(2)

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

COMMAND AND CONTROL SECURITY:
CONCEPTS AND PRACTICES

by

Willard L. Unkenholz

March 1989

Thesis Advisor: Milton H. Hoever

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b. OFFICE SYMBOL (If applicable) 74	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	7b. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
COMMAND AND CONTROL SECURITY: CONCEPTS AND PRACTICES

12. PERSONAL AUTHOR(S) Unkenholz, Willard L.

13a. TYPE OF REPORT	13b TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM _____ TO _____	March 1989	166

16. SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Command and Control (C^2); Command, Control, and Communications (C^3) Security; [illegible] thesis (w-)

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

The United States is placing greater emphasis and reliance on command and control systems to be able to span the distances involved in, and keep pace with, a modern battlefield. This greater reliance on command and control systems also creates a potential vulnerability to disruption or defeat through successful attacks against those same systems. Security is therefore of prime importance to the design and operation of command and control systems.

The goal of this thesis is to provide students of command and control (C^2), as well as designers and program managers of command and control systems, a basic understanding of the need for security in C^2 systems and an introduction to security measures used to counter C^2 threats.

The ultimate objective of this thesis is to provide a conceptual framework for the continued study and analysis of command and control security and to emphasize the need for designing security into command and control systems as an integral component.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Capt. Milton H. Hoever, USN	22b. TELEPHONE (Include Area Code) (403) 646 - 2995 22c. OFFICE SYMBOL 54Ho

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

* U.S. Government Printing Office: 1986—606-24.

Approved for public release; distribution is unlimited.

Command and Control Security:
Concepts and Practices

by

Willard L. Unkenholz
B.S., Virginia Polytechnic Institute and S.U., 1978
M.S., University of Southern California, 1981

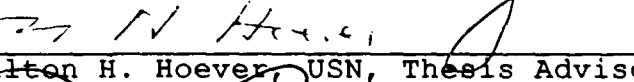
Submitted in partial fulfilment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(Command, Control, and Communications)

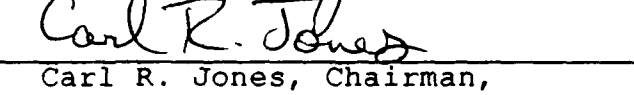
from the

NAVAL POSTGRADUATE SCHOOL
March 1989

Author: 
Willard L. Unkenholz

Approved By: 
Capt. Milton H. Hoever, USN, Thesis Advisor


Dan C. Boger, Second Reader


Carl R. Jones, Chairman,
Command, Control, and Communications
Academic Group


Harrison Shull, Provost and Academic Dean

ABSTRACT

The United States is placing greater emphasis and reliance on command and control systems to be able to span the distances involved in, and keep pace with, a modern battlefield. This greater reliance on command and control systems also creates a potential vulnerability to disruption or defeat through successful attacks against those same systems. Security is therefore of prime importance to the design and operation of command and control systems.

The goal of this thesis is to provide students of command and control (C^2), as well as designers and program managers of command and control systems, a basic understanding of the need for security in C^2 systems and an introduction to security measures used to counter C^2 threats.

The ultimate objective of this thesis is to provide a conceptual framework for the continued study and analysis of command and control security and to emphasize the need for designing security into command and control systems as an integral component.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

> To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself (Sun Tzu,p. 26).

A. WALKER-WHITWORTH

On May 19, 1985, John Walker was arrested in Rockville, Maryland for espionage--selling United States (U.S.) cryptographic secrets to the Soviet Union for the previous 17 years. The next day, his associate Jerry Whitworth was arrested in Sacramento, California. The consequences of the Walker-Whitworth spy ring were judged by then Director of Naval Intelligence, Rear Admiral W.O. Studeman as having ". . .jeopardized the backbone of this country's national defense. . . ." (Barron, 1987, p. 212) The Secretary of the Navy, John Lehman declared that ". . .had we been engaged in any conflict with the Soviets, it could have had the devastating consequences that ULTRA had for the Germans. . . ." (Barron, 1987, p. 212) These opinions were reaffirmed in court by George Carver, a former deputy to the director of the Central Intelligence Agency. He stated:

> The United States will have to invest an enormous amount of time and resources changing systems, changing procedures, at great dislocation. It [the United States] can never be positive that it has locked all the barn doors to keep future horses from straying. I cannot be totally confident about the security of its communications, particularly its military and especially

> its naval communications. And the damage thus done, in my opinion, could significantly, if not irrevocably, tilt the very strategic balance on which our survival as a nation depends. (Barron, 1987, p. 213)

It was not only U.S. officials that understood the magnitude of this breach in U.S. security. The KGB official and defector Vitaly Yurchenko related the importance the Soviet Union place on this spy ring:

1. The KGB regarded the Walker-Whitworth case as the greatest in its history, surpassing in import even the Soviet theft of Anglo-American blueprints for the first atomic bomb.

2. The cryptographic data supplied by Walker and Whitworth enabled the Soviets to decipher "millions" of secret American messages.

3. The three principal officers who supervised the case received the highest Soviet decorations.

4. One of the senior KGB officers who briefed Yurchenko stated that in event of war, this Soviet ability to read enciphered American messages would be "devastating" to the United States. (Barron, 1987, p. 148)

This was not a case of the communication security equipment failing to perform its designed security functions. It was a failure in the administration of personnel security that compromised U.S. communication systems. Failure in this one critical security element, caused the overall security system to fail and led to the devastation of United States military communication systems with the potential for equally devastating consequences to United States national security.

B. IMPORTANCE OF SECURITY IN MILITARY ACTIONS

Security is one of the primary elements required by military forces for the successful completion of their assigned duties. The U.S. Armed Forces Staff College lists security as one of the nine principles of war along with objective, offensive, mass, economy of force, maneuver, unity of command, surprise, and simplicity. It defines security as:

> SECURITY - Never permit the enemy to acquire an unexpected advantage. Security is achieved by establishing protective measures to counter surprise, observation, detection, interference, espionage, or sabotage. (AFSC Pub 1, 1986, p. 1-5)

The importance of security to military operations is not a new concept. Within his book The Art of War, written around 400-320 BC (Orr, 1983, p.1), the ancient Chinese warrior Sun Tzu also wrote about an army's need for security.

> Hence the skillful fighter puts himself into a position that makes defeat impossible and does not miss the moment for defeating the enemy. (Sun Tzu,p. 30).

In this passage from his discussion on tactics, Sun Tzu focuses on two aspects of war; the defensive and the offensive sides. The defensive portion of war seeks to prevent an adversary from gaining the advantage and exploiting a vulnerability or mistake. The offensive

portion seeks to exploit an adversary's vulnerabilities and achieve victory. Sun Tzu believed that defeat is the result of one's own vulnerabilities (Sun Tzu, p. 26). The Walker-Whitworth episode demonstrates clearly how vulnerabilities in command and control systems can seriously affect the security of a military force.

C. FRAGMENTATION OF SECURITY

Although security is an important element of military success, it is an element that is not well understood. Often it is assumed to be the responsibility of a select few to assure adequate security is provided. Part of this lack of understanding derives from the secrecy surrounding the application of many security measures such as cryptography. But the lack of understanding can also be partially attributed to the fragmentation of security into its supporting security elements. Cryptography resides within the academic bounds of mathematicians. Physical security is the responsibility of "security forces" and manufacturers of barriers and access equipment. Computer security is itself fragmented between groups that provide physical security for hardware and software storage mediums, the users with their procedural security measures, and computer programmers trying to design in rules within the software to prevent unauthorized access to information. Personnel security is relegated to an administrative

bureaucracy of background investigations and clearance messages. Unfortunately this fragmentation allows security to be unevenly applied often with oversights occurring which create serious vulnerabilities. The greater the reliance, the more devastating the consequences of exploited vulnerabilities.

D. SECURITY OF COMMAND AND CONTROL

The field of command and control (C^2) is receiving greater emphasis within the United States military today. To highlight its importance to effective modern warfare, the Secretary of Defense (SECDEF) has established an Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C^3I) and assigned him the responsibility to assure command and control requirements are fully considered in a weapon system's development and to coordinate C^2 development between the services. President Reagan also emphasized the vital need for command and control when he stated that the command and control systems must be given the same priority as the weapon systems that they control (DOD, 1988, p.100). Weapon systems are useless, no matter how well designed, unless there is also a reliable and survivable way to use them.

The modern battlefield is changing. Where once command and control consisted of organizing, training, and leading men armed with swords and spears on a small parcel of land,

today's battlefield can be global in size, last only minutes in duration, and result in the devastation of a nation rather than simply the defeat of an army. The commander now requires the means to communicate and "see" over the horizon or around the world. He needs to be able to assess potential threats within the precious few minutes provided him by the speed of modern weapons and be able to execute an appropriate response in the remaining few minutes. The command and control requirements for range, speed, and accuracy have drastically changed from Sun Tzu's requirement for drums and banners (Sun Tzu, p.64).

Along with this emphasis on the need for greater command and control is the application of advanced technology to attempt to satisfy this need. Computers and software are being employed to speed up the processing, integration, and display of information needed by the command and control system. Fiber optics, packet networks, satellites, and meteor burst are all communication technologies being used to transmit more data at a faster rate, and more reliably, in order to fulfill the needs of a command and control system. Modern command and control is becoming more complex because of the ability of electronics to record, process, and transmit data. With the pace of modern warfare, electronic command and control is vital to the effectiveness and safety of today's troops, planes,

ships, and weapon systems. They are no longer a luxury, but a necessity in combat.

This greater and greater reliance on electronics to provide command and control functions also increases the security requirements to maintain that capability in time of conflict and to prevent defeat through the destruction or disruption of the command and control systems. But security measures must be applied in a systematic manner to counter specific threats to be effective.

The systematic approach to security requires gaining an understanding of the nature of security, an understanding of the nature of command and control, recognition of the threats to command and control systems and possible security measures that can be applied to counter these security threats, and an appreciation for how each of these security measures must integrated into an overall security system. The rest of this thesis is devoted to providing a basic understanding of each of these subjects.

II. WHAT IS SECURITY? - A CONCEPTUAL PERSPECTIVE

> Protecting a nation's defense secrets from compromise is an age-old challenge. However, the stakes for the United States have never been higher. Given the extraordinary importance of advanced technology to our nation's military capabilities, its loss to a potential adversary - by espionage, theft, or other unauthorized disclosure - can be crucial to the military balance. So too, can compromise of operational plans or battle tactics. Thus to the extent that classified information can be kept from the hands of those who may oppose us, the qualitative edge of United States military forces is preserved and their combat effectiveness assured. (Commission to Review DOD Security Policy and Practices, 1985, p.5-6)

A. MULTIPLE DEFINITIONS

Security is a common word that is used in different contexts to mean many different things. The word "security" is often used to refer to the office that maintains security clearances or controls the local police force. Sometimes the word "security" is used to describe the procedures used to protect classified information. "Security" is also used to describe various technologies such as locks, barriers, alarms, or even more elaborate mechanisms that are used to protect something of value. Often, the word "security" is modified by a preceding adjective such as physical, procedural, or national. It can be even preceded by a noun such as communication, transmission, or operation. "Security" has a different meaning depending on who is using it and how it is used.

Webster's New World Dictionary actually has six definitions of security. The last three deal with peculiar financial uses of the term, such as providing collateral for loans or in describing stocks and bonds. But the first three definitions are of more direct interest to the military's use of the word.

SECURITY n. :

1. the state or feeling of being free from fear, care, danger, etc.

2. freedom from doubt; certainty;

3. protection; safeguard.

(Webster, 1969, p. 670)

The Joint Chiefs of Staff (JCS) use three definitions to further refine how the word security is used in the context of the Department of Defense (DOD). They define security as:

SECURITY -

1. Measures taken by a military unit, an activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness.

2. A condition which results from the establishment and maintenance of protective measures which insure a state of inviolability from hostile acts or influences.

3. With respect to classified matter, it is the condition which prevents unauthorized persons from having access to official information which is safeguarded in the interests of national security.

(JCS Pub 1, 1979, p.306)

These definitions describe security as the "measures taken", the "condition which results", and the "condition which prevents". They reinforce the confusion over what is actually meant by the term "security".

By comparing both the Webster and JCS definitions of security, the results can be grouped into two distinct categories. The first category describes security as a condition of being, feeling of being safe, or state of nature. This category encompasses the first two Webster definitions as well as the second JCS definition. The second category looks at security as being a process, an act, a procedure, or a mechanism. Security is something that acts upon its environment. These are two fundamentally different perspectives of what is meant by security.

For this thesis, the first category's definition will be implied when the term "security" is used - it is the condition, state, or feeling of being safe from danger; the level of security. The term "security measure" will be used to convey the second definition - the idea of the mechanisms or procedures which help to achieve this state of safety or certainty. By providing distinct terms for each class of definition, confusion over the precise meaning of the word will be avoided.

Individual security measures will be further grouped according to the type of protection they offer against

potential threats. These groups will be called "security elements" and refer to such broad categories of security measures as communication security, physical security, and procedural security. These definitions are summarized below:

> Definition 1 : Security - is a condition, level, state of nature, or feeling of being safe which results from the establishment and maintenance of security measures.
>
> Definitions 2: Security measures - are those procedures or technologies taken by an individual or group to protect against actions that threaten, impair, or destroy its survival or effectiveness.
>
> Definition 3: Security elements - are groupings of security measures that protect against a common threat or act in a similar manner. Examples of security elements are physical security, communication security, computer security, and emissions security.

B. THE NATURE OF SECURITY

Even with an agreed upon definition, what really is security? What are its components? How do these components relate and interact to achieve security? How is security measured? How are areas requiring higher states of security identified? And how much security is enough? These are not easily answered questions and yet, these are precisely the questions that must be answered in order to effectively incorporate security. These are also the questions that each military commander must correctly answer to achieve his assigned mission.

In order to sense the nature of security, an intuitive approach will be used to discover many of its underlying concepts. A person walking through several different sections of a city at night, intuitively senses that he is safe in one section of a city that is crowded with people, well lighted, and well patrolled by policemen. That same person walking along lonely, dark, and seemingly isolated sections of the city, has a feeling of danger and caution. In the first instance, there is a state or feeling of pure safety and well being (full security), and the second is the feeling of being in imminent danger (no security). Between these two extremes, a whole spectrum of states of security can be imagined with differing degrees of the feeling of safety and danger. This leads to the first hypothesis concerning the nature of security which is stated below and diagramed in Figure 1.

Hypothesis 1: Security can be considered a spectrum of states of nature ranging from imminent danger (no security) to pure safety (full security).

If the first hypothesis on the nature of security is accepted, what contributes to these varying levels of security? In the well lighted section of town, several factors contribute to this sense of security. First, the perception of the threat is very low. Because of the crowds of people and good lighting, the chances of a criminal getting away from the scene of a crime unnoticed

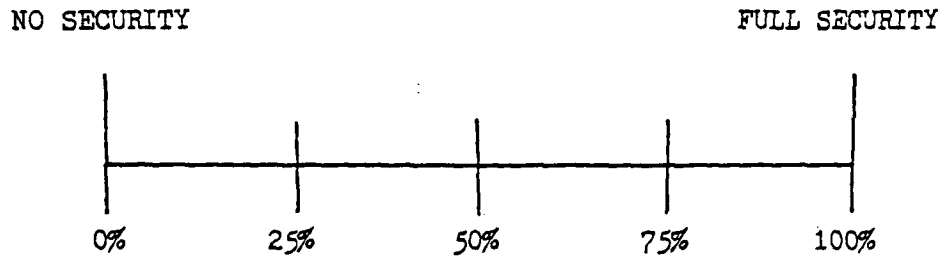


Figure 1. Security Spectrum

is much less likely. In other words, the probability of detecting a crime is greater in the well lighted section of town as opposed to the darker section. This detection is perceived to deter a criminal from an attempt.

In addition to detection, if a serious crime were attempted in the well lighted section, potential help is nearby either from the local police or simply from the nearby crowd. The reliability of that help or response is much greater than in the dark and lonely section of town. A crime committed in that section of town could not only be undetected, but also unaided. Under those circumstances, a criminal is much less likely to be caught and therefore may be more willing to attempt a crime.

A third aspect of this scenario, is not as readily obvious as detection and response. This is the concept of penalty for an action. If the only penalty that those responding to a detected crime could inflict upon the criminal was verbal harassment, this would not be sufficient to stop a determined criminal. If on the other hand the criminal was subjected to direct gun fire either from persons defending themselves or by the responding police, the crime could be stopped through the threat of death, or the actual wounding or death of the assailant. Between these two extremes are the penalties that the criminal justice system is able to administer. The greater the penalty, the greater the sense of security.

These intuitive observations lead to the next four hypotheses about the nature of security:

Hypothesis 2: Security is a function of the detection, response, and penalty mechanisms (security measures) applied to the environment.

Hypothesis 3: The greater the probability of detection, the greater the security.

Hypothesis 4: The greater the reliability of response, the greater the security.

Hypothesis 5: The greater the magnitude of the penalty, the greater the security.

These relationships may not be strictly true in all instances. The first exception is in the application of one of the three types of security measures (detection, response, penalty) without the other two. If there is detection, such as an activated burglar alarm, but there is no response or penalty associated with this detection, then the detection may be ignored by the assailant. Response by itself would never be summoned without first a detection and would be pointless without some measure of penalty. And penalty without detection and response would simply be indiscriminate. The three must work together. This leads to the next hypothesis:

Hypothesis 6: Detection, response, and penalty security measures cannot exist independent of each other.

Another example where the three relationships may be more complex is when time is considered as another

variable. One argument in particular concerns whether or not more nuclear weapons in a country's arsenals to inflict even greater damage on an adversary actually leads to greater security. Is it true that the possible penalty of inviting a nuclear retaliation has prevented war in Europe as Hypothesis 5 would predict, or does the increase on one side simply lead to an increase of force on the opposing side in a spiral fashion leading to less security than before? If time is also considered as a variable in the security equation, then it is quite reasonable to believe that both arguments may be true. Hypotheses 3, 4, and 5 may be true at any fixed point in time, but if these variables are also subject to variability in time, then an increase in penalty may not in fact lead to more security at a future point in time. It depends on how the threat has changed over time relative to the security measures employed. This leads to a seventh hypothesis:

Hypothesis 7: Security is a function of how the threat changes in time relative to security measures employed.

If the threat is relatively constant, then security measures once deployed to achieve an acceptable level of security, and maintained from deterioration, will continue to be an adequate safeguard. But if the threat is dynamic or if it evolves in response to applied security measures, then the security measures themselves must continue to

evolve to counter the new character of the threat. The following corollaries are derived from Hypothesis 7:

Corollary 7.1: Security is a function of time.

Corollary 7.2: Threat is a function of time.

Corollary 7.3: Security measures are a function of time.

Corollary 7.4: Security is a function of the threat.

Corollary 7.5: Security measures must be maintained relative to the threat or their effectiveness deteriorates over time.

Corollary 7.6: Security measures and the threat are in a constant, cyclical, action/response, and evolutionary relationship.

In summary, security is a function of time and the level of detection, response, and penalty applied to the environment by security measures. As the threat changes, the security measures must also change to meet the new challenges. And as security measures change, the threat will also inevitably change.

C. THE SECURITY PROCESS

In essence, the relationships between the threat, security measures, and value of the protected item can be considered to be a process function. The threat can be considered the input to the process, the security measure the transformation of the threat, and the remaining value the output of the process. A simplified model of the security process is depicted in Figure 2.

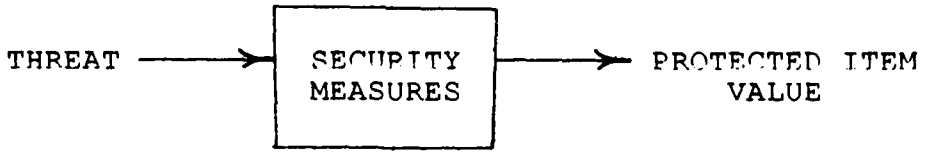


Figure 2. Basic Security Process

The threat is the potential hostile action that can change the value of the protected item. The security measures are actually the conglomeration of individual security measures employed to resist, impede, or minimize the impact of the threat on the security level.

If both the threat and security measures are reduced into finer components, a better picture of the complex nature of this process is obtained. For example, if the threat consists only of an aerial bombardment and a frontal tank assault, and the security measures employed consist of anti-aircraft guns and anti-tank missiles, the resulting security process is depicted in Figure 3. In this case the anti-aircraft gun is only effective against the aerial bombardment, and the anti-tank missiles effective only against the tanks. If the security measures are not 100% effective, then there are differing levels of effectiveness associated with each security measure which in turn affects the level of security. This discussion leads to the following hypotheses:

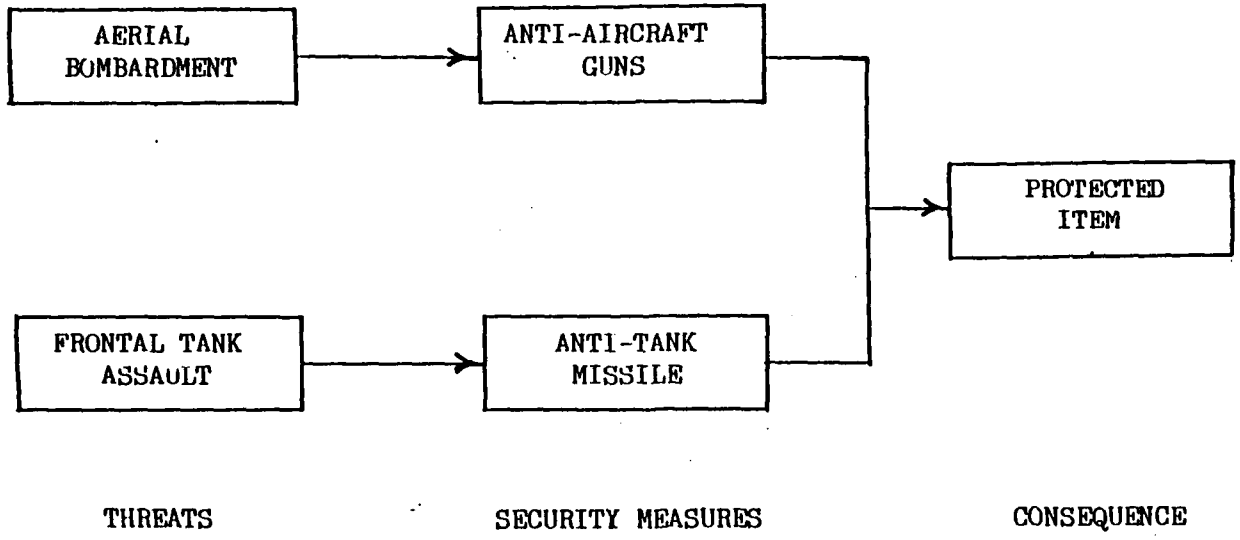


Figure 3. Dual Security Process

Hypothesis 8: The relationship between a threat, security measure, and value of a protected item is a process with threat as the input, the security measures as the transformation, and the remaining value as the output of the process.

Hypothesis 9: The threat and security measure can be composed of several different individual elements.

