler power rating is given in U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization for Military Procurement, Research and Development, op. cit., Part 10, p. 6678. The development of a higher power TACAMO VLF transmitter and plans for its deployment (TACAMO IV program) in the mid to late seventies are disclosed in U.S. Congress, House, Committee on Armed Services, Research, Development, Test and Evaluation Program for Fiscal Year 1971, 91st Congress, 2nd Session (Washington, D.C.: GPO, 1970), p. 8053; U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973 Authorization for Military Procurement, Research and Development, op. cit., Part 5, pp.

2837, 2846-47, 2851. The 200 kw. power rating for TACAMO IV VLF transmitters was provided in U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6721. The importance of antenna verticality for signal range is noted in General Accounting Office, Report PSAD-79-48 (May 2, 1979), op. cit., p. 46.

111. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1975 Authorization for Military Procurement, Research and Development, op. cit., Part 6, p. 3311.

112. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1973, op. cit., Part 4, p. 759.

113. The fact that SSBNs operated in the Mediterranean Ocean is from U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1976, 94th Congress, 1st Session (Washington, D.C.: GPO, 1975), Part 5, p. 904.

114. General Accounting Office, Report PSAD-79-48A (May 2, 1979), op. cit., p. 28.

115. Ibid.

116. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 4, p. 650.

117. In the early 1970s, test and evaluation of TACAMO vulnerability to EMP were being planned for the mid to late 1970s. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1973

Authorization for Military Procurement, Research and Development, op. cit., Part 5, p. 2847.

118. U.S. Congress, House, Committee on Armed Services, H.R. 8390 and Review of the State of U.S. Strategic Forces, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), p. 207; General Accounting Office, PSAD-79-48A (May 2, 1979), p. 45.

119. If recent figures are any indication, the number of subs at sea was approximately 23 and of this number about 12 were on station on full alert. The number at sea but not fully alert was about 11. These estimates are based on a submarine fleet totalling 41 boats, an at-sea rate of 55 percent, and a full alert rate of 30 percent. The estimated rate on full alert is taken from General Accounting Office, Report PSAD-79-48A (May 2, 1979), op. cit., p. 2.

120. General Accounting Office, Report PSAD-79-48A (May 2, 1979), op. cit., p. 45.

121. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 146.

122. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 179.

123. Congressional Record (October 29, 1971), p. 38381.

HEADLESS HORSEMAN OF THE APOCALYPSE:

COMMAND AND CONTROL OF U.S. STRATEGIC FORCES

VOLUME II

A Dissertation

Presented to the Faculty of the Graduate School

of

Yale University

in Candidacy for the Degree of

Doctor of Philosophy

by

Bruce Gentry Blair

May 1984

PART II

INTRODUCTION TO CHAPTERS SIX THROUGH EIGHT

The two superpowers added thousands more deliverable warheads to their arsenals during the 1970s. Inventories nearly doubled between 1972 and 1979: from 5,700 to over 9,000 for the United States and from 2,200 to nearly 5,000 for the Soviet Union. Chapter 2 summarized the impact of this buildup and accompanying qualitative improvement on strategic stability. Despite the twofold increase in aggregate numbers of deployed warheads, stable deterrence still existed under the established definition. Both sides possessed large numbers of survivable forces capable of inflicting massive destruction in retaliation to attack. Because both sides possessed more survivable weapons at the end of the decade than they did at the beginning, it could even be argued that the nuclear arms buildup contributed to strategic stability.

That was not the prevalent assessment, however. By decade's end, the prevailing view was that modernization of strategic forces, particularly Soviet forces, was undermining stability. The Soviet strategic threat loomed larger than ever, and the credibility of the U.S. strategic deterrent was being very seriously questioned.

Heightened Minuteman vulnerability was generally considered to be the most worrisome consequence of Soviet weapon fractionalization and accuracy improvement. Standard calculations showed that the long expected demise of Minuteman as a survivable force component was fast becoming reality. Another worrisome implication of deepening concern to professionals concerned with strategic deterrence was the increased vulnerability of the strategic command system. Though the problem has not been ventilated nearly as thoroughly as Minuteman vulnerability has been, assessments carried out during the late 1970s exposed some grave deficiencies in the then existing C^3I network. Few of these deficiencies were new. Command vulnerability had been acute for many years. But intensive analysis had finally exposed the deficiencies and underscored their significance.

Analyses of the two problems -- Minuteman vulnerability and command system vulnerability -- were based on quite different and seemingly contradictory assumptions about Soviet attack objectives. As discussed earlier, analysts usually associate force structure vulnerability with threat of enemy blackmail. Minuteman vulnerability could translate into exploitable Soviet bargaining dominance over the United States. A prevalent "scenario" envisages a "limited" counterforce attack that takes out Minuteman and reduces U.S. options to either retaliation against Soviet urban-industrial targets, which would be irrational because it would invite attack on U.S. cities, or capitulation to Soviet demands.

Command vulnerability, on the other hand, usually is invested with enormous military significance and only marginal bargaining significance. An attack that takes out the command system might deliver a decisive military blow. Although negotiated termination on terms favorable to Soviet interests would be precluded, bargaining dominance seems a poor substitute for neutralization of the entire U.S. strategic arsenal by means of command structure attack.

A Soviet attack designed to cause maximum damage to U.S. C^3I is considered in Chapter 6. U.S. command performance will be assessed against traditional requirements: reliable detection of enemy strategic attack and timely dissemination of retaliation orders to alert U.S. forces. Although some strategists argue that the command system must be able to absorb large-scale enemy attack and still support a range of options besides massive retaliation, including graduated responses over a long time frame, Chapter 6 does not directly address this topic.

Chapter 7, however, will examine it in an indirect way. It will be assumed that Soviet attack strategy is designed to cause maximum damage to U.S. forces, with a view to achieving exploitable bargaining dominance over the United States. The extent to which U.S. C^3I would be incidentally damaged by this counterforce attack, and the implications of collateral damage for graduated, protracted war-fighting will be assessed. If the flexibility and endurance of U.S. C^3I are sufficiently degraded by collateral damage alone that a policy of flexible response could not be implemented, then it is safe to conclude that the feasibility of such a policy would be even more doubtful in the event of massive, direct attack on the U.S. command system.

Chapter 7 also examines another important issue related to force structure attack: Minuteman launch-under-attack (LUA). The feasibility of LUA will be analyzed under two different attack conditions: (1) pure counterforce attack, that is, C^3I units not struck deliberately; and (2) comprehensive attack, that is, C^3I units struck deliberately to prevent launch-under-attack.

Chapter 8 will examine major elements in the administration's command modernization program.

CHAPTER SIX

COMMAND PERFORMANCE AND MASSIVE RETALIATION IN THE EARLY 1980s

Arms competition during the past decade did not radically alter the strategic balance, if standard measures are any indication. The potential second-strike capabilities in the respective force structures actually increased in most important respects.

The U.S. command structure, however, remained defective. In fact, it became even more fragile as a consequence of Soviet strategic modernization. The resilience of aging command systems deteriorated, while new systems fielded during the period in question (early 1970s to early 1980s) generally failed to produce appreciable improvement in overall performance. At the same time, Soviet strategic modernization so greatly devalued some of the major U.S. innovations that deployment plans had to be cancelled.

Since conditions in the early 1970s were previously described in bleak terms, the thesis that conditions deteriorated during the past ten years may sound implausible. We turn next to discuss selected vulnerabilities that substantiate the point.

GROUND NETWORK VULNERABILITY

At the present time, Soviet strategic forces can quickly overwhelm virtually all ground-based C^3I elements. While few observers harbored the notion that ground elements were very survivable in the early 1970s, modern Soviet forces remove any lingering doubt. They now can obliterate those elements with greater efficiency, speed and confidence. Possessing more and technically better weapons, the Soviets have put the entire spectrum of ground C^3I sites, which were already in considerable danger a decade ago, at great risk. With several thousand additional warheads at their disposal, Soviet planners can afford to target not only the primary command centers and communication sites, but also most secondary targets such as command aircraft ground entry points and land line switching centers. The set of primary and secondary U.S. assets comprise no more than about 400 targets, including the 100 Minuteman launch control centers. With 5,000 deliverable weapons in their strategic arsenal, Soviet planners can easily commit two warheads to every U.S. C^3I target.

Sanguine: A Case of Predeployment Obsolescence

An early "casualty" of Soviet strategic modernization, the Sanguine communications system was intended to be a survivable, jam-proof shore-to-ship system for communicating with submarines. An underground grid located in the United States and composed of antennas and transmitters enclosed in concrete capsules had been designed to ensure survivability. Transmitting radio signals on frequencies below

100 cycles per second -- an extremely low portion of the spectrum, Sanguine communications would have been practically impervious to enemy jamming and virtually immune to distortion caused by nuclear explosions in the atmosphere. Signals propagated at that frequency can also penetrate water to a depth of several hundred feet before they dissipate. As a result, missile submarines could have received messages from higher authority without trailing an antenna near the ocean's surface. Among other advantages, Sanguine would have eased restrictions on speed and depth of operation. Under current technical conditions, alert submarines must operate at shallow depths and slow speeds in order to deploy antennas that allow for continuous reception of broadcast traffic. [1]

The justification made most frequently during congressional hearings during the early 1970s touted Sanguine's relative invulnerability to physical and electronic attack. Sanguine was promoted on the grounds that: (1) "the existing fixed VLF stations are not survivable," [2] (2) "today's radio signals are subject to aberration by atmospheric effects (such as sunspots and those generated by nuclear weapons) and by enemy jamming," [3] (3) "satellites are vulnerable to jamming or direct attack," [4] and (4) "the TACAMO system could be disrupted by mechanical failure, direct attack, or suffer severe range limitation in a jamming environment." [5] These and other arguments buttressed the conclusion that, "rejecting Sanguine means that we would be relying on communications which are relatively vulnerable to attack and destruction." [6]

By 1975, however, the proposition that Sanguine could survive direct Soviet attack had been invalidated. The Soviet missile program precipitated the revised assessment: " ... as the Soviet MIRVed missile threat grew, it became clear that neither Sanguine nor any other ELF transmitter would be able to survive a concentrated Soviet attack even by a small fraction of their force." [7] The promise of Sanguine thus came to naught, and with its cancellation went the possibility of finding a near-term, high confidence solution to the problem of survivable submarine communications. For the next decade, U.S. planners were instead faced with the difficult task of revitalizing TACAMO, the permissive obsolescence of which had reached an advanced stage due to the expected replacement of TACAMO by Sanguine. [8]

Emergency Rocket Communications Vulnerability

As part of a silo upgrade program implemented by SAC during the past decade, silos housing emergency communications rockets were hardened to withstand greater blast overpressure and surges of electromagnetic energy. Nevertheless, standard calculations of Minuteman silo vulnerability predict that only a small fraction of a targeted force would survive attack if Soviet planners allocated two or more weapons against each silo. ERCS missile silos located at Whiteman AFB have become equally vulnerable to Soviet ICBM attack. A three-on-one attack against the Minuteman silos at Whiteman would theoretically destroy the communications rockets (reportedly housed in eight silos) [9] along with the nuclear tipped missiles.

The questionable ability of ERCS missiles to ride out a full attack, and their equally questionable ability to safely fly out through debris and ablative dust during an attack laydown, cast fundamental doubt on its worth as a vehicle for trans- and postattack communications. It is not a highly survivable system, and that means that a critical link between higher authority and all three force components — Minuteman launch control centers, bombers in flight, and alert missile submarines (via TACAMO) — probably would not exist.

If the traditional ERCS mission cannot be fulfilled, its potential contribution to strategic communications is quite limited. The need to launch ERCS prior to enemy missile impact has been recognized,[10] suggesting that ERCS operations presently are being aligned with launch-on-warning (LOW) tactics. Even this mission could not be carried out with high confidence. As Chapter 7 explains, modern Soviet strategic forces probably could prevent ERCS LOW.

Launch Control Center Vulnerability

Underground launch control centers (LCCs), integral components of the Minuteman weapon and ERCS systems, have become increasingly vulnerable to Soviet ICBM attack. Figures 6-1 and 6-2 give estimates of the expected damage to the land missile force resulting from a Soviet attack on underground centers in 1978.[11] The calculations are based on accuracy/yield combinations given for 1978 in Figure 2-3. Soviet attack strategy allocated two high-yield, single-warhead missiles to each launch control center.[12] The attack expended 14 percent of the total Soviet land missile force.[13]

SOVIET SS-9/SS-18 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[a]

1978

Soviet Missile Reliability	Land Missile Force Incapacitated[b] (Percent of Minuteman)[c]					Land Missile Force Degraded (Percent of Minuteman)[c]
	Expected	Risk≈20%	Risk≈10%	Risk≈5%	Risk≈1%	Expected
.75	70	80	85	90	100	30
.80	80	90	95	95	100	20
.85	85	95	100	100	100	20
.90	95	100	100	100	100	5
.95	95	100	100	100	100	5

---

[a] Launch control center hardness assumed to be 500 pounds per square inch. No attack reprogramming.

[b] Blast damage only.

[c] Percent of the Minuteman force of 1,000 missiles.

Figure 6-1

SOVIET SS-9/SS-18 ATTACK AGAINST

MINUTEMAN LAUNCH CONTROL CENTERS[a]

1978

Soviet Missile Reliability	-------Land Missile Force Incapacitated[b]------- (Percent of Minuteman)[c]					Land Missile Force Degraded (Percent of Minuteman)[c]
	Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%	Expected
.75	50	60	65	75	80	35
.80	60	70	75	80	85	30
.85	65	75	80	85	90	30
.90	75	80	85	90	95	20
.95	80	85	90	90	95	20

[a]Launch control center hardness assumed to be 1,000 pounds per square inch. No attack reprogramming.

[b]Blast damage only.

[c]Percent of the Minuteman force of 1,000 missiles

Figure 6-2

The results indicate that several years ago, airborne launch control of the Minuteman missile force became essential. Without an airborne launch system, in 1978 the damage from a Soviet attack aimed at the underground centers would have been expected to exceed by a wide margin the damage from an attack aimed at missile silos.[14] And absent the airborne launch system, the effects of blast damage from an attack on underground centers would have been about as severe as the effects of blast damage projected for Soviet attack on missile silos in 1985.[15] Due to the severity of the expected damage from blast effects alone, our calculations omit possible damage from other effects such as electromagnetic pulse. It should be noted, however, that even moderate damage from those effects would have compounded the overall damage and further reduced Minuteman launch control capabilities.

Other Communications Nodes

A partial list of other ground-based communications nodes and systems that Soviet forces could rapidly destroy follows. Particular emphasis is placed on communications assets whose destruction carries implications for airborne communications.

- Ground Entry Points -- Destruction of the 14 interfaces between C^3 planes and land lines would force aircraft to make direct radio contact with other air- and ground-based units (force and C^3I units).[16]

- LF/VLF Transmitters -- Destruction of Air Force and Navy fixed LF/VLF stations, numbering about 30, would force aircraft to deploy trailing wire antennas, which are neither as powerful or reliable as ground stations, in order to reach other command aircraft, TACAMO, Green Pine sites, LCCs, and SSBNs using the LF/VLF frequency.

- HF Transmitters -- Destruction of about 50 HF transmitters would eliminate systems that otherwise provide for ground-to-air HF communications from higher authorities to TACAMO aircraft and strategic bombers. Elimination of these transmitters would not be a great loss, because HF communications are not reliable in a nuclear environment.

- ERCS -- Destruction of ERCS missiles in their silos would remove a critical link connecting command aircraft with TACAMO, strategic bombers, CINCPAC's airborne command post, and Green Pine sites.

- Green Pine Sites -- Destruction of the Green Pine network would force command aircraft to use ERCS (vulnerable), HF (unreliable), or satellite UHF radio (susceptible to jamming and scintillation) to reach forward-operating bombers.

- FLTSATCOM Ground Stations -- Destruction of two Navy ground stations used as injection uplinks for FLTSATCOM satellites would sever the FLTSATCOM path to TACAMO. Presently, TACAMO is the only FLTSATCOM equipped aircraft in the airborne C^3 network, and SSBNs are the only force component equipped to receive FLTSATCOM communications (and SSBNs cannot receive communications from any other satellite system).

- DSCS Ground Stations -- Destruction of ground stations that transmit DSCS satellite signals would eliminate all DSCS links. Presently, the E-4B is the only DSCS equipped aircraft in the airborne

C^3 network, and none of the forces are equipped to employ DSCS satellite communications.

- Satellite Control Facility (SCF) -- Destruction of a single station at Sunnyvale, California, would greatly degrade the command and control of satellites. Command aircraft are not equipped to perform the "stationkeeping" operations that maintain satellites in proper orbit, orientation, and so forth. Communications satellites could begin to fail within hours following the loss of Sunnyvale.

Other Command Nodes

The ground-based primary and alternate command centers that support national authorities, unified/specified commanders, and subordinate military commanders responsible for directing strategic operations cannot survive direct attack. Excluding Minuteman launch control centers, the number of key facilities totals about fifteen. Terrestrial communications interconnecting these facilities are equally vulnerable. Destruction of a few nodes in the terrestrial networks would disable large segments at a time. The critical vulnerability, however, lies with the command centers themselves.

Early Warning Network Vulnerability

Soviet strategic modernization increased the vulnerability of the ground segment of the early warning network. The subject is discussed in a later section on airborne command system vulnerability.

Summary of Ground Network Vulnerability

To put it bluntly, the obliteration of the ground portion of the U.S. C^3I structure is a Soviet prerogative. In the event that Soviet decisionmakers exercise this option, the United States would have to rely on available back-up systems.

At present, the sole alternative system for authorizing and implementing retaliation is the airborne command network. As is widely known, the United States has staked its second-strike threat along with deterrence itself on airborne command operations. We turn next to assess the performance of the current airborne network.

AIRBORNE NETWORK PERFORMANCE

Performance of the airborne command network — whose elements include NEACP, CINCPAC/LANT airborne compound posts, SAC airborne command posts, SAC communications relay aircraft, SAC airborne launch control centers, and TACAMO submarine communications relay aircraft — depends upon (1) prelaunch vulnerability, (2) postlaunch vulnerability, and (3) communications effectiveness within the network and between the network and force components.

At the outset, it is important to note that Soviet strategic modernization has adversely affected virtually all aspects of airborne command operations. Aircraft would operate today in conditions that are unprecedented in terms of the level of possible fallout, turbulence, dust and other hazards encountered while airborne. And the degree to which the atmosphere — the transmission medium of strategic communications -- could be disrupted by nuclear effects has never been greater. Armed with 5,000 deliverable strategic nuclear weapons, the Soviet Union presently possesses a tremendous capacity for producing an extremely adverse environment for aerospace vehicles and aircraft radio communications.

Prelaunch Survival

Command and communications aircraft maintained on ground alert in the United States (including Hawaii) and Bermuda can be targeted by a larger, more modern Soviet submarine force than was the case in the early 1970s. Deployed Yankee submarines are more numerous and better-armed -- with SS-N-6 missiles that can launch multiple warheads at longer range (1,600 nautical miles).[17] In addition, the Soviets have deployed 33 Delta-class missile submarines since the first of its kind entered service in 1973.[18] The long-range SS-N-8 and SS-N-18 missiles carried by Delta submarines can reach targets as far away as 4,300 nautical miles, and SS-N-18 missiles can carry MIRVed warheads.[19]

General Ellis, the then CINCSAC, testified in 1979 that the SS-N-6 missiles on board Soviet Yankee submarines patrolling off U.S. coasts were suited for attacks on soft C^3 sites.[20] According to Ellis, these missiles could be ready for launch within 15 minutes of the launch order and all could be launched within the next two minutes.[21] The testimony also suggests that Soviet missile submarines have made bold deviations from their routine patterns of patrol;[22] that normal deployment rates allow for a sizable attack; and that increasing deployments of MIRVed SS-N-18 missiles have expanded their coverage of U.S. targets.[23] Although Delta-class submarines primarily patrol in the Barents and Norwegian Seas,[24] it would be safe to assume that these could occasionally be positioned for short range attack. It also seems safe to assume that at least five Yankee submarines would be patrolling near U.S. coastal waters at the time of an attack.[25]

If these are reasonable assumptions, then it is not implausible that one-half of the 400 primary and secondary strategic C^3I targets could be struck by Soviet missiles submarines on routine patrol. Of these targets, NEACP on ground alert at Andrews AFB would be among the most lucrative and most vulnerable. Even if enemy submarines fired from positions near Bermuda, where they have been observed in the past,[26] the flight time of the SS-N-6 missile over the 800 nm. distance would be shorter than the time required for NEACP to safely escape the base (12-13 vs. 14-15 minutes).

The recent replacement of EC-135 aircraft with E-4 aircraft did not mitigate this particular vulnerability. To the contrary, the prelaunch vulnerability of an E-4 aircraft is somewhat greater than the EC-135 it replaced.[27] The recent relocation of NEACP to an inland base (Grissom AFB, Indiana), however, does substantially improve its chances of survival.

Many other elements of the ground alert airborne command network are comparably vulnerable. The flight time of Soviet missiles launched from typical patrol stations in the Atlantic and Pacific is shorter than the 15-minute escape time of CINCLANT's command aircraft (based in

Virginia), CINCPAC's command aircraft (based in Hawaii), and TACAMO ground alert aircraft (based in California, Hawaii, Bermuda and/or Maryland). Furthermore, many ground alert aircraft in the PACCS network could be destroyed if only a small number of Yankee submarines crept within several hundred miles of the U.S. coasts prior to launch. Such movements might not be detected; and, detection would not necessarily trigger an increase in aircraft readiness. In such circumstances, Soviet submarines would jeopardize the survival of NEACP when based in Indiana. They would also threaten the following PACCS aircraft: communications relay aircraft based at Rickenbacker AFB, Ohio and Grissom AFB, Indiana; auxiliary airborne command posts based at Offutt AFB, Nebraska and Ellsworth AFB, South Dakota; and launch control aircraft based at Ellsworth AFB and Minot AFB, North Dakota. In sum, a surprise Soviet attack aimed at ground alert elements of the U.S. airborne command network poses a considerable threat. Conservative U.S. planners cannot count on the survival of any ground alert aircraft.

Measures that might be taken to protect aircraft during periods of heightened tensions range from dispersal/increased readiness to airborne alert. These measures should be generally effective against current Soviet forces. However, any "generated" posture short of full airborne alert is only as sound as the tactical early warning system upon which aircraft depend for their survival. Since the sensors, rearward communications (to command centers), and forward communications (from command centers to alert aircraft) designed to support a positive control launch of command aircraft are generally lacking in resistance to nuclear weapons effects [28] (they primarily consist of dedicated or leased land lines that may temporarily cease to function with the first high-altitude explosion designed to generate EMP), aircraft could react too slowly to survive attack. Such an event could occur a scant few minutes after the first enemy submarine missile is fired. [29] SS-N-6 missiles launched from a submarine stationed in U.S. coastal waters could be detonated four or five minutes after breakwater, during the upward part of their trajectory. These precursor attacks would blanket the United States with a high voltage EMP pulse that could so severely disrupt land line communications that orders from SAC Headquarters authorizing the launch of PACCS aircraft, and orders from national command centers authorizing the launch of NEACP, might not get through. In fact, rearward communications might be disrupted by EMP before sensor data could be transmitted to the authorizing command centers. In the resulting confusion, ground alert aircraft, regardless of their state of readiness, would be subject to destruction by follow-up SLBMs and perhaps even ICBMs.

Precursor EMP attacks could also directly damage aircraft on the ground or in the air. None of the PACCS EC-135 aircraft are protected against EMP. [30] In fact, there exists only two command post aircraft — the two E-4Bs currently assigned to NEACP — that are "hardened" against EMP effects. [31] Thus, the EC-135 airborne command posts operated by CINCPAC and CINCLANT as well as SAC are subject to damage from EMP effects. All EC-135s are exposed to this danger. [32] TACAMO aircraft, too, lack protection from EMP. [33]

Summary Assessment of Prelaunch Survival: During the past decade, the vulnerability of command aircraft has not been remedied. Although during this period the United States became totally dependent upon airborne command channels to execute a retaliatory strike, the basic vulnerabilities that existed in the early 1970s still exist. Surprise attack, or failure of tactical early warning, probably would result in the destruction of most aircraft on ground alert. Given the substantial increase in the number of Soviet submarine deployments during the period, the threat to ground alert command aircraft is undoubtedly greater.

Postlaunch Vulnerability

Command aircraft that manage to evade destruction on the ground, or that assume an airborne posture during a crisis, are not out of danger. They may still encounter many hazards. Besides EMP, the airborne network, particularly the network elements that operate in U.S. airspace, must deflect the direct and indirect effects of a nuclear attack of almost unimaginable proportions.

Among the major hazards are radioactive fallout, severe turbulence, and dust clouds.[34] Aircraft that encounter heavy concentrations of any of these unnatural phenomena would be quickly disabled.

Damage resulting from any or all of these hazards defy exact calculation, as the responsible agents are variable and largely unpredictable: number and yield of attacking weapons; target coordinates of Soviet weapons; height of weapon bursts; fission-fusion ratio of weapons; weather conditions; location and flight profile of command aircraft; and so forth. Accurate prediction depends on knowing conditions that are practically unknowable.

It is safe, nonetheless, to say that lethal conditions might exist. We can postulate a set of plausible targets and relate them to certain plausible conditions. For instance, we expect Minuteman missile complexes to be prime targets, and we can confidently predict that an attack on these complexes would use ground bursts. We know, furthermore, that multiple ground bursts would produce high levels of radioactivity, turbulence and dust in the vicinity. We also know that many command aircraft, particularly ALCC aircraft, would fly in the general vicinity of the attack and at some point they would position themselves within about 150 miles of the Minuteman complexes in order to establish line-of-sight communications with launch control centers and/or silos.

Though aircraft presumably would be assigned orbits that are expected, on the basis of wind pattern history, to be upwind from the target complex, there is always an irreducible, significant risk that unusual (not necessarily aberrational) weather would blow fallout in the wrong direction. The dose administered could easily be lethal to the crew. If the chance of exposure to unacceptable levels of radioactivity (about 200 rads) is only 10 percent on average per orbit, then the chances are greater than even (57 percent) that at least one of the eight crews in the PACCS airborne network would be incapacitated. The risk that at least two crews would be incapacitated is 19 percent. A small (4 percent) risk exists that three crews would receive a lethal dose.

Lethal turbulence can persist for ten minutes over a distance of ten miles or more following a high-yield nuclear explosion. Though aircraft would presumably follow routes that circumvent high risk areas such as Minuteman complexes, the boundaries of their assigned orbits would undoubtedly encompass many other designated ground zeros (DGZs); and, random flight profiles within those boundaries would be hazardous. Chance destruction of aircraft by turbulence is not a remote possibility.

Dust ingestion by aircraft engines also could destroy an aircraft or cause the sortie to be aborted. The experience of aircraft — a DC-9, C-130 transport, and two 727s -- that flew through the volcanic dust cloud produced by the Mt. St. Helen's eruption suggests that this problem is potentially severe.[35] It is reasonable to expect an engine to be damaged within about one hour when the density of dust ingested is about 10 mg per cubic foot, and it is reasonable to expect that the ingestion rate of some command aircraft would be that great following a large-scale nuclear attack involving thousands of ground bursts. The density of dust in the cloud of a single 200 kiloton surface burst is estimated to be about 5 mg per cubic foot; an aircraft that repeatediy flies into clouds of that density evidently could be disabled within two hours.

Summary Assessment of Postlaunch Vulnerability: All command network aircraft in the active inventory, except for two E-4B aircraft, lack adequate protection from EMP effects. In this respect, the past decade saw no significant improvement in the survivability of the airborne network. In other respects -- notably, vulnerability to radioactivity, turbulence and particulate matter -- the survivability of command aircraft decreased due to the twofold increase in the number of Soviet nuclear weapons that could be used against the United States.

Postlaunch Communications Performance

Evaluation of communications capabilities within the airborne command network and between this network and force elements begins with the observation that support from ground-based facilities and transmission media would be marginal, at best. Ground-based support systems could be degraded by EMP within several minutes of the launch of the first enemy missile. Following on the heels of this disruption would be blast destruction of many primary command centers and communications sites/lines. Follow-up attacks by ICBM warheads would result in wholesale destruction of primary, secondary and tertiary systems. Virtually all ground support could be lost in the first hour. Such, at any rate, is the possible consequence of a dedicated C^3I attack by modern Soviet forces.

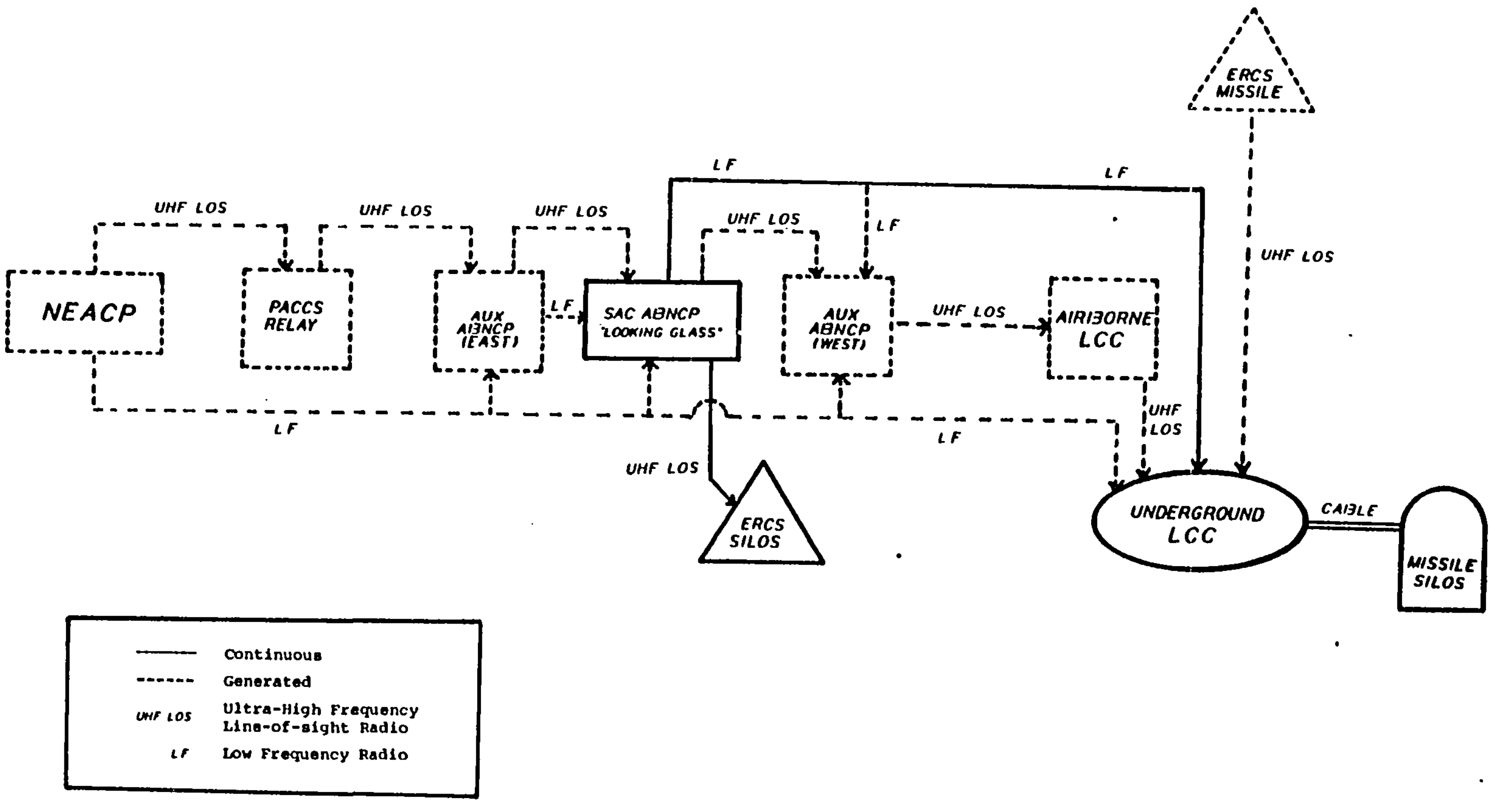
Airborne Communications: Under the weight of enemy nuclear attack, strategic communications would collapse to airborne channels. Potential airborne channels are depicted in the flow diagrams below. Their establishment partially depends upon the disposition of C^3 aircraft at the time of enemy attack. Two cases (dispositions) are considered: (1) day-to-day, with aircraft at normal levels of readiness; and (2) generated, with aircraft at peak readiness (airborne alert).

Satellite radio links are excluded from this assessment of airborne communications. A later section is devoted to this subject. It is shown that satellites currently used for strategic communications would make only marginal contributions to airborne force management.

High frequency (HF) radio links are also omitted from the diagrams. This frequency, as noted earlier, is not expected to function in a nuclear environment. There would be massive absorption of HF energy, resulting in HF blackout for tens of hours.

A. Minuteman Forces: The primary path running from higher authority to Minuteman forces consists of UHF transmissions among airborne units within line-of-sight of each other (see Figure 6-3a). End-to-end communications involves a large formation of PACCS aircraft in series (see Figure 6-3b).

This aerial chain is only as strong as its weakest link. Loss of any given link would break the chain, forcing aircraft to activate back-up channels — namely, LF/VLF or HF radio. These back-up channels provide for long distance communications to bridge gaps in UHF line-of-sight coverage. But they are far less reliable than UHF.



AIRBORNE NETWORK MINUTEMAN COMMUNICATIONS

Figure 6-3a

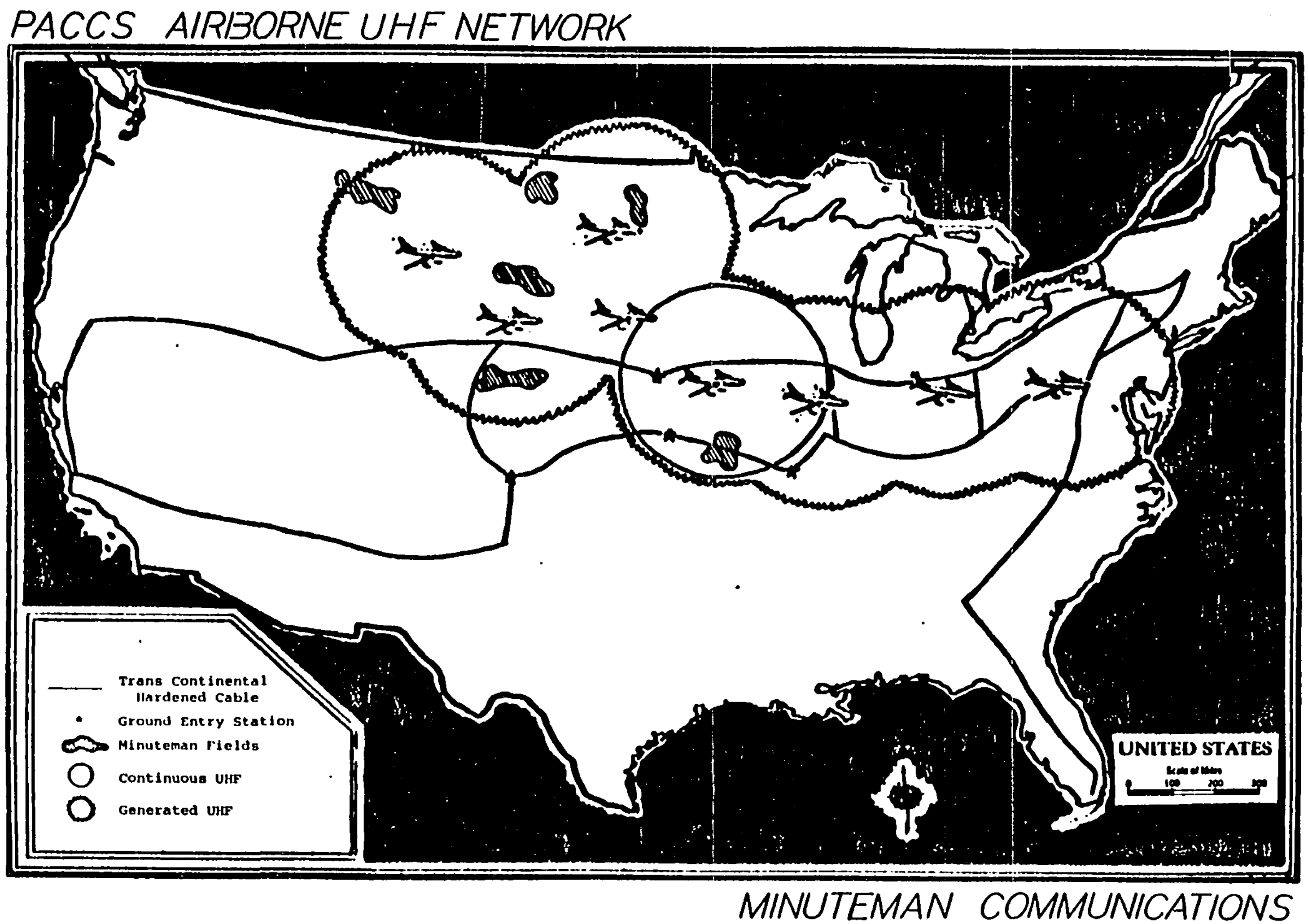

PACCS AIRBORNE UHF NETWORK
Trans Continental Hardened Cable
Ground Entry Station
Minuteman Fields
Continuous UHF
Generated UHF
UNITED STATES
MINUTEMAN COMMUNICATIONS

Figure 6-3b

Loss of one or more aircraft links in the UHF chain is likely to result if surprise attacks occurs. Under day-to-day conditions, the reaction time of C^3 aircraft on ground alert could be longer than the flight time of Soviet submarine missiles. Illustrative examples of the implications of such losses for communications with Minuteman forces are given below.

Loss of NEACP. All Minuteman forces would be isolated unless nuclear release authority resides with SAC's "Looking Glass" commander or other subordinate military commanders.

Loss of PACCS Relay Aircraft. Destruction of either relay aircraft based in Indiana and Ohio would disconnect NEACP from SAC unless LF/VLF communications could be established. Jamming, EMP, atmospheric disruption, trailing wire antenna breakage, and other problems prevent high confidence communications with "Looking Glass" and Minuteman launch control centers on the ground. Direct transmission to Minuteman launch control centers would be as doubtful, and, in fact, even less certain since the centers themselves are subject to attack (see p. 375).

