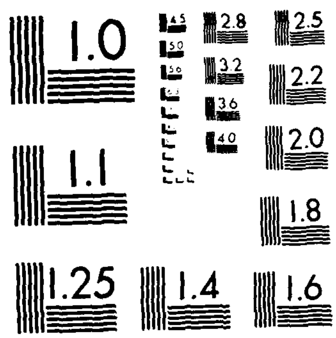
AD-A192 404 WHO IS GOING TO SHOOT DOWN THE FIRST ICBM (INTERCONTINENTAL BALLISTIC MISSILES) - MAN OR MACHINE (U) AIR COMMAND AND STAFF COLL MAXWELL AFB AL J O PIEPENBRINK APR 88 ACSC-88-2130

1/1

UNCLASSIFIED F/G 15/3.1 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

AIR COMMAND AND STAFF COLLEGE

STUDENT REPORT

WHO IS GOING TO SHOOT DOWN THE FIRST ICBM -- MAN OR MACHINE?

MAJOR JOHN O. PIEPENBRINK 88-2130

"insights into tomorrow"

REPORT NUMBER 88-2130

TITLE WHO IS GOING TO SHOOT DOWN THE FIRST ICBM -- MAN OR MACHINE?

AUTHOR(S) MAJOR JOHN O. PIEPENBRINK, USAF

FACULTY ADVISOR MAJOR BRUCE THIEMAN, ACSC/EDW

SPONSOR COLONEL NORMAN F. FENNELLY, SDIO/S

Submitted to the faculty in partial fulfillment of
requirements for graduation.

AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY
MAXWELL AFB, AL 36112-5542

A192 404

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) 88-2130	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION ACSC/EDC 6b. OFFICE SYMBOL *(If applicable)*	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS *(City, State, and ZIP Code)* MAXWELL AFB AL 36112-5542	7b. ADDRESS *(City, State, and ZIP Code)*
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL *(If applicable)*	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS *(City, State, and ZIP Code)*	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO / WORK UNIT ACCESSION NO.

11. TITLE *(Include Security Classification)*
WHO IS GOING TO SHOOT DOWN THE FIRST ICBM -- MAN OR MACHINE?

12. PERSONAL AUTHOR(S)
Piepenbrink, John C., Major, USAF

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT *(Year, Month, Day)*	15. PAGE COUNT
	FROM ______ TO ______	1988 April	22

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

The short time available to attack ballistic missiles with a Strategic Defense Initiative (SDI) weapon system will preclude traditional national level decision making. A unique command and control (C2) concept is required to best serve the balance between effectiveness and weapon system safety. This article develops that concept with a blend of autonomous operation with man in the loop and advocates early resolution to ensure C2 strategy and tactics push technology development.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL ACSC/EDC Maxwell AFB AL 36112-55[illegible]	22b. TELEPHONE *(Include Area Code)* (205)293-2867 22c. OFFICE SYMBOL

DD Form 1473, JUN 86 — Previous editions are obsolete. — SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

PREFACE

This research paper was sponsored by Colonel Norman F. Fennelly from the Strategic Defense Initiative Organization. Subject to clearance, this manuscript will be submitted to SIGNAL magazine for consideration. The specific statement of the problem discussed in the article is: Since timing considerations preclude traditional national level decision-making in an active Strategic Defense Initiative (SDI) Battle Management System, then a command and control (C2) concept must be devised to best serve the balance between effectiveness and weapon system safety. The basic question of who or what is going to push the button to shoot at the incoming missiles is critical to the entire program and requires early resolution because it reflects the operational strategy and eventual tactics for the system. The weapon system strategy and tactics are primary and should push technology development rather than being pulled in the wrong direction by the rapid flow of system development. This issue must be resolved soon to guide the current SDI program in it's research and concept development stage and certainly before development and deployment decisions are finalized.

