ADB971302

Weapon Systems and Information War

OFFICE OF THE SECRETARY OF DEFENSE WASHINGTON DC

01 JUL 1976

UNCLASSIFIED / LIMITED

UNANNOUNCED

AD-B971 302

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1 Jul 76	FINAL: JULY 1976

4. TITLE AND SUBTITLE
WEAPON SYSTEMS & INFORMATION WAR

5. FUNDING NUMBERS
NONE

6. AUTHOR(S)
T. Rona

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The Boeing Aerospace Company
P O Box 3999
Seattle, WA 98124

8. PERFORMING ORGANIZATION REPORT NUMBER
NONE

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Net Assessment
Office of Secretary of Defense
The Pentagon, Room 3A930
Washington, DC 20301-2950

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
84-0778

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
E. Distribution authorized to DOD Components only, DIRECT MILITARY SUPPORT, 29 JUL 91. Other requests shall be addressed to OSD/Net Assessment.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
Explores impact of information-related countermeasures on weapon systems.

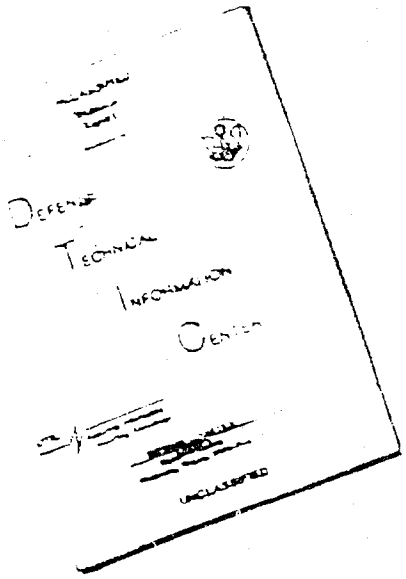
14. SUBJECT TERMS
Information-Related Countermeasures Weapon Systems

15. NUMBER OF PAGES
71

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

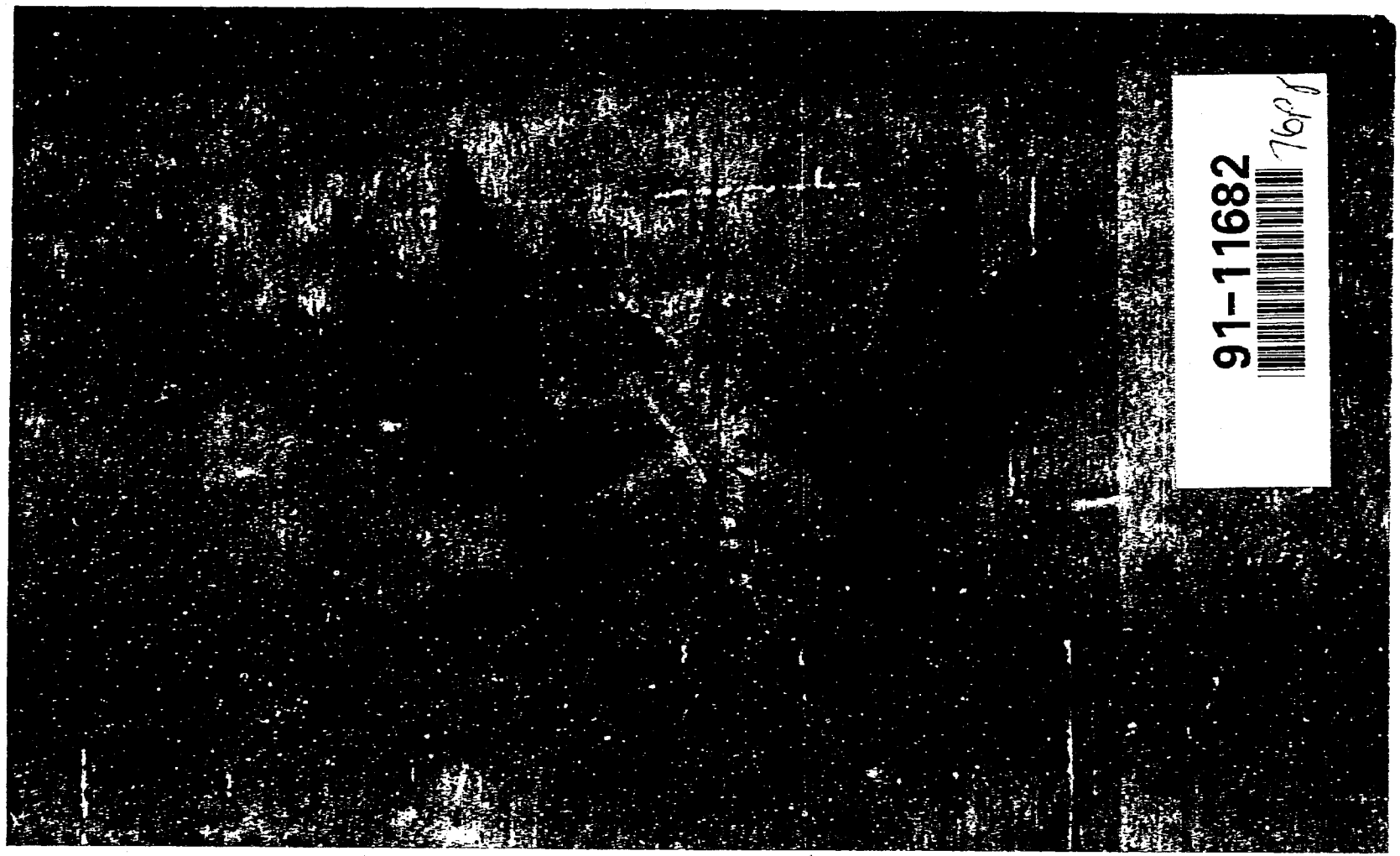
DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

Boeing Aerospace Company
Seattle, Washington 98124
July 1976

Weapon Systems and Information War



Weapon Systems and Information War

Boeing Aerospace Company
Seattle, Washington 98124

July 1976

Thomas P. Rona

CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

FOREWORD

This paper is a summary of thoughts and discussions which have taken place over the past few years as part of National Requirements studies within the Boeing Aerospace Company. While it is impossible to identify the individual contributions, the many helpful comments by my associates at Boeing and other organizations are hereby gratefully acknowledged.

The subject matter is concerned with warfare, weapons, and men. For traditional reasons, the masculine gender is used throughout to designate friend or foe alike. The reader may, however, rest assured that sexist stereotyping or aspersions are neither intended nor implied.

Thomas P. Rona

WEAPON SYSTEMS AND INFORMATION WAR

ABSTRACT

Since World War II, advances in technology have brought great increases in the complexity of weapon systems. The need to integrate the many sophisticated subsystems has vastly increased the information flow *within* the weapon system envelope. Overall performance also has come to depend rather critically upon the *external* information flow between the weapon system proper, the target, the command structure, navigation references, and other ancillaries. Because of their susceptibility to countermeasures, these external links and nodes have become major elements of system vulnerability.

Projections related to the information sciences and the associated technology suggest that countermeasures aimed at the external information flow of weapon systems will be further improved to the point that they may well become crucial in influencing the outcome of future engagements.

Functional analysis shows that the information flow to and from a generalized weapon system covers an unusually broad spectrum, ranging from the slowly evolving strategic intelligence all the way to optical communications. Operational information flow, as well as the gathering of intelligence, is susceptible to countermeasures; i.e., disruption and manipulation. The success of countermeasures, as well as that of attacks and counterattacks, hinges essentially on the knowledge of the opponents' order of battle and of the details of the opponents' information structure. Quantitative assessments of the value of countermeasures are possible in a few simple cases.

The potential introduction of advanced and multifaceted countermeasures gives new emphasis to the war-gaming aspects of requirements definition. Considerations of this type may be expected to lead to a modified set of systems requirements such as closing out of strategy options attractive to the enemy, greatly increased number of possible tactical moves for the friendly side, quick-change flexibility, and a systematically structured "information war" superimposed on the weapon engagements.

Specific examples from strategic nuclear warfare and from tactical air combat are used as illustrations of the principles involved.

SUMMARY

In the recent decades, many spectacular advances have taken place in military technology. Some of these have improved the performance of individual subsystems such as propulsion, structures, guidance, or warheads; some others have insured the efficient cooperation between all these increasingly complex subsystems by means of integration within the weapon system envelope.

The result of these changes has now been apparent for some time: whenever a weapon can be aimed at its assigned target, the destruction of the latter is assured with a high degree of probability. In the past, protection of targets was often based on passive means such as hardening or on timely counterattacks. There exists now a growing possibility of protecting targets by means of *information denial*. In this protection mode, the defense side aims at depriving the attacker of the essential information required to structure an effective offense. Camouflage, dispersion, and mobility have been used to this effect for many centuries, but modern technology has added strong new impetus to information denial. All forms of warfare, ranging from the highest level nuclear exchange through large-scale "conventional" war to counterinsurgency and guerrilla activity could be impacted.

In many instances, high-performance weapon systems have come to depend critically on interaction with *external* elements, friendly, neutral, or hostile. The command structure, the surveillance and support ancillaries, navigation references, and the target area observables are representative examples. Central to the concept of this *extended weapon* system is the remoteness of the physical elements. Communication links are thus introduced that require a new level of integration; more importantly, they introduce new opportunities for the enemy to practice modern and quite effective versions of information denial. Disruption and manipulation of the adversary's information flow by means of countermeasures have rapidly become some of the most potent means to secure military advantage.

There are numerous confluent technologies at hand to reinforce the belief that information-related countermeasures will further grow in efficacy and sophistication; many new areas of application can be readily envisioned. The basic technology aspects have to do with the theoretical and practical advances in the use of the full electromagnetic spectrum ranging from ELF* to gamma rays and of the acoustic spectrum from seismic and tidal pressure fluctuations to ultrasounds at thousands of megahertz in frequency. Transducers are available to transform just about any physical phenomenon into electrical signals, with the attendant capability for transmission, processing, and display for use by human operators. Equipment and software for rather sophisticated information processing, at rates compatible with the speed and frequency domains of interest to weapon systems, are now available within cost, power, weight, and reliability constraints required to satisfy the demands of the most advanced forms of countermeasures.

In the simplest form, information-flow-related countermeasures attempt to disrupt the communication and information links of the enemy in the last few moments immediately preceding the detonation of a weapon. Jamming of the command link of a surface-to-air missile is a typical example. It is, however, readily apparent that countermeasures of this type can be applied at many points of a weapon system, covering in fact the whole period of its evolution from development through deployment, mission, and post-mission phases. The spectrum of events pertinent to the information flow, which is the potential target of countermeasures, covers an extremely broad frequency domain: slowly varying strategic intelligence is updated in bursts occurring in a matter of months or years; tactical intelligence, surveillance, or reconnaissance may deal with event durations measured in days or hours; and events related to the terminal engagement can take place in seconds or even microseconds. Countermeasures may address any or all of these frequency domains; they may be concentrated in any one locale, or again dispersed over many elements of the

* See Glossary, page 71

weapon system. In point of fact, they can often be quite successfully applied over protracted time periods without the adversary's specific awareness.

Technology kindred to that being used to disrupt the enemy's information flow can be applied to the protection of our own. The protection of one's information against countermeasures would be properly termed counter-countermeasures, but there is no real conceptual difference between the two types of operation. The generic set of countermeasures can be defined as comprising the *disruption* of the enemy's information flow, the more intelligent *manipulation* of the hostile information flow and, conversely, all activities aimed at protecting our own systems against those of the enemy. The highest level of countermeasures consist of *misimprinting*. This is a carefully designed logical, but misleading, sequence of messages designed to teach the adversary the use of decision logic inappropriate to his objectives. While deliberate disruption is often detectable by the enemy, the more subtle forms of deception, manipulation, and misimprinting are most difficult to detect in practice.

The analysis of the role of countermeasures defined at this level of generality leads to the reexamination of the criteria used to derive weapon system requirements. If, given a set of initial conditions, resources, and available intelligence, two adversaries rationally structure their strategy choices and the corresponding tactical moves, the outcome of the engagement (battle or campaign involving several encounters) is to a large extent governed by the degree of match between the two opposing strategies. How accurately a commander can define his strategy so as to best use the resources available to him depends on the timeliness and accuracy of the *information* available to him in regard to the enemy resources, intent, and order of battle. The moves and countermoves related to the information flow, hereafter called *information war*, are intertwined with, and superimposed on, other military operations. They add, therefore, quite a large number of new significant options in the definition of strategies and tactics. Analytical derivation of weapon system requirements in order to "optimize" the outcome of some engagements becomes even less practical than without the consideration of the information-war aspects.

A modified set of criteria for defining new weapon system requirements can be derived from the insight afforded by the information-war concept. No uniqueness or originality can be claimed for the proposed criteria; most of them have more or less consciously been applied in many past instances. A new degree of emphasis may be the principal gain resulting from the analysis reported in this study.

The proposed requirement criteria must be applied to all the elements of the extended weapon system. Weapon systems addressing high-priority missions should be *multicomplexioned*; i.e., having several different and independent means for accomplishing the task. Strategy options attractive to the enemy should be eliminated by avoiding reliance on critical, high-value, and vulnerable elements within our weapon systems that may offer attractive aim points to his counterattacks or entry points for his countermeasures. For instance, our strategic deterrent forces rely on three essentially different basing modes and several weapon delivery techniques; additional complexions are envisioned with the advent of mobile/deceptive land basing and of long-range cruise missiles. On the other hand, concentration of sea-based strategic offense forces in a relatively small number of submarines and reliance on fixed land sites for transmission of launch commands to submarines are questionable trends in view of the criteria proposed here.

We should, in the concept development phase of new systems, consciously account for the dynamic aspects of the weapon system development process as impacted by the *informed* responses of the prospective enemy. Our exploratory research aimed at growth options and modifications should address the means for denying to the enemy the developmental moves that may effectively negate the value of our projected new capability. For instance, the multiple-shelter/deceptive-deployment mode considered for ICBM's should specifically provide for the possibility of the enemy converting its preemptive threat into payloads using small, terminally guided warheads, possibly cost effective against redundant shelters.

With a multicomplexioned force, the exercise of tactical flexibility on short notice is possible and highly desirable. The commander of the friendly side should be in position to rapidly modify the

nature of his engaged resources and the manner in which his forces are deployed ("order of battle"). Here again, the opportunities offered by manipulating the information flow in the sense of disruption and deception may be of considerable value. If the changes in our engagement posture occur at a faster rate than the enemy's intelligence/reaction cycle, his response will be found to be less than adequate and his chances for success are correspondingly decreased. Air mobility of strategic offense weapons, possibly extended in the longer term future to intercontinental missiles, appears to implement rather dramatically the principle of information denial by means of the "scramble-on-tactical-warning" employment doctrine.

Superimposed on all these requirements is the imperative need to address the information-war-related moves throughout the whole evolution and operational life of newly proposed or upgraded weapon systems.

This set of modified requirement criteria is expected to have corresponding impacts on weapon system development projects. Among those found of particular significance is an increased trend toward dispersal of major weapon system components; such dispersal in addition to survival and protection against countermeasures will favor the introduction of multiple complexions and tactical flexibility elements.

Some of the issues affecting the future of ICBM force can be discussed in the light of conclusions derived from the information war concept. The vulnerability of fixed-base ICBM's to preemptive attack is directly tied to the reliability of signals warning of critical events and also to the degree of certainty in the mind of the enemy that the U.S. is able and resolved to use such warning to launch the threatened ICBM's on targets *then* found to be appropriate to the strategy that is being pursued. More generally, the ICBM engagement scenarios are expected to include in the future, as part of flexible strategic options, an increased number of choices available to the commander on the basis of information developed as the battle events unfold. The related information channels are prime candidates for attempts at disruption and manipulation by the enemy; successful protection against these attempts is expected to remain an essential preoccupation of both superpowers.

The future of strategic undersea warfare has also been examined in the context of enhancing the sea-based nuclear deterrent weapons of the friendly side and that of threatening the sea-based deterrent of the enemy. The essential differences with respect to ICBM's are that submarines operate during protracted peacetime periods in ocean areas not subject to effective U.S. sea supremacy, thus preemptive first-strike threats are conceivable if reasonably reliable identification and localization can be assured. The same capability, when applied to individual submarines, may be used to effect surreptitious and incremental attrition of our deterrent force. In view of the foreseeable conceptual and technical progress in undersea strategic surveillance, we conclude that the submarines will no longer confidently rely on concealment alone but will have to resort to effective countermeasures such as jamming, spoofing, and decoying.

As a further illustration, the future of tactical air combat is discussed. The introduction of sensor-aided target acquisition and of guided missiles has revolutionized air-to-surface, air-to-air, and surface-to-air engagements to the point that whenever an air or ground target can be acquired, its destruction is almost certain in a "clear" environment. Effective countermeasures against the target acquisition and the weapon guidance have become decisive factors in tactical air engagements. The evolutionary trends clearly point to the *dispersion* of all air-strike, ground-defense, air-based defense elements. Air-to-surface attacks will increasingly rely on acquisition by ancillaries and weapon delivery by standoff missiles; in the more distant future, unmanned automatic or remotely piloted aircraft will be used for both target acquisition and weapon delivery. Ground-based defense will also disperse its fixed, transportable, or mobile sensor and weapon sites; netting of defense sites will considerably enhance their target acquisition and CCM performance. For longer range surveillance and for the vectoring of air interceptors, the defense will add airborne surveillance and control centers. In the more distant

future, the airborne surveillance and control nodes will also be dispersed and netted for increased survivability and counter-countermeasure performance.

It is left for future extensions of this study to explore the implications of military space technology for both interference and exploitation modes of the information war. The future of naval surface warfare will also be examined in the light of the conclusions presented here. Counterinsurgency and guerrilla-type warfare have fascinating ramifications that involve all the information war elements we have described; it is also considered as a topic for follow-on efforts in this area.

Our purpose will have been mostly accomplished if the problems of disrupting and manipulating the enemy's strategic and tactical intelligence (as well as protecting our own) over the entire development, deployment, and operational phases of weapon systems attract much increased attention of the defense community.

In conclusion, starting from a purely technical observation—the all pervasive nature of information flow in weapons and combat operations—the conceptual aspects of countermeasures have led us to define the elements of the information war. The possible impact on the outcome of engagements has been assessed on mostly analytical grounds, suggesting a shift in emphasis among system requirement criteria. A few important areas of application have been examined and the specific conclusions have been pointed out.

We hope that the reader will be motivated to raise a few intriguing questions. Is the information war concept recognized within the U.S. Department of Defense as an essential adjunct to mission and system requirement definition? In the affirmative, how are considerations derived from the information was concept reflected in policies, directives, and procurement procedures without destroying the essential merits of our initiatives or countermoves? How does the information war concept relate to arms limitation talks, including the associated inspection or monitoring systems? How does an "open" society, with its emphasis on freedom of information and public scrutiny, protect its interests in a hostile world suffused with long-term moves and countermoves of the information war? In particular, how does civilian propaganda and psychological warfare interface with the problems we have discussed?

As a direct result of this study, we can do no more than hint that these broader questions deserve exploration and that the answers may be of some relevance to our future military posture. The effort reported here should be considered as an initial foray, conducted from a specific viewpoint and subject to many limitations. Follow-on studies are being proposed and pursued in cooperation with the defense community.

INTRODUCTION

Since World War II, the widespread perception of military threats and the increasing availability of sophisticated technology have produced an unprecedented and sustained rate of development of military hardware. While strategic nuclear weapons have received most of the political and public attention, other forms of weaponry, associated with general-purpose forces, have absorbed the bulk of the global resources devoted to military preparedness.

The traditional components of weapon performance such as range, accuracy, and lethality have been improved individually and in combination for most of the projected military missions to the point that direct hits and high-probability target destruction can be assured at low cost in comparison to the target value. Passive protection by means of additional hardening can no longer economically keep pace with the progress in warhead accuracy and lethality; this is true for targets as diverse as ICBM silos, surface ships, aircraft, or tanks. Under such conditions, the survival of the targets depends increasingly on timely counter-attacks (i.e., the destruction of the attacker before it can accomplish its mission) or on target denial (i.e., prevention of the weapon reaching its destination). Mobility and camouflage have been used for the latter purpose since time immemorial.

Advances in modern sensory, communication, and data-handling technologies have given rise to a new form of target denial, which consists of interfering with the opponent's communications and information flow with the objective of degrading or eliminating the essential elements of his weapon accuracy and the timeliness of his attack. This new technique is called *information countermeasures* or, in short, *countermeasures*. Its impact was already quite perceptible in World War II, received further emphasis in the Korean War, and became recently a matter of predominant concern in the wars of Southeast Asia and of the Middle East. Even such powerful devices as the ICBM's had to express interest in, and concern about, countermeasures well before ballistic missile defense reached the state of operational hardware procurement.

From the relatively simple thought of denying to the opponent the information required for the efficient use of his weapons, the progress in the development of countermeasures has been so rapid that it is now possible to exploit the broader concept of information flow as it affects not only the detailed outcome of the terminal engagement but also the strategy choices and the tactical moves leading to that engagement. The idea of degrading the opponent's information flow and, conversely, to protect or improve our own, has gained reasonably widespread acceptance and has resulted in important applications. The need for a systematic examination of the foreseeable consequences of this "information war" has now been felt for some time.

This paper is an attempt in the direction of fulfilling that need. It examines the role of information flow as it affects the outcome of military engagements. Information flow is found to take place *within* and *among* weapons systems of both friendly and opposing sides. It occurs in many instances, at many hierarchical levels, and in widely different time domains. Because of its extreme influence on weapon system performance and on the eventual outcome of engagements, the opponents will exert considerable efforts to interfere with the hostile information flow or to exploit the same for their own purposes.

The paper first outlines a historical perspective on recent weapon system developments, with particular stress on the role of information flow. Technology projections are shown to illustrate the continuing vigorous growth expected in the field of information-related technology. Then, starting from the analysis of generalized military engagements, the specific roles and functional descriptions of information-related countermeasures are derived. Based on the conclusions that the information war superimposed on other combat elements will, in all probability, play a decisive role in future conflicts, its impact on future system requirements and on weapon development programs is assessed. Prior to formulating conclusions, specific examples drawn from strategic nuclear war as well as conventional war-related missions are discussed.

Even though a number of important advances are still expected in the state of the are pertaining to propulsion, flight control, structures, warheads, and other subsystems, the conclusions strongly suggest that conceptual and design improvements related to the information war as defined here may very well overshadow in the 5- to 20-year future perspective the advantages gained from other subsystem technology refinements.

1

1 HISTORICAL PERSPECTIVE

Since World War II, major advances in propulsion, flight control, materials and structures, navigation and guidance, and warhead technologies have significantly altered the character of many important forms of warfare. The changes have been most perceptible at the higher levels of conflict, such as those directly involving the vital interests of major nations. However, as progress is being made in the direction of stable mutual deterrence between the superpowers, increased and sustained attention is given to the applications of modern technology to conventional or "intermediate scale" warfare. The least obvious beneficiary to date has been the low-level guerrilla and counterinsurgency-type conflict in a primitive environment. While hardware technology alone may not offer decisive solutions in this latter case, the U.S. and other nations have supported related research and development with considerable resources; some progress has been observed and more can be expected.

The weapon delivery mechanism and platform combinations used in the recent past and anticipated for the future are shown in Figure 1. Human inventiveness has always vigorously explored all available technology and all conceivable combinations for placing a warhead in a position where it can hurt the enemy. The picture offered by Figure 1 is far from complete; many other combinations have been tried with some measure of success, and some others, not presently conceived, may well come into being. Weapon systems developed in the past and used for decades or even centuries do not disappear from the global inventory; they tend to be transferred to the industrially less developed nations or, in some remarkable cases, give rise to new developments with much improved performance or extended areas of application.

Growth in Subsystem Performance

The advances in technical performance levels can be portrayed in trend curves such as shown in Figures 2 through 5. Figure 2 shows the evolution in terms of cruise speed and payload/range of strategic bombers from the B-17 pro variable-wing supersonic bomber typ 1970's.

Figure 3 shows the improvement in t strategic offense missiles, starting fro to liquid rockets and advanced solid r of thermonuclear warheads has, of co warfare, but the practical availability ranges and hypersonic engagement ve to making the task of strategic missile and unrewarding.

Figure 4 portrays the great advancem gation systems made possible by impr electromagnetic sensors as well as t processing.

Figure 5 shows the much publicized i air-launched missilery. The missiles h car maneuver to the point where aircr of little practical value in a clear electr At the same time, much improved gui head lethality have resulted in signific

These and many other examples tend jections that weapon lethality will con decades ahead. The institutional mom and industry-sponsored developments forth evolutionary improvements that combination, are likely to result in ma New technologies such as high-power r use of tactical nuclear weapons, the pc chemical or biological weapons, the de platforms such as hydrofoil surface shi

* Lethality is defined as $nY^{2/3}$ $(CEP)^{-2}$ whe Y the yield, and CEP the circular error pr

SPECTIVE

ic bombers from the B-17 propeller-driven generation to the e-wing supersonic bomber typified by the B-1 of the late

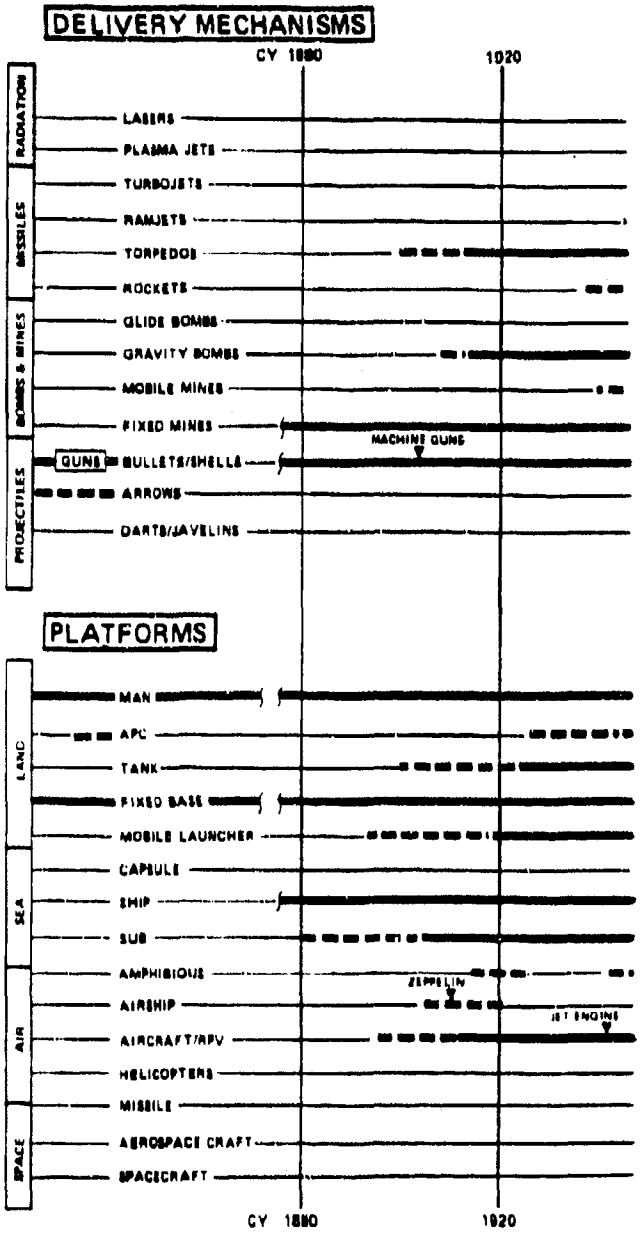
3 shows the improvement in terms of "lethality"* of c offense missiles, starting from World War II vintage V-2's d rockets and advanced solid rocket missiles. The advent nonuclear warheads has, of course, revolutionized strategic , but the practical availability of intercontinental delivery ınd hypersonic engagement velocities has also contributed ng the task of strategic missile defense quite expensive ewarding.

4 portrays the great advancements in guidance and navi- ystems made possible by improvements in inertial and nagnetic sensors as well as the advent of advanced signal ing.