Loss of Airborne Launch Control System Aircraft. Destruction of missile launch aircraft on ground alert in North Dakota and South Dakota would isolate the bulk of the Minuteman forces unless "Looking Glass" could establish LF/VLF communications with launch control centers on the ground.

For reasons given above, high confidence communications would not exist. Using UHF line-of-sight radio, "Looking Glass" could reliably reach surviving launch control centers at the Minuteman complex in Missouri, and could use its airborne launch control equipment to fire isolated Minuteman missiles at that complex.

Under generated conditions, reliable communications with Minuteman forces should be possible unless various airborne hazards -- EMP, radioactivity, dust, turbulence -- cause damage to radio equipment or the aircraft themselves. No one knows the extent of the damage that would be suffered. Conservative planners could reasonably expect that a sizable portion of the Minuteman force would be isolated as a result of this damage.

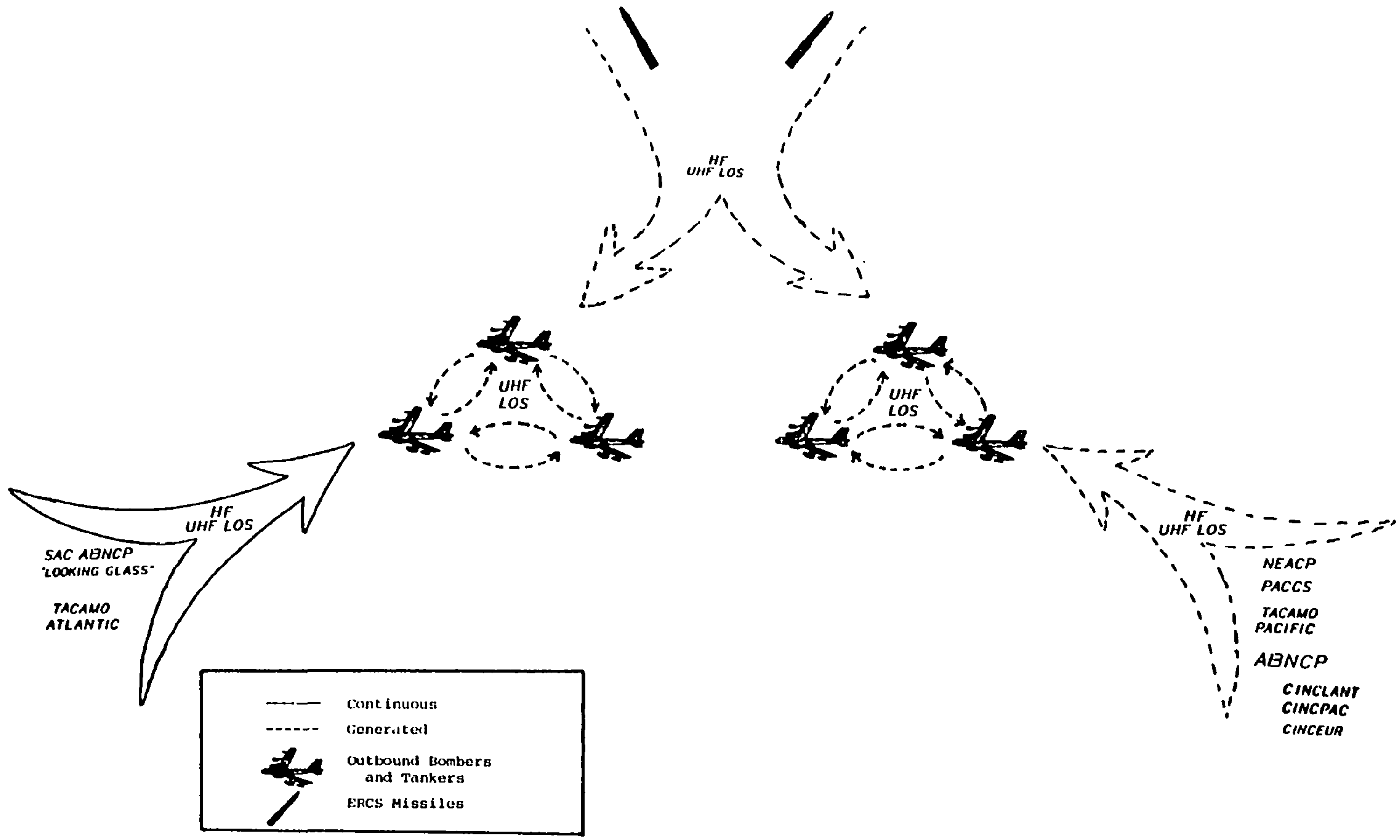
In both cases -- day-to-day and generated -- airborne communications with Minuteman forces would cease within a few hours, due to limitations on aircraft endurance. Conservative planners would heavily discount tanker support to extend aircraft endurance. Refueling, _if_ successful, could increase the endurance of some aircraft -- especially, NEACP and "Looking Glass" -- to a point where HF and satellite communications might be restored. It is possible, though not probable, that some aircraft would still be airborne when atmospheric healing permits restoration of these radio communications.

B. Strategic Bomber Forces: Airborne communication with bombers continues to be problematical. As depicted in Figure 6-4a, message delivery heavily depends upon ERCS and UHF line-of-sight relay. Both channels are transient and tenuous.

UHF radio provides a reliable link with outbound bombers that fly within line-of-sight range of "Looking Glass" and other PACCS aircraft (see Figure 6-4b). Several factors, however, impose sharp constraints on the utility of this link:

> Loss of C^3 aircraft. Destruction of C^3 aircraft would shrink the area of UHF coverage. In the worst case -- surprise attack destroys C^3 aircraft on ground alert -- the UHF envelope would be reduced to the area around "Looking Glass," or a circle of 400 miles radius with "Looking Glass" at its center.

> Timeliness of Decision to Retaliate. Outbound bombers quickly fly out of UHF radio range. Even aircraft based in the south would fly out of range within about three hours after takeoff. If a prompt decision to retaliate is made, most bombers stand a good chance of receiving the orders either directly from C^3 aircraft or from bombers/tankers following behind. If the decision is delayed, the forces would put great distances between themselves and C^3 aircraft, reducing the timeliness and effectiveness of UHF relay through other bomber/tanker units. Bombers loitering at



AIRBORNE NETWORK BOMBER COMMUNICATIONS

Figure 6-4a

PACCS AIRBORNE UHF NETWORK BOMBER COMMUNICATIONS

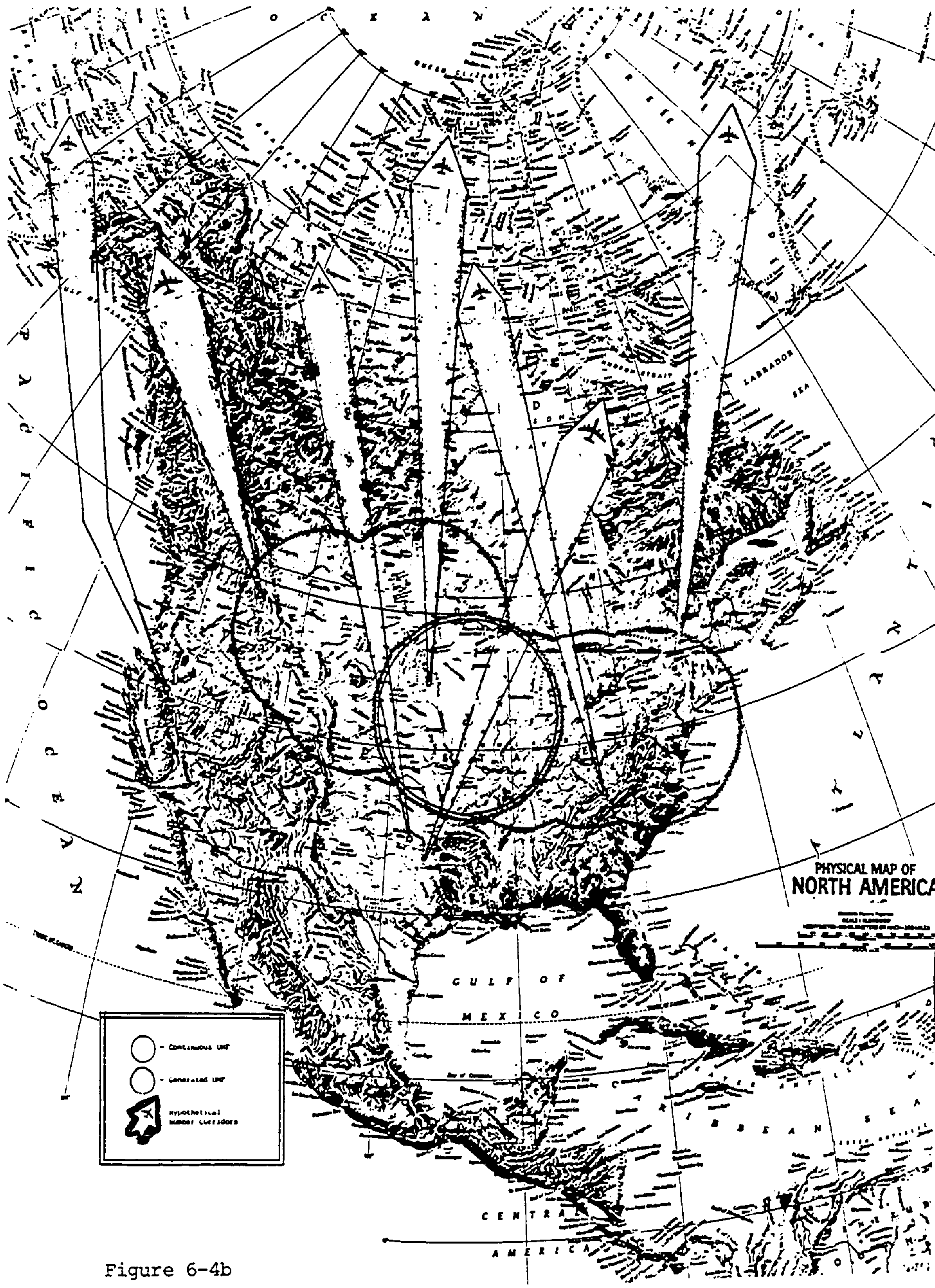


Figure 6-4b

their positive control turnaround points, waiting for other bomber/tankers to bring the orders, may fail to receive the message in time to complete their assigned mission.

In the event of surprise attack, and the destruction of NEACP on the ground at Andrews, the decision to retaliate probably would not be made promptly.

Loss of Bomber/Tanker Units. Destruction of bombers and tankers on ground alert would reduce the effectiveness of UHF line-of-sight relay and hands-off.

Emergency communications rockets represent an alternative means of reaching the dispersed bomber forces. It is an especially important link if the decision to retaliate is delayed. Well before bombers have arrived at their loiter orbits outside the Soviet Union, the UHF line-of-sight channel would be overextended and tenuous. By this time, however, ERCS deployments would have been massively attacked. Even if the rockets survived and were successfully launched, communications over this channel would be fleeting and tenuous.

The short-lived character of both channels -- UHF LOS relay and ERCS -- puts pressure on decisionmakers to commit the bomber force quickly and massively, lest severance of these channels isolate the force from authoritative direction.

C. Submarine Missile Force: Communication with missile submarines still critically depends upon TACAMO aircraft, whose capabilities apparently do not impress even the Navy's Chief of Naval

Operation (CNO). Not mincing words, the CNO stated flatly in 1981 that " ... the most serious deficiency in the Navy's strategic nuclear pasture, in my judgment, is the lack of reliable, survivable communications with SSBNs at sea." [36]

The single-thread TACAMO channel nearly disappeared during the 1970s, owing to anticipation at SANGUINE deployment. Between 1971 and 1979, the Navy drew down the Pacific-based fleet until only one aircraft was left, in order to maintain continuous airborne operations in the Atlantic basin. [37]

The Navy has since doubled the inventory of TACAMO aircraft. Plans call for continuous airborne alert in both ocean areas by the end of 1983, coinciding with the buildup of Trident submarine deployments in the Pacific. [38] At the same time, TACAMO aircraft have been equipped with an improved communications suite. The Navy has installed a jam-resistant, high power (200 kw.) transmitter on each aircraft, extending the effective communications range between TACAMO and U.S. missile submarines. TACAMO aircraft now can operate close to CONUS and still maintain reasonably good communications to far-flung alert missile submarines.

This range extension coincidentally alleviates the problem of delivering the message to TACAMO. In the 1970s, a severe trade-off existed between TACAMO-to-submarine communications and higher authority-to-TACAMO communications. Ideally, TACAMO could receive the message and immediately relay it to submarines. In practice, TACAMO was either "on station" to receive or "on station" to transmit. While this trade-off still exists, the problem is less severe, especially under generated conditions. As Figure 6-5 indicates, the primary path to TACAMO Atlantic runs from NEACP through CINCLANT's airborne command post. This LF radio link probably could be established if a TACAMO aircraft is operating in the Western Atlantic, and TACAMO retransmissions probably could be received by most alert submarines in the Atlantic Ocean. Additional TACAMO aircraft could be generated in a crisis to reinforce the linkage; TACAMO-to-TACAMO relay would provide greater assurance that the most distant submarines would copy.

Uncertainties that reduce confidence in TACAMO performance include the following:

> <u>EMP Damage to Communications</u>. Trailing wire antennas used in conjunction with LF/VLF communications are prime collectors of EMP energy. Damage to sensitive electronic components could result, impairing LF/VLF communications.

> <u>Loss of NEACP and/or CINCLANT ABNCP</u>. Under day-to-day conditions, surprise attack might destroy all but SAC's "Looking Glass" aircraft and the Atlantic-based TACAMO aircraft flown on 24-hour airborne alert. High confidence LF radio communications from "Looking Glass" to TACAMO does not exist, even when TACAMO is operating in the Western Atlantic. Furthermore, destruction of back-up ground alert TACAMO aircraft would reduce the likelihood that all alert submarines in the Atlantic would copy a message transmitted by a single TACAMO stationed in the Western Atlantic.

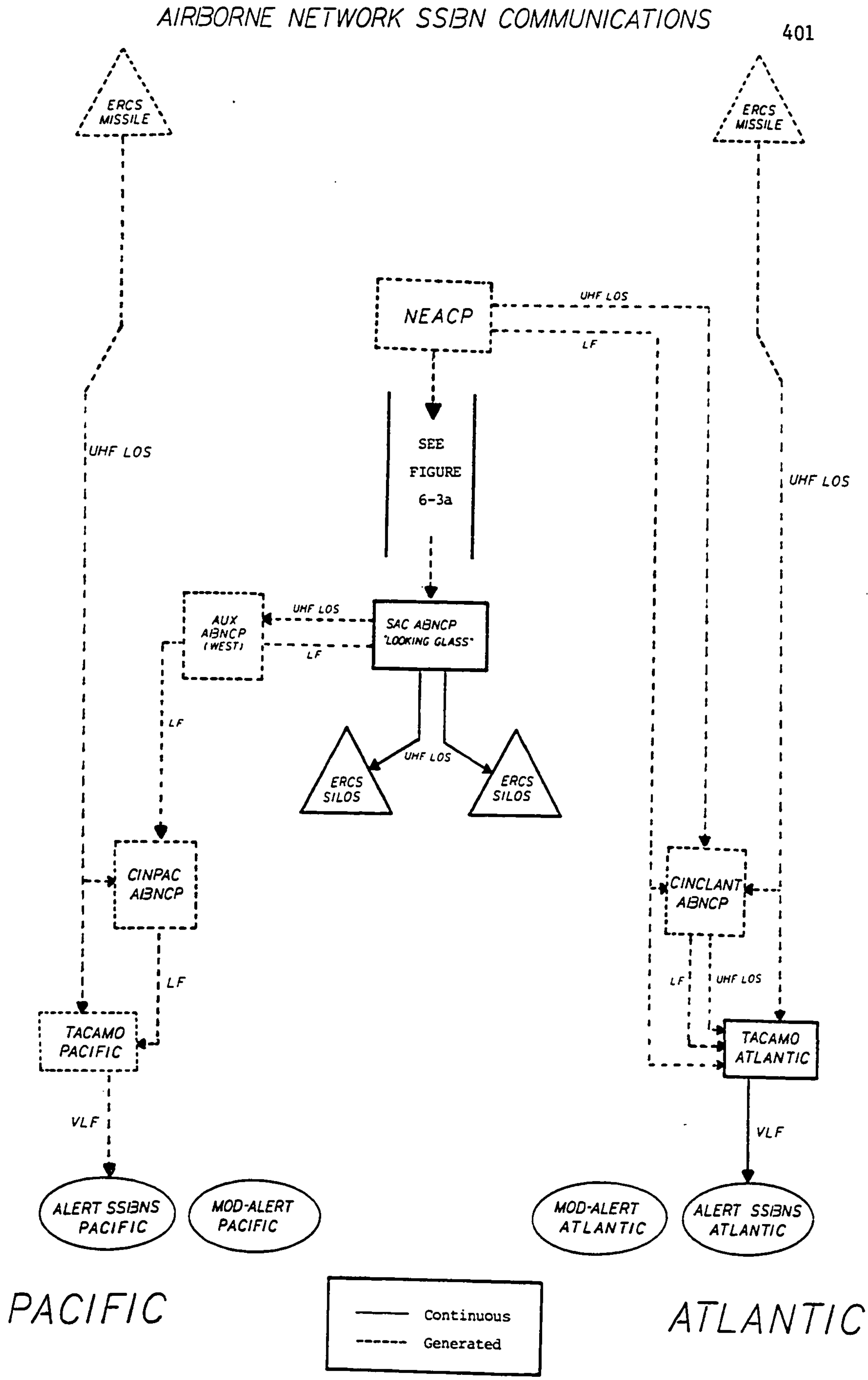

AIRBORNE NETWORK SSBN COMMUNICATIONS
ERCS MISSILE
ERCS MISSILE
NEACP
UHF LOS
LF
SEE FIGURE 6-3a
UHF LOS
UHF LOS
AUX ABNCP (WEST)
UHF LOS
LF
SAC ABNCP "LOOKING GLASS"
LF
UHF LOS
ERCS SILOS
ERCS SILOS
CINPAC ABNCP
CINCLANT ABNCP
LF
LF
UHF LOS
TACAMO PACIFIC
TACAMO ATLANTIC
VLF
VLF
ALERT SSBNS PACIFIC
MOD-ALERT PACIFIC
MOD-ALERT ATLANTIC
ALERT SSBNS ATLANTIC
PACIFIC
Continuous
Generated
ATLANTIC

Figure 6-5

Short Endurance of TACAMO. Since TACAMO aircraft cannot be refueled, endurance could be as short as a few hours, depending on the fuel supply on board at the time of attack. Delay in the decision to retaliate could result in the loss of TACAMO support and the isolation of the alert submarine force.

Communications Posture of Submarines. Under day-to-day conditions, off-alert and mod-alert submarines at sea do not monitor communications on a continuous basis. Such submarines could fail to copy the execution broadcast regardless of its source.

In the Pacific, the risk is greater that submarines would be isolated, even under generated conditions. The primary path of communications runs from NEACP through SAC PACCS aircraft to TACAMO PACIFIC and CINCPAC's airborne command post (see Figure 6-5). The LF channel used for this purpose does not offer high assurance of successful dissemination.

Emergency communications rockets offer a potential means of reaching Pacific-based C^3 units, as well as a redundant channel of communications with Atlantic-based C^3 aircraft. ERCS, however, does not offer a high confidence link, for reasons discussed earlier.

In sum, communications with missile submarines are problematical under a wide range of plausible circumstances. A large number of them could be immediately isolated if day-to-day conditions prevail. All would be isolated within a matter of hours, regardless of the circumstances, because TACAMO endurance is very short. Despite the long endurance of the submarines themselves, the short-lived character of their supporting communications puts pressure on decisionmakers to commit the submarine force quickly and massively. In this respect, the submarine force is like the bomber force.

Satellite Communications: The above analysis completely discounts the contribution of satellites to strategic communications. Many observers, such as W. J. Perry, former Under Secretary of Defense for Research and Engineering, share this pessimistic assessment:

> I see very significant command and control problems with all three legs of the Triad in that I do not envision that our fixed ground-based systems or our satellite systems would survive an attack.... In terms of enduring for a month or a week or even an hour after an attack, we become essentially dependent on our airborne systems, those that survive an attack. That problem is really common to the three legs of the Triad.[39]

Conservative Soviet planners, however, probably credit the United States with a significant capability for satellite communications with strategic forces. Current force deployments as well as C^3 aircraft are equipped with satellite receivers, and strategic communications satellites are fully operational at the present time. The capabilities and vulnerabilities of the operational systems deserve careful consideration.

A. Background: The first successful military satellite communications program -- called IDCSP -- was conceived in 1963 and put into operation in 1966. IDCSP was the forerunner of the Defense Satellite Communications System (DSCS) managed by the Defense Communication Agency (DCA). DSCS satellites were first launched in November 1971. DCA's mandate, and the purpose of its DSCS satellites, are to provide two-way, long-haul communications between national command centers and distant military headquarters. DSCS satellites now provide this capability using super high frequency (SHF) channels. The principal links interconnect Washington and the ground headquarters of overseas unified commands -- CINCPAC and CINCEUR.

A major disadvantage of current generation SHF satellite systems is that large terminals and antennas are required. Aircraft, except for jumbo-sized vehicles such as the E-4 airborne command post, cannot accommodate the heavy, bulky equipment. Using current technology, exploitation of SHF satellite communications by EC-135 command aircraft, strategic bombers and other small, mobile units such as missile submarines is impossible or impractical.

Terminals and antennas used in conjunction with UHF satellites can be built small. Recognizing the vast military applications of UHF satellites, the DoD conducted a series of experiments in the 1960s. In 1965, Lincoln Experimental Satellites (LES) demonstrated the feasibility of UHF satellite communications. The success of IDCSP generated more interest, and by 1970 a major military experimental program known as TACSAT had proved the usefulness of UHF satellites for military purposes. In the early 1970s, TACSAT UHF terminals were installed on some EC-135 command aircraft. Using a transponder carried by LES-6, an experimental satellite launched into geosynchronous orbit in 1968, EC-135 command aircraft could for the first time communicate with other airborne command posts via satellite.

Extensive use of UHF satellite communications did not occur until 1976, when the Navy leased the UHF portion of three Communications Satellite Corporation (COMSAT) satellites launched in 1976. (The program was called Gapfiller; the satellites were called MARISATs.) Each of the three satellites provided a wide-band UHF channel (500 Khz), and two narrow-band channels (25 KHz). By the end of the 1970s, 99 percent of the Navy's fleet (some 430 ships including missile submarines) could copy fleet broadcast messages transmitted from shore over Gapfiller's narrow-band channels.

Due in part to the degradation of LES-6 power, the Navy granted the national and unified/specified command aircraft access to its Gapfiller wide-band channel. Because the Gapfiller satellites were positioned to give maximum oceanic coverage for Navy operations, leaving a gap in coverage over the continental United States, only NEACP and the CINCLANT airborne command post could be connected.

The national command authorities also could use LES-9, an experimental satellite, launched in 1976, which became part of the MEECN network. LES-9 provided limited, operational UHF communications between NEACP and CINCLANT, CINCPAC, and CINCSAC airborne command posts.

The key satellite program designed specifically for strategic communications achieved initial operational capability in 1979. The space segment of this MEECN component -- known as Air Force Satellite Communications (AFSATCOM) -- consists of UHF radio equipment (transponders) on board "host" satellites. At the present time, AFSATCOM is merely a set of communications devices on: Satellite Data System (SDS) satellites; Fleet Satellite Communications (FLTSATCOM) satellites (the follow-up to Gapfiller); and certain classified satellites.

The operational ground and airborne segment of AFSATCOM mainly consists of terminals at major military command headquarters; terminals on most B-52 bombers; terminals on E-4 and EC-135 command aircraft; terminals at Minuteman launch control centers; and terminals on EC-130 TACAMO aircraft. Missile submarines are not equipped.

The Navy's FLTSATCOM satellites carry the AFSATCOM equipment required for communications coverage of most ground and airborne locations (see Figure 6-6). All four satellites depicted in Figure 6-6 are now "parked" in geosynchronous orbit. The constellation provides worldwide coverage except in the polar regions. Two SDS satellites in elliptical polar orbits provide coverage for strategic bombers at the extreme northern latitudes.

B. Satellite Vulnerabilities: The effectiveness of AFSATCOM appears to be very doubtful. A partial list of deficiencies includes the following:

AFSATCOM

COMMUNICATIONS COVERAGE

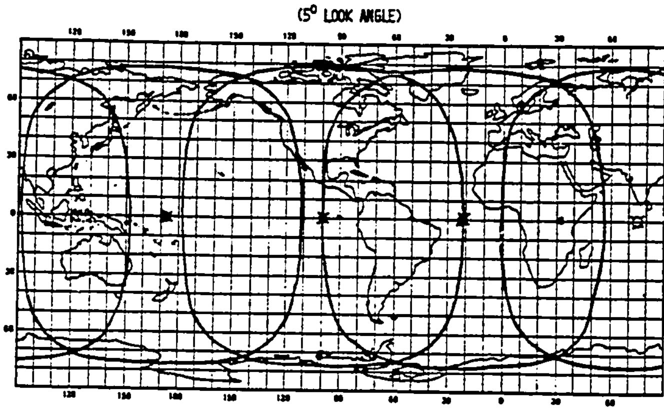


Figure 6-6

1. UHF Signal Absorption and Scintillation: AFSATCOM links to ground and airborne terminals are subject to severe degradation caused by signal absorption and/or scintillation. A small number of high-altitude nuclear explosions can negate AFSATCOM communications for long periods. According to then Assistant Defense Secretary Dinneen, testifying in 1979:

> ... many of our communications satellites' links are blocked out because if they explode a nuclear bomb in the atmosphere that blacks out ultra high frequency communications to the satellites ... we could not depend on the communications satellites because ... blackouts in UHF last for a long period of time.... [40]

Absorption effects produced by a single high-altitude explosion can black out UHF satellite communications for nearly an hour, but the affected region is relatively small -- about 200 miles in diameter. Scintillation effects, on the other hand, can persist for many hours over large areas (see Figure 6-7). By altering the electron density of the ionosphere, a single high-altitude burst could induce sufficiently large fluctuations in signal amplitude and phase that reception would not be possible throughout most of the North American Continent. Multiple ground bursts would cause comparably extensive and persistent scintillation problems.

As in the case of EMP effects, scintillation phenomena were belatedly recognized as a threat to critical elements of the MEECN network. Contrary to initial expectations, the performance of UHF satellites is very sensitive to disruption of the ionosphere from nuclear explosions.

AREA OF INTENSE SCINTILLATION
(30 MINUTES AFTER SINGLE NUCLEAR EXPLOSION)

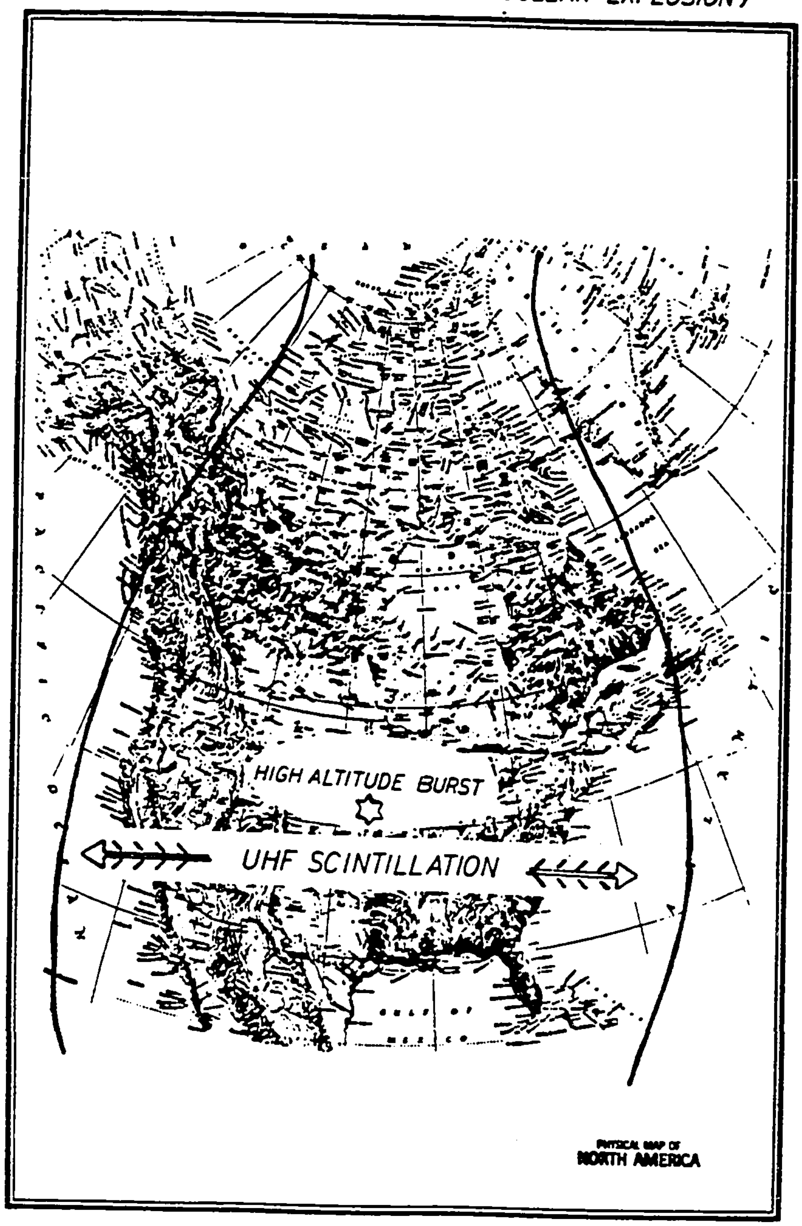


Figure 6-7

2. Jamming: AFSATCOM is also very susceptible to jamming. This threat has long been known. It is widely recognized that the jamming of communications satellites is "the greatest threat," the "easiest thing for them [the Soviets] to do." [41]

AFSATCOM is said to possess "modest" antijam features. [42] At present, it is more vulnerable to jamming than is DSCS II (E-4B aircraft are the only DSCS II-equipped elements in the airborne command network), which itself is "easily jammed." [43] According to G. Dinneen, current generation communications satellites, including AFSATCOM, "have very little if any anti-jamming capability," [44] and would be effectively negated:

> Communications satellites are vulnerable to electronic jamming. So in time of war, if they were attacked directly by electronic jamming, they could be blocked out. [45]

In general, Soviet capacity to exploit the antijam shortcomings of U.S. communications satellites is maximal vis-á-vis satellites positioned within line-of-sight of Soviet territory. Satellites positioned elsewhere, out of range of high-powered jammers inside Soviet boundaries, are somewhat less vulnerable. Jamming sources might include shipborne jammers, jamming facilities in places like Cuba, or jammers covertly operated inside U.S. territory. These sources probably could neutralize key AFSATCOM communication such as the channel located at 100^{o} West Longitude (see Figure 6-6), but forward-based sources are rather exposed to U.S. attack and countermeasures. Furthermore, Soviet nuclear attacks that employ high-altitude EMP bursts could result in a form of fratricide — that is, Soviet EMP attack degrades forward-based Soviet equipment used to jam U.S. communications.

Jamming, spoofing and other modes of electronic attack can cause a host of problems besides distorting the information content of emergency messages. For instance, they might alter the orientation of satellites so as to degrade user access, despite efforts by ground-based control facilities to keep the satellites properly oriented.

3. Nuclear Weapons in Space: Nuclear explosions in space may pose the greatest threat to communications satellites serving U.S. strategic forces and command aircraft. This threat stems from the properties of the medium — outer space, and the design characteristics of operational satellites. The medium permits the energy from exoatmospheric bursts to travel unimpeded. Although energy intensity falls off as the inverse square of the distance from the burst location, targets hundreds or thousands of miles away could be exposed to high levels of gamma and X-ray energy.

The pertinent design characteristic is nuclear effects hardening, the amount of which ranges from essentially zero to modest for operational satellites leased or owned by the DoD. Leased satellites (for example, Gapfiller) have the least protection. Certain military communications satellites — AFSATCOM space vehicles (FLTSATCOM) and DSCS II — reportedly have been hardened to some degree against some effects.[46] But military demand for satellite communications support of normal peacetime operations as risen so fast that channel capacity has taken precedence over wartime performance and survivability. Protective shielding and devices compete with the communications equipment itself for space and weight allocations. The inevitable compromises have historically favored capacity at the expense of survivability.

The table below (Figure 6-8) summarizes the main nuclear effects (column 1) that threaten satellites, and gives associated damage thresholds (column 2) and the range at which the thresholds would be crossed. The calculations assume a weapon yield of 1-megaton and an unhardened target satellited with electronics behind 0.06-inch aluminum.

The fragility of unhardened satellites is such that an exoatmospheric explosion at a relatively low altitude might upset communications satellites in geosynchronous orbit (37,400 kilometers, or about 22,400 miles, altitude). The damage mechanism is referred to as system-generated electromagnetic pulse (SGEMP). Appendix D demonstrates that a 25-megaton explosion 60 miles above the United States (an event which simultaneously produces the ground and airborne electromagnetic pulse problems discussed earlier) could in theory generate a level of SGEMP that is sufficient to upset satellite electronics in geosynchronous orbit. (As Figure 6-8 indicates, a 1-megaton explosion would not upset electronics unless it occurred at an altitude of at least 24,500 kilometers, or about 14,700 miles above the earth.)

NUCLEAR EFFECTS ON SATELLITES

Effects*	Assumed Threshold for Illustrative Purposes**	Distance (km)
X-Rays		
Ionization Upset	1 rad (Si)	37,400
SGEMP Upset	10^{-5} cal/cm^2	24,500
SGEMP Burnout	10^{-3} cal/cm^2	2,450
Ionization Burnout	10^4 rads (Si)	370
Thermomechanical Shock	1 cal/g (Au)	270
Gamma-rays		
Ionization Upset	1 rad (Si)	550
Ionization Burnout	10^4 rads (Si)	5
Neutrons		
Degradation	3×10^{11} n/cm^2	56

* 1-Mt weapon, 10 keV blackbody, 30 ns prompt pulse.

** Electronics behind 0.06-inch aluminum.

Figure 6-8

A 25-megaton explosion 12,600 km. (about 7,600 miles) above the earth could in theory generate a level of SGEMP that is sufficient to burn up satellite electronics in geosynchronous orbit. A 220-megaton explosion (an order of magnitude greater than the highest yield of present weapons in the Soviet inventory) 60 miles above the United States could in theory burn up geosynchronous satellites.

These estimates may not be valid approximations of real satellite responses under actual conditions. They are meant to serve illustrative purposes only. High-yield, low-altitude exoatmospheric explosions, however, would almost certainly disrupt satellite communications. Moreover, to the extent that SGEMP can disrupt, damage, or destroy one geosynchronous satellite "parked" above the United States, it can simultaneously cause similar problems for other communications satellites in geosynchronous orbit because such satellites tend to be clustered together in so-called "wells."

Even if SGEMP merely upsets satellite electronics, the resulting degradation is potentially serious. Degradation probably would be temporary if satellite control stations on the ground were not attacked. In time, those stations could restore satellite service. But if they immediately came under attack, the necessary corrective actions could not be taken. As a consequence, satellites could be permanently upset and thereby rendered useless.

4. Satellite Interception: So far, the Soviets have not demonstrated a capability to intercept geosynchronous satellites. They have conducted a series of tests apparently aimed at developing

the capability to disable low-altitude satellites using a space interceptor that maneuvers close to the target and detonates conventional explosives. But no interceptor satellite flew above 2,328 kilometers during tests conducted since 1967. Not every AFSATCOM space vehicle is geosynchronous, however. SDS is one type of satellite that has both an AFSATCOM mission and an orbit that places it in the low-altitude regime. The perigee of its highly elliptical polar orbit is about 400 kilometers. It is open to question whether or not SDS space vehicles could be intercepted during the low-altitude portion of their orbit.

5. <u>High Energy Beam Antisatellite Weapons</u>: The public record would suggest that the Soviets have not demonstrated a capability to attack AFSATCOM space vehicles with directed energy weapons such as lasers. AFSATCOM vehicles in low-orbit (for example, SDS), however, may not be totally immune from the effects of ground-based Soviet lasers.

STRATEGIC SITUATION: 1983

During the past five years, the command implications of large-scale nuclear deployments have been brought into better focus. The relevance of command performance to basic national security purposes is now generally appreciated. C^3I deficiencies have been exhaustively catalogued and remedies have been intensively researched. The need for a sound program of modernization is widely recognized. C^3I

modernization is a central theme of the Reagan administration's strategic agenda, and an improvement plan has begun to cohere under an umbrella of presidential endorsement and widespread approval.

The depth of this comprehension and commitment, however, remains in doubt (see Chapter 8). Command implications will need to be clarified, sharpened, and put in historical perspective before a solid, wise consensus can be forged.

U.S. Second-Strike Capabilities and the Overall Strategic Balance

Force structure analysis would support a judgment that U.S. strategic forces are adequately protected against Soviet attack. Although the vulnerability of land missiles, and to a lesser extent bombers, has grown, the United States possesses enough survivable weapons to strike back against an extensive enemy target base. These weapons, if actually launched, would inflict horrendous punitive damage in retaliation to attack. Retaliation would be devastating even if the U.S. force structure absorbed a massive attack with little or no advance warning. Our retaliatory forces would be powerfully destructive even under very adverse conditions — for instance, strategic and tactical early warning failure.

By contrast, the coherence of our strategic command system is precarious in wartime. A distinct possibility exists that attack on our command system would drastically reduce, or even negate, U.S. retaliation. Command structure attack continues to offer the most attractive military solution to the enemy planner's problem of limiting damage to the Soviet Union. A strategy designed to optimize damage to U.S. C^3I poses a much greater threat to U.S. second-strike capabilities than does a strategy designed to optimize damage to the U.S. force structure.

Negative Control

Various unofficial sources suggest that negative control has been strengthened during the past decade. Several programs designed to accomplish this aim can be cited. First, SAC reportedly installed PAL-type locks on Minuteman forces. Under the new arrangement, launch control crews acquire the physical capacity to launch Minuteman missiles only when unlock codes are passed down from higher authority. Previously, launch crews possessed at all times the physical capacity to target, arm and fire their forces.