Hypothesis 10: For each security measure, there is an associated theoretical probability of successfully stopping a particular threat, ultimately affecting the value of the protected item.

If each threat could be identified along with its associated security measures, and if all these threat processes were combined into a larger diagram, the result would be the overall security system.

Hypothesis 11: The combination of all security processes is a system (security system).

D. MEASUREMENT OF SECURITY

Another important topic to discuss concerns how security is measured. Often this is done by first placing a value on the item or characteristic that is to be protected. For an automobile, it may be the blue book value; for an individual, it may be his life; for a military unit, it may be its ability to perform its assigned mission; and for a nation, it may be the retention of its basic culture, principles, and goals. As is apparent from the preceding list, not all values are easily quantified. Even so, there is often extensive effort made to transform more qualitative values into monetary values to

be able to take advantage of the many financial decision tools available.

The Department of Defense has developed its own valuation system for national security information -- security classification. The following excerpt from JCS Pub 1 defines the DOD security classification system and its various categories:

> SECURITY CLASSIFICATION - A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. There are three such categories:
>
> a. TOP SECRET - National security information or material which requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communication intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.
>
> b. SECRET - National security information or material which requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

c. CONFIDENTIAL - National security information or material which requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

(JCS Pub 1, 1979, p. 307)

The three measurement levels that can be assigned are "extremely grave damage", "serious damage", and "damage". These are not easily quantified but constitute the method for identifying the change to the level of national security if these items were not protected. They are in effect measuring the decrease in national security from the 100% level rather than the remaining amount of national security.

To be able to measure security, the threat must first be measured or estimated. Using the two threat example of aerial bombardment and frontal tank assault, Figure 4 shows how each threat level can be diagramed as a probability distribution. Because a threat is a potential action, it is uncertain exactly what level of threat will be encountered. Figure 4 also shows the mean of the distribution and three possible combinations or scenarios of the aerial and tank threats: A, B, and C. Figure 5 shows these combinations in a matrix form. Because of its uncertainty, the threat level is a stochastic variable.

Figure 6 shows an expansion of Figure 1 with measurement scales assigned. On the left hand side is a measurement of the "Level of Threat" measured in a percentage of the maximum force that an adversary can apply. On the right

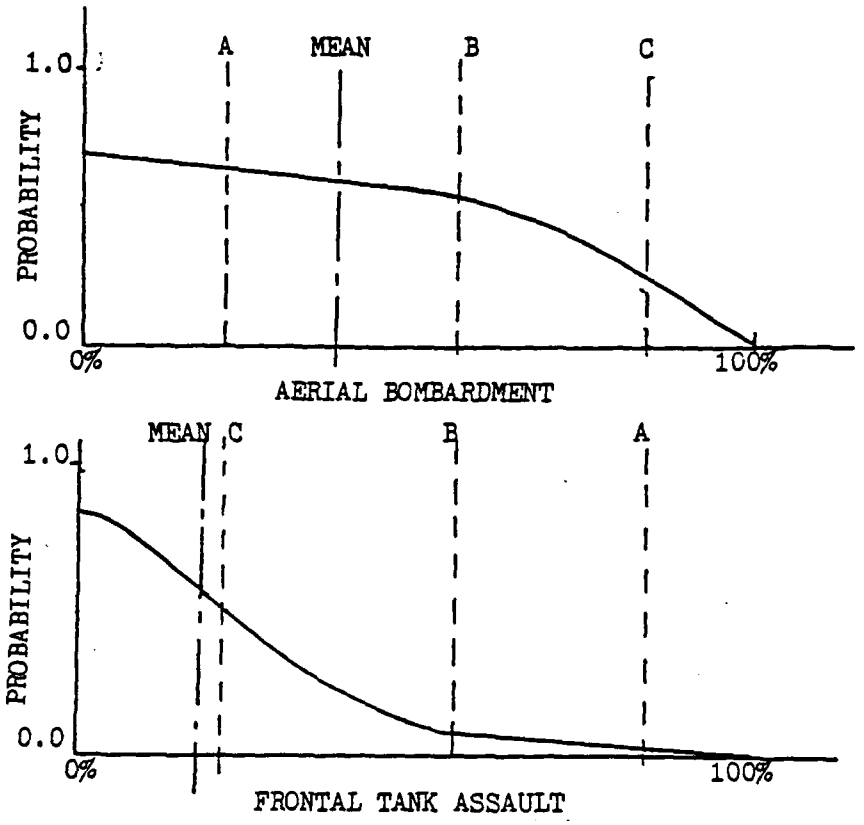


Figure 4. Threat Probability Distributions

	SCENERIO		
THREAT	A	B	C
AERIAL BOMBARDMENT	LOW	MED	HIGH
FRONTAL TANK ASSAULT	HIGH	MED	LOW

Figure 5. Scenerio Threat Matrix

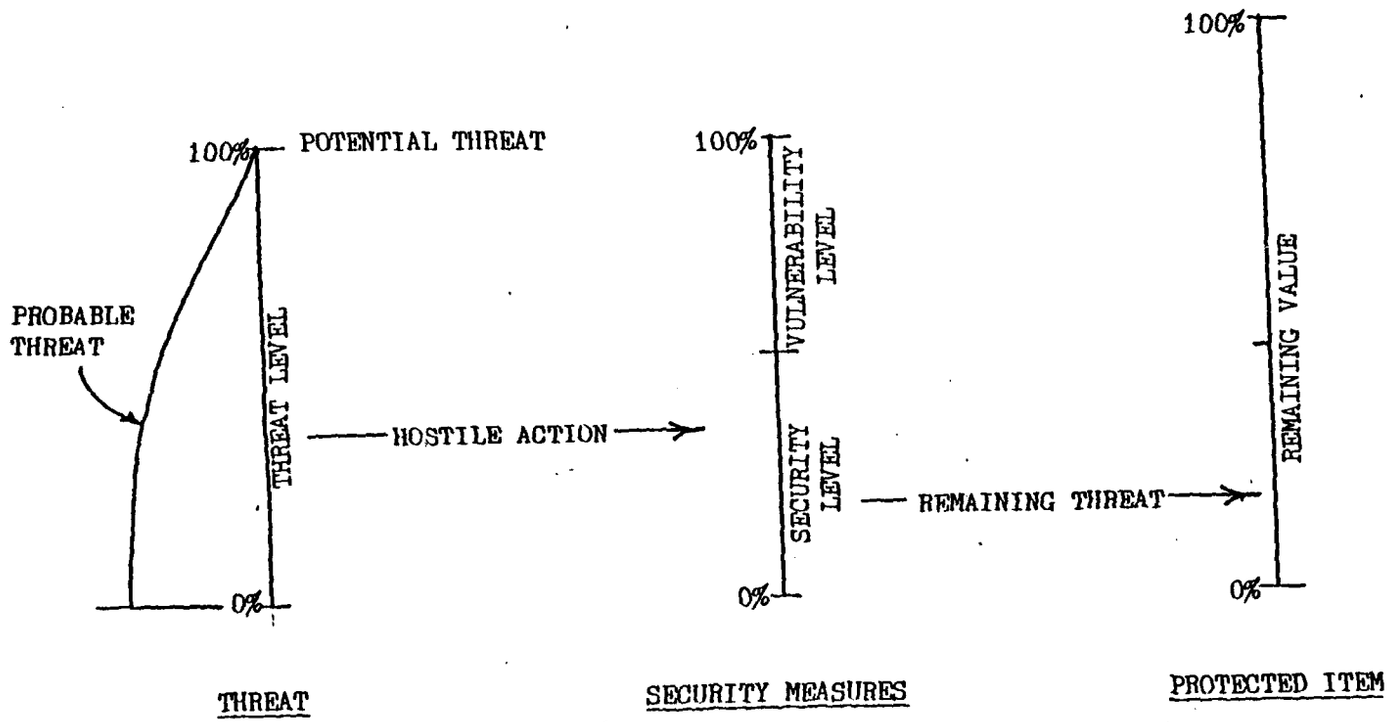


Figure 6. Measurement of Security Levels

hand side is a measure of the "Value" of the "Protected Item" and is measured in a percentage of its full value. In the middle is a scale of the level of security afforded by the applied security measures. It is a percentage of the potential threat that can be resisted by the security measures. The percentage of the potential threat that cannot be resisted is called the vulnerability of the security system. It is through the security system that the "threat level" is transformed into a change in the "value level".

For example, if the "protected item" is a museum painting, then the dollar value of the painting would correspond with the "value". If there are no security measures applied, but the threat has not been executed in a "hostile action", then the painting still retains its full value. The "security level" would be 0% of the threat and the "vulnerability level" would be 100%. Zero applied level of threat is transformed in this system to a zero level change in the value of the item. If on the other hand, the same security system is used but a 100% level of threat is applied in the "hostile action", then the painting could be either stolen or destroyed resulting in a remaining value of zero.

If the system is changed so that there is a 75% security level (25% vulnerability level) and only a 30% threat level is applied in the hostile action, then the value of the

protected item would remain 100%. The threat level was below that of the security level. If the threat were instead 80%, then 5% of the hostile action would be allowed to penetrate to the protected item which could result in possibly damage or vandalism which in turn would decrease the value of the painting.

The "protected item" does not always have to be an object with a monetary value. In the case of a communication system, the "protected item" may be the connectivity of the system. A state less than 100% would represent a degraded system, and 0% would represent a complete severance of the system. For this thesis, the following definitions will be used in the theoretical discussions:

Definition 4: Protected Item - The object, system, idea, information, or characteristic that requires security.

Definition 5: Value - The remaining importance or effectiveness of the protected item measured in a percentage of its full importance or effectiveness.

Definition 6: Security Level - The percentage of the potential threat that the security system can resist.

Definition 7: Vulnerability Level - The percentage of the potential threat that the security system cannot resist. The vulnerability level is equal to the difference between the threat level and the security level.

Definition 8: Threat - The potential force an adversary can exert to decrease the value of the protected item.

Definition 9: Threat Level - The measure of the potential force an adversary can exert measured in a percentage of the maximum force level.

Definition 10: Hostile Action - The actual execution of a threat.

(Security measure was already defined in Definition 2)

E. ECONOMIC LEVELS OF SECURITY

So far the discussion of security has centered only on the nature of security. The following discussion will now focus on factors determining how much security is economical.

The first observation in considering the economic level of security is that security measures have a cost associated with them. In the example of the person walking through a city at night, the various security measures employed were extra lighting and greater police protection. There was capital investment in the installation of the street lights as well as operating costs associated with providing electricity and maintenance costs in replacing defective bulbs, painting the lamp posts, and repairing damaged lines and equipment. There were also the hidden costs of the judicial system. If funds for street lights were reduced, the detection capability would also be reduced. If funds for the police were similarly reduced, detection, response time, and response ability could be seriously affected. And if funds for the judicial system were reduced, the court cases could begin to back up, jails would become crowded, and penalties may be reduced to ease

the crowding and backlog. Each of these decreases in funds could ultimately lead to a corresponding decrease in security.

Hypothesis 12: There are costs associated with employing security measures.

These costs are not only financial, they can also involve other characteristics of value. The elaborate security measures utilized by the Secret Service to protect the President not only have financial costs associated with them, but they often cost the public a disruption of normal traffic flow. They also cost the President mobility, flexibility, and public contact. The application of communication security equipment to radios can cost the operators flexibility with whom they can talk, possibly a degradation in the quality of the communications, and a restriction in the locations from which they can talk. This is in addition to the strict accounting procedures required for all cryptographic equipment and keys. The security measures employed to protect different classification levels of information can severely restrict the distribution of vital information that would be helpful in the conduct of a military mission. The cost, in this case, is that the mission operates with a greater level of uncertainty than if the participants were able to receive the information.

Recognizing the difficulty in determining (1) a quantitative value of security, (2) the true cost of security measures, and (3) assigning meaningful probabilities to the security process, it is instructive nevertheless to assume these difficulties away and utilize decision theory to describe how decisions can be made concerning economical security measures.

Again the city street example will be used with several assumptions applied. The first assumption deals with the value of the item to be protected. In this example, the item to be protected is a $100 bill carried in a man's wallet. A $20 can of mace is the only security measure that will considered. The police have determined that the man has a 40% chance of being involved with an attempted robbery in this section of town but robbery is the only threat. Figure 7 depicts this problem in the form of a pay-off matrix. The question is whether or not it is economical for the man to purchase the can of mace (pay the cost of security).

If the man knew precisely the state of the threat (decision under certainty - no probabilities) then in the first state, when he knew he would be robbed, he would always buy the $20 can of mace leaving him with a total of $80 after his walk as opposed to losing the entire $100 without buying the mace. If he knew for certain that he

would not be robbed, then he would always not buy the mace, saving him the $20 purchase price.

SECURITY MEASURE	THREAT ENVIRONMENT	
	ROBBERY (.4)	NO ROBBERY (.6)
CARRY MACE	$80	$80
NO MACE	-$100	$100

Figure 7. Security Application of Decision Theory

Most real world problems concerning the purchase of security measures are not that well defined and the states of nature are uncertain. When the element of doubt is included in the model, the decision making process becomes much more complicated. "Decision under risk" must be used where there is uncertainty about the state of nature that will be encountered but the probabilities of the states of nature can be estimated. Using an "expected monetary value" method of decision making, it would then be more economical to buy the mace. The expected monetary value for purchasing the mace would be $80 as opposed to only $20 for not buying the mace. If the probabilities were not known, then other techniques for decision making under uncertainty would then have to be used.

This was an extremely simple example to show how decision theory can be applied to making economic decisions regarding security measures. Expanding the threat,

increasing the number of security measures, making the threat and security measures variable over time, and not being able to quantify precisely the probabilities or security outcomes only further compound the complexity of the problem. Judgement and experience is often substituted for the purely analytical approach in extremely complex situations such as deciding the budget for national defense.

F. SYSTEM SECURITY

As was implied in Hypothesis 11, security is not achieved though a single security process consisting of only one threat and one security measure influencing the security level. Although it is helpful at times to study these fundamental processes, the acceptable level of security is more often achieved through the application of several security measures to thwart multiple threats. A military battlefield is a good example where the threat can be an intelligence threat, or a physical threat from land, sea, or air. A military commander employs a whole variety of security measures such as his assigned weapons, mine fields, guards and sentries, fences or obstructions, secure communications, patrols, and security procedures for protecting classified information. This then is the commander's security system.

Definition 11: System - a set of elements united as a whole for achieving a goal. (Taylor, 1988)

The set of elements in a security system incorporate the individual security measures. The goal of the system is maintaining an acceptable security level. By enhancing the block diagram of Figure 1 and drawing a system boundary, the security system can be defined. Figure 8 depicts this generalized model of a security system.

The system includes the collection of all security measures and the control process that coordinates each measure to achieve the final goal which is the acceptable level of security. The threat is the environment within which the system must operate. The level of security, or value of the item, becomes the measure of the effectiveness of the security system. Figure 9 illustrates how security measures can be integrated together to form a security system.

There are two major types of security measures, passive measures and active measures. The passive measures are boundaries and barriers that restrict access to the valueditem. These measures include optical barriers (optical security) to prevent visual observation of the valued item, electrical barriers (TEMPEST) to restrict the electrical emanations from the valued item, and physical barriers (physical security), such as fences and walls, that restrict physical access. If these barriers completely

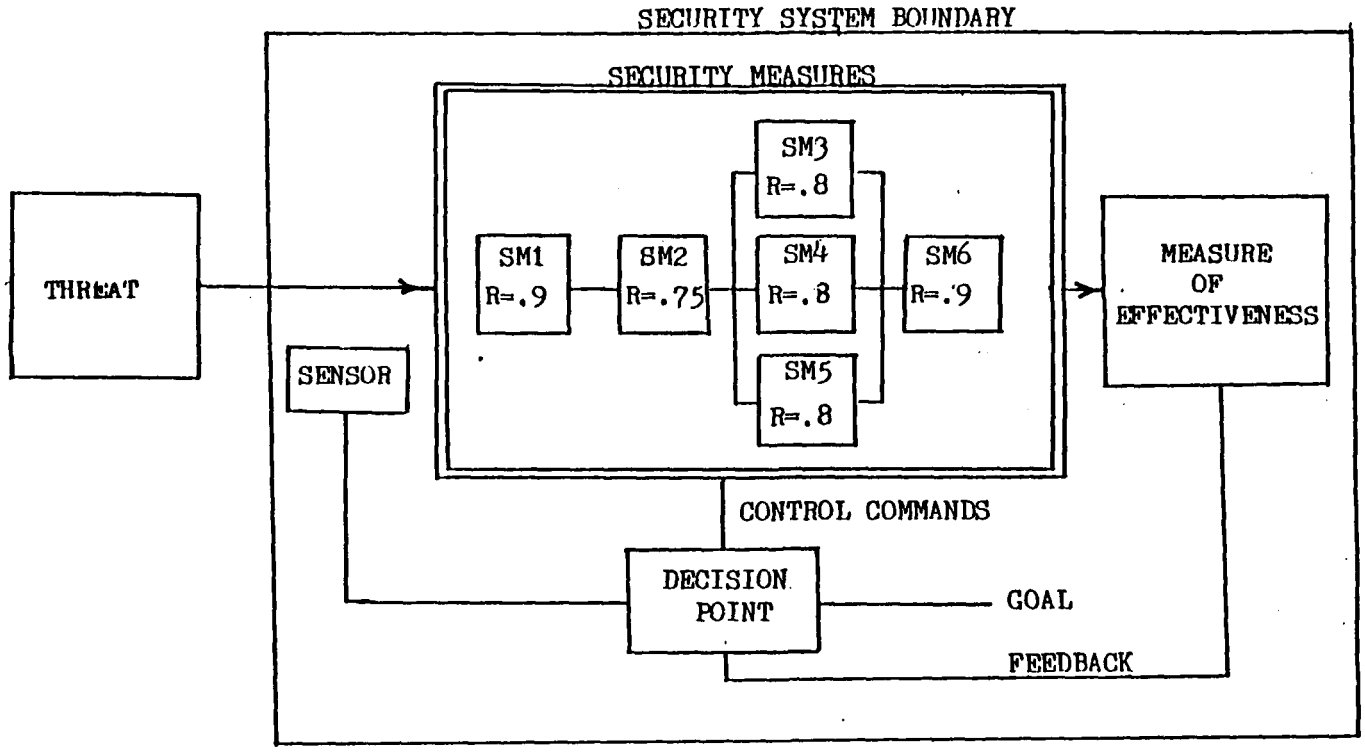


Figure 8. Generalized System Security Model

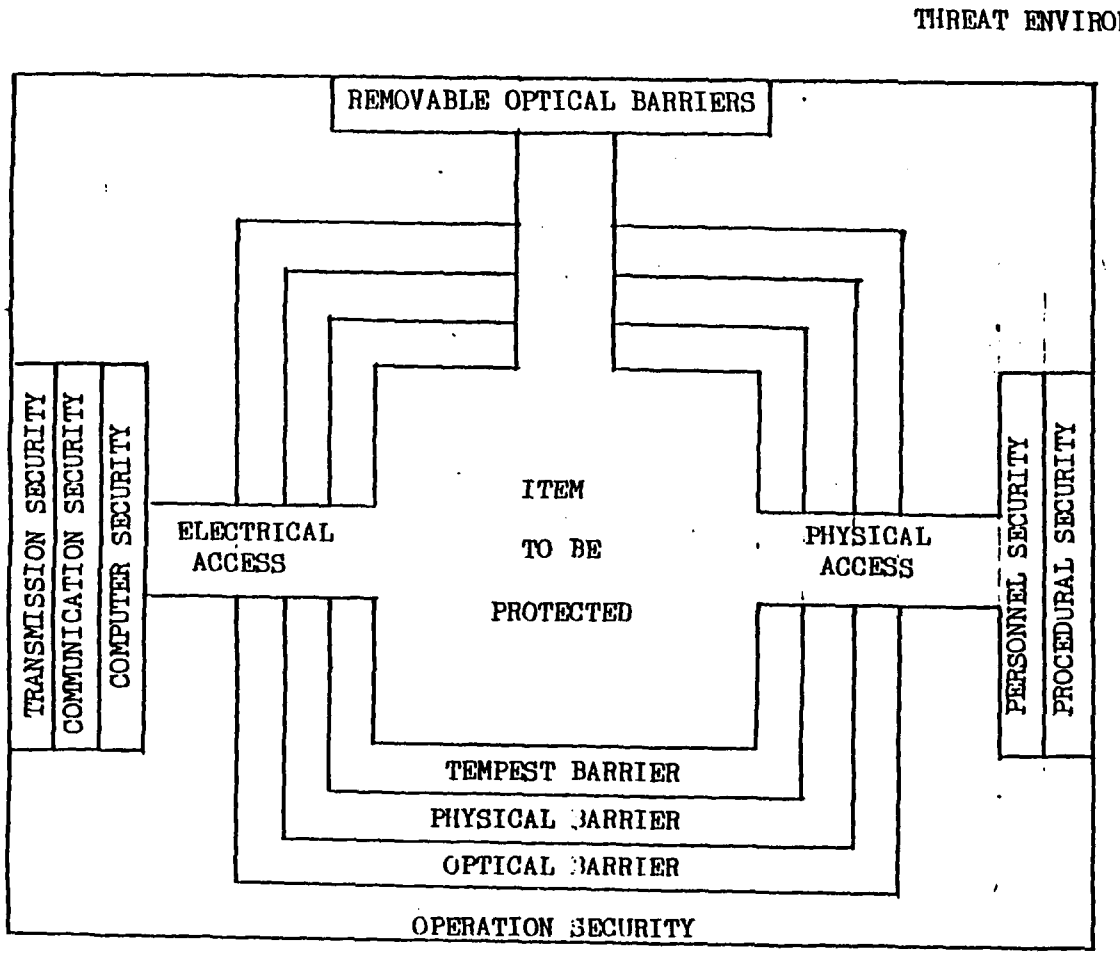


Figure 9. Application of Security Measures

surrounded the valued item, and were 100% effective, there would be no threat to its security. But it would alsobecome useless. Even those authorized for access would be prevented.

To allow for this authorized access, there are certain controlled paths, (optical, physical, or electrical) that penetrate the passive security barriers. Each of these controlled paths has certain active security measures used to maintain the security along that path. The optical control includes such things as removable screens and covers. The physical access paths are controlled by procedural and personnel security measures. Electrical paths are controlled by communication security, computer security, and transmission security measures. The active security measures can themselves be further sub-divided into the detection, response, or penalty components discussed previously.

Surrounding the entire security system is operation security which attempts to merge these divergent security techniques into a cohesive entity. Operation security also prevents the operations of the individual security measures from revealing information about the valued item or about vulnerabilities to the security system.

Vulnerabilities to security systems often exist due to the misapplication of security measures, gaps between security measures, or the fact that each security measure is

not 100% effective. To analyze how an individual security measure's vulnerabilities contribute to the vulnerability of the entire system, each security measure used to counter a specific type of threat can be thought of as a separate component with its own stochastic security rating. These ratings can be thought of as component reliability figures and can be analyzed in the same way reliability networks are analyzed. By combining the various security measures in series and parallel networks, an overall security rating for the system theoretically could be achieved as was depicted previously in Figure 6.