ABOUT THE AUTHOR

Major John O. Piepenbrink is a student in the Air Command and Staff College, Class of '88. His background in strategic command, control and communications (C3) includes both operational and staff experience with the Organization of the Joint Chiefs of Staff (OJCS) and the Strategic Air Command (SAC). His most recent assignment was with the OJCS C3 Systems Directorate (J6) as a systems engineer charged with assessing the current and proposed DOD space and strategic connectivity systems to satisfy operational requirements. That tour of duty included planning and participating in JCS worldwide command post exercises and briefing senior decision makers on the capability of the National Command Authorities to control strategic nuclear forces. He served at Hq SAC as a concepts development engineer in the C3 and Force Management Division, Deputy Chief of Staff/Plans. His responsibilities included developing and staffing operational requirements for strategic C3 systems with particular emphasis in strategic command centers. He has also served as a Minuteman Launch Control Officer with extensive experience as an instructor and standardization evaluator. He has a BS in Electrical Engineering Technology from Bradley University and an MBA from Marymount University of Virginia. He is a graduate of the Joint C3 Staff Officer School, Squadron Officer School in residence and Air Command and Staff College by seminar. As a member of the Armed Forces Communications and Electronics Association (AFCEA), he was named a Distinguished Young AFCEAN of the Year for 1985.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

FIGURES

EXECUTIVE SUMMARY

REPORT NUMBER 88-2130

AUTHOR(S) MAJOR JOHN O. PIEPENBRINK

TITLE WHO IS GOING TO SHOOT DOWN THE FIRST ICBM -- MAN OR MACHINE?

Many assumptions must be made to limit the scope of this article and focus on it's central issue concerning top level command and control of SDI. The political desirability of SDI and the eventual weapon system design issues are beyond the scope of this article. The President has already directed the effort in his March 1983 speech, yet the outcome is many years away and will continue to change as the research matures. The article first describes the basic SDI defense goals, the generic system and the timing considerations. It is a very brief discussion since the expected audience should have a basic understanding of SDI. The key assumption derived in this section of the article is that timing considerations will preclude the existing methods of "going to war" in most scenarios. The next section describes the problems that must be considered in developing the optimum C2 concept. This includes potential weapon system safety requirements and the ramifications of wrongful system activation. It also includes the advantages and disadvantages of an unmanned autonomous system. With those descriptions, tradeoffs of centralized versus decentralized command and control are discussed. An analyses of the various alternatives leads to a solution with both old and new concepts blended to match the national strategy and make military operational sense.

INTRODUCTION

President Reagan, in his address to the nation on March 23, 1983, called for achievement of "our ultimate goal of eliminating the threat posed by strategic nuclear missiles" (1:50). The effort he launched that evening has become known as the Strategic Defense Initiative (SDI). It is still only a research effort and there is much debate over the merit of strategic defense. The debate has focused on two ends of a spectrum. One end, argued by the engineers and scientists, concerns the technical feasibility and high cost. The other end, argued by the strategist, is the utility for defense, since nuclear deterrence through offensive capability has been the basis for keeping peace in the atomic age for over 40 years. An equally important issue that relates to both is the strategy anticipated to control the system. It can not be ignored or assumed away and must be resolved even before the system is fully defined. While it is true that technology influences strategy, command and control strategy should drive the technology and system architecture rather than visa versa.

SYSTEM DESCRIPTION

The basis of the Strategic Defense Initiative is a tiered defense against ballistic missiles. It is best described by the Director of the Strategic Defense Initiative Organization, Lt Gen James A. Abrahamson, in his presentation to the Virginia Military Institute in April 1986:

> SDI research is focusing on defenses against ballistic missiles of all ranges, including intermediate-range (IRBM), intercontinental (ICBM), and submarine-launched ballistic missiles (SLBM). Our emerging technologies have the promise of overcoming previous obstacles, thereby making possible a layered defense at each stage of a ballistic missile's flight: the boost (or launch) phase when the first- and second-stage rocket motors are burning and an intense infrared signature is created; the post-boost phase when the multiple warheads and penetration aids are deployed; the midcourse phase when the warheads and penetration aids travel on ballistic trajectories above the earth's atmosphere; and the terminal phase when the warheads and penetration aids reenter the atmosphere. Each phase offers different opportunities for a defense system; each poses different challenges. A highly effective counter to a massive missile attack on the US

will require multiple tiers of defense, each designed to significantly reduce the number of incoming warheads until their number is actually too small to be of any military utility (2:50).

The phases of ballistic flight are shown in Figure 1 along with the associated timing of each phase. It is clear that attacking each phase of an incoming missile is important for the overall success of the system, but the first phase attack--the boost phase attack--is the most vulnerable. This phase provides the most effective defense opportunity because the target is larger, still has all multiple warheads attached, is slower, is easier to track with bright rocket motor flames, and is full of volatile fuel. The space shuttle Challenger disaster is an example of what can happen to a rocket in boost phase. Technical advances offer new opportunities to attack missiles in this phase. As Gen Abrahamson said: "A decade ago there were no means available or even envisioned that were capable of intercepting a missile during the boost phase" (2:50). Advances in weapon technology to attack a missile in boost phase bring the problem of attack timing to the forefront.