Second, the serious false alarms experienced during the early 1980s led to procedural and technical changes that reduce the risk of accidental war. Erroneous warning indicators, and the untoward reactions they trigger, are less likely to occur.

Lastly, the United States and the Soviet Union signed an agreement whose provisions require advance notification of certain weapons tests; maintenance of reliable, timely communications between the two countries' leadership; and other steps designed to prevent accidental war.

To some extent, the imposition of tighter negative control has made the exercise of positive control more difficult.

Crisis Stability

From the standpoint of force structure vulnerability, the stability of deterrence appears assured. The threat of retaliation cannot be removed by either side, a condition that surely acts as a powerful deterrent and restraining influence in a superpower crisis. The knowledge that opposing forces are partially vulnerable to preemptive attack is very unlikely to affect superpower behavior in a crisis, however intense. That opposing forces are substantially invulnerable is the salient consideration.

Dangerous excitation is more likely to stem from command system vulnerability. The condition of the U.S. command structure creates a potentially severe penalty for delay in weapon release; the situation encourages early release by U.S. authorities. By the same token, the creaky state of our command system offers Soviet leaders potentially great rewards for prompt action; the situation discourages indecision and late release by Soviet authorities.

In sum, command vulnerability, not force vulnerability, presently is the primary potential source of crisis instability. That this has been the situation throughout the missile era is a point that ought not to be lost in the shuffle of national debate over strategic modernization and arms control. Command vulnerability actually materialized a long time ago, only to be overshadowed by anticipated force structure vulnerabilities that never have fully materialized. Contrary to common belief, the United States is not entering a period of unprecedented vulnerability and danger.

Force Components and Strategic Stability

Today an inverse relationship exists, as it always has, between the vulnerability of a given force component and the vulnerability of its supporting command system. Land missiles are the most responsive to higher authorities, and the least prone to isolation. Submarine missiles are the most difficult to manage in peacetime, crisis, or war. Bombers compare favorably with submarines but are less manageable than land missiles.

This rank order is reversed if the TRIAD components are differentiated with respect to their respective vulnerability to direct attack. The vulnerability of land missiles has increased dramatically during the past decade. Bomber vulnerability is marginally greater. Alert submarines, on the other hand, continue to enjoy virtual immunity to attack.

In short, the past decade witnessed a further divergence along the two dimensions of stability. The most controllable component became increasingly vulnerable to direct attack, while the least controllable component retained its invulnerable status and became the mainstay of our strategic deterrent.

Reliance on Tactical Warning

Reliable tactical early warning is of paramount importance to the efficacy of our current strategic posture. During the past decade, the rapid annihilation of the ground segment of the U.S. command structure became a Soviet prerogative, and the back-up airborne segment became increasingly exposed to attack from submarine missiles. The back-up system depends critically upon early warning and rapid reaction to escape destruction by these missiles.

Unless strategic intelligence alerts aircraft to impending attack, the ground alert units which constitute the vast majority of the elements in the airborne network could be caught on the ground and destroyed even if tactical early warning systems perform perfectly. Reliance on tactical and strategic warning has grown to a point where both are essential to the effective exercise of central positive control. As was the case a decade earlier, the two aircraft -- "Looking Glass" and a solitary TACAMO aircraft -- that are flown on continuous alert lack the capability effectively to manage the retaliatory forces.

Policy Implications

A variety of command deficiencies -- the extreme vulnerability of the ground segment; the considerable pre- and postlaunch vulnerability of C^3 aircraft; and the questionable performance of airborne, emergency rocket and satellite communications systems -- undermine the ability of U.S. authorities to direct retaliatory forces to national purposes.

Recent years have witnessed growing recognition of these deficiencies and growing appreciation of their implications for strategic policy and investment. A major breakthrough in this regard is the Reagan administration's unusual move to predicate force modernization on C^3I repair. The present administration has expanded the scale of C^3I research and development to create the most intensive, comprehensive effort to date. It has also voiced a strong commitment to C^3I modernization, and indeed portrayed it as the linchpin of its overall strategic modernization program. C^3I programs are supposed to compete, and fare well, against major weapons proposals.

This represents a notable first step toward a balanced set of strategic priorities. Weapons investment at the expense of C^3I investment runs contrary to the policy guidance issued by the administration.

But the administration's construction of the strategic command problem is flawed. In stressing the need to lay the C^3I foundations of a protracted war-fighting strategy, the administration may overlook the fact that basic C^3I capabilities need to be shored up. The first-order problem is to satisfy the requirements for assured retaliation. A credible threat of large-scale retaliation against a comprehensive target list ought to be established beyond all doubt before asking C^3I systems to carry other burdens. There is some risk that the misplaced emphasis of current policy will divert resources from programs that can feasibly provide a high confidence solution to the fundamental problem.

FOOTNOTES

1. See Chapter 8 for further discussion of extremely low frequency (ELF) submarine communications.

2. U.S. Congress, Senate, Committee on Armed Services, FY 1975 Authorization For Military Procurement, Research and Development, 93rd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 6, p. 3225.

3. Ibid., p. 3233.

4. Ibid., p. 3311.

5. Ibid.

6. Ibid.

7. U.S. Congress, Senate, Committee on Armed Services, FY 1978 Authorization For Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 10, p. 6678.

8. See U.S. Congress, House Committee on Appropriations, Department of Defense Appropriations For 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 144; also, U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization For Appropriations For FY 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 3345.

9. "Living on the Nuclear Firing Line," New York Times (October 16, 1983), p. 7.

10. U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 3296.

11. These are conservative estimates because the analysis excludes the possibility of airborne launch of isolated land missiles.

12. SS-9s and SS-18s (mods one and three).

13. 200 Soviet land missiles out of a total force of 1,386 were employed against 100 Minuteman launch control centers. Titan control centers were not struck in the analysis. As was noted earlier, the hypothetical attack on American missile silos in 1978 allocated one missile to each of the 1,054 targets (Minuteman only), expending 25 percent of the Soviet land missile force.

14. Recalling Figure 2-4, a Soviet attack on missile silos was shown to destroy 44 percent of the land missile force in 1978. This estimate assumed Soviet missile reliability to be 0.75; higher reliabilities result in the following estimates of expected damage:

Missile Reliability:	0.80	0.85	0.90	0.95
Expected Damage (%):	46	49	52	55

It should be mentioned that as the number of targets increases, the damage associated with various levels of risk tends to converge on the "expected" value. For instance, in a Soviet attack aimed at 1,054 missile silos, the damage for different levels of risk are:

Expected	Risk≥20%	Risk≥10%	Risk≥5%	Risk≥1%
44	44	46	48	51

15. The projection for 1985 is that 80-88 percent of the Minuteman land missile force would be destroyed by blast effects.

16. These 14 GEPs support NEACP and SAC Airborne Command Post. U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization for Appropriations for FY 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 1, p. 390.

17. See Robert P. Berman and John C. Baker, Soviet Strategic Forces: Requirements and Responses (Washington, D.C.: The Brookings Institution, 1982), p. 107.

18. Ibid., pp. 108, 131, 94.

19. Ibid., p. 107.

20. U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 1, p. 395.

21. Ibid.

22. Ibid., p. 367.

23. Ibid., p. 396.

24. Berman and Baker, Soviet Strategic Forces, p. 64.

25. Berman and Baker, Soviet Strategic Forces, p. 141, reports that five is a high but normal patrol number.

26. Ibid., p. 96.

27. This is due to the slower launch acceleration of the E-4. An EC-135 can be airborne in about six minutes after startup, compared to about eight and one-half minutes for the E-4. The startup time for the E-4 is about one minute faster, however. It takes about two minutes to start engines on an E-4 and about three minutes to start an EC-135. U.S. Congress, House, Committee on Armed Services, Hearings on Research, Development, Test and Evaluation Program For Fiscal Year 1973, 92nd Congress, 2nd Session (Washington, D.C.: GPO, 1972), p. 11054.

28. Efforts are underway to EMP-harden the command centers, themselves at least NORAD HQ in Cheyenne, Montana and selected SAC Command posts. U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization For Appropriates For Fiscal Year 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 7, pp. 4681, 4700.

29. Ibid., p. 4686.

30. U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), Part 6, p. 3457.

31. Ibid.

32. See U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization For Appropriation For Fiscal Year 1982, 97th Congress, 1st Session (Washington, D.C.: GPO, 1981), Report No. 97-58, pp. 106-7.

33. See U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 7, pp. 4696, 4718-19.

34. Testimony of the Deputy Under Secretary of Defense, U.S. Congress, Senate Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 7, p. 4678.

35. The aircraft suffered wing, wind screen, and turbine abrasion after 4 minutes of exposure. In one case, two engines stopped in flight and remaining engines lost power after four minutes of exposure (three engines were totally destroyed).

36. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for FY 1982 (Washington, D.C.: GPO, 1981), 97th Congress, 1st Session, Part 7, p. 4054.

37. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, pp. 141-142; U.S. Congress, Senate, Committee on Armed Services, DOD Authorization For Appropriations For FY 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6722.

38. Ibid.

39. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 3, p. 26.

40. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1980 (Washington, D.C.: GPO, 1979), 96th Congress, 1st Session, Part 3, pp. 98, 101.

41. To come.

42. U.S. Congress, Senate, Committee on Armed Services, DoD Authorization for Appropriations for Fiscal Year 1982 (Washington, D.C.: GPO, 1981), 97th Congress, 1st Session, Part 7, p. 3792.

43. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1980 (Washington, D.C.: GPO, 1979), 96th Congress, 1st Session, Part 6, p. 62.

44. U.S. Congress, House, Committee on Appropriations, DOD Appropriations for 1980 (Washington, D.C.: GPO, 1979), 96th Congress, 1st Session, Part 6, p. 153.

45. U.S. Congress, House, Committee on Appropriations, Military Posture and H.R. 10929 (Washington, D.C.: GPO, 1978), 95th Congress, 2nd Session, Part 3, Book 2, p. 1841.

46. According to one source, "at present no U.S. communications satellites are specifically hardened against nuclear effects." Eric J. Lerner, "Strategic C^3: A Goal Unreached," IEEE Spectrum, vol. 19, no. 10 (October 1982), p. 53. Other sources report the existence of some protection. AFSATCOM space vehicles, for instance, are reportedly "hardened to electromagnetic pulse." U.S. Congress, Senate, Committee on Armed Services, DoD Authorization for Appropriations for Fiscal Year 1982 (Washington, D.C.: GPO, 1981), 97th Congress, 1st Session, Part 7, p. 3792.

CHAPTER SEVEN

COMMAND PERFORMANCE, LIMITED COUNTERFORCE EXCHANGE, AND LAUNCH-UNDER-ATTACK IN THE EARLY 1980s

A strategy of deterrence based on massive retaliation against a comprehensive enemy target base remains the cornerstone of U.S. strategic policy. This strategy and the consensus behind it, however, have come under growing pressure to shift emphasis from massive to flexible response. Continue to provide for massive retaliation, but be prepared for any contingency.

A policy of flexible response is an appealing one. It not only seems to answer the paradox of massive retaliation (see Chapter 2), but also encourages healthy skepticism toward preconceptions about nuclear war. Doubt is admitted into the realm of nuclear planning; wisdom begins with the recognition that one can only speculate -- on the nature of nuclear conflict, on the preferences of national leaders, and on the appropriateness of attack options. However many options are programmed in advance, there is no assurance of their correspondence with the formulated preference of national authorities. And however close the correspondence, there is no assurance of their appropriateness. Any particular course of action represents, at best, a tentative, theoretical solution to conflict, and only experience can confirm or refute its wisdom.

In short, the highest form of rationality would be conscious trial and error. A strategy of flexible response sets up an elaborate experiment in conflict resolution, requiring an ability to tailor responses; to test and learn; to adapt to changing circumstances; and to modify goals and plans.

Both the weapons and C^3I programs of the Reagan administration can be understood as fresh attempts to align the U.S. strategic posture with the requirements of flexible response. In the C^3I arena, the predominant goal is the creation of a system that allows for central, flexible direction of strategic forces throughout a protracted nuclear conflict. To this end, the administration aims to increase C^3I endurance and provide for its reconstitution, in order to ensure continuing positive control (execution/termination for weeks or months) over strategic reserve forces. The administration also aims to improve the timeliness and accuracy of attack assessment, in order to better inform the decision process and allow for selection of a response that corresponds to the scale of provocation; to improve capabilities for postattack and postexchange damage assessment, in order to facilitate redirection and/or termination of in-progress force operations; and to improve other capabilities that strengthen overall deterrence by creating a situation in which the failure of deterrence could occur in stages. Lastly, the administration appears to be seriously considering launch-on-warning tactics to bolster Minuteman Missile survivability.

Building a command system that fulfills current policy aspirations is easier said than done. To begin with, large strategic organizations are heavily, and inherently, structured. They operate according to preestablished procedures that sharply delimit opportunity for improvisation and tailored response. The philosophy behind flexible response and the operation of actual organizations are based on fundamentally different principles of control. For this reason, attempts at overriding programmed behavior and inducing innovative organizational behavior are more likely to disorder than reorder activity. Would not central decisionmakers, especially given the way the missile age has compressed time, tend to adapt to the organization and its preestablished plans of action, rather than the other way around?

Regardless of how one characterizes organizations and the control principles on which they operate, strategic flexibility involves an extensive network of information channels, the protection of which presents a formidable challenge. Developers cannot exclude the possibility that Soviet planners would target whatever C^3I system is built. Designing a system to perform in the face of a carefully planned attack against it is, as previous chapters showed, a difficult undertaking even when the demands on the system are quite modest. The United States has not succeeded in designing a system that fully meets traditional, modest positive control requirements — those associated with a strategy of massive retaliation. And there is some doubt as to the technical and economic feasibility of the traditional policy aim, let alone the ambitious policy aspirations now being advanced under the rubric of flexible response.

The technical and economic feasibility of flexible response is harder to call into question under best-case attack assumptions. It seems reasonable to suppose that a command system could be developed to deal with low-level attacks -- for instance, attacks focused on the U.S. force structure, especially if the Soviet Union refrained from attacking C^3I assets. But there is scant evidence to suggest that the Soviet Union considers avoidance of U.S. C^3I assets to be advantageous under any circumstances. To the contrary, there is strong reason to believe that Soviet planners have long appreciated that exploitation of U.S. C^3I deficiencies offers the only route to meaningful damage limitation. They may or may not expect command structure attack to succeed in parrying U.S. retaliation, but no alternative attack strategy would appear to be as promising.

Western strategists have nonetheless popularized that well-known scenario in which the Soviets concentrate their attack on the U.S. force structure. In this "scenario," Soviet attack strategy is designed to inflict maximum damage to the U.S. strategic forces. Although enormous destructive power would reside in the surviving U.S. force, the bargaining positions of the two sides might be altered to Soviet advantage, according to these strategists. It is alleged that the Soviet Union could achieve exploitable bargaining dominance over the United States and limit damage to itself through coercion. Implicit in this argument is the notion that potential bargaining leverage, however incalculable, is worth more than the additional military advantages that would plausibly result from comprehensive attack.

We must restress that this Western view downplays the incentives and payoffs associated with command structure attack, and evidences scant appreciation of the high priority assigned to command suppression in Soviet military writings. There is not the slightest indication that the Soviets value, much less prefer, an attack strategy designed to work a politico-military solution to the problem of limiting damage to the Soviet homeland. By all indications, they prefer an attack strategy designed to fracture the U.S. command structure and disorganize counterattacks over a strategy designed to coerce nonuse of residual U.S. forces.

Besides being hard to reconcile with Soviet doctrine, apparent intentions, and incentives for attacking U.S. command structure, the scenario that focuses attack on U.S. forces downplays some important disadvantages associated with this strategy. A Soviet attack patterned after the "model strategy" in Western analysis requires a massive commitment of resources and surgical precision in implementation. Tolerances for operational degradation are slim. By contrast, a command structure attack requires a relatively small allocation of available strategic resources; coordination and timing requirements are not so stringent that orchestrating the attack would present extreme difficulty; and the high expected damage from such an attack is not terribly sensitive to operational degradation in missile reliability, accuracy, attack coordination and timing.

The scenario that underlies most current thinking and analyses related to strategic war has apparently gained credence because it appears to be (1) technically plausible, and (2) consistent with a form of theoretical rationality which says that strategic force can continue to have exploitable political utility after deterrence fails. Once the condition of the U.S. command structure is taken into account, however, this entire construction becomes farfetched. Apart from its distortion of the advantages and disadvantages of alternative attack strategies, it rests on some bald presumptions about Soviet capabilities for selective attack; about both sides' ability to distinguish levels of nuclear warfare; and about the viability of U.S. C^3I systems after a large-scale counterforce attack concentrated on the U.S. force structure.

SOVIET FLEXIBILITY: REAL OR IMAGINARY?

The feasibility of a "surgical" Soviet counterforce attack, and the potential bargaining leverage incidental to such an attack, spring largely from the observations that Soviet missile accuracy has improved and numbers of deliverable warheads have increased. These force structure developments translate into Soviet strategic flexibility, according to many analysts. B. Lambeth, for example, posits that the weapon characteristics of the newest Soviet forces by themselves:

> ... portended an unprecedently rich Soviet menu of targeting options short of the all-out attack scenario envisaged by formal Soviet military doctrine.... To note only the most obvious of these potential targeting options, the Soviets are

> progressively moving toward the point where they may be able to implement a high-confidence disarming attack against the U.S. Minuteman force with around 300 MIRVed SS-18s, leaving a residual force of 1,000 SS-17s and SS-19s (along with a fully alerted and undepleted SLBM fleet) for carrying out selective strikes against other targets in CONUS and elsewhere or for providing a credible intra-war deterrent against U.S. countervalue retaliation with its surviving elements of the Triad.[1]

This analysis treats flexibility as a force structure issue (see Chapter 2), in that it equates a surfeit of accurate Soviet warheads with the command-control wherewithal to carry out a surgical attack. The Soviets may in fact possess the requisite command-control sophistication. But this is of course an empirical question that warrants careful examination of Soviet C^3I systems; evidence of weapons sophistication is by itself inconclusive.

More than analytical convenience and a conservative bent among analysts lead many to grant the Soviets a high degree of sophistication in command and control. The attribution often reflects a highly stylized Western view of war conduct, which tends to combine technological determinism and the diplomacy of violence perspective. The result is an analysis that overstates the role of weapons technology and rational political choice in war conduct, while understating human and organizational constraints. To quote Lambeth, who treats implementation of national decisions as a minor administrative task, Soviet political and military leaders would mount a surgical counterforce attack "should they conclude that the exigencies of the moment warranted that as a preferred course of action." [2] He promotes the school of thought which maintains that the Soviets, "like all reasonable men, will unhesitatingly cast aside their avowed doctrinal preconceptions in favor of real-time improvisation if a nuclear crisis (and U.S. behavior in it) should suggest that as an appropriate course of action." [3]

This construction is common. Former Defense Secretary J. Schlesinger, for example, once described a limited U.S. strategic attack on the Soviet Union. He envisioned the use of a small number of Minuteman missiles to prevent the defeat of NATO in a conventional war. If the defeat of NATO loomed, and U.S. strategic forces were used against Soviet targets — for instance, remote oil refineries and storage facilities — Schlesinger foresaw Soviet strategic retaliation. But while conceding an historical Soviet aversion to limited war doctrine, Schlesinger argued that all-out Soviet retaliation (their avowed doctrinal preconceptions) would not happen because "when the existential circumstances arise, political leaders on both sides will be under powerful pressure to continue to be sensible." [4]

Ironically, Schlesinger developed this line of reason in testimony outlining and justifying his revision of U.S. targeting doctrine in 1974; he proceeded to note that selective application of U.S. strategic forces requires "indoctrination and planning in anticipation of the difficulties involved. It is ill-advised to attempt to do that under the press of circumstances." [5] In other words, when the existential circumstances arise, the course of action preferred by reasonable men had better be preplanned. With time in the nuclear age measured in hours and minutes, and with large, complex organizations responsible for war conduct, real-time improvisation (Lambeth's phrase) would be sharply constrained.

This is not to say that no preparations for selective attacks on U.S. targets have been made. We are merely suggesting that attack options do not come into existence spontaneously, on demand. The logic of rational choice may dictate preferences, but preferences do not necessarily correspond to available options. The relevant question is not whether limited counterforce attack, for instance, would be the preferred course of action in a particular set of circumstances, but whether the operational details of that course of action have actually been worked out.

Furthermore, the existence of a well worked out plan is not the only precondition for mounting a properly timed and coordinated counterforce attack. A plan which provides for the simultaneous operation of a number of fixed procedures is a <u>minimum</u> precondition. And paradoxically enough, the compilation of such a plan, which would depend for its success on the cooperation and smooth interaction of all concerned, invites its frustration. Human factors effects -- human skills, motivation, and error in control systems -- alone ensure that a Soviet attempt at implementation of a plan so intolerant of deviation would be risky.

Errors observed during training exercises in Minuteman control systems are suggestive of mistakes that Soviet forces might make in a first-strike attempt. For instance, the entry of a single wrong digit into a computer at a Minuteman launch center could hurl missiles at the wrong targets, including cities. Though targeting errors may be discovered prior to key-turn, correction of such mistakes can easily throw off the coordination and timing of the attack.

Consider another example that may be suggestive of the way organizational constraints affect performance. During force execution, Minuteman launch crews are expected to complete the firing sequence within a couple of minutes after receipt of their orders. If actions within any given squadron cannot be completed within the time allotted, missiles assigned to that squadron must be withheld, while missiles in squadrons which meet the time requirement are launched. The consequence is a loss of maximum forcewide coordination during the initial salvo. Although in simulation exercises crews usually demonstrate proficiency in meeting the stringent time requirements, conservative strategic planners know that such exercises fail to expose all of the technical and procedural problems that may be encountered in real situations. Prudent planners know that unforeseen problems in the established launch sequence exist, and that these problems could substantially degrade force coordination. In the example of a Minuteman salvo launch, one can cite any number of operating rules that could have systematic, adverse effects on attack timing. An example of such a rule is one that requires crews to copy and react to the latest valid emergency action message. The problem is that while crews are responding to the first message received, the same message may arrive over any or all available means of communications -- telephone, HF voice, UHF satellite teletype, ERCS voice, SACCS teleprinter, and SLFCS teletype. Actions undertaken in response to the initial message must be temporarily suspended while crews copy and examine successive messages as they arrive. These incoming messages would probably be repeats, but rules dictate that crews examine them to be sure. This processing may disrupt activities and waste precious time (unless, of course, one of the messages does supersede the one currently being acted upon), and as a result crews may be hard pressed to complete the launch sequence in the time allowed. There would be a good chance that some launches would be postponed. (Crews would resume launch activities at a time specified by a predetermined launch schedule.)

Small and often overlooked details such as the rule applied to message processing can have important ramifications, especially for attack strategies that depend on precise timing for their success. An effective countersilo attack demands such perfection. Yet no one has established that either side has perfected, or could perfect, a countersilo attack strategy. There is a strong case for the presumption that unanticipated procedural complications would result in imperfect implementation of such a strategy.

Levels of Nuclear Conflict

Some analysts deduce that Soviet planners have indeed attended to the operational details of selective counterforce, a deduction sometimes based on apparent Soviet interest in conflict gradients. Lambeth detects a shift in Soviet thinking:

> Soviet writings now seem more disposed than before to admit threshold distinctions between theater and intercontinental nuclear war and between conventional and nuclear operations within the theater-war context. They also seem prepared to accept the possibility of threshold restraints within each of these categories as long as the Soviet side remains ahead and the U.S. has the good sense not to escalate.[6]

Recognition of "threshold distinctions" and the possibility of "threshold restraints" is surely the first step toward creation of operational plans for selective counterforce attack. To equate the existence of such plans with recognition of conflict gradients, however, is to take a bold leap of inference. The translation from the abstract and conceptual to the concrete and practical is not straightforward. Threshold distinctions are hard to define and even harder to connect to force operations.

Threshold categories in common usage — theater versus strategic nuclear warfare, limited versus massive strategic attack, and so forth — tend to be lacking in specificity. The categories form an inexplicit, almost dimensionless typology in need of refinement along specific, explicit dimensions such as: (1) types of targets attacked; (2) types of weapons used; (3) scale of attack; (4) identity of nations and actors undertaking hostile action; (5) location of combat or weapons detonation; and (6) damage and casualties suffered.

Much analysis of escalation control merely pretends that distinct thresholds exist — conceptually and practically — and proceed to treat escalation and deescalation as bargaining tactics. Upon the outbreak of war, an endurance contest ensues. Violence mounts and thresholds are crossed, as part of a campaign of terror in which each side inflicts pain to show that more pain can come. Conflict intensifies until one side -- the side with the lowest threshold of pain, or the side unwilling to move a notch higher on the conflict scale -- finally accedes to the opponent's demands.

Such imaginative, abstract formulations leave one without satisfactory working definitions of thresholds, fail to address the question of whether force operations would actually embody rules of engagement implied by such definitions, and beg the question whether the opposing leaderships could accurately assess the situation.

To illustrate the conceptual and practical problems of distinguishing thresholds, consider the level of conflict frequently labeled "strategic." In what sense is this level of conflict distinct from "theater" nuclear warfare? A prevalent view is that the threshold between "theater" and "strategic" is crossed when one or both sides employ strategic nuclear weapons. But both the United States and the Soviet Union deploy nuclear weapons which, although classified as "strategic" under the terms of SALT, have strong association with "theater" nuclear war and regional defense. The Soviets probably aim thousands of "strategic" weapons -- ICBM and SLBM warheads as well as bomber forces -- at Western Europe and China. Similarly, the United States stands ready to launch, as part of a "theater" nuclear campaign, hundreds of warheads from strategic missile submarines. Aimpoints doubtless include targets inside Soviet borders. The American nuclear umbrella over Western Europe also provides for Minuteman land missile strikes against targets in the Soviet Union. The question arises: Do missile submarine launches or surgical Minuteman strikes meant to prevent the collapse of NATO cross what Lambeth calls the threshold distinction between theater and intercontinental war, or do they relate to what Lambeth calls threshold restraints within a particular category? Answers to such questions are not obvious. Most Western observers do not see implementation of such options as tantamount to entry into the realm of "strategic" warfare. The Soviet Union may or may not share the West's vision. In any case, "strategic" warfare is indistinguishable from "theater" warfare in at least two key respects: type of weapons employed, and employment of nuclear weapons against targets in Soviet territory.

Other potentially important distinctions may disappear in the initial phases of conflict. For instance, it might seem desirable to refrain from attacking the opponent's "strategic" forces, especially if nuclear weapons remain leashed, in order to preserve this distinction as long as possible, but the ability to restrict activity that blurs this distinction seems questionable. U.S. Navy officials suggest that Soviet missile submarines would immediately become subject to attack in wartime. Prosecution of an antisubmarine campaign evidently would not entail discrimination between types of Soviet submarines: the Navy "would not be in a position of differentiating their attack submarines from their SSBNs."[7] Moreover, U.S. military leaders apparently accept that "in a conventional war all submarines are submarines. They are all fair game."[8] There would thus appear to be little likelihood of preserving the distinction between attacks on strategic and nonstrategic forces. At the outset of a major conflict, Soviet missile submarines in the open oceans, at launch stations near U.S. coasts, in transit, and in home waters become "fair game."

In conjunction with the prosecution of an antisubmarine warfare campaign, there may be an attempt to destroy targets inside Soviet borders. The Chief of Naval Operations has testified that:

> Our plan would be as the first line of defense to strike the airbases from which the Backfire bombers fly and the submarine bases from which the nuclear-powered submarines operate.[9]

He gives no more particulars in this regard, but it is easy to infer that Navy strategists contemplate an assault on missile submarines in Soviet home ports, and on aircraft (Backfire) that some Western analysts insist are "strategic" bombers, as an early or opening move in a war. Regardless of the type of munitions employed, a key distinction is blurred: the lower levels of conflict seem to be indistinguishable from the highest level — "strategic nuclear" — in a dimension which could be labeled "type of weapon system attacked." Attacks on "strategic" forces possibly would be mounted at an early stage, well before the employment of nuclear weapons.

In this same vein, one is led to ask whether Soviet military operations that reduce U.S. strategic capabilities necessarily take us across the "strategic" threshold. Does Soviet antisubmarine warfare conducted during a conventional war constitute an act of "strategic" warfare if some attrition of U.S. deterrent forces — namely, missile submarines — results? Does Soviet electronic or physical attack on strategic command and warning elements constitute "strategic" attack? Some observers regard Soviet attack on any of these elements as tantamount to "strategic" warfare, even though individual strategic weapons may not be attacked. A remark from the historical record is germane. Admiral Galantin, testifying in 1963, concluded that Soviet attack on any one of the shore-based VLF stations used to broadcast messages to missile submarines "would probably mean an all-out war."[10] As this example shows, distinguishing between "strategic" and "nonstrategic" attack involves a subjective determination as to what elements belong in the category of "strategic weapon system."

Galantin's remark also reflects a subjective assessment of Soviet intentions and motives. There is a widespread belief that Soviet command structure attack on any scale would presage a large-scale missile barrage against targets in the United States. But while intentions are potentially a key distinguishing feature of conflict levels, actual motives are often ambiguous. A range of different but equally plausible motives can be inferred from a limited command structure attack — for instance, an attack on U.S. reconnaissance satellites. The attack may be designed to degrade the ability of the United States to assign targets to its strategic forces. But such an attack may be designed to send a political signal or demonstrate resolve while minimizing the scale of provocation. ASAT attack may be like some of our limited nuclear options in that demonstration of resolve is the primary objective.

In discussions of U.S. limited nuclear options, individuals have stressed the importance of conveying U.S. intentions through direct communications with the enemy, in order to prevent misinterpretation. Former Defense Secretary Schlesinger, for example, considers escalation control and execution of limited nuclear options to be compatible provided that "we were to maintain continued communications with the Soviet leaders during the war, and ... we were to describe precisely and meticulously the limited nature of our actions, including the desire to avoid attacking their urban industrial base...."[11] The importance of uninterrupted dialogue is quickly grasped; the proverbial fog of war would be closing in. Along most perceptible dimensions, "strategic" warfare and lesser levels of conflict fast become indistinguishable. Events leading up to and including execution of a limited nuclear option blur most major distinctions. "Strategic" nuclear weapons have been employed, "strategic" nuclear weapons have come under attack, and "strategic" nuclear weapons have landed on the sovereign soil of the enemy. Except for the comprehensiveness and exact aimpoints of the attack, few if any major distinctions remain to be drawn. And if it is thought that U.S. leaders must carry on a dialogue with Soviet leaders to prevent misperception of U.S. actions and objectives, there has to be some doubt about the opponent's ability to understand them by independent means.

For its part, the United States plans to develop the capabilities needed to perform an independent, accurate assessment of the character of a Soviet attack. The ability of U.S. decisionmakers to select an appropriate response option — one which corresponds to the scale of enemy provocation while serving the national security purposes at stake — depends in large measure upon these capabilities.

We turn shortly to discuss current capabilities to assess in-progress enemy strikes. Popular scenarios in which the enemy attempts to maneuver into a position of bargaining dominance by attacking the U.S. force structure rest on the implicit assumption that U.S. decisionmakers are able to distinguish a limited counterforce attack from a comprehensive attack. But what is the actual state of affairs? Are standard calculations of postattack and postexchange counterforce advantage and disadvantage relevant to actual conditions, or are they mere paper exercises that bear scant relation to current operational realities?

The relevance of limited counterforce calculations, moreover, depends on considerations besides attack assessment capabilities. Many other factors affect the feasibility of a strategy of flexible response extended in time. Protracted war scenarios depend for their plausibility upon the continuing performance of command centers and communications channels. Tactical warning/attack assessment systems, too, must be capable of functioning for weeks or months in a nuclear environment. If C^3I systems are lacking in endurance or cannot be effectively reconstituted, then the United States would be unable to use strategic weapons as instruments of diplomacy after the initial exchange. In-progress U.S. operations could not be terminated or otherwise controlled. U.S. reserve forces could not be executed or otherwise controlled. A fluid situation could not be monitored and politico-military objectives could not be adapted to the exigencies of the situation. Thus, any U.S. effort to deter the enemy's residual forces or otherwise exert influence on the Soviet decision process would be incoherent and probably ineffectual.

Popular counterforce scenarios rest on the implicit assumption that U.S. and Soviet C^3I systems do remain viable for an indefinite period of time. This assumption may be partially justified on the grounds that the hypothetical attacks are concentrated on the respective force structures. But even in the event of attacks designed solely to inflict damage on opposing forces, each side's command system would be stressed. At a minimum, these systems would be subject to collateral damage.

We turn now to consider the effects on U.S. C^3I produced by a Soviet attack designed to cause maximum damage to the U.S. force structure. How well would the present U.S. command system support a strategy of flexible response?

U.S. FLEXIBILITY: REAL OR IMAGINARY?

A Soviet counterforce attack designed to maximize damage to the U.S. force structure — the scenario that underlies the principal perceived weakness of U.S. deterrence — would coincidentally produce extensive damage to the U.S. command structure. Many C^3I elements would come under direct attack by dint of physical proximity to SAC bomber, tanker and Minuteman bases. Figure 7-1 lists many of them.

Figure 7-1

COLLOCATED STRATEGIC COMMAND AND FORCE ELEMENTS[1]

- STRATEGIC COMMAND ELEMENTS -	COLLOCATED SAC BASES: Bomber Bases	Minuteman Bases	Tanker Bases
Warning:			
PARCS Radar		Grand Forks AFB	
Pave Paws Radars (2)	Westover AFB*		Beale AFB
FPS-85 Radar	Eglin AFB*		
FSS-7 Radar	MacDill AFB*		
Command-Control:			
2nd Air Force HQs	Barksdale AFB		
15th Air Force HQs	March AFB		
NEACP Home Bases	Blytheville AFB		Blytheville AFB Grissom AFB
West Aux. ABNCP	Ellsworth AFB	Ellsworth AFB	Ellsworth AFB
Airborne LCC-1	Ellsworth AFB	Ellsworth AFB	Ellsworth AFB
Airborne LCC-2	Minot AFB	Minot AFB	Minot AFB
Airborne LCC-3	Minot AFB	Minot AFB	Minot AFB
All Ground Minuteman LCCs		All Six Minuteman Bases	
Communications:			
ERCS	Whiteman AFB	Whiteman AFB	
PACCS Relay 1			Grissom AFB
PACCS Relay 2			Rickenbacher*
Short Order HF Radio (3)	Barksdale AFB March AFB Westover AFB*		

[1] Partial Listing

* Bomber/Tanker Dispersal Bases

Among the command centers collocated with bomber/tanker bases are the two numbered Air Force headquarters located at Barksdale AFB and March AFB. Other fixed command centers subject to direct attack include the underground LCCs within the Minuteman fields.[12] Mobile command centers include the national command aircraft (NEACP) stationed at Grissom AFB and EC-135 aircraft stationed at Ellsworth AFB (West Auxiliary ABNCP and ALCC aircraft) and Minot AFB (ALCC aircraft). Key communications units include PACCS Relay aircraft stationed at Grissom AFB and Rickenbacker AFB. Emergency communications rockets deployed at Whiteman AFB would also be struck. Ironically, this system of last resort is interspersed among the targets (Minuteman silos) that in typical counterforce scenarios absorb the brunt of Soviet attacks. Since silos housing these rockets are supposed to be indistinguishable from other Minuteman silos, in order to avoid preferential targeting, they are certainly subject to collateral damage; indeed, they would be attacked directly and massively. Among the tactical warning facilities that would be struck are the two modern phased array PAVE PAWS radars located at Beale AFB and Otis AFB; the FPS-85 radar at Eglin AFB; and the FSS-7 radar in Florida. This collection of radar sites constitutes the entire radar network devoted to detection of submarine missile attack. Another radar -- the perimeter acquisition radar (PARCS) situated near the Minuteman complex at Grand Forks AFB -- which provides the most accurate attack assessment of SLBMs and ICBMs aimed at the central United States, probably would suffer extensive collateral damage.

If Soviet counterforce strategy employed high-altitude explosions to expose unhardened bombers and tankers to electromagnetic pulse effects, then virtually all CONUS-based C^3I elements would be incidentally exposed to the same pulses: early warning sensors (including satellites); terrestrial communications channels which feed tactical warning data into NORAD Headquarters in Colorado; NORAD itself (especially computers); terrestrial communications channels that deliver early warning information to the national command centers and the nuclear-capable military commanders (CINCSAC, CINCLANT, CINCPAC); the national and major military command headquarters themselves (especially computers); and the communications networks (including satellites) linking central decisionmakers with subordinate commanders.

In addition to the specific elements mentioned above, networks such as land lines interconnecting sensors, NORAD Headquarters, and national and major military command headquarters would be prone to collateral damage produced by blast effects from multiple and widely distributed ground explosions at the SAC bases.

Many C^3I elements would also come under indirect attack due to the nonlocalized nature of various nuclear weapons effects. Fallout, for example, would drift over C^3I elements located hundreds or thousands of miles from targeted areas. Depending on prevailing weather conditions, fallout from a large-scale Soviet attack on the six Minuteman complexes and bomber/tanker bases could endanger virtually the entire PACCS airborne network as well as contaminate the airfields at which PACCS aircraft must eventually land. At the same time, major command facilities such as SAC Headquarters, NORAD Headquarters, and 8th Air Force Headquarters would be exposed. Major communication nodes — for instance, the Elkhorn control station near Omaha that connects SAC with Green Pine sites, and the SLFCS ground station at Silver Creek, Nebraska — also would be at risk. As well, early warning radar sites at all locations in CONUS are situated close enough to targets to be potentially exposed. The satellite control station at Sunnyvale, California, also falls into this category.

Counterforce attacks aimed at the force structure would also disrupt the transmission media used for strategic communications. All long distance strategic radio communications -- LF/VLF, HF, UHF (satellite) — would be degraded to a considerable degree even if the counterforce attack involved mostly surface and near-surface explosions.

Apart from the collateral damage actually sustained during the attack, surviving ground-based installations would remain under continuing threat of direct, deliberate assault by Soviet forces held in reserve. National policy officials, therefore, would have compelling reason to adapt their decisionmaking to the exigencies of airborne command-control-communications.

Damage to the airborne network would be less severe than it would be if the Soviets had mounted an attack designed to neutralize it. Nevertheless, collateral damage would impair the performance of this network.