The final element of the security system that needs to be discussed is the security system control. The control mechanism measures the outcome of the security process, provides feedback to a decision point to compare the outcome against some desired goal or security level, and adjusts the security system to adapt when required. It may also be desirable to have feedback from sensors that measure the character and strength of the threat. This then becomes classic decision making or a cybernetics loop.

G. SECURITY SUMMARY

Security is vital to protect things of value whether they are the national character, the effectiveness of a military unit, or a child's piggy bank. Unfortunately security measures are often misapplied or not thoroughly

applied. This can lead at best to a waste of resources, men, equipment, and money. It can also lead to a false sense of security - the feeling of being safe when a careful analysis of the security system would reveal glaring vulnerabilities that have been overlooked. By understanding the nature of security, how security measures can be effectively combined into a system, and how to analyze them with respect to the threat, more effective and economical security systems can be designed and fielded to meet a constantly changing and evolving threat.

III. THE NATURE OF COMMAND AND CONTROL

> United States superiority on the future battlefield will require application of technologically superior weapons in precise places and time. Command and control systems will be required to locate and confirm quickly the identity of specific enemy units; determine the proper response; direct weaponry on the target; confirm destruction; and assess battle damage. (DOD, 1988, p.153)

A. AN EXPLORATION OF THE MEANING OF COMMAND AND CONTROL

In order to be able to effectively provide security, the nature of what is to be protected must first be understood. This chapter is therefore devoted to describing the nature of command and control and highlighting its characteristics that are important to security.

Just as security is a misunderstood word, the term command and control is even more confusing. This is reflected in the many labels that are used to mean command and control, such as C^2, C^3, C^3I, C^4, and C^4I^2. Each of these labels is important to emphasize the different and important aspects of command and control such as communications, computers, intelligence, and interoperability, but it tends to confuse discussions on the true nature of command and control.

It is more than simply acronyms that cause this confusion. The term command and control is used just as

often to refer to communication systems as it is used to mean the process by which commanders make and disseminate decisions. In some circles, command and control means the data processing capability while others see it as a collection of interconnected electronic devices. The Joint Chiefs of Staff have decided not to join in the battle of acronyms. In their Dictionary of Military and Associated Terms - JCS Pub 1 they use only the term "command and control". Their definition incorporates all of these elements of command and control. The JCS define command and control as follows:

> COMMAND AND CONTROL - The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures which are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JCS Pub 1, 1979, p. 74)

Taking a close look at this definition is helpful in understanding exactly what the JCS means by command and control. The central player in this definition is the commander. He is the person performing the action of command and control. This leads us to the first hypothesis concerning command and control.

> Hypothesis 13: Command and control is a function performed by the commander.

But there is more to the description of the commander. He is not just any commander, but a "properly designated" commander. This implies that there is an organization and a process by which commanders are selected and assigned to specific position with authority over assigned forces and with specifically assigned "missions". These observations lead to the following hypotheses:

Hypothesis 14: The commander operates within a larger organization.

Hypothesis 15: The commander is specifically assigned to his position by the organization.

Hypothesis 16: The commander is assigned a specific mission to accomplish.

Hypothesis 17: The commander is assigned authority over specific forces.

Hypothesis 18: The commander accomplishes his mission through his assigned forces.

The most crucial portion of this definition to the understanding of command and control, is that command and control is the "exercise of" the commander's authority. This leads to the next hypothesis:

Hypothesis 19: Command and control is the process by which a commander exercises his authority.

Command and control is not a communication system; it is not intelligence collection; it is not the computer processing, analysis, or fusion of data; and it is not how well forces can operate together on a battlefield. Command

and control is simply the process by which a commander exercises his authority.

A vital definition that is missing from the JCS Pub 1 is that of "authority". Again using Webster's dictionary, authority is defined as:

> AUTHORITY, n. - the power or right to give commands, enforce obedience, take action, or make final decisions. (Webster, 1969, p.50)

In essence, command and control is a process by which commanders make decisions and direct actions by use of their assigned forces. This leads to another hypothesis:

> Hypothesis 20: Command and control is a decision making and force directing process.

The JCS definition of command and control does not stop simply at defining command and control. It continues to divide "the exercise of authority" into subgroups: planning, directing, coordinating, and controlling.

> Hypothesis 21: Command and control incorporates the functions of planning, directing, coordinating, and controlling of forces and operations to accomplish its decision making and force directing process.
>
> Hypothesis 22: Essential elements of command and control are the commander, the mission, the assigned forces, the organization, and the means to decide and direct.

To summarize, command and control is a process by which a designated commander determines what courses of action need to be performed to accomplish his assigned mission, and

directs his assigned forces to carry out those actions. Supporting the commander is the organizational structure and the physical means to decide and direct. The command and control process integrates human behavior, decision making, and technology to direct the accomplishment of an assigned mission.

B. THE COMMAND AND CONTROL PROCESS MODEL

Functionally the command and control process can be divided into a series of functions. There are many ways of grouping theses functions. The JCS definition divides them according to "planning, directing, coordinating, and controlling". Dr. Joel S. Lawson suggests another division of functions that is more suited to an analysis of the nature of command and control (Orr, 1983, p.24). Figure 10 depicts the Lawson Command and Control Process Model.

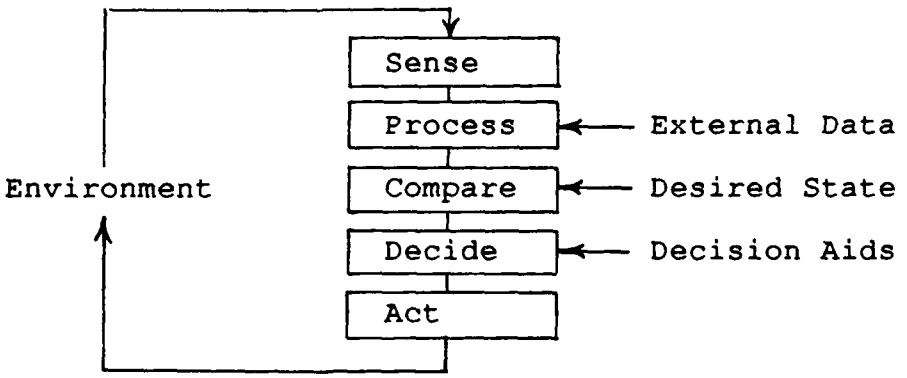


Figure 10. Lawson's C^2 Process Model

The model consists of the external environment, five functions, external data, a desired state or goal or the system, and decision aids.

The external environment refers to all of the activities and actions outside the control of the command and control process. These can include the actions of the enemy, physical and natural phenomena, and the actions of people or organizations outside that controlled by the C^2 process. The external data consists of all the information needed to help to analyze the sensed data and help make the proper decision. The desired state is the goal of the command and control system which is some position or relationship between the organization and the external environment. And finally, decision aids refer to the tools, automated or heuristic, that help to determine the selection of one course of action over another.

The five functions are: sense, process, compare, decide, and act. They are described in a military context by Maj. George Orr, USAF in the following excerpt from his book, Combat Operations C^3I: Fundamentals and Interactions:

> The SENSE function corresponds to all data-gathering activities (radar sites, forward observers, photo reconnaissance systems, and so forth). It is concerned with extracting signals from the environment. The PROCESS function acts upon these signals to attempt to extract meaning from them. External data, not directly from the environment, may be used. These may include intelligence analyses indicating patterns representative of division headquarters, etc. The PROCESS function produces event reports and status reports for use by

later functions. The COMPARE function compares the state of the environment, as determined by reports from the process function, with a desired state as specified by some external source. Based upon this comparison, the DECIDE function determines what should be done to move the actual state to the desired state, and the ACT function executes that decision. (Orr, 1983, p. 24-25).

If these five functions are translated into military terms, there is not an exact one to one correspondence. Figure 11 shows a similar functional diagram as Lawson's with more traditional military terminology.

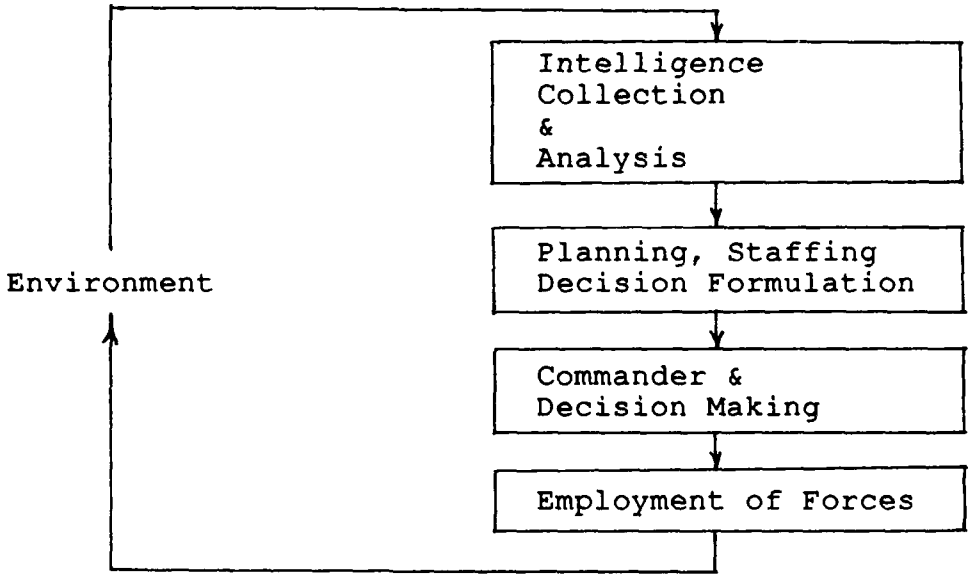


Figure 11. Military Command and Control Model

In this model, the functional groupings have been reduced from five in Lawson's model to four in the military model. The difference is that the process function, rather than appearing as a function itself, is split and incorporated into the intelligence function and the planning function. In reality the functions have not changed. In

Lawson's the emphasis is on the action that takes place. In the military model, the focus is on allocating those functions to individuals, groups, or communities. The military model will be the model used throughout the remainder of this thesis.

C. THE COMMAND AND CONTROL SYSTEM

The JCS definition also recognizes that a commander does not perform his command and control function in complete isolation. He is dependent on an organizational structure or system consisting of personnel, equipment, communications, facilities, and procedures through which he exercises his authority. JCS Pub 1 calls this the "command and control system" (JCS Pub 1, 1979, p. 74). The command and control system is the means by which he directs his forces to accomplish the mission.

Hypothesis 23: The command and control system is the means by which a commander directs his forces to accomplish a mission.

Hypothesis 24: The command and control system consists of personnel, equipment, communications, facilities, and procedures.

The command and control system is a subset of the overall command and control process. It is a combination of human and technology means. The specific mix of humans and technology is dependent on the situation, resources available, and the technology available. It is divided into

five distinct and vital elements: personnel, equipment, communications, facilities, and procedures.

The command and control system can be depicted as a series of functions (ie., the military model functions) connected by communications. Figure 12 shows the representation of one function. As is obvious from the diagram, each function has some mix of personnel, procedures, equipment, and facilities. Exactly what that mix is depends on the function to be performed and the technology and resources available. Redrawing the military model using these symbols results in the diagram pictured in Figure 13.

Since combat is the interaction of two opposing forces, the battlefield actually has two opposing command and control systems. Each command and control system is trying to effectively direct its forces into actions and positions that will defeat the opposing force. At the same time, each command and control system is also trying to sense the capabilities of the opposing force and may even direct measures to try to degrade the opposing force's command and control. The sensing is usually called intelligence and the degrading of an opponent's C^2 system is C^3 countermeasures. This conflict of two opposing command and control systems is depicted in Figure 14.

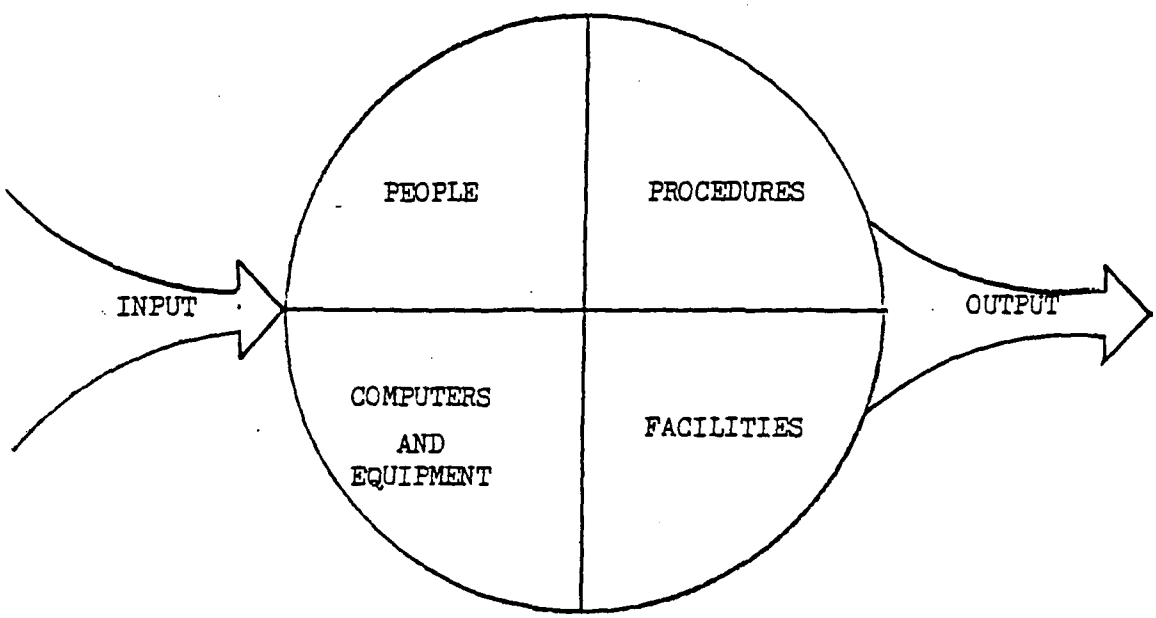


Figure 12. Command and Control Function

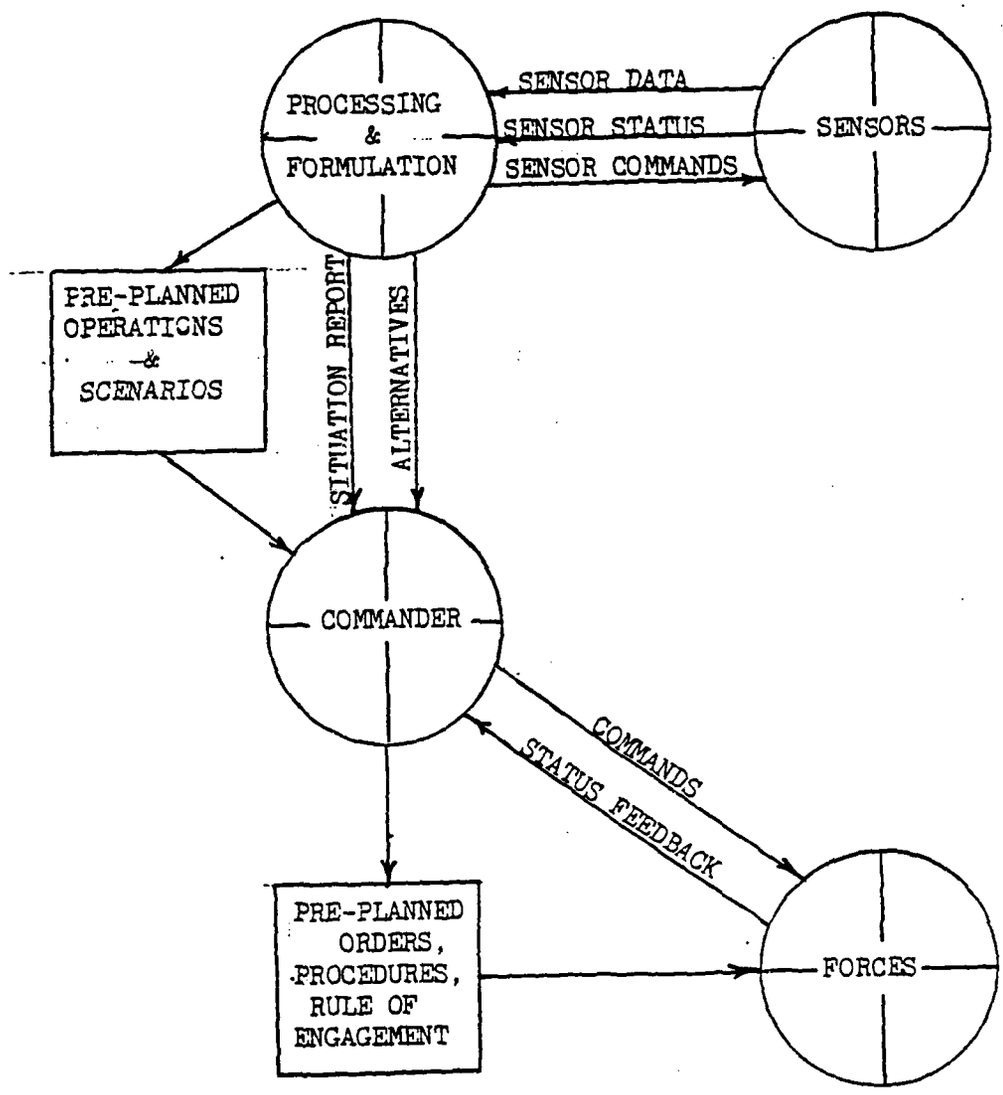


Figure 13. Military Command and Control Systems

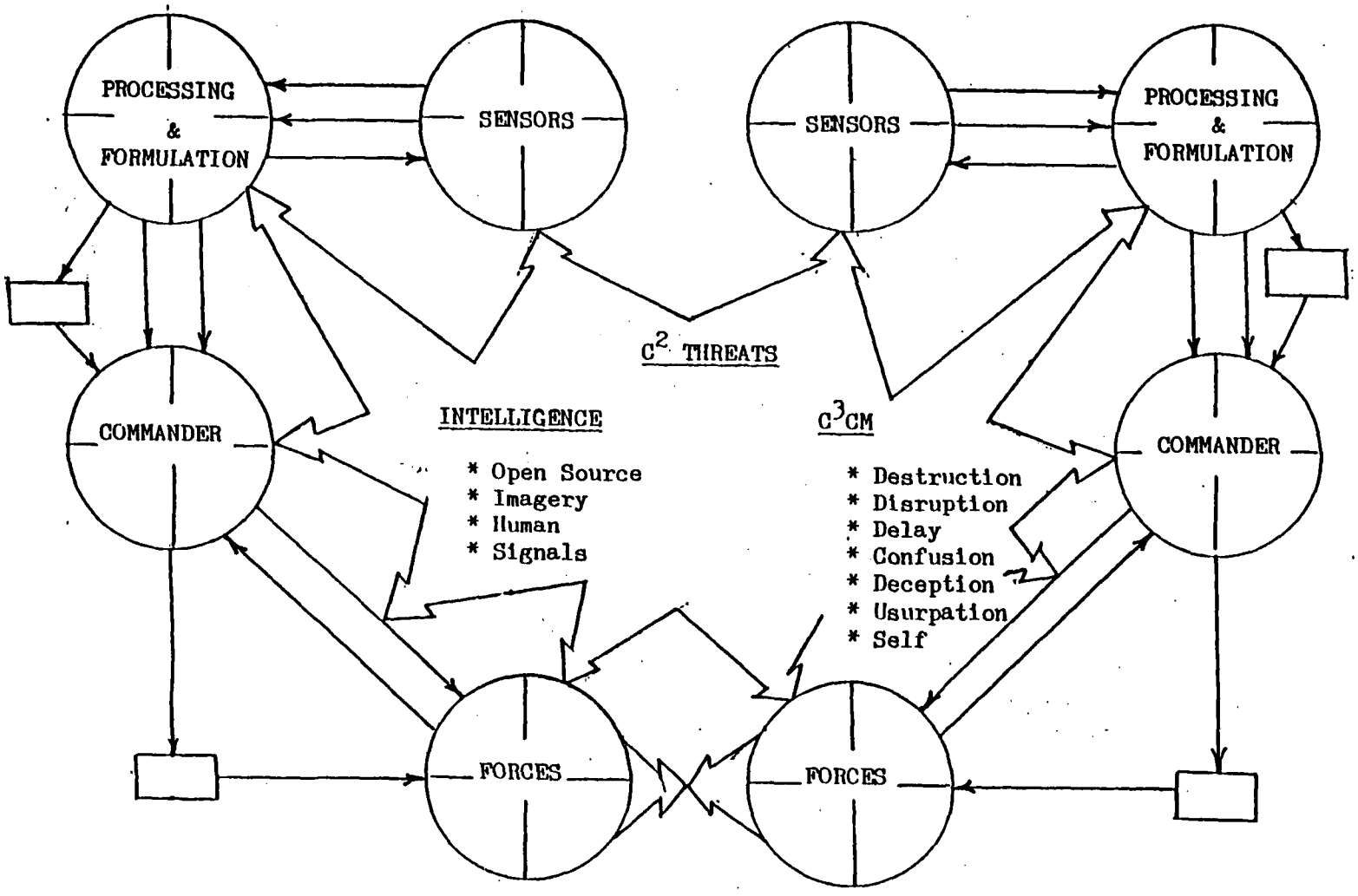


Figure 14. Opposing Command and Control Systems

D. CHARACTERISTICS OF COMMAND AND CONTROL

Although the preceding sections have discussed in great detail the nature of command and control, the functions are still too broad to begin to determine how to provide security for the overall process. This requires an exploration of actual characteristics of command and control. The characteristics that will be discussed are:

1. Connectivity.
2. Accuracy.
3. Timeliness.
4. Authenticity.
5. Secrecy.
6. Covertness.
7. Availability.
8. Affordability.

Depending on the application of the command and control system, these characteristics will appear in varying degrees. Some command and control systems may have a minimum required response time of two days. Others, such as the Strategic Defense Initiative, may require the entire process to be executed in several seconds or minutes. Some command and control systems may require secrecy only to the SECRET level rather than TOP SECRET. Some command and control systems may require mobility. These systems would therefore not be able to afford large, heavy, bulky communication systems and processors. Each command and control system has its own unique blend of these

characteristics. Each of these characteristics is elaborated in the following paragraphs.

1. Connectivity

One of the most obvious characteristics of a command and control system is that it requires connectivity of its communication systems. As is easily observed in the previous Figure 14, if the communications between any of the functions is severed, then the process becomes seriously degraded if not brought to a complete halt. If the communications between the intelligence community and the planning staff is severed, they are forced to formulate plans without the best, current information. Similarly, if the communications between the staff and the commander is destroyed, the commander is left to make a decision without the analysis of his staff. Finally, if the communication link between the commander and his forces does not exist, the commander is powerless and his forces are no longer under his control.

2. Accuracy

The commander and the forces have placed a tremendous amount of reliance on the information provided to them by the command and control system. Accuracy is vital. Garbled communications can lead to misunderstood commands. Incomplete staff analysis, inaccurate or inappropriate

processing algorithms, can all lead to faulty decisions. Deceived intelligence can lead to manipulated decisions.