Each phase of a ballistic missile's flight takes a different amount of time as shown in Figure 1. The first or boost phase is very short and therein lies the problem. One of the longest burning ballistic missiles is the Russian SS 18 ICBM. The SS 18 missile spends about 300 seconds accelerating and another 300 seconds deploying it's 10 reentry vehicles (8:13). The five minute boost phase is not very long to accomplish the necessary actions required to destroy the missile. A faster burning booster has been discussed as a counter to SDI. A moderately fast burning booster, critics propose, could have a burn time of 100 seconds (8:13). However, a degrade in accuracy would result. Technology advances in weapon reaction time together with computer and signal processing speed and efficiency make it plausible that the hardware and software can be developed to react to this 1.66 minute boost phase but the human reaction time and decision-making process may be the limiting factor.

The command and control system for SDI will have to cope with these timing considerations. Today, many command and control functions must take place in a relatively short period of time. If not, the capability to respond to an attack with nuclear weapons may be seriously degraded. Existing nuclear weapon execution requirements very stringently mandate Presidential authority for release to ensure control of the US nuclear arsenal rests with our elected officials--the President or his successor. A very extensive command, control and communications (C3) system is designed to ensure that type of control exists in case of nuclear war. The strategic C3 system used today to respond to a ballistic missile attack is undergoing a massive modernization to meet the evolving threat and maintain