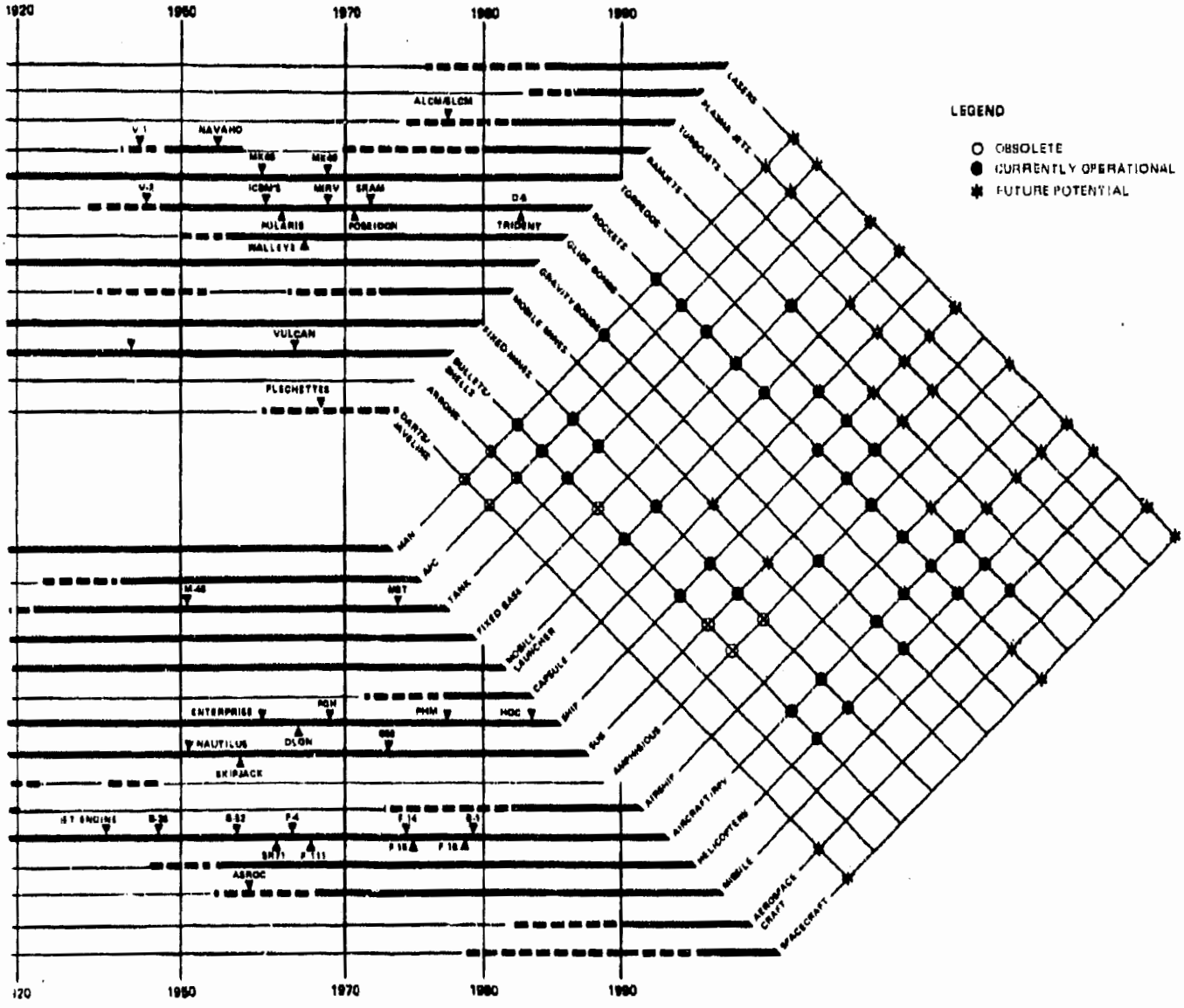
5 shows the much publicized improvements in surface and ched missilery. The missiles have become much smaller and neuver to the point where aircraft speed and turn radius are practical value in a clear electromagnetic environment. ame time, much improved guidance accuracies and war- hality have resulted in significant kill probability.

nd many other examples tend to lend credence to pro- that weapon lethality will continue to increase in the ahead. The institutional momentum of government- ustry-sponsored developments will continue to bring olutionary improvements that, in cumulation and ition, are likely to result in major performance advances. hnologies such as high-power radiation weapons, the uctical nuclear weapons, the possible reintroduction of l or biological weapons, the development of advanced ns such as hydrofoil surface ships, and individual air-

ity is defined as $nY^{2/3}(CEP)^{-2}$ where n is the number of warheads, yield, and CEP the circular error probability.



3


1920
1950
1970
1990
LEGEND
OBSOLETE
CURRENTLY OPERATIONAL
FUTURE POTENTIAL
LASERS
PLASMA JETS
TURBOJETS
RAMJETS
TORPEDOES
ROCKETS
GLIDE BOMBS
GRAVITY BOMBS
MOBILE MISSILES
FIXED MISSILES
BALLISTIC SHELLS
ARROWS
GUIDED MISSILES
FLECHETTES
MAIN
AUC
TANK
FIXED BASE
MOBILE LAUNCHER
CAPSULE
SHIP
SUB
AMPHIBIOUS
AIRSHIP
AIRCRAFT/MPV
HELICOPTERS
MISSILE
AEROSPACE CRAFT
SPACECRAFT
V-1
V-2
NAVAHO
MK-48
ICBM'S
MIRV
SRAM
POLARIS
POSEIDON
TRIDENT
D-5
RALLEYE
ALCM/GLCM
VULCAN
M-48
M-60
ENTERPRISE
NAUTILUS
SKIPJACK
DLGN
SSN
AOH
PHM
HOC
ASROC
JET ENGINE
B-36
B-52
F-4
F-14
F-15
F-16
F-18
SR-71
F-111

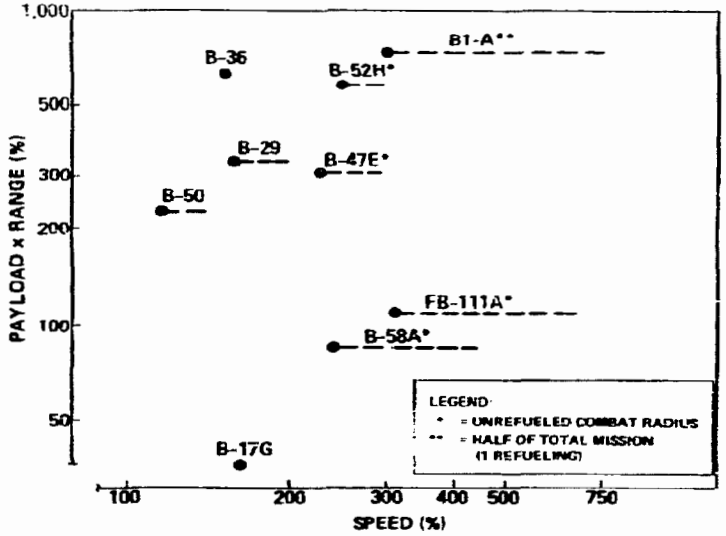


Figure 2. Strategic Bomber Performance

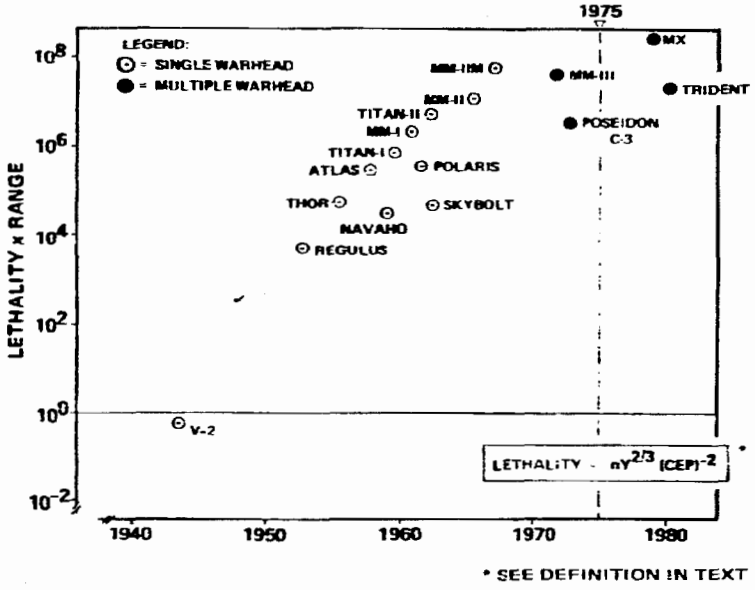


Figure 3. Strategic Offensive Missile Performance

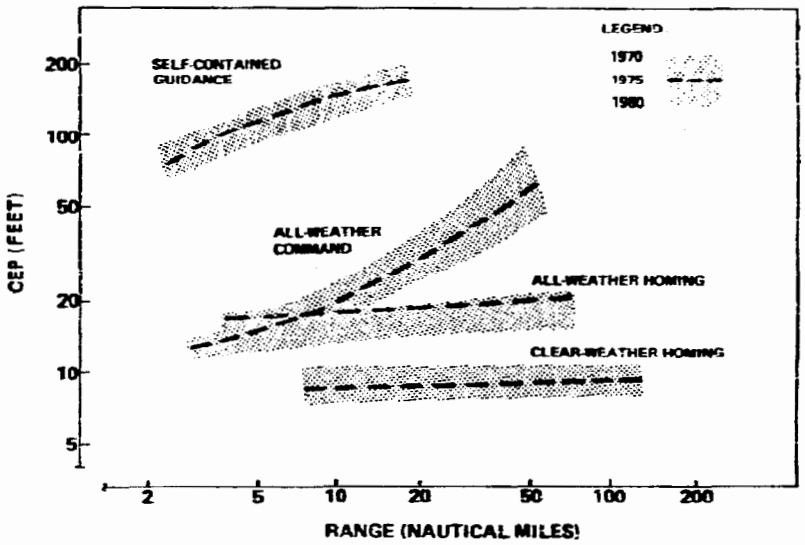


Figure 4. ASM Miss Distance Projections

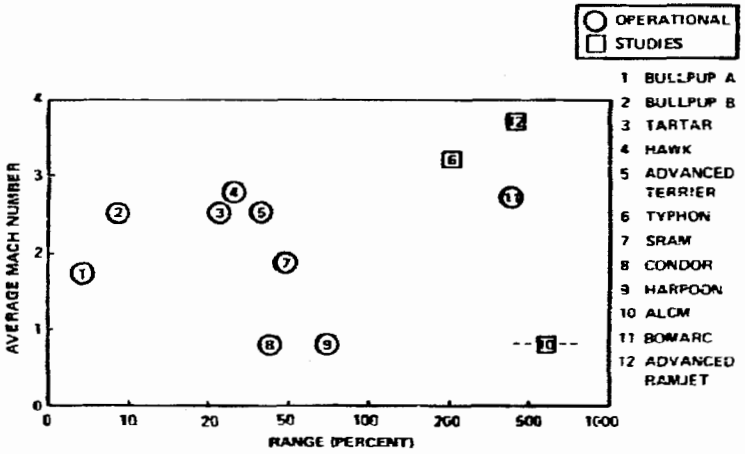


Figure 5. Surface and Air Launched Missile Performance

mobility vehicles for land combat are likely to cause further rapid rates of change far exceeding those experienced over past evolutionary periods.

In view of the much increased lethality of weapons, the efforts of the enemy to protect himself have shifted focus. Instead of physically protecting the target, he must apply his ingenuity to preventing the weapon from reaching the vicinity of the target. It so happens that one of the inseparable features of high weapon performance offers the enemy increased opportunities for doing just that.

Since system integrity is essentially ensured by the flow of *information* between the individual subsystems, the vulnerability of this information flow to enemy action becomes increasingly recognized as being a key factor in overall effectiveness. The nature of this information flow will now be examined.

Internal Information Flow

Figure 6 shows the essentials of a weapon system. All weapons designed to inflict damage remotely on the enemy target comprise at least the warhead, the delivery vehicle that transports the warhead to the target, and the guidance, which translates the instructions of the commander as to the desired path from release to the target. Even in this much simplified representation containing only the weapon-essential functions, the information links between the commander, the guidance, the target, and the delivery vehicle are clearly present.

As the performance requirements have become more ambitious, additional functions have been added (Figure 7). These can be loosely subdivided into mission-essentials (i.e., those that allow the weapon to accomplish efficiently its mission) and flight or transportation essentials (i.e., those that ensure safe and efficient travel). The latter may pertain to the delivery vehicle, but also refer quite often to fixed or mobile launch platforms. The functions of the launch platform are to transport the delivery vehicle to the appropriate launch point, contribute to target acquisition and weapon guidance through direct contact with the target, and serve as a relay between the commander and the delivery vehicle. All these functions are not necessarily present in all weapon systems; on the other hand, new functions soon appear as the complexity and the cost of the platform increases. In particular, self-defense often appears quite rewarding and in some cases even threatens to become the principal function of the platform. Other air-, sea-, or land-mobile platforms are especially designed to serve as relay, processing, and command nodes while the storage, transportation, and launch of weapons take place elsewhere in the system.

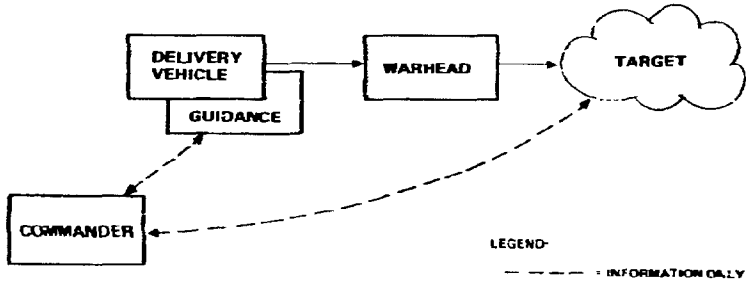


Figure 6. Weapon Essential Subsystems

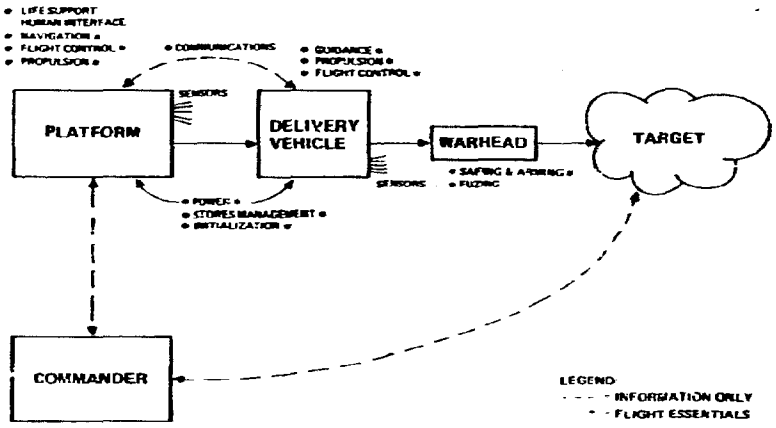


Figure 7. Weapon System Evolution

The understanding of interactions between subsystems is greatly facilitated by the use of functional block diagrams such as shown in Figure 8. Block diagrams of the same kind could be drawn to describe any lower level functional detail within any of the subsystems shown. Connections between individual blocks represent physical interactions, such as forces, fields, position constraints, or the information flow (signals). Information in this context means to convey the state of, or the inputs available to, a given subsystem to others. Information signals are mostly electrical in nature, but optical, acoustic, and fluid phenomena are also being used. The flexibility of modern information-handling techniques allows integration of all the subsystems for accomplishing the weapon system objectives.

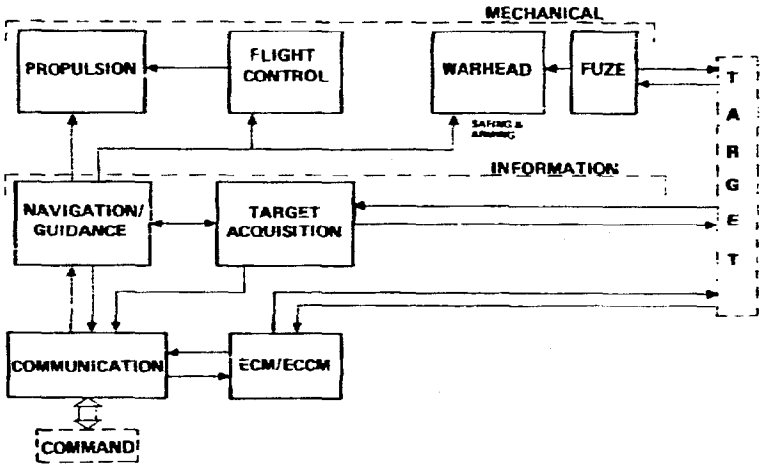


Figure 8. Functional Block Diagram (Weapon)

Those familiar with weapon system integration will point to the many recent technical developments that have occurred in handling the information flow. The following categories are of particular significance:

- Sensing and translation (transduction) of most physical phenomena into electrical signals and often vice versa
- Transmission of electrical signals while satisfying the requirements of linearity, bandwidth, reliability, short time delay, and freedom from extraneous interferences
- Processing, storage, and retrieval capability compatible with the reliability and data rates available within the communication links
- Theoretical understanding and practical implementation of the organization of information flow (software)
- Much reduced power and weight requirements
- Much improved reliability and maintenance characteristics
- Efficient human interface equipment for operations, maintenance, and training

Within the confines of a weapon system then, the many subsystems at various levels of hierarchy are tied together by an *information system* insuring integrated operation. One of the significant aspects of recent weapon developments is the explicit treatment given to the design of information systems under tasks such as "avionics integration." The functional performance of these systems is the prime objective of the designer, who must give due regard to weight, power, reliability, flexibility, and cost. Standardization and modular design as factors promoting maintainability and low cost are of increasing concern. Environmental factors due to natural causes are handled as routine design requirements and so are manmade (nonhostile) environments such as radio frequency and electromagnetic interference.

Hostile environmental factors often impose expensive design constraints, such as hardening against nuclear weapons effects, physical security against intrusion, or protection of communications against jamming, spoofing, or compromise of secret information. The point of interest here is that, even though the information system is complex and to some extent vulnerable to enemy actions, requirements can be defined for the entire integrated system, and overall performance in a given environment can be assessed with some degree of confidence.*

* The statement that requirement definition and system performance assessment *can* be performed should not be misconstrued to mean that they have been, or are being, performed on most of currently implemented systems.

External Information Flow

Up to the present, we have examined the information flow within the weapon system envelope. We must now go one step further. Referring to Figure 9, the weapon system (A), including the platform, is now shown in the center. The relation of the weapon system to other elements contributing to its operation has been made explicit. On the friendly side, the weapon system must interact with its own command structure (C), with the ancillary and support systems (F), and with the friendly, neutral, or natural navigation reference systems (D). Both weapon and platform have to cope with the natural or hostile man-made environment (E). Finally, the weapon must interact with the target (B) prior to the instant of contact.

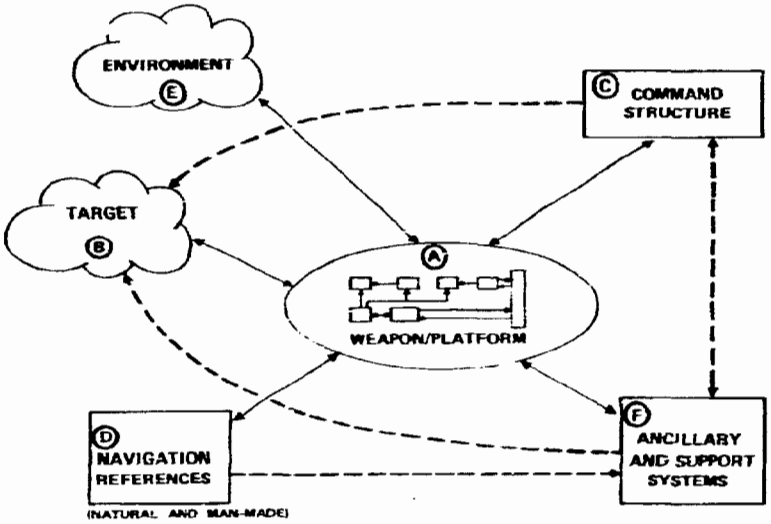


Figure 9. Extended Weapon System and External Information Flow

It is convenient to call all the information-related components within the weapon system (A) the *internal information system* and to consider that all the other elements such as (B), (C), (D), (E), and (F) are tied together by what could be called the *external information system*. All the elements and all the links are, or conceptually could be, present in all weapon systems, even though some of them are less important or evident than some others. Elements other than the weapon system; i.e., boxes (C), (D) and (F), may have *internal* information systems of the same order of complexity and cost as the weapon system (A).

A few examples will allow us to gain more concrete understanding of what these external information links really contribute. The link (A)-(B) between the weapon and the target may convey terminal guidance, or, if properly decoyed, false terminal guidance. If the target is surrounded by active defense, that same link may also serve to convey false observables (decoying) to the defense. Link (A)-(C) between the weapon and the command structure would typically transmit target designation, status report, launch command/confirmation type information. Link (A)-(D) between the weapon and navigation references may sense position of stars, satellites, terrain elements, or artificial land beacons. Link (A)-(F) between the ancillary/support systems and the weapon would typically provide surveillance and reconnaissance information, target identification, warning, intercept control, and vectoring or IFF.

An escort airplane intended to protect a bomber can be considered as an ancillary; all information related to such aerial engagements would flow through link (A)-(F).

The link (A)-(E) between the weapon and the environment allows the weapon to sense its own environment and adapt its surveillance or guidance sensors to the prevailing conditions.

The foregoing is reasonably well understood and may be analyzed within the purview of the weapon system itself. The situation becomes more complicated when we consider links and interactions between the external elements. For instance, a relationship exists between link (D)-(F) and link (B)-(F). The location of the target must be defined with respect to the navigation references. Similarly, link (B)-(C) should be present, either directly or via ancillaries

Ⓒ-Ⓕ-Ⓑ. If the latter is too slow, the commander may want to have direct access to the target. This would be the case, for instance, when the Command Information Center of a combatant ship directs the air battle between fighter/interceptors and the enemy strike forces.

The link Ⓒ-Ⓕ exists mostly to convey the status, availability, and confirmation-type data in relation to the ancillary and support systems.

As an illustration, in Figure 10 the role of ancillaries in a "smart missile" is represented. The missile is capable of illuminating the target and sensing target observables, provided that a pre-mission intelligence element has supplied *in advance* the criteria for signature classification and that a pre-mission surveillance/reconnaissance element has supplied rough target location.

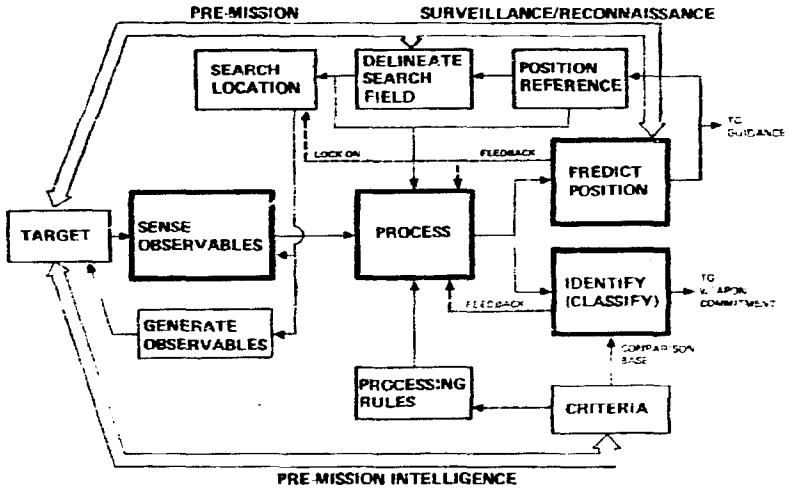


Figure 10. Missile Acquisition and Tracking Functional Relationships – Ancillaries

These examples have been described at some length to support the argument that successful operation of the weapon system is just as critically dependent on the operation of all pertinent elements portrayed in Figure 9 as on the intrinsic capability of the weapon system itself. To put it another way, no matter how complex, competent, or costly the weapon system and its platform might be, if the surrounding external elements fail to perform their tasks, the mission objectives will not be achieved.*

The situation is even more complex owing to the possible interaction of external links with each other. For instance, if guidance or navigation signals are emanating from the weapon system (and this may be highly desirable from the accuracy viewpoint), they may reveal the platform position at the same time and thereby open the way to enemy counterattack.

Complexity is not the only reason why the "extended" weapon system, including all the external elements, is not considered in general as an integrated supersystem. Institutional barriers also exist. The various elements shown in Figure 9 are not necessarily under the cognizance of the same agency; sometimes they involve several sovereign countries. Developments are not necessarily simultaneous; budget considerations quite often cause relatively modern weapon systems to interface with obsolete ancillaries and vice versa. For whatever reasons, integrated system requirements at the extended weapon system level are hardly ever formulated. Examples of this type of difficulty can be found in the areas of "warning on critical events" as related to ICBM launch command, or in the operation of hard-site ABM defense as related to the ICBM launch environment.

The common characteristic of external information systems is that it requires sensing or communications at a distance between physically remote elements. These all involve electromagnetic or acoustic propagation and are, therefore, potentially accessible to hostile interference.

* For instance, in World War II, even though the Germans had what at that time was considered to be a highly competent strategic bomber force, the successful interference with their land-based long-range navigation beams resulted in quite unacceptable targeting errors.

We have thus created a situation in which the gains resulting from the careful and costly integration and protection of the *internal* weapon system are counteracted by the difficulty in the integration of the *extended* weapon system (including all the external elements) and by the new, vulnerable links introduced between these elements remotely located from each other and from the weapon.

The following sections examine in more detail the consequences of these observations, but first we must rapidly survey the pertinent technology horizons.

2 THE FUTURE OF INFORMATION TECHNOLOGY

Background

In the past 30 years, a fundamental new development has taken place within the "Western" civilization as represented by the advanced industrial nations. The core of the novelty is the applied science background and the engineering and manufacturing technology which, taken together, support the systematic handling of large masses of organized information at heretofore unimaginably high data rates.

Whenever, in the history of recorded human civilization, a major technical advance has taken place, the impact on warfare was immediate and far-reaching. The steel sword, the war chariot, the use of gunpowder, the oceangoing ships, the jet aircraft, and the nuclear weapons are examples of such breakthroughs.

Owing to the relatively close time perspective, our assessment of information technology is apt to be quite distorted. One is easily impressed with spectacular achievements such as global video coverage via satellite repeaters, giant and microminiaturized computers, or the fantastically accurate navigation of interplanetary vehicles. Those who are in everyday contact with the state of the art are, however, just as prone to warn about our management failures in keeping system organization and software development capabilities in synchrony with the potential of hardware technology.

The true long-range impact of advanced information technology on our society must be assessed on a far broader basis. Fundamentally, civilization complements our biological evolution by creating tools for beneficial interaction of our bodies with the environment. The invention of printing in the 14th century was the first man-made auxiliary to the *human brain*; i.e., additional mass data storage/retrieval, enabling information to be preserved over many generations and accurately disseminated over intercontinental distances. Its historical impact on religious and political concepts and (not so incidentally) on the advent of the industrial revolution and the concomitant rise of western military power in less than a few hundred years is a matter of record.

Advanced information technology brings two new major auxiliaries to supplement the capabilities of the human brain: *accurate mass data processing* and *rapid broadband communication*. The latter includes long-distance communications between humans but also man-machine communications and high data rate machine-to-machine communications. By historical analogy, a new fundamental impact on society can be confidently predicted. The effects are being currently felt and will quite substantially transform our lives within the next few decades, since by its very nature information technology contributes to the further acceleration of technical innovation in this and other fields and helps in the dissemination of the corresponding research, development, and production disciplines. The impact on warfare is likely to be equally important; we have seen some of the initial consequences in Chapter 1, but far more profound consequences may well occur within our professional lifetimes.

Causes and Effects of Rapid Growth

It is necessary to establish the fundamental causes of the recently observed rapid growth in order to predict with some measure of confidence the continuation of the growth trend.