3. Timeliness

The command and control system must be able to match the pace of changing events in the environment. The environment imposes the time-line within which decisions are made and acted upon. The overall time-line must be apportioned to each command and control function, including the communication time. If intelligence is received by the commander after the battle, it is useless. If planning functions take longer than the allocated time, the commander may have to make decisions without thorough analysis. If a commander is unable or unwilling to make decisions within the time allowed by the environment, opportunities may be lost by the forces in the field. Timeliness is an important characteristic of the command and control system.

4. Authenticity

One of the tenets of command and control states that the system is the means for a commander to exercise his authority over assigned forces. It is through the command and control system that he directs and maintains control. In contrast to a system where orders are transferred face to face, authenticity of orders received over radio communication systems are not as easily verified. Forces

must respond to valid orders, but how are valid orders distinguished from an order that appears valid but was sent by someone other than the commander? The commander also must be assured that the status reports he receives from his forces and isolated sensors are authentic representations of their actual condition. The command and control system needs to verify that the message received is the message that was sent and by whom that message was actually sent.

5. Secrecy

The command and control system is the means by which actions and reactions are planned and assigned. This information can be of vital importance to an adversary. This includes the sources of intelligence, the options under consideration, the decisions reached, and the details of the execution. With this information, the enemy can be prepared to counter every action. The ability to maintain secrecy is essential to most command and control systems.

6. Covertness

Often times it is not only necessary to protect the details of missions or operations, but also the mere existence or location of forces and sources. In these circumstances covertness of the command and control system is of vital importance.

7. Availability

Another characteristic of the command and control system is its availability. This characteristic encompasses a wide variety of factors. The reliability of the equipment and personnel is of vital importance. If the equipment is off line for repairs, or personnel are not at assigned locations, those functions that the command and control system is relying on are not "available". There may be perfect connectivity of the communication system but if frequencies have not been assigned to the mission, priorities assigned, or there are differing editions of cryptographic keys, then the communication system is not available to support command and control. If vital analysis support is either destroyed or engaged in other processing activities then it is not available. It is not only important to have command and control capabilities, but also to have it when it is needed.

8. Affordability

Affordability is more than simply the development and purchase cost of the command and control system. It also includes the operating and maintenance costs of the system, power and processing costs, personnel and training costs, size and weight costs, the information gathering, storing, and analyzing costs, the cost of losing it to the adversary, and the cost of its destruction to the

effectiveness of the command and control system. Specific missions may not be able to afford assigning large numbers of people to operate a command and control system. This system may require the gathering and storage of large amounts of information, but that information may not be effectively stored or processed because of the limitation of human resources. Another system may so centralize the command and control function such that its destruction or disruption may paralyze command and control or its loss to the enemy would in essence provide him the ability to control friendly forces. All of these are affordability issues in the broadest sense.

Hypothesis 25: The primary characteristics of a command and control system are connectivity, accuracy, timeliness, authenticity, secrecy, covertness, availability, and affordability.

E. THE COMMANDER'S PERCEPTION

The final command and control issue to be addressed concerns the isolation of the commander from reality. Modern command and control allows the commander to be physically removed from the actual battlefield, over the horizon, or halfway around the world. One advantage of this is that the commander in a distant command center is not in imminent danger of being captured. The glaring disadvantage is that once he is removed from the actual battlefield, he is totally dependent on his command and

control system to perceive the battle. The commander no longer sees actual events but sees a reflection or representation of the events. All external information is filtered through his command and control system. This total dependence on the command and control system provides a requirement for greater accuracy and authenticity. The commander must also recognize the errors and biases that can be introduced to the system and make allowances for them in his decision process. This leads to the final conclusions about the nature of command and control.

Hypothesis 26: The commander is shown a filtered representation of the current situation through his command and control system, not the actual situation.

Hypothesis 27: Errors and biases can be introduced by the command and control system.

Hypothesis 28: The commander is totally reliant on his command and control system to provide accurate information and to accurately disseminate his decisions.

* * * * *

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. (Sun Tzu, p.25).

IV. THREATS TO COMMAND AND CONTROL

> The Soviets recognize clearly the systemic dependencies of modern military forces on command, control, and communications (C^3). As a result, they have developed a formidable capability to degrade the C^3 assets of enemy forces. The Soviet doctrine of radioelectronic combat (REC) includes an integrated program of C^3 countermeasures using a combination of reconnaissance, jamming, firepower, and deception to disrupt effective command and control. REC is integrated into all aspects of the Soviets' combat operations, displaying their intention to control the electromagnetic spectrum and deny it to their enemy. (DOD, 1988, p. 88)

A. WHAT IS A THREAT ?

Just as the need for having common terminology was important for the previous two chapters concerning the nature of security and the nature of command and control, it is equally important to the discussion of threat. Unfortunately, The Joint Chiefs of Staff do not define the term "threat". As a substitute, Webster defines threat as:

> THREAT - n.
>
> 1. an expression of intention to hurt, destroy, punish, etc., as in intimidation.
>
> 2. an indication of imminent danger: as, the threat of war.
>
> (Webster, 1969, p. 772)

Analyzing this definition, "threat" is seen as a <u>potential</u> injurious action. Because it is a possible future action, there is uncertainty whether or not it will

actually occur and therefore it has an associated probability of occurrence. This is in contrast to a "hostile action" that is actually taking place and where there is no uncertainty about its occurrence. This leads to the following hypotheses:

Hypothesis 29: A threat is a possible, future hostile or injurious action.

Hypothesis 30: There is a probability of occurrence associated with each threat.

Hypothesis 31: A "hostile act" is the realization of a threat. It is a threat that is being executed.

There is much emphasis placed within military intelligence operations on defining all the possible threats and trying to determine their likelihood of occurrence. The better the intelligence, the less the uncertainty, the better the employment of security measures, and the less damage the threat can cause.

In designing security measures to counter threats, there are two types of threats that must be considered. The first is the "potential threat" which is the maximum force or effort an adversary can expend if he concentrated all of his resources into this single effort. The second type of threat is the "probable threat" which takes into account the fact that there are possibly other priorities for the adversary and that he will probably not apply all of his resources in this one effort.

Hypothesis 32: The "potential threat" is the maximum force or effort an adversary can expend if all of his resources were applied to this single effort to breach security measures.

Hypothesis 33: The "probable threat" is an estimate of the most likely levels of force an adversary will expend in his effort to breach the security measures.

What level of threat should the system be designed to resist? Ideally, a system should be designed against all possible "potential" threats. Unfortunately, the cost of this method is often exorbitantly high. Because of constrained resources, security is often designed to a "probable threat" level or at least some threat level less than 100%. If the adversary actually exerts a force greater than the designed security level, then security can be breached. This difference between the designed security level and the security level required to repel the full potential threat is called a vulnerability.

B. VULNERABILITY

While the JCS do not have a definition for "threat", they do define the word "vulnerability". The following is the JCS definition:

VULNERABILITY -

1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.

2. The characteristics of a system which causes it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

(JCS Pub 1, 1979, p.367)

In this definition, the JCS define a vulnerability as a characteristic of the object or system. When this characteristic is exposed to an outside hostile force or action, the consequence is a decrease in the effectiveness or value of the object being protected. The vulnerability can then be considered any characteristic that will allow a hostile action to degrade the system.

Since security measures are system design characteristics that prevent a hostile action from affecting the system, there is an unmistakable relationship between security measures and vulnerabilities as was previously discussed in Chapter II.

In essence, what that discussion described was a security process. The input to the system is a hostile action that was some percentage of the maximum threat level. The security measures are designed to repel a specific level of the potential threat, and the vulnerability is the percentage difference between the potential threat and the applied security measures. The consequence of this interaction between the hostile action and the security measure is a degradation of the value of the protected item.

The "security process" transforms the hostile action into a percentage change of the value of the protected item.

Hypothesis 34: A vulnerability is the lack of adequate security measures to protect against potential threats.

C. EXAMPLE OF THREATS AND VULNERABILITIES

The following example may help to explain further the concepts of threat and vulnerability. A hypothetical gymnasium roof was designed to hold 20,000 lbs. of snow weight. During the night, a record level of snow fell with 25,000 lbs. accumulating on the roof. The structural members of the gym buckled and the roof collapsed. In this example the interlocking architectural structure was the security system. The protected item was the interior of the gym and the value measure was the amount of snow allowed in the interior of the gym.

The architect assumed the maximum load the roof would have to hold was below 20,000 lbs. The roof was therefore designed with a built in vulnerability to any weights over the design maximum 20,000 lbs. Figure 15a shows the assumed probability distribution of snow weight. Implied in this distribution is the assumption that the probability of a threat greater than 20,000 lbs. was zero. Clearly in this example, the maximum potential threat was not 20,000 lbs. but at least 25,000 lbs. Figure 15b shows a new distribution, with 25,000 lbs. as the maximum potential

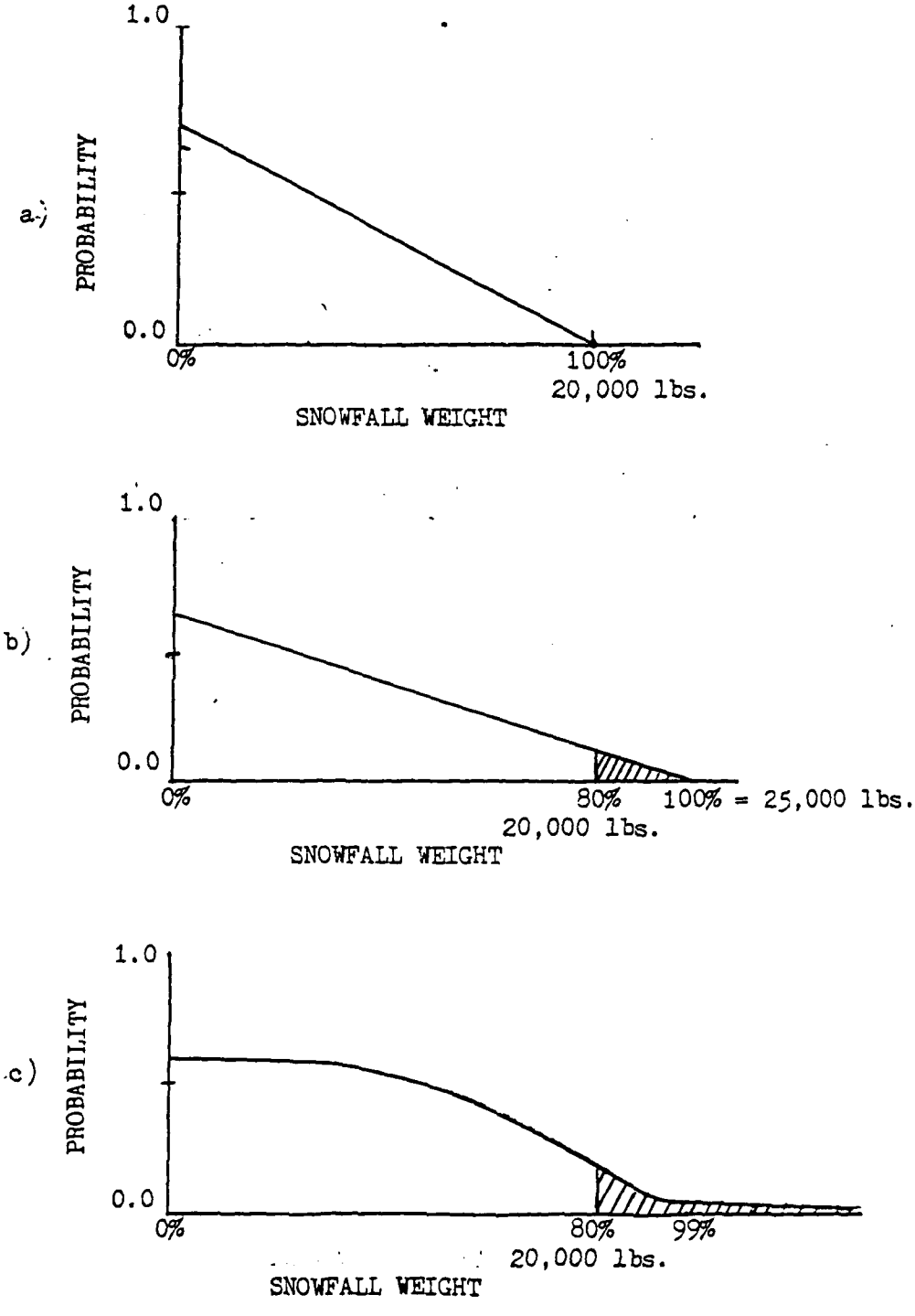


Figure 15. Snowfall Threat Probability Distributions

threat. The vulnerability level is shaded. If the 25,000 lbs is used as the estimate of the 100% potential threat level, then the following calculations can be made:

Potential Threat	= 25,000 lbs.	= 100% Threat
Security Level	= 20,000 lbs.	= 80% Threat
Vulnerability Level	= 5,000 lbs.	= 20%

A probable threat in this example would be an assumed "most likely" snow fall. This could correspond to the normal or average snowfall which would be some level less than the maximum 25,000 lbs. On the probability distribution, the normal snowfall would be the mean of the distribution and the probability of its occurrence would be 50% (the area under the curve less than or equal to the mean).

A more realistic view of this problem would be to view the potential threat as a continuous infinite probability distribution with an ever decreasing probability of occurrence. Figure 15c shows this type of distribution. There is always a possibility that the threat level is higher than whatever level is assumed, but its probability becomes much less as the threat level increases. In this case, the security level and the probable threat levels can be established, but the potential threat and vulnerability levels are theoretically infinite. If a confidence level is established, then calculations can be computed from the

assumed potential threat level. For instance, if 25,000 lbs. is again established as the potential threat, but with a 99% confidence level (the area under the curve less than or equal to 25,000 lbs.) instead of 100%, the calculations for the security level, probable threat, and vulnerability would remain the same as in the second distribution. The architect would only be 99% confident of his estimate though. At least he would recognize the possibility of a threat greater than his designed security level. The system could then be designed with an agreed upon maximum vulnerability level, in this case, 1%.

Hypothesis 35: Vulnerabilities are inherent characteristics of a design.

Hypothesis 36: A system designer does not have control over the threat.

Hypothesis 37: A system designer does have control over the design vulnerabilities through the design security level.

These conclusions imply that if a system is to be designed properly to operate within its environment, the threat to the system must be identified. And in order to design a secure system, the security level must be set to exceed the level of the potential threat.

It is also apparent from the previous example, that good information about the potential threat and the probable threat is important. Unfortunately that information is often not accurate, not current, incomplete,

and, especially if the adversary is trying to operate secretly and covertly, difficult to obtain. Security designers are therefore faced with the task of trying to design a security system to withstand assumed threat levels. How well those estimates are made can be a fundamental factor in the outcome of a hostile action.

D. THREAT MOTIVATION

In designing a security system with limited resources, two fundamentally different types of threat must be considered. The first type of threat is the natural or environmental threat such as snowfall, floods, weather, seasons, physical laws, and natural radiation. The second type of threat is manmade. This includes theft, robbery, assault, and murder in society and jamming, espionage, bombardment, and nuclear attack on the battlefield.

In order to design safeguards against the first, an understanding of the environmental conditions and processes is required. To design effectively against the second type requires an understanding of the motivation of the adversary. Is the adversary's purpose to disrupt or to halt an operation? The force level required to disrupt may be much less than that required to halt an operation and security measures designed to protect against one may be totally useless against the other. Unless there are enough resources to protect against both, an evaluation of the

motive and therefore the most likely methods become a necessity.

E. THE PROTECTED ITEMS OF COMMAND AND CONTROL

To analyze the security of command and control systems it is helpful to translate the C^2 system into a series of security processes. The protected items in this case are the eight primary characteristics of a command and control system: connectivity, accuracy, timeliness, authenticity, secrecy, covertness, availability, and affordability. These represent the real goals of an adversary in attacking a command and control system. His hope is that by degrading or destroying these traits in the system, he can prevent the successful execution and coordination of the mission.

The value measurement level for each of these characteristics is different. Conceptually they can be considered as follows:

1. Connectivity: The percentage of the original communication capability that is available to transmit command and control messages.
2. Accuracy: The percent of accurate information that is transmitted or stored in the system.
3. Timeliness: The percent of operations and messages that are performed within their allocated portion of time to respond.
4. Authenticity: The percent of messages and orders that can correctly be determined to have come from their stated source in the same form as they were sent.

5. Secrecy: The percent of operational information that is unknown to the adversary.

6. Covertness: The percent of the operation's existence and location that is unknown to the adversary.

7. Availability: The percent of the required command and control resources (communications, personnel, equipment, and facilities) that are available at the required times.

8. Affordability: The percent of total required resources available to execute, operate, and maintain the operation.

The security measures applied to command and control systems will be discussed in the next chapter. This chapter will now focus on the nature of the threat to command and control.

F. TWO COMMAND AND CONTROL THREAT MOTIVATIONS

There are two major threat motivations affecting command and control. The first is an adversary's desire to gain information about the operation or mission. This is an intelligence threat to command and control. Because of the wealth of information transmitted between and stored within the personnel and equipment of a C^2 system, it is a prime intelligence target.

The second major motivation is to disrupt or destroy the command and control system from performing its decision making and force direction function. This is a C^3

countermeasure (C^3CM)[1] threat (Littlebury, 1986, p.33). Since the command and control system is the means by which a commander directs his forces to accomplish the mission, degradation or destruction of this system can paralyze the forces without the need for destroying the firepower.

These two major motivations by an adversary to exploit command and control lead to very different threats. Figure 16 shows a tree of potential command and control threats and Figure 17 shows a matrix of which command and control characteristics these intelligence and countermeasure threats can affect.

The emphasis the adversary places on each motivation can also change during different phases of war. During peacetime or heightened tensions, the intelligence motivation may be of prime concern with very little actual motivation to disrupt U.S. command and control. During the first stages of actual war, the predominance shifts to disrupting or destroying command and control in order for an adversary to execute his operations with as little resistance as possible. In later phases of war, a balance is struck between the need for information about the enemy and the need to decrease the potency of the opposing

---

[1] Although throughout this thesis C^2 has been emphasized, the most commonly used term for this threat is C^3CM. Rather than develop a new term to maintain internal consistency, the more common C^3CM will be adopted.

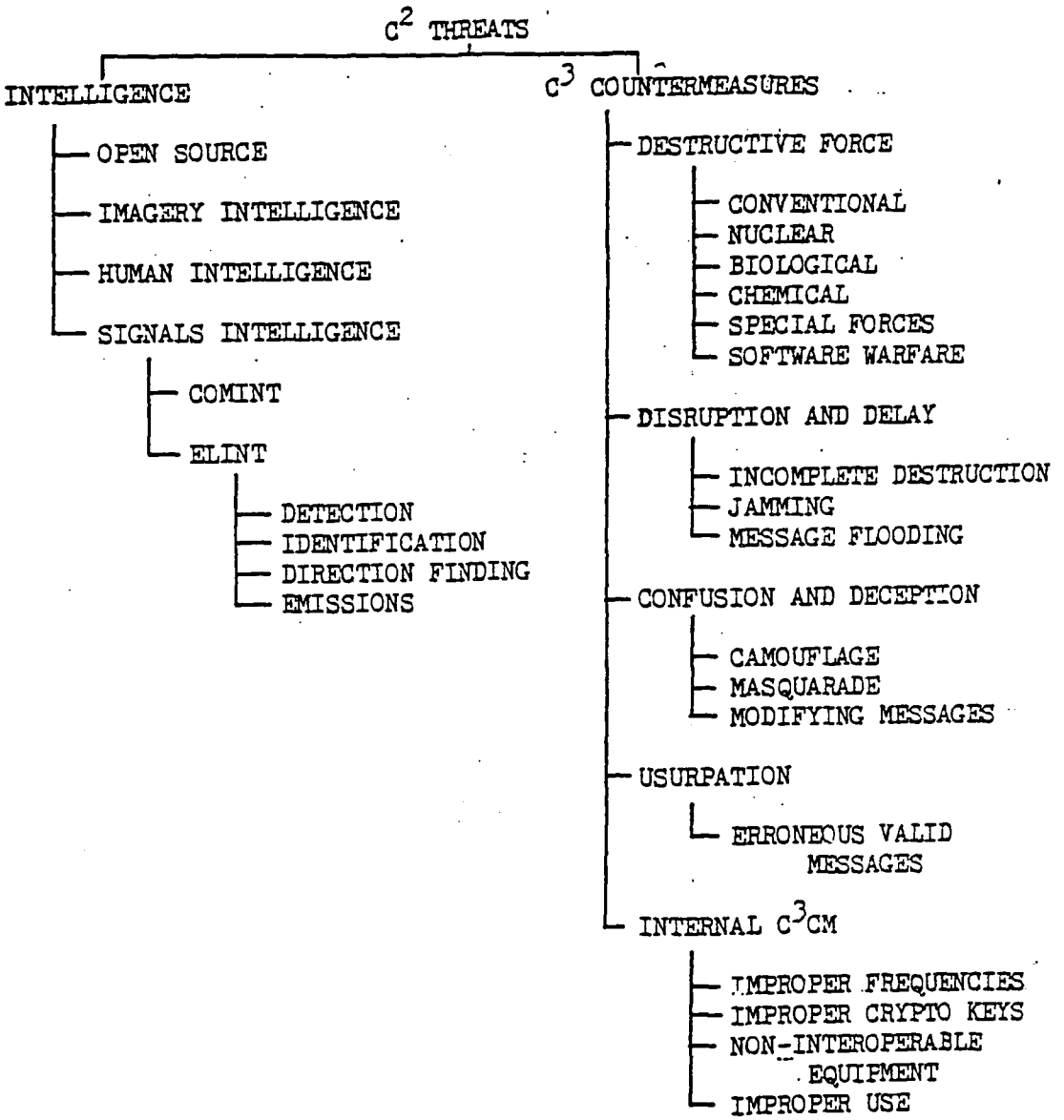


Figure 16. Command and Control Threats

THREATS \ CHARACTERISTICS	CONNECTIVITY	ACCURACY	TIMELINESS	AUTHENTICITY	SECRECY	COVERTNESS	AVAILABILITY	AFFORDABILITY
OPEN SOURCE INTELLIGENCE					X	X		X
IMAGERY INTELLIGENCE					X	X		X
HUMAN INTELLIGENCE					X	X		X
SIGNALS INTELLIGENCE					X	X		X
DESTRUCTIVE FORCE	X	X	X				X	X
DISRUPTION AND DELAY	X	X	X				X	X
CONFUSION AND DECEPTION		X	X	X				X
USURPATION				X				X
INTERNAL C^3CM	X	X	X	X	X	X	X	X

Figure 17. C^2 Threats vs. Characteristics Matrix

forces. Different security measures are required to defeat each class of motivational threats.