Theoretically, the airborne network could sustain considerable collateral damage and still function well enough to establish a line of communications between central decisionmakers and the strategic forces. The technical possibilities are such that despite damage to some circuits a viable channel might be established and kept open; the network might even be able to absorb the complete loss of some aircraft. If an outside observer possessed a "wiring diagram" of the interconnection possibilities within the airborne network, and knew which circuits had been degraded or destroyed, the observer probably could trace one or more complete paths over which information may flow.

In practical terms, however, wartime communications channels would not be established so easily. Airborne units obviously do not have the outside observer's omniscience. No up-to-date "wiring diagram" exists for figuring out which specific media, frequencies, and circuits need to be employed in order to establish a path through a partially damaged network. These things are figured out through trial and error -- units try different media, switch frequencies, and so forth in accordance with established procedures. The establishment of a complete path would be an epiphenomenal outcome produced when subunits enact appropriate routines in concert. Technical redundancy in communications may be adequate, but operating procedures determine whether this technical potential can be realized. Preplanned organizational routines must be appropriate and consistent across the C^3 and force units involved. And units must be geared to enact routines with speed and efficiency.

The organizational routines executed to establish communications consume a considerable amount of time, no matter how benign the environment. C^3 aircraft must, in the first place, move into position. It takes at least thirty minutes just to set up the PACCS network.[13] Additional time is lost when units activate and adjust communications equipment once aircraft reach their preassigned orbits. In all, an hour or more may elapse before the network is prepared to receive, process, and transmit emergency war orders in any coherent way.

A partially damaged network would be even slower to establish a line of communications, and programmed tasks would have to be frequently reaccomplished in order to keep a channel open in a fast-changing, unstable environment. Furthermore, reliance on back-up channels of questionable effectiveness and reliability -- for instance, HF ionospheric radio and AFSATCOM UHF radio -- would be substantially greater. There would be increased dependence on relatively sluggish one-way channels -- for instance, VLF radio -- and attempts at communications over certain channels -- especially, communications rockets (if available) -- would entail some very elaborate and time-consuming procedures.

Other major factors that might limit airborne communications capabilities in the scenario postulated (force structure attack) include electromagnetic pulse effects and partial destruction of SAC's tanker force. Exposure to EMP could substantially degrade communications and reduce the endurance of aircraft in the airborne command network. The status of the SAC tanker force is pertinent because the endurance of EC-135 aircraft depends on in-flight refueling. It is generally thought that tanker support would be marginal. TACAMO aircraft are not configured for in-flight refueling, of course, and that deficiency imposes a definite constraint on the endurance of the airborne network as a whole. The airborne endurance of the network as a whole would not exceed several hours, depending on the fuel load aboard TACAMO, "Looking Glass" and other aircraft that happen to be airborne at the time of attack.

Furthermore, successful reconstitution of the airborne command network is unlikely. As noted, a force structure attack aimed at SAC bomber/tanker bases would coincidentally destroy many of the runways, facilities and logistics used by C^3 aircraft. Off-alert C^3 aircraft would be destroyed, and alert aircraft that survived the attack could be denied the ground support needed for servicing and replenishment. Furthermore, aircraft landing at any undamaged home base or at any intact secondary base would put themselves in jeopardy. In all likelihood, the early warning system on which ground-based aircraft completely depend for their survival would have suffered extensive collateral damage during the initial force structure attack. It is also apparent that, regardless of the performance of early warning systems, aircraft undergoing maintenance could not react rapidly enough to escape destruction by incoming weapons. Lastly, aircraft crews could receive lethal doses of radiation from fallout.

All of these factors together work to impose severe constraint on the decisionmaking of central actors. In formulating a strategic response to a focussed attack on the U.S. force structure, decisionmakers should realize that the ground segment of strategic command had suffered considerable damage and would remain under threat of sudden and total destruction; that the attack had automatically triggered the launch of command aircraft and initiated an operation of relatively short endurance; that a coherent airborne network would be difficult to establish and maintain; that communications would be degraded; that reconstitution of the network would be highly improbable; that communication channel capacity would be so limited as to preclude delivery of detailed instructions; and that many of the communication subsystems that would be patched together to deliver emergency messages allow for only one-way communication.

Under these constraints, a radical departure from any plausibly rational course of action seems a foregone conclusion. U.S. reaction could hardly be rational in either the subjective or objective sense.

Subjective rationality, in its simplest version, is an attempt at value maximization: specify objectives, calculate expected payoffs for alternative choices, and select the alternative with the highest payoff. Under the constraints outlined above, decision time would be too compressed -- because the endurance of airborne network is so short -- to permit a subjectively rational decision process to run its course.

The decision process is also unlikely to produce an objectively rational choice. Regardless of what calculations U.S. political leaders might make at the time, they would come under intense pressure to choose (without delay) an option that will provide for all that they ever expect to accomplish in retaliation. There would be strong incentive to order early and comprehensive retaliation, which runs contrary to what deterrence theory says is objectively rational. According to deterrence theory, an objectively rational policy would correspond to the scale of provocation and extend deterrence into war itself. In the event of limited Soviet counterforce attacks, the United States should hold certain forces in reserve in order to deter Soviet reserve forces and reduce the opponent's bargaining leverage. Such an attack should not be met with comprehensive retaliation.

Even if U.S. decisionmakers exercise restraint by ordering a limited counterattack, there would be little if any scope for meaningful negotiation with the adversary. By the time the counterattack ended and negotiations ensued, withheld U.S. strategic forces would no longer be exploitable instruments of diplomacy. The airborne command network would have lost coherence, and the crippled ground network would remain vulnerable to sudden destruction by Soviet reserve forces. Inasmuch as the responsiveness of U.S. reserve forces would decline or hinge on Soviet restraint, U.S. bargaining leverage would be weak. U.S. threats in the postexchange period would not be very credible.

There are other reasons why the U.S. command structure cannot support a policy based on graduated response and negotiated termination. Foremost among them is the inability of the tactical warning network to perform the fine-grained assessment needed to determine the scale and character of Soviet attacks. At present, the United States could not reliably distinguish a limited Soviet counterforce attack from a comprehensive attack.

The tactical early warning network, excluding early warning satellites and the Cobra Dane ground radar in the Aleutians, [14] is depicted in Figure 7-2. Of the ground radar sensors shown, only PARCS (the only portion of the Safeguard ABM site in North Dakota still in service) gives accurate predictions of impact points for large numbers of reentry vehicles. Before describing the attack assessment capabilities, and limitations, of PARCS, let us briefly discuss other early warning sensor capabilities.

Initial detection of Soviet ICBM and SLBM missile launches occurs within approximately one minute after booster ignition. [15] Several minutes later, the booster(s) stop burning and the satellites lose track of the missile(s). During this brief period of powered missile flight, early warning satellites estimate the approximate number of attacking missiles, their launch points, and their flight corridors, but they cannot determine the missile(s) destination. [16]

The Ballistic Missile Early Warning System (BMEWS) radars would confirm ICBM attack ten minutes later and begin transmitting predicted impact locations to NORAD. [17] BMEWS would predict the general class of

Land Based Ballistic Missile Warning Sites and Detection Sweeps

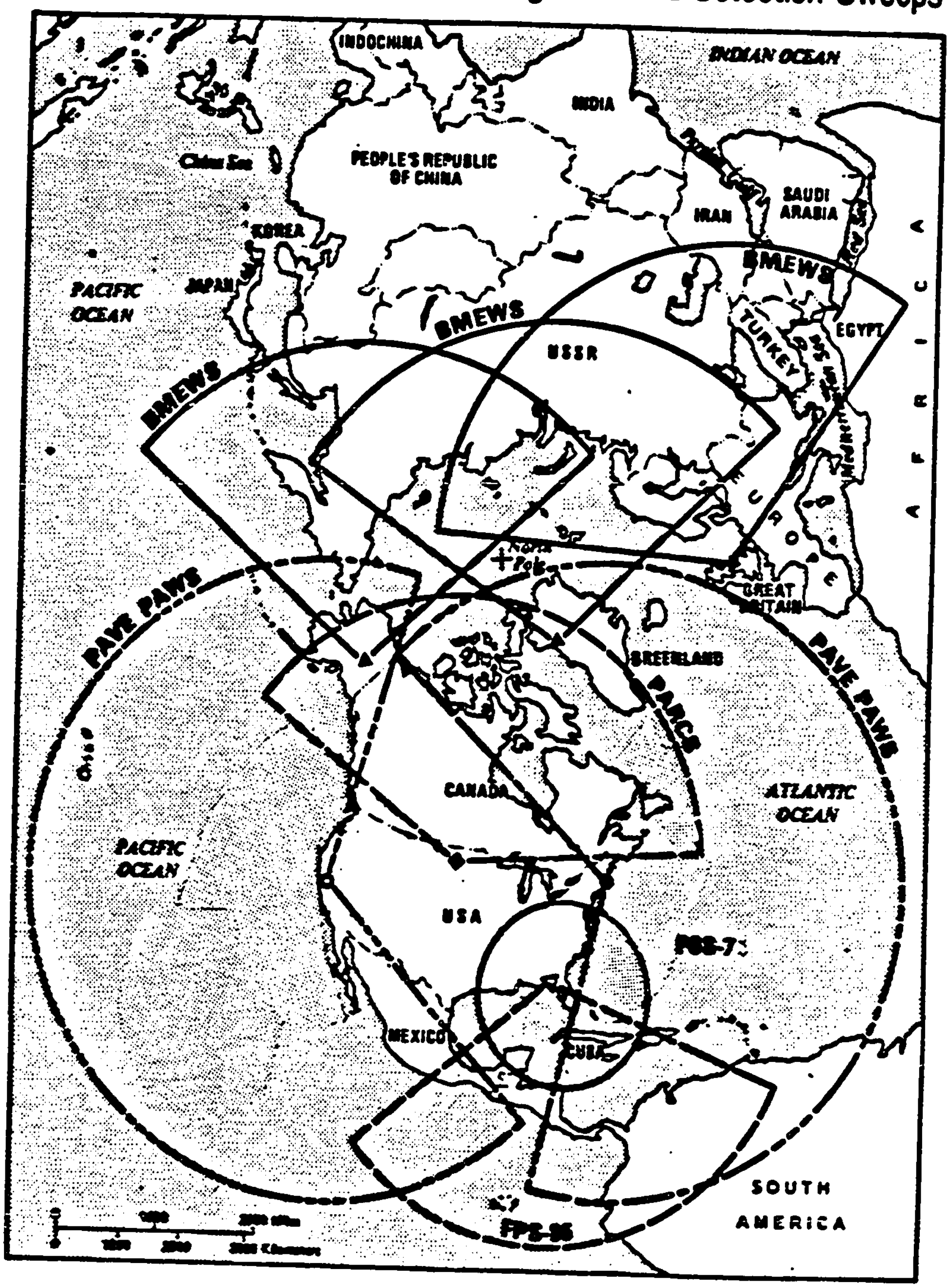


Figure 7-2

targets under attack, using categories such as nuclear retaliatory forces, command-control nodes, and cities.[18] BMEWS predictions, however, would be suspect. This twenty-year-old system was originally designed to detect a mass attack (twenty or more missiles incoming within a five-minute interval) consisting of large booster tanks with a single reentry vehicle.[19] In the words of the NORAD Commander, BMEWS were designed "to just detect a raid and say 'the missiles are coming' to support the national policy of massive retaliation in the 1960s."[20] In order to accurately count thousands of reentry vehicles and predict their destinations, the existing pre-1960 vintage BMEWS computers and tracking radars would have to be extensively upgraded.

PAVE PAWS, FPS-85, and FSS-7 radars would confirm SLBM attacks but would provide only marginal assessment of the character of the attack. The long-range, phased array PAVE PAWS radars deployed in 1980-81 are the most capable in this respect. Compared to the FSS-7 radars they replaced, PAVE PAWS provide a better capability to characterize SLBM attacks.[21] The older FSS-7 radars, including the currently operational site, lack the accuracy needed to provide credible impact predictions.[22] Although PAVE PAWS represent an improvement, power upgrades would be required to achieve the tracking capacity and discrimination necessary for accurate counting of MIRVs and accurate MIRV impact prediction.[23] Two additional PAVE PAWS radars, furthermore, would be required to close radar gaps in coverage of potential Soviet submarine launch stations.[24] These additional radars, together with power upgrade to the existing PAVE PAWS, would help "provide the attack assessment capabilities required to support National Command Authority option selection." [25] This expanded PAVE PAWS network would also eliminate reliance on the FSS-7 and FPS-85 radars still in use; these radars partially fill the gaps in the present two-site PAVE PAWS network. The FPS-85 radar, which became operational in 1968, was originally designed to track satellites. It was modified to perform an SLBM warning function in 1975. It doubtless outperforms FSS-7 radar but probably cannot match PAVE PAWS in terms of attack assessment.

The PARCS radar, as previously noted, is the most accurate attack characterization sensor in operation. [26] The sensor can track hundreds of reentry vehicles, at least, and predict impact points with high accuracy (within several thousand feet). [27] PARCS provides, among other reports, a raid count, an impact profile, and a target class summary (number of weapons expected to land on (1) cities; (2) missile fields; (3) bomber/tanker airfields; (4) U.S. command-control centers; and (5) Washington, D.C.). [28]

Located seventy-five miles northwest of Grand Forks AFB, North Dakota, PARCS provides radar coverage of SLBM attacks from near-arctic areas behind BMEWS, as well as radar coverage of ICBM attacks. [29] Its limitations, however, are considerable. First, official statements indicate that accurate assessment is restricted to ICBMs aimed at the central United States. [30] The radar reportedly views <u>most</u>, but not all, trajectory "windows" that Soviet ICBMs would pass through in an attack against the United States. [31] Second, few SLBMs would be detected/tracked. Last, the radar would not lock on the incoming weapons until late in their profile. Initial detection and assessment would occur only six to twelve minutes before impact, depending on target.[32] In fact, the U.S. command system, including PARCS, could be attacked and effectively destroyed by SLBMs before PARCS detected a single incoming ICBM. If the attack were comprehensive rather than limited, PARCS assessment would not be sufficiently timely.

In summary, attack assessment capabilities are marginal, owing mainly to the fact that present attack characterization sensors "track boosters or post boost vehicles, not reentry vehicles."[33] The MIRVed payloads of modern Soviet forces are practically invisible to all present U.S. sensors except for PARCS, which by itself cannot provide any assurance that Soviet weapons are aimed exclusively at U.S. strategic forces.

Additional information may be provided after weapon impact. Sensors designed for damage assessment (versus attack assessment, a preimpact function) have been deployed since the mid 1960s. A bomb alarm system, deployed in 1966 and phased out in 1970, used visible light detectors to observe nuclear detonations at ninety-nine target areas (ninety-seven in the United States, including cities, Minuteman sites and SAC bases).[34] Nuclear detonation (NUDETS) sensors on board early warning satellites launched since the early 1970s evidently replaced the bomb alarm system.[35] The public record contains scant information on the utility of these satellite-borne NUDETS sensors, but comments on the vast improvements expected with the deployment of the next generation's system (called IONDS) would suggest that current sensors lack the coverage and accuracy needed to characterize enemy attack patterns. [36]

Other technical and procedural factors further undermine a policy based on graduated response and intra-war bargaining. Among these constraints is a finite set of preplanned response options. Available options for retaliation revolve around a limited number of preconceived situations. The actual situation may recommend a tailored, unprogrammed response. But the ability to reprogram so as to produce the desired force operations would be extremely difficult under current conditions.

Reprogramming bomber and submarine targets would not be practicable even without damage to the command system. Regarding submarines, communication channels likely to be available could not handle detailed instructions because of their low data rate. Submarine location and disposition, which higher authorities may or may not know, may also impose missile range and other limitations that sharply constrain target flexibility. Constraints on bomber flexibility are equally sharp. Replanning of bomber attacks must take into account a host of considerations: home base, tanker rendezvous, flight path, navigation, Soviet defenses, penetration/defense suppression, aircraft recovery, and so forth. Such replanning could not be accomplished well, if at all, in wartime; wartime communication channels, furthermore, could not handle the information load necessary to accomplish this aim. Lastly, radio emission control practices preclude both bomber and submarines from acknowledging receipt of reprogramming instructions.

Minuteman forces are easier to retarget against unprogrammed targets but the means by which this is accomplished -- called Command Data Buffer (CDB) -- would not survive the collateral damage received during a limited Soviet counterforce attack aimed at nearby Minuteman silos. SAC relies on terrestrial communications to deliver the detailed retargeting instructions to the Minuteman launch control centers equipped with CDB. The link to these select LCCs would probably be severed at the receiving end.

Another deficiency that undermines this trial-and-error approach to conflict resolution is the lack of precise control over implementation of the chosen plan. As discussed in earlier chapters, a partially damaged command structure can produce all kinds of unexpected outcomes. Interactions among technical systems, standard operating procedures, and people can easily result in dramatic deviation from the intended plan. And central decisionmakers would not be quickly informed of such deviation and its consequences.

The lack of a reliable, timely method of terminating in-progress attacks is another constraint on strategic flexibility. By the time strategic force operations reached an advanced stage of execution, the airborne command network would not be coherent and the forces themselves, particularly bombers, would be harder to reach. Under the best of postattack circumstances, termination instructions could not be reliably issued or received. And virtually none of the units that received the message could report that fact to higher authorities.

As a rule, technical systems and operating procedures are not geared for expeditious termination of offensive operations. For instance, land missiles in terminal countdown to launch are irrevocably committed. They cannot be stopped, even though some of the missiles may be timed to lift off an hour or more after crews complete launch procedures. Land missiles in a long-term but not terminal countdown could be prevented from launch as a technical matter, but crews are not instructed to stop the countdown upon receipt of termination orders. (A long-term countdown means that a single LCC performed the launch sequence; this activates a long-term timer whose expiration launch crews could technically override, thus preventing launch.) The use of the inhibit command to cancel the launch is not authorized, even though orders directing immediate termination may have been received. In this vein, it is noteworthy that missile launching aircraft are not instructed to transmit launch inhibit commands upon receipt of special termination orders from higher authorities. This procedure could facilitate enforcement of the orders in the event that launch control centers on the ground failed to receive or implement them.

The questionable feasibility of directed termination of in-progress attacks further reduces the scope for meaningful, productive bargaining and negotiations. Negotiated termination, moreover, critically depends on tenuous communication links between Washington and Moscow.

Launch-On-Warning

Instead of absorbing the full weight of an attack on land missile silos, the United States might attempt to launch the Minuteman force before incoming warheads arrive. In the past, this tactic — called launch-on-warning, or launch-under-attack — was generally eschewed because it heightens the risk of accidental nuclear war. Now, due to diminishing confidence in the ability of land missiles to ride out enemy ICBM attack, the merits of launch-on-warning are being reconsidered. A higher risk of accidental war may be tolerated in order to reduce the risk that large numbers of Minuteman missiles would be destroyed in their silos.

The trade-off between force survivability and risk of accidental war is much starker in the case of land-based missiles than it is in the case of bombers. Bombers (and command aircraft) on ground alert can be sent aloft upon receipt of even equivocal information from early warning sensors. These units can be ordered into the air as a precautionary action, and recalled if the alarm proves to be false. There is substantial tolerance for human and technical error, and for this reason the authority to launch aircraft for survival has been delegated to military commanders. By contrast, land missiles cannot be recalled or disarmed after they have been fired, a fact which makes missile launch-on-warning more dangerous and difficult. It is more dangerous because the tactic demands a quick decision and a practically foolproof filter against false or misleading attack indications. It is more difficult in part because the authority to fire cannot be responsibly predelegated to military commanders, while the exercise of this authority by national policy officials would be slower and more susceptible to enemy disruption.

Regarding the current official position on launch-under-attack, Richard Perle, Assistant Secretary of Defense (ISP), says:

> I can state categorically that this is not and never has been U.S. policy to rely on such a policy as a means of ensuring ICBM survivability....
>
> ... As a practical and realistic matter, when one considers the amount of time available to a president to make a decision in such a situation as to whether or not to launch strategic nuclear weapons at the Soviet Union, it would put any president to a severe test to expect that a decision to launch nuclear weapons could be made.
>
> I would hope that we could bear the burdens and pay the price to free our president, whoever he may be, from having to make a decision of that consequence in the small number of minutes available to him.[37]

How short is the time available to make the decision? General Burke reckons that in the very best of circumstances involving Soviet ICBM attack, the President has only a few minutes to decide, not only to launch U.S. missiles, but at what targets to launch them.[38] Decision time is even shorter in the event of submarine missile attack; General Burke entertains missile flight times as short as eight minutes, which "is just not enough time to do anything."[39]

A launch-on-warning attack option was nonetheless programmed into the SIOP and Minuteman launch control centers in the late 1970s, and many believe that the tactic might not only be warranted, but successfully implemented, under certain circumstances. One such set of circumstances was outlined by the President's Commission on Strategic Forces, which stressed that Minuteman forces might be launched before they were struck, but after other targets on U.S. soil had been hit:

> ... if Soviet war planners should decide to attack our bomber and submarine bases and our ICBM silos with simultaneous detonations — by delaying missile launches from close-in submarines so that such missiles would arrive at our bomber bases at the same time the Soviet ICBM warheads (with their longer time of flight) would arrive at our ICBM silos — then a very high proportion of our alert bombers would have escaped before their bases were struck. This is because we would have been able to, and would have, ordered our bombers to take off from their bases within moments after the launch of the first Soviet ICBMs. If the Soviets, on the other hand, chose rather to launch their ICBM and SLBM attacks at the same moment (hoping to destroy a higher proportion of our bombers with SLBMs having a short time of flight), there would be a period of over a quarter of an hour after nuclear detonations had occurred on U.S. bomber bases but before our ICBMs had been struck. In such a case the Soviets should have no confidence that we would refrain from launching our ICBMs during that interval after we had been hit. It is important to appreciate that this would not be a "launch-on-warning," or even a "launch-under-attack," but rather a launch after attack — after massive nuclear detonations had already occurred on U.S. soil.[40]

This common assessment is somewhat flawed because it considers a scenario in which only the forces are attacked. The technical feasibility of launch-on-warning, launch-after-attack, or any other tactic that envisions the launch of Minuteman forces before their silos are hit by Soviet ICBMs, is extremely doubtful if the U.S. command system is attacked along with the forces. Such an attack would have a good chance of preventing the early launch of Minuteman missiles.

Perle cites the vulnerability of U.S. warning sensors in reaching this conclusion:

> .. as a practical matter, the ability to launch under attack depends on the security of one's warning systems. While we have succeeded to some degree in proliferating the number of weapons in order to make them more survivable, the vulnerability of warning systems would continue to be a problem. A well-designed Soviet attack might well deprive us of the realistic option of launching under attack in any case.[41]

What would a well-designed Soviet attack on the warning system look like? It would probably involve submarine missile attacks on the BMEWS and PARCS radar sites. These radars, particularly PARCS, are relied on to distinguish Soviet ICBM attacks on Minuteman complexes. But they could be destroyed by Soviet SLBMs before ICBMs penetrated their detection fans. (Recall that PARCS, for example, would not detect ICBMs until six to twelve minutes before ICBM impacts, or approximately twenty minutes after ICBMs lift off; SLBMs launched from U.S. coastal waters could easily strike PARCS within twenty minutes of launch.)

Even if PARCS and BMEWS radars were not attacked, their attack assessment reports would be submitted too late for launch-on-warning to be implemented. In the case of PARCS, six to twelve minutes is insufficient time to digest the information, render a decision, encode/transmit launch orders, and perform the launch sequence at the Minuteman control centers.

The president would therefore have to make a launch-under-attack decision on inconclusive, indeed ambiguous, data from satellite sensors. The decision would have to be made long before a clear impression of the attack could possibly form. In effect, Minuteman launch-under-attack would be triggered by detection of an enemy missile salvo that might be directed at U.S. Minuteman complexes.

But even this hasty, untailored reaction could not be carried to fruition with high confidence under a wide range of circumstances. A well-designed Soviet attack probably could preclude Minuteman launch-under-attack altogether. It might even prevent SAC from flushing the bomber/tanker force and PACCS fleet for survival. Using submarine missiles launched at close range, the Soviets could destroy the National Military Command Centers before a Minuteman launch-under-attack decision could be made, and disrupt the fast data rate communications channels used by national authorities to transmit launch orders to Minuteman and by SAC commanders to transmit orders to flush bombers, tankers, and PACCS aircraft. This attack would be based on EMP effects to disrupt terrestrial communications, the only high-speed channels, within a few minutes of missile breakwater. It would also be based on blast effects to destroy national command centers as early as seven to ten minutes after breakwater.[42] Early neutralization of these assets would leave authorization of Minuteman launch-under-attack and bomber launch-under-attack up to the airborne command network -- the primary back-up strategic command channel -- which uses relatively slow-speed communications to transmit instructions. Except under the most favorable conditions, the airborne network could not deliver the necessary instructions in time to launch Minuteman forces and flush ground alert aircraft before incoming Soviet ICBMs arrived.

This conclusion is especially firm for the surprise attack case. As noted earlier, the airborne network takes about thirty minutes to establish itself under day-to-day conditions with most aircraft on fifteen-minute ground alert. Soviet ICBMs would begin to land on CONUS by the time the airborne network could establish UHF line-of-sight communications among PACCS aircraft, Minuteman launch centers, and SAC bomber/tanker airbases. Furthermore, the flushing of PACCS aircraft on ground alert presupposes transmission of take-off instructions from higher authority, a transmission that EMP effects could block in the first instance.

Generated alert is the only situation in which both Minuteman launch-under-attack and bomber/tanker/EC-135 launch for survival might be effected successfully in the face of deliberate Soviet efforts to block these actions. With the airborne network fully generated, instructions possibly could be delivered and acted upon in time. But the time constraints are such that virtually no tolerances exist for indecision, equipment malfunction, or other performance degradation.

In summary, Minuteman launch-under-attack requires that a decision be made very early, without benefit of clear indications that Minuteman forces were actually under attack, and even then the implementation of this policy would be problematical if the Soviets made a concerted effort to counter it.

Launch-under-attack is arguably a feasible policy if Soviet attack strategy conforms to the popular Western construction: limited counterforce attack. If no deliberate attempt is made to interfere with U.S. C^3I, the prospects of Minuteman launch-under-attack are improved. Whether or not there would be considerable improvement, however, depends on the specific character of the counterforce attack. An attack based partially on EMP effects to degrade bomber/tanker performance, for instance, would coincidentally disrupt the terrestrial communications channels on which launch-under-attack policy depends for its success. This collateral effect by itself could prevent rapid employment of Minuteman forces.

Regardless of the specific character of a Soviet counterforce attack, and no matter how permissive the enemy attack is from the standpoint of launch-under-attack, a U.S. decision would have to be made on the basis of ambiguous sensor data. Technical and procedural constraints do not permit decisionmakers to wait until unambiguous sensor data arrive. By that time (six to twelve minutes before impact), it would be too late.

SUMMARY

A minimalist's version of current U.S. strategic policy aspirations might be this: in the event of a limited Soviet attack designed to maximize damage to the U.S. force structure, the United States should be able to retaliate against an appropriate subset of the Soviet target base, while retaining central direction of reserve forces for as long as necessary. Current policy is actually more ambitious; it calls for an enduring, sophisticated command system that can operate effectively in the face of a deliberate Soviet effort to neutralize it. But, at a minimum, the system must be designed for extended deterrence and intra-war bargaining in the context of a limited counterforce exchange.

The postulated "limited" Soviet attack, which conforms more closely to a Western construction than a Soviet one, but which nonetheless underlies standard calculation of the strategic balance, carries a high risk of triggering an all-out nuclear war. Although rationally calculating decisionmakers may prefer to respond in a limited fashion, a technical-organizational bind creates strong pressure to respond massively. The bind is that U.S. forces held in reserve would not continue to be responsive beyond several hours after the initial Soviet attack.

At the onset of Soviet attack, the burden of U.S. force management would shift to an airborne system of very limited endurance. It would strain just to carry out its basic mission, that is, establishing a temporary command channel to trigger large-scale retaliation in the immediate aftermath of Soviet nuclear attack. Maintenance of a functional airborne network beyond a few hours after attack could not be reasonably expected, given the limited endurance of aircraft; the complex coordination and timing problems involved in the operation of an interactive system with mutually dependent parts; the lack of experience in conducting such operations under realistic, adverse conditions; all the unpredictables that affect performance (ranging from the availability of tankers for in-flight refueling to the effects of turbulence, dust and radioactivity on aircraft performance); and a host of human factors effects such as air crew and battle staff fatigue. It is simply unrealistic to think that the present airborne network would be viable many hours or days later, when threatened or actual execution of reserve forces might be called for. It is in fact probable that the airborne network would have disintegrated by the time strategic forces completed their attack in accordance with initial execution orders. Breakdown of the airborne network would probably begin while some bombers were still en route to targets, some missile submarines were en route to launch stations, and some land missiles were being readied for launch. By the time negotiations ensued, sometime following the initial exchange, the United States would depend on ground-based systems to manage strategic reserve forces, but these systems would have suffered extensive collateral damage and would remain under constant threat of attack and destruction by Soviet reserve forces.

These circumstances encourage comprehensive retaliation. A limited Soviet counterforce attack would trigger preplanned operations which, in conjunction with extensive collateral damage to the command system, creates strong pressures for rapid escalation regardless of what calculations political leaders might make at the time.

A limited Soviet counterforce attack could also cause enough collateral damage to weaken capabilities for Minuteman launch-under-attack. Even under relatively favorable conditions, successful implementation of a launch-under-attack decision would be uncertain. Under unfavorable conditions involving deliberate Soviet attack on U.S. C^3I to prevent launch-under-attack, the chances of successful implementation would be low. In any case, current technological conditions force a launch-under-attack decision before the character of enemy attack can be accurately assessed.

FOOTNOTES

1. Benjamin S. Lambeth, Selective Nuclear Options and Soviet Strategy (Santa Monica, California: The Rand Corporation, 1975), pp. 1, 18.

2. Ibid., p. 18.

3. Ibid., p. 4.

4. U.S. Congress, Senate, Subcommittee on Arms Control, International Law and Organization, U.S.-USSR Strategic Policies (Washington, D.C.: GPO, 1974), March 4, 1974, p. 13.

5. Ibid., p. 9.

6. Lambeth, Selective Nuclear Options and Soviet Strategy, p. 11.

7. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1977 Authorization For Military Procurement, Research and Development, 94th Congress, 2nd Session (Washington, D.C.: GPO, 1976), Part 4, p. 1972.

8. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Authorization For Military Procurement, Research and Development, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 10, p. 6699.

9. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 5, p. 4321.

10. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1964, 88th Congress, 1st Session (Washington, D.C.: GPO, 1963), Part 5, p. 819.

11. Senate Subcommittee on Arms Control, International Law and Organization, U.S.-USSR Strategic Policies, p. 13.

12. The missile silos nearest the launch centers are about three miles away. Silo attack using blast effects would generate blast overpressures of sufficient magnitude (5-10 p.s.i.) within a three-mile radius to destroy land lines and exposed antennas around launch center complexes. Ground bursts would also generate strong fields of electromagnetic energy within this three-mile radius. EMP might severely degrade VLF communications -- the system that is least vulnerable to blast overpressure -- and the unhardened computers and electrical systems used by launch centers.

13. This estimate applies to day-to-day conditions with most PACCS aircraft on ground alert. With the transfer of EC-135 aircraft from Grissom AFB to Rickenbacker AFB in the late 1970s, the set-up time for the PACCS network as a whole was reduced from one hour to thirty minutes. Interview with an Air Force General Officer in 1980.

14. Cobra Dane would be activated for attack early warning purposes at DEFCON 3 or higher. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations For Fiscal Year 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 4, p. 483.

15. "Improved U.S. Warning Net Spurred," Aviation Week and Space Technology, vol. 112, no. 25 (June 23, 1980), p. 41.

16. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1978, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), Part 2, pp. 392, 418.

17. Ibid.

18. Ibid.

19. Ibid, p. 387; and "U.S. Upgrading Ground-Based Sensors," Aviation Week and Space Technology, vol. 112, no. 24 (June 16, 1980), p. 241.

20. U.S. Congress, Senate, Committee on Armed Services, DoD Authorization for Appropriations for Fiscal Year 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 7, p. 4699.

21. House Committee on Appropriations, DoD Appropriations for 1978, Part 2, p. 390.

22. Ibid.

23. Senate Committee on Armed Services, DoD Authorization for Appropriations for Fiscal Year 1983, Part 7, p. 4700.

24. Ibid., p. 4705.

25. U.S. Congress, Senate, Committee on Armed Services, DoD Authorization for Appropriations for Fiscal Year 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), Part 6, p. 3456.

26. "Improved U.S. Warning Net Spurred," p. 38.

27. Ibid., p. 44.

28. Ibid.

29. U.S. Congress, Senate, Committee on Armed Services, DoD Authorization for Appropriations for Fiscal Year 1982, 97th Congress, 1st Session (Washington, D.C.: GPO, 1981), Part 7, p. 4222.

30. House Committee on Appropriations, DoD Appropriations for 1978, Part 2, p. 389.

31. "Improved U.S. Warning Net Spurred," p. 44.

32. Ibid., pp. 38, 45.

33. House Committee on Appropriations, DoD Appropriations for 1978, Part 2, p. 458 (emphasis added).

34. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 7, p. 1057. This testimony states:

> Each detector was connected to a separate signal generating station which was installed in a smalltown Western Union telegraph office located 30 to 40 miles from the target area. The communication links that interconnect the detector, the stations, the control centers, and the users were circuits routed over Western Union, Bell System, and railroad facilities.

35. See Chapter 5. See also "Early Warning Satellite Picked Up Flash Over South Atlantic," Defense Daily, vol. 114, no. 34 (February 23, 1981), p. 271; House Committee on Appropriations, DoD Appropriations For 1974, pp. 1057-58; and House Committee on Appropriations, DoD Appropriations for 1978, Part 2, pp. 386, 392.

36. Ibid., p. 386; and Senate Committee on Armed Services, DoD Authorization for Appropriations for Fiscal Year 1982, Part 7, pp. 4205-06. See also Chapter 8.

37. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 5968, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 2, p. 65.

38. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), Part 3, p. 1045.

39. Ibid., pp. 1045-47.

40. Report of the President's Commission on Strategic Forces (April 1983), pp. 7-8.

41. House Committee on Armed Services, Military Posture and H.R. 5968, p. 65 (emphasis added).

42. Time estimates attributed to D. Latham, Deputy Under Secretary of Defense (R+E). See U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 5, p. 47.

CHAPTER EIGHT

COMMAND MODERNIZATION PROGRAMS: THE DECADE AHEAD

Improvement in strategic C^3I is being advertised as the centerpiece of President Reagan's plan for strategic modernization. According to Reagan, C^3I modernization is crucial to the success of the overall plan. Without dependable C^3I, new weapons cannot be transformed into effective power.

Support for the decision to assign high priority to C^3I modernization runs deep and wide. Representative of the main body of opinion on this matter is the view expressed by the Scowcroft Commission:

> Our first defense priority should be to ensure that there is continuing, constitutionally legitimate, and full control of our strategic forces under conditions of stress or actual attack.... The Commission urges that this program continue to have the highest priority.[1]

The appearance of consensus is deceiving, however, for it masks a number of devisive issues. At issue are the proper aims of C^3I development, their technical feasibility, and their affordability. This chapter discusses these issues, which do not bode well for command modernization, before turning to assess specific programs in the modernization package.

ISSUES

Aims of C^3I Modernization

National security officials, both uniformed and civilian, frequently emphasize flexibility and endurance "through the post attack period" [2] in their formulation of both the essence of modern-day deterrence and the thrust of future C^3I development. Recitation of the underlying rationale is presumably tiresome by now; suffice it to mention once more the widely perceived need to solve the paradox of massive retaliation. A flexible, enduring command system is a logical derivation of the postulates of extended deterrence which currently prevails over traditional deterrence strategy based on massive retaliation.

The prevailing formulation, and its implications for command system development, are of course rejected, or at least challenged, by those who believe that a threat of swift and severe punitive damage in retaliation to nuclear attack is a sufficient deterrent. Many continue to subscribe to this view. If deterrence works at all, the argument runs, it will work at this level.

But there are also numerous observers who are at once sympathetic toward the administration's pursuit of flexible response and dubious of heavy investment in C^3I systems designed to support that strategy. One reason given is that timely, reliable C^3I in the early phase of conflict is needed in any case, and there is still ample room for improvement in this area. C^3I investment should therefore be channeled, at least for now, into programs that provide for high confidence force execution in the initial stage of a nuclear war. General L. Allen, Jr., former Air Force Chief of Staff, said recently that programmed modernization of the command system is, in fact:

> ... aimed at correcting deficiencies in survivability and performance of the glue that holds our systems together and permits us to control them in order to execute the forces. The principal efforts in this area are aimed at improving the survivability for our warning and communications systems because we think that those <u>initial communications are the most critical aspects to improve at the present time</u>. In time, we will move forward with additional improvements that will permit some increased enduring survivability of our command and control systems to permit survival in the event of a protracted nuclear conflict.[3]

General Allen's observation is accurate. The lion's share of investment in strategic C^3I is indeed devoted to improving initial survivability. For all the rhetoric about gearing C^3I for protracted conflict, remarkably little attention and resources are actually being devoted to managing strategic weapons beyond the first few hours of a nuclear conflict. Resources allocated to this purpose, moreover, are concentrated in research and development, not deployment, as the <u>FY 1984 Annual Report</u> testifies:

> Over the next five years, we are proceeding with several programs that will improve the survivability of our strategic C^3 systems. We are also pursuing a comprehensive research and development program to ensure enduring communications connectivity during a nuclear war.[4]

This pursuit of "enduring connectivity" is just beginning. And the challenge is not simply technological in nature. A political consensus must also be garnered. The solid consensus behind near-term improvements designed to enhance initial C^3I survivability does not by any means imply blanket approval for any C^3I endeavor. The more ambitious goals, for example endurance, whose programmatic embodiments have found temporary refuge in R & D, will eventually surface to face aggressive scrutiny. And certain resistance. It is open to question whether the political-bureaucratic support needed to buy and field advanced systems can be mustered. But there is little doubt that the abstractly stated aims of this administration have not yet been embraced in their entirety, and that future endorsement of concrete measures to accomplish these wide ranging aims will require very spirited promotion. And there is no doubt that many will insist upon correction of basic C^3I deficiencies as a condition of support for more ambitious undertakings.