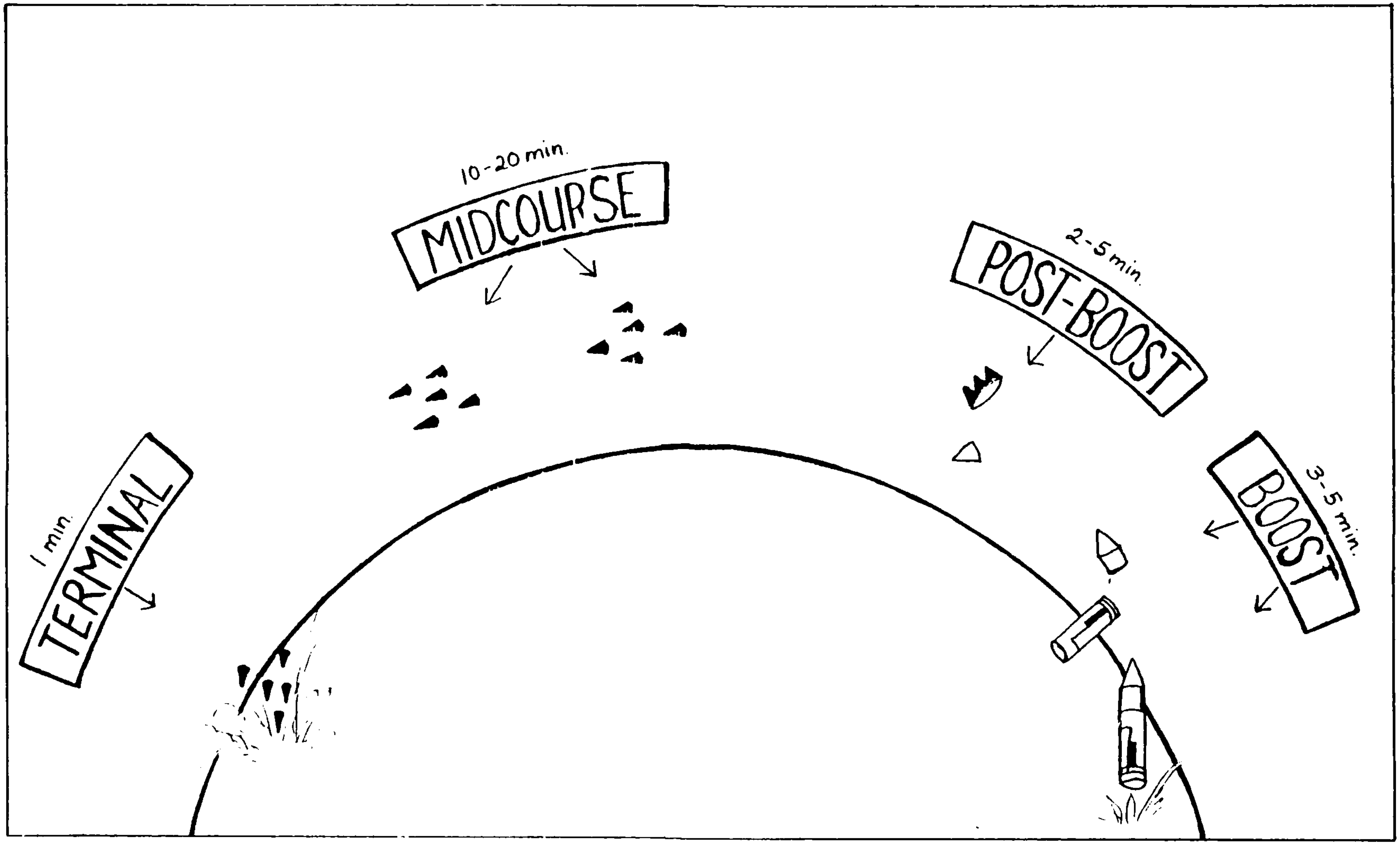


FIGURE 1. Ballistic Missile Flight Phases (9:31)

deterrence. This modernization effort is designed to cope with very demanding time constraints to detect an attack, assess that attack, decide how to respond and ensure that the chosen response is carried out prior to destruction by the incoming missiles.

Figure 2 shows the strategic C3 cycle designed to respond to a nuclear attack. The first portion of this system is attack detection. This includes both strategic warning; e.g., the indicators that provide pre-launch warning as far in advance as possible and tactical warning; e.g., the satellite and radar sensors. Besides these indicators and sensors, the processors and communication systems used to sort out and present the data are essential to ensure timely, clear, reliable and unambiguous warning.

This warning information is assessed as to its origin, composition and general objectives then presented for decision-making actions. Forces and control assets must be postured for survival and decisions on employment options must be made by the National Command Authorities (NCA) in conference with the military commanders in chief (CINCs) and Chairman of the Joint Chiefs of Staff.

After the decision process, many redundant means of communications, each with differing forms of survivability, are employed to convey the Presidential attack orders to the forces. Each leg of our strategic Triad (land based intercontinental ballistic missiles, submarine launched ballistic missiles, and manned bombers) has individual peculiarities that are considered to ensure connectivity in the event of nuclear war. All of these systems, starting with the warning to eventual execution of nuclear weapons, comprise the strategic C3 capability we depend on to deter war. One critical aspect of this entire system is its capability to function under the time lines imposed by enemy ballistic missile flight time.

Figure 1 shows the typical intercontinental ballistic missile flight time. The total time varies depending on the distance from launch origin to target. Coastal bomber bases or Washington D.C. may have as little as 10 minutes between launch from Russian submarines off the Atlantic Coast till weapon impact due to the short flight time (6:51). The more accurate, Russian land based ballistic missiles could arrive within 30 minutes. The strategic C3 system is designed to react within those time constraints and ensure the retaliatory capability to inflict damage unacceptable by any standards. This is the classic form of deterrence in today's offensive posture. However, deterrence through SDI requires different reaction times.

It is not reasonable to expect an SDI system (even with perfect/instantaneous C3, if that was possible) will allow the President to get enough information and make a rational decision