G. INTELLIGENCE THREATS TO COMMAND AND CONTROL

Intelligence threats to command and control involve a whole class of actions by an adversary to determine the nature, capabilities, and intentions of an opposing force. The JCS define intelligence as:

> INTELLIGENCE - The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or area. (JCS Pub 1, 1979, p.177)

Intelligence can be gathered in a variety of ways from a command and control system. These include: Open Source Intelligence, Imagery Intelligence (IMINT), Human Intelligence (HUMINT), and Signals Intelligence (SIGINT). The primary purpose of intelligence is to gain a better understanding of the environment and an adversary, thereby reducing the level of uncertainty on the battlefield. It allows commanders to anticipate an adversary's actions and to more effectively apply his own resources, both offensively and defensively.

1. Open Source Intelligence

Open source intelligence comprises three different collection activities: collection of legally available

documents; open observation of foreign political, military, or economic activity; and the monitoring and recording of public radio and television broadcasts (Richelson, 1985, p.173). Although open source intelligence deals primarily with sources other than a military command and control system, there are still open source threats to command and control.

One open source intelligence threat against command and control systems concerns the broadcast and publishing of command and control information by reporters and journalists. Their information may come from leaks to the press by political or military leaders, inadvertent statements of command and control information to the press or in open forums by informed individuals, or through conclusions drawn by reporters and journalists observing the military operation. Once in the public medium, this information is readily available for use by an adversary. Because all of this information was collected within the public domain, its collection and reporting is not illegal, however it can be just as damaging to an operation as covertly collected information. The press in this instance is like a "public" intelligence collecting and reporting agency.

The observations and hearing of public comments do not necessarily have to be restricted to reporters. Any operation in public view or statements made in public can be

picked up and relayed to an adversary for his use and analysis. This may be through informing the media, or it may be through direct or indirect communications with an adversary.

The information transferred may be the existence of an operation, the location, the time of movement, the strength or capabilities of the operational force, or even speculation on the actual mission itself. All of this command and control information can be damaging when in the hands of an adversary. Thus security of command and control systems must take into account the possibility of open source intelligence and take the necessary safeguards to protect itself.

2. Imagery Intelligence (IMINT)

Imagery intelligence is the collection of "pictures" of a region or item of interest and the analysis of those images for information. Although the word "picture" was used, imagery intelligence coveys more than just conventional photographs using the visual spectrum. It can include infra-red images or even radar images. Whatever the actual medium or spectrum that is used, the objective of IMINT is to obtain useful information from the analysis of images. Photographic intelligence is one aspect of IMINT focusing on the visual spectrum. The JCS defines photographic intelligence as:

PHOTOGRAPHIC INTELLIGENCE - The collected products of photographic interpretation, classified and evaluated for intelligence use. (JCS Pub 1, 1979, p.259)

In essence it is the use of visual images and pictures to provide information about an adversary.

IMINT can provide evidence of an operation, a force's location, the size, nature, and location of command centers, and, over time, provide an indication of increases or decreases in operations or movement. It can provide evidence of physical presence, noticeable physical characteristics, location, and orientation. These are all useful pieces of information for an adversary.

Since command and control systems utilize sensors, command centers, and antennas, their physical observation can provide information to the adversary. Therefore, if the operation is to be covert, physical observation of the command and control system must be reduced to an absolute minimum.

3. Human Intelligence (HUMINT)

As was previously mentioned, there is a wealth of critical information residing within the command and control system. While good design and operation of a command and control system can reduce the amount of electromagnetic information an adversary can extract from the system, there are still the human elements of the system that pass in and

out of the secure boundaries of the system. These personnel retain a tremendous amount of the information in the command and control system within their memories when operating outside the confines of the system. This is opposed to the memory of command and control computer systems that may have severe restrictions and controls placed on them if they were to leave the command and control system for use elsewhere or for maintenance. It is because the personnel in the system acquire tremendous amounts of information that human intelligence is a serious potential threat to command and control.

One type of human intelligence that is used is the recruiting of individuals already within the command and control system. John Walker and Jerry Whitworth are prime examples of this type of human intelligence. They both had already passed the screening process and were afforded access to sensitive cryptographic information.

Another type of human intelligence is the actual penetration of a command and control organization by spies of the adversary. This may include break-ins to collect information or the planting of informants within the organization to obtain information from individuals, communications, or computer systems within the secured facilities. Although there is tremendous risk involved in these operations to an adversary, a success can provide a rich dividend of command and control information.

A third type of human intelligence is actually a combination of human and signals intelligence. This involves the planting of transmitting devices within the facilities or equipment of the command and control system. This implantation could occur within the facilities itself or during transportation and maintenance of equipment. Rather than waiting for the information to be transmitted or radiated, the adversary provides the transmission medium. Once implanted, the threat then becomes an enhanced signals intelligence threat.

4. Signals Intelligence (SIGINT)

Modern command and control systems are depending more and more on electronic equipment to obtain the required processing, storage, speed, and communication distances. Each electronic system emits its own type of electromagnetic radiation, both intended and secondary. Communication systems utilize the properties of electromagnetic fields and waves to transmit information over the horizon. Those electromagnetic waves are available not only to the intended receiver but to anyone, including an adversary, in a proper location to receive that radiation. Similarly the secondary radiation such as side lobes from antenna configurations or general radiation emission from electronic equipment can also reveal

information to an adversary if they are properly positioned to receive that radiation.

Signals intelligence includes many different aspects of collecting information from an adversary's electromagnetic radiations. The following is the JCS definition of signals intelligence:

> SIGNALS INTELLIGENCE - A category of intelligence information comprising all communication intelligence, electronic intelligence, and telemetry intelligence. (JCS Pub 1, 1979, p. 314)

a. Communication Intelligence (COMINT)

Communication intelligence, as its name implies, is the derivation of information from an adversary's communications. This includes the monitoring of an adversary's un-encrypted communications, deciphering its encrypted communications, and analyzing the amount communication traffic.

The easiest form of communication intelligence is the simple monitoring of the unprotected conversations and messages that are transmitted through the electromagnetic ether. Once the proper frequencies and modes of transmission are determined, an adversary can listen and understand the transmitted command and control information at the same time as the intended recipient. An adversary can receive a tremendous amount of information from monitoring "clear" communications.

Once the communication systems are encrypted, the contents of a conversation or message are much more difficult to obtain. This requires either breaking the encryption system used, or stealing the cryptographic equipment and cryptographic key being used. Cryptanalysis requires the expenditure of tremendous resources and can be time consuming. The British and American effort to break the German ENIGMA code in World War II is a testimony to the difficulty of this process (Kozacuk, 1984).

The stealing of cryptographic equipment and code is another method. This, like human intelligence is risky but can provide tremendous amounts of information. Walker and Whitworth are an example of this type of threat and the damage it can cause. The threat is not only to current communications, but the theft of cryptographic key may also allow an adversary the capability to read previously recorded encrypted traffic and collect command and control information from those messages as well.

The damage of stolen cryptographic key is further enhanced by the assumption by users that the encrypted communication systems are still secure. Under those circumstances a user would still be willing to transmit very sensitive command and control information. If that same user had only a known, unsecured communication path, he would be more cautious about the information transmitted.

Even if a communicated encrypted message is not deciphered, there is still information that can be obtained from communications. Traffic analysis studies the amount of traffic that is transmitted and where that information is being sent. An increase or decrease in message traffic or traffic routing can indicate a change in the operation to an analyst.

Call signs, frequencies, and other operator signatures are also indicators of the identity of a transmitting unit. Even the transmission itself can reveal the existence and location of a unit. There is a tremendous amount of information that can be derived from communication intelligence.

b. Electronic Intelligence (ELINT)

The derivation of information from electromagnetic signals other than communication signals is called electronic intelligence. This type of radiation includes radar, beacons, and the telemetry from satellites and weapons. The JCS define electronic intelligence as:

> ELECTRONIC INTELLIGENCE - Technical and intelligence information derived from foreign, non-communications, electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JCS Pub 1, 1979, p.121)

The first aspect of electronic intelligence is simply the detection of a signal. Its mere presence is

information that something is out there that needs to be investigated further to determine if it is hostile. This is a detection threat.

Another aspect of electronic intelligence is the monitoring of all electronic emissions from an adversary to try to determine the nature of the source from the frequency and characteristics of the signal. One radar system associated with an anti-aircraft unit may have an entirely different electronic signature from a command and control center. There also may be subtle differences that can be detected between similar type equipment. By studying these emissions, an analyst may be able to determine the type and nature of units they are opposing. This also applies to the telemetry of satellites and weapon systems. By understanding the signals, an analyst can often draw conclusions about the characteristics of the satellite or weapon system. This is sometimes called telemetry intelligence (TELINT).

A third aspect of electronic intelligence attempts to determine the precise bearing, or, using two or more bearings, the precise location of the source of an emission. This is called direction finding or location finding. The JCS define direction finding as:

> DIRECTION FINDING - A procedure for obtaining bearings of radio frequency emitters with the use of a highly directional antenna and a display unit on an intercept

receiver of ancillary equipment. (JCS Pub 1, 1979, p.110)

If an adversary knows that a signal exists, its location, and its composition, then countermeasures can be employed against that source. And if that source is a critical command and control element, the countermeasures may seriously disrupt or destroy effective command and control. Whenever ELINT is determined to be a serious threat, security measures should be applied to lessen or eliminate the impact of the threat on the command and control system.

A final area of electronic intelligence concerns the secondary radiation of electronic equipment into its immediate environment. Although the radiation level is quite small in comparison with communication system or radar emissions, information may be passed for relatively short distances by this secondary radiation (Hsiao, 1979, p.99). If an adversary is able to receive and record these signals, information that was assumed to be protected may actually be within the hands of the adversary.

H. COMMAND, CONTROL, AND COMMUNICATION COUNTERMEASURES

Unlike the intelligence threat that welcomes the open use of command and control systems so that it can obtain critical information, the command, control, and communication countermeasure (C^3CM) threat seeks to

interfere with the command and control process. The overall objectives of C^3CM are listed below:

1. Destroy - To destroy or render useless an adversary's communication system or command and control functions.

2. Disrupt - To disrupt an adversary's communication system or command and control functions to the point where they are no longer considered reliable.

3. Delay - To delay an adversary's communications, processing, or execution of command and control functions to the point where the command and control system can no longer respond within the required time frame.

4. Deceive - To deceive an adversary's sensors or personnel into believing the environment is different than what actually exists.

5. Confuse - To confuse automatic and human decision making processes to the point where appropriate decisions are no longer reliably made.

6. Usurp - To usurp control of an adversary's command and control process allowing for direction of his forces.

These objectives are not mutually exclusive of one another and can be executed in a partial fashion. For example, if an adversary were to know the proper telemetry signals controlling a communication satellite, he would then possess the ability to usurp control of that satellite. By then moving the satellite in its orbit or directing a reorientation of its antenna, the adversary will then be able to cause a certain amount of disruption, delay, and confusion in the transmission of command and control information. Assuming that there are redundant

communication paths, after a period of time, all users would realize that this one communication path was no longer available and switch to another. If there were not redundant paths, this same action could destroy the only communication path.

Another example would be an adversary covertly usurping control of an isolated radar site. If this action were truly covert and the status feedback messages to the controlling site did not register any change in status of the radar, then the adversary could use that radar site to send false information, and deceive his enemy.

The Joint Chiefs of Staff first define a broader category of "countermeasures" and then define a subcategory of "electronic warfare". These are restated below:

> COUNTERMEASURES - That form of military science which by the employment of devices and/or techniques has as its objective the impairment of the operational effectiveness of enemy activity. (JCS Pub 1, 1979, p.91).
>
> ELECTRONIC WARFARE - Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. Also called EW. There are three divisions within electronic warfare:
>
> a. electronic warfare support measures - That division of electronic warfare involving actions taken under direct control of an operational commander to search for, intercept, and identify/locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support measures provide a source of information required for immediate decisions involving electronic

countermeasures, electronic counter-countermeasures, avoidance, targeting, and other tactical employment of forces. Also called ESM.

b. electronic countermeasures - That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Also called ECM. Electronic countermeasures include:

(1) electronic jamming - The deliberate radiation, re-radiation, or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment, or systems being used by an enemy. Also called jamming.

(2) electronic deception - The deliberate radiation, re-radiation, alteration, absorption, or reflection of electromagnetic energy in a manner intended to mislead an enemy in the interpretation or use of information received by the enemy's electronic systems. There are two categories of electronic deception: (a) manipulative electronic deception - The alteration or simulation of friendly electromagnetic radiations to accomplish deception. (b) imitative electronic deception - The introduction of radiations into enemy systems which imitate the enemy's emissions.

c. electronic counter-countermeasures - That division of electronic warfare involving actions taken to retain effective friendly use of the electromagnetic spectrum. Also called ECCM. (JCS Pub 1, 1979, p. 121)

Electronic warfare is a major aspect of C^3CM but it does not encompass the non-electromagnetic aspects of the command and control process. A more comprehensive definition is found in the Armed Forces Communications and Electronics Association (AFCEA) book Invisible Combat: C^3CM - A Guide for the Tactical Commander. They define C^3CM as:

Command, control and communication countermeasures (C^3CM) is the integrated use of physical destruction, electronic warfare (EW), operations security (OPSEC), and military deception; all supported by intelligence,

> with a two-fold intent - one, degradation of enemy C^3, and two, protection of friendly C^3 from enemy degradation. (Littlebury, 1986, p.33)

One last definition that requires study is the Soviet Union's doctrine of radioelectronic combat (REC). REC is the electronic portion of "maskirovka" which is an overall military and political "masking" of true intentions and deception (DOD, 1988, p. 88). Radioelectronic combat is integrated into all aspects of the Soviet's military operation and consists of countermeasures using a combination of reconnaissance, jamming, firepower, and deception to disrupt enemy command and control (DOD, 1988, p. 88). The Soviet definition encompasses all of the U.S. definition of electronic warfare and adds the firepower used to destroy communication nodes and command and control elements, plus other non-electromagnetic means to deceive and disrupt command and control. This includes the use of 27,000 to 30,000 personnel in the GRU (a Soviet military intelligence organization) special forces known as Spetznaz to operate behind enemy lines, neutralizing command centers, staffs, and lines of communications (Richelson, 1986, p. 162).

From the preceding discussions, it is apparent that the threat to command and control encompasses more than "electronic warfare". C^3CM also takes into account the applied destructive firepower, sabotage, actions against

command and control personnel, and the introduction of errors. The following sections will describe the following broad C^3CM motivations: Destructive Force, Disruption and Delay, Confusion and Deception, Usurpation, and Internal C^3CM.

1. Destructive Force

a. Conventional Weapons

This is the most familiar threat in a military conflict--the application of destructive firepower on a specific target. Artillery fire, aircraft bombardment, and targeted missiles are just a portion of the conventional arsenal of weapons that can be used to destroy critical command and control nodes. This type of threat assumes that by destroying the communication systems and critical command and control operations, the means to direct and manage forces will also be destroyed. The destructive force can be applied to communication medium (i.e., telephone cable), their communication centers, antenna, relay points, or satellites. The destructive force can also be applied to the personnel, equipment, and facilities of each command and control function. This would include the sensors, intelligence and analysis centers, command centers, or the forces themselves.

b. Nuclear, Biological, and Chemical Weapons

Conventional weapons are not the only potential threat source. Nuclear, biological, and chemical weapons can also be employed for the destruction of command and control elements. Nuclear weapons can destroy command and control functions not only through their massive destructive capability, but also through the electromagnetic pulse (EMP) and radiation released during detonation (Carter, 1987, pp. 273 - 278). Humans in the command and control system can be seriously affected by the radiation released (L. Martin, 1987, p. 98) and electronic equipment can be damaged by both the radiation and EMP (Carter, 1987, p.277). Just as devastating to the human element of command and control are chemical and biological weapons.

c. Special Forces

As was previously discussed, sabotage can also effectively destroy command and control capabilities. One of the primary goals of the Soviet Union's Spetznaz forces are the destruction of command and control facilities (Richelson, 1986, p. 162). Sabotage can also be conducted by internal opposition groups, traitors, or spies.

d. Software Warfare

Sabotage can include more than the planting of explosive forces. One potentially menacing form of sabotage

is "software warfare" (Boorman, 1988, p. 76). Software warfare is the deliberate modification or insertion of computer software code to cause adverse operations of the computer. Several categories of software warfare include "trojan horses", "logic bombs", "algorithm sabotage", "worms" and "viruses".

Trojan horses are lines of code surreptitiously included in valid code. This code may cause computer systems to shut down, erase files, or perform endless calculations such as computing the square root of two. A "logic bomb" is one form of trojan horse that remains inactive and undetected until a particular date or set of conditions occur (Boorman, 1988, p. 76). A logic bomb rendered several internal records of the Los Angeles Department of Water and Power useless for a week by creating a denial-of-access condition (Boorman, 1988, p. 76).

Algorithm sabotage is not the insertion of erroneous lines of code, but instead alters the underlying algorithm from which the code is later developed. During the Falkland War, the British Sea Wolf missile's guidance algorithm was not provided instructions on how to respond to two enemy aircraft attacking on parallel courses. Unable to resolve the priority of targets, the software shut the system down (Boorman, 1988, p. 77). Other oversights in the underlying algorithm of the software of command and

control systems may prevent the use of computers at critical moments.

Computer worms and viruses are programs that can regenerate themselves and in the process use up tremendous processing time. A worm is a self contained program that, once activated, will continue to replicate itself, often destroying files of data, and with the ability to be transferred over computer networks. On November 2, 1988, a computer worm was released from Cornell University into the Defense Data Network (DDN). For two days the worm infected the computers across the United States that were attached to the DDN. The result was a curtailment or a serious degradation in processing of authentic programs during that period of time. (Buzzard, 1988)

Viruses are programs that are attached to a host program and, like worms, are able to regenerate themselves and destroy data files. Viruses are spread by the sharing of software disks or the transfer of infected programs over a network. Once a virus is resident within a host, it can attach itself to all other programs through the disk operating system. (TIME, 1988, p. 63).

Software warfare or sabotage does not have to occur on the battlefield itself, but can be performed during the writing, development, or installation of the code into command and control equipment (Boorman, 1988, p. 78) and can be spread to several locations from a single attack.

Because of the reliance of modern command and control equipment on software, software warfare must be considered a serious threat.

2. Disruption and Delay

a. Incomplete Destruction

If total destruction is not possible or desirable, an adversary may desire to disrupt or delay the command and control elements. Incomplete destruction is one method of achieving disruption and delay. It will require time to reorganize and reconstruct the command and control network. Disruption and delay can also be achieved by attacking antenna and power sources.

b. Jamming

An effective disruption technique is electronic jamming. This technique attempts to place a sufficient amount of energy over the frequencies used by sensors and communication systems so that the receiver is unable to discriminate the true signal. The following paragraph from the Soviet book Fundamentals of Command and Control shows that the Soviet Union considers jamming to be an effective C^3CM technique:

> Today jamming is considered one of the chief methods of disrupting the operation of enemy electronic equipment. It is capable for a certain period of time of depriving the enemy of the opportunity to receive and transmit

> information over electronic equipment, or it can significantly reduce the audibility and visibility of the signals, deceive the operators, and cause errors in the operation of automated communication devices. (Ivanov, 1977, p.268)

c. Message Flooding

Another form of jamming is the flooding of communication paths with bogus or recorded messages. This can strain the capacity of communication systems while at the same time create queues for automatic message processing systems as they try to sort out the current valid messages from the bogus ones.

3. Confusion and Deception

Confusion and deception require more information about sensors, analysis methods, and use of the processed information than the preceding threats. Camouflage, decoys, simulation of "friendly" signals, emitting electronic signatures of different units or weapon systems, and maneuver techniques are all capable of providing misleading information to the enemy. The hope is that through these actions, the adversary will make erroneous conclusions about the nature or location of the threat which will allow for future exploitation. But in order to effectively utilize these deception techniques, a good understanding of how the adversary collects and utilizes this information is vital. If an aircraft is to masquerade

as a "friendly" aircraft, it must be able to reproduce the radar signature and Identification Friend or Foe (IFF) signal of the friendly aircraft. In order for stealth technology to be effective, knowledge of enemy radar capabilities is required. Deception requires an understanding of the adversary and his methods of operation.

Another method of causing confusion and deception is by modifying current or previous messages and broadcasting those changes. Not only will this cause confusion over the validity of the message and whether the new or previous message were correct, but will also cause a delay in an adversary's action until the confusion is resolved.

4. Usurpation

Usurpation of control is the actual control of friendly forces, sensors, and weapons by enemy forces. The modern battlefield requires forces, weapons, and sensors to be located over vast distances with the communication systems being the only connection between these command and control elements. If an adversary were to be able to send valid appearing messages over those command and control communication systems, the receiving weapon or unit would respond as if they had received an authentic message. Any communication system without an authentication technique is vulnerable to manipulation and usurpation of control. Even with authentication methods applied, communication systems

still must protect those authentication devices from compromise or again the system is subject to exploitation.

5. Internal C^3CM

The final category of C^3CM is not a threat by an adversary on friendly command and control, but what friendly forces can do to themselves. Using improper frequencies, improper cryptographic keys and settings, and equipment that is not interoperable can prevent the transfer of vital command and control information as effectively as enemy jamming. Complete planning, coordination, and training of how command and control equipment will be utilized is crucial in preventing incompatibility from destroying the command and control process.

Similarly improper use of systems designed to protect against enemy countermeasures can render the protective measures useless. Excessive use of the radio, predicable call signs and procedures, and identifying characteristics of operators are all operation errors that degrade the protective character of command and control systems (Ivanov, 1977, p. 269). Just as much emphasis should be placed on eliminating poor planning, coordination, and operation of command and control systems as in preventing an adversary from exploiting it.

V. SECURITY MEASURES

A. REVIEW OF SECURITY THEORY

As was discussed in Chapter II, security measures are the means by which the impact of a hostile action is minimized to retain the greatest remaining value of the protected item. Unfortunately there is not one security measure for each threat to command and control. Security is really a system of security measures working together to provide the required protection (see previous Figure 6).

Chapter II also identified two major categories of security measures which were shown previously in Figure 7. These two classes were passive or boundary security measures and active security measures. The passive security measures serve to create a secure operating environment for the protected item to work within. By restricting the operating environment, there is less area that must be secured and therefore other security measures can be applied with greater concentration. The active security measures monitored and controlled access through the barriers.

B. OPERATIVE SECURITY PRINCIPLES

Security measures can operate under one or more of the following principles:

1. Discourage Hostile Actions (Deterrence).
2. Prevent Successful Hostile Actions (Prevention).
3. Minimize Impact of Hostile Actions (Minimize Impact).

1. Deterrence

Discouragement of a hostile action is often referred to as deterrence and can be thought of as a counter-threat. Nuclear deterrence is a good example of this type of security. Although the Soviet Union possesses significant nuclear capability to threaten the existence of the United States' society, the U.S. also possesses an adequate amount of nuclear retaliation capability to inflict heavy enough damage on the Soviet Union to discourage their converting their nuclear threat into a hostile action (Blair, 1985, p.16). Three important ingredients of deterrence are: a good probability of detecting an attempted hostile action; making the cost of a successful hostile action costly in resources to the adversary; and finally, making the penalty or retaliation high enough and reliable enough so that the expected penalty is greater than the adversary's acceptable threshold.