Technical Feasibility

A technological challenge of daunting dimensions accompanies the C^3I goals laid out by the Reagan administration. Defense officials seem keenly aware of this. As C. Weinberger states in his FY 1984 Annual Report: "Protecting a command, control, and communications system for nuclear forces is particularly difficult." [5]

The difficulties notwithstanding, the administration seems convinced that C^3I flexibility and endurance are realistic goals. But skepticism runs deep throughout the defense community. Among others who do not share the administration's sanguine view of the possibilities, Ball and Steinbruner question whether a high confidence solution to the C^3I problem even exists. Ball concludes that:

> The capability to exercise strict control and coordination would inevitably be lost relatively early in a nuclear exchange [and] the allocation of further resources to improving the survivability and endurance of the strategic command-and-control capabilities cannot substantially alter this situation. [6]

In this same vein, Steinbruner contends that a high-confidence technical solution probably cannot be achieved at feasible cost. [7]

The administration official who is closest to current research and development activity admits that the magnitude of the "enduring connectivity" problem is indeed very great: "I will tell you, we haven't solved all the problems by any means yet.... It has a long way to go." [8]

In the meantime, threats to the developing technologies could emerge. Since the time frame for deployment of new C^3I systems generally extends well into the 1990s, both the character of the Soviet threat and its impact on the performance of new U.S. systems are difficult to gauge. Not only are solutions to some problems not at hand, in some cases the problems have not yet crystallized.

It is nonetheless possible to anticipate some specific threats that may surface to diminish the present value of certain key R & D programs. Those devoted to "enduring connectivity," for instance, will lose import if Soviet antisatellite (ASAT) capabilities expand faster than expected.

U.S. R & D is concentrating on ground mobile C^3I and advanced communications satellites to bolster endurance. The proposed satellite network will consist mainly of extremely high frequency (EHF) channels provided by a constellation of MILSTAR satellites. This constellation would be an integral part of ground mobile operations since it is programmed to be the primary communications link between ground mobile units. MILSTAR is also expected to connect these units with the individual forces.

The promise of this R & D thrust clearly hinges on future Soviet capabilities to conduct antisatellite warfare against MILSTAR. If this critical node could be effectively destroyed, ground mobile units could be isolated from each other and from the forces. Although a threat to MILSTAR apparently has not been projected, the Soviets cannot fail to notice that the MILSTAR constellation will become the future backbone of the U.S. command system. It would be quite unreasonable to assume that the Soviets will not pursue MILSTAR ASAT programs. To the contrary, it is reasonable to suppose that our MILSTAR program will stimulate a concerted Soviet effort to design ASATs to counter it.

There are many other aspects of the future threat environment that diminish confidence in the technical feasibility of C^3I systems under development. For instance, the vulnerability of ground mobile units to direct nuclear effects would depend on the Soviets' intelligence-cycle-time. The pertinent question is whether ground units could be detected, and if so, whether they could be safely relocated between the time of detection and the time of enemy weapon arrival. There are no good answers to these questions.

Only in the most narrow sense of the term "technical feasibility" is any confidence in ongoing R & D warranted. Merely as pieces of equipment, many of the items under development will undoubtedly work. Many others will almost certainly work. But such demonstrations will say little about wartime performance of the various elements, much less their collective capability to satisfy operational demands such as "enduring connectivity." Optimism is unwarranted, we believe, particularly in light of the very real potential of the Soviet Union to develop offsetting systems.

Cost Control

While strategic C^3I programs are being trumpeted as the new centerpiece of U.S. strategic policy, a massive infusion of new funds into this area has not been forthcoming. Contrary to common belief, obligated funds will remain virtually constant in real terms over the next five years (see Figure 8-1) in almost every major category of interest. MILSTAR, an all-purpose satellite system intended to serve a

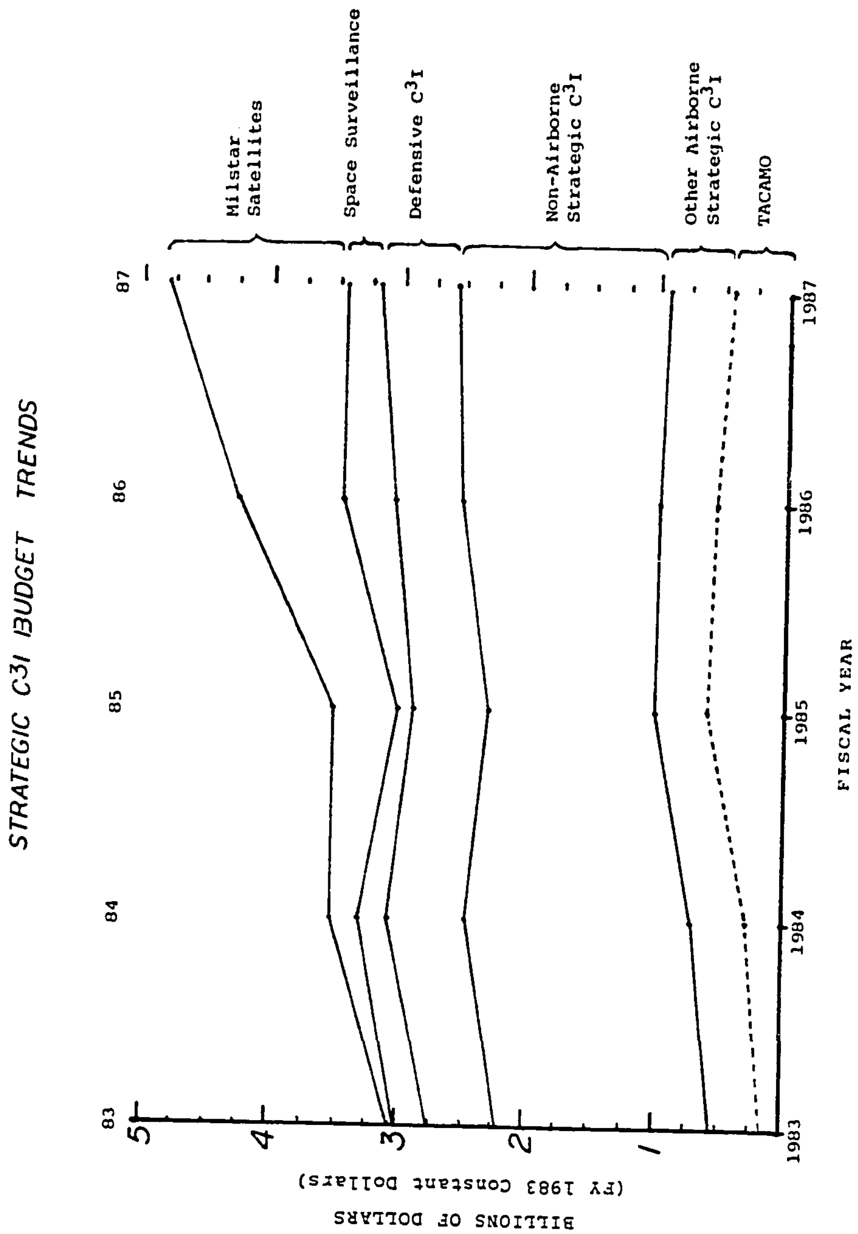

STRATEGIC C3I BUDGET TRENDS
Milstar
Satellites
Space Surveillance
Defensive C^3I
Non-Airborne
Strategic C^3I
Other Airborne
Strategic C^3I
TACAMO
83
84
85
86
87
5
4
3
2
1
BILLIONS OF DOLLARS
(FY 1983 Constant Dollars)
1983
1984
1985
1986
1987
FISCAL YEAR

Figure 8-1

variety of users besides strategic units, is responsible for any substantial real growth in the strategic C^3I budget. If the total cost of MILSTAR is assigned to the strategic C^3I account, the strategic C^3I budget will grow at an average annual rate of 11.9 percent between 1983 and 1987 (see Figure 8-2). If MILSTAR is not counted, the budget will grow at an average annual rate of only 3.6 percent.

Figure 8-2

RATE OF REAL GROWTH IN STRATEGIC C^3I

	1983-1984	1984-1985	1985-1986	1986-1987	Avg.
Without MILSTAR	+10.3%	-7.8%	+10.9%	+0.9%	+3.6%
With MILSTAR	+15.3%	+0.4%	+17.5%	+14.5%	+11.9%

Relative to the defense budget as a whole, strategic C^3I represents a thin slice of the pie. And its share will not expand significantly. In FY 1983, strategic C^3I represented 1.3 percent of the total defense budget. Whether MILSTAR costs are included or not, strategic C^3I will still claim the same small share of the total defense budget for the next five years (see Figure 8-3).

As a fraction of the total strategic budget, strategic C^3I will actually decline in real terms during this period. Due to the large projected increase in strategic offensive weapon investment, strategic C^3I expenditure will decrease from about 12 percent in FY 1983 to about

STRATEGIC C^3I BUDGET 1983 - 1987

(FY 1983 CONSTANT DOLLARS)

	ALL STRATEGIC C^3I PROGRAMS (MILLIONS)		PERCENT OF TOTAL STRATEGIC BUDGET[a]		PERCENT OF TOTAL DEFENSE BUDGET[b]	
	MILSTAR INCLUDED	MILSTAR EXCLUDED	MILSTAR INCLUDED	MILSTAR EXCLUDED	MILSTAR INCLUDED	MILSTAR EXCLUDED
1983	3,074	2,994	11.8	11.5	1.3	1.3
1984	3,544	3,301	11.8	11.0	1.4	1.3
1985	3,558	3,045	10.2	10.2	1.2	1.1
1986	4,179	3,376	10.2	8.2	1.4	1.1
1987	4,783	3,407	10.4	7.4	1.5	1.1

	AIRBORNE WWMCCS (BILLIONS)	PERCENT OF TOTAL STRATEGIC BUDGET[a]	PERCENT OF TOTAL DEFENSE BUDGET[b]
1983	576	2.2	0.24
1984	704	2.4	0.29
1985	1,026	2.9	0.40
1986	1,005	2.5	0.39
1987	978	2.1	0.31

[a] Based on est. Strategic Budgets (in billions constant FY 83 dollars): 1983=26; 1984=30; 1985=35; 1986=41; 1987=46.

[b] Based on est. DoD Budgets (in billions constant FY 83 dollars): 1983=240; 1984=254; 1985=289; 1986=305; 1987=317.

Figure 8-3

7 percent (excluding MILSTAR) or 10 percent (including MILSTAR) by FY 1987. Strategic weapon programs will take a larger and large share of the total strategic budget, at the expense of strategic C^3I. The all-important airborne segment of the strategic command system will continue to claim about 2 to 3 percent of the strategic budget, or about 0.3 to 0.4 percent of the total defense budget.

These figures raise some doubt as to whether the Reagan administration's pledge to overhaul the command system is genuine. If it is truly believed that major C^3I repair is urgently needed, and if the administration truly intends to preside over a fundamental shift in strategic priorities, there is no marked shift in near-term spending to evidence this intention. There are of course better barometers of prevailing resolution, but the absence of strong economic correlates seems to belie the impression given by this administration that effort to revamp C^3I is being redoubled, that weapons and C^3I programs are competing for funds on an equal basis, and that C^3I modernization is really regarded as the key to a revitalized strategic posture.

In reality, weapons programs continue to be the main preoccupation of the Department of Defense and the main beneficiaries of this administration's defense largess. Flirtation with the idea that the strategic problem should be redefined simply has not developed into a deep commitment.

The Reagan administration, however, has stimulated a research and development program that could eventually summon such a commitment. There are many embryonic programs under development which promise to serve up an expansive and very costly C^3I system, one that would put commitment to an actual test. These programs could force the kind of hard choices that the present administration says it is prepared to make (indeed that have supposedly been made already).

The cost of deploying these programs cannot be precisely estimated, but a severalfold increase over the current level of expenditure is not farfetched. Sustained investment on this scale would doubtless meet stiff and widespread resistance. The view that the United States can afford such investments is not likely to be advanced, and even less likely to prevail.

PROGRAMS

Virtually all of the programs examined in this section were begun before President Reagan took office. Most deal with problems of positive control launch during the initial phase of Soviet attack; initial SIOP decisionmaking; and communications for SIOP execution. Few were designed to endure beyond a few hours or days. The Reagan administration is usually responsible for those systems designed to operate for weeks or months in a nuclear environment. In many instances, though, such systems are outgrowths of earlier concepts or prototypes. Under the Reagan administration, development of these concepts/prototypes has been accelerated as part of an intensified search for solutions to the "enduring connectivity" problem. But although this is the administration's central research and development theme, few solutions have been produced and C^3I R&D today is mainly oriented to completion of systems that improve upon current capabilities to execute the SIOP. In sum, the thrust of the projects described below is to ensure that the threat of massive retaliation cannot be removed by a Soviet attack on the U.S. command system.

Major modernization programs were recently itemized and grouped as follows: [9]

I. Warning and Attack Assessment

- Survivability upgrades to early warning satellites
- Mobile ground terminals (MGTs) for warning data readout
- Two new PAVE PAWS radars
- Modernization of BMEWS radars
- Integrated Operational Nuclear Detonation Detection System (IONDS)
- Advanced warning concepts in R&D

II. Command and Decision

- Nuclear effects hardening for NCA/JCS and CINC airborne command posts
- Mobile Command Centers (MCC) for NCA/JCS and CINCs
- Survivability and capabilities improvements for fixed command centers
- Other survivable command basing options under study

III. Strategic Communications

- Ground Wave Emergency Network (GWEN)
- New ECX aircraft for TACAMO
- MILSTAR EHF communications satellite system
- LF/VLF radio receivers on bombers
- DSCS-III satellite production
- ELF for communications to submarines
- Three additional fleet communications satellites (FLTSATCOM)
- Reconstructible communications concepts under study

These programs are intended to improve upon existing capabilities to perform the following functions: (1) positive control launch of ground alert bombers and command-communications aircraft during the early phase of Soviet attack; (2) national decisionmaking; (3) dissemination of retaliatory orders; and (4) postattack management of reserve forces. As shown in Figure 8-4, the systems that support these functions cut across the three categories delineated earlier.

Positive Control Launch

Because the entire bomber force and most command-communications aircraft are normally maintained on ground alert, survival measures must be promptly instituted to prevent their destruction on the ground. Sensors must reliably and rapidly detect enemy missile launches. Sensor data must be transmitted over rearward communications channels

Programs	Positive Control Launch	NCA Decisionmaking (Initial SIOP Decisions)	SIOP EAM Dissemination (Initial Execution Msg)	Protracted War Force Management
I. Warning and Attack Assessment				
Satellite Survivability Upgrades	X	X		
Mobile Ground Terminals	X	X		X
Pave Paws Expansion	X	X		
BMEWS Modernization		X		
IONDS		X		X
Advanced Warning Concepts		X		X
II. Command and Decision				
Airborne Command Post Hardening		X	X	
Mobile Command Centers				X
Fixed Command Center Improvements	X	X	X	
III. Strategic Communications				
Ground Wave Emergency Network	X	X	X	
ECX Tacamo Aircraft			X	
MILSTAR Satellites	X	X	X	
Bomber LF/VLF Mini-receivers			X	
DSCS III Satellites	X	X	X	
Extremely Low Frequency Submarine Comm.			X	
FLTSATCOM Satellites			X	
Reconstructable Networks				X

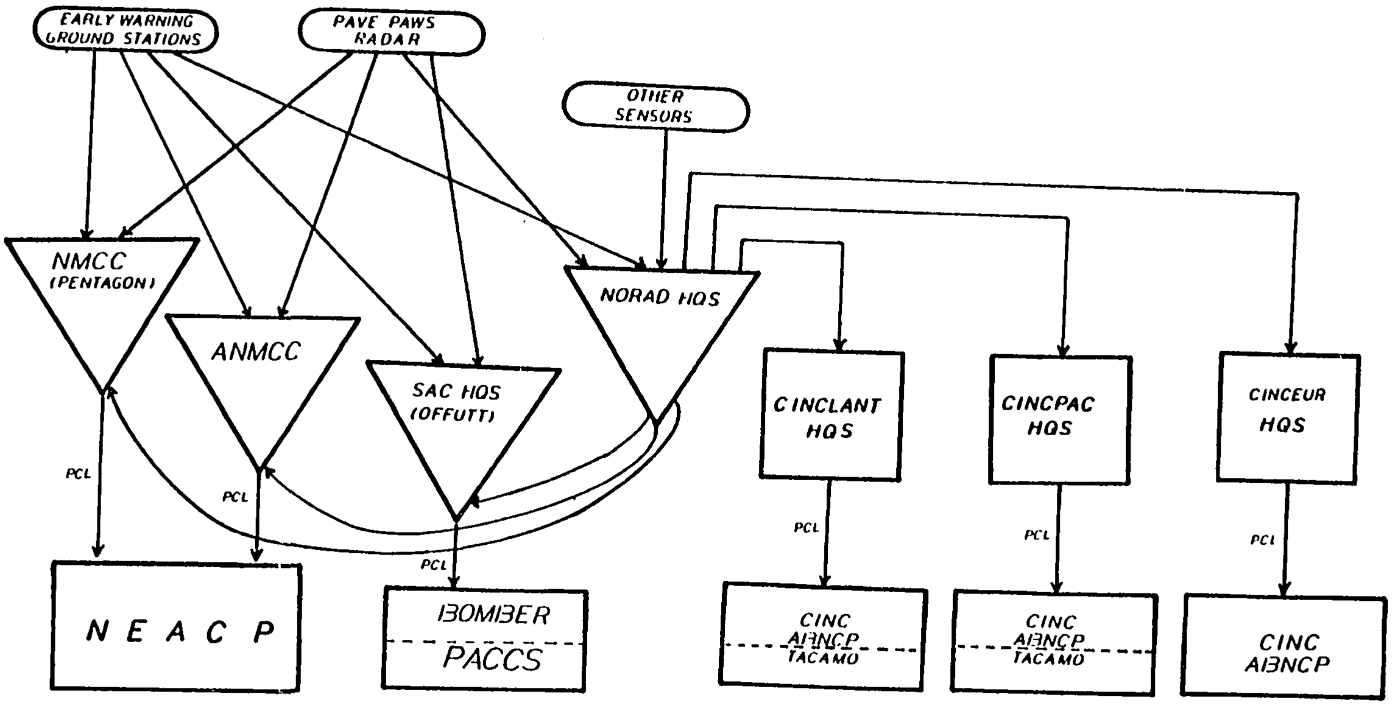
Figure 8-4

to commanders. PCL decisions must then be made and sent over forward communications channels to the aircraft units on ground alert. The basic circuitry used to effect PCL is depicted by the flow diagram in Figure 8-5.

Destruction of this circuitry by blast effects could begin as early as 7-10 minutes after the first launches of enemy submarine missiles.[10] Serious degradation could be experienced even earlier from sabotage, jamming, and various nuclear weapons effects produced by high altitude nuclear explosions. DoD therefore plans:

> ... improvements that let us survive the first minutes of an attack, even before the destructive bursts on the ground come in, through the period of high altitude burst with the electromagnetic pulse and various atmospheric disruptions and magnetic field interruptions, the jamming periods, and the destruction as the SLBMs begin to arrive....[11]

Since enemy missile launches are initially detected by early warning satellites,[12] — the one early warning satellite over the Eastern Hemisphere and the two satellites over the Western Hemisphere provide the first warning of launches of ICBMs and SLBMs, respectively[13] — considerable effort is being made to protect the satellites themselves, the ground readout stations, and the associated communications from sudden attack. Upgrades to the satellites themselves include improved sensors,[14] which will be more sensitive to the infrared signature of Soviet SS-N-6 submarine missiles.[15] Features that protect the infrared detectors against laser attack are also being incorporated.[16]



POSITIVE CONTROL LAUNCH (PCL)
CIRCUITS

Figure 8-5

Protection of the ground readout stations is the primary focus of current effort. At present, the early warning satellite system is said to be vulnerable because the satellite data comes down to fixed ground stations,[17] where the data is processed and disseminated.[18] In the official estimation, while the synchronous altitude satellites themselves are "relatively survivable," the fixed ground stations "would be vulnerable to physical attack or even sabotage."[19] An unofficial assessment is that:

> the ground stations at Buckley Field, Colo., and Pine Gap/Alice Springs [Woomera], Australia, are the weakest link. These are now the only two fully operational DSP ground stations, and early warning officials are extremely concerned about their vulnerability to acts of sabotage as well as to internal accident, which could cut by half, or even 100% in the case of coordinated sabotage, the front-line early warning capability.[20]

The loss of ground stations to sabotage, accident, conventional or nuclear attack could have untoward consequences of two sorts. On one hand, failure to PCL in response to an outage (of perhaps undetermined origin) would put bombers and command aircraft in jeopardy if enemy missile attacks were subsequently initiated. On the other hand, bomber PCL in response to the loss of a ground station could be a dangerous overreaction. Regarding the latter situation, the director of DCA once speculated on the possible consequences of an outage of the overseas ground station:

> It could be neutralized or destroyed using a number of pretexts during a period of tension, depriving us of warning at a critical juncture. This could force the NCA to place a large proportion of the

> SAC bomber fleet on airborne alert, which in itself becomes a provocative action since it could be interpreted by an enemy as an intent to preempt and thus spark the very attack we are trying to deter.[21]

A set of transportable Simplified Processing Stations (SPS) was originally planned to augment, and possibly replace, the vulnerable fixed stations. One such unit was actually developed. Testimony discloses that the SPS was to be redeployed from CONUS to an overseas location in 1982 as a backup to an existing ground terminal, and was expected to be operational there in April 1982.[22] This deployment would add a small increment of readout redundancy but not survivability, as SPS becomes a fixed target once it is set up. It is transportable but hardly mobile in any practical sense.

Mobile ground terminals (MGTs) were therefore developed to augment the existing fixed readout stations. DoD is procuring six of these truck-mounted terminals.[23] The terminals will receive early warning satellite data, process it, and then relay the data through supporting communications to various users.[24] Because MGTs can be moved around in a random manner, they are expected to present a very difficult targeting problem to Soviet planners.[25] At least, the MGTs "will be far more survivable than the existing fixed terminals."[26]

Accompanying each MGT truck will be a communications van equipped with a jam resistant secure communications (JRSC) terminal.[27] JRSC terminals, described as providing a sensor data network and secure voice/graphics for tactical warning,[28] will operate with the Defense Satellite Communications System III (DSCS-III), a four-satellite constellation to be fully operational by 1986. (Launch dates: 1982, 1983, 1984, 1985.)[29] DSCS-III satellites were designed to withstand jamming and nuclear effects such as SGEMP.[30] They were also designed to function autonomously, for weeks or months, without ground assistance for on-board maintenance.[31]

This combination of new systems -- MGTs, JRSC vans, and DSCS-III satellites -- will appreciably mitigate current vulnerability to jamming, sabotage and direct attack. To the extent that this system reduces reliance on leased terrestrial communications for data dissemination to users, it will also mitigate vulnerability to electromagnetic pulse effects.

Additional insurance against disruption of the PCL circuitry will be purchased in the form of the Ground Wave Emergency Network (GWEN). This system will consist of numerous unmanned, LF radio sites. The sites will be hardened against electromagnetic pulse,[32] and they will ultimately interconnect warning sensors such as PAVE PAWS radars with NORAD, national command centers, SAC Headquarters, and other strategic units including bomber and ICBM bases. The LF ground radio wave will permit secure, two-way data exchange in a nuclear environment. Deployment of GWEN is proceeding in stages. By the end of 1983, a nine-node network connecting SAC Headquarters, NORAD and a few other units is expected to be operational. Figure 8-6 shows the locations of these nodes (asterisks). The other nodes in the diagram will be added to the network in the second stage of deployment. This network is referred to as the thin line network, which is expected to be

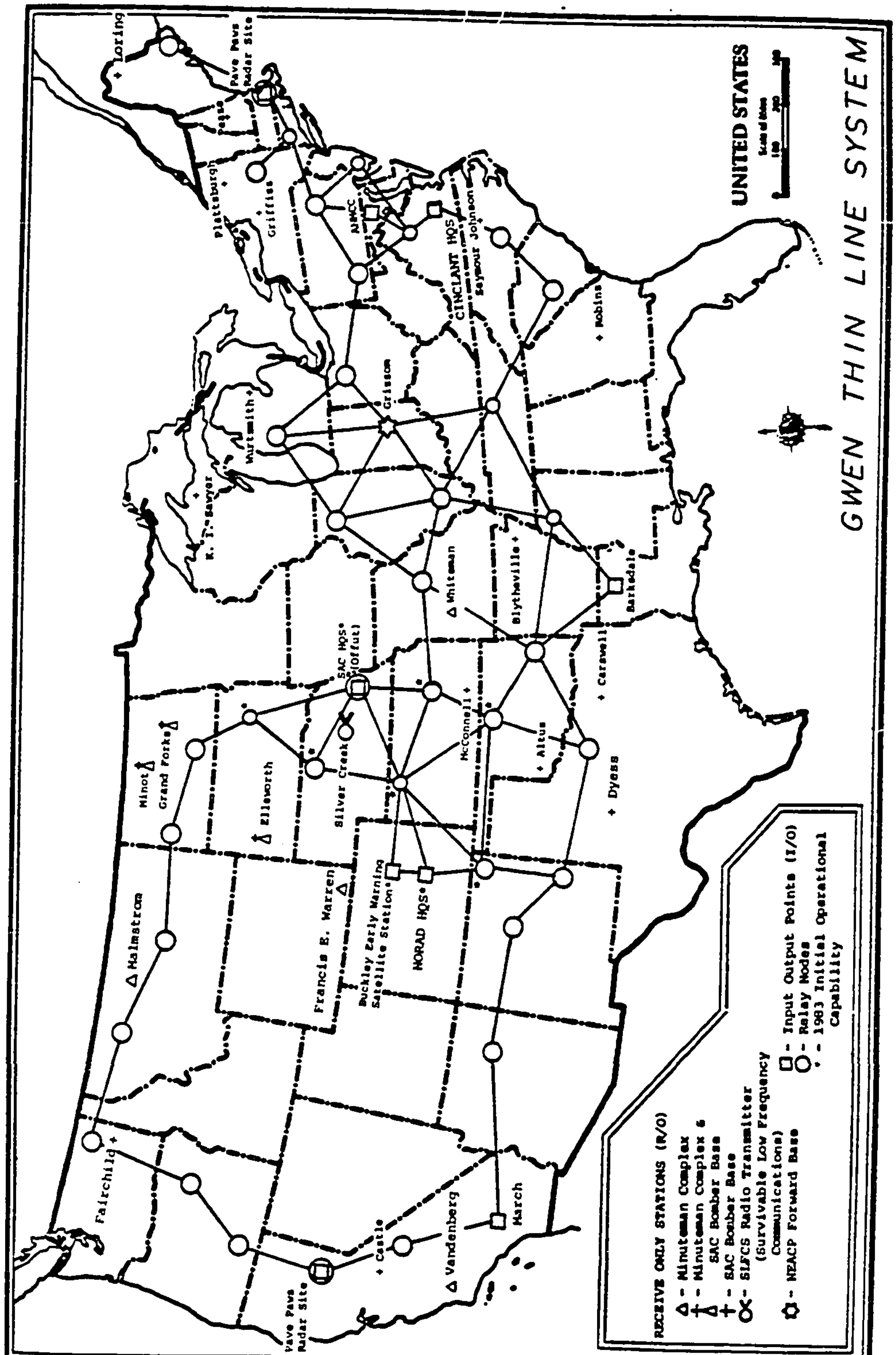

GWEN THIN LINE SYSTEM
UNITED STATES
Loring
Pave Paws Radar Site
Pease
Plattsburgh
Griffiss
ANMCC
CINCLANT HQS
Seymour Johnson
Robins
Grissom
Wurtsmith
K. I. Sawyer
Whiteman
Blytheville
Barksdale
Carswell
SAC HQS (Offutt)
McConnell
Altus
Dyess
Minot
Grand Forks
Ellsworth
Silver Creek
Francis E. Warren
Buckley Early Warning Satellite Station
NORAD HQS
Malmstrom
Fairchild
Castle
Vandenberg
March
Pave Paws Radar Site
RECEIVE ONLY STATIONS (R/O)
Minuteman Complex
Minuteman Complex & SAC Bomber Base
SAC Bomber Base
SLFCS Radio Transmitter (Survivable Low Frequency Communications)
NEACP Forward Base
Input Output Points (I/O)
Relay Nodes
1983 Initial Operational Capability

Figure 8-6

operational in 1984.[33] In the third stage, a network composed of several hundred nodes would be deployed.[34]

It has been contended that GWEN could serve many purposes: convey minimum tactical warning information to national and senior military authorities along with CINCNORAD's assessment of its validity; carry PCL decisions to the forces; and even disseminate the SIOP execution message.[35] Initial capability is of course very limited; the nine-node network merely augments the EMP-vulnerable leased circuits that connect an early warning satellite ground station (Buckley), NORAD, and SAC Headquarters. This link is intended to withstand the effects of high altitude explosions, not direct SLBM/ICBM attack. The thin line network could, in theory, serve all the various purposes, but only under a restricted set of circumstances. If directly attacked by even a relatively small number of nuclear weapons, the thin network would be readily severed. Its utility is therefore mainly limited to the period of high altitude explosions and jamming which could precede weapons impact by several minutes. Full deployment of several hundred nodes would increase the chances that GWEN could continue to function during an SLBM attack, and possibly during an ICBM attack, especially if the nodes were not attacked directly. This expansion is hard to justify, however, in view of the high risk that the fixed C^3I facilities that GWEN serve would be struck and destroyed. Many of these facilities could be neutralized by SLBMs; all could be destroyed by ICBMs. In short, the promise of GWEN lies primarily in its resistance to indirect nuclear effects produced during the short period that precedes weapon impact.

Two other programs that could improve PCL capabilities are PAVE PAWS and improvements to fixed command posts. (MILSTAR is also promising in this regard, but this is not its primary role.) PAVE PAWS are phased-array radar sensors designed to detect submarine missiles launched against the United States. Two radars, one on each coast (Massachusetts and California), are presently operational. Their 3,000 n.mile range extends coverage over a vast expanse of both oceans, but deployment of two additional PAVE PAWS radars is necessary to close gaps in coverage of potential launch stations to the southeast and southwest.[36] Although these areas are continuously monitored by early warning satellites, DoD contends that both space-based infrared and ground-based radar coverage of the same events increase the probability of detection while lowering the risk of false alarm. Without "dual phenomenology," the United States might, for instance, hesitate to flush the bombers in the event of an actual attack. Alternatively, we might order the bombers into the air on the basis of false indications from a single detection source.

PCL decisions require confidence not only in the performance of the sensors and communications channels (rearward and forward), but also the decision centers themselves. Various improvements in survivability and capability have been proposed to increase this confidence. Protection against EMP effects which threaten to disrupt tactical warning computers and displays as well as communications is especially important. If such disruption occurred during the first few critical minutes of an attack, fatal delays in CINCNORAD and SAC decisionmaking, for example, could result. CINCNORAD is responsible for determining whether detected missile launches pose a threat to North America.[37] That assessment may well be the principal basis on which other commanders, for example CINCSAC, decide whether to flush their bomber and/or command-communications aircraft. At NORAD's Cheyenne Mountain Complex -- the hub of tactical warning/attack assessment processing and decisionmaking -- hardening against EMP is reportedly under way, as is a program to supply battery-based uninterruptible power.[38] The SAC Command Post, where PCL decisions are made, is also being shielded against EMP effects.[39]

Even if the details of these programs were open to public examination, it would still be premature to pass judgment on their impact on U.S. capability to effect a successful positive control launch of bombers and command aircraft. On the surface, they appear to be addressing critical deficiencies such as the vulnerability of existing PCL circuitry to electromagnetic pulse effects.

In the end, however, they cannot alter the fact that submarine-launched missiles could impact at approximately the same time that aircraft would be taking off. As analysis presented in earlier chapters explained, some aircraft would react too slowly to survive attacks, even if the warning sensors and PCL circuitry performed perfectly. And in instances where aircraft survival is theoretically expected, the margin of safety is thin. An unanticipated failure of some unknown component -- technical or procedural -- in this complex system could have catastrophic consequences for the prelaunch prospects of aircraft on ground alert.

NCA Decisionmaking

As soon as initial detection of an attack is received at SAC Headquarters and other selected CINC headquarters, actions are taken to increase the readiness of respective alert units.[40] For instance, when indications of SLBM attack appeared on the SAC command post display on two separate occasions in June, 1980, the SAC duty controller directed all alert crews to move to the alert aircraft and start their engines in order to prepare to take off should that become necessary in order to survive.[41] If the NORAD commander determines the possibility of a threat, the next step is to convene a Threat Assessment Conference.[42] This telecommunications conference brings the JCS Chairman and other senior commanders at various command posts -- mainly, the NMCC, ANMCC, SAC HQs, and NORAD -- into the evaluation.[43] Further steps to enhance the survivability of alert units are taken.[44] For instance, a Threat Assessment Conference was convened in June 1980 and "as part of the ongoing reaction of the threat assessment conference, the Pacific Command airborne command post took off...."[45]

If the threat persists a Missile Attack Conference, which brings in all senior personnel, including the president, is convened.[46] NORAD's role through this period is to "analyze the attack, characterize the threat, and provide the most current information available to Washington, D.C. and certain other locations."[47] This tactical warning/attack assessment information is processed and displayed in common format at four major command centers equipped with so-called CCPDS computer-based displays. [48] These command centers are NORAD, NMCC, ANMCC and SAC. [49] The objective of the conference among these major command centers "is to get to the National Command Authority [the NCA] the information he needs to make a coherent, useful decision.... the purpose of that conference is to get a decision." [50] The NCA must digest the information, weigh it, evaluate response options, and reach a SIOP decision. [51] And the decision must be reached quickly. In CINCSAC's words, "the time available to reach a decision is critically limited due to the flight time of Submarine Launched Ballistic Missiles (SLBM)." [52] As noted earlier, SLBM impacts could begin as early as 7-10 minutes after the first enemy missile breaks water.

Information forwarded to the president during this short period, assuming the president has by then been added to the Missile Attack Conference, originates at the warning sensors. Improvements to these sensors, besides providing greater assurance of early detection in order to effect PCL actions, are meant to provide the president and his senior advisors a better picture of the character of the attack, on the basis of which a SIOP option could be selected from the alternatives available. PAVE PAWS radars, for example, are slated for a power upgrade that increases these sensors' ability to observe MIRVs, estimate raid size, and predict impact areas. [53] BMEWS radars, which are oriented toward ICBM arrival corridors, are also slated for modernization. DoD plans to replace the pre-1960 vintage computers and enhance the tracking radars to allow discrimination of smaller targets for more accurate counting of incoming warheads.[54] The BMEWS system originally (early 1960s) was designed to detect an attack consisting of twenty or more missiles incoming within a 5-minute interval.[55] DoD now requires the ability to detect and characterize an attack involving thousands of reentry vehicles.[56] The basic deficiency in the present system is that the tracking radars cannot resolve objects well enough to determine their number and direction.[57] BMEWS is prone to undercounts and can only determine whether the ICBM attack "is headed toward the continental limits of the United States."[58] The proposed improvement would allow better estimation of attack size and impact points -- estimates that should be sufficient to verify, for example, an attack on the Minuteman force.[59] The importance of this improvement is summed up by a DoD official in this way:

> If the NCA discovers that the attack is on him, he can transfer early to the succession of command. If he determines that it is headed toward the [U.S.] ICBM field, he can make one decision. If he determines it is headed toward New York City or Chicago, he can make another decision. This is what this is all about.[60]

Several of the programs discussed in the preceding sections -- survivability upgrades to warning satellites, mobile readout terminals for the satellites, GWEN and DSCS-III communications for rearward transmission of attack assessment information -- will also expand the potential for an informed national decision on the employment of strategic weapons. In addition, the early warning satellites are reportedly being redesigned to provide more refined calculations of missile launch azimuth and missile type; these parameters define where the hostile missiles came from and where their weapons are headed.[61] Advanced warning concepts in R&D, however, offer the best hope of accurate assessment of incoming missiles. The most promising concept involves application of new infrared sensor technology to warning missions. Using current infrared technology, early warning satellites lose track of missiles in their midcourse flight after booster burnout, owing to a drastic decrease in the missile's infrared emissions.[62] The new infrared technology, though in its infancy, could permit future early warning satellites to track dispensed reentry vehicles until ground radars acquire them late in their trajectory.[63]

The president, aided by the NORAD commander, CINCSAC, other senior military commanders and civilian advisors, is supposed to reach a decision on the basis of this attack assessment information within a very compressed time frame. In the extreme case of SLBM weapon impacts 7-10 minutes after breakwater, some information would be unavailable before targeted command centers on the ground were destroyed. Several sensors such as BMEWS (and PARCS) radars would not have detected a single ICBM before the principal users of sensor data began to come under attack. Disruption of the telecommunications Missile Attack Conference could occur even earlier if some SLBMs are detonated at high altitude during the upward portion of their trajectory.

As noted earlier, EMP-resistant communications such as GWEN, coupled with EMP-shielding for major command centers such as SAC Headquarters, will help protect PCL circuitry. But additional EMP-protected circuitry, with higher channel capacity for voice communications is needed to support a telecommunications conference. Two programs under development could improve upon existing telecommunications media (EMP-vulnerable leased circuits for voice conference and blackout-prone AFSATCOM circuits for low-speed teletype conference): DSCS-III and MILSTAR. DSCS-III satellites, besides providing channels for relaying warning data to major command centers, would provide a separate wide-band channel for voice conferencing among those centers. There is a major drawback, however. Operating at SHF frequency, DSCS-III signals are susceptible to scintillation effects from high altitude nuclear explosions. By contrast, the proposed MILSTAR constellation (see description and discussion below) will operate at the extremely high frequency (EHF) band of the radio spectrum, which is not susceptible to blackout or scintillation.[64] EHF also presents an opportunity to build a very high degree of jam resistance into the system.[65] DoD reports that MILSTAR will incorporate features that effectively counter jamming threats postulated for the 1980s-1990s.[66] For this reason, and because satellite-to-satellite cross-links will interconnect the NCA and CINCS without using intermediate ground stations,[67] MILSTAR could help ensure the participation of even the most distant parties, for example CINCPAC and CINCEUR, in the Missile Attack Conference during the critical period between missile launch detection and weapon impact, a period in which existing telecommunications conferencing media could be severely degraded by a combination of jamming, sabotage and high altitude nuclear explosions.