First, we must observe the remarkable confluence of mutually supportive technical developments in the period immediately following World War II. Just as World War I saw the birth and growth of air transportation and radio transmission, World War II supplied the direct impetus for the development of missilery and radars. Missiles have intensified the demand for sophisticated and miniaturized electronics, while radar has introduced important new high-frequency power generation and modulation devices, as well as the pulse technology that eventually has led to the whole new world of digital signals with its fascinating implications of logical

organization and mass data processing. Not surprisingly, scientists such as Norbert Wiener, Claude Shannon, and John Von Neuman have addressed the developing science of information theory, while applied physicists have at the same time developed fundamental knowledge in quantum and solid state physics. These have rapidly led to semiconductors, microwave devices, and lasers that in turn have helped the development of large-scale integrated microcircuitry and gigahertz-range communications, with optical communications rapidly entering the state of the art.

The second major driving force was a no less remarkable interplay of dynamic military and commercial markets within the U.S. and allied countries. Consumer markets for electronic equipment are measured in billions of dollars per year for entertainment and communications; commercial and industrial applications of computer control and communications equipment are equally significant and growing at a sustained rate. Computers, in particular, have first been used by large research institutions but they very rapidly became the mainstay of business data processing equipment and are currently reaching the individual consumer market. The military, having demonstrated the power of sophisticated weaponry during World War II, had no difficulty in laying claim to ever-increasing electronic R&D budgets and follow-on production contracts. The synergy between military and commercial markets has generated an unusual intensification of institutionalized public and private reaserch in the fashionable fields of electronics, solid state physics, and microwaves, lasers, and many other related areas. Such promising market potential for scientific activity has given rise first to a new generation of highly talented graduate students and then eventually powerful centers of attraction within the universities, Government, and private research establishments. With this kind of long-term intellectual investment, further rapid advances in technology and product applications can be safely predicted.

Specific Projections

In this section, we give an all too rapid overview of a few selected technology examples in terms of past and future trends.

Figure 11 and 12 are related to our capability of observing and storing two-dimensional visual patterns. Figures 13 through 15 portray the recent and expected advances in high-frequency communications with the potential of integrated optical components shown in Figure 16. Digital processing of data is being used for error correction, with substantial improvement promised over the next decade, as shown in Figure 17. Figures 18 and 19 support the viewpoint that large-scale complex data processing at low volume and low cost will be increasingly available and therefore amenable to packaging in just about any military vehicle or missile. Finally, Figure 20 shows a few projected trends in regard to airborne avionics.

None of these examples should be seen as authoritative or exhaustive, but we can safely suggest that they are indicative, in broad qualitative terms, of future trends.

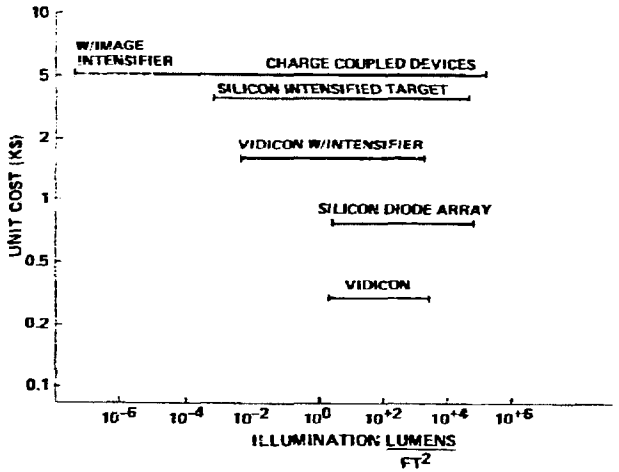


Figure 11. Optical Sensing Devices

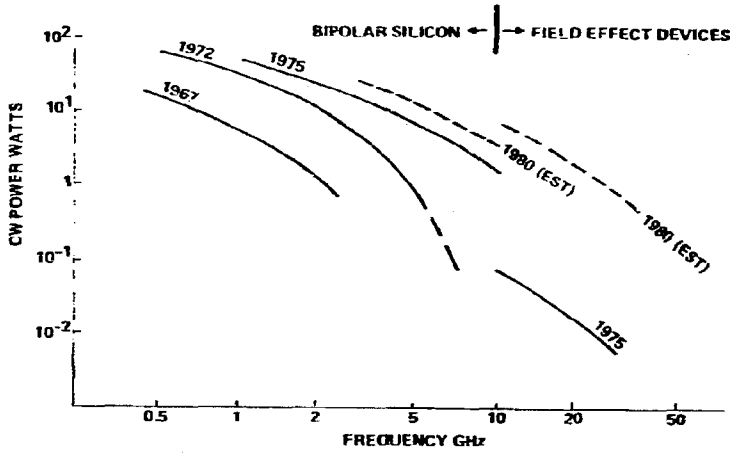


Figure 13. Microwave Power Transistors

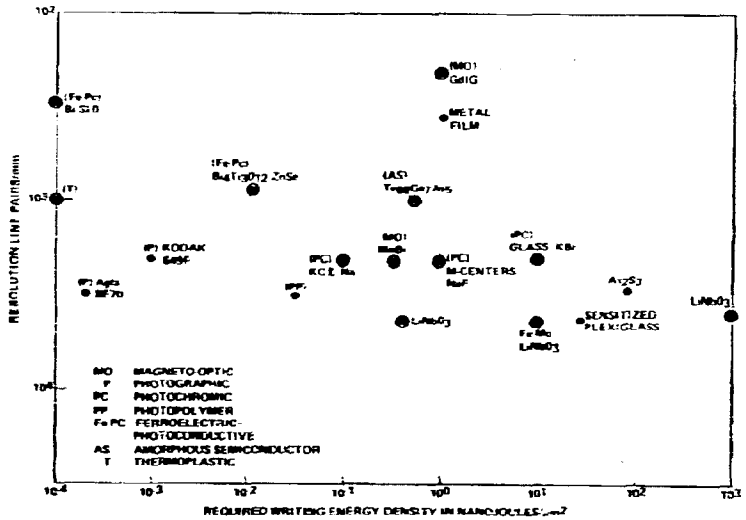


Figure 12. Optical Memory Elements

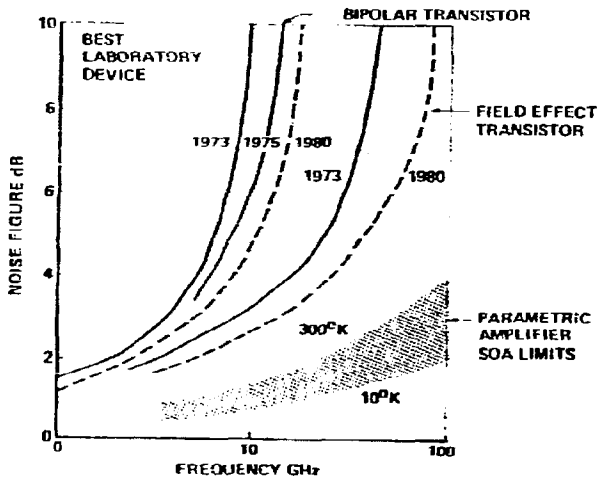


Figure 14. Low-Noise Solid State Device Trends

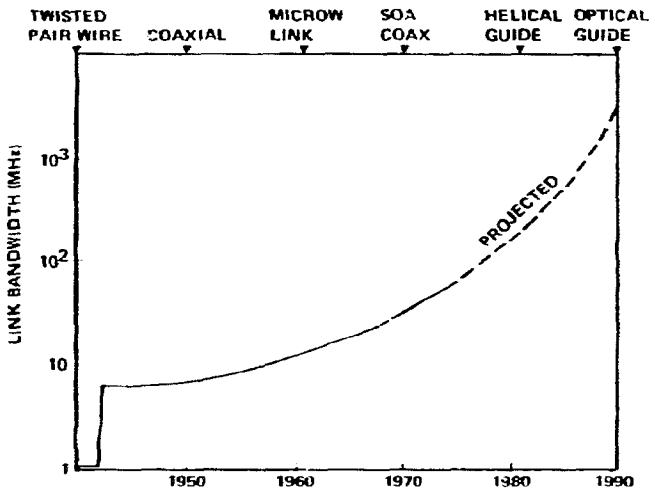


Figure 15. Hard-Line Communications

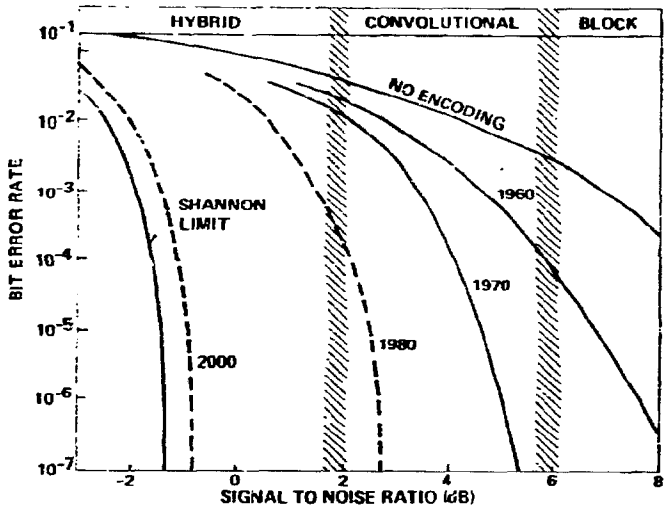


Figure 17. Error Correction by Coding

	Present (1974)	IOCs (1980 +)
Switching (1→N Poles)		
A. Speed	10^{-3} Sec	10^{-9} Sec
B. Number of poles	8	2,024
Switching (N→N Poles)		
A. Speed	10^{-3} Sec	10^{-9} Sec
B. Number of poles	2	20
Carrier-frequency multiplexing		
A. Number of frequencies	5	50
B. Loss	5 dB	0.5 dB
Access couplers		
A. Loss	3 dB	0.5 dB
B. Number of terminals without repeater	10	50
Beamwidth		
A. Short lengths	50 MHz	10 GHz
B. Long lengths	100 MHz/km	10 GHz/km

Source: NERC TR 1931 (1974)

Figure 16. Integrated Optical Components (IOC) Performance Projections

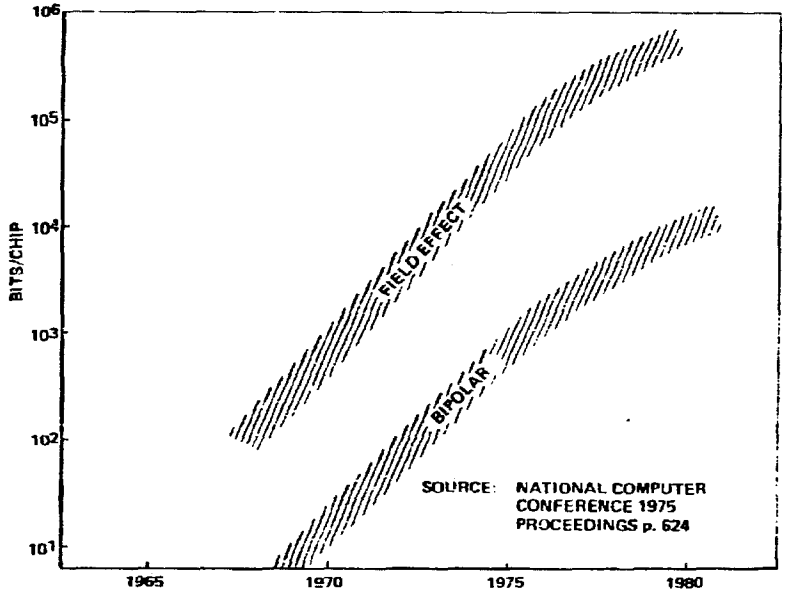


Figure 18. Semiconductor Storage Trends

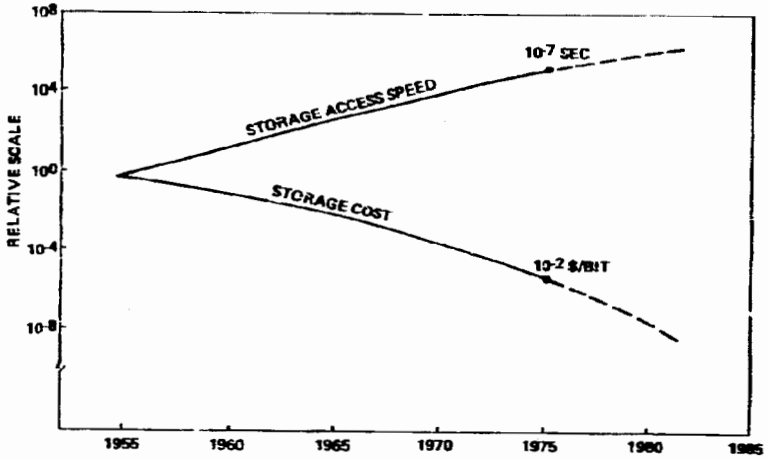


Figure 19. Computer System Trends

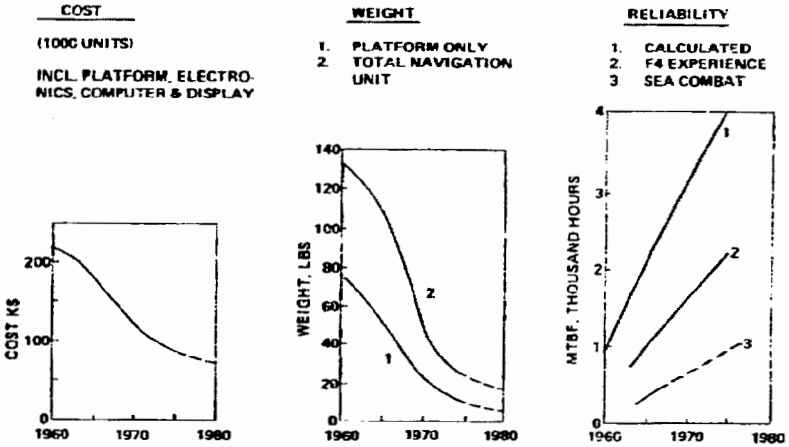


Figure 20. Airborne Avionics Trends

(This page intentionally left blank)

3 ANALYSIS

The purpose of this section is to describe the mechanisms involved in military engagements. The word "engagement" is used in its most general sense to comprise all actions undertaken by all sides present for the purpose of defeating their opponents.

Engagements, as described here, cover conceptually all forms and levels of military conflict, even though some of the functions discussed may be embryonic, trivial, or nonexistent in particular instances. The analysis applies to central strategic wars involving massive nuclear exchanges between superpowers; it also should fit lower level nuclear wars, the socalled "conventional" wars involving land, air, sea, and all types of combined tactical operations as well as undersea warfare and even counterinsurgency or guerrilla-type engagements.

Offense vs. Defense

"Offense" and "defense" are convenient terms to describe the role assumed at a given instant by the opponents, but these terms rapidly lose their meaning as the engagement proceeds. Modern analysts avoid confusion by referring to the two sides as "Blue" and "Red" respectively, with other colors added as the conflict widens. These designations have the merit of being devoid of any connotation of approval or righteousness, but even so, "Yellow" is usually avoided among English-speaking scholars. Be that as it may, the roles of the opposing sides are confusingly symmetrical at various stages of the engagement. The classic statement that the "best defense is to attack" or the uncertainty as to the range at which a ballistic missile interceptor (defense) begins to play the role of a counterforce weapon (clearly an offense mission) bear witness to the difficulty involved in distinctions that are too precise. Except for a Pearl Harbor type abrupt change in the state of hostilities, clearly attributable to one of the participants, even a so-called first-strike type situation may be misleading as to the identity of the offense side.

We are now in position to examine the conceptual aspects of engagements. The "offense" side marshalls its resources to deliver an attack on some target thought to be of value to the "defense". If this value is set high enough, the defense side will in turn attempt to minimize the damage incurred by the specific target, or, if that is not practical, the attempt will at least be focused on preventing recurrence against other targets. Defense has basically three types of mechanisms at its disposal (Figure 21):

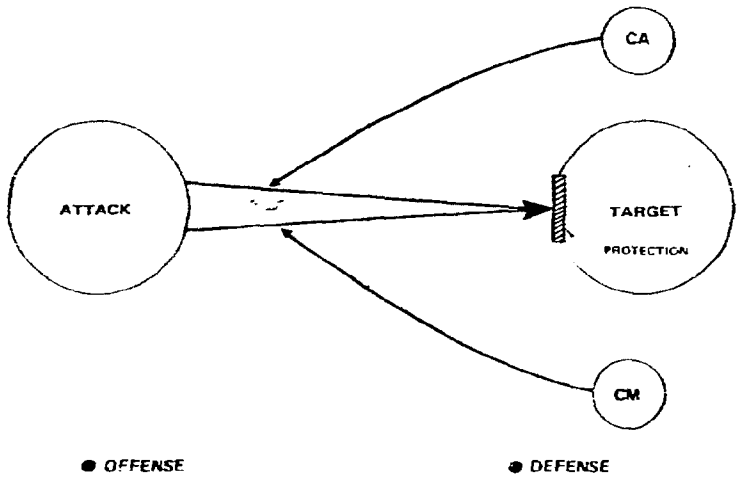


Figure 21. Conceptual Engagement (First Moves)

It can protect the target by passive means such as hardening ; it can attack (with the hope of destruction in time) the offense elements (CA for "counterattack");* or again, it can interfere with the information flow of the attack (CM for "countermeasure"). Interference in this context is to be taken in its most general sense; jamming, spoofing, decoying, and mobility are just a few obvious examples. Instead of discussing the many implementation tech-

* Counterattack may also be aimed at targets unrelated to the military force components directly engaged. In these cases, experts describe the counterattack as strategic retaliation, unhumanitarian terror bombing, daring commando operations, or terrorism, all dependent on the level of hostilities and the allegiance or convictions of the writer.

niques, we focus at this point on two features of the defense countermove:

1. Passive protection must apply in the immediate vicinity of the target and is therefore presumably anticipated by the attacker and accounted for in the structuring of the attack. In contrast, both counterattack and countermeasures may be concentrated or may be dispersed over many elements of the attack. These *active* countermoves do thus offer the essential features of tactical choice, flexibility, and possible surprise.
2. In anticipation of the attack, a rational defender will carefully distribute his resources between passive protection, counterattack, and countermeasures. In order to allow even a gross approximation of such desirable distribution of resources ("order of battle"), the defender will sedulously gather all available strategic intelligence ("What can the attacker do?") and all possible tactical intelligence ("What are the attacker's plans?", "What is he in the process of doing?").

Assuming that the opponents have fully defined their respective moves—attack, protection, counterattack, and countermeasures—and that at least one of them is able and willing to commit further resources, the sequence of moves and countermoves is far from being concluded. The very same options heretofore employed by defense can now be used by offense to defeat both counterattack and countermeasures. In addition to passive protection of the elements of the primary attack, offense can use counter-counter-attacks (C^2A) or counter-countermeasures (C^2M) to interfere with the opponent's countermeasures (Figure 22). Cross-terms in the mathematical sense are possible; one may think of counterattack against countermeasures (CA.CM) or countermeasures against counterattack elements (CM.CA). In simple terms, this may mean a move to shoot down the defense's jammer aircraft or to jam the command link of an interceptor.

It is logically satisfying to mention higher order interactions. These represent for instance the countermoves of defense against the second moves of offense. The eight types of active moves are shown in Figure 23 and could be described by the symbols C^3A (counter-counter-counterattack) C^3M, $C^2A.CM$, CA.CM.CA, etc.

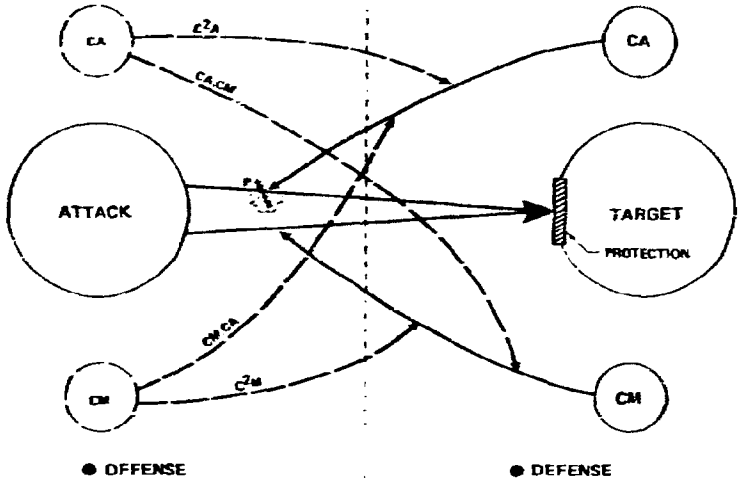


Figure 22. Conceptual Engagement (Second Move — Offense)

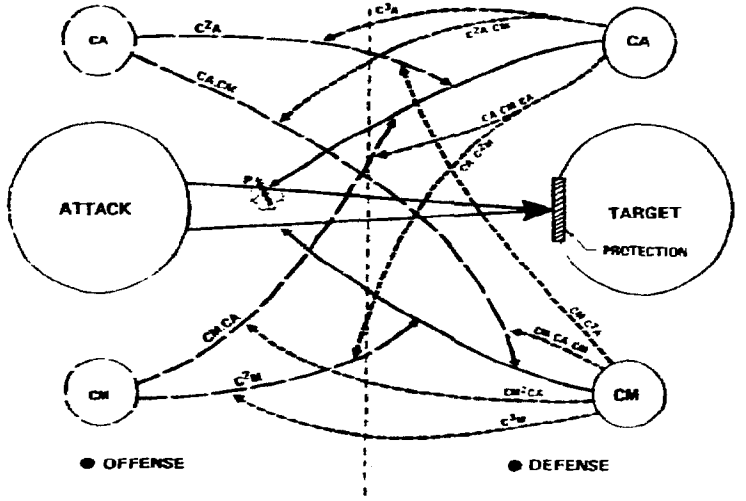


Figure 23. Conceptual Engagement (Second Move — Defense)

There is no conceptual limit as to how far one can go in this direction; fortunately, however, practical limitations intervene well before the analyst has to confess that there are no satisfactory mathematical models whereby the outcomes of such complex engagements can be studied. These practical limitations are apt to arise in connection with having in readiness a large number of attack and countermeasure elements, each playing a specific role in the sequence of moves and countermoves. It is far more likely that both opponents will simply use whatever resources they have available at any point in the engagement whenever such use appears promising on an ad-hoc basis, rather than attempting the implementation of some complex multistep optimal strategy based on questionable input data.

In recapitulation, the essential points in regard to the conceptual nature of engagements are as follows:

- Offense and defense moves are closely interwoven; they are symmetrical and often indistinguishable.
- Interactions (at least in large-scale modern engagements) rapidly grow complex to the point of defying rigorous analysis (hence the respect paid to "brilliant tacticians").
- Intelligence is always important, and often the decisive factor influencing the outcome.
- Countermeasures (interference with the enemy's information flow) rank as an equal to counterattack (destruction of the enemy's physical attack components).

In regard to the last point, as shall be presently argued, countermeasures are, in general for rather fundamental reasons, far more effective. (We have just given, not quite unwittingly, a tantalizing glimpse of the final conclusions.)

Attack vs. Counterattack

Attack Functions

The functional description of the attack is facilitated by a flow diagram (Figure 24). In contrast with functional block diagrams (Figures 7 and 8) where the emphasis was on the identification of the *participants* (humans, machines, systems) with the functions implied, here the *functional roles* are made explicit, with the participants implied.

Four phases of the attack are represented in Figure 24.

Procurement/Deployment—The systems and subsystems are developed, tested, and subsequently modified (1); the procurement results in production of operational equipment, complete with hardware, software, spares, and training manuals, with significant operational system testing occurring in the production phase (2). Deployment (3) follows production and places operational weapons in the hands of the user.

Pre-mission—Hardware and software components must be stored, protected, and maintained (4); human crews must be continuously trained, and exercises are conducted to demonstrate operational readiness and performance. If mobile weapon platforms are used, the weapon is loaded on the platform (5) or is in some other way associated and integrated with the platform. Information flow and common data bases between the platform and the weapon are established at this point.

Mission—The commander orders the launch platform to transport the weapon to the launch point (6) and to transmit to the weapon all mission-related information.

This "initialization" (7) may also involve communication by the platform or by the weapon to and from navigation references; at least, it must explicitly contain the identity (designation) and the location of the target (8); the assignment of a specific weapon to a specific target if there are more than one in either category (9); and the selection and presetting of the terminal engagement parameters, such as warhead and fuze options, aim point designations, or even terminal guidance sensor selection or counter-countermeasure tactics (10). The last element of the initialization sequence is an irreversible "go" or launch command (11). The target designation and acquisition function 8 may receive indepen-

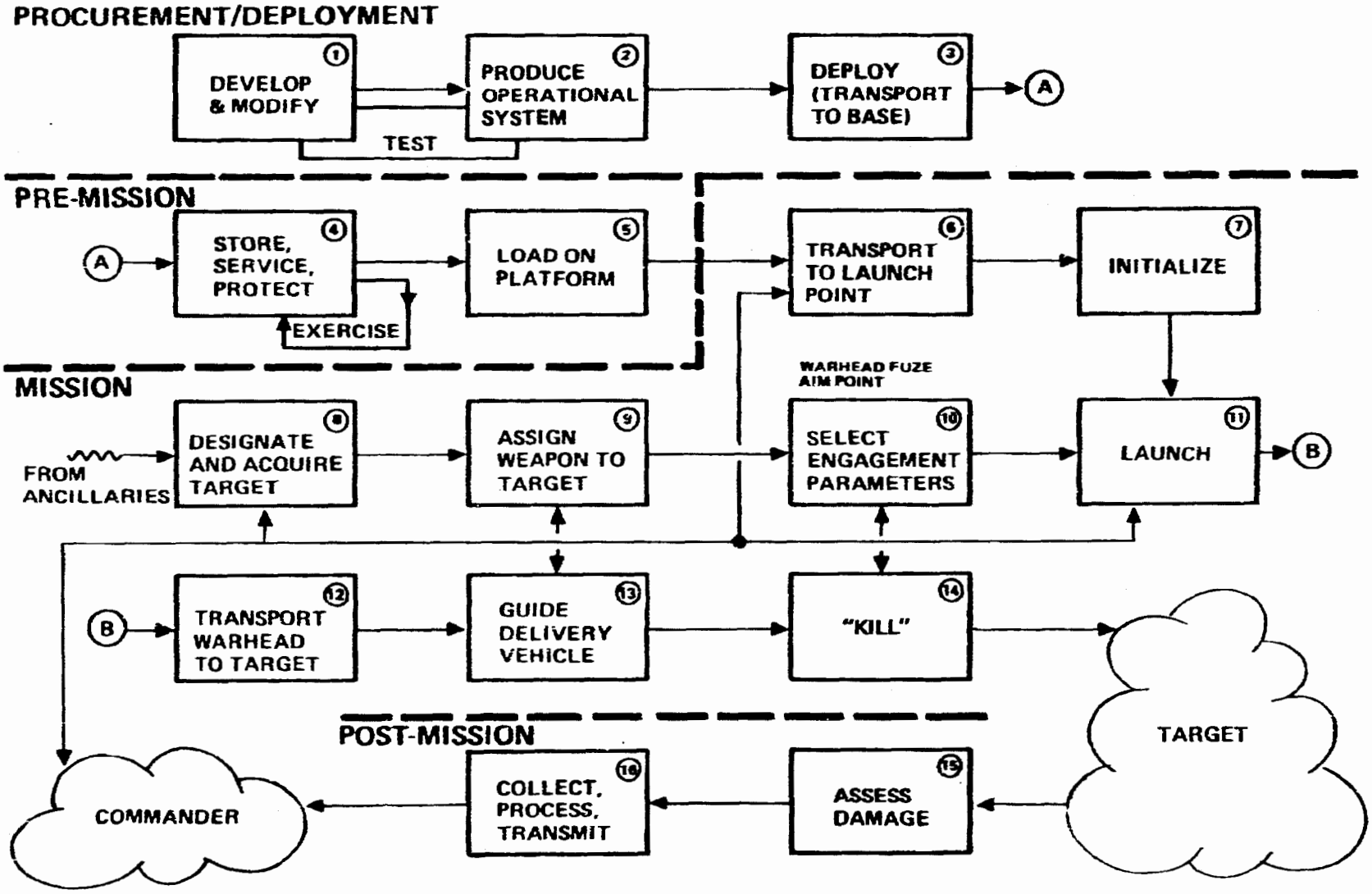


Figure 24. Attack — Generalized Functional Flow

dent support or confirmation via ancillaries such as reconnaissance, surveillance, or warning systems. The initialization chain ⑧-⑨- ⑩ - ⑪ , including launch, can occur separately as shown or alternatively via the launch platform ⑥-⑦- ⑪ . In both cases, the initialization transmits the specific intention of the commander in the operational format directly usable by the weapon. Following launch, the delivery vehicle is on its way to transport the warhead to the target ⑫ using internal or external guidance references ⑬ to reach its destination. It will again use internal or external signal sources to initiate the warhead ⑭ by means of a "detonate" command. Both the vehicle guidance and the warhead initiation may involve the direct participation of the commander, as shown by dotted lines. Most command links contain explicit confirm (feedback) provisions.