2. Prevention

Prevention of a hostile action can be accomplished by attacking the threatening forces (preemptive strikes) or by constructing defenses greater than the opposing hostile action. Jamming of an enemy's anti-aircraft radar can be

considered an offensive form of providing security for the friendly attacking aircraft. A field of land mines can be an effective defense against enemy personnel.

3. Minimize Impact

The final principle of security is minimizing the impact of a successful hostile action. If communication systems are established in a network fashion rather than in a serial fashion, the network will continue to operate even with the destruction of one or more nodes or circuits. Redundancy is one application of this principle. Another application of this principle is the concept of "security in depth". Security in depth applies several different security measures simultaneously to counter threats. If one security measure fails, others will be available to catch the remaining hostile action. The several different levels of the Strategic Defense Initiative are an example of security in depth. "Don't put all your eggs in one basket" is another way of describing this principle. Dispersal of resources such as antennas will prevent one attack from destroying all antennas.

C. TYPES OF SECURITY MEASURES

There are thousands of types of security measures available to add to the level of security. Doors and walls, fences and gates, patrols, alarms, locks, and identification

devices are all types of security measures. In addition to the variety of types, there are many variations of methods and quality within each type. For instance, each type of padlock, door lock, or cipherlock operates in a slightly different fashion. Rather than trying to describe each type of security measure currently available, the remainder of this chapter will provide an overview of various classes of security measures. Figure 18 shows the types of command and control security measures.

To repeat what was discussed in the last chapter, there is not a one to one correspondence between threat and security measures. In other words, there is not one security measure by itself that can prevent a hostile action. Security measures must be applied as a cohesive system in order to be effective.

Assume, for instance, a valuable jewel necklace is placed in a hotel vault for safe keeping. The vault can be considered a physical security measure creating a secure environment for the necklace. Even with the radical assumption that the vault is impenetrable once locked, the necklace is still not entirely safe. There is a combination to the vault that allows access to the interior. This is a cryptographic security measure. If an adversary can steal or determine the combination of the vault, he would be free to steal the necklace. The combination to the vault must also be protected in order for the necklace to be safe.

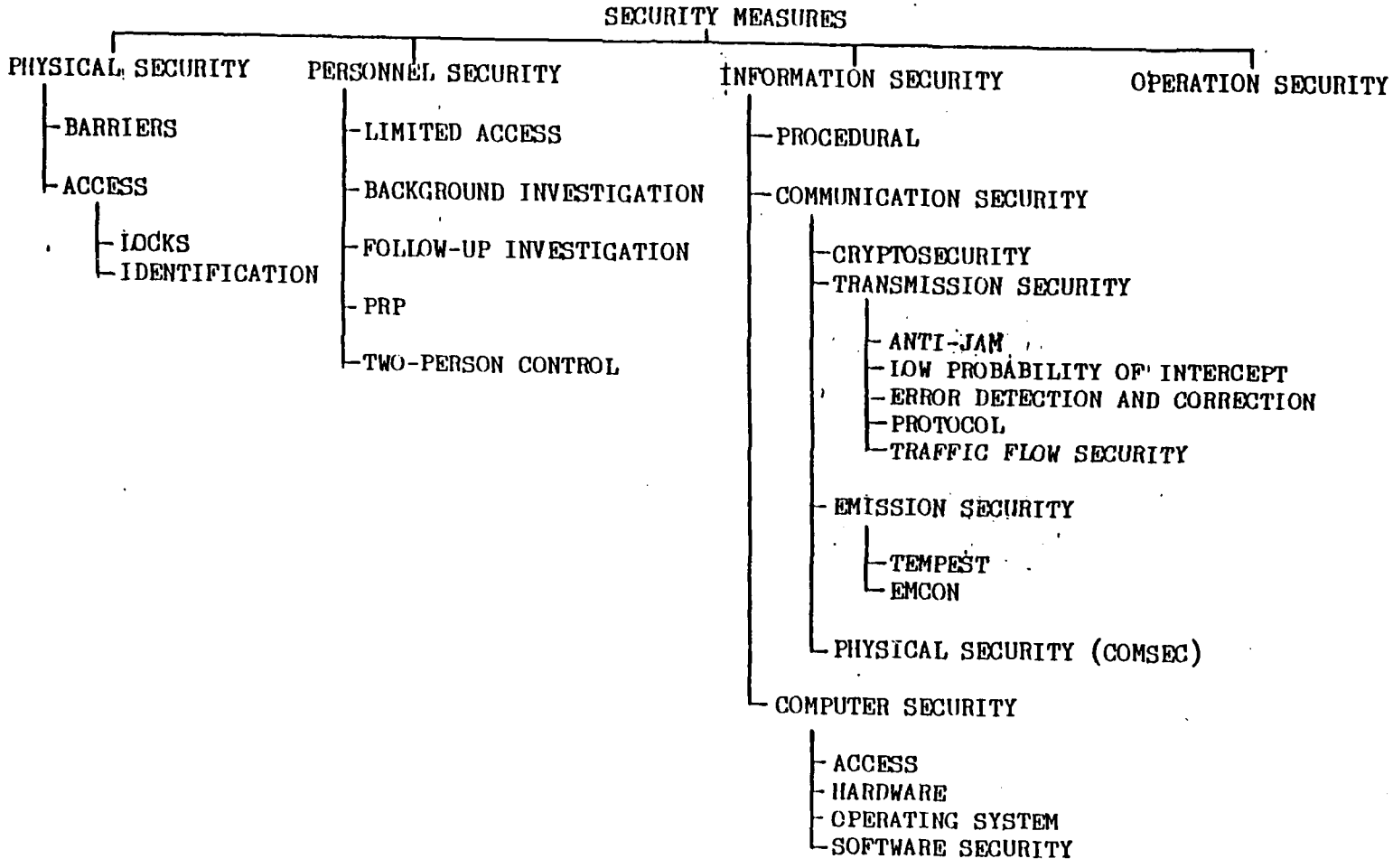


Figure 18. C^2 Security Measures

If individuals know the combination, security measures must be taken to assure that these individuals will not use, or allow to be used, that special knowledge to steal the necklace. This then involves personnel security measures and procedural security measures.

By just concentrating on the security of the necklace, one important threat may be overlooked, the theft of the vault itself. A adversary may not even attempt to break into the vault at its present location. If the vault itself is not secure, the adversary may simply carry it away and work to open it in a location comfortable to him. Security is the result of a system of security measures working together to provide protection.

1. Physical Security

Physical security measures are security devices that create a physical area or environment that is free from unwanted access. Usually this area is relatively small. It can be the confines of a box containing a single integrated chip, the housing of a larger piece of equipment, a room, a building, a base or post, or even a sector of a battlefield. The JCS define physical security as :

> PHYSICAL SECURITY - That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. (JCS Pub 1, 1979, p.260)

Walls, fences, and screens are all examples of passive physical security measures that create a boundary around the safe environment. Patrols, alarms, inspection stations, guard posts, and gates are examples of active security measures controlling the flow of people and equipment through the passive boundaries. In a public airport, the walls of the terminal and the fences surrounding the runway form the passive physical boundaries. Without active physical security measures, these passive measures could eventually be overcome. The active physical security measures assure the integrity of the passive measures and control the flow of passengers, luggage, and equipment into the secure environment. As was previously discussed, active measures involve detection, response, and penalty mechanisms. In this case, the metal detectors at the entrance to each terminal are one detection device; the response is the airport security force; and the penalty is inconvenience of being more closely inspected, missing the flight, or if the offense were serious enough, arrest, trial, and fine or imprisonment.

There are several techniques available to help to improve the security access problem. In order to help protect combinations from being compromised, split-knowledge combinations can be used. Two people, each with a different part of the combination, are then required in order to open

the lock. Many safe deposit boxes operate on this same principle with two separate keys.

Many different identification techniques are also being used. In addition to the standard identification card or badge an authorized individual must carry, some also contain a magnetic chip or magnetic strip similar to credit cards. When entering a secure area, the card is entered into a machine along with a personal identification number. This technique reduces the chance of an unauthorized individual using a valid ID to gain access. Other identification techniques involve the use of eye maps, hand prints, or voice recognition in order to improve the security and efficiency of the access process.

2. Personnel Security

A major portion of the command and control system is performed by individuals. It is essential that the personnel assigned critical command and control functions be trustworthy to perform their assigned duties and to protect the sensitive command and control information.

The first aspect of personnel security is actually performed by physical security methods. That is limiting access to secure areas to only those individuals carrying proper and current identification of authorization.

The process is much more complex when it comes to determining which individuals should be given the proper

authorization for access. This begins with the background investigation process and involves investigators researching an individual's current and past associations and actions to determine the trustworthiness of the individual. The JCS describe this process as "personnel security investigations".

> PERSONNEL SECURITY INVESTIGATIONS - An inquiry into the activities of an individual which is designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability. (JCS Pub 1, 1979, p.258).

Polygraphs can also be used to augment the background investigation process.

Once background investigations have been conducted and a person is allowed access to vital information, periodic or aperiodic follow up investigations are necessary. This follow up investigation is to help detect compromises or a situation that can lead to a compromise. The possibility of having the compromise of sensitive information detected during the follow up investigation also serves as a deterrence.

In addition to the background and follow up investigations, the Department of Defense institutes a more rigorous screening and monitoring program for individuals who have direct access to nuclear weapons or nuclear command and control information. This is called the Personnel

Reliability Program (PRP). The standards are much more strict than normal classified material access. These individuals do not receive assignment or training for the critical positions until they have been fully screened. (Carter, 1987, p. 60)

Another personnel security measure that is applied to control of nuclear weapons and nuclear command and control material is the policy of two person control. Under this policy, nuclear weapons and certain nuclear command and control material must be under the protection of two individuals at all times. This increases the personnel requirements, but also assures, to a greater extent, that theft, tampering, modification, or substitution cannot occur.

Despite all of these techniques, personnel security remains one of the most difficult security measures to design into a security system. Personnel security involves human behavior and is therefore subject to the seeming inconsistencies between motivation and action. Different people will respond in different fashions to the same situation. The uncertainty of human behavior must be considered when designing a security system that involves individuals. As the Federal Bureau of Investigation points out in the following passage from the DOD Security Review Commission's Report, personnel security is based on the loyalty of the individual.

> It is the responsibility of each individual, who has been entrusted with sensitive data, to do his or her share in protecting America's strategic knowledge. If Americans do not conduct themselves in a responsible manner, or do not recognize that this country's national security is based upon the loyalty and efforts of its citizens, then the tightest document classification system, the most efficient security organizations, and the strongest armed forces may be completely ineffective in protecting citizens from "all enemies, foreign and domestic." (Commission, 1985, p. 101)

3. Information Security

Information security is an extremely broad field. It involves techniques for protecting sensitive information from being acquired by the adversary. Usually this information is thought of as written documents or designs, data or verbal messages transmitted over communication systems, data stored within a computer, or information transmitted over communication systems. The protection of this information involves three types of security measures: procedural security, communication security (COMSEC), and computer security (COMPUSEC).

a. Procedural Security

Within the Department of Defense there are three security classification levels which were defined in Chapter II: TOP SECRET, SECRET, and CONFIDENTIAL. Along with these classification levels are a series of policies and procedures issued by organizations up and down the chain of command describing how to handle, store, disseminate, and

destroy classified information (Commission, 1985, p. 47). Executive Order 12356 provides the overall policy for the entire Executive Branch of the United States Government (Commission, 1985, p. 47). These policies and procedures identify methods for individuals to determine classification levels for specific categories of information, with whom they can share that information, the proper storage containers within which the information can be stored, and the proper methods for destroying the information once it is no longer required.

Personnel security is concerned with assuring that only trustworthy individuals are placed in positions responsible for classified information. Procedural security provides the rules under which these individuals must perform in order to protect the information with which they are entrusted. The procedures can only specify how classified information should be handled, it is up to the individual to follow those procedures.

Because of this dependence on the individual to follow this guidance, procedural security is only as effective as the least conscientious individual. If nine out of ten individuals who have access to a particular piece of classified information properly follow security procedures, but one individual fails, for whatever reason, to protect the information, the information is not 90% protected. It is 100% compromised.

Again, because procedural security is dependent on the uncertainties of human behavior, intentional or unintentional, it is one of the least reliable security measures that can be applied. It is also the most extensively used. Although it does not give 100% effectiveness, when combined with other security measures, it provides an extremely important layer of protection in a security system.

b. Communication Security

Communication security is a vast and highly technical field of security involved with protecting information and data as it is transmitted over communication systems. The JCS define communication security as follows:

> COMMUNICATION SECURITY - The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communication security includes a. cryptosecurity; b. transmission security; c. emission security; and d. physical security of communication security materials and information.
>
> 1. cryptosecurity - The component of communication security which results from the provision of technically sound cryptosystems and their proper use.
>
> 2. transmission security - The component of communication security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.
>
> 3. emission security - The component of communication security which results from all measures taken to deny

unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunication systems.

4. physical security - The component of communication security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JCS Pub 1, 1979, p. 77)

(1) Cryptosecurity. Cryptosecurity is probably one of the most sensitive and highly classified of all security measures. Effective cryptographic systems take years to develop, evaluate, and field, but can be rendered useless with even one compromise. It is also the security measure that command and control is most heavily dependent upon. Without the means to provide secure communications, all secrecy of remote operations would be lost.

Cryptosecurity is an encryption/decryption process by which the plaintext, voice or data messages, are transformed into a ciphertext form for transmission. The desired characteristics of the ciphertext include:

1. Non-disclosure - Only the intended recipient of the message can decrypt and understand the contents of the message.
2. Integrity - The message that is received is the same message that was sent.
3. Authenticity - The message could only have come from an authorized source.

Although each cryptosystem is different in its method of providing one or more of the desired characteristics, they usually consist of:

1. Plaintext - The original message that is to be securely transmitted over a communication system.
2. Cryptographic Transformation - The algorithm or logic, used to transform the plaintext into the ciphertext.
3. Cryptographic Key - The unique settings of the cryptographic transformation held only by the authorized sender and intended receiver of the message. This is often the most sensitive part of the cryptosystem.
4. Synchronization Method - This is a means to assure that the sending and receiving stations apply the same cryptographic transformation to the same portion of the message.
5. Ciphertext - The transformed message.
6. Key Management System - The method for assuring that only the authorized sender and intended receiver have the cryptographic key and that the proper cryptographic key is utilized.

Chapter VI provides a general introductory discussion on the field of cryptography.

(2) Transmission Security. Transmission security deals with all methods used to protect communications from interception and exploitation that do not involve cryptography. These include anti-jam (AJ) techniques, low probability of intercept (LPI) techniques,

error detection and correction (EDAC) techniques, proper communication protocol, and traffic flow security.

(a) Anti-Jam Techniques. Anti-jam techniques try to minimize the effects of enemy jamming on a communication system. Frequency hopping is one technique in this category where portions of the signal are transmitted in time blocks over changing frequencies (Ricci, 1986, p. 35). Often the frequency changes are driven by a cryptographic engine to assure a random appearance of the hopping pattern. Another method to provide anti-jam capability is by use of spread-spectrum techniques (Ricci, 1986, p.35). Spread-spectrum techniques increase the required transmission bandwidth thereby forcing a jammer to increase its power requirements to jam this wider band of frequencies. A third technique is the use of highly directional antennas to minimize jamming energy that is not located directly in the path between the authentic transmitter and receiver.

(b) Low Probability of Intercept (LPI). Another category of transmission security involves trying to prevent the interception, detection, or direction finding of the signal. Spread spectrum technology can be used not only for anti-jam purposes but also for LPI. By spreading the bandwidth of the signal, the energy level transmitted at

each frequency is reduced. If the signal is spread large enough, the signal can become indistinguishable from the surrounding noise making it difficult to discover and intercept unless an adversary possesses the proper spreading codes. Once the signal and noise are reconverted by authorized receivers to their original bandwidth, the signal will again become recognizable. Burst communications and directional antennas can also improve the low probability characteristics of a communication system.

(c) Error Detection and Correction. Error detection and correction usually involve the transmission of additional information about the message that will help to indicate that an error has occurred in transmission. This can be performed by a check-sum that is a mathematical function of the message (Hoffman, 1977, p. 96). If there has been any error in transmission or an attempted modification of the message, the check-sum computed at the receiving station will not match the transmitted check-sum. This will provide for detection of errors. More sophisticated mathematical functions called forward error correcting codes can not only help to detect errors in messages but can often help to return the message to its original status (J. Martin, 1976, p.586).

(d) Communication Protocol. Communication protocol refers to how disciplined a communication system operator is in using the system. This is related to procedural security but deals directly with the use of communication systems. Several techniques that fall into this area include:

1. Using a communication system only when necessary (Littlebury, 1986, p. 76).
2. Not using home made codes (JCS Pub 18, 1982, p. D-1).
3. Not "talking around" classified material on unsecured systems (JCS Pub 18, 1982, p. D-1).
4. Operating only at the power output required to communicate or achieve sensor functions (Littlebury, 1986, p.76).
5. Reducing radio transmissions to no longer than 10-15 seconds (Littlebury, 1986, p. 76).
6. Limiting tuning time of transmitter (Ivanov, 1977, p.269).
7. Changing call signs frequently (Ivanov, 1977, p. 269).
8. Eliminating operator "signatures" or identifying characteristics (Ivanov, 1977, p. 269).
9. Turning off transmitter high voltage after completion of transmission. (Ivanov, 1977, p. 269).

(e) Traffic Flow Security. Traffic flow security is a means for assuring that an adversary monitoring the volume of traffic over communication systems will not be able to gain significant indicators of a change in operations. The JCS define traffic flow security as:

> TRAFFIC FLOW SECURITY - The protection resulting from features, inherent in some crypto-equipment, which conceal the presents of valid messages on a communication circuit, normally achieved by causing the circuit to appear busy at all times. (JCS Pub 1, 1979, p. 354)

(3) Emission Security. There are two main categories of emission security -- TEMPEST and emission control. TEMPEST refers to a series of design and shielding techniques to reduce the amount of secondary radiation emitted by a piece of electromagnetic equipment that may reveal sensitive information. Shielded containers and vaults fall into this category.

The second major category of emission security is emission control, often called EMCON. EMCON is an order to friendly units specifying either forbidding primary emission of radiation (radio or sensor), or the selective emission of specific radiation. This is often used to conceal the presence, size, or formation of friendly forces. The JCS define EMCON as:

> EMISSION CONTROL - The selective control of emitted electromagnetic or acoustic energy to minimize its detection by enemy sensors or to improve the performance of installed friendly sensors. Also called EMCON. (JCS Pub 1, 1979, p. 124)

(4) Physical Security. Although physical security was discussed as a topic unto itself, communication security relies so heavily on physical

security, that it is also included as a subheading of communication security. In this case it refers to the physical security of communication security components. If for instance a piece of communication security equipment containing a cryptographic algorithm and cryptographic key were compromised, the adversary would have access to any message sent over that communication system until the key or the algorithm were changed. Cryptosecurity depends on physical security to assure that only the authorized sender and intended receiver have the means to transmit and receive the encrypted message.

c. Computer Security

Computer security, like communication security, is a vast topic unto itself. With the ever increasing use and dependence on computers to perform and assist virtually every aspect of command and control, there is also increasing recognition for the importance of computer security.

Computer security as a discipline is relatively new although some of its security techniques, such as passwords, have been used all through the development of computers. The primary objectives of computer security are:

1. To protect the information residing within the computer system from access by unauthorized individuals.

2. To protect the integrity of the information residing within the computer system from unauthorized modification or elimination.

3. To protect the integrity of the process performed by the computer system.

Although the objectives may be relatively easy to state, the achievement of those objectives is a much more difficult task. Two of a computer's primary assets, its accessibility and the ease with which its instructions can be changed, run counter to the objectives of computer security. Even so, computer security is a dynamic and growing field of security with the need for security outrunning the available techniques.

(1) Access Control. The first aspect of computer security is the ability of a computer to control access to information to only authorized individuals. This can be performed through first allowing only certain individuals to use a computer system or network. Passwords and interactive query password systems can perform this function. Once given access, there still must be a mechanism to assure only the authorized users of stored and processed information can retrieve or manipulate that data. All users may not have authorization for all the information in the computer system. A set of internal rules must be established to assure this separation of information. This is especially true if several levels of classified

information are stored in a computer system and users carry a variety of clearance levels. This is the multi-level security problem. The access control problem becomes even more difficult when multiple computers are linked together in a network.

(2) Hardware Security. Computer hardware can be subject to bugging, sabotage, modification, and substitution. All of these actions can contribute to the compromise of information or disabling the computer at crucial times making them unavailable to perform critical command and control tasks. Hardware security involves maintaining the integrity of the hardware from as early as when it is manufactured, through shipment, installation, operation, maintenance, and even its disposal. Physical security, inspections, equipment accountability, and maintenance logs are all vital elements of hardware security.

(3) Operating System Security. The operating system is just as important to a computer system as the hardware. And just like the hardware, its integrity must be protected to assure that critical command and control information is processed properly. The operating system must also be protected through all phases of its life cycle. If not, trojan horses can be implanted during development, installation, updating or, upgrading of operating systems

with new changes. These can all be sources for unwanted changes.

(4) Software Security. Finally, software security is of vital importance to assure that the application programs themselves do not contain errors, trojan horses, viruses, or worms. While independent line by line inspection of software code can help to ensure the accuracy and integrity of software, the magnitude of code involved with many command and control projects precludes using that technique for the entire project. There are efforts to isolate critical functions or "security kernels" (Hoffman, 1977, p. 142) to help to reduce the evaluation effort. But again, once the software is determined to be correct, it must be controlled to prevent modification after certification.

4. Operation Security

The origin of operation security developed out of lessons learned in Vietnam. Although traditional security measures were employed, the enemy was still able to determine operation times and objectives (JCS Pub 1, 1982, p. I-2). Analysis found that many unclassified indicators were revealing the times and objectives as clearly as if there were a compromise of classified information. Operation security therefore deals with unclassified actions

that reveal operational information. These include such items as the sudden recall of men from leave, the stockpiling in logistics channels of an unusual quantity of supplies or unusual supplies, the arranging of tugs and pilots to escort ships within harbors, or even submitting change of address forms. All of these can reveal a change from normal operations. The JCS define two terms important to the discussion of operation security. They are the definition of operation security itself and a definition of operation security indicators.

> OPERATION SECURITY - The protection of military operations and activities resulting from the identification and subsequent elimination or control of indicators susceptible to hostile exploitation. Also called OPSEC. (JCS Pub 1, 1979, p. 247)

> OPERATION SECURITY INDICATORS - Actions or information normally considered unclassified, or things not normally assigned a classification which provide an adversary a tip-off that an operation or other activity will occur, and bits and pieces needed in preparing appreciations [assumptions, estimates, and facts about an opponent's intentions and capabilities] prior to and during operations or other activities, or about the classified characteristics and capabilities of systems or procedures, doctrine, tactics and techniques. (JCS Pub 1, 1979, p. 247)

JCS Pub 18, expands on these definitions. It states that the key objective of OPSEC is to ensure mission effectiveness (JCS Pub 18, 1982, p. II-3). It also states that the planning for secrecy extends beyond the simple exposure of raw information to an adversary, but must also

involve assumptions and estimates made by an adversary through monitoring friendly habits of operation (JCS Pub 18, p. II-3). OPSEC also applies when activities cannot be concealed. In order to then maintain operation security, military deception will be required to maintain the secrecy of the mission.