None of these improvements, however, can relax the severe time constraint under which the decision process must strain. The time available to decisionmakers at fixed ground facilities will continue to be extremely short. It seems unreasonable to expect a rational decision on the employment of strategic forces to be reached in less than ten minutes (give or take five minutes, depending upon the location of enemy submarines), with or without support from a sophisticated modern command system.

During the short preimpact period, the United States would be doing well just to flush the bomber force and the airborne command system (unless already generated to airborne alert), and to transfer the SIOP decisionmaking function to airborne platforms. And after this transition, the United States would be doing well if a rational decision on the employment of strategic forces could be reached.

The prospects of a successful PCL of command aircraft were evaluated earlier. As noted, the prelaunch survival of some command aircraft will be uncertain even after PCL circuitry has been modernized. In the category of doubtful survivors are the aircraft normally maintained on ground alert within close range of enemy submarines: CINCLANT airborne command post, CINCPAC airborne command post, CINCEUR airborne command post, and NEACP when forward-based at Andrews AFB, Maryland. Relocation of NEACP to Grissom AFB, Indiana,[68] increases its chances of survival, but by no means assures it.

Transfer of SIOP execution authority could be relatively straightforward if NEACP is successfully launched on tactical warning (PCL launch) or strategic warning (crisis-generated launch). Upon the destruction or isolation of fixed national command centers, NEACP could immediately assert release authority if an NCA successor were onboard (a generated scenario). NEACP could eventually assert release authority if communications with the NCA or a successor on the ground could be established (a surprise or possibly generated scenario). Transfer of authority to an airborne platform could be problematic if NEACP fails to survive the initial SLBM attack or fails to make contact with the NCA or a successor.

Three of the programs listed in Figure 8-4 directly address problems of SIOP decisionmaking once that responsibility shifts to airborne platforms: IONDS, MILSTAR, and ABNCP hardening. The first, called Integrated Operational NUDET Detection System (IONDS), places nuclear explosion detectors on a constellation of eighteen satellites, whose primary mission is navigation. These piggyback detector packages will be deployed on the GPS NAVSTAR navigation satellites intended to supply reconnaissance and strike forces with position fixes and precise clock time.[69] The IOC is 1988.[70] The IONDS packages dispersed on this navigation constellation which spans the globe will provide real-time measurements of nuclear explosions anywhere in the world.[71] Its purpose, according to DoD, is to provide trans- and postattack damage assessment information to the national command authority.[72] Its accuracy is reported to be less than 100 meters.[73] Its most significant feature, though, may be its ability to transmit reports directly to airborne command posts.[74] Today, the "fusion" centers for collection, analysis and dissemination of pre- and poststrike attack assessment information are the major fixed facilities, for example, NORAD; NEACP and other airborne command posts tie into this network via ground entry points and leased terrestrial communications. By all indications, aircraft access to attack assessment information could be permanently lost shortly after SLBM attack commences. Early destruction of the ground entry points, or the fusion centers, or the interconnecting land lines, leads to early isolation of airborne command posts. They lose access to intelligence data at the same time that responsibility for SIOP decisionmaking devolves to them. IONDS may ensure that the airborne commanders have continuing access to vital data. Indeed, accurate information on the number and location of nuclear explosions as they actually occur seems essential to informed SIOP decisionmaking. It also seems far more informative, reliable and definitive than prestrike assessments of the attack's apparent character.

MILSTAR's contribution to airborne SIOP decisionmaking lies in its potential to provide direct voice communications channels among key command aircraft -- NEACP, CINCLANT, CINCPAC, CINCSAC, and CINCEUR airborne command posts. At present, AFSATCOM provides the only means by which these aircraft could practically conduct a Missile Attack Conference in the absence of ground entry points and access to distributed commercial lines. But the limitations of this media are such that a conference probably could not be held. AFSATCOM conferencing between the NCA and CINCS uses low-speed teletype, [75] and is very susceptible to jamming and scintillation. By contrast, MILSTAR will permit officials in EC-135 and E-4 command aircraft to confer directly by voice, [76] on a frequency (EHF) whose only known disadvantage is a susceptibility to interference from heavy rainfall, which normally could be overflown by the aircraft. [77]

Hardening airborne command posts against nuclear effects, particularly EMP, assumed higher priority after DoD's decision in 1982 to deploy only four E-4B command aircraft instead of six, as originally planned. Prior to this decision, a fleet of at least six of these EMP-hardened jumbo jets had been envisaged with full operational capability in July 1987. [78] DoD reported as late as 1982 that no less than six aircraft were needed in order to support the NEACP and SAC "Looking Glass" missions. [79] Acceleration of the delivery schedule, and procurement of a seventh aircraft, were strongly recommended by CINCSAC. [80] (With seven E-4B aircraft, the United States could simultaneously maintain a NEACP E-4B on 24-hour ground alert and a "Looking Glass" E-4B on 24-hour airborne alert. With a fleet of six E-4Bs, SAC would need to retain two EC-135s as back-up aircraft to support its "Looking Glass" mission.) [81]

Although the E-4B was the only EMP-hardened airborne command post in the entire inventory, [82] the decision was made to deploy four instead of six or seven aircraft and thereby continue to rely on unhardened EC-135 aircraft to fly "Looking Glass" missions. (Two E-4B aircraft are now operationally deployed in support of the NEACP mission. The third and fourth NEACP E-4Bs should enter service in 1984 and 1985, respectively.) At the same time, DoD decided to provide EMP hardening to elements of the EC-135 airborne command post fleet. [83] DoD proposed to spend $13.7 million for this program, [84] a figure that closely corresponds with DoD estimates of the cost of EMP hardening all twenty-five EC-135 aircraft in SAC's Post Attack Command Control System (PACCS). [85]

The potential contribution of IONDS, MILSTAR and command aircraft hardening, to airborne SIOP decisionmaking would appear to be considerable. Their contribution of course presupposes the successful launch and continuing survival of key command aircraft, particularly NEACP, that are normally maintained on ground alert. Other caveats are warranted. First, hardening aircraft, particularly older aircraft, against EMP effects is more art than science. There are still major uncertainties surrounding the EMP-resistance of the modern E-4B, which was deliberately shielded against EMP in the design stage. [86] Also, only partial protection of EC-135 aircraft could be provided on a budget of $13.7 million. The Congressional Budget Office has estimated the cost of hardening twenty-seven EC-135s at $65 million. [87] Second, deployment of MILSTAR is a long way off (early 1990s), and the terminal segment for airborne command posts will doubtless lag behind by several years. As MILSTAR is just getting off the drawing board, there remains considerable uncertainty about the final configuration of both the space and terminal segments. And due to past investment of billions of dollars in UHF terminals, the switchover to full EHF operation will take years. During what could be a very lengthy period of transition, a less capable hybrid system, part EHF and part UHF, will be necessarily employed. DoD reports that MILSTAR will incorporate an EHF-UHF interlink to provide continuity of service with AFSATCOM terminals.[88] Reliance on UHF for part of the circuit means that MILSTAR channels will be susceptible to threats such as jamming and scintillation. Third, MILSTAR (as well as IONDS platforms, early warning satellites, and DSCS-III satellites) may have to cope with dramatic improvements in Soviet ASAT capabiiities. In light of intensifying military competition for space dominance, it would not be prudent to assume that a decade from now space will be a sanctuary for the U.S. satellite systems under development.

Initial SIOP EAM Dissemination

Senior defense officials hope that U.S. retaliatory orders can be disseminated to the forces during the short preimpact period when the U.S. command system is still intact and coherent. As CINCSAC put it in 1981:

> The ultimate, of course, is to recognize that we are under attack, to characterize that attack, get a decision from the President, and to disseminate the decision to the forces prior to the first weapon impacting upon the United States.[89]

Effective EAM dissemination during the preimpact period presupposes minimal disruption of the ground command and communications network from jamming and high altitude nuclear explosions. At present, this network — both the fixed command posts and the leased terrestrial communications linking NCA to the CINCS and individual strategic forces — is subject to serious disruption from these effects. Command post hardening will mitigate this vulnerability. GWEN deployment will reduce reliance on EMP-vulnerable leased lines. According to DoD, GWEN will carry the initial SIOP execution message directly to the forces.[90]

Actually, GWEN cannot carry the message directly to the submarine and bomber forces. GWEN is a terrestrial network of LF radios whose signals would travel for short distances along the ground to other GWEN radios and other fixed locations such as Minuteman launch control centers. The Navy's shore-based VLF radio stations and other facilities would still be needed for EAM dissemination to missile submarines. Similarly, various radio systems would be needed to relay messages received via GWEN circuits to the bomber forces, whether those forces were still on the ground or en route to positive control turnaround points.

It is of course a matter of considerable doubt whether an execution message would be ready for dissemination before the ground network began to sustain heavy blast damage from SLBM attacks. To the prudent planner, the <u>key links</u> in the dissemination process (as well as the earlier decisionmaking process) are the various aircraft that constitute the <u>airborne command network</u>.

Several programs are intended to fortify the ability of the airborne command network to communicate within itself and with the bomber, submarine and land missile forces. Before examining these programs, it is useful to review present capabilities to send retaliation orders from command aircraft to various force components.

Bombers: At present, the United States heavily depends upon air-to-air line-of-sight UHF communications to pass war orders to bombers. After being flushed on a positive control launch, outbound bombers could receive their instructions from PACCS aircraft so long as the bomber corridors traverse the PACCS orbits and so long as the PACCS transmissions start before the outbound bombers have flown beyond UHF range (about 400 miles).

If PACCS transmissions are not timely, owing to delays in SIOP decisionmaking or to difficulties in communicating the orders throughout the PACCS network; or if bomber corridors do not happen to traverse PACCS orbits; or if PACCS aircraft on ground alert do not survive SLBM attacks (SAC's "Looking Glass" is the only PACCS aircraft maintained on continuous airborne alert), the EAM dissemination channels would collapse to the emergency rocket communications system (ERCS), the AFSATCOM system, and HF radio. ERCS is increasingly vulnerable, if standard calculations are to be believed, to early destruction because the rockets are housed in Minuteman silos that cannot ride out attacks by modern Soviet ICBM forces. AFSATCOM effectiveness is also questionable because of its high susceptibility to negation by jamming and scintillation. HF radio would be blacked out for hours.

The major initiative designed to fortify the communications link between the airborne command network and the bomber force involves equipping bombers with mini LF/VLF receivers.

Alert Submarines: This component of the force structure presently relies on TACAMO VLF communications relay aircraft for EAM dissemination. Message injection to TACAMO depends on ERCS, AFSATCOM, and LF/VLF transmissions from command aircraft such as SAC's "Looking Glass."

TACAMO deficiencies include vulnerability to EMP; VLF susceptibility to jamming; and uncertain availability due to very limited endurance. Message injection to TACAMO via ERCS and AFSATCOM is precarious for reasons cited earlier. The most survivable source of EAMs is LF/VLF transmissions from SAC's "Looking Glass" airborne command post, which lacks sufficient radio range to reach TACAMO with high confidence in a nuclear and jamming environment.

The major initiative meant to fortify the link between TACAMO and alert submarines is ECX, a replacement aircraft for the current EC-130 TACAMO aircraft. Other significant initiatives include MILSTAR and an extremely low frequency (ELF) radio system being built in Wisconsin and Michigan.

Minuteman Land Missile Force: Airborne launch control center (ALCC) aircraft provide the most survivable source of launch commands to this component of the force structure. Except for SAC's "Looking Glass" aircraft, all ALCC aircraft are normally maintained on ground alert. If ground alert ALCC aircraft along with the rest of the ground alert aircraft in the Post Attack Command Control System (PACCS) network survive SLBM attacks, UHF radio links for transmitting launch commands to missile forces probably would be established. The links are line-of-sight and are not very susceptible to jamming or nuclear effects.

There are no major plans to fortify the links to ALCC aircraft and Minuteman forces.

Communications Initiatives for SIOP EAM Dissemination:

A. DSCS-III and FLTSATCOM Satellites: All C^3 aircraft, most bombers and all ground-based Minuteman launch control centers are equipped with AFSATCOM satellite communications terminals. The space segment of AFSATCOM is currently carried piggyback on host satellites called FLTSATCOM and SDS. Many of these satellites will cease to be functional in the near future. The current FLTSATCOM constellation, for example, consists of four satellites launched between 1978 and 1980, each with an estimated life span of six years.[91] There is therefore a statistical probability of losing a satellite as early as 1984.

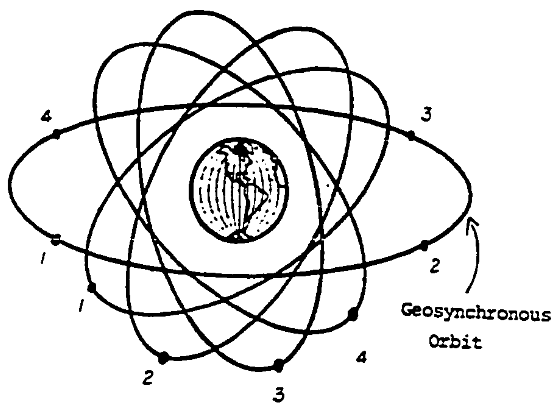
To extend full FLTSATCOM-AFSATCOM service until about 1992, DoD plans to launch three additional FLTSATCOM satellites beginning in 1985.[92] Additional redundancy in the AFSATCOM space segment will be acquired through the deployment of piggyback AFSATCOM transponders on DSCS-III satellites, four of which will be operational by 1986.[93] The so-called single channel transponders will permit only one-way communications to the forces, but will feature better jam resistance than FLTSATCOM-AFSATCOM devices. [94]

Since these programs basically serve to sustain existing communications, they do not offer any substantial improvements in EAM dissemination capabilities.

B. MILSTAR: MILSTAR is described as "the next generation military satellite communications system which will provide a survivable and enduring warfighting communications capability into the next century." [95] It is the centerpiece of the present administration's plans for C^3I modernization. As DoD puts it:

> Our current dependence on vulnerable military and leased commercial communications for SIOP execution, emergency action messages, warning information and other strategic communications is not deemed acceptable, and this MILSTAR will fill a terribly important requirement for survivable and enduring communications. [96]

The MILSTAR constellation will consist of eight satellites, as depicted in Figure 8-7. Three operational satellites and one spare will be placed in geosynchronous orbit; four operational satellites will be placed in polar orbits. [97] Coverage will extend to all areas of the earth except for the south polar region. [98] Laser cross-links will provide for satellite-to-satellite relay, thereby eliminating intermediate (read vulnerable) ground stations. [99] MILSTAR's signal bandwidth, extremely high frequency (EHF), will be highly resistant to nuclear effects and jamming and will permit use of a small (1 1/2 ft.)



MILSTAR CONSTELLATION

Figure 8-7

receive antennas.[100] A variety of mobile users can thus be serviced. Furthermore, EHF will permit transmissions to be focused along a narrow beam, which confers the benefits of low probability of intercept -- a high degree of covertness for mobile users.[101]

The projected date of the first launch of a MILSTAR satellite is reported to be 1987 or 1988.[102] According to official statements, the MILSTAR constellation will replace the AFSATCOM system on host FLTSAT and SDS satellites by the early 1990s.[103]

It is purported that MILSTAR will be immune to jamming and ASAT threats that have been projected through the end of this century.[104] Among the features that the satellite will incorporate to defeat ASAT threats is a maneuvering capability.[105]

But such assurances are surely difficult to offer without some reservations. Space appears to be an arena of intensifying arms competition. There are already semiofficial projections of Soviet development of ASATs designed for attacking satellites in geosynchronous orbit. According to one report, Soviet development of a large booster will threaten such satellites before the end of this decade.[106] In the absence of effective arms control constraints, the Soviets may field direct ascent nuclear missiles, space mines and/or space-based ASAT lasers. A qualitative improvement in Soviet ASAT capability may emerge during the 1990s when the United States becomes heavily dependent on MILSTAR for strategic communications.

C. LF/VLF Mini-Receive Terminals for Bombers: After bombers execute positive control launch on tactical warning and exit the CONUS, line-of-sight UHF communications from PACCS aircraft are no longer possible due to range constraints, while EAM dissemination to the bomber force via other means is unreliable. DoD plans to strengthen communications with distant bombers by equipping them with LF/VLF mini-receive terminals. These terminals will be designed for long distance reception of LF/VLF signals transmitted by EC-135 and E-4 airborne command posts. Effective communications over a range of 2,000-3,000 miles are predicted, a vast improvement over existing capabilities.[107]

Related improvements in LF/VLF airborne systems include a program to extend the reception range of EC-135 and E-4 aircraft by 1,000-2,000 miles.[108] Another program would increase the transmitting power of EC-135 aircraft and thereby extend their transmission range by 1,000 miles.[109]

D. TACAMO ECX: Plans call for the inventory of TACAMO EC-130 aircraft to be expanded to eighteen by FY 1983 and for the Pacific TACAMO fleet to be relocated from Guam to a West Coast base.[110] When eighteen aircraft become available, it should be possible to maintain continuous airborne coverage over both the Atlantic and Pacific submarine fleet operations areas.[111] Relocation of the Pacific TACAMO fleet to California will reduce the distance between TACAMO and higher authority command aircraft, thereby easing the communications problem.

A variety of deficiencies nevertheless plague the current TACAMO fleet. EC-130 aircraft lack adequate protection from EMP. Their communications suites need to be modernized. They are 10,000 lbs. overweight, causing airframe stress and limiting airborne endurance.[112] They cannot be refueled while airborne. Nine aircraft are on the verge of retirement.[113] And an estimated fleet of twenty-nine EC-130 aircraft would be needed to fulfill mission requirements, according to the Navy.[114] (Continuous airborne alert in both ocean areas, a mission that requires eighteen EC-130 aircraft, is evidently only one of many mission requirements.)

The TACAMO ECX program addresses all of these deficiencies except for communications suite modernization. ECX refers to a replacement aircraft, which is a Boeing Co. 707-based airframe like the one used in the E-3A Airborne Warning and Control System (AWACS). DoD will eventually acquire fifteen such aircraft,[115] with the first ECX operational by the time that nine existing EC-130 aircraft must be retired.[116] Initial operational capability is expected to be achieved by 1987.[117] ECX will be EMP-hardened and employ fan-jet engines that provide twice the airspeed of EC-130 aircraft.[118] Aircraft endurance with refueling could be as long as "several days."[119] Maximum endurance without refueling could exceed fourteen hours.[120]

Due to the lead time involved in ECX procurement, and the imminent block obsolescence of existing EC-130 aircraft, the Navy has been forced to place orders for a number of new EC-130 aircraft in order to ensure continuity during the transition to ECX. Nine new EC-130s will be purchased between FY 1982 and FY 1985, at a total cost of $825 million.[121] The Navy plans to EMP-harden the new EC-130s as well as ECX aircraft.[122]

The major outstanding question with respect to future TACAMO performance is whether the communications suites onboard the new EC-130 and ECX aircraft are adequate. Present plans call for transferring communications suites from worn-out EC-130 aircraft to the new EC-130 and ECX aircraft.[123] ECX communications are not slated for replacement or modernization.[124]

E. ELF: The planned ELF communications system is an austere version of the original Seafarer proposal (see Chapter 6). The austere configuration will consist of a two-site system operated synchronously (see Figure 8-8a). The Wisconsin site already exists. Its transmitter and twenty-eight miles of antenna will be upgraded and EMP-hardened.[125] IOC is 1985.[126] Meantime, a transmitter and fifty-six miles of antenna will be installed in Michigan.[127] The two sites will be electronically synchronized as they transmit extremely low frequency signals.[128] Full operational capability is expected to be achieved by 1987.[129]

Some U.S. SSBNs have been routinely patrolling with ELF R&D receivers for several years.[130] Using the Wisconsin facility, the Navy has conducted numerous successful tests of the basic concept.[131] The range of ELF communications from the Wisconsin Test Facility (WTF) is shown in Figure 8-8b, along with the coverage that could be expected for a hypothetical two-site system and for a full Seafarer system.

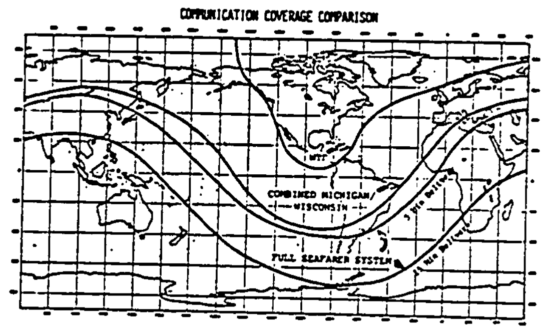


Figure 8-8a

U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 10929, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978) pt. 3, bk 2, p.1323.

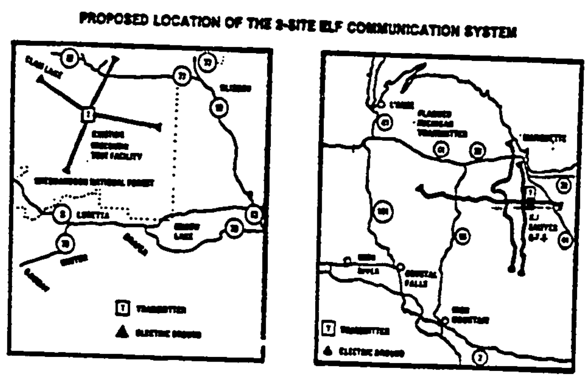


Figure 8-8b

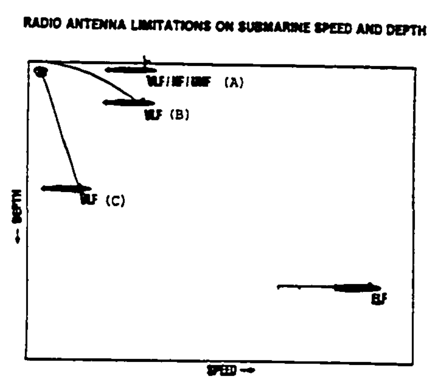


Figure 8-8c

U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, 97th Congress, 1st Session (Washington, D.C.: GPO, 1981) pt. 7, p.4236.

Figure 8-8

(The two-site coverage shown assumed 130 miles of antenna in Michigan and thus somewhat exceeds the coverage of the planned two-site system. The full Seafarer system would have used 2,400 miles of antenna.) [132]

SIOP EAM dissemination is not the primary purpose of the planned ELF system. The main purpose is to eliminate the possibility of intermittent Soviet detection of conventional submarine antennas, detections which could help narrow the location uncertainty of U.S. SSBNs and thereby jeopardize their survival. [133] Conventional antennas are depicted in Figure 8-8c. [134] In disposition A, the submarine is at periscope depth with an exposed antenna sticking above the surface; the antenna is visible and if the submarine operates at any significant speed, it leaves a trail. [135] In disposition B, the submarine trails a wire antenna of great length (about 2,000 feet), 200 feet of which must float on the surface for proper reception. [136] A salty Admiral once testified that "I have looked through my periscope on the USS Will Rogers and have been horrified to find there are birds roosting on the doggoned wire back here...." [137] In disposition C, the submarine uses a buoy that floats to within fifteen to twenty feet of the surface; if the submarine operates at significant speed or changes course the buoy sinks and reception is lost. [138] The towed buoy installed in SSBNs also has low reliability. [139]

With ELF receivers, SSBNs could operate at much deeper depths and at higher speeds while maintaining reception without an umbilical to the ocean surface. [140] ELF will permit submarines to patrol at a depth of 300-400 feet and to travel at speeds up to twenty knots. [141]

The role of ELF in SIOP EAM dissemination is extremely limited for two reasons. First, ELF will be a peacetime "soft" system that will not withstand a major attack.[142] Second, the transmission data rate is very low. While it would be technically possible to transmit retaliatory instructions over ELF, the transmission would take hours and therefore is not practical.[143]

It is envisioned that ELF would send three-letter messages,[144] which could be simple coded references to more elaborate instructions stored in the submarine. For instance, ELF could be used to deliver a short alerting message that directs the submarine to change its communications posture so that it can continuously monitor TACAMO and other SIOP EAM frequencies. Upon receipt of this instruction, the submarine would slow down, reduce its depth and deploy a conventional antenna to receive emergency messages from TACAMO or other sources.

In the case of alert submarines, this capability is not exactly a virtue. Current arrangements, in fact, allow for more timely dissemination. Alert submarines today monitor TACAMO and other SIOP EAM frequencies on a continuous basis. In the case of mod-alert or nonalert submarines, however, the virtue of ELF is clear. ELF could be used to notify those submarines to assume a posture of maximum communications. Today, without ELF, such submarines could not be so notified, at least not immediately. Attack submarines (SSNs) which today monitor communications as infrequently as once every twelve hours could also be notified. Such a capability will be valuable if attack submarines are armed with nuclear-tipped Tomahawk cruise missiles capable of hitting Soviet territory.

If ELF were destroyed before any alerting message could be sent, the loss of the ELF signal (it will be continuously broadcast in peacetime) would implicitly send an alerting message to the entire at-sea missile submarine fleet. This function is described as follows:

> The ELF system transmits at all time.... If, however, ELF were destroyed in a surprise attack, the loss of the ELF signal by the submarine would in effect tell the submarine to come to a shallower depth and copy other broadcasts; for example, the survivable TACAMO.[145]

In the case of alert submarines, this bell-ringer feature of ELF makes a virtue out of a liability, for it is ELF itself that will keep these submarines from monitoring TACAMO and other EAM dissemination channels on a continuous basis. In the case of mod-alert and other submarines that today listen only periodically for message broadcasts, ELF bell-ringing allows for unscheduled communications and thus improves upon existing capabilities.

Protracted War

As discussed earlier, the Reagan administration stresses the need for strategic systems capable of operating for a long time in a nuclear environment. To date, research and development efforts to attain the desired capability have been far less vigorous than the administration's rhetoric, but the effort is intensifying. Major programs being pursued to this end can be grouped into three categories: (1) warning and attack assessment, (2) command and decision, and (3) strategic communications. These programs are discussed next.

Warning and Attack Assessment: All missile warning radar sensors in current operation are fixed and as such are subject to destruction within a few minutes after the initiation of Soviet missile attack. If the Soviets also target the fixed readout stations for early warning satellites, the existing warning network would be rapidly neutralized.

The Mobile Ground Terminal (MGT) readout stations for early warning satellites that are planned for deployment in the next few years probably could survive an initial attack. They might be able to operate for several days or longer, thus providing tactical warning of follow-up Soviet missile attacks against withheld bombers and other strategic reserve assets.

The Advance Missile Warning System, however, appears to be the preferred long-term solution to the problem of enduring warning. "Designed to ensure continued operation throughout a nuclear conflict,"[146] the system would eliminate all intermediate processing/relay nodes by incorporating on-board data processing so that warning messages could be transmitted directly to users.[147] A decision on whether to undertake full-scale development of the system is expected in FY 1987, with initial deployment possible in the 1990s.[148]

IONDS could provide enduring attack assessment. It is being designed to furnish commanders with information on above-ground nuclear detonations as they occur. Detailed knowledge of this sort is considered to be very important for damage and strike assessment and the employment of strategic reserve forces.[149] Knowledge of nuclear detonations in the United States (damage assessment) could aid in determining residual U.S. strategic capabilities and in targeting those forces for maximum retaliatory effect. Such knowledge could also aid commanders in identifying areas that escaped destruction so that they could direct recovery of bombers, tankers, command post aircraft, and so forth, to them.[150] Knowledge of detonations in enemy territory (strike assessment) could aid in assessing enemy residual capabilities following the initial U.S. attack, and in identifying targets to be covered in a second U.S. strike.[151]

Since IONDS sensors will be dispersed aboard eighteen satellites, the whole system is not expected to be subject to negation by Soviet ASAT attack.[152] Some of the sensors would be expected to survive and function over time.[153] Furthermore, the host satellites that will carry the IONDS devices are being designed to function autonomously for weeks so that the constellation could endure despite the loss of ground command-control-telemetry stations.[154] Mobile units may eventually be able to perform certain essential satellite command-control-telemetry functions.[155]

Lastly, plans to reconstitute NORAD have been drawn. NORAD is forming a Rapid Emergency Reconstitution Team (RAPIER).[156]

<u>Command and Decision</u>: Existing strategic command posts lack appreciable endurance. No fixed command center stands much chance of weathering any deliberate attack by ICBMs which could be delivered in a mere thirty minutes. Airborne command posts would be expected to remain in operation for much longer; but their initial airborne

endurance could be as short as several hours, depending upon the availability of tankers for in-flight refueling. Successful recovery and relaunch would then depend on the availability of usable runways, ground fuel stocks and maintenance, crew health, and exposure to follow-up enemy attacks. The utility of aircraft communication while grounded would be limited by the availability of external electrical power; radio range would be shorter and certain radio systems, for example LF/VLF radios with trailing wire antennas, could not be employed. The role of command aircraft in postattack battle management is further limited by their inability to store and process large amounts of data; force reconstitution and other battle management functions are presently performed by ground facilities such as SAC Headquarters and the National Military Command Center.[157]

Two possible solutions to the general problem of command endurance have been given serious consideration. One solution still under study entails development of more versatile aircraft to replace the present fleet of EC-135s and E-4s. The replacement aircraft would be designed to operate from smaller airfields (longer runways required for current operations are far fewer in number and more likely to be targeted).[158] They would burn less fuel and require less maintenance.[159] A complementary system to aid these aircraft (existing aircraft, for that matter) in identifying operating airfields following a nuclear attack has also been proposed. Airfield locators would consist of radio beacon devices at the airfield which command aircraft could interrogate to determine its status.[160] (Absence of beacon signal implies airfield destruction.) This program has not been funded.[161] Neither has the replacement aircraft proposal.

DoD favors an alternative approach that would field a set of austere command centers in ground mobile vans. As described by CBO, some vans would operate on a continuous basis; the rest could be generated in a crisis.[162] Similar to truck-mounted MGTs for early warning satellites, the command vans would be deployed in areas away from major targets.[163] Movement within operational areas would be random, covert and frequent in order to avoid Soviet detection and attack.[164] With prestored caches of fuel, food and critical spare parts hidden in these areas, command vans might be able to operate indefinitely in a nuclear environment.[165]

Mobile Command Center (MCC) is the official designation of this program. According to DoD, MCCs will support the National Command Authority, the Joint Chiefs of Staff and subordinate commands as a fourth element of the National Military Command System.[166] (NMCS presently consists of two fixed facilities — the primary and alternate command centers at the Pentagon and Ft. Richie — and the mobile National Emergency Airborne Command Post.) The few elements are seen as complementary, providing a strategic command system "capable of spanning the full spectrum of modern warfare, from crisis operations through execution of an initial nuclear exchange and conduct of a prolonged nuclear war to conflict termination."[167] Fixed centers would manage peacetime and crisis operations. Command aircraft would manage strategic operations during the initial stages of nuclear conflict. MCCs would assume control over protracted engagements. In the words of D. Latham: "The airborne command posts will endure long enough to ensure continuity of command through the transition from the initial phase to the follow-up phases, and then the covertly deployed MCCs could take over...." [168]

A prototype ground mobile command post (GMCC) has been developed. [169] As presently planned, each GMCC unit will actually consist of two semitrailer vans. A cutaway view of the two vans is presented in Figure 8-9.

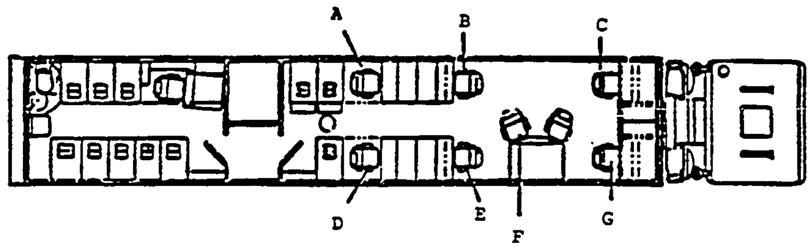
This GMCC prototype may or may not be adopted as an exemplar for the MCC program. Although MCCs will probably be housed in modified trucks, [170] GMCC is but one of many possible truck-mounted options, and other nonvehicular options are being considered. For example, deployment of MCCs on ships has been considered. [171] A modular MCC that could be loaded on transport aircraft, permitting airborne as well as ground operations, has also been proposed. [172]

The timetable of deployment reportedly calls for MCCs to be in full operation by the late 1980s. [173] It is reported that phased elements will come on line in 1985, 1987 and 1989 as part of an "evolutionary development toward modular command center capability." [174]

The potential for MCCs to provide for command endurance in a nuclear environment is very difficult to gauge, given that the physical configuration and concept of operations have not yet been specified. There are more questions than answers at this point. Would a strictly

GROUND MOBILE COMMAND CENTER
2-VAN CONFIGURATION

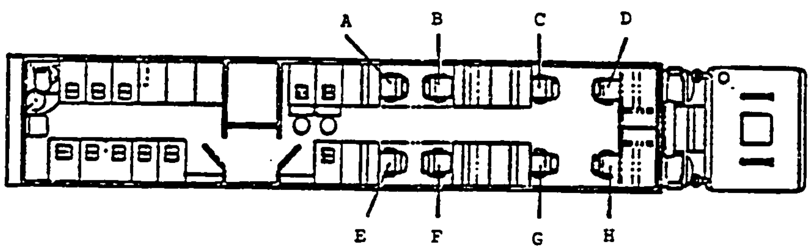
VAN-1



VAN-1 PERSONNEL ASSIGNMENTS:

A - Information
B - Emergency Actions
C - Surveillance
D - Communications
E - Emergency Actions
F - GMCC Team Chief
G - SIOP Plans/Analysis

VAN-2



VAN-2 PERSONNEL ASSIGNMENTS:

A - Administration
B - Reconnaissance/Damage Assessment
C - Intelligence
D - Force Operations Planning
E - Communications
F - Reconnaissance/Damage Assessment
G - SIOP Plans/Analysis
H - Force Operations Planning

Power Supply:
- Commercial Hookup
- Diesel Generators

Figure 8-9

ground mobile version be susceptible to detection and direct attack. Would it be exposed to a lethal level of fallout? Could the Soviets identify which ships carried MCCs and successfully attack them at sea? Could MCC-loaded transport aircraft safely launch and later find a usable runway to unload the MCCs?

Strategic Communications: Using existing systems, strategic communications would be marginal at best after C^3 aircraft were forced to land. Grounded aircraft, surviving ships at sea, and residual space-based assets might be able to support some limited communications once the atmosphere heals itself sufficiently to allow restoration of HF and satellite UHF radio transmissions. High-confidence communications, however, would be nonexistent. Present systems were not designed to endure for weeks or months in a nuclear environment.

DoD predicts that MILSTAR will dramatically improve U.S. capabilities for postattack strategic communications. It is the centerpiece of current aspirations for communications endurance. Apart from features noted earlier, MILSTAR's potential to support the management of strategic forces in a multiple exchange campaign [175] stems importantly from its capacity to function autonomously. DoD asserts that MILSTAR will not need to be constantly linked to major ground tracking stations for command-control-telemetry.[176] It is being designed to operate for weeks without ground involvement and to accept command-control-telemetry data from small, proliferated terminals.[177] Small, portable terminals may be able to provide the essential telemetry, tracking and mission data needed to keep MILSTAR in operation over time.[178] DSCS-III was also designed to function for long periods without ground assistance for on-board systems maintenance.[179]

The role of MILSTAR in a protracted strategic campaign is further enhanced by its ability to transmit EHF signals with low probability of intercept (LPI). This translates to covertness, hence greater survivability for mobile users.[180] LPI would be essential to mobile command center (MCC) communications, for example. LPI would also help prevent the Soviets from locating bombers and submarines that break communications silence. One of the touted advantages of MILSTAR is that strategic missile submarines will be able to use MILSTAR communications for "report back."[181] Covert, two-way communications are considered to be essential for battle management, force retargeting, and related postattack operations.

To avoid complete dependence on MILSTAR for enduring communications, DoD is exploring possibilities for postattack reconstitution of communications. The idea is to reconstitute communications as needed in the event that MILSTAR, which would be operational at the start of hostilities, failed to survive and endure throughout a protracted conflict.

Investment in reserve communications is almost negligible. The FY 1980 budget requested a total of $21 million for reconstitution initiatives not only in the area of communications, but also in the areas of surveillance/warning and command-control.[182] This request covered, for example, the cost of testing the GMCC prototype discussed earlier under the MCC program.[183] As of 1980, many ideas had been proposed but not seriously acted upon. In 1980, DoD conceded that "today there is insufficient technical data available to assess performance or cost risk of these potential alternatives."[184] $21 million was then requested to permit DoD "to pursue an aggressive advanced research and development program to obtain viable programmatic options in time to allow early 1990s deployment."[185]

In 1982, reconstructible communications concepts were still "under study."[186] FY 1983 funding requests for concept development totaled $2.4 million.[187] Options considered in recent years include the following:

- Postattack Launch of Communications Satellite.[188] Launch of satellites following a Soviet missile attack would require survivable launch facilities. Submarines are among the candidate launch systems under consideration.[189]

- Land Transportable ELF. A mobile van transportable ELF grid has been proposed as a reconstructible means of submarine communications.[190]

- Land Mobile VLF.[191] Land mobile vans could be equipped to transmit VLF radio signals using a tethered balloon and/or an erectable tower as antennas.

• Free-floating VLF Relay Balloons.[192] High altitude balloons with trailing wire antennas could be dispensed from aircraft, surface ships, submarines (via torpedo tubes), or land mobile units. Launch of these relay balloons could be rocket-assisted. Once deployed, utility and endurance would be determined by wind drift and on-board battery power (approximately 2-7 days).

• Other Technologies. A congressional committee recently expressed support for reconstructible communications based on adaptive HF and meteor burst technologies.[193] Communications systems based on these technologies could be versatile enough to support transattack as well as postattack operations. They would lend themselves to a variety of purposes besides reconstitution.

Adaptive HF refers to long-range HF radio communication using one of two general techniques to avoid signal blackout caused by a nuclear-disturbed ionosphere. One technique "tests" different HF frequencies to identify the most promising link. The system selects the best frequency from those sampled, and adjusts transmitter power to attain proper signal-to-noise ratio. The alternative technique simply repeats messages across the time and frequency domain. Rapid repetition in different frequencies would eventually allow receivers to piece together the message.