Post-mission—From the standpoint of success of a specific attack, the post-mission phase is only concerned with target damage assessment (TDA) ⑮ and the interpretation, collection, processing , and transmission of TDA ⑯ . From a broader viewpoint, the return to base of the launch platform and/or its availability for other missions, the recovery of the crew, or even the return of unmanned recoverable delivery vehicles are important considerations, even though for reasons of simplicity these have not been represented. Also omitted from the diagram are the means by which information stored aboard the delivery vehicle or launch platform will be retrieved at mission end or destroyed if the mission fails. This particular consideration is important and will have to be examined in future extensions of this analysis.

Concluding the description of the attack functions, two important observations appear to be in order:

1. The time domains covered by the described functions vary between rather broad limits. The procurement/deployment phase events are measured in years; the pre-mission phase may involve hours, days, months, or sometimes years; the mission phase rarely exceeds a few hours and may be compressed to a few seconds. The terminal engagement phase is, in general, quite short; it is measured at the best in minutes or even seconds, with some important interactions taking place in microseconds. The target damage assessment may take a few seconds in a small-scale tactical engagement but many hours in a high-level nuclear encounter. Very little practical experience is at hand to guide us in the latter situation.*
2. The functional description of the attack, stated in terms of a first move (primary attack), would in fact be quite identical for a second move (counterattack), third and subsequent moves, except for the total resources engaged and the specific or unique attack elements designated for the respective roles. The only conceptual difference is, as mentioned earlier, that the primary attack is aimed at a unique target set for a given mission, whereas the second and subsequent moves are targeted at many physical elements of the countermoves of the enemy and should ideally take into account the nature of these countermoves.

No claim is made in this description for completeness or uniqueness. Many other viewpoints can be taken in order to accomplish the present purpose, which is to discuss the relative applications and merits of counterattacks versus countermeasures. The descriptions should be considered illustrative rather than rigorous or exhaustive.

Counterattack Aim Points

The general flow diagram of the attack can now be used (Figure 25) to show some (by no means all) aim points where counterattack may be applied with potential profit for the defense side. As stated earlier, counterattack is defined as attempted destruction of, or damage to, the physical structure of primary, second-move, or subsequent attacks.

The operational system production phase ② can be damaged by means of preemptive attack. The test phases are often conspicuous

* Damage to humans in a nuclear battlefield environment may not be assessable for several days following the engagement.

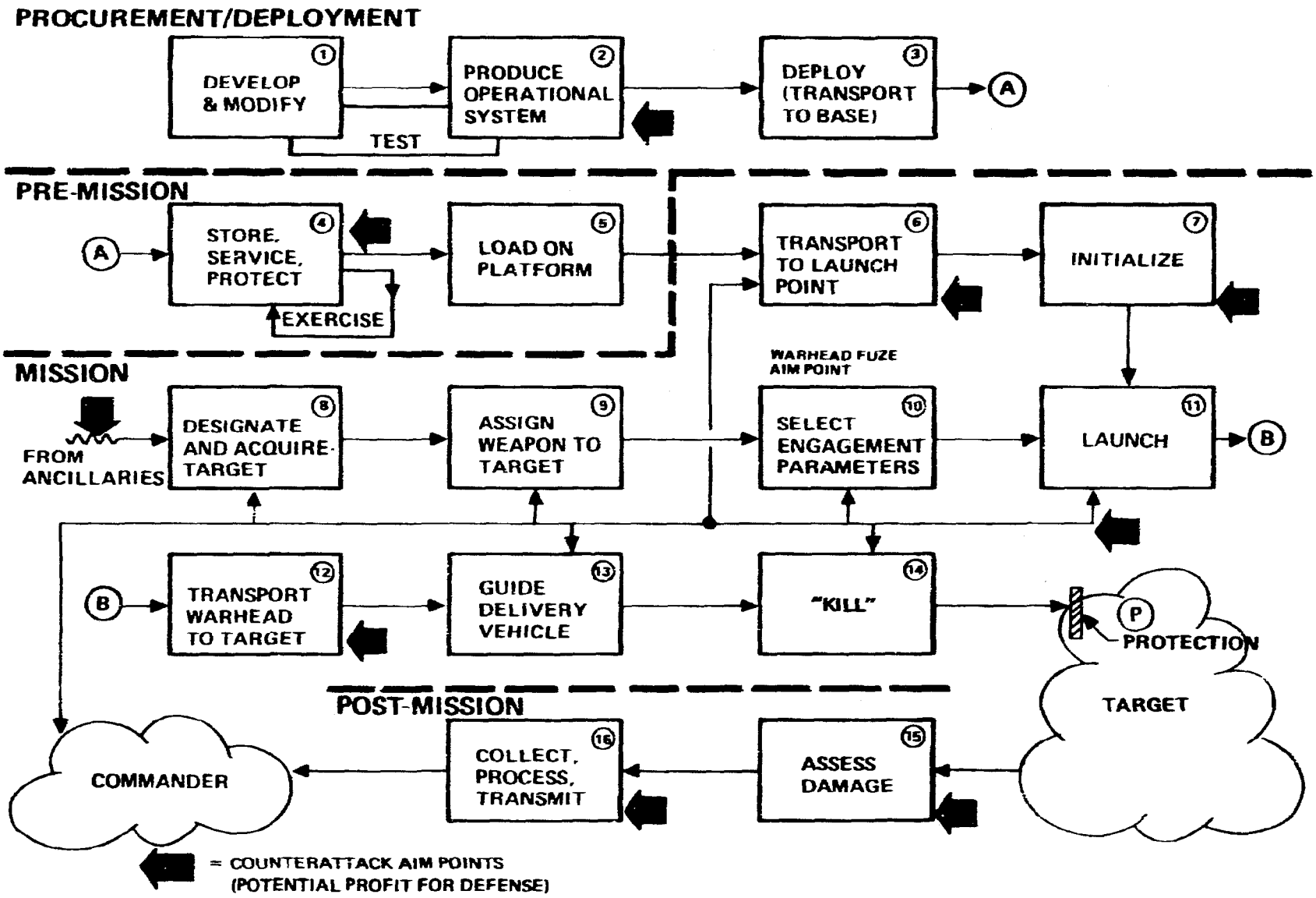


Figure 25. Attack — Generalized Functional Flow (Counterattack Aim Points)

and may become prime targets.* Covert attacks by means of saboteurs are possible and may be found attractive in some instances.

The weapon base (4) may also be attacked. This type of threat (sabotage, preemption or pin-down) is being widely discussed in the context of land-based ICBM's and strategic bombers; preemption of sea-based strategic missiles by attacking submarine bases is also one of the issues currently engaging the attention of the superpowers. In this category, too—though at the other end of the conflict scale—is the destruction by means of sabotage or rocket attacks on bombers or on other strike forces. Counterattack aimed at specific attack elements cannot always be separated from so-called strategic attacks, where one side seeks to destroy the enemy's resources irrespectively of any immediate engagement in sight.**

Attack against the launch platform in the transit phase (6) is the generally recognized threat against penetrating strategic bombers, but should also include the threats to airborne long-range offense missile platforms and to missile-carrying submarines. Attacks against high-flying aerial tankers may represent one of the vulnerable features of intercontinental strategic bombers. Air-to-air and surface-to-air interceptor threats to tactical strike forces are representative of this attack category in conventional warfare.

(7) indicates that when initialization depends on space-, land-, or sea-based beacons, their overt or covert destruction impairs the weapon accuracy.

(8) and (11) represent attacks on ancillary data sources and on the command and control structure, respectively. Attack against the command link threatens the definition of the attack objectives, the weapon assignment, and the launch command mechanism; thus it is considered as a particularly important aspect of the defense's countermoves. Destruction of the command and control apparatus is a classical and essential military objective for strategic offense forces, even though there is a school of thought which holds that under certain conditions destruction of the central command links is not in the interest of either side. We suggest here that to the extent that impairing his command structure creates uncertainty in the opposing commander's mind, it will be eagerly pursued by both sides as a military objective.

(12) illustrates the problem of missile or remotely piloted vehicle (RPV) intercept. In the latter case, the designers' dilemma is typical of the theme of the present discussion. Assuming that the acquisition, guidance, warhead, and propulsion features of the weapon are adequate, how much should he invest in *protecting* the individual vehicle at the obvious detriment of other performance elements, cost, and command complexity? The presence of a human crew, although contributing to self-defense, also greatly increases the unit vehicle cost and brings nontechnical considerations to bear on the importance of survival.

Some passive protection techniques (P) may be considered as counterattacks against the delivery vehicle. They cannot be discussed here in detail for reasons of classification, but are nonetheless conceptually important.

(15) and (16) portray the possible destruction of target assessment components. They may include attacks on reconnaissance aircraft or satellites or against communication relays and ground terminals. Launch confirm and trajectory assurance type signals would probably travel via (11) ; all contribute to the degree of certainty about the outcome of a given mission and are thus valuable to the attack side.

While not being fully comprehensive, the point has been made that at all levels and types of conflict many counterattack modes are possible and practical. All the counterattack modes, individually and collectively, threaten the success of the attack. Except

---

* The British raids on Penemunde in 1943-1944 are classic examples. The Soviet Union's alleged plan to strike the fledgling Chinese nuclear weapon developments in the mid-1960's, had it been carried out, would have fallen in the same category.

** Examples abound in World War II: manned torpedo attacks on British capital ships in the port of Alexandria; Japanese attack on Pearl Harbor against the U.S. Pacific Fleet; and British air attacks against the V-1 and V-2 launch bases in Western Europe.

for sabotage, all the counterattack modes are overt. So, in general, the attacker knows exactly to what extent and by whom his attack structure has been damaged, and can either provide additional standby resources or take other circumventive actions.*

Countermeasures

Definitions and Extensions

In order to argue the merits of countermeasures in the context of engagemer , it is necessary to define the meaning attached to this term. Countermeasures refer essentially to actions against the information flow present within the extended weapon systems. In many instances, electronic countermeasures are of major concern, but optical, infrared, and acoustic signals are often of importance. In the general sense, whenever information is being transmitted by any medium, by any mechanism at any frequency, countermeasures can be applied.

A rapid inspection of the attack functional flow diagram will reveal many available information sources within the weapon system. Figure 26 shows some, but by no means all, of the possible information sources falling in two categories: First, the *strategic intelligence*, which attempts to describe the opponent's capability, the technical characteristics and the associated operational plans pertinent to his attack system, and the associated ancillaries. Second, *tactical intelligence*, pertains to the opponent's specific (selected) plans and actions aimed at performing a certain mission, the resources he plans to engage, his timing and order of battle. Because of the multiple sources associated with tactical intelligence, this category is often discussed under the headings of surveillance, reconnaissance, warning, tracking, and others. Every one of these has its corresponding lore, disciplines, and equipment. Nonetheless, the information provided by tactical intelligence has to do with status and resources, order of battle, location and nature of target, guidance, navigation, and command signals. Many other sources of tactical intelligence may readily be identified.

* The covert attrition of nuclear missile-carrying submarines is an important exception.

A separate and important category of information is provided by the communications expressly transmitted between the elements of the extended weapon system, as shown in Figure 9 during the premission and subsequent phases. These will be discussed later under the heading of *operational information flow* and are often gathered and scrutinized by the enemy's signal intelligence (SIGINT) or communications intelligence (COMINT).

The message in Figure 26 is that the attack system as a whole radiates over an incredibly broad frequency domain a multiplicity of signals which a smart opponent can, and in general will, exploit.

Figure 27 shows the "frequency spectrum" of a complex weapon system over its life cycle. The numerical information is intended to be illustrative rather than precise or authoritative. On the other hand, the same figure may be used to portray the opponent's response spectrum; i.e., his attempts to exploit, or interfere with, the weapon system information flow. *We suspect that the failure to recognize weapon systems as complex, broad-spectrum signal sources has caused wide gaps and inadequate response characteristics in the techniques of countermeasures.*

With this as background, we can now discuss more in detail a somewhat broader definition of countermeasures (Figure 28). Countermeasures may have two separate although often interacting objectives:

1. Disrupt; i.e., prevent the opponent from sensing, transmitting, and/or receiving the signals that are correct and required for his purposes. Included are signals, messages, and information in general that are used by the opponent to implement his operations (*his* extended weapon system model as shown in Figure 9), but also, quite explicitly, those which he attempts to sense and analyze in order to gain understanding about *our* preparedness and operations. As explained earlier, we shall continue to refer to these as *operational* information flow and *intelligence* information flow, respectively.

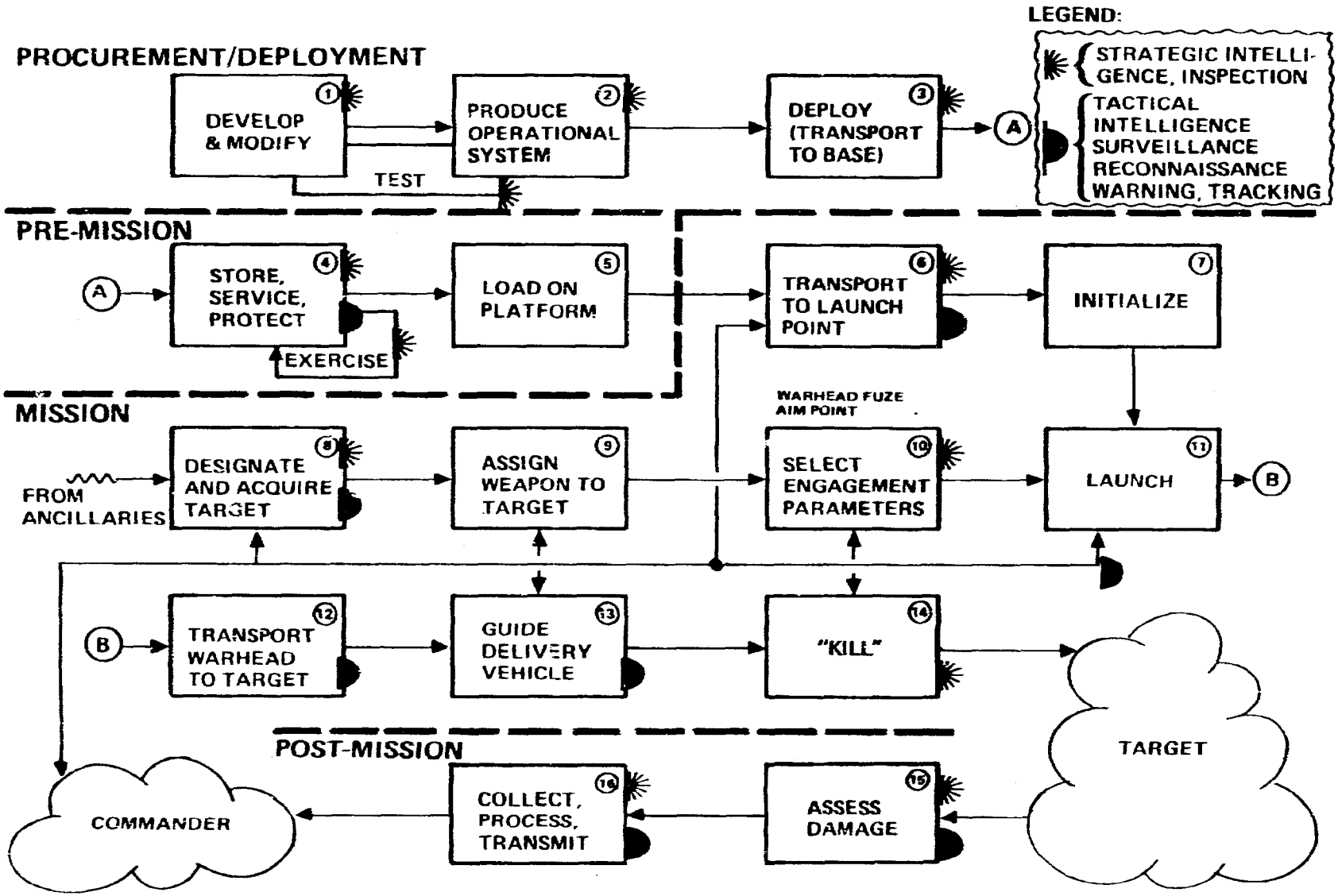


Figure 26. Attack — Generalized Functional Flow (Information Sources)

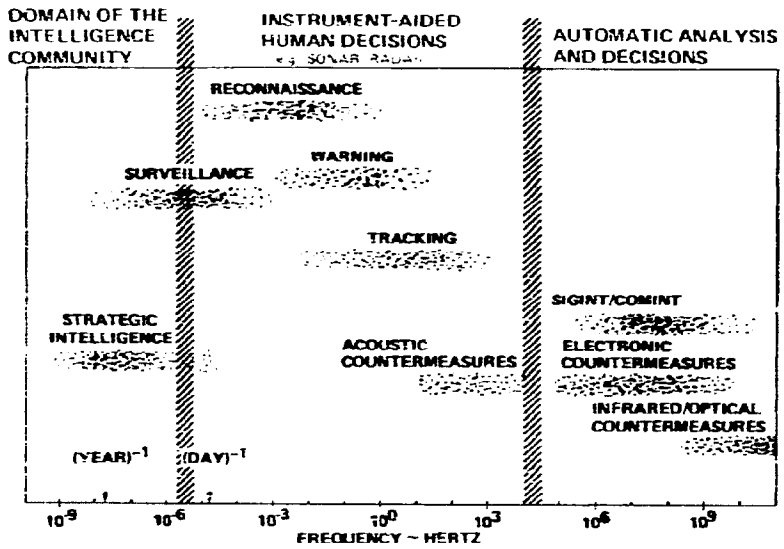


Figure 27. Event Spectrum (Typical Military Engagements)

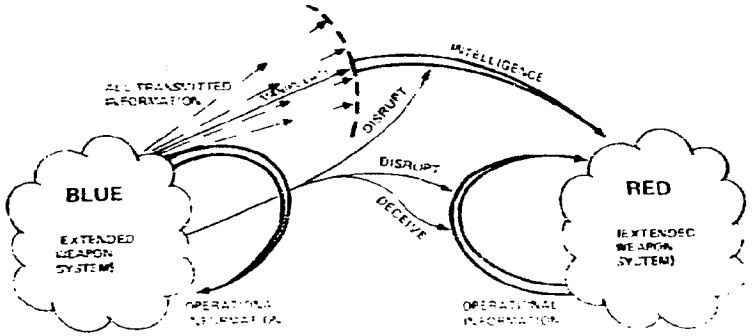


Figure 28. Conceptual Aspects of Countermeasures (Seen From the Viewpoint of "Blue")

2. Deceive; i.e., cause inaccurate or erroneous signals to be sensed, transmitted, or received without the hostile originator or recipient realizing their true nature. Once again, this countermeasure mode should be thought of as clearly (and perhaps emphatically) applicable to both operational and intelligence type information. In regard to the latter, the term "manipulation" rather than "deception" is more appropriate, since quite often emphasizing a true message via the intelligence channel may serve as an effective deterrent. The possibility of creating uncertainty in the opponent's mind by a judicious mixture of truth and plausible falsehood should not be overlooked.

Typical Entry Points

Let us rapidly survey some of the practical application points of countermeasures (Figure 29). The development phase (1) can be misinformed by sending the wrong intelligence signals in terms of capabilities, plans, status, and, most importantly, test results. Misleading inspection results or deliberate deception would enter at this point. Communication interference (jamming or spoofing) may degrade platform navigation and initialization functions (7). Targets can be decoyed or camouflaged; target mobility puts a time constraint on the ancillaries (8). Deception in regard to optimal aim points may lead to wrong fuze settings (10).

Interference with launch commands (11) is considered to be a substantial threat to the U.S. strategic offense forces; some differences of opinion are voiced as to corresponding concerns of the U.S.S.R. A higher form of the same interference with the targeting role of the command structure is the camouflage or spoofing of the true nature of the targets. This in time may lead to interference with missile terminal guidance, causing them to go to the wrong target or to explode prematurely. (14) represents interference with the firing signal of the fuze. (15) and (16) correspond to causing the wrong signals to be transmitted to the opposite command, giving erroneous information on target damage. This can be done either by spoofing the communication links or by decoying the surveillance component of the target damage assessment system.

The arrow within the target area is a reminder that tactical warning may be used to cause the target to disappear or to be of little

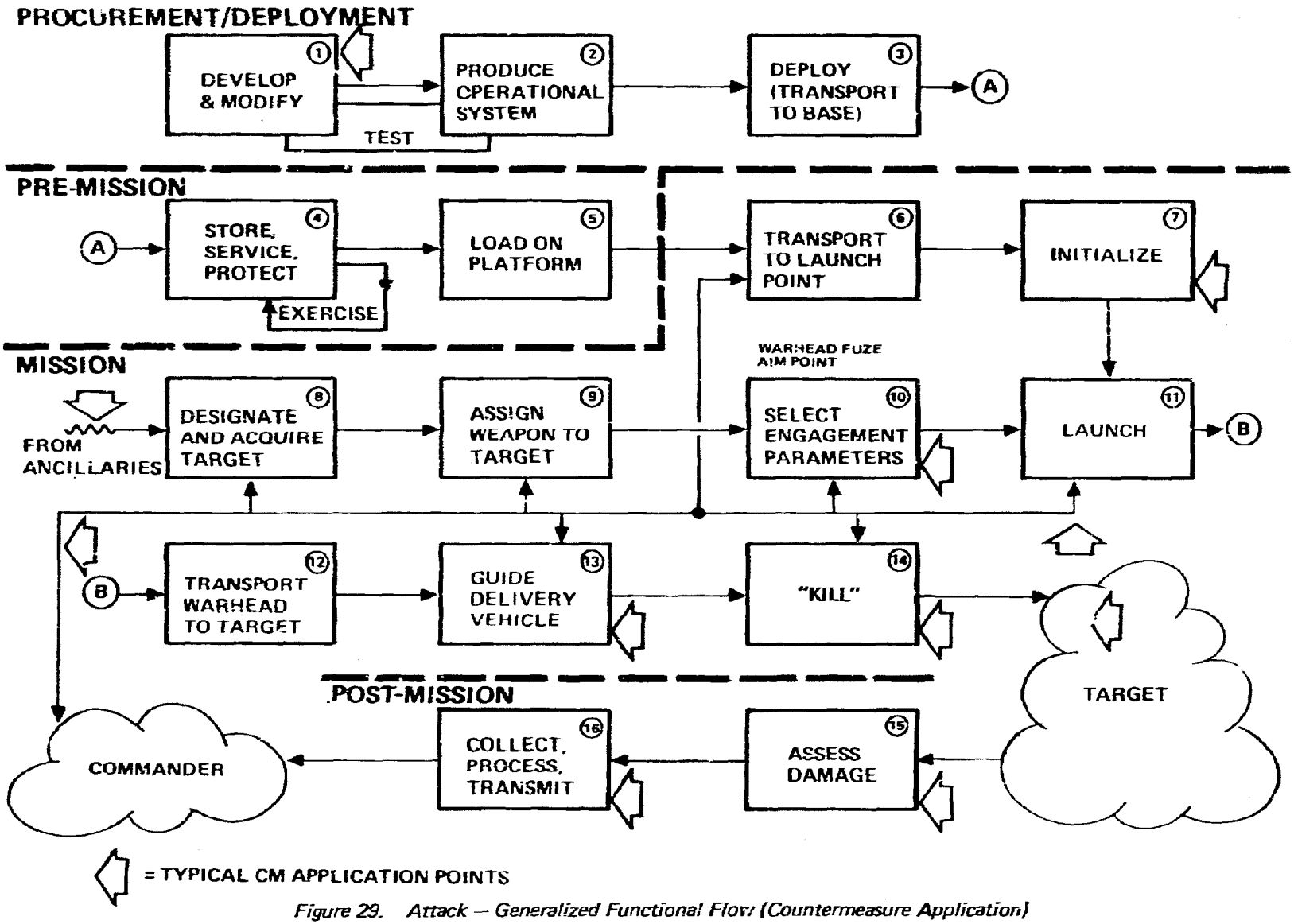


Figure 29. Attack — Generalized Functional Flow (Countermeasure Application)

residual value to the enemy. If the attack is aimed at a ground-based bomber force, "scrambling" to the airborne alert mode radically decreases the attacker's chances of success. In much the same way, if a counterforce missile is aimed at a land-based ICBM using "warning of critical events," prompt launch may prevent the attack from accomplishing its purpose.

Target denial is also possible based on strategic intelligence. For instance, the highly publicized "countervalue" deterrent mode of the U.S. strategic nuclear missiles is based on massive destruction of cities, population, and industrial capability. The Soviets may attempt, by means of a long-term civil defense and industrial dispersion program, to eliminate this target set as part of a viable military mission.*

Functional Description

We must still examine the functional mechanism involved in developing countermeasures. As shown in Figure 30, the generalized functional flow for countermeasures is strikingly similar to the one shown for counterattacks. The differences are that (6) now has the meaning of "transport to operating station," and (7) is "verification of engagement geometry" as contrasted to "initiation." This in actual fact means, for instance, that the fixed or mobile jammer platform has to ascertain it is in the proper position for accomplishing its mission. (9) has now a slightly different meaning. The specific CM functions have to be defined by the commander, his delegate, or by the initiative of some manned or automated countermeasure station. Similarly, engagement parameters (frequency and specific countermeasure tactics) have to be selected in very much the same way as the lethal warhead mechanisms must be selected in the case of the attack. Note that arrows between the commander and functions (8), (9), and (10) are two-directional. This communication traffic itself is potentially a most vulnerable point of the countermeasure structure. In regard to (11), instead of launch, the proper terminology for countermeasures should be "start."

* There is substantial evidence at hand that this in fact is an ongoing activity within the U.S.S.R. [1, 2].

On the other hand, (13) continues to be important since monitoring of the countermeasure "delivery" is necessary. Another new facet is that, because of the extremely short time periods usually involved, the damage assessment may feed back directly into the selection of engagement parameters (10) rather than going back all the way to the commander. In practical terms, this means that the electromagnetic engagement is most frequently monitored on a quasi-real-time basis and the engagement parameters presumably are adjusted to supply the best possible effect.

Interference and Exploitation

A more detailed examination of the countermeasure mechanisms becomes now possible and necessary to enable assessment of performance in quantitative terms. Figure 31 shows the basic features of generalized countermeasure interactions. It is appropriate to regard this model as a representation of the terminal engagement of what can be properly termed the "information war"** between the opponents. The actions of only one side are shown; those of the other side are symmetrical and in addition comprise the C^2M type countermoves, as explained earlier.

The information link in the center represents any target of the information war. As seen in the previous paragraph, it may be part of an intelligence link such as those in Figure 28 or of an operational link such as some of those identified in Figure 9.

The functions required to effect interference (destruction or manipulation) are shown at the top of the figure. After having decided the objective, it is necessary to generate a message that eventually will be injected into the opponent's information channel. The content of the message should be appropriate to the objective; it may be conveying the "truth" if for any reason we wish him to know and to believe it. It may just as well be a deliberately "false"

** Sir Winston Churchill has recognized the incipient aspects of what we are discussing here under the chapter entitled "The Wizard War" in his memoirs of World War II [3]. Today we have passed from wizardry to a more potent and dangerous form of warfare, certainly more widely pursued, if not better understood, by most of the potential combatants.