Appendix D of JCS Pub 18 provides a listing of many "indicators" that OPSEC seeks to eliminate or mask. A sampling of these indicators is provided below:

1. Using homemade codes.
2. Requiring that routine reports be submitted at fixed times.
3. "Talking around" a classified subject.
4. Discussing logistic support needed, personnel reporting, personnel arrival dates, dates, times, plans, on non-secure radio or telephone.
5. Arranging the itinerary of senior officials to attend classified conferences over non-secure radio or telephone.
6. Using static call signs for particular units or functions, and unchanging or infrequently changed radio frequencies.
7. Open-source data showing spare parts availability for systems.
8. Budgets
9. Tests and exercise schedules.
10. Notices to mariners and airmen.
11. Special planning conferences.
12. Unusual actions with no apparent communications having directed the actions.

13. Having intensive maintenance and repair activity or unusual volumes of requisitions to be filled by a particular date.

14. Procuring of maps and charts.

15. Providing tailored training of personnel

16. Making personal arrangements with families.

17. Trash and garbage dumped by units or from ships at sea.

18. Discussion of repair and maintenance requirements in unsecured areas.

(JCS Pub 18, 1982, Appendix D).

VI. INTRODUCTION TO CRYPTOGRAPHY

A. CODES AND CIPHERS

Because cryptography is so important to command and control in protecting sensitive and classified information, the following section introduces basic cryptographic principles and techniques. It is intended to provide insights into how cryptographic systems operate and the various factors involved in their development and use.

Cryptography is a process by which an original message (plaintext) is transformed into another form that cannot be understood or changed by unauthorized individuals. It is also one of the most sensitive and relied upon security measures used to protect transmitted and stored command and control information. The word cryptography is Greek for "hidden writing" (Hoffman, 1977, p. 42). Codes are one form of transformation that are often used. For example, ASCII (American Standard Code for Information Interchange) is a binary code for representing standard typewriter symbols such as letter, numbers, and punctuation marks. For each typewriter symbol there is a corresponding seven bit ASCII binary code that represents that symbol. A matrix can be constructed that relates each symbol to its binary code. If the simple phrase "How are you?" were the original message

or plaintext that was to be encoded, the previously constructed table of relationships could be used to "transform" the plaintext into the ASCII or ciphertext of the message. The message would appear as follows:

Plaintext: How are you?

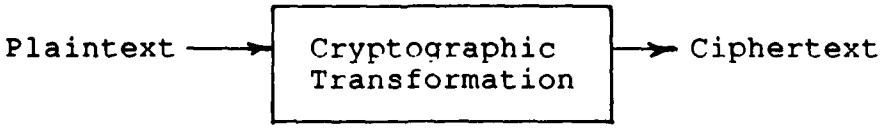
Transformation:

H = 0001001
o = 1111011
w = 1110111
  = 0000010
a = 1000011
r = 0100111
e = 1010011
  = 0000010
y = 1001111
o = 1111011
u = 1010111
? = 1111110

Ciphertext:

000100111110111110111000001010000110100111101001100000101001111101110111000001010000111010011110100110000010100111111110111010111111111110

In essence, the original message was the input to a transformation process (ie., the set of instructions describing how to change the plaintext into ciphertext). The output is the ciphertext. The cryptographic process can be represented by the process diagram below:



As long as the transformation is known, the message can be easily converted from plaintext to ciphertext and back

again. The transformation from plaintext to ciphertext is often called encryption or encoding. The reverse process recovering the plaintext from the ciphertext is called decryption or decoding.

Although the words codes and cipher are often used synonymously, there are actually subtle technical differences between the two. Ciphers usually operate on plaintext units of fixed length such as single letters, or fixed length groups of numbers (Hoffman, 1977, p.42). Technically speaking, the ASCII "code" would be considered a cipher since it always operates on a single letter or symbol at a time. Codes on the other hand can operate on variable length linguistic entities, such as words or phrases (Hoffman, 1977, p. 42). Instead of using a letter for letter substitution in the plaintext, a single code word could be substituted for the entire phrase. If "How are you" is represented by the code word "HARVEST", the name "Mr. Brown" is represented by "WHEAT" and "Mrs. Brown" is represented by "CORN", then the following encoded messages could be written:

Plaintext: How are you Mr. Brown Ciphertext: HARVEST WHEAT
Plaintext: How are you Mrs. Brown Ciphertext: HARVEST CORN

The JCS define codes and ciphers as follows:

> CIPHER - Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text of regular length, usually single letters, or in which units of plaintext are rearranged, or both, in accordance with certain predetermined rules. (JCS Pub 1, 1979, p. 64).

> CODE -
>
> 1. Any system of communications in which arbitrary groups of symbols represent units of plaintext of varying length. Codes may be used for brevity or for security.
>
> 2. A cryptosystem in which the cryptographic equivalents (usually called "code groups") typically consisting of letters or digits (or both) in otherwise meaningless combinations are substituted for plaintext elements which are primarily words, phrases, or sentences. (JCS Pub 1, 1979, p.69)

In the case of the ASCII system, the cipher is used to translate from a typewriter character set to a binary character set in order to facilitate the use of computers. Sometimes codes are used to shorten messages. Most often, both codes or ciphers are used to provide security for transmitted messages. When that is the case, not only does knowledge of the transformation process need to be restricted to authorized senders and intended receivers of messages, but careful attention must be paid to the rules of the transformation to assure that the process cannot be derived from the ciphertext.

B. SECURITY CHARACTERISTICS OF CIPHERTEXT

As was briefly described in Chapter V, cryptosecurity is the utilization of cryptography to provide security to transmitted and stored messages or data. The three desired characteristics of the ciphertext resulting from the secure cryptographic process are:

1. Non-disclosure - Only the intended recipient of the message can decrypt and understand the contents of the message.
2. Integrity - The message that is received is the same message that was sent.
3. Authenticity - The message could only have been sent by an authorized source.

While not all cryptographic systems provide all three characteristics, they all provide at least one. It depends on the specific requirements of the application, which characteristics should be incorporated. The implementation of each charateristic has its own financial and operational costs. To achieve non-disclosure, all users of the system must have the same cryptographic key installed and a means for distributing and protecting those keys. Message integrity may require the transmission of longer messages than the original in order to obtain error detection. While each of these characteristics is desirable, they each have their own costs to the user. Their implementation costs must be weighed against the benefits they provide.

C. GENERAL CIPHER SYSTEMS

The following discussion on cipher systems will deal with five general classes of ciphers: simple substitution ciphers, polyalphabetic substitution ciphers, infinite key word ciphers, modern cipher systems, and public key cryptography. This does not imply that these are the only systems that are available, or even that they represent the most important systems. The selection was made simply to provide a basic understanding of the general mechanics of cryptographic systems and to demonstrate the evolutionary nature of cryptography. The public key cryptography is included to show how cryptographic systems can be based on different principles.

1. Simple Substitution Ciphers

Simple substitution ciphers can be thought of as taking each letter of the original plaintext message, and substituting another letter or symbol to represent that letter. The ASCII cipher discussed earlier is one example of this type of system. Each potential letter or symbol of the plaintext is replaced by one and only one unique grouping of seven ones and zeros. An easier example to visualize would be the use of two alphabets (including a blank) - one in normal alphabetical order and the other scrambled. By knowing the relationship between the plaintext alphabet and the substitution alphabet, messages

can be easily encrypted and decrypted. Without that knowledge, the ciphertext appears on the surface to be nonsense. For example, take the following plaintext/substitution alphabet relationship to translate the message "HOW ARE YOU MRS BROWN":

Plaintext alphabet:
b A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Substitution alphabet:
K E C Q H b P S N Z W A G R U J L Y V B M F X T O I D

Plaintext:
HOW ARE YOU MRS BROWN

Ciphertext:
NJTKEV KIJFKRVBKCVJTU

In order for this system to be secure, the transformation process (the relationship between the two alphabets) must be kept secret or anyone could easily read messages, change messages, or construct false messages. In this case, recovery from a compromise would simply involve developing a new substitution alphabet. But this also requires a means for distributing the new cipher system to authorized users and a means for protecting the new transformation. Not all transformations are as easily changed. An important principle in cryptography is that the security of a system should not depend on the secrecy of something which cannot be changed if it is compromised (Diffie, 1979, p. 218).

Unfortunately, simply protecting the transformation method is not enough to assure the security of this system.

According to the prominent U.S. cryptologist William F. Friedman, almost any simple substitution cryptogram of 25 characters or more can be broken by a skilled cryptanalyst (Diffie, 1979, p. 220). In other words, the transformation process is not strong enough to prevent an adversary from "breaking" the system even without a compromise of the alphabet. Knowledge of the frequency with which letters appear in general usage and performing a frequency analysis of the ciphertext can reveal which substitution letter corresponds with which plaintext letter (Hoffman, 1977, p. 49). The longer the length of the message the better the statistics for frequency analysis.

2. Polyalphabetic Substitution Ciphers

One method used to overcome the problems of the simple substitution cipher is a polyalphabetic cipher. In this method, rather than having one letter always represent another letter, each ciphertext letter could actually represent any or all plaintext letters at some point in the message. This method requires not only a transformation process, but also a key. Consider the example in Figure 19.

This example points out several concepts of modern cryptography. This first point is that cryptography is, in essence, a mathematical process. By assigning each letter in the alphabet a numerical value, the transformation process can use arithmetic or algebra to determine the

Plaintext:
HOW ARE YOU MRS BROWN

Key:
BISON

Transformation:
Modulo arithmetic

Ciphertext:

H + B =	8 + 2	MOD 27	= 10	= J
O + I =	15 + 9	MOD 27	= 24	= X
W + S =	23 + 19	MOD 27	= 15	= O
b + O =	0 + 15	MOD 27	= 15	= O
A + N =	1 + 14	MOD 27	= 15	= O
R + B =	18 + 2	MOD 27	= 17	= Q
E + I =	5 + 9	MOD 27	= 14	= N
b + S =	0 + 19	MOD 27	= 19	= S
Y + O =	25 + 15	MOD 27	= 13	= M
O + N =	15 + 14	MOD 27	= 2	= B
U + B =	21 + 2	MOD 27	= 23	= W
b + I =	0 + 9	MOD 27	= 9	= I
M + S =	13 + 19	MOD 27	= 5	= E
R + O =	18 + 15	MOD 27	= 6	= F
S + N =	19 + 14	MOD 27	= 6	= F
b + B =	0 + 2	MOD 27	= 2	= B
B + I =	2 + 9	MOD 27	= 11	= K
R + S =	18 + 19	MOD 27	= 10	= J
O + O =	15 + 15	MOD 27	= 3	= C
W + N =	23 + 14	MOD 27	= 10	= J
N + B =	14 + 2	MOD 27	= 16	= P

Plaintext: HOW ARE YOU MRS BROWN
Ciphertext: JXOOOQNSMBWIEFFBKJCJP

Figure 19. Polyalphabetic Substitution Cipher

ciphertext. In this case, a straight numerical ordering of the letters of the standard alphabet is used with a "blank" equal to 0, "A" equal to 1, and "Z" equal to 26.

The mathematical transformation was a simple modulo addition. Modulo addition can be thought of as "clock arithmetic". On the face of the normal clock are twelve characters. If the first number in an addition process is "2" and the second number is "4", then the modulo addition process would count four positions from "2" to arrive at "6" on the face of the clock (2 + 4 MOD 12 = 6). If instead the first number was "9" and the second number was "6", the same procedure would yield an answer of "3" on the face of the clock (9 + 6 MOD 12 = 3). Using military time, if an operation were to begin at 2100 (9:00pm) and take 6 hrs. for completion, the operation would conclude at 0300.

(2100 + 600) MOD 2400 = 2700 MOD 2400 = 2700 - 2400 = 0300.

The modulus military time works with is MOD 2400. The modulus of the original example was 27 (the length of the alphabet plus a blank).

Since computers perform many functions in modern electronic systems, often a convenient modulus to use in these binary operations is a modulus of 2. This corresponds to binary addition without a carry or, in electrical circuits, to an "exclusive OR" gate. The truth table for modulo two addition is shown below:

MODULO TWO ADDITION

0 + 0 = 0

0 + 1 = 1

1 + 0 = 1

1 + 1 = 0

An interesting property of modulo two addition is that if the same key that produced a ciphertext is modulo two added again to the ciphertext, the result will be the plaintext. This makes the decryption process exactly the same as the encryption process with the roles of ciphertext and plaintext reversed.

Another important point that the BISON key example on page 128 demonstrates is that using a polyalphabetic cipher, the same plaintext letter is not always represented by the same ciphertext letter, and the same ciphertext letter can represent many plaintext letters. In this short message, the plaintext letter "O" is represented respectively by the ciphertext letters "X", "B", and "C". Similarly, the ciphertext letter "O" represents the plaintext "W","b", and "A". While this is an improvement over the simple substitution system, it also requires more effort to encrypt and to decrypt the message.

This polyalphabetic transformation consists of three important elements; the transformation algorithm (MOD 27 addition); the key (BISON); and the alignment or "synchronization" of the plaintext to the key. In this

case, the transformation algorithm is a simple process. But even if an adversary knew that the algorithm was MOD 27 addition, he should not be able to determine the plaintext from the ciphertext unless he could determine the cryptographic key. If the key were securely protected from compromise, then, theoretically communications would be secure provided the ciphertext does not reveal information about the underlying key. This requires a key management system in order to distribute and protect the proper key.

In regards to synchronization, if the key were shifted by one letter of the plaintext, then an entirely different ciphertext would be produced. If an intended recipient did not know where to begin the key, it would be difficult, if not impossible to decrypt the message.

One last point to notice in this example of polyalphabetic substitution is that a major portion of the key was actually transmitted. Because a blank was assigned the value of zero, and because the blank appeared four times in this short message, the key was therefore added to the blank's zero value four times, resulting in transmission of a portion of the key. The irregular spacing of the blanks throughout the message allowed a different key letter to be transmitted in place of each blank so that four out of the five key letters were transmitted: "O", "S", "I", "B". If the message were even longer, the entire key may have been

transmitted. This begins to show how difficult it is to design secure transformations.

3. Infinite Key Word Ciphers

Conceptually, as the key of polyalphabetic substitution ciphers becomes longer and longer, and approaches a random nature, the cryptographic system should become more and more secure (Hoffman, 1977, p.59). If this concept is taken to its extreme limit, then a key, infinitely long and completely random, should be completely secure. In fact many one time systems can be mathematically proved to be "unconditionally secure" from cryptanalysis (Diffie, 1979, p.219). One time tapes and many codebooks represent this type of system. Although this type of system appears to be ideal, it requires that a new key be used for each message (one time use), and everyone receiving the message must know what key is being used for which message and where to start the synchronization. The problem then becomes a key development, distribution, storage, security, destruction, and accounting nightmare, especially when the volume of transmitted traffic is high. Despite these logistics problems, one time tapes and codebooks are still used.

4. Modern Cipher Systems

In order to decrease the burden of storing an infinite amount of cryptographic key, many modern cryptographic systems have modified their cryptographic processes and adapted them to modern digital electronics. Instead of using an infinite key, many modern systems use a finite key and a complex mathematical transformation (algorithm) to generate a pseudo-random number called a keystream. This keystream is often a binary stream of ones and zeros that are then modulo 2 added to a digital representation of the plaintext message. The result of this modulo two addition is the ciphertext. If the same keystream can be generated at a receiving site, and can be properly aligned or synchronized with the plaintext, then a simple modulo 2 addition of the ciphertext and the keystream will again reveal the digital plaintext. This process is shown in Figure 20.

If the transformation process is designed properly and the key has not been compromised, the next pseudo-random number in the keystream cannot be predicted. In actuality the pseudo-random process will eventually cycle back to its beginning and repeat itself. The key must be changed prior to the beginning of a new cycle in order to preserve security. The security of this process is highly dependent on protection of the key and a secure key management system.

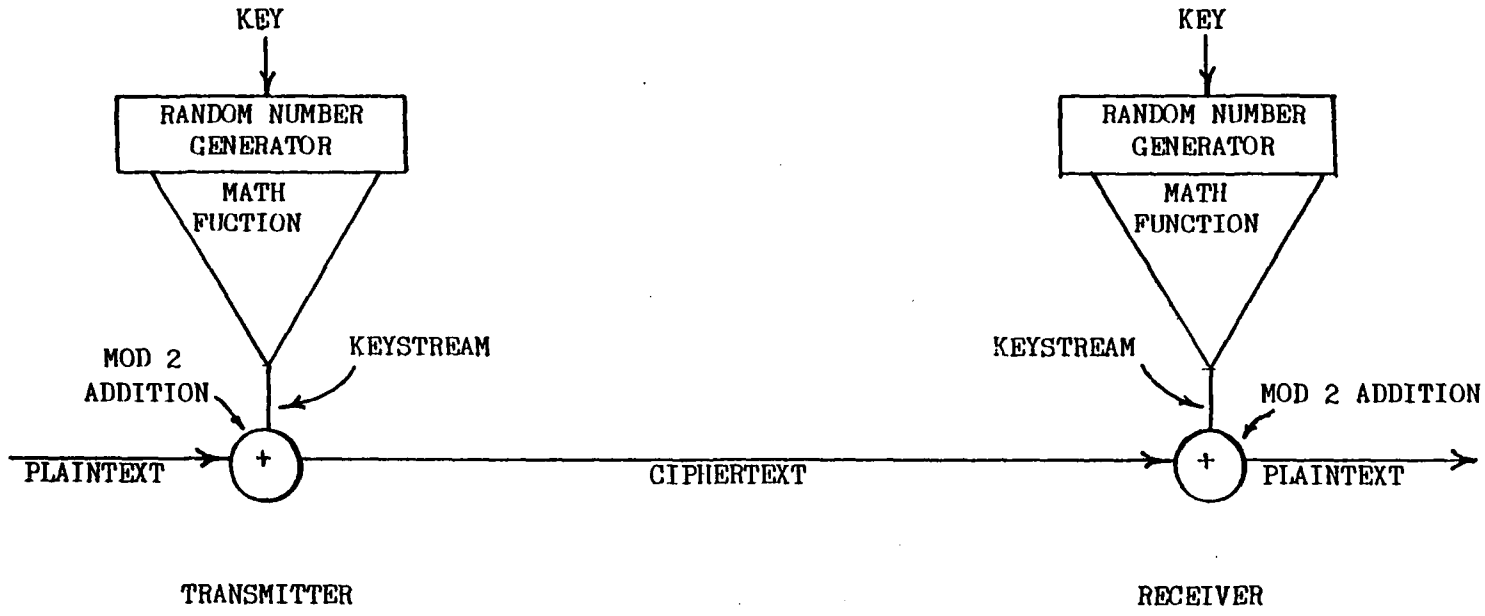


Figure 20. Modern Cipher System

With this type of system, both the sender and the recipient must be able to generate the same keystream and therefore must possess the same key. A compromise at either site will result in an insecure system and the key must be securely changed.

5. Public Key Cryptography

Public key cryptography (PKC) is a relatively recent development (Bamford, 1982, p.350). Rather than basing its security on a securely generated keystream, the security is based on the difficulty (computational infeasibility) of solving certain mathematical relationships. One of the beneficial aspects of a PKC system is that both the sender and the receiver can have different keys, thereby reducing the possibility of compromise. One key is held secret and the other can be made public, hence the name "public key cryptography". The following discussion will describe how a sender can use a publicly published key to encrypt a message that can be read only by the intended recipient. The example will use a publicly available algorithm developed by the mathematicians Rivest, Shamir, and Adleman (RSA) as described in Whitfield Diffie and Martin Hellman's paper, "Privacy and Authentication: An Introduction to Cryptography" (Diffie, 1979, pp. 233-234). While there are other usages of public key systems, and other approaches to

public key cryptography, the RSA algorithm will provide a good understanding of how public key systems operate.

The RSA algorithm operates on a fixed block of a plaintext digital message (roughly 700 bits) at a time. The message will correspond to a number "M". RSA uses the mathematical property that a number (M), successively raised to two different numbers (E and D), is the same as raising the original number to the product of the later two. This can be mathematically shown as follows:

$$(M^E)^D = M^{E*D}$$

Also, if the product of E and D is equal to one, then $(M^E)^D$ is equal to M.

$$(M^E)^D = M^{E*D} = M^1 = M \quad (\text{If } E * D = 1)$$

Another mathematical property that the RSA algorithm uses is the fact that finding the prime factors of the product of two large (over 100 digits) prime numbers is computationally infeasible (Diffie, 1979, p.233). In other words, given only a very large number that is the product of two prime numbers, it is extremely difficult to find the original pair of prime numbers. For example, given only the number 146,550,809, it is computationally infeasible to factor that number into its two prime components 9533 and 15,373. It is easy to find two primes and multiply them together. It is not easy to find the two primes given only the product.

The last mathematical concept that is used is a property discovered by the mathematician Leonhard Euler (1707 - 1783). Beginning with a number (N) which is the product of two prime numbers (P and Q), he proved that the number of integers less than N, that are relatively prime to N, is equal to (P-1) * (Q-1). This property is known as the "Euler totient function", PHI(N). Relatively prime numbers are numbers that have only one as a common prime factor. An example of PHI(N) follows. Given the two prime numbers 3 and 7, their product would be 21. Factoring all the numbers between 2 and 21, and eliminating those with common prime factors, there are only 12 numbers (1,2,4,5,8,10,11,13,16,17,19, and 20) that do not have 3 or 7 as one or more of their prime factors. The Euler totient function would predict that there would be:

$$PHI(21) = (3 - 1) * (7 - 1) = 2 * 6 = 12$$

This process becomes even more difficult and lengthy as the numbers become larger.

The RSA system begins with the following variables:

M = The numerical representation of the message.

P = First selected large prime number.

Q = Second selected large prime number.

N = Computed product of P * Q

E = An arbitrary number (to be published)

D = A computed number such that E * D = 1 MOD (PHI(N))
(D is kept secret)

The first step in establishing the RSA system so that anyone can encrypt a message but only the intended recipient can decrypt the message, is to compute the number N.

$$N = P * Q$$

N is made public but its factors P and Q are kept secret by the intended recipient. Next, the intended recipient computes PHI (N).

$$PHI(N) = (P-1) * (Q-1)$$

Since only the recipient has P and Q, only he can compute PHI(N) since it requires knowledge of P and Q. It is the difficulty of factoring N that protects P and Q.

The recipient then arbitrarily selects a number E that is greater than 2 and less than PHI(N). He then computes the number D so that E * D = 1 in the modulus PHI(N). D is kept secret by the recipient, but both E and N can be published in a telephone book type listing of public keys. The system is now established.

If someone wants to encrypt a message so that only a specific person could read it, they look up in a book the public E and N listed for the intended recipient and perform an exponentiation of the message.

$$M^E \text{ MOD } N = C = \text{Ciphertext}$$

Nothing in the public information would allow for the recovery of the original message. That would require being able to determine D. Since D requires the knowledge of PHI(N) and PHI(N) requires knowledge of P and Q, D cannot be determined unless P and Q are known. Since P and Q are held only by the recipient, only he can decrypt the message.