Meteor burst refers to long-range (600-1,200 miles) VHF radio communications using the microscopic ionized trails of meteoroids in the upper atmosphere to reflect signals between users. Such trails occur at altitudes of roughly sixty miles. They last only a fraction of a second but appear very frequently (approximately every second). During their brief appearance, useful burst transmissions could be sent between small, proliferated units such as mobile command centers and surfaced submarines. The data rate would be low and the message probably would have to be repeated several times (the rapid degeneration of trails could prevent a given message from getting through). Meteor burst communications have been proven. In fact, several systems are in operation today. The Department of Agriculture routinely uses meteor burst communications to collect data from 500 remote stations located in eleven western states.

Among these concepts, three are the most developed and the strongest candidates for actual deployment. They are, in order of deployment status: (1) free-floating VLF balloons, (2) adaptive HF radio, and (3) meteor burst communications.

SUMMARY

The current plan for modernizing C^3I is ambitiously wide-ranging. Numerous problem areas compete for attention and resources. One of these areas concerns the initial few minutes of enemy attack. Improvements to fixed command centers and terrestrial communications are being made so that emergency messages could be effectively disseminated prior to the first impact of an enemy nuclear weapon. The improvement plan is funded and technically defined but slides past the issue of whether a responsible, considered emergency decision is humanly and organizationally possible when there are only a few minutes to decide.

Another problem area receiving attention concerns command performance during the first several hours of enemy attack. Improvements are being made to the back-up airborne network which might be called upon to assume responsibility for initial SIOP decisionmaking and dissemination. These improvements are only partially funded, as many extend well into out years. Most are likely to be financially authorized, however, owing to the strongly held belief that a viable airborne system capable of performing SIOP execution functions is an essential hedge against a decapitating attack on the ground network. The improvements are fairly well-defined in technical terms, but they are neither comprehensive nor uniformly promising. Modernization of the TACAMO communications suite, for example, is not planned at all.

Another problem area concerns the postattack period of weeks and months following the initial strategic exchange. Planners have been instructed to develop an enduring command system for managing a multiple exchange campaign, strategic reserve forces, and other protracted operations. With some notable exceptions, for example IONDS, this pursuit is neither technically defined nor financially authorized. Cases in point are Mobile Command Centers (MCCs) and MILSTAR, the core elements of the envisaged system. The MCC program is undefined in technical and operational respects, while the more developed MILSTAR system will operate in a threat environment that cannot be projected confidently. Both costly programs are being promoted for their potential contribution to the management of a protracted nuclear campaign, a justification of dubious merit to many observers who wield authority over the defense budget.

FOOTNOTES

1. Report of the President's Commission on Strategic Forces (April 6, 1983), p. 10.

2. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), part 7, p. 494.

3. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 5968, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), part 2, p. 247 (emphasis added).

4. Department of Defense Annual Report For Fiscal Year 1984 (Department of Defense, 1983), p. 229.

5. Ibid., p. 54.

6. Desmond Ball, "Can Nuclear War Be Controlled?" Adelphi Papers, no. 169 (London: International Institute For Strategic Studies, 1981), p. 37.

7. John D. Steinbruner, "Nuclear Decapitation," Foreign Policy, vol. 45 (Winter 1981-82), p. 26.

8. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 5, pp. 4, 24.

9. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, 97th Congress, 2nd Session (Washington, D.C.: GPO, 1982), Part 7, pp. 4644-46.

10. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 47.

11. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4686.

12. "Improved U.S. Warning Net Spurred," Aviation Week and Space Technology vol. 112, no. 25 (June 23, 1980), p. 40. AWST reports that DSP will normally see the lift-off of a missile within about sixty seconds of ignition (p. 41). Elsewhere it is revealed that DSP ground readout stations transmit warning messages to national authorities, NORAD, and SAC in near real time. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4701.

13. U.S. Congress, Senate, Committee on Appropriations, Department of Defense Appropriations for Fiscal Year 1975, 93rd Congress, 2nd Session (Washington, D.C.: GPO, 1974), Part 1, p. 116.

14. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., p. 4234.

15. "Improved U.S. Warning Net Spurred," op. cit., p. 40.

16. "Spacecraft Survivability Boost Sought," Aviation Week and Space Technology, vol. 112, no. 24 (June 16, 1980), p. 260.

17. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, 97th Congress, 1st Session (Washington, D.C.: GPO, 1981), Part 7, p. 4234.

18. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), Part 6, p. 3409.

19. Ibid., p. 3416.

20. "Improved U.S. Warning Net Spurred," op. cit., p. 40.

21. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1974, 93rd Congress, 1st Session (Washington, D.C.: GPO, 1973), Part 6, p. 1691.

22. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, pp. 4620, 4645.

23. Ibid., pp. 4645, 4701.

24. Ibid., p. 4692.

25. Ibid., p. 4655; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4234.

26. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4699.

27. Ibid., p. 4701.

28. Ibid., p. 4618.

29. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 59.

30. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, op. cit., Part 6, p. 3449; "Spacecraft Survivability Boost Sought," p. 261.

31. "Spacecraft Survivability Boost Sought," p. 261.

32. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 155.

33. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4683.

34. Ibid., pp. 4646, 4683.

35. Ibid.

36. Ibid., pp. 4700, 4701, 4710.

37. Ibid., pp. 4683, 4700.

38. Ibid., pp. 4700, 4705.

39. Ibid., p. 4681.

40. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, pp. 4216, 4218.

41. U.S. Congress, Senate, Committee on Armed Services, Recent False Alerts from the Nation's Missile Attack Warning System, 96th Congress, 2nd Session (Washington, D.C.: GPO, 1980), Report October 9, 1980, p. 5. This was a false alarm.

42. Ibid.

43. Ibid.

44. Ibid.

45. Ibid., p. 6.

46. Ibid., p. 5.

47. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4683.

48. Ibid., p. 4717.

49. Ibid.

50. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, pp. 4212-13, 4218.

51. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4683.

52. Ibid.

53. Ibid., p. 4700.

54. Ibid., p. 4699.

55. "U.S. Upgrading Ground-Based Sensors," Aviation Week and Space Technology, vol. 112, no. 24 (June 16, 1980), p. 241.

56. Ibid., pp. 241-42.

57. U.S. Congress, Senate, Committee on Armed Services, Fiscal Year 1978 Supplemental Military Authorization, 95th Congress, 1st Session (Washington, D.C.: GPO, 1977), p. 81.

58. Ibid.

59. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, op. cit., Part 6, p. 3400.

60. Ibid.

61. "Improved U.S. Warning Net Spurred," op. cit., p. 40.

62. Ibid., p. 41.

63. Ibid.

64. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1981, op. cit., Part 7, p. 438.

65. Ibid.; U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, pp. 64-68.

66. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4619.

67. Ibid., p. 4712; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, op. cit., Part 6, p. 3432.

68. Washington Post, September 27, 1983, p. 8.

69. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Fiscal Year 1983, op. cit., Part 7, p. 4680.

70. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 16.

71. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4206.

72. Ibid.

73. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4625.

74. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4206.

75. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, op. cit., Part 6, p. 3437.

76. Ibid., p. 3432; U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1981, op. cit., Part 6, p. 438.

77. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1981, op. cit., Part 6, p. 438.

78. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4205.

79. Ibid.; U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1981, op. cit., Part 6, p. 417.

80. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4233.

81. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, op. cit., Part 6, pp. 3401, 3447.

82. Ibid., p. 3457.

83. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 151.

84. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4690.

85. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4234.

86. In particular, the crucial VLF trailing wire antenna on which the E-4B greatly depends for communications in a nuclear environment has not been EMP-tested. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 162.

87. Congressional Budget Office, Strategic Command, Control, and Communications: Alternative Approaches for Modernization (October 1981), p. 35.

88. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4618.

89. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4213.

90. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4683.

91. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 71.

92. Ibid., p. 11; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, pp. 4618, 4684.

93. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, pp. 59, 154.

94. Ibid; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4618.

95. U.S. Congress, Senate, Committee on Armed Services, _Department of Defense Authorization for Appropriations for Fiscal Year 1983_, op. cit., Part 7, p. 4618.

96. Ibid., p. 4712.

97. Ibid., p. 4618.

98. Ibid.

99. Ibid., p. 4712.

100. U.S. Congress, House, Committee on Appropriations, _Department of Defense Appropriations for 1983_, op. cit., Part 5, p. 64.

101. Ibid., pp. 68-69.

102. Deborah G. Meyer, "Strategic Satellites: Our Eyes in the Sky," _Armed Forces Journal International_ (February 1983), p. 38.

103. U.S. Congress, House, Committee on Appropriations, _Department of Defense Appropriations for 1983_, op. cit., Part 5, p. 70.

104. U.S. Congress, Senate, Committee on Armed Services, _Department of Defense Authorization for Appropriations for Fiscal Year 1983_, op. cit., Part 7, p. 4619.

105. Ibid., p. 4712.

106. "Soviet Threat in Space Said to Be on Rise," _Aviation Week and Space Technology_ (May 16, 1983), p. 47.

107. U.S. Congress, House, Committee on Appropriations, _Department of Defense Appropriations for 1980_, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 2, p. 554; U.S. Congress, Senate, Committee on Armed Services, _Department of Defense Authorization for Appropriations for Fiscal Year 1982_, op. cit., Part 7, p. 4230.

108. U.S. Congress, House, Committee on Appropriations, _Department of Defense Appropriations for 1980_, op. cit., Part 2, p. 554.

109. Ibid.

110. U.S. Congress, Senate, Committee on Armed Services, _Department of Defense Authorization for Appropriations for Fiscal Year 1982_, op. cit., Part 7, p. 4049; U.S. Congress, House, Committee on Appropriations, _Department of Defense Appropriations for 1981_, op. cit., Part 7, p. 403.

111. U.S. Congress, Senate, Committee on Armed Services, _Department of Defense Authorization for Appropriations for Fiscal Year 1981_, op. cit., Part 6, p. 3458.

112. U.S. Congress, Senate, Committee on Armed Services, _Department of Defense Authorization for Appropriations for Fiscal Year 1982_, op. cit., Part 7, p. 4048.

113. U.S. Congress, Senate, Committee on Armed Services, _Department of Defense Authorization for Appropriations for Fiscal Year 1983_, op. cit., Part 7, p. 4707.

114. Ibid., pp. 4697, 4706.

115. Ibid.

116. Ibid., p. 4722.

117. Clarence A. Robinson, Jr., "Technology Key to Strategic Advances," _Aviation Week and Space Technology_, vol. 118, no. 11 (March 14, 1983).

118. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, pp. 4049-50.

119. Ibid., p. 4049.

120. Aerospace Daily, June 9, 1982, p. 210.

121. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4207.

122. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, pp. 4718-19.

123. Ibid., pp. 4694-95; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4207.

124. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 6; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4695.

125. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 14.

126. Robinson, "Technology Key to Strategic Advances."

127. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, p. 14.

128. Ibid.

129. Robinson, "Technology Key to Strategic Advances."

130. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4724.

131. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 10929, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 3, Book 2, p. 1314.

132. Ibid., p. 1323.

133. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, pp. 4095-96.

134. Ibid., p. 4236.

135. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1980, 96th Congress, 1st Session (Washington, D.C.: GPO, 1979), Part 6, p. 137.

136. Ibid.

137. Ibid.

138. Ibid.

139. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4107.

140. Ibid., p. 4096.

141. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 10929, op. cit., Part 3, Book 2, p. 1860.

142. Ibid.

143. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization For Appropriations For Fiscal Year 1979, 95th Congress, 2nd Session (Washington, D.C.: GPO, 1978), Part 9, p. 6794.

144. U.S. Congress, House, Committee on Armed Services, Military Posture and H.R. 10929, op. cit., Part 3, Book 2, p. 1323.

145. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, pp. 4054-55.

146. Department of Defense Annual Report for Fiscal Year 1984, (Department of Defense, 1983), p. 230.

147. Ibid.

148. Ibid.

149. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4645.

150. Congressional Budget Office, Strategic Command, Control, and Communications, p. 24.

151. Ibid.

152. Ibid.

153. Ibid.

154. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4693.

155. Ibid.

156. Ibid., p. 4700.

157. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations For 1980, 96th Congress, 1st Session (Washington, D.C.: 1979), Part 6, p. 192.

158. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4683; U.S. Congress, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4013.

159. Ibid.

160. U.S. Congress, Senate, Committee on Armed Service, Department of Defense Authorization for Appropriations for Fiscal Year 1982, 97th Congress, 1st Session (Washington, D.C.: GPO, 1981), Report No. 97-58, p. 108.

161. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, pp. 4689-90.

162. Congressional Budget Office, Strategic Command, Control, and Communications, p. 34.

163. Ibid.

164. Ibid.

165. Ibid.

166. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, pp. 4645, 4715.

167. Ibid., p. 4715.

168. Ibid., p. 4680.

169. Congressional Budget Office, Strategic Command, Control, and Communications, p. 34.

170. Philip Taubman, "U.S. Command Will Be Mobile to Elude Attack," New York Times (February 25, 1983).

171. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, pp. 46-47.

172. Congressional Budget Office, Strategic Command, Control, and Communications, p. 34.

173. Taubman, "U.S. Command Will Be Mobile to Elude Attack."

174. Robinson, "Technology Key to Strategic Advances."

175. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4680.

176. Ibid., p. 4692.

177. Ibid.

178. "Spacecraft Survivability Boost Sought," p. 261.

179. Robinson, "Technology Key to Strategic Advances."

180. U.S. Congress, House, Committee on Appropriations, Department of Defense Appropriations for 1983, op. cit., Part 5, pp. 68-69.

181. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4095.

182. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, op. cit., Part 6, p. 3422.

183. Ibid., p. 3406.

184. Ibid.

185. Ibid.

186. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4646.

187. Ibid., p. 4690.

188. Ibid., p. 4646.

189. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1981, op. cit., Part 6, p. 3422.

190. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Part 7, p. 4098; U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4729.

191. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1983, op. cit., Part 7, p. 4729.

192. Ibid.

193. U.S. Congress, Senate, Committee on Armed Services, Department of Defense Authorization for Appropriations for Fiscal Year 1982, op. cit., Report No. 97-58, p. 108.

CHAPTER NINE

SUMMARY AND RECOMMENDATIONS

Strategic analysis has long suffered from a methodological affliction known as the "law of the instrument," which states that problems must be tailored to the tools at one's disposal. Since available tools are generally honed for problems that can be readily quantified, rigorous assessment has steadily advanced in but narrowly circumscribed areas of interest: size, technical composition and economics of nuclear weapons. Although quantitative measures of strategic capability based on weapon characteristics have contributed to an understanding of certain aspects of the strategic problem, progress toward assessment of the central question -- command system performance -- has not been commensurate. Standard calculations, in fact, have obscured the problem of force management, a subject that generally defies meaningful quantification.

Nor does rational decision theory throw adequate light on the subject. The management and behavior of strategic organizations are not patterned after the highly abstract models of rational decision that are commonly used to explain and prescribe nuclear operations. The models are defective because strategic organizations operate according to a fundamentally different control principle, which involves built-in decision rules that link information to preprogrammed responses. These diffuse rules serve two basic purposes: negative and positive control. Negative control is the prevention of accidental or unauthorized use of nuclear weapons. Much of the information technology and established routine of strategic organizations is designed to accomplish this aim. Positive control is the direction and coordination of preparations for engagement with opposing forces, as well as direction and coordination of actual attacks. Much of the information technology and established routine is designed to accomplish that aim.

Effective positive and negative control requires appropriate rules and adequate information, but neither requirement is easily met. The appropriateness of rules is uncertain because they have not been tested under realistic conditions. This uncertainty would manifest itself in unintended consequences if modern strategic organizations attempt to institute crisis alert or wartime procedures. In the absence of experience and learning, rules governing emergency operations are bound to be unstable.

The adequacy of information is uncertain because it flows through channels that are subject to direct or collateral damage from attack. Given the inherent destructiveness of nuclear weapons, total protection of information channels is not yet feasible. Presently, the protection afforded these channels is marginal at best.

The vulnerability of information channels creates a particularly knotty problem inasmuch as it brings positive and negative control into conflict. Negative control cannot be tightened to a point where all activities of strategic units require the direct personal approval of the president. Not only would that degree of centralization be immobilizing (no individual or committee could manage all the activities involved in operating strategic forces), but it would also increase exposure to command decapitation. Control cannot be so centralized that a carefully planned attack against the national command authority would neutralize the entire U.S. arsenal. Yet decentralized arrangements instituted to reduce the risk of command decapitation and oil the elaborate machinery of positive control also heighten the risk of accidental or unauthorized use of nuclear weapons. Decentralization inevitably enlarges the scope for discontinuity between formulated national intentions and force operations.

This practical trade-off, or tension, between the two control priorities has created a situation in which they are neither equal nor static. In peacetime, negative control is predominant. In wartime, positive control takes precedence. Somewhere in between these circumstances -- peace and war -- a transition occurs. The transition may or may not be centrally directed, orderly or complete.

This simple construction offers a basis for historical perspective on three important questions with major C^3I dimensions. The following discussion summarizes historical trends in: (1) the strategic balance, (2) crisis stability, and (3) negative control.

STRATEGIC SITUATION: MID 1960s-PRESENT

Strategic Balance

Since the mid 1960s, the Soviet Union has possessed the military strength needed to disrupt the process by which the United States would organize strategic forces for coordinated attack. Before a smooth transition culminating in coordinated retaliation could be accomplished, the vehicle of this transition — the C^3I network — could be severely degraded by a relatively small attack. Preemptive Soviet attack designed for this purpose could massively disrupt the transition process by isolating very large numbers of U.S. forces and reducing coordination among the remaining forces.

Transition to effective positive control has been especially vulnerable to surprise attack. The predominance of negative control in peacetime means that C^3I readiness is relatively low and thus exposed to sudden attack. Peacetime readiness is such that the C^3I network could not simply ride out such an attack.

To mitigate this high static vulnerability, strategic organizations are primed to shift rapidly to a state of high positive control once an attack is detected. But accomplishing this aim before the attacker's threat can be applied is extremely difficult when negative control is predominant at the start of the attack. Initial organizational reactions, though largely decentralized and highly automated, are unlikely to be as rapid and coherent as the situation demands. In all likelihood, the attacker's threat would be substantially applied before C^3I protection measures (for instance, launch of command aircraft) could be implemented and before authorization to retaliate could be passed to the executing forces.

Consequently, surprise attack has posed a severe threat to U.S. capabilities for retaliation. Since the mid 1960s, the United States has faced a risk that sudden attack would produce such a severe concussion to the command system that U.S. retaliation would be blocked.

This risk would not be as great under crisis conditions because the transition to positive control could begin much earlier. A high state of C^3I readiness could be reached before the opponent attacked. Nevertheless, even the theoretical optimum of past and present C^3I networks has not been sufficient to ensure coordinated retaliation. Communication deficiencies that have plagued the airborne MEECN network have by themselves greatly diminished confidence in second-strike capabilities. Preemptive Soviet attack on a "generated" U.S. command system could isolate many forces and disrupt coordination among connected forces.

Soviet planners probably credit the U.S. command system with greater resilience than this report does. They could hardly fail, however, to appreciate that their <u>only</u> chance of <u>blocking</u> retaliation is to induce paralysis of U.S. C^3I. Failing success at that, such an attack against C^3I systems could still serve to <u>blunt</u> retaliation. Compared to an attack strategy designed to inflict maximum damage to individual U.S. forces, command attack better serves to limit damage that U.S. forces could inflict in retaliation. This has been the situation throughout the missile age.

Soviet planners must be wary of the standard calculations that weigh the strategic balance by pitting Soviet weapons against U.S. weapons in formal statistical combat. Such calculations are simplistic and misleading. They not only mask the operational difficulties and risks involved in force structure attack, but also overstate the potential for limited counterforce attack to produce exploitable bargaining dominance. Today, as in the past, a limited Soviet counterforce attack would produce heavy collateral damage to the U.S. command system, enough to pressure U.S. authorities to choose immediately an option that provides for everything they expect to accomplish in retaliation to attack. Instead of producing bargaining leverage that would coerce residual U.S. forces into nonuse, limited counterforce attack would create almost irresistible pressure on U.S. authorities to massively commit their forces before greater C^3I disruption takes place. At the same time, Soviet planners, anticipating a massive U.S. response to a limited counterforce attack, could hardly fail to realize that it would be advantageous to fracture the U.S. command system at the outset.

The general historical implication is that the overall strategic balance has been relatively unaffected by changes in the size and technical composition of the U.S. and Soviet nuclear arsenals. The state of C^3I has been the primary determinant of overall strategic capabilities. And along this dimension, the United States (and doubtless the Soviet Union) has lived with enormous vulnerability for a long time. Exposure to potentially incapacitating command attack has been the salient feature, and central problem, of the strategic situation for nearly two decades. Major developments in the areas of perceived importance -- size and technical composition of strategic force deployments -- have not had nearly as much impact on the strategic balance as many have believed or alleged.

Crisis Stability

Two decades of development in force deployment have also had only marginal effect on crisis stability. Both standard indicators and command structure analysis agree that the parameters of stability have been relatively constant. They disagree, however, on the amount of stability that has existed.

According to standard indicators, strategic modernization has created some second-order problems of deterrence -- notably, a counterforce asymmetry stemming from ICBM vulnerability -- but has not created any strong incentives to strike first in a crisis. The number and characteristics of survivable weapons in the respective inventories since the mid 1960s have firmly established that nuclear attack risks massive retaliation. Crisis stability has been high because neither side could confidently remove the threat of massive retaliation by means of preemptive attack on the opponent's forces.

According to command analysis, strategic modernization has not created any new incentives to strike first, but strong incentives have existed all along. The Soviet Union has long possessed the capability to effectively destroy the U.S. command system. Soviet command vulnerability probably has been comparable. Inherent in such mutual vulnerability is an appreciable degree of latent instability. Command deficiencies weaken crisis stability because of the heavy penalty incurred by the side struck first, and the tremendous advantage gained by the side that initiates attack. Fortunately, an occasion for this instability to surface has not risen, but the fact remains that it has existed as a potential combustible in a crisis.

Pressures for formal adoption of a strategy of launch-under-attack are symptomatic of this instability. Mutual command vulnerability creates strong incentive to order retaliatory strikes before the opponent's threat to C^3I could be fully applied. This strategy is nonetheless very difficult to implement in the face of countermeasures designed to prevent it. For this reason, both sides would come under increasing pressure to initiate nuclear attack in a crisis of increasing gravity.

This instability is again not new. The U.S. strategic posture, at least, has long been geared to first-use and launch-on-warning tactics. They were rooted in U.S. strategic employment policy long before the problem of Minuteman vulnerability drew attention to them. Command vulnerability has virtually dictated a philosophy of early use.

Policy advisors aware of this state of affairs would hesitate to recommend raising the alert level of strategic forces for diplomatic purposes. To flex military muscle as part of crisis diplomacy is to magnify a critical strategic vulnerability that has the potential to leave both superpowers unnerved. The chinks in their respective armors are worrisome enough to alarm decisionmakers subjected to threatening gestures from their opposites.

Sensitivity to the great potential for mobilized, agitated strategic organizations to cause unintended consequences is also desirable in time of crisis. All too frequently, policy officials evidence an exaggerated sense of control over organizations that are inherently decentralized. To flex military muscle as part of crisis diplomacy is to trigger diffuse organizational responses that national policy officials cannot fully grasp or manage.

Negative Control

Despite the chronic weaknesses that have plagued the U.S. system of positive control, negative control was gradually tightened over the past twenty years. The physical capacity to fire nuclear weapons was further centralized, and signs point to a further centralization of nuclear release authority. Additional safeguards designed to reduce the risk of accidental war, at the expense of positive control, have also been introduced.

Although firm conclusions are not warranted, given the paucity of public information, the high priority assigned to negative control in peacetime would seem to warrant high confidence in peacetime safeguards against accidental or unauthorized use of nuclear weapons. In abnormal circumstances -- crisis or war -- negative control would be harder to maintain as strategic organizations become more active and decentralized. A relevant theme that lightly runs through the open literature is that release authority could be exercised by military commanders under some circumstances, especially verified nuclear attacks on U.S. territory coupled with a loss of communications with national authorities. Unambiguous guidance on the delegation of nuclear authority seems unlikely, however. This raises additional questions about the integrity of safeguards since the physical capacity to undertake strategic attacks resides below the national command level.

One of the most severe tests of negative control would be a situation in which enemy attacks isolated subordinate strategic units from the president or his successors and communications could not be expeditiously restored. But in a real sense the command system is primed to avoid this test. The weaknesses in positive control that risk such isolation create strong pressures and urgency to issue authoritative instructions while the command system is still intact. A potentially severe strain on negative control is thus ameliorated, by virtue of a bias to transmit nuclear release orders at the earliest possible moment. In other words, command deficiencies work to force an early positive control decision that makes unauthorized retaliation a somewhat moot question.

A command system primed for early release of nuclear weapons, however, increases the scope for miscalculation and accidental war. This risk, though negligible in peacetime, increases considerably during a crisis. During an intense crisis or conventional war, the priority of positive control would grow to a point where faulty intelligence, for example false alarms, might trigger the final stages of the nuclear release process. The danger of stumbling into nuclear war grows exponentially when crises flare up and superpower tensions rise.

LOOKING AHEAD

The present administration is planning a modern command system that can support protracted counterforce operations. The context of this plan is an image of strategic conflict that begins with a large-scale Soviet counterforce attack and an immediate U.S. counterattack against "time-urgent" military targets. Unless and until a bargain to end the war is struck, the campaign is prolonged with follow-up exchanges and escalation to countervalue attacks among the envisaged possibilities.

In this context, an effective program for strategic modernization would introduce both new weapons capable of prompt hard target attack and new command networks capable of supporting a variety of aims -- ranging from launch-on-warning to management of strategic reserve forces. It would also have to address a sharpened conflict between negative and positive control that results from the requirement to maintain strict negative control over forces that are withheld during the exchange(s).

Several pertinent points may help put the current program in proper perspective. First, existing command structure cannot begin to support a doctrine of flexible response extended in time. Second, standard calculations of Soviet advantage in protracted counterforce exchanges bear no relation to actual circumstances because they presuppose a command structure that does not exist. Third, the technological and procedural foundations of such a structure have not yet been fully defined, much less fully developed. (An especially formidable challenge is to ensure that negative control over withheld forces can be preserved during and after the execution of authorized SIOP strikes.) Fourth, deployment of such a structure has not been funded, is bound to be costly, and would compete with force modernization programs for scarce resources. Fifth, preparing forces and command networks for protracted nuclear war is not palatable to significant segments of the defense community, a fact that dims the outlook for financial authorization. Sixth, even if the large outlays required for extensive command modernization are ultimately approved, the investment almost certainly would stimulate aggressive Soviet development of countermeasures.

A final point, and one of key significance, is that pressures for preemptive attack or immediate retaliation to attack would remain strong even if substantial improvement in the versatility, survivability and endurance of the command structure were realized. Although such improvement would allay fear of a sudden collapse of command-control and relieve that impulse for early release of weapons if war appears imminent, decisionmakers would still come under other pressures to unleash the forces without delay. One such pressure is counterforce doctrine itself. Since a strategy based on effective counterforce attack depends for its success on the rapid delivery of weapons against "time-urgent" military targets, incentives to initiate offensive operations at the earliest possible moment would be powerful.

Before passing final judgment on any proposal for strategic modernization, planners and policymakers should consider whether sufficient time and information would be available to make a responsible decision on the employment of nuclear weapons. This entails difficult judgments. In the first place, defining "sufficient" and "responsible" is highly subjective. But common sense can at least tell us when time and information seem plainly insufficient to produce a responsible decision.

Consider present circumstances. In the event of a Soviet nuclear attack, national officials have at most several hours in which to weigh their options and reach a decision. Strategic organizations actually expect to receive retaliatory authorization within minutes after initial detection of Soviet missile launches. That expectation is so deeply ingrained that the nuclear decision process has been reduced to a drill of sorts — a brief, emergency telecommunications "conference" whose purpose is to "get a decision" from the national command authority.

Can a responsible decision be reasonably expected within a time frame as short as several minutes or even several hours? A moment's reflection would suggest that much more time is needed. It would further suggest that retaliation should not be authorized before national policy officials have assessed actual damage; evaluated Soviet political and military objectives; defined U.S. national security interests; and determined the role of nuclear weapons in promoting those interests. This is obviously not a brief drill, but rather a careful, deliberate exercise of national leadership that may take days or longer.

Today, the vulnerable state of the U.S. command system precludes leadership of this sort and modernization plans scarcely envision it. Planned investment in weapons for prompt counterforce attack together with increased inclination to rely on launch-on-warning for ICBM protection will reinforce already strongly institutionalized predispositions to respond quickly and massively to enemy nuclear provocation. Provisions for command endurance and strategic reserve force operations will not relax the onerous time and information constraints that operate during an initial counterforce engagement.

If these constraints on nuclear employment decisionmaking are so oppressive as to be intolerable, as common sense would suggest, then there is need for some radical adjustments to U.S. strategic doctrine. A policy of "no immediate second use" would be called for. Its primary aim would be to extend strict negative control over all forces well into the period after the brunt of the enemy's attack had been absorbed, and then provide for an orderly transition to effective positive control if and when national officials authorize retaliation. This doctrine may seem absurd to some. It is certainly ambitious -- technically, politically, and psychologically. Nevertheless, as argued below, it is both sensible and feasible. With earnest effort, the United States could enforce strict negative control during and after the transattack period; provide for positive control in the postattack period; and, in the process, create conditions that are conducive to crisis stability.

The basic adjustments necessitated by the proposed doctrine, and the general implications of these changes, are discussed next.

Operations and Deployments

Organizational response to impending or actual Soviet nuclear attack would initially be geared to force and command structure survival. Under current arrangements, protective dispersal and other survival actions — for instance, positive control launch of bombers — are folded into organizational preparation for an immediate offensive campaign. Under a doctrine of "no immediate second use," survival actions would take strong precedence over counterattack coordination during and after the transattack. National officials would not authorize offensive operations during this period, and subordinate military units would be programmed to operate accordingly.

Since SIOP retaliation would be eliminated as an organizational priority during the transattack period, the main purpose of early warning systems would be to alert units to impending attack and trigger preprogrammed responses that minimize exposure to that attack. Early warning systems would not be required to support early SIOP decisionmaking and force execution. Having dropped immediate SIOP response from the organizational repertory, the United States would design its early warning system to meet the narrower requirements of organizational survival. Planned upgrades to early warning components -- sensors, computers, communications, and so forth -- would be judged solely on the basis of their potential contribution to this objective. Their contribution to other missions would not be grounds for approval.

To reinforce defensive reaction and suppress the offensive impulses of strategic organizations, negative control would be tightened. Conditional authority to release nuclear weapons would not be predelegated to military commands. If arrangements of this kind presently exist, they would be revoked. Physical, mechanical, and procedural restraints on nuclear weapons would also be strengthened. PAL locks would be installed on all weapons, including submarine missiles, to prevent their launch until enabling codes are transmitted by higher authority. Positive control activities in general would require prior approval from central authorities, reducing the scope for decentralized preparation for immediate counter attack.

At the same time, activities associated with force and command survival could be highly decentralized. Since these activities are defensive in character, strategic units at all levels, including the lowest echelon, would be programmed for rapid dispersion, and so forth, and would be granted unprecedented authority to take unplanned steps necessary for their continuing survival. Various information channels, particularly tactical warning circuits, would be modified to provide maximum support for this decentralized activity. Direct links between warning sensors and individual units, for instance, could be installed. Sensor outages or other degradations would deliberately trigger extensive defensive responses on the part of affected units.

Among the three force components, the bomber force is most affected by this reposturing. Extensive revision of preplanned bomber operations would be required. Under current arrangements, alert bombers with traditional SIOP missions are flushed on tactical warning and flown toward loiter orbits on the periphery of enemy territory in anticipation of imminent dissemination of retaliatory orders. Under the proposed doctrine, bombers might be flushed on tactical warning but they would not leave the CONUS area (where communications, particularly UHF line-of-sight radio communication, would be vastly superior) until retaliation had been authorized. Instead, they would operate like strategic reserve bombers. Bomber take off, flight profile, tanker rendezvous, and recovery would be designed to ensure the continuing survival and coherence of the bomber force and would not be offensive in character.

The survival of bombers over a prolonged time period is of course an objective of questionable feasibility. Despite careful planning, attrition could be very high. Airborne endurance is inherently limited, useable runways could be scarce, fuel could be in short supply, crew exposure to radiation could be very high, and so forth. Without negotiated deep reductions in the adversary's nuclear arsenal, and without development of a bomber aircraft capable of landing at austere airfields, the future of this leg of the force structure may not be bright under the proposed doctrine.

The same problems plague the airborne segment of the U.S. command structure. While it can, and does, play a vital role in current strategy which envisions an immediate, large-scale nuclear counteroffensive, it is ill-suited to a doctrine of delayed response. The airborne command network could not play a major role in the proposed strategy unless more versatile aircraft are developed to replace current ones, and unless deep reductions in nuclear weapons deployments are achieved. Although those conditions are not unattainable, reliance on the airborne command network probably would be reduced greatly if a doctrine of "no immediate second use" is adopted. Command aircraft along with bombers might even be phased out entirely in favor of force and command elements that can endure for long periods or that lend themselves to reconstitution.

The role of fixed land-based missiles might also be diminished. These forces could not ride out a well coordinated Soviet missile attack and they would not be afforded the putative protection of launch-on-warning. (Under the proposed doctrine, launch-on-warning becomes strictly anathema.) Furthermore, residual survivors could not endure very long given existing provisions for supplying back-up power and other essential logistical support. On the other hand, Soviet attack coordination may well fall short of conservative expectation, and additional steps could be taken to increase the endurance of surviving forces. Development of mobile land-based missiles such as Midgetman could further expand the potential contribution of this leg of the Triad to the proposed policy.

Missile submarines would undoubtedly play the pivotal role in the proposed strategy by virtue of their invulnerability and capacity to endure over time. Submarine operations would require only minor adjustment.

Regardless of the ultimate composition of the force structure, the command system that stands behind the forces must possess attributes that the existing system lacks. Provision must be made for enduring or reconstructible command, control, communications and intelligence in order to allow for effective retaliation if and when national authorities decide to execute U.S. forces.

The existing intelligence system is acutely vulnerable and therefore cannot be relied on to assess damage caused by Soviet attack. Its worth mainly derives from the <u>preimpact</u> tactical warning and attack assessment it could provide to reduce exposure to initial Soviet strikes. Preimpact information is too fragmentary and unreliable to be a sound basis for strategic policy formulation in the postattack period. The United States needs to develop intelligence systems that can generate reliable, accurate, and current reports as the damage occurs. IONDS is the only system being developed for this purpose.

Also needed are command centers that can withstand large-scale attack and function long afterwards. Current arrangements place too much reliance on airborne command posts. Alternative arrangements under study and development envisage a major change in crisis relocation plans for national authorities and senior military commanders as well as the introduction of ground mobile command centers. It is understood that such arrangements would provide for eventual reconstitution of essential command functions regardless of the scenario. A portion of the system would not depend on strategic or tactical warning for protection. The rest of the system would be designed for rapid generation in time of national emergency.

The merits of the planned system depends on details that have not been publicly disclosed. The level of effort in this area, however, is clearly insufficient. Programs that show promise ought to be accelerated and alternative technical options ought to be pursued more vigorously. One alternative option that deserves serious consideration is the development of undersea command posts. Trident submarines, for example, could be adapted for use in this role.

Technical options for postattack strategic communications also need to be pursued more vigorously. Virtually all present networks are subject either to direct attack or to sharp constraint on endurance, and planned networks appear to offer only marginal improvement in these terms. MILSTAR holds out some promise as a partial solution to the problem but a high confidence solution will surely entail development of other capabilities. Efforts ought to be concentrated on development of robust communications between national authorities and missile submarines. As discussed at length in earlier chapters, such communications are presently tenuous. Communications with missile submarines are vastly inferior to bomber and land-based missile communications, yet this is the force component on which the United States relies most heavily. If the proposed doctrine is adopted, reliance on missile submarines would grow even more.

The backbone of postattack communication ought to be constructed from elements that can be reconstituted. Such elements include meteor burst, adaptive HF, and mobile HF, LF, VLF, and ELF radio communications. A dedicated strategic network comprised of these elements would be coupled with ground mobile and undersea command posts as well as the missile submarines and other strategic forces. In addition, various units such as submarine command posts and designated land missile silos could be equipped with rockets capable of launching austere communications satellites into orbit.

The United States also should reexamine the technological feasibility of survivable ELF submarine communications using railroad tracks or the geological formations of the continental shelf. DoD investigated these promising technical possibilities in the early 1970s but did not pursue them vigorously because of technological risk and high cost. The two programs -- PISCES (railroad tracks) and SHELF (continental shelf) -- ought to be seriously reconsidered.

Development of virtually all these technical options is presently underfunded. Substantially higher investment and accelerated delivery schedules are warranted.

Targeting Doctrine and Counterforce Weapons

Although a doctrine of "no immediate second use" is theoretically neutral with respect to targeting principles, certain practical ramifications of the doctrine would affect target selection. Adoption of the proposed doctrine would lead to greater reliance on missile submarines and low data rate communications, and would substitute delayed response for prompt retaliation. The aggregate effect of these changes is to deemphasize counterforce targeting, especially strikes against "time-urgent" military targets. The presumed value of such targets would be diminished, and the generally high "hardness" of most "time-urgent" targets would not normally permit judicious targeting by submarine-launched weapons.

Deployment of the D-5 missile on U.S. submarines could compensate for the decline in capabilities for prompt hard target attack that would otherwise result from changes in U.S. force composition. The time delay factor in U.S. retaliation, however, would by itself reduce greatly the worth of weapons for prompt hard target attack. In general, adoption of the proposed doctrine would invalidate most counterforce requirements and hence lower the priority of counterforce weapon development.

If there is any targeting principle rooted in the philosophy of delayed response, it is that command systems should not be struck by either side. Even though U.S. command modernization should be based on the conservative assumption that destruction of U.S. C^3I would be a prime objective of Soviet attack strategy, it seems highly desirable to promote the idea that the maintenance of maximum control over strategic forces on both sides serves a mutual interest. It should be established that command system attack is not only militarily unattractive, but also undesirable in principle.