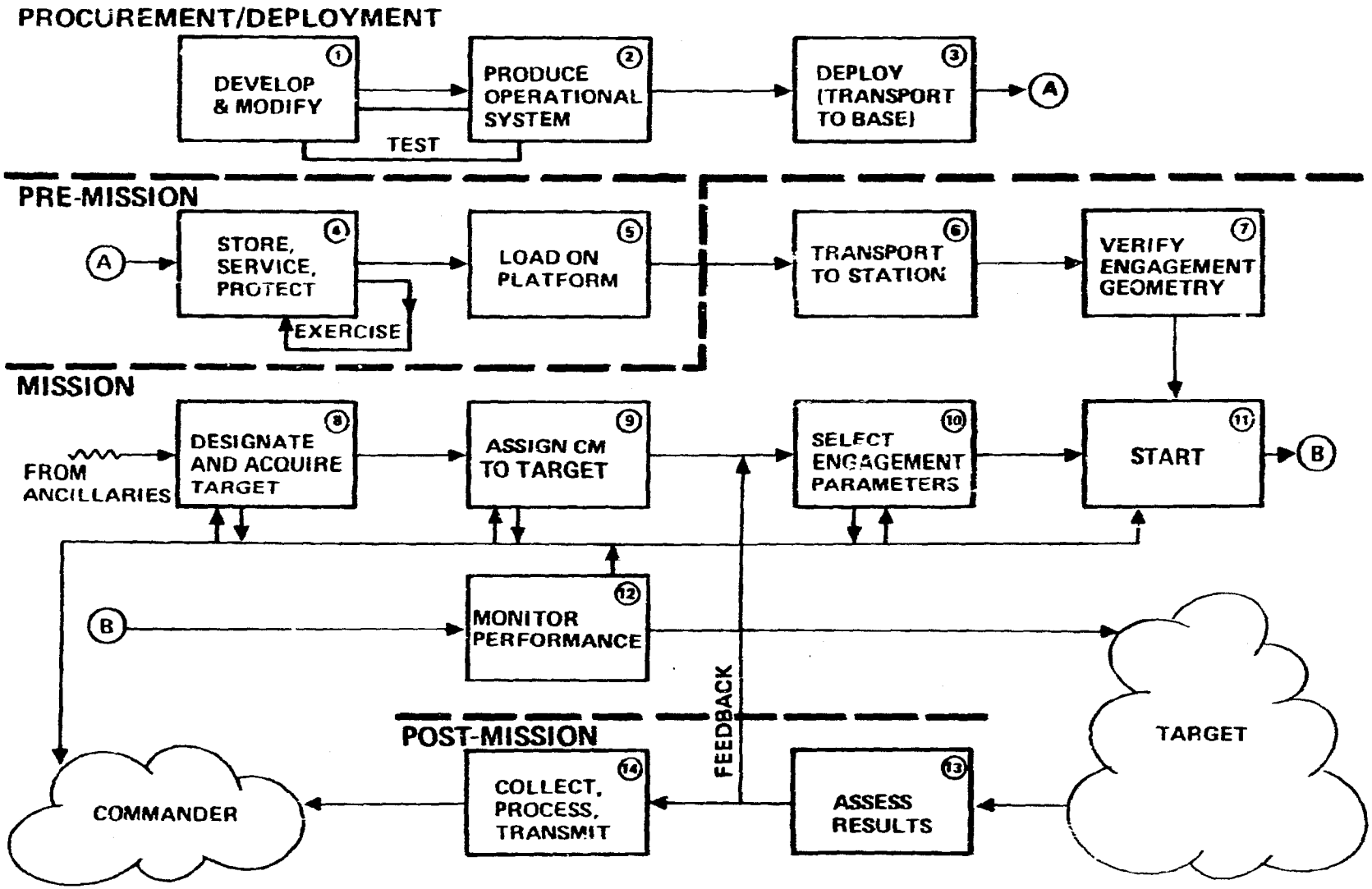


Figure 30. Countermeasure – Generalized Functional Flow

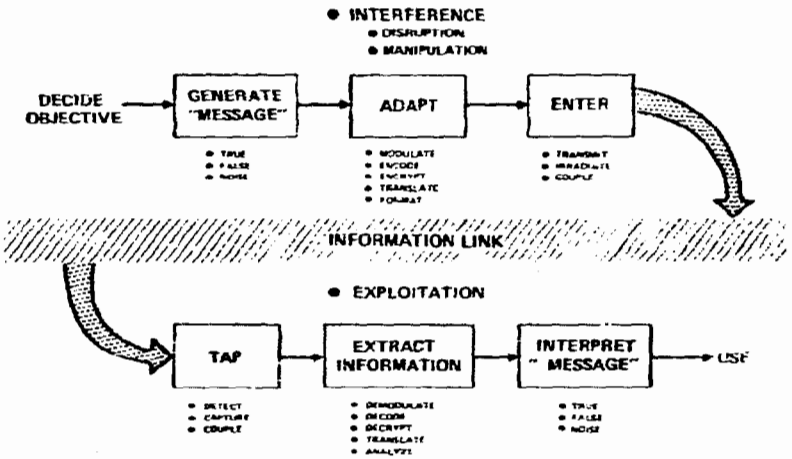


Figure 31. The Information War (Conceptual Engagement)

message intended to be accepted as being the truth; it may be a mixture of both; and finally, it may be a "random" or "noise" message meant to increase the error rate and thereby the probability of misinterpretation by the enemy.

The second essential function is to adapt the message to the format that will cause it to be physically and psychologically accepted. To effect this, the message must be modulated, encoded, encrypted, and/or translated into the logical language or pattern of the opponent and transmitted via the right signal frequencies. For interference to take place with any reasonable probability of success, adequate knowledge of the opponent's signal processing techniques must be at hand.

Third, a physical entry into the information link is required; i.e., coherent* energy transfer either through some transmission or irradiation of the enemy's sensors or even direct electromagnetic, acoustic, or other coupling.

* In the sense of information-carrying.

Obviously, the side attempting to use the interference-type countermeasures requires in-depth knowledge (inteiligence) about the opponent's information link. Just as obviously, the gathering of such intelligence and its application to countermeasures will be actively resisted by the enemy. He will attempt *deception* regarding his decision criteria (what he would accept as a true or false message); he will impose elaborate security precautions to safeguard his adaptation processes (modulation, encoding, encrypting, etc.); and he will use any and all reasonable physical precautions to prevent unauthorized entry of his information links. In particular, the hardware installations will be secure, and electromagnetic or acoustic radiation links will be protected by directivity and sidelobe suppression.

The lower portion of Figure 31 portrays the "exploitation" mode of the information war. The purpose here is to secure and use information extracted from the opponent's information links in order to improve our own decision processes: The operations that take place in the exploitation mode are exactly the converse of those described for interference. We have to tap the enemy's communication links by either detection, capture, or direct coupling; coherent energy must be transferred from his information link to ours. We have to extract the information content by means of demodulation, decoding, decrypting, translation, and analysis, essentially the converse operations of those performed in the adaptation process.

Finally, we must interpret the message; i.e., understand its true meaning and decide whether it is a true or a false (deceptive) message or simply noise. The information thus obtained will be used as an aid in decision-making, either to select the correct strategy or, having such a strategy, to implement the corresponding tactical moves.

It must be emphasized that both strategic and tactical moves include the implementation of countermeasures as well as other attack-counterattack type operations. *The exploitation mode of the information war is thus seen as indispensable to success*, and

all sides will go to extreme exertions to secure its benefits and to prevent its detriments.

From the description of the exploitation process, it is quite clear that a substantial amount of detailed and correct prior intelligence will be required for success. The value of the exploitation is therefore *cumulative*; once we have extracted data pertaining to the opponent's information channel, further exploitation is facilitated. Small wonder then, in view of the high and cumulative value of exploitation, that both opponents will stress physical and processing security of their respective information links. Carefully safeguarded adaptation techniques will be utilized to prevent extraction of meaningful information. Both sides will strive for special adaptation techniques (encrypting) with time-variable characteristics, in principle not amenable to exploitation by the enemy.

Although this picture, once explained, is intuitively clear to everybody, very little systematic background exists to develop and implement corresponding operational doctrines and equipment. These may exist in selected engagements, mostly at the terminal mission phase, but in general they are not explicitly formulated for the pre-mission and post-mission phases. There appears to be ample room for improvements in both doctrine and equipment. It is not evident that the relationship between the objectives of interference and the results of exploitation is widely understood, accepted, or even explored. While the results of the *exploitation* mode are often used for the technical details of *interference* in the terminal mission phases, this same connection appears lacking in the formulation of proper input messages (true or false) for interference with the upstream portions of the weapon system functional flow (Figure 24) and is also often absent in the post-mission phase.

Measures of Performance

The discussion of countermeasures up to this point has been conducted at the conceptual level, but the system designer, in view of allocating his resources, will want to have qualitative and, if possible, quantitative measures of performance available. These will now be examined for the disruption, deception, and exploitation modes.

Disruption—The message (or sequence of messages) in the opponent's information link* should be thought of as being the input channel to some decision process. The elementary decision may be binary (yes or no) or quantitative (whether or not a quantity derived from the message falls within prescribed intervals). The primary physical phenomena sensed are electromagnetic or acoustic fields and their derived properties such as amplitude, frequency, polarization, spatial distribution, contrast, contour, etc.; but basically, after the appropriate preprocessing or demodulation, a signal-to-noise ratio (S/N) is obtained.

The simplest situation is when the information channel is in the "clear," and the opponent uses no adaptation other than that necessary for satisfying the technical demands of the transmission link. Demodulation of such a signal may then be subjected to time sampling or to spectral analysis. In both cases, the meaning of the message is determined by the weighted combination of all time samples or of all spectral components. (A more detailed discussion is given in Appendix A.) The probability of error on any one sample is a decreasing monotonic function of the signal-to-noise ratio. Disruption then, in this simple case, means to deliberately degrade the signal-to-noise ratio of the opponent's demodulated signal. If this is to be carried out with reasonable power requirements, the carrier frequency and the modulation technique of the opponent must be known.

The problem becomes more difficult when the opponent protects his information channel by superimposed modulation specifically aimed at defeating attempts at disruption. This *antijam modulation or protection* consists of diffusing the information content of the message over a broader frequency spectrum than required by the clear modulation alone. Many ingenious antijam protection schemes have been proposed and applied; all of them render the task of disruption more expensive in terms of noise power effectively introduced into the opponent's information link. Even if

* It is immaterial in this instance to distinguish between communications (messages deliberately generated in view of transmission of information) and sensing (where messages are extracted from radiation or other phenomena not primarily intended for transmission to *this* receptor).

the disruptor has perfect information on the spectral density of an opponent's modulated message, he must acquire expensive adaptation equipment to selectively apply noise power in the appropriate spectral regions. He is heavily penalized in terms of power requirements if he lacks adequate information and must inject noise power over the whole extent of the opponent's deliberately broadened spectrum. In the presence of antijam protection, the noise-to-signal ratio is still the appropriate measure of the error rate, but now this ratio must be expressed with due regard to the effective "noise" attenuation due to the adaptation process. It is seen that the antijam protection, by making the adaptation more difficult, requires either greatly improved intelligence or imposes a substantial power penalty on the disruptor. Quantitative expressions are to be found in Appendix A.

Deception—All the statements of the previous paragraph remain valid; in order to have any probability of success in the deceptive mode, a signal must be introduced into the opponent's information link that will be accepted by the intended user as a valid message. In practice, the signal-to-noise ratio of the deceptive signal (accounting for the adaptation loss) must be at least equal to, but preferably higher than, that of the opponent's own signal. Formatting requirements may be quite demanding, especially at the longer period strategic intelligence levels or, on the contrary, may be relatively simple camouflage or decoying of optical signatures against visual detection. In order to design rational deceptive countermeasures, one must theoretically be informed of all the message channels entering the opponent's decision process; the decision logic (the weighting of the individual messages) must be known or postulated. These conditions are hardly ever satisfied in practice, but, in a few simple cases, numerical evaluations are possible, as given in Appendix A.

In order to protect against deceptive techniques, the opponent will—

- Protect most or all of the message channels entering his decision process by means of adaptation techniques discriminating against nonadapted (extraneous) messages
- Use as many as possible of independent high S/N channels to formulate his decisions
- Carefully protect his decision logic against compromise.

Exploitation—Let us assume that one or several of the information channels of the opponents have been "tapped," and signal energy is being captured for the purpose of exploitation. A message *extraction* process (the converse of the adaptation) must take place. In a manner exactly corresponding to the disruption and deception modes, the side attempting meaningful exploitation must strive for as high S/N ratios relative to the captured signals as possible and must, therefore, have near-perfect information in regard to the adaptation used by the opponent. Two novel aspects of successful exploitation must be emphasized:

1. The message(s) extracted, singly or in combination, must have some *relevancy* to the characteristics present or the events taking place within the opponent's force structure.
2. Deceptive signals, deliberately intermixed with those truthfully representing characteristics or events, must be separated and rejected. This task is rendered far more difficult by the opponent's perfect knowledge of his own adaptation processes, which enables him to use efficiently the power expended in deception.

In simple cases, where the relevancy question is trivial, the problem of successful exploitation is essentially one of the number of independent message channels and the high individual S/N ratios. High-resolution, high-contrast optical patterns are remarkable in this respect, in addition to being amenable to correlation (pattern recognition) by the biologically adapted human eye-brain combination. This type of situation still prevails when tactical intelligence attempts to establish the radiation frequencies and patterns of defense radars or sonars *not protected by deceptive techniques.*

When the relevancy problem is relatively tractable, the number of independent message channels may offer protection against deception. Thus, optical camouflage is rendered more difficult by multispectral sensors; submarine acoustic decoys may be defeated by

magnetic gradient measurements. Many other examples can be found.

It is in the slow event-rate strategic intelligence domain that the problem of relevancy sets the limits of applicability for exploitation and the corresponding deception processes. First, owing to the unusually low information bandwidth* measured in very small fractions of hertz (see Figure 27), the total signal energy is very small; thus theoretically, the introduction of noise and deceptive signal power should be easy for an opponent provided with perfect information. Time domain matching ("coincidence") plays a role analogous to frequency spectrum matching but is by far predominant at low event rates. Second, the extraction process, having to provide an extremely high gain, must have a highly matched filtering, which in turn implies knowledge of the model to which the captured signals are thought to be relevant. By analogy with biological processes, we chose to call this iterative process *imprinting*. The intelligence apparatus, once it has gained access to a small and credible portion of the opponent's system characteristics, can and will use this information to incrementally interpret the available information flow. By virtue of imprinting, the value of individual messages in terms of meaningful information increases with time.

The reader will certainly have realized by now that this section deals with an area where the esoteric and the arcane intersect. To the extent that any knowledge is available, it is most jealously protected by all potential opponents. The purposes of this discussion are amply served if the following conclusions are retained:

1. The signal-to-noise ratio and the number of independent channels are the primary figures-of-merit of the exploitation mode.
2. Deception can be overcome in simple cases (mostly in the vicinity of the terminal engagement of the mission phase) by increasing the number of channels and by securely safeguarding the logic used for decisions.
3. Both the possibility of deception and problem of relevancy become of predominant interest in terms of success probability in the domain of strategic intelligence. The process of imprinting (adapting the filter to the type of signal-to-noise mix) can cumulatively improve performance in this area, but very little theoretical background is at hand to support quantitative performance estimates.

In closing, a deception technique of a higher order must be briefly mentioned. The iterative and cumulative nature of the imprinting process related to strategic intelligence suggests that imprinting the enemy intelligence system by false decision logic ("misimprinting") may offer a higher payoff than that achieved by simply practicing deception on any particular message. Misimprinting consists of a carefully designed sequence of false messages, each reinforcing those preceding, with the hope that the enemy intelligence will learn how to rely on input data and decision logic different from what would be appropriate to his true objectives. Examples can be found in World War II;** also, with the benefit of hindsight, it may be suspected that the CONUS air-defense buildup in the 1950's was at least partially the consequence of deliberate Soviet misimprinting. Submarine acoustic signatures offer another potentially fertile field, but, quite understandably, those in a position to discuss this topic are most reluctant to do so publicly.

* The applications of thermodynamic aspects of information theory have not yet been explored, leave alone formally or successfully applied to strategic intelligence-type problems.

** In rather ambitious undertaking, the British Intelligence Service leaked false invasion plans to the German High Command. The chosen transmission medium was an artificially synthesized officer playing the part of a courier, who was impersonated with considerable thoroughness by a cadaver appropriately equipped and disposed for the purpose. According to reliable account, the operation was successful. [4]

(This page intentionally left b'ank)

4 IMPACTS ON MILITARY DEVELOPMENTS

The purpose of this section is to assess the consequences and the probable impacts of the conclusions reached at this point on the definition of weapon system requirements and on some significant aspects of future weapon system developments.

We have seen that modern weapon systems include a number of essential external information links accessible to enemy as a result of the long propagation distances. We have shown that advances in technology make countermeasures more sophisticated and possibly more potent in the future; we have also seen that multiple entry points over an extremely broad time domain exist for countermeasures in extended weapon systems, with ample opportunties for covertness and deception. We expect to show in this section that the generalized concept of countermeasures should significantly influence the weapon development process and perhaps the evolution of corresponding operational doctrines. Beyond that, the insight into countermeasures may well shed additional light on areas not heretofore fully accepted as being of military significance.

Military and Technical Environment

The possible consequences in regard to the future of weapon systems information flow need to be examined in the context of the military and technical environment predicted for the next 5 to 20 years.

In spite of its advanced technological and industrial base, the U.S. will no longer enjoy the benefits of monopoly in innovative military technology. The U.S.S.R. and some of its allies appear to be in position to develop, procure, and effectively inject substantial concentrations of military equipment into wars that further their policy objectives. The appropriate level of technology appears to be at hand when required, but more importantly, equipment and capability-in-being seem to be designed for, and amenable to, rapid transfusion to groups or nations not known until quite recently for their military prowess. For the purposes of our own concerns here, we should assume that (1) a number of major power centers will continue to pursue their policy objectives by the threat or the actual use of military force; (2) continuing development and refinement of strategic nuclear weapons and the associated ancillaries will remain a permanent feature of mutual or multilateral deterrence, irrespective of the direction and the rate of progress in arms control negotiations; (3) the U.S. will continue to invest, even in a much constrained funding environment, in the development and operational readiness of military capabilities covering a broad range of conflicts in widely different theaters; (4) the superpowers as well as the major secondary powers will develop the equipment and the doctrines required to conduct effective military operations in nuclear land, sea, and air battle environments; and (5) the opponents of the U.S. side will have at their disposal technology and proficiency in the use of military equipment essentially equivalent to that of the U.S.S.R., except in the area of strategic nuclear weapons.

In regard to this last point, it is not necessary to distinguish the origins of the assumed military capability; they may be as diverse as the possible conflict scenarios. The central thought is that the U.S. should not posture its forces (in conflicts of any real degree of significance) in keeping with the assumption that the enemy will only have primitive organization and weapons at his disposal. In the recent past, we have been powerfully reminded that equipment, while not necessarily at the forefront of the state of the art, can, in fact, if properly used and supported by dedicated personnel, decide the outcome of wars.

Game Aspects of Requirements

We must come to grips with the realization that the design of a weapon system that will be successful over its life cycle is no longer exclusively a problem of satisfying in an engineering sense a well-established set of requirements.

During its operational life, but also during the development and procurement/deployment phases, a new weapon system will potentially face malicious, well-informed, and quite capable opponents. The enemy will know, well in advance of the war, what our systems can in general accomplish and the manner, often down to specific design details, in which our systems operate. He will have carefully monitored the information sources radiating from within the U.S. defense community and he may have even dissected or tested operational specimens for his own benefit. He will thus have ample time to ponder the effective means to counter our possible initiatives. Rather than wasting his resources in attempts against the strong characteristics of our weapons, he will concentrate his attacks on the weak points that we may have neglected or insufficiently developed. *Countermeasures against our information flow, being efficient and susceptible of covert use over long periods of time, are prime options of the enemy.*

The broader definition of "requirements" in the future will thus logically include all the significant and foreseeable moves and countermoves potentially occurring between the concept development phase and the end of the operational employment phase. Briefly stated, the definition of weapon system requirements has explicitly developed all the attributes of a *game* (in the theoretical sense of the word) where the success of the strategies chosen by the "players" depends critically on the quality and the effective use of information respectively available to them.

The use of the word "game" should not allow us to forget the deadly connotations of what we are discussing here. Effectiveness of specific weapons in the field, outcome of specific engagements or campaigns, and also the rational use of technical and funding resources made available by our society may well hinge on the in-depth understanding of the gaming aspects of future weapon system developments.

The nature of the game played by two opponents can be represented in the classical form of a matrix (Figure 32) with the columns X_j representing the strategy choices of say, the Blue side, and the lines Y_i, Y_j, etc., those of the Red side. A strategy, in the sense used here, is a predetermined set of future decisions contingent upon the observed or suspected moves of the opponent. In the customary form of conventional war games, strategies are developed for a specific military engagement or perhaps a sequence of engagements, such as a campaign affecting a whole theater of operations. In recent years, considerable effort has been expended in trying to apply war gaming to the problem of evolving longer term military postures.

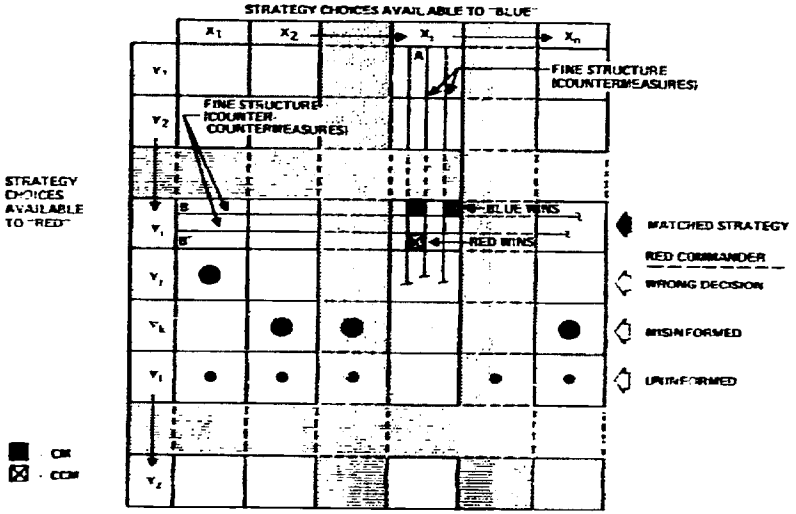


Figure 32. Engagement Matrix

What is proposed here for the definition of weapon system requirements is somewhat less ambitious, but it still represents a considerable effort of imagination.

In our view, the range of strategic choices, as represented by the dimensions of the matrix in Figure 32, should be broadened to cover all possible interactive moves, including those affecting the elements of the *extended* weapon system shown in Figure 9. The time domain pertinent to the use of a hypothetical new weapon system (or to major modifications of the current inventory) should be extended to cover the whole development, deployment, and

operational life cycle. The fine structure of the matrix should recognize the information-flow-related interactions (countermeasures ranging all the way from strategic intelligence to terminal engagement), as described in Chapter 3.

The engagement matrix of Figure 32 should then not only comprise the major strategy choices by both sides (say X_i opposing Y_i), defined mostly by the commitment and assignments of the essential force elements, but also the relevant countermeasure-related fine structure, $X_i^{(1)}$, $X_i^{(2)}$, $X_i^{(3)}$, ... $X_i^{(n)}$ potentially opposed by any counter-countermeasure, $Y_i^{(1)}$, $Y_i^{(2)}$, $Y_i^{(3)}$ ..... $Y_i^{(m)}$. There is no essential distinction between the major matrix cases and the information-related fine structure, but the graphical separation intends to suggest that for most major engagement pairs such as X_i Y_j a large number of subordinate complexions can be generated rapidly and at relatively little expense by exploiting the potentialities of this fine structure. The key fact that ought to be retained is that mismatch within the fine structure may be decisive with respect to the engagement outcome *whenever the major strategy choices of the opponents are reasonably matched*. In other words, it would take a mighty clever countermeasure scheme for a primitive tribe equipped with bows and arrows to defeat a modern army equipped with machine guns and armor; on the other hand, given reasonably well-matched capabilities and strategies, the respective choice of countermeasures may well decide the eventual outcome.

Coming back to the matrix of Figure 32, X_i may be defeated by Y_j, but this outcome may be reversed if the Blue side uses countermeasure (A) within strategy X_i while the Red side attempts to counter-countermeasure (B) within strategy Y_j, not properly matched to (A). If the Red side adjusts its CCM's (B'), so as to match and overcome (A), Y_j may again defeat X_i.

It is fully recognized that these suggestions, which expand the range and increase the resolution of strategy choices, extinguish the faintest glimmer of hope that analytical solutions to the problem of defining optimal strategies, and therefore a well-justified set of requirements, would ever be available in practice. The model in Figure 33 illustrates what would be involved. Fortunately, the very perception of this hyperastronomically complex game structure gives us some encouraging and directly usable conclusions as to definition of requirements criteria.

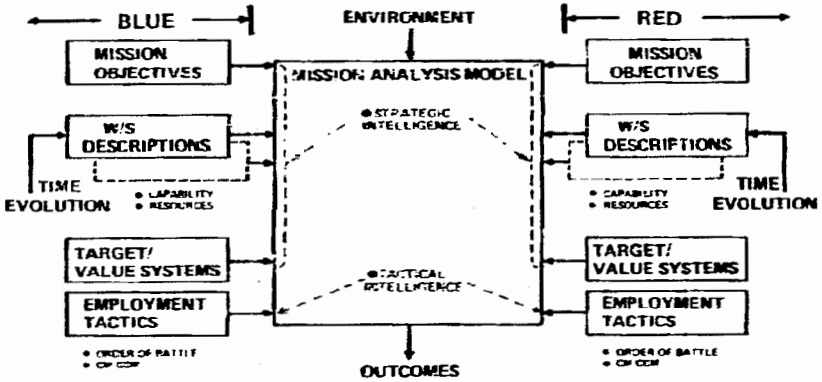


Figure 33. Combat Mission Analysis (Engagement Outcomes)

Criteria for Requirements Definition

It has been known for a long time that in presence of constrained resources and a substantially large number of plausible choices, investment in any particular subsystem characteristic such as range, speed, payload, hardness, etc., must be weighted against the demands and the merits of other subsystems. This process is usually called "balanced system synthesis." In the light of the recognized emphasis on the gaming aspects of requirements definition, two new questions must be raised with increasing urgency and insistence:

1. Will the proposed new system characteristics offer additional opportunities for implementing new and attractive strategy choices to the friendly side, or will they simply allow quantitative improvements in the performance of known missions according to known operational doctrines?
2. Will the proposed new system characteristics offer new and attractive strategy options to the enemy or will they, on the

contrary, eliminate one or several of the important strategy choices currently available to him?

The criteria proposed for requirements definitions reflect systematic primary preoccupation with these questions.

Requirements of the Extended Weapon System

The general criteria set forth in the following sections are applicable to all elements of the extended weapon system as defined in Chapter 1. In particular, the vulnerability to counterattack and to information-flow-related countermeasures of the weapon/platform links, weapon/platform-command structure links, navigation references, surveillance, target acquisition, and other ancillaries should be considered. When the constituents of the extended weapon system are not subject to unique procurement or operating agency, interface characteristics must be specified and accepted as constraints on the weapon system performance.

Multiple Complexions

It is recognized that one of the major difficulties the enemy faces in preparing his winning strategy is to know at any given time what we might be doing or capable of doing. So the range of our choices, including the proposed new acquisition and the use of all other components of the currently planned inventory having to bear on this particular mission, should be based on a very large number of strategy options. In other words, our game should be "multicomplexioned."* For major missions, the total resource investment should be distributed among several independent systems all available to the military command responsible for the mission but all calling for generically different reactions by the enemy. Information-flow-related countermeasures should be considered as part of individual system complexions.