To decrypt the message, the indented recipient simply raises the ciphertext to the D power in MOD N to recover the plaintext.

$$C^D \text{ MOD } N = (M^E)^D \text{ MOD } N = M^{E*D} \text{ MOD } N = M^1 \text{ MOD } N = M$$

Although the process is based on sophisticated mathematics, its implementation can easily be adapted to the computer.

VII. CONCLUSIONS

A. THE BALANCE OF SECURITY AND OPERATIONAL EFFECTIVENESS

The previous chapters have highlighted the importance of security to command and control. Since command and control is the decision making and coordination process of an organization and a military force, it is crucial that the elements of command and control be preserved. Collecting and processing of information, developing of decision alternatives, making the decisions themselves, and disseminating those decisions to those tasked with various actions, are all crucial to the effective and efficient accomplishment of the organization's goals and objectives. They not only must be preserved from destruction or disruption, but they also must protect the confidentiality of the organization's plans and methods.

Security is required to preserve the command and control process in a hostile environment. Once security is recognized as a indispensable element of command and control, the required level of security must next be determined. The actual achieved security is dependent on both the threat and the costs of the security measures. It is also a balance between security needs and operational objectives.

A threat is uncertain in nature. An estimate of the threat must be established and security measures designed to oppose or repel that design baseline threat level. This can be the maximum or "potential" threat; it can be a probable threat; or it can be a likely scenario threat. Whatever the designed level of security, there is always the possibility or probability that the actual hostile action will exceed the security level. This is especially true over time. Static security measures may deteriorate over time or fail to meet an evolving threat. Security is highly dependent on the threat.

Ideally, all systems would be designed to repel the maximum potential threat. Unfortunately this is often impossible both financially and operationally. The price of all the security measures, their operation, and maintenance can be exceedingly high. The restrictions and constraints they impose upon operations, may be overly restrictive. Security must be viewed as one of a combination of elements needed to accomplish the commander's mission. It is not the objective in and of itself. JCS Pub 18 identifies seven factors that should be weighed when balancing security with operational effectiveness:

1. Adversaries must have some knowledge of friendly capabilities and intentions so they will perceive threats.

2. The public must know something about military capabilities to foster recruitment of friendly

personnel and gain internal political support and support for alliances.

3. The Military Departments/Services must test rigorously and in realistic environments, systems, procedures, doctrine, and tactics.

4. The Armed Forces must broadly understand capabilities, conduct extensive and thorough training, and execute realistic, demanding exercises to develop personnel skills, determination, unity, morale, and readiness.

5. Allies must share information and exercise together to develop competence and mutual trust.

6. Planners and those preparing to execute actions must thoroughly understand plans to realize optimal coordination and effectiveness of undertakings.

7. Commanders must test and exercise command procedures, organizations, communications, staffs, and operational concepts to ensure readiness.

(JCS Pub 18, 1982, pp. II-4 - II-5)

In addition to the operational factors that must be balanced against the need for security are the underlying motivations for the mission. The purpose of national defense for a country is the safety and security of its citizens, its territory, and the preservation of its national principles and character. Providing "for the common defense" is clearly established in the preamble to the Constitution of the United States as one of the primary objectives of the United States Government. But that is not its only objective. Within the same sentence, the Constitution also establishes securing "the blessings of liberty to ourselves and our posterity" as an equal

objective and further enumerates the individual's rights of liberty within the Bill of Rights. There must be a balance between the need for security and the preservation of individual rights. The balance is not always easily established. Still, that balance must be sought. Without a balance, national security may be preserved, but at the cost of liberty; or liberty may be lost for the lack of security. In both cases, the principles to be protected have been lost. Security must not destroy what it is supposed to protect. Placed in its proper perspective, security must always be viewed as the means to preserve what is important.

B. RECOMMENDED FUTURE STUDIES

This thesis has attempted to provide a conceptual foundation for the further study of command and control security. Because the thesis covered a wide range of topics, its depth in any one area was limited. The following is a list of possible future topics that deserve further development:

1. Studies to prove or disprove the hypotheses stated in this thesis.
2. Studies to expand the knowledge base of specific security measures or threats.
3. Studies to determine effective measures of threat levels and security levels.
4. Studies on how to develop the probability distributions of various threats.

5. Studies on how to determine the most appropriate level of threat to design for.

6. Studies on the economics of security.

7. Studies and analyses of historical C^2 security failures or successes and their implications for C^2 security designs.

8. Studies on the effectiveness of specific security measures.

9. Studies on how to effectively design security measures and systems.

APPENDIX A - FORMAL DEFINITIONS

Definition 1: Security - is a condition, level, state of nature, or feeling of being safe which results from the establishment and maintenance of security measures.

Definition 2: Security measures - are those procedures or technologies taken by an individual or group to protect against actions that threaten, impair, or destroy its survival or effectiveness.

Definition 3: Security elements - are groupings of security measures that protect against a common threat or act in a similar manner. Examples of security elements are physical security, communication security, computer security, and emission security.

Definition 4: Protected Item - is the object, system, idea, information, or characteristic that requires security.

Definition 5: Value - is the remaining importance or effectiveness of the protected item measured in a percentage of its full importance or effectiveness.

Definition 6: Security Level - is the percentage of the potential threat that the security system can resist.

Definition 7: Vulnerability Level - is the percentage of the potential threat that the security system cannot resist. The vulnerability level is equal to the difference between the threat level and the security level.

Definition 8: Threat - is the potential force an adversary can exert to decrease the value of the protected item.

Definition 9: Threat Level - is the measure of the potential force an adversary can exert measured in a percentage of the maximum force level.

Definition 10: Hostile Action - is the actual execution of a threat.

Definition 11: A system is a set of elements united as a whole for achieving a goal.

APPENDIX B - HYPOTHESES

Hypothesis 1: Security can be considered a spectrum of states of nature ranging from imminent danger (no security) to pure safety (full security).

Hypothesis 2: Security is a function of the detection, response, and penalty mechanisms (security measures) applied to the environment.

Hypothesis 3: The greater the probability of detection, the greater the security.

Hypothesis 4: The greater the reliability of response, the greater the security.

Hypothesis 5: The greater the magnitude of the penalty, the greater the security.

Hypothesis 6: Detection, response, and penalty security measures cannot exist independent of each other.

Hypothesis 7: Security is a function of how the threat changes in time relative to security measures employed.

Corollary 7.1: Security is a function of time.

Corollary 7.2: Threat is a function of time.

Corollary 7.3: Security measures are a function of time.

Corollary 7.4: Security is a function of the threat.

Corollary 7.5: Security measures must be maintained relative to the threat or their effectiveness deteriorates over time.

Corollary 7.6: Security measures and the threat are in a constant, cyclical, action/response, and evolutionary relationship.

Hypothesis 8: The relationship between a threat, security measures, and the value of a protected item is a process with threat as the input, the security measures as the transformation, and the remaining value as the output of the process.

Hypothesis 9: The threat and security measure can be composed of several different individual elements.

Hypothesis 10: For each security measure, there is an associated theoretical probability of successfully stopping a particular threat, ultimately affecting the value of the protected item.

Hypothesis 11: The combination of all security processes is a system (security system).

Hypothesis 12: There are costs associated with employing security measures.

Hypothesis 13: Command and Control is a function performed by the commander.

Hypothesis 14: The commander operates within a larger organization.

Hypothesis 15: The commander is specifically assigned to his position by the organization.

Hypothesis 16: The commander is assigned a specific mission to accomplish.

Hypothesis 17: The commander is assigned authority over specific forces.

Hypothesis 18: The commander accomplishes his mission through his assigned forces.

Hypothesis 19: Command and control is the process by which a commander exercises his authority.

Hypothesis 20: Command and control is a decision making and force directing process.

Hypothesis 21: Command and control incorporates the functions of planning, directing, coordinating, and controlling of forces and operations to accomplish its decision making and force directing process.

Hypothesis 22: Essential elements of command and control are the commander, the mission, the assigned forces, the organization, and the means to decide and direct.

Hypothesis 23: The command and control system is the means by which a commander directs his forces to accomplish a mission.

Hypothesis 24: The command and control system consists of personnel, equipment, communications, facilities, and procedures.

Hypothesis 25: The primary characteristics of a command and control system are connectivity, accuracy, timeliness, authenticity, secrecy, covertness, availability, and affordability.

Hypothesis 26: The commander is shown a filtered representation of the current situation through his command and control system, not the actual situation.

Hypothesis 27: Errors and biases can be introduced by the command and control system.

Hypothesis 28: The commander is totally reliant on his command and control system to provide accurate information and to accurately disseminate his decisions.

Hypothesis 29: A threat is a possible, future hostile or injurious action.

Hypothesis 30: There is a probability of occurrence associated with each threat.

Hypothesis 31: A hostile act is the realization of a threat. It is a threat that is being executed.

Hypothesis 32: The potential threat is the maximum force or effort an adversary can expend if all of his resources were applied to this single effort to breach security measures.

Hypothesis 33: The probable threat is an estimate of the most likely levels of force an adversary will expend in his efforts to breach the security measures.

Hypothesis 34: A vulnerability is the lack of adequate security measures to protect against potential threats.

Hypothesis 35: Vulnerabilities are inherent characteristics of a design.

Hypothesis 36: A system designer does not have control over the threat.

Hypothesis 37: A system designer does have control over the design vulnerabilities through the design security level.

LIST OF REFERENCES

Armed Forces Staff College, National Defense University, Joint Staff Officer's Guide 1986 - AFSC Pub 1, Government Printing Office, Washington, DC, 1986.

Bamford, James, The Puzzle Palace - A Report on NSA, America's Most Secret Agency, Houghton Mifflin Co., Boston, MA, 1982.

Barron, John, Breaking the Ring - The Bizarre Case of the Walker Family Spy Ring, Houghton Mifflin Co., Boston, MA, 1987.

Blair, Bruce G., Strategic Command and Control - Redefining the Nuclear Threat, The Brookings Institution, Washington, DC, 1985.

Boorman, Scott A., Levitt, Paul R., "Software Warfare and Algorithm Sabotage," Signal, Vol. 42, No. 9, p. 75-78, May 1988.

Buzzard, Greg, "Avoiding Worms and Viruses in a Networked Environment", briefing presented at the Naval Postgraduate School, Monterey, CA, January 1989.

Carter, Ashton B., Steinbruner, John D., Zraket, Charles A., Managing Nuclear Operations, Brookings Institution, Washington, DC, 1987.

Commission to Review DOD Security Policies and Practices, Keeping the Nation's Secrets, Department of Defense, 19 November 1985.

Department of Defense, Soviet Military Power - An Assessment of the Threat 1988, Government Printing Office, Washington, DC, 1988.

Diffie, W., Hellman, M.E., "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, Vol. 67, No. 3, pp. 397-427, March 1979.

Hsiao, David K., Kerr, Douglas S., Madnick, Stuart E., Computer Security, Academic Press, New York, NY, 1979.

Hoffman, Lance J., Modern Methods for Computer Security, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977.

Ivanov, D.A., Savel'yev, V.P, Shemanskiy, P.V., Fundamentals of Tacical Command and Control - A Soviet View, Government Printing Office, Washington, DC, 1977

Joint Chiefs of Staff, JCS PUB 1 - Department of Defense Dictionary of Military and Associated Terms, Joint Chiefs of Staff, Washington, DC, 1979.

Joint Chiefs of Staff, JCS PUB 18 - Operations Security, Joint Chiefs of Staff, Washington, DC, 1982.

Kozacuk, Wladyslaw, Enigma: How the German Machine Cipher was Broken and How it was Read by the Allies in World War Two, University Publications of America, Inc., 1984.

Littlebury, F.E., Praeger, D.K., Invisible Combat: C^3CM - A Guide for the Tactical Commander, AFCEA International Press, Washington, DC, 1986.

Martin, James, Telecommunications and the Computer, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1976.

Martin, Laurence, The Changing Face of Nuclear War, Harper & Row Publishers Inc., New York, NY, 1987.

Orr, George E, Maj. USAF, Research Report No. AU-ARI-82-5, Combat Operations C^3I: Fundamentals and Interactions, Air University Press, Maxwell AFB, AL, 1983.

Ricci, Fred J., Schutzer, Daniel, U.S. Military Communications - A C^3I Force Multiplier, Computer Science Press, Inc., Rockville, MD, 1986.

Richelson, Jeffery T., Sword and Shield - Soviet Intelligence and Security Apparatus, Ballinger Publishing Co., Cambridge, MA, 1986.

Richelson, Jeffery T., The U.S. Intelligence Community, Ballinger Publishing Co., Cambridge, MA, 1985.

Sun Tzu, The Art of War: The Oldest Military Treatise in the World, Luzac and Co., London, 1910.

Taylor, James G., "Class Notes to OS-3636", Naval Postgraduate School, Monterey, CA, September 1988.

TIME, "Invasion of the Data Snatchers," TIME, Vol. 132, No. 13, p. 62-67, 26 September 1988.

Webster's New World Dictionary of American Language - Concise Edition, The World Pub. Co., Cleveland, OH, 1969.

BIBILOGRAPHY

Ackerman, Robert K., "Soviet Military Advances," Signal, Vol. 42, No. 3, pp. 53-61, November 1987.

Ackerman, Robert K., "The Art of Deception", Signal, Vol. 43, No. 1, pp. 47-51, September 1988.

Ang, Alfredo H-S., Tang, Wilson H., Probability Concepts in Engineering Planning and Design, Vol I: Basic Principles, John Wiley & Sons, Inc., New York, NY, 1975.

Armed Forces Staff College, National Defense University, Joint Staff Officer's Guide 1986 - AFSC Pub 1, Government Printing Office, Washington, DC, 1986.

Bamford, James, The Puzzle Palace - A Report on NSA, America's Most Secret Agency, Houghton Mifflin Co., Boston, MA, 1982.

Barron, John, Breaking the Ring - The Bizarre Case of the Walker Family Spy Ring, Houghton Mifflin Co., Boston, MA, 1987.

Berkey, Dennis D., Calculus, Saunders College Publishing, Philadelphia, PA, 1983.

Blanchard, Benjamin S., Fabrycky, Wolter J., Systems Engineering and Analysis, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1981.

Blair, Bruce G., Strategic Command and Control - Redefining the Nuclear Threat, The Brookings Institution, Washington, DC, 1985.

Blum, Howard, I Pledge Allegiance: The True Story of the Walkers - An American Spy Family, Simon & Schuster, Inc., New York, NY, 1987.

Boorman, Scott A., Levitt, Paul R., "Software Warfare and Algorithm Sabotage," Signal, Vol. 42, No. 9, p. 75-78, May 1988.

Boyes, Jon L., VAdm, USN, Andriole, Stephen J., Principles of Command and Control, AFCEA International Press, Washington, DC, 1987.

Buzzard, Greg, "Avoiding Worms and Viruses in a Networked Environment", briefing presented at the Naval Postgraduate School, Monterey, CA, January 1989.

Carter, Ashton B., Steinbruner, John D., Zraket, Charles A., Managing Nuclear Operations, Brookings Institution, Washington, DC, 1987.

Chemical Rubber Co., Standard Mathematical Tables, Chemical Rubber Co. Press, Cleveland, OH, 1976.

Cimbala, Stephen J., "C^2 and War Termination," Signal, Vol. 43., No. 4, pp. 73-78, December 1988.

Clausewitz, Karl Von, On War, Vol. III, Kegan Paul, Trench, Trubner & Co., Ltd., London, 1911.

Clausewitz, Karl Von, Collins, Edward M., Col., USAF, ed. War, Politics, and Power - Selections from On War, and I Believe and Profess, Henry Regnery Co., Chicago, IL, 1962.

Coats, Wendell J., Brig. Gen, USA, Armed Force as Power - The Theory of War Reconsidered, Exposition Press, New York, NY, 1966.

Commission to Review DOD Security Policies and Practices, Keeping the Nation's Secrets, Department of Defense, 19 November 1985.

Denning, Dorthy E.R., Cryptography and Data Security, Addison-Wesley Publishing Co., Reading, MA, 1982.

Department of Defense, Soviet Military Power - An Assessment of the Threat 1988, Government Printing Office, Washington, DC, 1988.

Diffie, W., Hellman, M.E., "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, Vol. 67, No. 3, pp. 397-427, March 1979.

Everett, Robert R., "Command, Control, and Communications", The Bridge - National Academy of Engineers, (Reprint).

Freedman, Lawrence, US Intelligence and the Soviet Strategic Threat, Westview Press, Boulder, CO, 1977.

Fritz, F., "Soviet C^2 Information Systems: Theories, Concepts, Evaluations," Signal, Vol. 43, No. 4, pp. 35-41, December 1988.

Halperin, Morton H., Hoffman, Daniel N., Top Secret: National Security and the Right to Know, New Republic Books, Washington, DC, 1977.

Hsiao, David K., Kerr, Douglas S., Madnick, Stuart E., Computer Security, Academic Press, New York, NY, 1979.

Hoffman, Lance J., Modern Methods for Computer Security, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977.

Ivanov, D.A., Savel'yev, V.P, Shemanskiy, P.V., Fundamentals of Tacical Command and Control - A Soviet View, Government Printing Office, Washington, DC, 1977

Joint Chiefs of Staff, JCS PUB 1 - Department of Defense Dictionary of Military and Associated Terms, Joint Chiefs of Staff, Washington, DC, 1979.

Joint Chiefs of Staff, JCS PUB 18 - Operations Security, Joint Chiefs of Staff, Washington, DC, 1982.

Kahn, David, Kahn on Codes - Secrets of the New Cryptography, Macmillian Publishing Co., New York, NY, 1983.

Kozacuk, Wladyslaw, Enigma: How the German Machine Cipher was Broken and How it was Read by the Allies in World War Two, University Publications of America, Inc., 1984.

Kranakis, Evangelos, Primality and Cryptography, John Wiley & Sons, New York, NY, 1986.

Krone, Robert M., Systems Analysis and Policy Sciences, John Wiley & Sons, New York, NY, 1980.

Lewis, Ronald, The American Magic: Codes Cipers and the Defeat of Japan, Farrar Straus Giroux, New York, NY, 1982.

Littlebury, F.E., Praeger, D.K., Invisible Combat: C^3CM - A Guide for the Tactical Commander, AFCEA International Press, Washington, DC, 1986.

Markland, Robert E., Sweigart, James R., Qunatitative Methods: Applications to Managerial Decision Making, John Wiley & Sons, New York, NY, 1987.

Martin, James, Telecommunications and the Computer, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1976.

Martin, Laurence, The Changing Face of Nuclear War, Harper & Row Publishers Inc., New York, NY, 1987.

Meyer, Paul L., Introductory Probability and Statistical Applications, Addison-Wesley Publishing Co. , Reading ,MA, 1970.

Morris, William T., "On the Art of Modeling," Management Science, Vol. 13, No. 12., August, 1967. (Reprint)

Orr, George E, Maj. USAF, Research Report No. AU-ARI-82-5,Combat Operations C^3I: Fundamentals and Interactions, Air University Press, Maxwell AFB, AL, 1983.

Ostrofsky, Benjamin, Design, Planning and Development Methodology, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977.

Paret, Peter, Makers of Modern Strategy - From Machiavelli to the Nuclear Age, Princeton University Press, Princeton, NJ, 1986.

Parrish, Thomas, The Ultra Americans: The U.S. Role in Breaking the Nazi Code, Stein Day, Inc., Briarcliff Mannor, NY, 1986.

Peterzell, Jay, "Spying and Sabotage by Computer", TIME, Vol. 133, No. 12, p. 25, 20 March 1989.

Pieruschka, Erich, Principles of Reliabiity, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977.

Ricci, Fred J., Schutzer, Daniel, U.S. Military Communications - A C^3I Force Multiplier, Computer Science Press, Inc., Rockville, MD, 1986.

Richelson, Jeffery T., Sword and Shield - Soviet Intelligence and Security Apparatus, Ballinger Publishing Co., Cambridge, MA, 1986.

Richelson, Jeffery T., The U.S. Intelligence Community, Ballinger Publishing Co., Cambridge, MA, 1985.

Sage, Andrew P., Methodology for Large-Scale Systems, McGraw-Hill Book Co., New York, NY, 1977.

Schoderbek, Peter P., Schoderbek, Charles G., Kefalas, Asterios G., Management Systems: Conceptual Considerations, Business Publications, Inc., Plano, TX, 1985.

Stanley, William D., Electronic Communication Systems, Reston Publishing Co., Reston, VA, 1982.

Sun Tzu, The Art of War: The Oldest Military Treatise in the World, Luzac and Co., London, 1910.

Taylor, James G., "Class Notes to OS-3636", Naval Postgraduate School, Monterey, CA, September 1988.

TIME, "Invasion of the Data Snatchers," TIME, Vol. 132, No. 13, pp. 62-67, 26 September 1988.

Unkenholz, Willard L., "A Conceptual Approach to Systems Security," paper for Naval Postgraduate School Course OS-3636, Naval Postgraduate School, Monterey, CA, 17 September 1988.

Webster's New World Dictionary of American Language - Concise Edition, The World Publishing Co., Cleveland, OH, 1969.

Westwood, James T., "Coming to Grips with Soviet Strategic Logic," Signal, Vol. 42, No. 3, pp. 111-113, November 1987.

Wickham, John A., Gen., USA (Ret.), "Protecting our Computers," Signal, Vol. 43, No. 5, pp. 17-19. January 1989.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Assistant Secretary of Defense (C^3I) Washington, DC 20301	1
4.	Director for Command, Control and Communications Systems Joint Staff/J6 Washington, DC 20318-6000	1
5.	Superintendent C^3 Academic Group, Code 74 Naval Postgraduate School Monterey, CA 93943-5000	1
6.	Director National Security Agency 9800 Savage Rd. Fort George G. Meade, MD 20755-6000 Attn: V6	1
7.	Director National Security Agency 9800 Savage Rd. Fort George G. Meade, MD 20755-6000 Attn: E122	1
8.	Director, C^2 Systems Division (OP-942) Washington, DC 20350	1
9.	Office of the Director, Center for Command and Control Communications System Bldg. A, Arlington Hall Station Arlington, VA 22212-5410	1
10.	Office Director of Information System for Command, Control, Communications and Computers, U.S. Army Attn: SAIS-PPP Washington, DC 20310-0107	1

11. Director, Defense Intelligence Agency 1
Washington, DC 20301
Attn: Mr. Tom Haug

12. Director, Command Control 1
Communications Division, USMC
Washington, DC 20380-0001

13. HQ/SCTT U.S. Air Force 1
Attn: Maj. Steve Lower
Washington, DC 20330-5000

14. Willard L. Unkenholz 1
15520 Plaid Dr.
Laurel, MD 20707

15. Superintendent 1
Capt. Milton H. Hoever, USN, Code 54Ho
Naval Postgraduate School
Monterey, CA 93943-5002

16. Superintendent 1
Dan Boger, Code 54Bo
Naval Postgraduate School
Monterey, CA 93943-5002