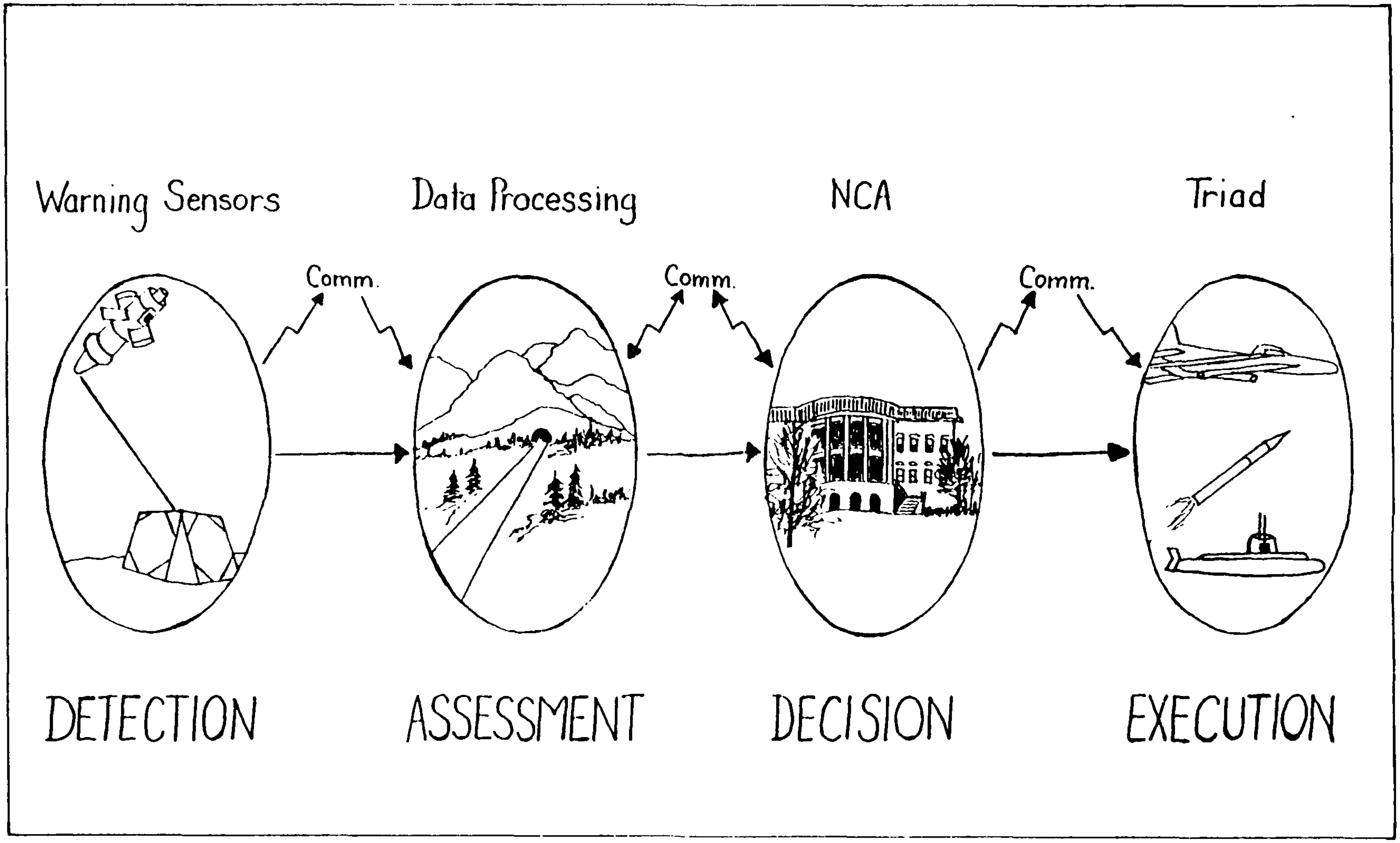


FIGURE 2. Strategic C3 Cycle

about system employment in a little more than the minute and a half boost phase of a fast burning enemy ICBM. This is especially true if the enemy used one of the basic principals of war--surprise--or acted in accordance with the wisdom of Sun Tzu who said: "All warfare is based on deception" (4:79). It can be debated that surprise is not possible in today's era of vast and marvelous intelligence indicators, but wasn't that assumed prior to the Pearl Harbor raid? It is naive to depend on intelligence alone and not plan or prepare for surprise attack, no matter how remote the possibility may be. Napoleon, in his Maxims of War stated: "To be defeated is pardonable; to be surprised--never!" (4:317). If surprise is the only way to defeat a system, then an enemy will surely develop a capability to exploit that weakness. Capability to react to surprise with effective responses deters the enemy from surprise tactics. Therefore, SDI success requires the capability to react to surprise. It also must attack missiles in all flight phases to be truly effective (2:50). The first phase is so short in duration that it is not feasible for a Presidential response to be given in time. The question then becomes what other command and control concept is the most feasible.

COMMAND AND CONTROL CONSIDERATIONS

As with any defensive or offensive weapon system, there are safety considerations to ensure against inadvertent or wrongful system activation. These safety precautions, referred to as positive control, must be considered when designing the command and control system. The human element becomes important to these considerations and provides advantages and disadvantages when compared with unmanned autonomous system concepts.

The amount of positive control built into the system can vary from the extreme, used with nuclear weapons, to the limited amount over soldiers guarding a boundary line with rifles. In one case, Presidential authority, numerous codes, two man policies, and human reliability measures protect the system. In the other case, only the judgement of a single young soldier determines when the defenses become active. Positive control of SDI must fall between these two extremes--not as sensitive as unleashing weapons of mass destruction, yet not as simple as shooting a rifle whenever the enemy crosses a line. A sensitive or strong positive control over SDI, with layers of checks and balances against unauthorized or accidental use, can limit it's ability to perform it's mission in a timely fashion. On the other hand, a "hair trigger SDI" could invite a disaster. A key determinant in the amount of positive control required for SDI is the ramifications of false alarm or improper activation.