While this need was always essentially recognized for general-purpose missions (conventional tactical warfare), applications to strategic offense deterrent forces are being questioned to some extent by those who advocate sole reliance on (say) sea-based nuclear strike weapons.

For future weapon system procurements, the need for a large number of strategy options is likely to result in more development and modification programs, each leading to relatively limited production runs. While this trend may increase the burden of procurement and ownership cost (in particular the cost of training and maintaining specialized military personnel), the cost disadvantages are likely to be more than compensated by the operational superiority in terms of overall mission performance capability.

Critical Aim Points

When defining a new or modified weapon system concept, it may be assumed that each element has been specified as representing the obtainable performance levels within reasonable state-of-the-art projections. Presumably, the system designer will also have attempted to include novel features that offer new strategy options to the friendly side, as contrasted to just quantitative improvements.

The system concept must then be critically reviewed from the viewpoint of presence of high-value and vulnerable critical aim points in the light of the broadened definition of counterattacks and countermeasures over its whole development, procurement, and operational life cycle. The threat against such potentially critical aim points should be assessed with realistic growth projections in the enemy's technical preparedness and resource availability. Should the individual engagements show preponderance of unfavorable outcomes, the system concept must be correspondingly modified. In simple words, if an easy application point for enemy action can be found in the system, it must be eliminated preferably at the concept formulation stage.

System Development Dynamics

Because of the large choice of plausible strategies and complexions within the systems potentially aimed at countering our missions,

* The Triad concept of strategic deterrent forces was consciously, albeit intuitively, based on the recognition of this principle.

it is hopeless to expect a system, as a matter of fact *any system*, to reliably and over a significant period of time consistently defeat the informed initiatives of the enemy. This has been well recognized in the past by the military in the classical threat-requirement-development-procurement-upgrade cycle but is implicitly ignored in many arms limitation related discussions. In particular, when it comes to hardware design choices, systematically selecting desirable but expensive technical characteristics bordering on the projected state of the art may be unnecessary or even self-defeating if, following responsive changes in the opponent's development programs, it locks us into a basically inferior posture. A classical example was the investment in battleships during World War II at the time when the evolving threat of carrier-based aircraft was already well authenticated. Similar questions may arise in the future in regard to aircraft carriers in presence of multiple target acquisition mechanisms and long-range strike missiles.

The timing of our development programs and the corresponding resource and technology investment levels must be defined relative to a time window open until the opponents have found a way to exploit the appropriate countermoves permitted by their state of development.

Tactical Flexibility

Assuming that the enemy has been successful in marshalling the appropriate resources and that at the same time his information is adequate to pursue a winning strategy, we may elect to switch our next move (i.e., our instantaneous* posture) at a rate that exceeds the response rate of the opponent. Stated otherwise, our initiatives based on design features built into the system are faster than his reaction cycle; we change our posture before he can interpret and react effectively. This feature is usually referred to as "flexibility." Here again, the opportunities offered by manipulating the information available to the enemy in the sense of countermeasures and counter-countermeasures may be of considerable value.

* "Instantaneous" means rapid in comparison to typical event frequencies, as shown in Figure 27. Actual duration of the posture change may take anywhere from years to microseconds.

Information War Aspects

We have seen that the "outcome" of engagements is vitally determined by the information respectively available to each of the two sides to evolve their respective decisions as the engagement unfolds. Let us be reminded once again that the "engagement" includes many years of development, testing, production, and deployment, as well as the actual operational mission. To overcome the opponent in the actual conduct of the hostilities, we have understood that another war is being conducted with the dual purpose of exploiting the full spectrum of information that can be extracted from the opponent's weapon systems (and, by extension, his strategy choices and tactical moves) and at the same time preventing him from exploiting information sources in regard to our own weapons, strategies, and tactics that we are unable to suppress. The need for systematically recognizing and exploiting this *information warfare* as superimposed on, and intertwined with, the more visible physical aspect of military preparedness and combat operations is perhaps the most important message of this study.

In order to degrade the information flow forthcoming from our own military posture the conceptual options are as follows:

- Increase the total volume of the information to be collected, transmitted, and processed. This can be done by increasing the nature and the number of our strategic choices. "Multi-complexioned" systems offer this characteristic automatically to a high degree. The fine structure of countermeasures should be considered as an outstanding opportunity to increase the number of available "complexions."
- Reduce the enemy's access to our *true* information flow by means of security and interference measures. Security will prevent the enemy from tapping our information lines, or, having succeeded, he will not be able to extract useful information. Interference means injecting noise or other signals into enemy information links in order to reduce intelligibility or increase the error rate.
- Actively inject highly credible but false elements into the enemy's information channels with the hope of misleading,

or at least saturating, his means for intercepting and interpreting the messages to his advantage.

If the information flow available to the enemy is substantially degraded, two simultaneous or alternative results are achieved, both beneficial to the friendly side: (1) The enemy will realize the inadequacy of his knowledge and, because of this uncertainty will refrain from aggressive military action, (2) Realizing his state of ignorance, he will spread his resources in order to cover a considerable range of our strategy choices, weakening thereby the chances of overcoming most of them.* Even better, (from our standpoint, that is) if deception is successful to the point that the enemy concentrates on a strategy not effective in countering ours, his defeat is virtually assured.

Impacts on Future Weapon Developments

Corresponding to the requirement definition criteria of the preceding section, a few predictions may be made regarding expected changes in emphasis in future weapon system developments.

Increased attention will be given to the elements of the extended weapon system as defined in Chapter 1. Those external elements under the control of the system designer will receive increased protection against counterattacks and countermeasures to a degree consistent with their role and value in the total system performance. Hardening, dispersal, mobility, redundancy, and suppression of observables will be utilized in combination.

The use of target-connected observables for high-accuracy terminal guidance of missiles will be avoided whenever possible. They are likely to be under the control of the enemy and therefore amenable to relatively inexpensive countermeasures.

A trend away from high-value concentrated mobile platforms will be observed. This will affect Navy surface ships and airborne weapon platforms as well as airborne command and control nodes.** Instead of large high-performance vehicles, of necessity procured in small numbers, we expect future systems to rely more on the combination of mobility and dispersal. A number of relatively small, possibly unmanned, platforms will be synchronized by means of secure wideband data links and will cooperate with the envisioned airborne and shipborne surveillance, warning, target acquisition, command and control, and weapon delivery tasks.

The trend toward dispersal of the major weapons systems components will, in addition to survival and protection against countermeasures, favor the introduction of multiple complexions. When a large number of cooperative elements are at hand, designing into the system relatively small but significant individual differences becomes possible. Modification programs, in order to overcome the reactions of the enemy, can be defined in advance for specified portions of the "distributed" weapon system and can be considered in the assessment of system life-cycle costs.

Detailed design features favoring multiple complexions and rapid changes in the field even during actual combat operations will be emphasized.*** For instance, when future emplacements for ICBM's are being planned, the avoidance of conspicuous and predictable observables may become a consideration. If terminal homing of RV's attacking the ICBM bases is within the enemy's capability, each aim point should have a different, and possibly time-variable, signature. Frequency hopping and frequent changes in modulation processes are already standard means of protection against compromise and jamming; they will become far more widespread,

* It is part of the information war to take all necessary steps proper to insure that the enemy fully realizes his state of ignorance.

** The high asset concentration represented by the Trident weapon system must be seen as an anomaly in this respect.

***An early example was the attempt in the mid-1960's to design multiple reentry vehicles of widely variable optical and radar observables. Conceivably, reentry systems could have been engineered to set the penetration tactics prior to launch or even prior to post-boost dispersal. Operational implications have rendered this approach impractical.

particularly in communications systems using a large number of "subscriber" nodes. The SEEK-BUS project and technology is a step in that direction.

Early consideration of the potential of information-related countermeasures will result in the use of disruptive and deception techniques at many points in the weapons' life cycle, as well as protection against the use of these same techniques by the enemy. All phases of the life cycle, specifically including the development, procurement, deployment, pre-mission, and post-mission phases, will receive CM/CCM scrutiny from the conceptual phase and onward.

The systematic use of strategic and tactical intelligence and counterintelligence for the purpose of improving the cost effectiveness of future weapons may require additional analytical efforts and concomitant development of hardware.

Considerable efforts will be invested to improve, simplify, and automate the signal analysis techniques, especially in regard to the end-game countermeasure, CCM, and tactical intelligence. Equipment will be developed to improve the effectiveness of human interaction with most of the information-war-related functions. (Technology applications to *strategic* intelligence and counterintelligence are conceptually possible but not sufficiently known to the writer to make prognostications.)

Having developed some measure of understanding of how humans make decisions in those situations, the CM/CCM and tactical intelligence related equipment will be increasingly automated. It will insure that human operators can retain management and overview responsibility but will not be involved in the detailed analysis and actuation details on a near-real-time basis.

Equipment for training people to handle various aspects of information war will be required, in particular for the training of military personnel with different cultural backgrounds. Skills and equipment required for the transfusion of military capability to foreign nations should be included.

Finally, in the context of the information war, it should be recognized that while political negotiations, national defense budget allocations, and scrutiny of intelligence activities do serve major national purposes, the widespread and detailed publicity given to weapon system performance and to operational employment tactics may significantly detract from the military value of the U.S. force structure. Coupled with the "background radiation" of an essentially open society, the total information flow available to the enemy before and even during hostilities may well frustrate the long-term purpose of some of our defense investments.

(This page intentionally left blank)

5 EXAMPLES AND APPLICATIONS

ICBM Basing and Tactical Flexibility

Land Mobility

The major problem associated with the prelaunch survivability of hardened and dispersed ICBM's is that the aim points for preemptive attack can be acquired with considerable accuracy by means of space-based cumulative reconnaissance. The miss distance of a weapon aimed at a fixed silo is thus mostly determined by the system errors rather than by the target localization errors. In view of the projected weapon yields and guidance accuracies, there is a tendency to credit the U.S.S.R. with high single-shot silo kill probability by the mid-1980's. Considering the ICBM's in a counterforce role, an argument can be made to the effect that the introduction of MIRV's on both sides offers incentives to first-strike action. If N_1 and N_2 are the respective numbers of warheads per launcher of the opposing forces, one fully successful missile used in a counterforce mode by one side may eliminate the threat to $N_1 \times N_2$ of its launchers. It is not surprising then that new basing concepts are being eagerly explored, the well-established performance levels of fixed-silo-based ICBM's in terms of reliability, accuracy, and low O&M costs notwithstanding.

Land-mobile concepts rely on various combinations of mobility, deception, and hardening. Deception is usually embodied in some redundant weapon shelter concept, which forces the enemy to target all shelters (including those not then containing a weapon) if total destruction of force is desired. Mobility protects the shelter concept against compromise by changing the weapon locations at variable time intervals, preferably much shorter than the enemy's assumed intelligence/targeting cycle. By hardening to a sufficently high level the individual shelters, the alternative of pattern bombing the whole deployment area is rendered unattractive to the enemy.

The land-mobile concept responds to some of the requirement criteria discussed earlier:

- It adds a new "complexion" to the U.S. land-based ICBM force.
- It attempts to deny *real* aim points; the enemy must expend his RV's to attack many shelters *not* containing missiles.*
- It protects the aim-point denial feature against compromise by means of cumulative intelligence. Moving the weapons from one shelter to another forces the opponent to either rapidly update his targeting information or to accept the penalty of aiming his weapons at a large number of (mostly empty) shelters.

The success of such land-mobile deployment hinges in the shelters having no easily identifiable signature.** In particular, no differential signature should be associated with the presence of missiles. The missile transporters themselves must have much reduced observables or must be effectively decoyed by dummy transporters if they are not to be identified and tracked by space-based surveillance. Surreptitiously placed seismic transducers have been mentioned as a possible means for detecting the movement of transporters.

The throw-weight penalty exacted on the enemy by the preemption of deceptive land-mobile based system is strongly influenced by his warhead yield/accuracy/cost trades. For this reason, if conspicuous observables remain associated with the shelter location, the system cost for a given level of survivability may be prohibitive. Based on the high signal-to-noise ratio, reliable shelter signature, the enemy may develop a "responsive threat," such as

* In common parlance, we "buy" one Soviet reentry vehicle at the cost of one credible shelter. Detailed conceptual and design factors decide whether this is a cost-beneficial transaction.

** The cost of shelter hardening and of transportation are assumed sufficiently low for acceptable cost/benefit trades. This assumption has not as of yet been fully supported by detailed investigation.

a low-yield, high-accuracy terminally homing weapon specifically aimed at countering the deceptive land-mobile concept. In other words, by failing to control, suppress, or otherwise countermeasure the target signature, *a possibly attractive strategy option is being offered to the enemy.*

The initialization of missiles having recently entered one of the shelters may not be assured within the accuracy required for hardened aim point kill capability. If external navigation references are contemplated for in-flight updating, their own vulnerability must be taken into account to a possible enemy first-strike.

Air Mobility

The basing of long-range strike missiles on aircraft has been suggested [5] as a means for overcoming possible threats to the survivability of the U.S. land-based ICBM forces. In the air-mobile ICBM concept, the carrier aircraft and the associated tankers are dispersed in peacetime over the continental U.S. airbases. Following tactical warning, the aircraft are scrambled and proceed to reach "orbit patterns," those routes or areas appropriate to possible weapon launch under positive control of the National Military Command. If the mission is recalled, the carriers return to their bases and are readied for the next "scramble."

At first glance, the air-mobile basing concept offers attractive solutions to some of the requirements suggested in Chapter 4.

- It is a different complexion for carrying out the strategic deterrence mission. As such, it forces the enemy aiming at a first-strike capability to conceive, develop, and deploy a generically new and different surveillance, command/control, and weapon delivery system combination that is not expected to be within the state-of-the-art until the late 1980's.
- The characteristics of the communication links permit data transmission rates compatible with secure command/status/retargeting requirements over long distances.

On the other hand, a certain number of conceptual features will require substantial further thinking before the air-mobile basing can be accepted as a reliable, cost-effective new component of the deterrent force.

- The reliability and time delays associated with tactical warning must be ascertained. In particular, the warning against a large number of submarines present within short time-of-flight missile ranges from the centrally located U.S. airbases remains marginal.*
- The carrier aircraft and tanker survival depends essentially on their location not being known to the enemy. The progress in space-based and other long-range surveillance as applicable to high-flying aircraft must be ascertained.
- Discrimination based on infrared signature and tracking must be evaluated as a possible means for acquiring aim points for a possible preemptive attack. Conversely, the means of reducing or decoying signatures should be given emphasis in selecting the carrier aircraft.
- If accuracy compatible with hard-target kill capability is required, the navigation references associated with air launch, whether updating the platform or the individual missiles, must be evaluated from the viewpoint of vulnerability to preemption.
- The concept may prove to be vulnerable to some of the more subtle aspects of the information war. The enemy may protract the period of tension until a substantial fraction of the air-mobile force has exhausted its airborne endurance, refueling included. The turnaround period on the ground then offers a "critical aim point," where a large number of intrinsically soft, high-value weapons can be destroyed.

---

* Continuous airborne deployment has been mentioned as a means to avoid reliance on tactical warning. Except in periods of extreme tension, the fuel consuption rate and the safety problems associated with continuous airborne deployment are considered prohibitive.

Improved Silo Deployment

If the U.S. strategic deterrent force is to be augmented in the relatively near time frame, the existing logistics base of the Minuteman system offers significant cost advantages. The volume of the current silos, upgraded in hardness, allows deployment of missiles with a throw-weight and accuracy combination resulting in much increased lethality with respect to the currently planned ICBM force. Such force augmentation is thought to be compatible with the constraints fo the arms control agreements currently being negotiated. It also satisfies an apparent requirement for strike capability against hardened targets. With the augmented lethality of individual missiles, the fraction surviving a hypothetical preemptive attack must remain a major factor in the enemy's thinking.

Other solutions are being proposed to improve silo survivability. Technical concepts have been explored purporting, after suitable developmental confirmation, to assure at relatively low cost the ability to withstand the impact of several megaton yield weapons at miss distances measured in small fractions of a mile. Based on the conclusions of Chapter 4, some caveats must be voiced in regard to the development path of this "superhardened" silo concept. Assuming that the technical features of the superhardening are confirmed, strong emphasis should be given to the concealing of the aim-point location. Ways must be found to avoid localization from spaceborne sensors and also to prevent other intelligence channels from establishing the silo positions to better than a few miles' accuracy. Failure to do so would result in the new silo type being threatened by new "responsive" RV developments, not necessarily requiring radically new technology or imposing insuperable constraints on the enemy. The use of soil-penetrating unexploded reentry vehicles, fuzed to sense missile launch signals, has been mentioned in this context.

If proliferation of silos is permitted, thought should be given to additional dispersion with specific attempts at denying the knowledge of aim points to the enemy. Natural or man-modified sites could be prepared in relatively large numbers at moderate unit cost with missiles* deployed and moved around by means of soft transporters only in periods of crisis.

Since the proliferation of silos may not be permitted, an alternative is to prepare and hold in reserve self-contained elements of active hard-point defense. Assuming that the enemy threat to the ICBM's is the relatively large close-in surface burst, then short-range, high-firepower, automatically controlled interceptors may offer a chance of silo survival. Tactical quick-change flexibility could be insured by changing at variable time intervals the deployment of hard-point defense elements in the vicinity of selected silos. The enemy's first strike is presumably not informed about the then current deployment of active defense resources; he must therefore attack every silo with the assumption of maximum defense capability.

Tactical Flexibility

A number of recently introduced factors has led to doubts about the so-called "classical" theory of the use of strategic weapons. This theory is based on predetermined tactics that are not keyed to the perception of the unfolding engagement. In the words of Gustavson [6], the engagements are seen as relatively simple first-order interactions, with no dynamic response planned or expected on either side. Measures of utility are survivable nuclear throw-weights, and the fraction of surviving industrial production or civilian populations.

Among the relatively new elements, the advent of sophisticated global surveillance, rapid and reliable command and control, and fast-reaction weapons create a potentially very different type of engagement. If, furthermore, arms limitations agreements result in similarity and gross parity in deployed systems, an increased emphasis on operational innovation may be necessary [6].

---

* These missiles, encapsulated if necessary, would become the "launchers" specified by the arms control agreements.

Many consequences are expected of this evolving situation; among these, the attacks and countermeasures aimed at the ancillaries (surveillance, navigation, and C&C elements) and the possibility of multiple-channel credible warning, coupled with quick launch, fast-retargetable ICBM's, are likely to fundamentally affect the force postures and operational doctrines of the adversaries.

The relationship to what in previous chapters was defined as the information war is clearly apparent. The ICBM engagement scenarios emphasize more and more choices and options based on information that becomes available as the battle events unfold. The information flow within and between the opposing extended weapon systems as well as that taking place within and between the opposing national command structures is likely to become even more vital to damage limitation and conflict termination. All participants will perfect and protect their respective information systems; most information channels will be degraded or exploited by the enemy. The communication links most likely to remain immune from intentional degradation are those that insure conflict termination capability for all sides.

Strategic Undersea Warfare

In this section, the offensive and defensive aspects of undersea warfare are examined as they apply more particularly to nuclear missile-carrying submarines in the 1980 to 1995 period.

Fleet ballistic missiles are generally being considered as the mainstay of the U.S. second-strike retaliatory forces. As such, they command impressive support of the U.S. Navy, the Department of Defense, and even of those responsible for articulating our arms limitation policies. This support has been translated in continuing investments in improved submarines and missiles over the past 20 years; there are strong reasons to believe that the rate of investment will remain high in the next decade or so.

Nuclear missile-carrying submarines are generically different from other weapon systems in some essential respects:

1. They are deployed in international waters, in areas not effectively under our peacetime military control, where neutrals and adversaries are potentially present and engaged in both military and commercial activities. The enemy, intent on threatening or attacking a submarine, may use several air, sea-surface, or subsurface units in combination. The submarine must remain isolated in most scenarios unless it wants to expose its only defensive weapon (concealment) to possible compromise.
2. The submarine, as a weapon platform, is structurally vulnerable. Lethal radii compared to typical miss distances for both conventional and nuclear warheads insure relatively high single-shot kill probability.
3. The submarine, containing up to 24 missiles with each carrying up to 10 warheads, is a highly valuable aim point; investment in preemptive capability against the sea-based weapons is economically warranted *if the target localization problem can be solved.*
4. The secure communications to submarines from the command structure is severely restricted in data rate. The submarine cannot receive (and even less transmit) at higher radio frequencies without compromising its concealment.

It is apparent that the submarine basing is attractive only to the extent that its concealment from enemy surveillance and tracking can be assured. The theme of the discussion here is that, in view of the expected progress in undersea surveillance technology and capability-in-being, submarines will have to resort increasingly to protection by other means, in particular to those derived from information-war considerations. As matters now stand, submarine-based strategic missile systems fail to measure up to just about every one of the requirements criteria discussed in Chapter 4; *the mission success probability is narrowly contingent on a single technical feature.*

The discussion emphasizes submarine vehicles as manned missile-carrying platforms. Other forms of undersea warfare, including those using unmanned vehicles and fixed or mobile mines, should be considered as implicitly covered by most of the conclusions.

Missions and Requirements

The general nature of the offensive and defensive missions is shown in Figure 34. Major powers consider the missions aimed at protecting their submarine forces as legitimate and desirable; there is no such broad acceptance of the offensive missions aimed at hostile submarines. The latter are regarded in some quarters as destabilizing the strategic deterrent balance and are thought by some to be incompatible with arms control limitations. Within the U.S. Navy, some ambivalence can be observed. To admit that the offensive threat to the submarines is serious (which is the rationale supporting most of the strategic USW) is at the same time equivalent to questioning the survivability of the U.S. sea-based deterrent (a high-priority USN mission).

In Figure 34, the individual missions are shown separately since the detailed technical requirements may be quite different. The actions related to preemptive strike and to surreptitious attrition take place essentially in a peacetime environment and may use nonsurvivable ancillaries. On the other hand, quick-reaction counterforce (QRCF), damage-limiting (DL), and interference with command/status communications may have to take place in a battle environment.

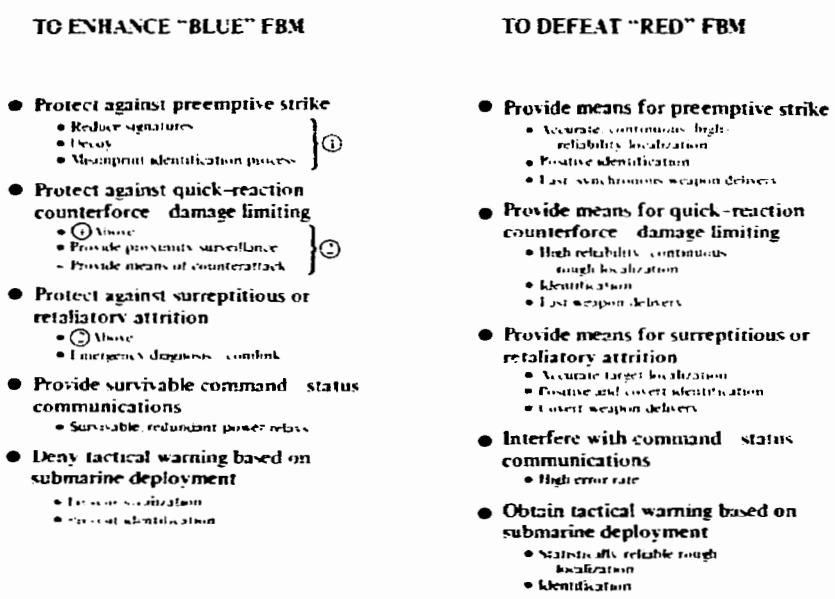


Figure 34. Strategic USW Missions and Requirements

In spite of the differences in detail, there is strong mutual support between the capabilities related to the individual missions. In particular, the statistically reliable rough localization capability, which one side may wish to develop in order to obtain tactical warning to protect other components of its forces, may be construed by the other side as a major step in the direction of acquiring preemptive capability. Further complicating factors arise from the strong interplay between the general-purpose forces (tactical) and the strategic aspects of undersea warfare.

Preemptive Strike—The mission objective is to destroy the enemy nuclear submarines before they have engaged in any overt hostile action. Meaningful preemption must be successful against a large fraction of targets; 90% is considered only marginally adequate.* The following types of mission scenarios are contemplated: (1)The weapon carrying platforms are dedicated to the mission and are within delivery range of the targets; (2) A fraction of long-range strategic missiles is continuously targeted to cover the enemy submarine force. In both cases, reasonably accurate target localization with positive identification is required over most of the targets. The preemptive strike being presumably part of a broader first-strike action, arrival on target of the weapons should be preferably simultaneous with those attacking other components of the strategic strike forces.

The enemy has no way to react prior to the start of the preemptive strike. If detected early, or if tactical warning is received from other sources, fast launch-on-warning may be the only real counter-

* This figure may be much lowered if complemented by ABM and/or civil defense measures aimed at further reducing the damage to value targets.

move. All countermeasures aimed at defeating localization and identification will, however, effectively contribute to negating the preemptive potential.

Quick-Reaction Counterforce and Damage Limiting (QRCF/DL)—The mission objective is to destroy the submarine (counterforce) or the missiles (damage limiting) immediately preceding or following launch. The difference with respect to preemption is that this mission must take place within a fraction of a minute following some enemy initiative. The capability and the deployment necessary to accomplish the mission must therefore continuously and *overtly* be available in peacetime.* The overtness feature is thought to promote deterrence, although examined from another viewpoint it may be considered as threatening its stability. In periods of higher defense readiness conditions, presumably proper enabling procedures would allow the QRCF/DL mission to take place with the concurrence of the National Authority; the command and return link must be extremely well protected if near-real-time weapon release permission is envisioned.

Owing to the short available time period for weapon delivery, the QRCF/DL platforms must be in the close vicinity of the target submarines. Counterattack by the submarine prior to launching its strategic weapons must be considered in defining the QRCF/DL requirements. Overall probability of success must be in excess of 90% of deployed submarine force of the enemy unless, as mentioned earlier, ABM and civil defense measures contribute to damage limitations.**

All three platform modes (aircraft, surface ship, and submarine) are expected to make sufficient advances in the next 5 to 20 years in terms of range, speed, endurance, and self-noise to suggest reasonable cost trades for the QRCF/DL mission. Among the platform-related advances, the use of small attack submarines and of ocean-going hydrofoils appear to hold considerable promise. The possible use of ship- or aircraft-based lasers as boost-phase missile killers should be seriously considered.

Among the major technical problems associated with the mission is the need for highly reliable, continuous rough localization. The identification function is important, although perhaps somewhat less stringent than in the preemption mode. The enemy, of course, will attempt all the countermeasures aimed at defeating detection, localization, and identification. In the case of this particular mission, the submarine may even use *passive* proximity surveillance in order to structure the terminal engagement (including the *intelligent* use of countermeasures) to its advantage. In any event, the QRCF/DL mission, in order to offer any serious probability of success, must rely on the performance of surveillance/rough localization systems. Once having acquired the target, the QRCF/DL units must ensure stationkeeping and reacquisition capability on their own.

Surreptitious or Retaliatory Attrition—The mission objective is to destroy one or several enemy nuclear submarines at the option of the "offense" side in an overt or covert mode. Since only a small fraction of the enemy force is involved, the localization requirements are much alleviated. On the other hand, positive identification must take place, preferably through completely passive means, and, in the covert mode the weapon delivery itself must be surreptitious. Attack submarines, unmanned submarine vehicles, and mobile or fixed mines are the likely platforms for this mission. The interface with the surveillance/rough localization system is mostly to confirm the presence of a likely target in a given area. The opponent's countermoves consist of self-defense weapons and countermeasures such as reduction of active and passive signatures, decoys, and noise jammers. Underwater proximity surveillance appears to be an essential protective requirement if it can be accomplished by purely passive means. ***

---

* Covert QRCF capability is fully equivalent to preemptive posture.

** The well-authenticated Soviet efforts in civil defense lead one to suspect that they may well invest (if they have not already done so) in damage limiting as related to our nuclear sea-board deterrent forces.