Crisis Stability

The doctrine would promote crisis stability in several ways. First, it may lead to reduced incentives for preemptive attack insofar as it fosters deployment of a more survivable C^3I network. Pressures for early employment of U.S. forces would be relieved by the creation of a robust network. By the same token, the United States would establish that its threat of retaliation cannot be removed by a sudden attack on its command system. A viable system would presumably alter Soviet calculation of the military advantage of first strike, thereby reducing the incentive to initiate attack in a crisis. At present, Soviet planners may believe that rapid suppression of the U.S. command system would deliver a decisive military blow, an assessment that could only undermine crisis stability. The command modernization resulting from adoption of the proposed doctrine would work to dispel this belief.

Second, by emphasizing defensive response over preparations for offensive engagement, the doctrine would permit the United States to take military precautions in a crisis without signaling aggressive intent. At present, increases in strategic readiness associated with crisis alert have an offensive orientation that works to heighten tensions. By raising the level of strategic readiness only one notch in a crisis, the possibility of nuclear war seems less remote. Peak readiness represents a serious offensive threat that could engender Soviet fear of imminent attack and provoke rather than deter attack. By contrast, a doctrine of delayed response has a defensive orientation that should dampen escalation; allay Soviet fear of nuclear attack; and prevent the dangerous perception that nuclear war may be unavoidable. Under this doctrine, increases in strategic readiness are less provocative, more apt to raise the psychological threshold of the imminence of nuclear war. This would promote crisis stability.

Third, the doctrine inhibits development of destabilizing counterforce capabilities. Since the utility of weapons for prompt hard target attack against "time-urgent" military targets such as ICBM installations would be greatly diminished, the doctrine would moderate investment in those weapons. The technical composition of the resulting force structure would not pose a first-strike threat to the opponent's retaliatory forces, and thus would not undermine crisis stability. At present, confidence in second-strike capability is declining on both sides due to sustained parallel investment in counterforce technology. If present trends continue, as they are expected to, there will be further erosion of crisis stability. The proposed doctrine would work to arrest these trends.

Lastly, efforts to strengthen command performance and hence crisis stability, are more likely to succeed if they are disassociated from war-fighting doctrine. Compared to the proposed doctrine, protracted war-fighting does not appeal as strongly to traditional strategic principles and constituencies. Programs advanced under a war-fighting label are apt to be derided and strongly resisted at home. At the same time, command preparation for protracted nuclear war is apt to stimulate Soviet countermeasures. Command preparation for delayed response, by contrast, is generally consistent with traditional declaratory policy based on assured destruction. The aims of the proposed doctrine require substantial adjustments to U.S. operational posture, but they do embrace the core traditional principles of deterrence that emphasize the inadmissibility of nuclear war and the negligible military utility of nuclear weapons. Programs advanced under this construction ought to appear as reasonable and legitimate to Soviet audiences as they do to our own.

Critics may argue that "no immediate second use" undermines crisis stability on the grounds that it evinces a loss of will and jeopardizes our capacity for retaliation. In this view, the threat of retaliation would be weakened militarily and discredited politically. The Soviet Union would perceive a defeatist attitude and an opportunity to prosecute an offensive campaign without the interference, disruption, and devastation that a prompt U.S. counterattack would produce.

Such criticism, we argue, misses the key point that the proposed doctrine would channel resources into programs, namely C^3I programs, that are crucial to our future ability to carry out our threat of retaliation. This doctrine aims to <u>restore</u> confidence in our ability to exercise positive control under a wide range of adverse conditions. At present, notwithstanding a strong inclination to retaliate immediately if attacked, the state of U.S. C^3I casts fundamental doubt on the ability of American leaders to direct U.S. forces to coherent national purposes in the wake of Soviet nuclear attack. It is the chronic imbalance in force and command structure development that really jeopardizes our capacity to retaliate.

Arms Control

By accentuating the command aspects of strategic stability, a doctrine of "no immediate second use" encourages consideration of C^3I topics in arms control negotiations. An agenda could include a wide range of prospective measures intended to lend protection to the respective command structures and reduce risks of misperception in time of crisis. Among the items worthy of consideration are the following:

Ban Antisatellite (ASAT) Deployments: The United States suspended ASAT negotiations with the Soviet Union after the invasion of Afghanistan in 1979. These talks should be resumed. A recent Soviet offer to impose a moratorium on ASAT launches provides a basis for initial discussion that would hopefully lead to a total ban on ASAT testing and deployment.

Although the United States will soon conduct initial tests of an F-15 based ASAT weapon which is superior to ASAT weapons in the Soviet inventory, the long term costs of unrestrained ASAT competition could vastly outweigh any near-term advantages that we may hope to gain. Space-based assets play important, in some instances vital, roles in national defense. Both sides have a strong interest in preserving the accepted legitimacy of these activities -- notably, worldwide communications and intelligence collection -- but the stakes are especially high for the United States. Its strategic forces are more far-flung and hence more dependent upon satellite communications. By contrast, the Soviets rely to a far greater extent on land-based missile forces, which in turn depend less on satellites for communications. Furthermore, the United States is becoming increasingly dependent upon satellites for strategic communications and tactical early warning. Under the provisions of the current C^3I plan, MILSTAR communication satellites and early warning satellites will form the backbone of our future C^3I network. The emergence of an ASAT threat to these systems, a development that should be anticipated in an environment of unrestrained ASAT competition, could derail current plans for command modernization.

Prohibit Missiles Stationed with Short Flight Times Close to Enemy Borders: Both sides currently operate nuclear forces at forward locations that can strike enemy command facilities within a few minutes after launch. U.S. and Soviet strategic submarines are now poised for such short warning attacks. Pershing II deployments in Western Europe will, from a Soviet standpoint, aggravate the problem because they could strike key Soviet command facilities within ten minutes after launch.

An arms agreement that restricts nuclear deployments to zones that preclude short range attack would mitigate the threat of sudden command decapitation. Stipulations of this sort would promote crisis stability and ought to be a subject of negotiation.

Prohibit Tests of SLBM "Depressed Trajectories": The flight time of SLBMs can be substantially reduced by lowering the missiles' trajectory. To date, neither side has conducted tests of depressed trajectories. Were they to do so, the threat of command decapitation would become more pronounced, thereby undermining crisis stability. An agreement that prohibits tests of depressed trajectories should therefore be negotiated.

Ban Forward Deployment of Cruise Missiles: Although cruise missiles are much slower than ballistic missiles, they are much less susceptible to detection. Cruise missiles could therefore be used in a decapitation attack, especially if launched from delivery systems in close proximity to the targets.

To mitigate the threat of precursor cruise missile attacks on command facilities, the parties could agree to prohibit close-in deployment of cruise missile carriers — ships, submarines, aircraft and ground bases.

Create Ocean Sanctuaries for SLBMs and Undersea Command Posts: The aim of this proposal is to prevent inadvertent or deliberate engagements between antisubmarine warfare (ASW) forces and central strategic systems (forces and command units). As reliance on sea-based strategic systems grows, the value of measures that increase confidence in the survival of these systems also grows. One such measure is to prohibit ASW forces from operating in certain ocean areas.

Establish Risk Reduction Centers: Senators Nunn and Warner have proposed that the two superpowers establish jointly manned centers in each country to deal with various events — acts of nuclear terrorism, nuclear explosions of ambiguous origin, accidental or unauthorized nuclear attacks, and so forth — that could potentially trigger an inadvertent nuclear war. The idea is to facilitate crisis communications and clarification of situations that could produce a war that was not intended.

Improve "Hot Line" Between Washington and Moscow: Timely emergency communications between the leaders of the United States and the Soviet Union presently depend on the so-called "Hot Line." The "Hot Line" provides for teletype communications only, is accessible from few locations, and is routed through circuits having little redundancy. A desirable expansion of the "Hot Line" system would feature the addition of a satellite voice channel with greater accessibility and more redundancy. For instance, a direct satellite link between NEACP and alternate Soviet command facilities should be installed.

Institutional Reorganization

Implementation of a doctrine that elevates the priority of command development to the same level as weapons systems requires that a powerful C^3I advocate be created within the defense bureaucracy. Advocates have historically lacked the clout necessary substantially to alter the logic and pattern of strategic investment. They still operate with this handicap. Sponsors of command modernization wield too little program and budget authority to prevail over advocates of force modernization. Unless a countervailing power base is created, weapon programs will continue to take precedence, regardless of the prominence of command modernization themes in presidential oratory and/or defense guidance.

CONCLUSION

In making command improvement the pivotal component of its plan for strategic modernization, the Reagan administration formally acknowledged the importance of command performance to national security. More than that, it defined command modernization as the overriding aim of U.S. strategic policy. For the first time in twenty-five years, the United States Government is saying that C^3I is being elevated to the top of the strategic agenda.

Underneath the encouraging rhetoric, however, lies the depressing reality that we are scarcely any closer to answers to the central command questions than we were a decade ago. In fact, we are scarcely any closer to knowing how to pose the questions. The outlook for genuine progress in rectifying command deficiencies is therefore not as bright as one might initially imagine given the administration's profile on the matter.

It is also open to question whether or not command modernization can remain a priority aim of U.S. security policy. The United States Government still has to contend with analytic, technical, economic and bureaucratic conditions that detract from this goal. These conditions have historically undermined command system development, and the Reagan administration has not yet confronted them squarely. Indeed, the administration is preoccupied with other foreign policy and defense issues. The amount of attention and resources being devoted to command modernization does not square with its supposed priority. The command problem has been overshadowed by other pressing matters that have arrived on the security agenda: deadlocked arms control negotiations; hostile relations with the Soviet Union, Central America, and the Middle East. Even the part of the security agenda having to do with strategic issues treats the command problem as secondary to other issues. Security officials spend more time and energy on such issues as MX deployment and Soviet compliance with arms treaties than they do on problems of command-control. In practical terms, command modernization does not appear to be a priority objective at all. Contrary to official contention, it appears to have a relatively low priority. Put in historical perspective, the administration's handling of the command question is beginning to look like another recurrence of false starts and faltering commitment that results in marginal or no real improvement in command performance.

Nevertheless, the climate for new conceptualization and new initiative in this area has never been more favorable. It is incumbent upon defense professionals to underscore the fact that command performance is a central question of national security and to actively support the search for answers. This search needs to be conducted without the emotional extremes of despair or wildly inflated expectations. With sustained and sober effort, the United States could at least begin to come to grips with one of the most important security dilemmas of our time.

Appendix A

Land Missile Force Characteristics (1962-1973)

	Launchers (number)	Type	Yield (megatons)	CEP (miles)	Hardness (p.s.i.)
1962					
U.S.	120	Atlas	3	1.0	5
	30	Titan I	4	1.0	100
U.S.S.R.	30	SS-7	5	1.5	5
1963					
U.S.	120	Atlas	3	1.0	5
	54	Titan I	4	1.0	100
	54	Titan II	5	0.7	300
	186	Minuteman I	1	0.7	300
U.S.S.R.	100	SS-7	5	1.5	5
1964					
U.S.	120	Atlas	3	1.0	5
	54	Titan I	4	1.0	100
	54	Titan II	5	0.7	300
	630	Minuteman I	1	0.7	300
U.S.S.R.	150	SS-7	5	1.5	5
	50	SS-8	5	1.5	100
1965					
U.S.	54	Titan II	5	0.7	300
	800	Minuteman I	1	0.7	300
U.S.S.R.	150	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	42	SS-9	25	0.7	100-300
1966					
U.S.	54	Titan II	5	0.7	300
	800	Minuteman I	1	0.7	300
	80	Minuteman II	1	0.3	300
U.S.S.R.	150	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	110	SS-9	25	0.7	100-300
	10	SS-11	1	1.0	300

	Launchers (number)	Type	Yield (megatons)	CEP (miles)	Hardness (p.s.i.)
<u>1967</u>					
U.S.	54	Titan II	5	0.7	300
	700	Minuteman I	1	0.7	300
	300	Minuteman II	1	0.3	300
U.S.S.R.	150	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	162	SS-9	25	0.7	100-300
	178	SS-11	1	1.0	300
	10	SS-13	1	1.0	300
<u>1968</u>					
U.S.	54	Titan II	5	0.7	300
	600	Minuteman I	1	0.7	300
	400	Minuteman II	1	0.3	300
U.S.S.R.	150	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	192	SS-9	25	0.7	100-300
	426	SS-11	1	1.0	300
	20	SS-13	1	1.0	300
<u>1969</u>					
U.S.	54	Titan II	5	0.7	300
	500	Minuteman I	1	0.7	300
	500	Minuteman II	1	0.3	300
U.S.S.R.	150	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	228	SS-9	25	0.7	100-300
	550	SS-11	1	1.0	300
	30	SS-13	1	1.0	300
<u>1970</u>					
U.S.	54	Titan II	5	0.7	300
	490	Minuteman I	1	0.7	300
	500	Minuteman II	1	0.3	300
	10	Minuteman III	3 x .170	0.2	300
U.S.S.R.	150	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	288	SS-9	25	0.7	100-300
	751	SS-11	1	1.0	300
	40	SS-13	1	1.0	300

	Launchers (number)	Type	Yield (megatons)	CEP (miles)	Hardness (p.s.i.)
1971					
U.S.	54	Titan II	5	0.7	300
	390	Minuteman I	1	0.7	300
	500	Minuteman II	1	0.3	300
	110	Minuteman III	3 x .170	0.2	300
U.S.S.R.	139	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	288	SS-9	25	0.7	100-300
	956	SS-11	1	1.0	300
	60	SS-13	1	1.0	300
1972					
U.S.	54	Titan II	5	0.5	300
	290	Minuteman I	1	0.7	(80% at 300
	500	Minuteman II	1	0.3	p.s.i./20% at
	210	Minuteman III	3 x .170	0.2	1500 p.s.i.)
U.S.S.R.	139	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	288	SS-9	25	0.7	100-300
	970	SS-11	1	1.0	300
	60	SS-13	1	1.0	300
1973					
U.S.	54	Titan II	5	0.5	300
	140	Minuteman I	1	0.7	(60% at 300
	510	Minuteman II	1	0.3	p.s.i./40% at
	350	Minuteman III	3 x .170	0.2	1500 p.s.i.)
U.S.S.R.	139	SS-7	5	1.5	5
	70	SS-8	5	1.5	100
	288	SS-9	25	0.7	100-300
	970	SS-11	1	1.0	300
	60	SS-13	1	1.0	300

APPENDIX B

SAMPLE COMPUTATIONS

A. Nonreprogrammable Attacks

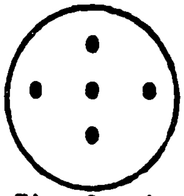
This section of the appendix derives the results entered in the third row of Figures 4-5 and 4-7. The results in this row correspond to an assumed Soviet missile reliability of .85, and to other assumptions given in the notes on page 182.

Figure 4-7 assumed that the Soviets allocated one SS-9 missile to each of the 88 launch control centers. Based on the formula given on page 48, the probability that any LCC would have remained functional following the attack was 24 percent. Calculated next is the probability that zero, one, two, three, four, or five LCCs would have survived in any squadron, given that the probability of survival is 24 percent for an individual control center. This set of probabilities were derived as shown on the following page.

The expected number of Minuteman squadrons with zero, one, two, three, four, or five surviving launch control centers was obtained by multiplying each of these probabilities times the total number of squadrons deployed.

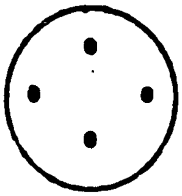
Five centers survive in zero squadrons because
(.00) (18) = .00

Four centers survive in zero squadrons because
(.01) (18) = .18



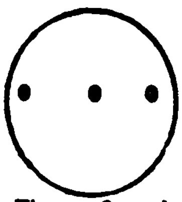
Five Survive

$$C(5,0)(.24)^5 = .00$$



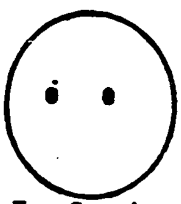
Four Survive

$$C(5,1)(.24)^4(.76) = .01$$



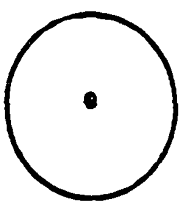
Three Survive

$$C(5,2)(.24)^3(.76)^2 = .08$$



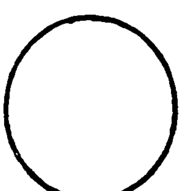
Two Survive

$$C(5,3)(.24)^2(.76)^3 = .25$$



One Survives

$$C(5,4)(.24)(.76)^4 = .40$$



None Survive

$$C(5,5)(.76)^5 = .25$$

where $C(\underline{n},\underline{r}) = n!/r!(n-r)!$ and $n = 5$, $r = 1,2,3,4,5$

Three centers survive in one or two squadrons because (.08) (18) = 1.44

Two centers survive in four or five squadrons because (.25) (18) = 4.5

One center survives in seven squadrons because (.40) (18) = 7.2

No centers survive in four or five squadrons because (.25) (18) = 4.5

This arithmetic indicates that four or five squadrons, or 200-250 land missiles, or 22-28 percent of the total Minuteman land missile force, would have been deprived of launch control. In the analysis, estimates were rounded to the nearest unit (full squadrons). In this example, the expected number of destroyed squadrons was rounded to five, which represented 28 percent of the American land missile force. This estimate is shown under the column headed "expected" in Figure 4-7, row three.

The next step in the quantitative treatment of this case was to compute the probability that more than the expected number of squadrons would have been destroyed. The risks of losing all five control elements in zero to eighteen squadrons were estimated as shown on the following page.

Risks were calculated by reading up from the bottom of the column headed "results," summing the probabilities at each step, and reading off the corresponding number in the column headed "squadrons destroyed." The cumulative percentage represents the risk that N or more squadrons would have been destroyed in 1966. For example, 27

SQUADRONS DESTROYED*	FORMULA	RESULTS (Probability)
0	$C(18,0)(.75)^{18}$	.01
1	$C(18,1)(.25)(.75)^{17}$	.03
2	$C(18,2)(.25)^{2}(.75)^{16}$	.10
3	$C(18,3)(.25)^{3}(.75)^{15}$	.17
4	$C(18,4)(.25)^{4}(.75)^{14}$	.21
5	$C(18,5)(.25)^{5}(.75)^{13}$	.20
6	$C(18,6)(.25)^{6}(.75)^{12}$	.14
7	$C(18,7)(.25)^{7}(.75)^{11}$	.08
8	$C(18,8)(.25)^{8}(.75)^{10}$	.04
9	$C(18,9)(.25)^{9}(.75)^{9}$	.01
10	$C(18,10)(.25)^{10}(.75)^{8}$	.00
11	$C(18,11)(.25)^{11}(.75)^{7}$	.00
12	$C(18,12)(.25)^{12}(.75)^{6}$	.00
13	$C(18,13)(.25)^{13}(.75)^{5}$	.00
14	$C(18,14)(.25)^{14}(.75)^{4}$	.00
15	$C(18,15)(.25)^{15}(.75)^{3}$	.00
16	$C(18,16)(.25)^{16}(.75)^{2}$	.00
17	$C(18,17)(.25)^{17}(.75)$	.00
18	$C(18,18)(.25)^{18}$	.00

Risk of six or more destroyed=27%[a]

Risk of seven or more destroyed=13%[b]

Risk of eight or more destroyed=5%[c]

Risk of nine or more destroyed= 1%

*Squadrons in which all five launch control centers are destroyed or deprived of communications, based on previous estimate that the probability of destruction was 25 percent for any single squadron.

[a]Sum of .14 + .08 + .04 + .01; [b]Sum of .08 + .04 + .01; [c]Sum of .04 + .01.

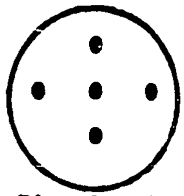
percent (the sum of 1 percent, 4 percent, 8 percent, and 14 percent) represents the risk that six or more squadrons would have been disabled.

Since 27 percent fell within the first risk category (headed "risk" $\geq$ 20%) of Figure 4-7, the number of missiles deprived of launch control in six squadrons was converted to a fraction (33 percent) of the total number of Minuteman land missiles and then entered in Figure 4-7. The same procedure was used to fill in the other risk categories in the third row.

The Soviets could have increased the expected damage from an attack on the launch control centers by adopting a different attack strategy. With a force of 110 SS-9 missiles, they could have allocated two missiles to each of the control centers in eleven squadrons (55 control centers in all). Figure 4-5 shows the results of the alternative attack strategy using SS-9 missiles with an assumed reliability of .85 (OAR).

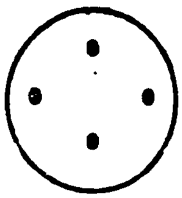
In deriving the results, it was found that this attack strategy decreased the probability that any individual LCC would have survived from 24 percent to 6 percent. This probability is the simple product of the probability of an LCC surviving the first missile times the probability of that same center surviving the second missile, or 24 percent times 24 percent.

The expected number of LCCs that would have survived in any of the squadrons attacked was estimated by the same procedure used previously:



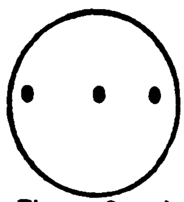
Five Survive

$C(5,0)(.06)^5$ = .00



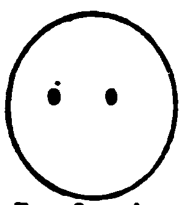
Four Survive

$C(5,1)(.06)^4(.94)$ = .00



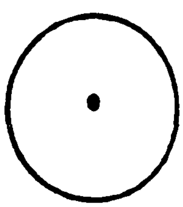
Three Survive

$C(5,2)(.06)^3(.94)^2$ = .00



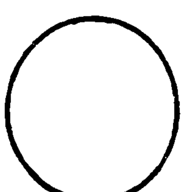
Two Survive

$C(5,3)(.06)^2(.94)^3$ = .03



One Survives

$C(5,4)(.06)(.94)^4$ = .23



None Survive

$C(5,5)(.94)^5$ = .73

where $C(\underline{n},\underline{r}) = n!/r!(n-r)!$ and $n = 5$
$r = 1,2,3,4,5$

In the seven squadrons that were not attacked, five centers survive with communications capabilities intact. In the other squadrons:

> Five centers survive in zero squadrons because (.00) (11) = .00
>
> Four centers survive in zero squadrons because (.00) (11) = .00
>
> Three centers survive in zero squadrons because (.00) (11) = .00
>
> Two centers survive in zero squadrons because (.03) (11) = .33
>
> One center survives in two or three squadrons because (.23) (11) = 2.53
>
> No centers survive in eight squadrons because (.73) (11) = 8.03

The expected destruction of eight squadrons would have rendered 400 Minuteman missiles unusable. This represents 44 percent of the total Minuteman land missile force, which was entered in Figure 4-5, in the third row under the column headed "expected."

Finally, the risk categories were filled in using the procedures explained above, and the computations shown below.

B. Reprogrammable Attacks

The Soviets were assumed to possess modest capabilities to reprogram reserve missiles to replace known launch failures. The

SQUADRONS DESTROYED*	FORMULA	RESULTS (Probability)
0	$C(11,0)(.27)^{11}$	.00
1	$C(11,1)(.73)(.27)^{10}$	.00
2	$C(11,2)(.73)^{2}(.27)^{9}$	.00
3	$C(11,3)(.73)^{3}(.27)^{8}$	.00
4	$C(11,4)(.73)^{4}(.27)^{7}$	.01
5	$C(11,5)(.73)^{5}(.27)^{6}$	.04
6	$C(11,6)(.73)^{6}(.27)^{5}$	.10
7	$C(11,7)(.73)^{7}(.27)^{4}$	.27
8	$C(11,8)(.73)^{8}(.27)^{3}$	.26
9	$C(11,9)(.73)^{9}(.27)^{2}$	.24
10	$C(11,10)(.73)^{10}(.27)$	.13
11	$C(11,11)(.73)^{11}$	.03

*Squadrons in which all five launch control centers are destroyed or deprived of communications, based on previous estimate that the probability of destruction was 73 percent for any single squadron.

method used is described by Davis and Schilling,[1] which in effect produces new SSKP inputs for the statistical calculations described above.

---

1. See Lynn Etheridge Davis and Warner R. Schilling, "All You Ever Wanted to Know About MIRV and ICBM Calculations But Were Not Cleared to Ask," Journal of Conflict Resolution, vol. 17, no. 2 (June 1973), esp. pp. 218-22.

APPENDIX C

Electromagnetic pulse (EMP) is like a brief pulse of sunlight in that it must be collected into a small volume to cause damage. This focusing and damage are especially likely in the case of long electrical wires connected to sensitive equipment. Nelson notes:

> A prime example here would be a radio receiver, connected to a long antenna and to the A.C. power line. The wires pick up the energy in the electromagnetic field over a large area and then deliver it in the form of current and voltage pulses to the attached equipment.[1]

Metallic objects collect and focus EMP energy because they are sensitive to the radio frequency region of the spectrum, and it is in that region where EMP energy tends to be concentrated. For a high-yield, high-altitude explosion, the EMP energy is concentrated at the high-frequency radio band. The principal frequency of the EMP produced by a surface burst tends toward lower frequencies, depending upon the weapon yield. The higher the yield, the larger the ionized sphere surrounding the burst point and the lower the principal frequency. For example, the radius of the ionized sphere generated by a high-yield surface burst can be as large as five miles. The principal frequency for this (or any other) burst is given by:

---

1. David B. Nelson, "EMP Impact on U.S. Defense," Survive, vol. 2, no. 6 (November-December 1967), p. 4.

Frequency (cycles/second) = speed of light/diameter of sphere

Thus, the principal frequency in this case is 18-19 Khz (very low frequency).

Soil only partially insulates buried cables from the energy of electromagnetic pulse. Dry, sandy soil, such as that found in many areas where Minuteman missiles are deployed, permits the very low-frequency component of EMP to penetrate about 500 feet. [2] Low-frequency components penetrate 150 feet. About one-half of the strength of the high-frequency component penetrates 30 feet.

This analysis assumes the presence of dry, sandy soil and an impinging EMP pulse of 50,000 volts per meter. The decay time constant (the time required to decay from 50,000 volts to 18,400 volts) of the pulse is assumed to be one-millionth of a second. The underground cable connecting a hypothetical missile silo and launch control center is two inches in diameter, tubular, and shielded with a 100-mil-thick lead sheath. And it is five kilometers, or three statute miles, long.

The direction of arrival (elevation and angle of incidence) of the EMP at the earth's surface depends on the dip angle of the magnetic field below the burst location. In this analysis the direction of arrival is constrained to vectors that apply to bursts anywhere over the continental United States. Assuming the worst-case direction of

---

2. Assumptions and method of calculation are taken from L.W. Ricketts, J.E. Bridges and J. Miletta, <u>EMP Radiation and Protective Techniques</u> (New York: John Wiley, 1976).

arrival, EMP generates an estimated peak current of 2,850 amperes on the exterior sheath of the cable. This current penetrates into the cable and a voltage surge propagates to the ends. A peak inside surge of about 1,200 volts occurs at the ends, rising from 10 to 90 percent of this value in about 1.3 millionths of a second.

Such a surge greatly exceeds the voltage damage threshold of components used in modern computers. The direct coupling of this surge into a modern computer, which typically has an interference threshold of about two volts and a damage threshold of ten volts for a pulse lasting one-millionth of a second, would be expected to disable it.

Other possible angles of arrival should be considered. The table below gives the estimated exterior current surge and interior voltage surge (at the ends) for various direction vectors applicable to targets in the United States. As shown, voltage surges in excess of the tolerances of computer components are predicted. An average surge might be on the order of 1,000 amperes and 400 volts.

These calculations identify a potential threat. Validation, however, would require experimental testing and simulation. In general, such tests have established that modern communications and electronics equipment, owing to the extensive use of sensitive semiconductors, transistors and integrated circuits, are highly susceptible to damage from EMP-induced currents and voltages. According to Gaul, "without special design considerations, these

Elevation Angle

Azimuth Angle	10	20	30	60	90
10	86	171	257	428	542
30	228	428	684	1140	1340
50	399	684	912	1710	1995
70	456	855	1197	2280	2850
90	485	912	1368	2337	2850

Exterior Sheath Current

Elevation Angle

Azimuth Angle	10	20	30	60	90
10	35	71	106	177	224
30	94	177	282	470	553
50	165	282	376	705	823
70	188	353	494	941	1176
90	200	376	564	964	1176

Interior Voltage Surge

FIGURE C-1

devices normally cannot handle the voltage and current surges that result from EMP coupling." [3]

3. Edwin James Gaul, "Electromagnetic Pulse," Military Review, vol. 55, no. 3 (March 1975), p. 16.

Appendix D

When the radiated energy from a nuclear explosion in space strikes a satellite, several different interactions occur. The likelihood of damage from each interaction effect increases, _ceteris paribus_, the closer the weapon is to the target at the moment of detonation. This relationship holds because impinging X-ray energy -- the source of the interaction effects -- falls off as the inverse square of the distance between the weapon and target.

The interaction effect of primary interest in this appendix is called system-generated electromagnetic pulse, or SGEMP. Two other prime causes of satellite damage should be noted. They are: (1) thermal overload, and (2) transient-radiation effects on electronics (TREE). Thermal overload is simply an overheated state produced when satellite materials absorb X-ray energy. Although satellites are very sensitive to thermal load, disabling TREE effects are likely to occur before thermal effects become pronounced.

"Hard" X-rays, particularly gamma rays, generate TREE*. Incident X-rays penetrate the outer structures and internal electron boxes, exposing semiconductor components to a direct dose of radiation. The rate of exposure (dose rate) and the total exposure (bulk dose) are both responsible for damage. A bulk dose on the order of 10^4 to 10^5 rads (silicon) alters the threshold voltage of transisters, for example, resulting in damage to communications equipment.

* A nuclear explosion releases most of its energy in the form of X-rays, whose energies range from relatively low ("soft") to high ("hard" X-rays which include the very high energy gamma rays).

Thermal overload and TREE effects are generally thought to be weak damage mechanisms so long as weapon detonation occurs far away from the target. At relatively close range -- hundreds or a few thousands of kilometers -- these effects are considered lethal to satellites. Due to the clustering of U.S. communications satellites in geosynchronous orbit, in all likelihood a very small number of weapons detonated at close range would cripple strategic satellite communications. However, the positioning of nuclear-armed spacecraft within close range of U.S. communications satellites would consume at least six hours; it might alert the United States to impending attack; and it would carry a significant risk of technical failure inasmuch as the feat has not been exercised in the past. Furthermore, an alternative, less demanding attack strategy exists.

The alternative strategy is to detonate high-yield weapons at relatively low altitudes -- say, 60 miles. A land missile such as the SS-9 could be the delivery vehicle. The objective is to generate SGEMP against geosynchronous satellites.

It might be recalled that an explosion at this altitude generates strong electromagnetic effects which can degrade command elements on the ground or in the atmosphere. Thus, the attack strategy would entail a simultaneous electromagnetic attack on both satellites and ground/airborne command networks. The attack on ground/airborne systems takes advantage of the Compton-effect produced when the weapon's gamma rays collide with air molecules. The resulting electrical field interacts with the earth's magnetic field to blanket the United States and surrounding airspace with intense electromagnetic energy.

From the same weapon but traveling in the other direction are "soft" and "hard" X-rays that encounter no air molecules. There is no absorption of the "soft" X-rays (in the earthbound direction, such absorption creates the fireball), nor are there any collisions between gamma rays and air molecules (in the earthbound direction, such collisions create electromagnetic pulse). Consequently, a large fraction of the energy emitted by a nuclear explosion in space travels unimpeded until it strikes an object like satellites. About 80 percent of the total energy of a nuclear explosion escapes into space in the form of X-ray energy, energy which, though not absorbed, spreads out radially in accordance with the inverse square law.

SGEMP is simply current flow on the surface of a satellite; it is the product of the photoelectric effects generated when X-rays strike a satellite. Photoelectric effects occur when incident X-rays transfer all their energy to the electrons of atoms in satellite materials, e.g., aluminum. Energized electrons are then ejected from the atoms, especially those at the surface where exposure to incident X-rays is most intense. When negatively charged electrons that are ejected from the surface escape permanently into space, the satellite is left with a positive charge. SGEMP is this positive photocurrent. It tends to spread evenly across all external surfaces -- skin, antennas, solar arrays, etc. -- where it couples into electrical cables that run along the surface. These cables, e.g., antenna cables, feed the energy into electronic components inside internal boxes.

SGEMP strength cannot exceed a certain limit. The greater the number of ejected electrons, the greater the positive charge left behind, and the harder it becomes for ejected electrons to escape the rising potential. Some of the ejected electrons are so strongly attracted by the positively charged satellite that they return to the surface. This dynamic process which limits the permanent escape of electrons, hence the strength of the photocurrent, is called space-charge-limiting.

SGEMP damage is likely to occur if (1) a nuclear explosion produces a surface current of sufficient magnitude to feed into satellite electronic boxes more energy than internal components can tolerate, and (2) space-charge-limiting allows surface current to reach or exceed this threshold. According to the chief civilian scientist at the Defense Nuclear Agency, surface currents on the order of 50-100 amperes per square meter would be a matter of concern for communications satellites having little or no protection from SGEMP effects. This individual also reported that a one-megaton weapon detonated at an altitude of 17,950 kilometers, or half the distance to geosynchronous satellites, would in theory cause current flow of that magnitude on the surface of representative satellite materials. Such calculations have questionable validity. They are based on "representative" satellite materials and geometries. But in this field of analysis hard facts are hard to come by; the geometry of actual satellites is too complex and varied to permit precise calculation, and the response of electronic components to different SGEMP currents defies prediction. And so analysts resort to simplification and gross assumption.

Therefore, it is potentially misleading to demonstrate, as the following calculations do, that a high-yield weapon detonated 60 miles above the earth could generate 350-700 amperes/m^2 on the surface of representative satellite materials in geosynchronous orbit. Nevertheless, the theoretical values, which are six times greater than the purported danger threshold for basically unhardened satellites, may be reasonable approximations of true values if they could be known. It is at least worthwhile to show the derivation of the estimates. The computational steps given below are used to estimate satellite surface current produced by a one-megaton burst at an altitude of 17,950 kilometers, or half the distance between the earth and satellites in geosynchronous orbit. The same steps were followed to estimate SGEMP from a low altitude (100 kilometer) SS-9 land missile explosion with a yield of 25 megatons. The representative satellite material is aluminum (3 mils thick).

Step 1: Convert weapon yield to joules.

Since 1-kiloton equals 4.18×10^{12} joules, 1-megaton equals $\underline{4.18 \times 10^{15} \text{ joules}}$.

Step 2: Compute the amount of joule energy that is emitted as X-ray energy.

Since 80 percent of the total yield of an exoatmospheric burst is emitted as X-ray energy,

X-ray joule energy equals $0.8 \times 4.18\text{x}10^{15}$ joules or $\underline{3.34 \times 10^{15} \text{ joules}}$.

Step 3: Apply inverse square law to obtain X-ray energy incident on target at a distance r(meters) from the weapon at the moment of detonation.

Formula: $\dfrac{\text{X-ray joule energy}}{4\P(r^2)}$

Since r = 17,950,000 meters, X-ray joule energy incident equals

$$\frac{3.34 \times 10^{15} \text{ joules}}{12.57\ (3.22\text{x}10^{14} \text{ meters}^2)} = \underline{0.83 \text{ joules/m}^2}$$

Step 4: Convert joules/m_2 to calories/cm_2 by dividing results at step 3 by 4.18×10^4

$$\frac{0.83 \text{ joules/m}^2}{4.18 \times 10^4} = \underline{2.00 \times 10^{-5} \text{ calories/cm}^2}$$

Step 5:[a] For a range of plausible weapons characteristics (so-called blackbody temperatures), estimate the electron yield, in coulombs per calorie , ejected at the surface of 3-mil aluminum due to X-rays incident at 1 calorie/cm^2.

Blackbody Temperature (keV)	Electron Yield (Coulombs/calorie)
2	2.80×10^{-6}
5	5.72×10^{-7}
8	2.16×10^{-7}
10	1.32×10^{-7}
12	8.00×10^{-8}

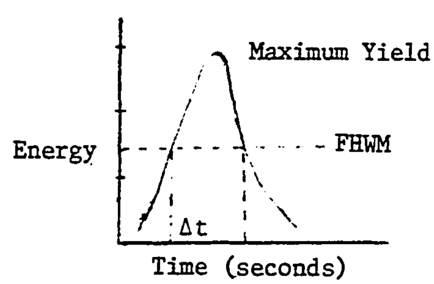
a. I indebted to the Defense Nuclear Agency for these estimates.

Step 6: Multiply previous results (step 5) by 2.00×10^{-5} calories/cm^2 (step 4 result), giving product in coulombs/cm^2. Convert results to coulombs/m^2 by dividing by 10^{-4}.

Note: coulombs/m^2 equals amps/m^2/sec.

Blackbody Temperature (keV)	Coulombs/cm^2	Coulombs/m^2 (amps/m^2/sec)
2	5.60×10^{-11}	5.60×10^{-7}
5	1.14×10^{-11}	1.14×10^{-7}
8	4.32×10^{-12}	4.32×10^{-8}
10	2.64×10^{-12}	2.64×10^{-8}
12	1.60×10^{-12}	1.60×10^{-8}

Step 7: Step 6 results give currents over a one-second interval. Nuclear weapons yield energy much faster. Analysts use a summary measure of energy emission time known as the full half width maximum (FHWM) shown as Δt on the diagram below.



Divide step 6 results by a range of plausible Δts, expressing final results in amps/m^2, or SGEMP photocurrent.

The results below are consistent with DNA's estimate that a one-megaton weapon exploded half the distance between the earth and a satellite in geosynchronous orbit could generate SGEMP currents as high as 50-100 amperes per square meter.

Following the steps outlined above, the estimates for a 25-megaton bomb detonated only 100 kilometers above the United States are about six times greater.

SGEMP PHOTOCURRENT

Amps/m^2

1 Megaton Explosion

Blackbody Temperature (keV)	$\Delta t = 5x10^{-9}$ sec	$\Delta t = 1x10^{-8}$ sec	$\Delta t = 2x10^{-8}$ sec	$\Delta t = 4x10^{-8}$ sec
2	112	56	28	14
5	23	12	6	3
8	9	5	2	1
10	5	3	1	1
12	3	2	1	-

25 Megaton Explosion

Blackbody Temperature (keV)	$\Delta t = 5x10^{-9}$ sec	$\Delta t = 1x10^{-8}$ sec	$\Delta t = 2x10^{-8}$ sec	$\Delta t = 4x10^{-8}$ sec
2	694	347	174	87
5	142	71	36	18
8	53	27	13	7
10	33	16	8	4
12	20	10	5	3