Regardless of the design of the SDI sensors and algorithms used to pick out threats and ensure the validity of those threats, basic positive control measures will allow only targets with specific signatures, which identify it as a threat, to be attacked. With this limited target base, only events that so closely resemble a threatening missile attack could "fool" the system and invite false alarm. The signature definitions must not be so stringent that the enemy could attack with a new or non-standard event to deceive and cause SDI not to react.

The ramification of shooting a false target could be severe, such as destroying a Russian manned space launch in peace time, but not nearly so severe as initiating a nuclear war. When the Russians shot down an airliner full of civilians in September of 1983 (KAL 007), it created a very serious situation, but not a war. The false alerts from the U.S. missile attack warning system, back in 1980, caused a serious uproar over the credibility and danger of our warning system. Although the false alerts were quickly noted and corrected before any serious actions were taken, the uproar was over the envisioned ramifications of reacting to false information with nuclear retaliatory forces--a much more serious crisis than reacting with defensive weapons (5:65). The false defensive action of destroying a peaceful (possibly manned) rocket, by mistake, over sovereign territory, has more serious overtones than the soldier's rifle going off, by mistake, in a tense border control situation. The safety on the rifle trigger and the SDI sensor algorithms are relatively simple forms of positive control but they are hardware controls not human controls. The ramifications of mistakes in these two examples may dictate human control/responsibility at the level of the young soldier in one case and at the Presidential level in the other case. The proper level of human control over SDI will be discussed later but first, the issue of human versus machine control merits discussion.

MANNED VERSUS UNMANNED CONTROL

There are pros and cons to both manned and unmanned command and control concepts. Much study has been done on this subject for other reasons such as man in space, remotely piloted vehicles (RPVs), robotics and artificial intelligence. Usually, the solutions recommend man in the loop except in cases where the environment or life support requirements severely impact the mission (such as high threat military missions like tactical reconnaissance where RPVs are used). Positive control considerations for SDI, discussed above, may require man in the loop. This does not have to be in the traditional sense of maintaining total control, but only to satisfy specific positive control demands.

SDI requirements for sensors and processors to fuse information and implement reactive actions are so constrained by the timing considerations that adding man in the loop may not be possible. Human decision-making demands that fused information be displayed or presented in a format for comprehension. Unmanned command and control systems can be faster since the information used for decisions does not have to go through a display and human comprehension process before being acted on. Unmanned autonomous systems can be designed for speed and efficiency. Onboard satellite processing can reduce transmission delays and take advantage of advanced technology such as parallel processing techniques whereby the numerous battle management tasks can be performed simultaneously. Since decisions can be programmed into algorithms developed to cope with anticipated indications, the human decision-making can be done over time with the input of many experts and approved at any level desired. In other words, the President, his staff, or even the Congress can decide how to respond to various threats using SDI. This is programed into the system to then allow autonomous operation. The human frailties (such as fatigue, emotion, personality, etc.) associated with limited reaction time decisions won't interfere with successful time sensitive command and control. However, are the human decision-making qualities necessary for SDI?

History has proven the need for human control over situations that could have led to disaster without intervention. Dr. Stephen Cimbala points out an example in discussing crises:

> Throughout U.S. history but particularly during the post-World War II era, U.S. Presidents have had to exert strong personal control over crises to prevent standard operating procedures and organizational routines from propelling events beyond policy control. The Cuban missile crisis is one example. President Kennedy had to order the Navy to move its original blockade line closer to Cuba in order to provide decision time to Soviet leaders. Instructions about the interception of surface ships that approached the blockade line were important to the President and to Secretary of Defense Robert S. McNamara, who argued about the procedures with the Chief of Naval Operations. Political leaders failed to exercise equally strict control over the U.S. Navy anti-submarine warfare (ASW) exercises, known as hunter-killer routines. Six Soviet submarines were forced to surface during the crisis before the President ordered the ASW efforts restricted (7:24).

The Cuban missile crisis measured in days can be very different than SDI scenarios measured in seconds. A crisis requiring intense negotiation between sides needs human decision-making, but time does not permit such actions in other situations. Flexibility is a key attribute to a command and control system allowing ultimate control to shift according to the situation.