*** The threat of overt retaliation against enemy submarines or land-based strategic forces can not be effective against surreptitious attrition. First, the identity of the attacker can not be established with satisfactory level of certainty; second, in an era where "essential equivalence" is accepted in the respective strategic postures of the two superpowers, neither of them can risk escalation to higher level central nuclear war.

Interference With Command/Status Communications—This mission is not usually considered as part of undersea warfare; it is briefly discussed here on account of its bearing on the survivability of the sea-based deterrent forces considered as part of an *extended weapon system* and because of its possible interplay with surveillance.

The technical aspects of the communication links to and from the submarine are intrinsic to the undersea environment. Radio frequencies are rapidly attenuated by seawater; the attenuation loss increases as the square of the frequency and the square of the depth. On the other hand, the protection of the submarine requires effective suppression of all surface-detectable observables such as visual observation, infrared wakes, surface wave patterns, etc. The relative attenuations of the radio signals and observables are qualitatively shown in Figure 35 for VLF, ELF, and thermal wakes. [7] If the wake contrast is to be held at or below a given attenuation level, it is seen that ELF communications are possible, whereas VLF, and *a fortiori*, MF and higher frequencies cannot be utilized unless a gain of the order of 40 to 50 dB in signal strength can be provided with respect to ELF. This would require powerful relays distributed in the near vicinity of the submarine deployment areas.

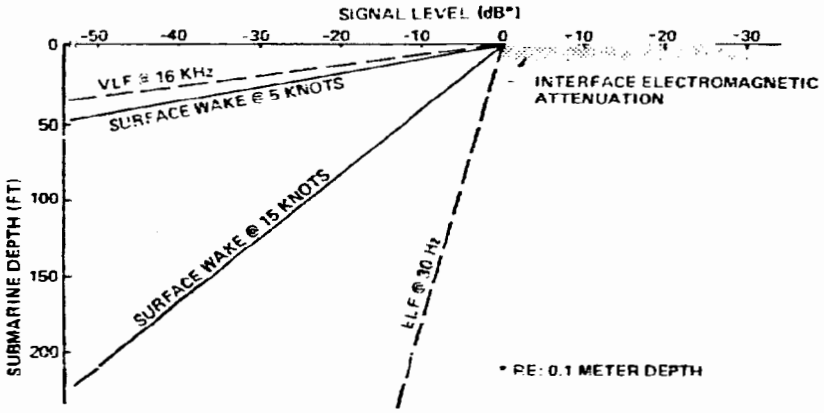


Figure 35. The Submarine Dilemma (Communications Versus Observables)

If the approximate location of enemy submarines is known, the competition with the communication signal becomes possible on a power-level basis. In simple terms, if a jammer can be located for example at 20 nmi from the receiver and competes with a transmitter 1000 nmi away with no other protection than modulation, the jammer has an advantage of the order of approximately 68 dB.

To overcome such power disadvantage, the transmitter/relay has to come closer to the submarine (risking compromise of the submarine location) or must use much increased antijam modulation, which, for a limited bandwidth, means much increased message length. This is marginally possible for emergency launch commands but not practical for high-message-content retargeting data and status return links.

The tie-in with the rough localization capability of the opponent is clear; it allows deployment of jammers in a manner ensuring relatively high power advantage with respect to the far-distant transmitter locations.

Strategic Surveillance and Localization

The preceding brief discussion for all the strategic USW missions has shown the essential role played in most of them by the surveillance/localization capability. It pervades practically all USW missions; in point of fact, even those who would not support the other USW offensive and defensive missions tend to recognize the undersea surveillance/localization function as a required component of the tactical warning system aimed at protecting the soft components of the U.S. strategic forces and C&C structure. We shall discuss the strategic undersea surveillance and localization mission mostly in this context, recognizing its strong relevance to the information war.

The mission objective is to keep track of hostile missile-carrying submarines present within specific ocean areas. The surveillance information may, among other purposes, be used as tactical warning to alert the vulnerable elements of the U.S. strategic forces

and the National Military Command. The mission would at first cover areas immediately adjacent to the U.S. coasts out to ranges of the order of 1000 nmi, since the primary interest is in warning against short-time-of-flight missile attacks against the U.S. mainland. A successful surveillance system would no doubt extend eventually its coverage to other ocean areas.

The mission must be performed over protracted periods of peace and cold war; it should remain viable under wartime conditions, even those directly or indirectly involving major nations in the "conventional" mode. Beyond the nuclear threshold with the participation of major nations, other actions far more drastic than ocean surveillance are likely to take place.

Underwater strategic surveillance should preferably remain covert, although in some circumstances the submarine "situation map" may be publicized for political reasons. The task should be performed with good statistical reliability; i.e., both the leakage rates and the false alarm rates* should be within tolerable limits. False alarm rate (FAR) is mostly objectionable on account of the system processing load; there is no objection, therefore, to relatively high FAR so long as the total number of contacts is small. On the other hand, when the number of contacts is relatively large, it is important that the order of magnitude of true targets be properly ascertained; however, the absolute accuracy requirement on the true target count (leakage rate) can be relinquished to some extent (Figure 36).

Other system requirements include location accuracy of the order of 10 to 20 miles; reaction time** of the order not exceeding a few hours; and the hold ratio*** in excess of 70 percent. There is a very stringent requirement on positive differentiation between friend, foe, and neutrals. The communication links associated with the surveillance system should be preferably secure and survivable within the context of hostilities mentioned above. The location accuracy range is critical; if better than the stated accuracy is envisioned, the surveillance system supplies targeting data for preemption that may be objectionable for political reasons.

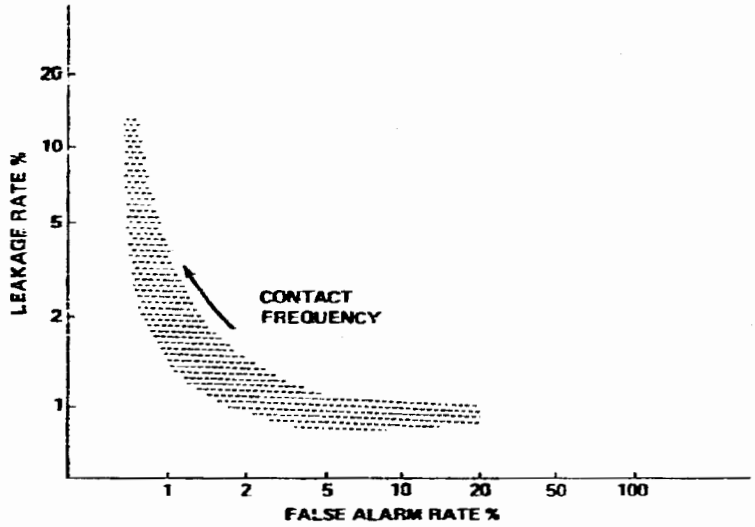


Figure 36. Undersea Surveillance—Statistical Reliability

There are three fundamental problems, all information link related, that render the strategic surveillance task extremely difficult. First, all the observables of properly designed submarines are of low energy density with respect to the ambient environment at more than a few miles and sometimes a few hundred feet away from the source. This is to a great extent true for acoustic observables and magnetic and surface wake**** phenomena. *All the*

* In the statistical sense, leakage rate is equivalent to the rate of incidence of errors of the first kind, namely failure to include an object in the appropriate set. False alarm rate is equivalent to the rate of incidence of errors of the second kind; i.e., inclusion of an object in the wrong set.

** Defined as time delay between the target entering the surveillance area and the first contact.

*** Proportion of time when the correct location information is available for each individual contact.

**** Under favorable sea conditions, wakes allow integration-type processing due to their size and permanency. The sensory instrumentation techniques have only recently come close to being practical.

other effects, without exception, have been found wanting by several orders of magnitude as potential tools in submarine detection. Second, the man-made non-hostile environment is expected to increase with the progress of civilian activities over the open ocean and on the ocean floor. Third, the propagation of acoustic signals up to very recent times was considered extremely unpredictable and, in general, undependable.

For the near future, it may be safely asserted that, with reasonable design precautions, a submarine can effectively discourage heavy investment in surveillance sensor deployments and can also render superfluous other types of countermeasures. In other words, submarine designers have been satisfied up to now with the reduction of the radiated acoustic observables and of the magnetic moment of the vehicle. Other conceptually possible countermeasures have not heretofore received significant development support.

A large number of new developments have taken place recently and are foreseeable in the next few years that are expected to modify the situation quite radically.

The investment in nuclear missile-carrying submarines has been larger than any other single weapon system since World War II. Nuclear submarines are seen by many as the senior partner in the U.S. deterrent forces; with cost increases and additional refinements, the U.S. cost of ownership over 10 years may well be in excess of $100B. Assuming that the enemy wishes to neutralize the submarine threat or at least to make it as vulnerable to counterattack as (allegedly) other components of the U.S. strategic forces, investments of $5 to $10 billion over half a decade appear perfectly reasonable.

The sensor and instrumentation techniques have progressed rapidly, and further progress is expected. Underwater acoustic sensors, including beam forming and time correlation, are now available.* Space systems are soon expected to be capable of scrutinizing on a long-term basis the ocean surface at high resolution in the radar, infrared, and optical spectrum.

A number of technological advances pertaining to the survival and the longevity of sensors placed under the ocean are now taking place. Equipment manufacturing and packaging techniques can be envisioned that render subsurface investment cumulative; i.e., instrumentation placed in the ocean will be present and operating when the book value of the investment has long been amortized. We have described in some detail in Chapter 2 the new technology capabilities in peacetime mass data communication and processing.

Conceptual advances are constantly occurring within the ASW community. It has apparently understood and accepted that submarine surveillance can accomplish its primary purpose even though it supplies statistically reliable information only. This concept of *statistical transparency* of the ocean is extremely important. So long as the surveillance system creates a significant degree of doubt at any given time in the mind of the opponent as to whether or not a fraction of his nuclear submarines are under track, it will have accomplished its purpose.

The ASW community fully understands that no surveillance system concept by itself is likely to perform the overall mission efficiently. The solution will in all probability involve the cooperation of several sensor/platform combinations. Submarines represent an extremely elusive quarry; it is, therefore not economically possible in general to concentrate the resources required for proximity detection. The solution is likely to involve long-range sensors that can establish approximate location of fast-traveling submarines. Space-based sensors will supply near-surface detection and discrimination against surface shipping. A certain number of fixed-area or barrier-type moored sensors will detect the submarine with a relatively high degree of probability in critical areas. Deployable underwater sensors, properly vectored by aircraft, ships, submarines, or even unmanned undersea "tractors,"

* The cumulative gain due to directivity and time correlation permits adequate discrimination levels for signals more than 65 dB below the isotropic broadband ambient background under reasonable prevailing conditions.

will agglomerate in the vicinity of suspected targets and locally increase the accuracy and hold periods of surveillance coverage. This concept of *adaptive deployment* is expected to hold the key to mission feasibility and practicality.

For all these reasons, we believe that the fear of increased susceptibility to detection will force the submarines to engage in a number of countermeasure-type actions. Among these, the creation of a large number of false targets by means of physical decoys or by synthetic signatures; reduction of the active acoustic radiation and of the sonar cross-section; the dispersion of submarine force in much smaller units, each carrying a relatively small number of missiles; and finally, the systematic misimprinting of the enemy's signature library, will be explored and probably applied.

One of the important features of submarine surveillance is that the performance capability of the opponent cannot be assessed on the basis of reliable tests or observations. There is a strong possibility of surreptitious development. The enemy may develop and test separately all the critical elements. Then, having achieved a high confidence level, he can train the corresponding personnel and store the hardware until political developments warrant its unveiling. At that point, especially in view of the strong interaction with the QRCF/DL, or even preemptive capability, strategic surveillance potentially represents a strong winning move in the evolution of hostilities.

Tactical Air Combat

Since the first military applications of aircraft, the state of the art in tactical air combat has passed through successive cycles, all characterized by some initial breakthrough followed by prompt exploitation by most major nations and eventually by technological stalemate between air strike and air defense. It is of some interest to briefly review the past developments with emphasis on the information war aspects.

In the early years, the aircraft role was mostly reconnaissance. Visually aimed gravity bombs were the principal means for attacking the ground. The ground target areas were protected by balloon barrages and nonspecialized artillery fire. Camouflage was often used to prevent visual acquisition of aim points. Soon the defense means were improved by the use of visually aimed antiaircraft artillery (AAA) and eventually by machine guns mounted on interceptor aircraft. The strike aircraft was forced to increasingly rely on fighter aircraft protection and on improved maneuvering capability for survival. "Dog-fights" between opposing fighter-interceptors were conducted mostly by visually controlled machine guns, with each aircraft being essentially on its own.

Starting with World War II, ground-based AAA was rapidly improving its performance by the increase in firepower and by developments in fire control and fuzing. Acquisition and fire control radars, ground-controlled vectoring of interceptors, and the use of proximity fuzes have increased the attacker's attrition rates to unacceptable levels at hitherto normal penetration altitudes. Strike aircraft, most felicitously helped by the progress of aerodynamics, structural and engine design, were forced to high-altitude penetration. This in turn required automatic bombsights and terrain-mapping radars; the latter has also fostered night attack capability. The use of radars in both attack and defense led to more sophisticated ECM and ECCM. By the end of World War II, the advent of guided missiles ushered in the era where strike aircraft, even supported by powerful fighter forces, could no longer have penetrated a competent ground-based defense without prohibitive attrition rates. For a while, during the Korean and Vietnamese wars, the rapid progress in electronic warfare on the U.S. side contributed to holding down attrition rates to a tolerable level, but by the time of the 1973 Arab-Israeli war, it became apparent that any aircraft flying within the

line of sight of a competent and alerted defense faces considerable odds against successful penetration and safe return.* Battle tactics have evolved to include terrain-hugging low-altitude approach, standoff air-to-surface missiles, aided by a multitude of decoys and penaids with added advantages of supersonic dash speed and high maneuver capability. The strike aircraft has in fact become so concerned with its own survival that the target acquisition function had to be delegated to specialized ancillaries. In the recent past, the air-to-air fight was somewhat closer to balance; while in many cases the interceptors were vectored to the target by ground or air control centers, the target acquisition and weapon delivery functions have remained essentially associated with the aircraft.

The ground-based defense is in the process of catching up with the new offense tactics by developing netted defense sites, very-low-altitude coverage of ground radars, integration with airborne surveillance/control centers with elaborate tracking, IFF, and vectoring capabilities.

The near future developments are clearly perceptible. High-value aircraft will attempt to use antimissile missiles in self-defense unless the advances in radiation weapons leapfrog that requirement. In clear weather, within less than a decade, power lasers are expected to play a decisive role in aircraft self-defense and also in surface-to-air defense and air-to-air combat. In a preponderant number of cases, clear weather prevails over distances of the order of less than a mile. When the combat takes place within the clouds, short-range radar-guided missiles will remain available.

A number of important conclusions can be drawn for both air-to-ground and air-to-air engagements from this rapid overview. When examining these conclusions, one should bear in mind that we focus our attention on the 5- to 20-year future in the context of the technically most advanced military forces. On a worldwide basis, there will be a large number of battles fought with essentially today's and yesterday's technology level. Insofar as first-line engagements are concerned, however, the following conclusions and prognostications appear valid:

1. Direct line-of-sight (LOS) exposure of an aircraft to hostile acquisition and tracking sensors will be avoided at all cost. To prevent or at least to minimize such exposure, aircraft will attempt to *obstruct* the LOS by low-altitude approach; countermeasures such as jamming, chaff, and decoys will be used whenever penetration within a sensor's envelope is required. When radiation weapons enter the inventory, clear-weather engagements will rapidly become unattractive.
2. When direct LOS exposure is absolutely required, the aircraft will strive to reduce it to the shortest possible duration. This will impose further constraints on the two essential functions of the aircraft, namely target acquisition and weapon delivery/guidance. Target damage assessment by the strike aircraft may also be subjected to constraints.
3. Ground-based defense, because of the tactical superiority afforded by direct LOS, will attempt to multiply and disperse its acquisition and tracking sensors. It will establish a synchronized ("coherent") time base among them and, through centralized area command, will use this *distributed* ground-defense network to perceive and to defeat the penetration tactics of the air attacker. This dispersion of the ground resources also affords some measure of self-protection, especially when the individual sensors are mobile or at least transportable.** In view of the lesser weight and other design constraints affecting ground equipment, the ground-based defense has the cost advantage with respect to air attack over relatively limited areas.
4. To overcome the horizon limitations of ground-based sensors and also to help rapid intertheater redeployment, airborne surveillance and tracking technology has already come into existence and will be further emphasized as an essential complement to ground-based sensors and air-defense weapons.

---

* The air-to-surface munitions have also made considerable progress, but the hardening and concealment of ground defense units appears to be a technically more tractable problem than that of hardening or concealing aircraft.

** The distributed mobile-ground-defense-network concept may hold the key to overcoming the sophisticated radiation-locating defense suppression weapon systems.

It is natural for the air component to also assume the role of vectoring interceptor airplanes; from there, the placing of the whole direction of the air-defense engagement within the airborne command center is a short (although institutionally delicate) step.

5. In the face of this impressive panoply of defense resources, the chances of a *penetrating* aircraft appear to be rather slender. Once its trajectory is reliably tracked while flying anywhere within the defense envelope of the interceptors, its survival to the point of accomplishing the mission is seriously endangered. The natural next step on the attack side is then to *stand off*; i.e., accomplish its objectives without penetrating the defense perimeter. This means that the attack aircraft will be designed to *acquire the targets by proxy* and to *deliver/guide weapons by proxy* or at least from a *safe distance* ("standoff").

   The aircraft then, in this view, will increasingly depend on satellites and reconnaissance or surveillance aircraft to acquire its targets; it will use standoff missiles, remotely piloted vehicles, or even fully automated (unmanned) strike vehicles to delivery the weapons. Special mission auxiliary aircraft will be used to carry out ECM, ECCM, and electronic intelligence functions.

In summary, if the above view is accepted as valid, tactical air engagements involving first-line forces of the technically advanced nations are seen as encounters between a large number of offense and defense elements, many internetted sensors, and processing and decisionmaking nodes. These will include aircraft of several types, most of them strenuously attempting to keep out of the reach of the enemy's weapons. The burden of survival and of success will be placed on an *electronically integrated multi-element structure*, as contrasted to individual aircrafts mostly dependent on their aerodynamic prowess, aided by the skill and the heroism of human pilots.

This perception is prototypical of the main topic of this paper. In view of the extended weapon systems involved, the opportunities for information-related countermeasures are numerous, and in some cases, lethal. A few specific application areas will further illustrate the points under discussion.

Pathfinder and Precursor Concepts

Within the last few years, those concerned with the future of tactical air strike missions have become aware of the difficult design trades between aircraft survival, target acquisition, and weapon delivery capabilities. Many approaches have been explored; most of them involve the delegation of some of these functions to vehicles other than the strike aircraft. Two concepts are pertinent for our purposes here.

Pathfinder—An auxiliary vehicle launched from the strike aircraft (unpowered glider, cruise missile, remotely or automatically piloted aircraft) is equipped with the navigation, sensor, and communication gear necessary to acquire the target in near-real time in the coordinates used by the attack system. The acquisition data is transferred to the strike aircraft, which can deliver relatively unsophisticated weapons from a safe standoff range with essentially hitting accuracy.

Precursor—The purpose of the concept is to avoid the exposure of the strike aircraft to the ground defense concentrated in the vicinity of the target. At the same time, the guidance used to insure very high accuracy for the weapons is purported to be impervious to countermeasures while imposing a relatively low cost penalty on the carrier aircraft or on the strike missiles.

The rough target location is assumed to be known from previous reconnaissance. Its signature is assumed to be accessible to remote sensing by aircraft or space sensors. A precursor vehicle is aimed at the approximate target location and dispenses a small number of beacons (3 to 10), which are lodged in the vicinity of the target. The beacons are interrogated by the reconnaissance system and accurately localized within the target area *with respect to the aim points*. The strike missiles arrive soon thereafter and use the

beacons in a *trilateration** rather than in the triangulation mode to generate terminal guidance inputs. The advantages of this "terminal T.O.A." guidance is that the strike aircraft is not directly exposed to the defense and, furthermore, that the terminal guidance pattern, being established on a strictly temporary basis immediately preceding the weapon impact, is secure and practically countermeasure-proof for the duration of the ephemeral operation. Of course, the concept is dependent upon the availability of reconnaissance access to the target prior to the attack.

These two concepts are offered to illustrate two principles related to the information war:

1. The high-value component of the attack (the manned strike aircraft) is kept out of the defense perimeter; penetration is accomplished by unmanned and preferably simple components transferring essential targeting and guidance information to the weapons or to the unmanned aircraft.
2. The terminal guidance beacons have locations and signal characteristics established and revealed for a very short time period only. They represent essentially a rapid posture change, most difficult for the enemy to counter in time before the impact of the strike missiles.

Remotely Piloted Vehicles and Automatically Piloted Vehicles

At first glance, the idea of using a remotely piloted vehicle (RPV) to accomplish an exposed mission appears to be technically and economically sound. It also embodies a rather instinctive desire of the modern military to have automated machines accomplish the dangerous tasks of the war, with the humans preferably monitoring and controlling at a safe distance.

It is basically proposed to have all the sensory and flight-essential equipment on board the RPV, with the human pilot tied into the mission control loop by remote communication link. RPV mission objectives comprise a broad spectrum from reconnaissance through ECM all the way to strike weapon delivery.

If RPV's are designed to accomplish some essential mission, the enemy will develop a responsive threat system to counter them. The RPV's attractive features are dispersion, mission flexibility, and implicit expendability. On the other hand, their essential shortcoming is that in actual fact the contributions of the human "pilot" are sharply limited by fundamental technical trades.

The role of the pilot can be understood from Figure 37. He responds to an extremely broad set of stimuli through six or seven biologically adapted sensors ** coupled directly or though preprocessors to his brain. His brain acts as a storage/retrieval mechanism, a bandwidth compression device, and a rather sophisticated decision box. The output communications, at much lower data rate than the input set, are conveyed to other elements of the extended weapon system, (commander, ancillaries, or subordinates) and also directly to the actuation devices such as flight control, weapon release, and countermeasures.

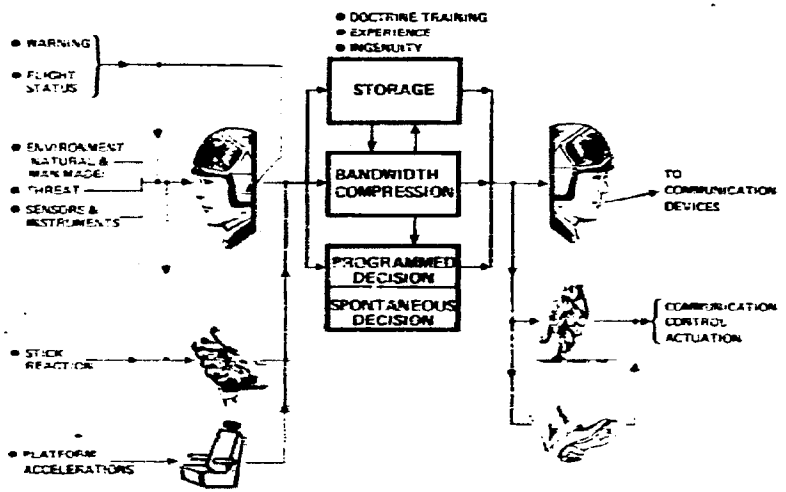


Figure 37. The Role of Man

* Measurement of time of arrival (T.O.A.) of signals in a three-node system.

** Vision, hearing, olfaction, tactility, acceleration, balance, and temperature sensing.

If the human is not physically present in the vehicle, the only way his unique decision capabilities can be made to bear on the mission is to transmit in near-real time *all* the significant information normally available to him directly in his cockpit. Even when aided by a large number of preprocessors, the information required is quite extensive. (A sample display of *one* operator station is shown in Figure 38 for an admittedly high-level weapon system, the B-1 strategic bomber.) To transmit the complete information flow with the required level of security takes an extremely broad bandwidth, not easily affordable in a battle environment involving several tens of vehicles. If the wideband information is not transmitted, then the human capabilities are not really utilized, except for the almost trivial purpose of flight control. Specifically, if the enemy uses active defense or reasonably sophisticated countermeasures, the absence of near-real-time human decision makes the RPV's eminently vulnerable. If, on the other hand, wideband transmission is attempted, a relatively attractive strategy option is opened to the enemy by the vulnerability of such communication links to interference and perhaps deception.

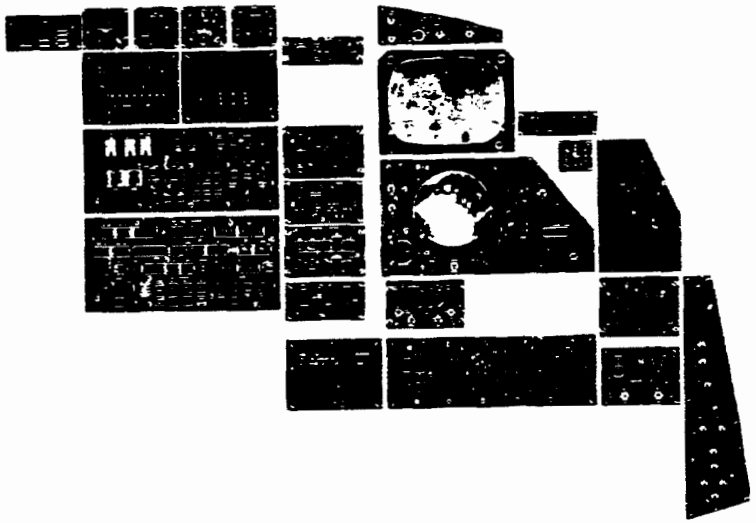


Figure 38. B-1 Offensive System Operator Station

As we see it, the solution lies in much increased automation within the remote vehicle. Specifically, future developments will probably emphasize the automation of all the storage, bandwidth compression, and most of the programmed decisions that are now attributed to the human brain. The actuation functions can be automated as well. The only communications with the "supervisor" or "commander" (emphatically not the pilot) would be related to the nonprogrammable *spontaneous* decisions such as those required in an emergency. Otherwise, the narrowband communication link would primarily carry essential commands and summary status data.

The RPV concept is very much part of the future tactical air combat picture; however, within the confines of the current development focus, it appears to suffer from inherent technical contradictions. As now advocated, with the human tied in by means of wideband data link, it will probably prove impractical on account of its vulnerability to countermeasures and to active defense. The development trend will in all likelihood evolve in the direction of increased onboard automation (Automatically Piloted Vehicles) aided by the promising and rapidly growing microprocessor technology. Vehicle self-defense, evasive maneuver, and ECCM will be part of the capabilities built in the APV's.

Airborne Surveillance and Command Centers

In the past few years, the advent of clutter-free radars capable of detecting and tracking aircraft from a high-altitude airborne platform at several hundreds of miles in range has given birth to a new generation of airborne surveillance and command centers. The Airborne Warning and Control System (AWACS) is foreshadowing future developments of this type. In addition to the surveillance/tracking, communications, IFF, vectoring, and relay functions are being incorporated; they are thought of as components of an integrated air/ground battle command and control system. The detection of sea-surface and land-mobile targets is also being investigated.

There is ample reason to believe that the airborne command centers (ABCC) will play a critical role in future air, land, and probably sea combat. They can assure the integrated command and cooperation of the air-and ground-based air-defense forces and are fully capable of handling most of the sensing, communication, and data processing functions that enable the field commander of a whole theater of operations to make decisions based on up-to-date information. The airborne command center being such an essential element of the overall conduct of the battle, the enemy will quite naturally attempt to defeat it. Counterattacks by means of surface-to-air missiles and by interceptor aircraft with the aid of long-range air-to-air missiles will be attempted. The ABCC will therefore have to invest rather heavily in self-defense, first in its immediate proximity and eventually as part of a complete regional defense structure for the major purpose of assuring its survival in the battle environment. If tactical nuclear weapons are part of the engagement scenarios (and in thought of many, they *are*), the resources devoted to protect the ABCC must be substantial indeed. A significant fraction of the total mission capability may have to be diverted to support the self-defense function.