I define the command and control needed for SDI operation as either strategic or tactical. Strategic command and control decides what constitutes a threat or if lethal actions should be taken in a given situation. Tactical command and control determines the optimum detailed system functions such as tracking, identification, discrimination, intercept, negation, and kill assessment. Most, if not all, strategic decisions about an SDI system can be made in advance and the immediate tactical command and control can be automatic. The requirements for strategic command and control and human decision-making can be reduced by having specific rules of engagement detailed for SDI. If the human decision will follow the rules of engagement like a "cookbook recipe" or checklist, then a machine can follow it instead--quicker and more efficiently.

Upon activation, friend and foe could be notified of SDI capabilities and the rules of engagement. This leaves human decisions required only if something malfunctions or if a situation unfolds requiring different rules of engagement or a shift in control to higher authority. Man is better suited to deal with the unexpected situations, yet advances in computers associated with artificial intelligence and expert systems can lead to new roles for autonomous systems. The only requirements demanding man in the loop are to maintain positive control and to ensure proper system operation. These requirements can be interpreted as being major and very significant, or minor. It depends on the trust in system integrity and likelihood of unexpected situations. The significance placed on these requirements determines the degree of human command and control and it's hierarchy.

CENTRALIZED VERSUS DECENTRALIZED COMMAND AND CONTROL

The question of where the ultimate command and control of SDI should reside is a tough one. The most highly centralized C2 concept would have the President control the "button" while the most decentralized concept would have the system autonomous with only maintenance technicians on duty to monitor. Time will not always allow for the President to control SDI and the system is too lethal to operate so decentralized that no man is in the loop. Somewhere between these extremes lies the proper concept for SDI.

Centralized structures provide the highest level of positive control. Highly centralized (Presidential) command and control is required for nuclear release due to positive control and the nature of the orders. Specific top authority guidance is needed concerning which offensive response to use (such as retaliation against military targets or cities or additional countries). Once that top level guidance is given, the more detailed decisions, such as which weapons to use for which target, can follow pre-planned procedures (7:51). However, this offensive decision-making must be closely tied to defensive actions, once that capability is fielded. Offensive response options should be optimized by indications from surveillance sensors to know which friendly weapons are under attack and which enemy targets are empty holes. There is an economy and an offensive mission effectiveness imperative that must be gained from linking SDI C3 to the existing centralized strategic C3 architecture. Linking SDI to the existing C3 structure does not mean they must share the same control procedures. The SDI actions can take place within the limited time constraints while under a more decentralized control, yet still report actions taken through existing C3 channels. This will enhance offensive responses and maximize the offense-defense synergism.

Decentralized control offers more survivability since control is distributed to other locations and not confined to a central node or to single point failure. Proliferated and dispersed control centers can share duties in normal operation and hand-off control if portions go down under attack. Geographic or mission segmentation of control allows for parallel operations, decreased data transmission, and decreased processing loads at a central location. This means faster performance. Of course, there are hybrids of all these control concepts.

SOLUTION

Developing a right solution on how to command and control SDI requires taking the best attributes of the various alternatives and combining to form a concept which makes the most operational sense. Military operational sense should come as the first concern rather than political or technical concerns. Some solutions follow today's way of doing business while others call for completely new and different concepts. SDI may cost less money by relying on existing national command and control systems in it's architecture, and that may placate those cautious of radical new procedures. New technology under research may suggest different methods of command and control. The best solution has both old and new concepts blended to match the national strategy for SDI.

First of all, man must be involved in the command and control process. This is required for safety (positive control) and to deal with unexpected situations. In contrast, quicker and more efficient autonomous operation is also required to meet the threat timing. This indicates a compromise that gives man veto power to deactivate the system for safety or malfunctions but if left alone, SDI takes automatic lethal action to defend against attack. This action must be under detailed and unambiguous rules of engagement. These rules are the key aspect of the C2 system and must be very precise, yet not so rigid that deception could defeat the system. By operating under automatic control, SDI deters surprise. The veto switch maintains positive control. If control nodes are attacked, the system remains in an automatic mode deterring a decapitation attack. This form of command and control should be the normal day to day concept. Flexibility to adjust the command and control with changing conditions is also needed.

Capability to shift control must be available to meet different scenarios. If a crisis builds and alert readiness conditions change, stricter positive control measures may be required. Higher authority "hands-on" control options must be available. The building crisis scenario has less chance of the surprise that requires decentralized automatic control and has more call for human logic to negotiate an end to the crisis without use of weapons. This shift away from automatic control to direct human control could be linked to the procedures taken when higher states of readiness are sought. Flexibility is needed to shift back to decentralized automatic control if the higher authority human control nodes are confirmed lost to attack.

In normal operations, the human control element should reside at a level that can guarantee technical expertise and functional responsibility over the entire SDI. The controllers must devote full effort to the SDI system and maintain proper technical knowledge to recognize and anticipate problems. Positive control measures should require two man authorization, much like our control of nuclear weapons. This is because possession of the critical veto power to stop the system is so important that no one person should be given power to act alone when controlling SDI. The Personal Reliability Program is also applicable to personnel controlling SDI. This program monitors the physical and mental health of people holding critical responsibilities.

The human control element must have a full understanding of the military offensive and defensive employment strategy and capability that was used to program the SDI system. Knowledge of world events which comprise the strategic situation and the real time tactical situation are critical to the control element. This implies access to national level intelligence and direct control resting with a military officer of flag rank. Automatic reporting should follow existing command, control and communications systems and procedures to the National Command Authorities (NCA). This is the greatest departure from traditional strategic C2 concepts. The NCA must be content with a concept that reports actions taken rather than asks or makes recommendations on what to do. While this concept of decentralized control is unlike nuclear control procedures, it has congruence with other conventional weapon control procedures. Ship captains at sea are given authority to defend their ships from attack and air defense pilots scrambled to protect sovereign air space are armed with lethal weapons and authority to fire under their rules of engagement.

SDI should not be controlled like a nuclear weapon system, yet should have sound positive controls. Its importance and worldwide range should not cause the top level control architecture to be cumbersome and less effective. The proper architecture should be very simple and streamlined. No one should be fooled into thinking SDI command and control can go through many layers of decision-making and still react in time nor should they think there can be no man in the loop.

BIBLIOGRAPHY

A. REFERENCES CITED

Books

1. Brezezinski, Zbigniew K. and Richard Sincere, Marin Strmecki, and Peter Wehner (eds.). Promise or Peril, The Strategic Defense Initiative. Washington, D.C.: Ethics and Public Policy Center, 1986.

2. Guerrier, Steven W. and Wayne C. Thompson (eds.). Perspectives on Strategic Defense. Boulder, CO: Westview Press, 1987.

3. Guertner, Gary L. and Donald M. Snow. The Last Frontier. Lexington, MA: D.C. Heath and Company, 1986.

4. Heinl, Robert D.,Jr, Col, USMC (Ret). Dictionary of Military and Naval Quotations. Annapolis, MD: U.S. Naval Institute, 1966.

Articles and Periodicals

5. Cammarota, Richard S., Lt Col,USAF. "Defensive Watch." Air Force Magazine, (February 1985), pp. 63-67.

6. Cimbala, Stephen J. "U.S. Strategic C3I." National Defense, (April 1985), pp. 50-54.

7. Cimbala, Stephen J. "Is A Soviet Bolt From The Blue Impossible?" Air University Review, (May/June 1985), pp. 23-27.

8. Lerner, Eric J. "Old Problems Nag New SDI." Aerospace America, Vol. 25 (August 1987), pp. 12-14.

9. Offutt, James, Cmdr, USN and Dr J. Bryan Danese. "Communications for SDI." Signal, Vol. 39, No. 11 (July 1985), p. 31.

B. RELATED SOURCES

Books

Dallmeyer, Dorinda G. and Daniel S. Papp (eds.). The Strategic Defense Initiative New Perspectives on Deterrence. Boulder, CO: Westview Press, 1986.

Articles and Periodicals

No Author. "National Security: Why C3I is the Pentagon's Top Priority." Government Executive, (January 1982), pp. 14-20.

CONTINUED

Herres, Robert T., Gen, USAF. "C3I Strategic Aerospace Defense: The Challenges." <u>Defense Science and Electronics</u>, Vol. 4, No. 6 (June 1985), pp. 42-50.

Latham, Donald C. "Deterring Nuclear War, Supporting National Policy." <u>Defense Science and Electronics</u>, Vol. 4, No. 6 (June 1985), pp. 71-78.

Merritt, Jack, Lt Gen, USA. "Strategic C3I: An Overview." <u>Defense Science and Electronics</u>, Vol. 4, No. 6 (June 1985), pp. 52-60.

Sagan, Scott D. "Nuclear Alerts and Crisis Management." <u>International Security</u>. (Spring 1985), pp. 79-139.

Sloss, Leon and Marc Dean Millot. "U.S. Nuclear Strategy in Evolution." <u>Strategic Review</u>, Vol. XII, No 1 (Winter 1984), pp. 19-28.

END
DATE
FILMED
6-1988
DTIC