The opponent may also devise relatively sophisticated counte.. measures. In particular, the distributed, ground-based noise jammers appear to be somewhat of a threat to a single surveillance/tracking aircraft.

The answer is to have several airborne units operate in cooperative and/or multistatic modes. In this manner, the surveillance and command centers can take advantage of multiple vantage points looking at a given jammer source; if *coherent** coordination is assured between the participants, the chances of the jammers being successfully identified, localized, and screened out are much increased.

From the foregoing, the future development trends in airborne surveillance and command centers can be discerned with some measure of confidence. There will be a relatively short period during which the major military powers enter this type of capability in their inventory; both friend and foe will adjust their doctrines and equipment to its presence. Soon, counterattack and countermeasure capabilities will be developed and introduced during training exercises and also perhaps in real-life military engagements of local wars. At first, the AWACS and similar type of systems will respond by developing cooperative and multistatic concepts supported by the corresponding deployment modes. As new aircraft become available in the 10- to 15-year time frame, there is a strong likelihood that the total resources will be distributed in a *larger number of relatively smaller units* so as to permit graceful degradation in the presence of a strong enemy counterattack environment. This trend will enhance requirements for further advances in surveillance/tracking radars, supported by additional sophistication and miniaturization of the processor electronics and human interface equipment.

Future Complexions of Tactical Air Combat

In the past 15 years, two trends have evolved. One has led to an extremely capable and therefore expensive aircraft (strike or fighter) embodying just about all the functional performance offered by the most advanced state of the art and depending on minimal cooperation from external control centers. The operation of the aircraft is almost entirely autonomous; only command and status information is relayed back and forth. On the other hand, the procurement and ownership cost, including the training of pilots of such aircraft, makes it an extremely expensive choice. Also, since it operates essentially alone and is vulnerable, the mission performance will suffer if the opponent has competent countermeasures. In presence of heavy air defense, the attrition rate may not be justified by the results.

---

* Time base synchronized within a tolerance small compared to the shortest period present within the signal spectrum.

The second approach goes to the opposite extreme. The actual strike or defense vehicles are minimum-capability aircraft* associated with a relatively large mothership. Such a mothership may serve also as a command and control center, but more often a separate high-value aircraft is depicted in this role. This approach has the advantage of offering rapid intertheater deployment and lesser reliance on airfields immediatelv adjacent to the battle zone; it also assures that the system will degrade gracefully so long as the mothership remains outside of the combat zone dominated by the enemy air defense. The mothership, because of its size and critical mission role, represents a vulnerable and high-value target. The enemy would obviously concentrate its resources on destroying the mothership well before the individual aircraft are released. If the U.S. structures a significant portion of its tactical air combat capability around concepts akin to the "microfighter," the opponent will most probably reemphasize its long-range surface-to-air and air-to-air interceptor missiles. At the same time, it is not readily obvious that a minimum-capability strike aircraft can survive in a heavy terminal defense environment, including the radiation weapons of the future.

In view of the drawbacks of both approaches, it is most likely that the actual development trend will show a convergence between the two. Individual first-line aircraft will retain for institutional reasons high structural, aerodynamic, and propulsion performance but will have less sensory and onboard countermeasure equipment. On the other hand, they may be mostly utilized in association with relativeiy small C&C aircraft that will be concerned with the overall supervision of the many individual functions of the air engagement. In particular, the C&C aircraft will, possibly in cooperation with space-based ancillaries, accomplish most of the air battle control for a group of 6 to 12 fighter/bomber aircraft; it will designate the targets and insure navigation update to standoff air-to-surface missiles; it will direct the deployment of specialized countermeasure-carrying aircraft; and it will be mainly responsible for the assessment of target damage. The individual aircraft forming the team will contribute their counterattack and countermeasure resources to ensure the survival of the C&C aircraft.

Seen in this light, future tactical air combat embodies most of the features required by the considerations set forth in Chapter 4. Resources are distributed and multicomplexioned; high-value critical targets are mostly denied to the enemy; and the distribution of resources permits increased exercise of tactical flexibility.

Netted Air Defense Versus Antiballistic Missile Defense

In closing the section on Tactical Air Combat, this illustration is offered as an example of deception involving strategic intelligence. It is well known that the differences between a highly competent air-defense interceptor and an antiballistic missile (ABM) defense system are mostly the accuracy and timeliness of target acquisition associated with the individual defense sites. By means of the *netting* of the defense sites and adding nuclear warheads, a competent air-defense system, such as the U.S.S.R. SA-5 for instance, can most certainly be operated as a quite capable antiballistic missile defense system. Publicizing the air-defense mission capability when a relatively inconspicuous addition can transform it into ABM defense is prototypical of deceptive countermeasure attempts against strategic intelligence. This effort may not prove to be successful but may well portend others of the same type, less well understood but perhaps more dangerous.

---

* These range all the way from unmanned cruise missiles to the so-called microfighters. The latter are manned, have about 10,000-lb GTOW, are capable of 200-to 300-nmi combat radius, and can be recovered by the mothership.

6 CONCLUSIONS

The historical, conceptual, and technical bases for the large and growing role played by the information flow in military engagements have been examined. The susceptibility to information-related countermeasures of extended weapon systems involving many remote elements supports the view that such countermeasures will further grow in sophistication and will find many new areas of applications.

- Countermeasures aimed at degrading the enemy's information flow and, conversely, at protecting our own information against enemy disruption or deception; and exploitation for our own purposes of the intelligence extracted from the enemy's information channels are all part of the *information war* superimposed on other military operations. In fact, moves of the information war may be undertaken many years prior to the actual outbreak of hostilities; they also may long remain hidden from the adversary. Viewed in this broad generality, the information war permeates and impacts the whole military posture of the prospective belligerents. This impact ranges all the way from the definition of mission requirements through the development and deployment of weapon systems to the outcome of specific engagements.

- The consequences of this relatively new apperception should be a shift in emphasis among the criteria used to define new weapon system requirements. Explicit consideration of the *extended weapon system* elements, the increased need for *multiple complexions*, the *avoidance* of high-value *critical aim points*, the *dynamic* nature of the *weapon development/ threat-response* mechanism, and the paramount importance of *tactical flexibility* have been identified as part of the modified requirement criteria set. The systematic exploration of the *information war* related aspects of proposed new weapon systems or modifications *in the conceptual stage* has been rather strongly urged.

- Tactical flexibility has, of course, always been part of sound military doctrine, in particular as applicable to land combat operations. The illustrations we have introduced tend to suggest that mostly because of increasingly systematic recognition of the information war concept, tactical flexibility will become a very essential characteristic of other, higher level, engagements. The process has now been well underway for more than two decades in tactical air combat; it has been seriously considered in recent years for strategic nuclear war involving ICBM's and bombers. Strategic undersea warfare will very soon be forced by the progress of technology to call on the merits of tactical flexibility, including the full range of information-related countermeasures.

it is left for future extensions of this study to explore the implications of military space technology for both interference and exploitation modes of the information war. It is also hoped that the future of naval surface warfare will be examined in the light of the conclusions presented here. Counterinsurgency and guerrilla-type warfare have fascinating ramifications that involve all the information war elements we have considered; it is a matter of some regret that no more than a passing mention could be given to this topic within the limits of this study.

Much of our purpose will have been accomplished if the problems of disrupting and manipulating the enemy's strategic and tactical intelligence (as well as protecting our own) attract increased attention of the defense community. In particular, the problem of strategic deception by weapon developments under false mission pretenses should receive rather careful scrutiny.

Before taking leave of the reader, we should summarize what has and what has not been accomplished. Starting from a purely technological observation—the all-pervasive

nature of information flow in weapons and combat operations—the conceptual aspects of countermeasures have led us to define the elements of the information war. The possible impact on the outcome of engagements has been assessed on almost entirely analytical grounds, leading us to suggest a shift in system requirement criteria. A few important areas of applications have been examined, and the specific conclusions have been pointed out.

Rather than arguing in detail the technical pros and cons of the conceptual and technical suggestions brought up as illustrations, we hope that the reader will be motivated to raise a few intriguing questions. Is the information war concept recognized within the U.S. Department of Defense as an essential adjunct to mission and system requirement definition? If so, how are considerations derived from the information war concept reflected in policies, directives, and procurement procedures without destroying the essential merits of our initiatives or countermoves? How does the information war concept relate to arms limitation talks, including the associated inspection or monitoring systems? How does an "open" society, with its emphasis on freedom of information and public scrutiny, protect its interests in a hostile world suffused with long-term moves and countermoves of the information war? In particular, how does civilian propaganda and psychological warfare interface with the problems we have discussed?

As a direct result of this study, we can do no more than hint that these broader questions deserve exploration and that the answers may be of some relevance to our future military posture. Out effort reported here should be considered as an initial foray, conducted from a specific viewpoint and subjected to many limitations.

Appendix A

DECISION RELIABILITY vs. SIGNAL QUALITY

APPENDIX A
DECISION RELIABILITY VERSUS SIGNAL QUALITY

The Decision Process

We shall assume that all information channels associated with the extended weapon system, as defined in Chapter 1, convey messages to be used in some decision process. Figure A-1 shows the logic involved in the simplest model—the single-channel decision. Source S sends the signal to the sensor, which at the same time receives noise inputs uncorrelated with the signal.* The processor is used to enhance the signal characteristics used for the decision. Information predicted or acquired through intelligence in regard to the source characteristics is conveyed to the decision box via a separate "predictor/intelligence" channel, not necessarily operating in real time.** Grossly speaking, the function of the decision box is to compare the message in the real-time "signal" channel (signal + noise) to that contained in the predictor/intelligence channel. The results of the comparison are indicated by "yes" or "no", dependent on whether or not the message is part of a set contained in the reference "library."

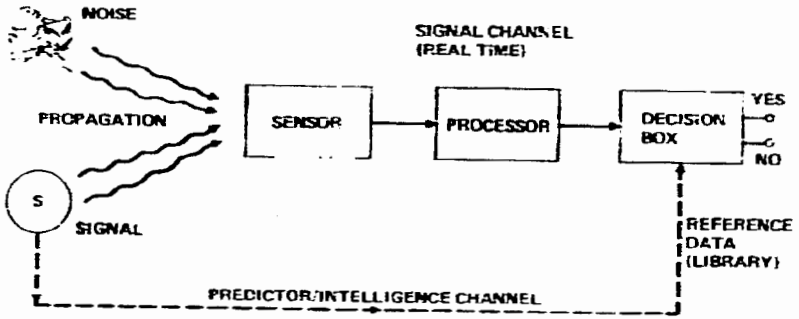


Figure A-1. The Single-Channel Decision Process

* In a communication channel, we would rather speak of the transmitter and the receiver. Those terms are strictly equivalent in the present context to the source and the sensor, respectively.

** No decision can be performed without adequate reference data ("library"). Obtained directly through intelligence or developed by analytical prediction, such reference data takes days, months, or years to acquire, with all the attendant problems of physical protection, systematic retrieval, and perishability.

All messages entering the signal channel are in the final analysis *quantitative* in nature. Theoretically, a message will convey information on the state of a system (target or transmitter); i.e., a point or a small region in the phase space specifying all degrees of freedom of the system. By extension, a word or a coded message can be considered a system, with each information bit representing one degree of freedom of the total system complexion. Messages are thus always quantitative and therefore specifically include all types of analog and digital signals irrespective of the modulation mechanism.

The quality of decision depends then on the signal-to-noise ratios of the message and of the reference, on the relevance and accuracy of the reference information, and on the refinement of the comparison process. The purpose of this appendix is to relate quantitatively the decision quality to its constituent parameters.

Signal Quality

Once we have accepted that each message is composed of signals representing quantities, the signal fluctuation due to noise is given by

$$\sigma = \left(\frac{\overline{N^2}}{\overline{S^2}} \right)^{1/2}$$

where σ is the signal standard deviation, $N(t)$ is the noise, and $S(t)$ is the signal. If the signal is integrated over a period T, the fluctuation is given by the expression

$$\sigma = \left\{ \frac{\int_{\Delta\omega} N(\omega) d\omega}{\overline{S^2}} \right\}^{1/2} \frac{1}{\sqrt{\Delta\omega T}}$$

where ω is the angular frequency, $\Delta\omega$ the bandwidth, and $N(\omega)$ the power spectral density of the noise signal.***

*** Digital signals are in fact analog in physical form; they can be modulated in amplitude, frequency, phase, etc. Their characteristic is to have in general tolerably large individual signal-to-noise ratios and a large number of degrees of freedom by the introduction of artificial coding redundancy. The designation "word" to designate a digital message gives a clue to such redundancy.

Decision Parameters

The magnitude of the signal observed after suitable processing is portrayed in Figure A-2 as a Gaussian (normal) probability distribution. Non-Gaussian distributions are not treated in this analysis.

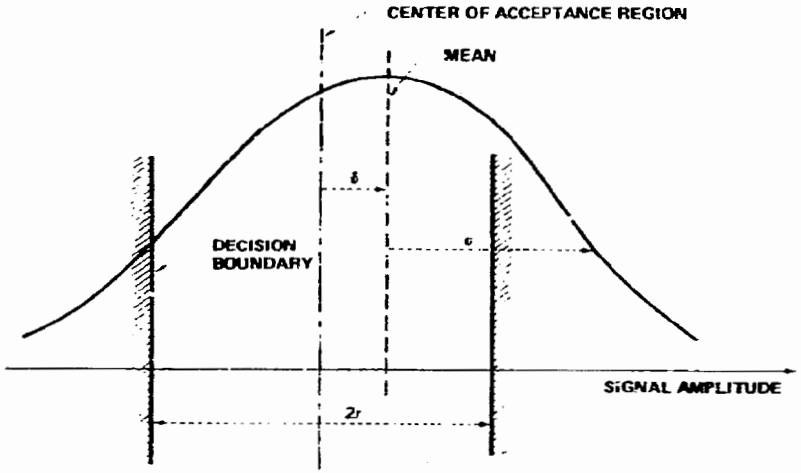


Figure A-2. Probability Distribution and Elements of the Decision Process

Two parameters fully specify the decision process:

1. The *acceptance domain*, 2r, arbitrarily set as part of the decision logic. It defines the boundaries within which the signal will be *accepted* to generate a "yes" output. Outside of the acceptance domain, the signal will be *rejected* to generate a "no" output. At a first glance, it might seem advantageous to use relatively small acceptance domains since presumably to should discriminate against undesired (false) signals. But if the true signals—those we wish to accept—are strongly fluctuating in the presence of noise, we may reject a large proportion of signals that ought to be accepted.
2. The *bias* or *displacement* δ expressed as a multiple of σ is the difference between the center of the acceptance domain and the mean value of the signal. If the reference obtained from the predictor/intelligence channel is accurate, δ should be very small. We should hope, on the other hand, that the enemy's bias is rather large, since the enemy's intelligence in regard to our information channel should be of lesser quality than that of our own intelligence. Both decision parameters r and δ are expressed as multiples of the signal standard deviation σ.

Acceptance Probabilities

The quality of individual decisions can be characterized by the matrix of probabilities.

Decision	Signal	
	True	False
Yes	P_{11}	P_{12}
No	P_{21}	P_{22}

Out of the four parameters shown, only two are independent. We choose to define P_{11} as "*justified* acceptance probability"; i.e., the probability that a true signal will be interpreted as such (produce a "yes" decision). We define P_{12} as the "*unjustified* acceptance probability"; i.e., that a signal which ought to have been rejected as false is being accepted as true (produce a "yes" decision). These expressions are sometimes described as errors of first kind (P_{21}) and errors of second kind (P_{12}). Obviously $P_{21} = (1-P_{11})$ and $P_{22} = (1 - P_{12})$ is the probability of rejection of a false signal.

The distribution probability is defined by

$$Y(S) = \frac{1}{\sqrt{2\pi}} \exp\left\{\frac{-S^2}{2}\right\}$$

where all S values are expressed in fractions of σ and the function Y is the probability density of the Gaussian (normal) distribution. Examination of Figure 2 gives the following expressions:

$$P_{11} = \int_{-(r+\delta_0)}^{(r-\delta_0)} Y(S)dS$$

$$P_{12} = \int_{-(r+\delta_1)}^{(r-\delta_1)} Y(S)dS$$

where δ_0 is the bias for true signals (assumed to be small, owing to our good intelligence) and δ_1 is the bias for false signals (assumed to be relatively large since the enemy is not allowed to possess perfect information). The values of acceptance probabilities (P_{11} or P_{12}) are shown in Figure A-3 and tabulated in Table A-1. It is obvious that if the "true" signals do not enjoy bias advantages (i.e., $\delta_0 \cong \delta_1$) then the difference between acceptance probabilities of true and false signals is insignificant. The quality of the decision could be defined as the difference $Q = (P_{11}-P_{12})$; the higher this value, the higher the probability is that a "yes" output of the decision box is justified.

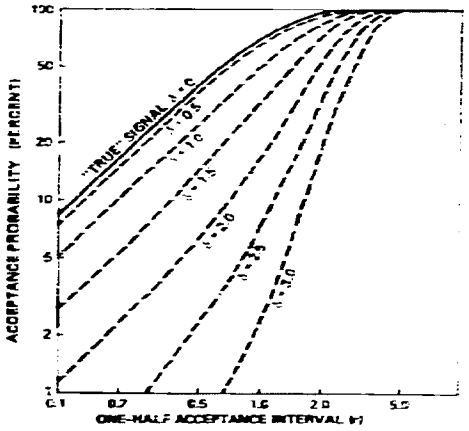


Figure A-3. Single -Channel Acceptance Probability

If the enemy has small bias (in absolute value), which is equivalent to saying that he has excellent intelligence information, we must counteract this by decreasing the corresponding σ; i.e. increase the signal-to-noise ratio. This in turn increases the relative value of δ_1 so that the acceptance domain can be safely set in the vicinity r = 1 to 1.5. This is the quantitative explanation of why the decrease in signal-to-noise ratio in our sensory channel is so important. To accomplish this purpose, we might increase sampling or integration time, or introduce coding redundancy so as to decrease the signal-to-noise ratio, especially when the noise includes that introduced by random (barrage) jamming.

Table A-1. Acceptance Probability Vs. Decision Parameters

r ↓ / δ →	0.0	0.5	1.0	1.5	2.0	2.5	3.0
0.1	.0636	.0738	.0508	.0273	.0114	.0037	~
0.2	.1663	.1471	.1016	.0549	.0232	.0076	~
0.5	.4005	.3573	.2538	.1433	.0643	.0229	.0064
1.0	.7065	.6484	.4998	.3209	.1698	.0733	.0233
1.5	.8851	.8401	.7126	.5289	.3351	.1772	.0769
2.0	.9646	.9409	.8638	.7259	.5399	.3443	.1837
2.5	.9915	.9826	.9482	.8703	.7345	.5499	.3535
3.0	.9984	.9960	.9817	.9512	.8758	.7429	.5499
10.0	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

All the techniques aimed at decreasing the signal-to-noise ratio in presence of a given information signal and a given noise level involve increased sampling time-bandwidth product. If the bandwidth is limited by technical reasons, we must increase the sampling time, but quite often the signal is not sufficiently stationary for that purpose. If both bandwidth and sampling time are limited, we have no other recourse but to sample independent (uncorrelated) features of the source (targets or message) and combine the decisions resulting from several uncorrelated channels in some form of voting.* The usual problem is that for physical reasons we cannot get the appropriately high P_{11} values and low P_{12} values in a single channel,

* Theoretically, of course, this is equivalent to increasing the total information bandwidth, even though in practice the multichannel decision may be easier to implement.

especially in presence of deliberate enemy action. If more than one channel is available (e.g., multispectral observation in a reconnaissance mission) composite decision process is possible.

Composite Decisions

We now assume that n independent decision processes are at hand, related to the same information channel, and having each the same individual acceptance probabilities, P_{11} and P_{12}. We also assume that all "votes" of all channels have the same weight.*

The problem is to express the quality of the composite decision process

$$Q_n^k = (P_{11})_n^k - (P_{12})_n^k$$

where n is the number of uncorrelated channels and k the decision threshold; i.e., the minimum number of "yes" votes in order to generate a composite "yes." The quality of this decision is shown in Table A-2 and represented in Figures A-4 through A-6.

Table A-2. Composite Acceptance Probability (n = 10)

P \ k	1	2	3	4	5	6	7	8	9	10
0.95	1.000					1.000	.999	.988	.914	.599
0.90					1.000	.998	.987	.930	.736	.384
0.85					.999	.990	.956	.820	.544	.197
0.80				.999	.994	.967	.879	.678	.376	.107
0.75				.996	.980	.922	.776	.526	.244	.056
0.70			.996	.989	.953	.850	.650	.383	.149	.028
0.60	1.000	.993	.980	.945	.834	.633	.382	.167	.046	.006
0.50	.999	.989	.945	.828	.623	.377	.172	.055	.011	.001
0.40	.994	.954	.833	.618	.367	.166	.055	.012	.002	-
0.25	.944	.756	.474	.224	.078	.020	.004	-	-	-
0.20	.893	.622	.322	.121	.033	.006	.001	-	-	-
0.15	.803	.456	.180	.050	.010	.001	-	-	-	-
0.10	.651	.264	.070	.013	.002	-	-	-	-	-
0.05	.401	.086	.012	.001	-	-	-	-	-	-

Figure A-4 shows the case where P_{12} (the acceptance probability of false signals) is rather low and the quality of decision Q_n^k is shown for various P_{11} values. In general, the voting process at its best is better than the quality of the individual channels and is obtained for k less than one-half of the total channels available.

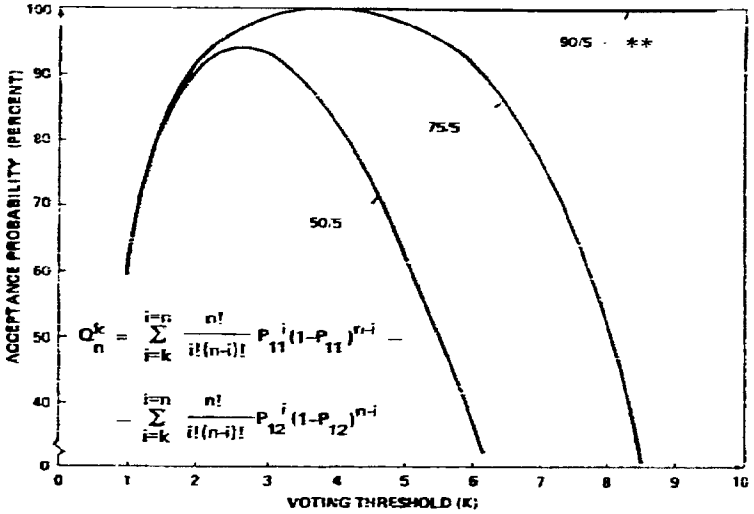


Figure A-4. Composite Acceptance Probability (n = 10)

In Figure A-5, the acceptance probability of both true and false signals is relatively low, but the quality of individual decision ($P_{11}-P_{12}$) remains in the 40 to 50% range. When the decision process is optimized, it always improves on the quality of individual channels; the optimum k's are seen to occur between 30 and 60% of the available channels.

* This is a gross simplification and is hardly ever encountered in practice. One would also hope that instead of having each channel equally weighted, we would weigh heavily the channels known to be of high quality and give relatively little weight to those that are questionable. A more complete treatment of the general case is required, but the simple examples shown are sufficient to illustrate our point.

** This parameter is P_{11}/P_{12}.

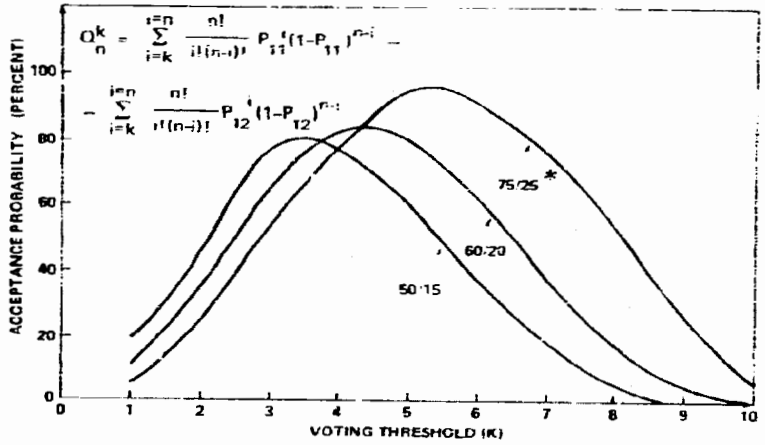


Figure A-5. Composite Acceptance Probability (n=10)

Figure A-6 shows the effects of multiple voting on channels with poor false signal rejection. Here again the Q_n^k at optimum voting threshold shows improvement over the quality of single channels, but the optimum k values tend to be in excess of one-half of the number of available channels.

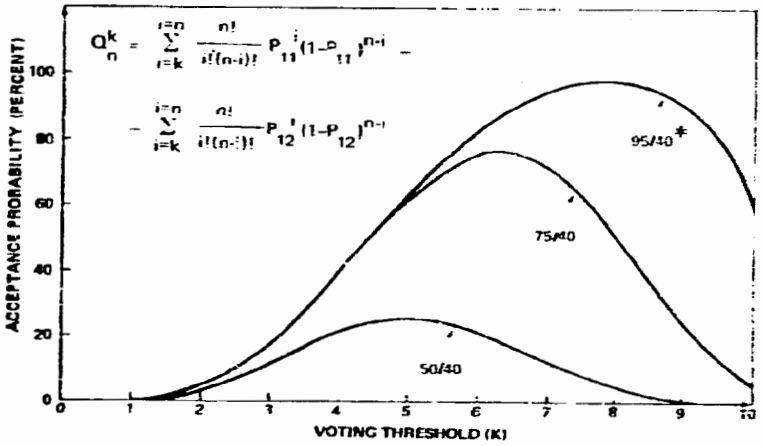


Figure A-6. Composite Acceptance Probability (n=10)

Conclusions

In relatively simple cases, the quality of decision channels can be expressed in terms of numerical parameters related to the signal-to-noise ratio (σ), the quality of intelligence available (δ), and the setting of acceptance domains (r). Jamming and disruption are relevant to σ; spoofing and manipulation depend on the low value of bias (δ) that can be achieved by the enemy. In general, sampling time and bandwidth limitations do not allow arbitrary setting of δ and r with respect to σ, so multiple channels are used in a "voting" mode to improve the decision quality.

In all cases, the use of multiple channels is very much justified in terms of improving the composite decision quality with respect to that of the individual channels. The process of optimization of the voting is in general extremely sensitive to the proportion of channels actually used as threshold (k). Using too many channels as vote threshold is just as prejudicial to high-quality decisions as using too few of them. When optimized, the composite decision process is preferable to single-channel decisions.

* This parameter is P_{11}/P_{12}.

(This page intentionally left blank)

GLOSSARY/REFERENCES

GLOSSARY

AAA	Antiaircraft artillery
ABCC	Airborne Command Center
ABM	Antiballistic missile
ASW	Antisubmarine warfare
AWACS	Airborne warning and control system
C&C	Command and control
CA	Counterattack
CCM	Counter-countermeasure
CEP	Circular error probability
CM	Countermeasure
COMINT	Communications intelligence
CONUS	Continental United States
DL	Damage limiting
ECCM	Electronic counter-countermeasure
ECM	Electronic countermeasure
ELF	Extremely low frequency
FBM	Fleet ballistic missile
GTOW	Gross takeoff weight
ICBM	Intercontinental ballistic missile
IFF	Identify friend/foe
IR	Infrared
LOS	Line of sight
MF	Medium frequency
MIRV	Multiple independently targeted reentry vehicles
nmi	Nautical miles
O&M	Operation and maintenance
QRCF	Quick-reaction counterforce
RPV	Remotely piloted vehicle
SIGINT	Signal intelligence
S/N	Signal-to-noise ratio
SSBN	Fleet ballistic missile submarine (nuclear powered)
TDA	Target damage assessment
T.O.A.	Time of arrival
USN	United States Navy
USW	Undersea warfare
VLF	Very low frequency

[This page is intentionally left blank.]