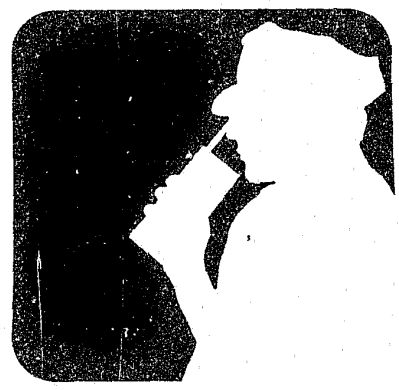
NBS Special
Publication
480-24

The Role of Behavioral Science in Physical Security.

Proceedings of the First Annual Symposium, April 29-30, 1976



Law Enforcement
Equipment
Technology

U.S. DEPARTMENT OF
COMMERCE
National Bureau of
Standards

ACKNOWLEDGMENTS

This report was prepared by the Law Enforcement Standards Laboratory of the National Bureau of Standards under the direction of Lawrence K. Eliason, Manager, Security Systems Program, and Jacob J. Diamond, Chief of LESL.

NBS Special Publication 480-24

The Role of Behavioral Science in Physical Security.

Proceedings of the First Annual Symposium, April 29-30, 1976

Edited by
Joel J. Kramer
Human Factors Section
Center for Consumer Product Technology
National Bureau of Standards
Washington, D.C. 20234

This work was sponsored by the Defense Nuclear Agency under:
Subtask Code P99QAX DE910
Work Unit 13

Sponsored by
Law Enforcement Standards Laboratory and
Human Factors Section
National Bureau of Standards and
The Intelligence and Security Directorate
Defense Nuclear Agency

Prepared for
Intelligence and Security Directorate
Defense Nuclear Agency
Washington, D.C. 20305

Issued November 1977

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, *Secretary*
Dr. Sidney Harman, *Under Secretary*
Jordan J. Baruch, *Assistant Secretary for Science and Technology*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

Libary of Congress Catalog Number: 77-600058
National Bureau of Standards
Special Publication 480-24
Nat. Bur. Stand. (U.S.), Spec. Publ. 480-24, 122 pages
CODEN:XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON:

For sale by the Superintendent of Documents,
U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. 13.10:480-24). Stock No. 003-003-01868-6. Price $3.00
(Add 25 percent additional for other than U.S. mailing).

FOREWORD

The Defense Nuclear Agency (DNA) is engaged in a continuing effort to enhance the security of nuclear weapons storage. In this effort, it is receiving technical support from the National Bureau of Standards' Law Enforcement Standards Laboratory (LESL), whose overall program involves the application of science and technology to the problems of crime prevention, law enforcement and criminal justice.

LESL is assisting DNA's physical security program with support in the behavioral science, the chemical science and the ballistic materials areas, among others.

Among the tasks being performed by LESL for DNA are the preparation and publication of several series of technical reports on the results of its researches. This document is one such report.

Technical comments and suggestions are invited from all interested parties. They may be addressed to the authors of the report or to the Law Enforcement Standards Laboratory, National Bureau of Standards, Washington, D.C. 20234.

Jacob J. Diamond
Chief, Law Enforcement Standards
Laboratory

PREFACE

These proceedings are the results of a symposium/workshop held on April 29-30, 1976, at the Defense Nuclear Agency (DNA). The purpose of the symposium/workshop was to begin defining the role of behavioral science in physical security systems and to share information and ideas among the participants and other interested parties.

The symposium was jointly sponsored by the Law Enforcement Standards Laboratory (LESL) and Human Factors Section of the National Bureau of Standards (NBS) and the Intelligence and Security Directorate of the Defense Nuclear Agency, attracting some 93 attendees from government and industry. Papers were presented in the areas of threat analysis, human reliability, and behavioral impact measurement methodology, with many of the papers followed by open discussion sessions.

The editor wishes to acknowledge the cooperation of the staff of the Defense Nuclear Agency. Special thanks go to Captain S. G. Galing, USN, Director, Personnel and Administration, Defense Nuclear Agency for a stirring welcoming address, and to the Program Committee consisting of Lawrence K. Eliason, Program Manager for Security Systems, LESL; Dr. Herbert B. Leedy, Department of the Army; Dr. John Nagay, Office of Naval Research; Dr. George H. Lawrence, National Academy of Sciences; and Dr. Thomas Shea, Nuclear Regulatory Commission.

Joel J. Kramer
Product Systems Analysis
Division
National Bureau of Standards

ABSTRACT

This document contains the proceedings of a 2-day Symposium/Workshop held in April 1976 on the application of behavioral science to the problems of physical security. The formal papers are divided into three topical sections: (1) Threat Analysis—Behavioral Factors and Consequences, (2) Human Reliability—Response Forces vs. Adversary, and (3) Methods of Measuring Behavioral Impact—Quantitative vs. Qualitative. Timely questions and challenges were explored in open discussion sessions following many of the presentations. The volume concludes with a brief summary of the panel-type workshop on the subject of threat analysis held on the second day.

Key words: Behavioral science; human factors; human reliability; perpetrator attributes; physical security; psychological deterrence; terrorism; threat analysis.

CONTENTS

ANALYZING THREATS FROM TERRORISM
A WORKING PAPER*

Eric D. Shaw, Leo Hazlewood, Richard E. Hayes, and Don R. Harris

CACI, Inc.–Federal, Arlington, VA 22209

INTRODUCTION

Within the last 10 years Western industrialized countries have become increasingly better acquainted with terrorism, a special form of political violence. By terrorism, we mean the selective application of violence to a limited target undertaken to influence the attitudes or behavior of a larger group. These acts are undertaken from an initial position of tactical and political weakness to wage a primarily psychological battle for support. While the strategy and tactics of terrorists may often seem bizarre and unconventional, they are appropriately suited for the position that the terrorist occupies in society.

This paper examines the patterns behind the seemingly random acts of violence performed by terrorists. The first part of the analysis presents some basic information on terrorist activity since 1945, particularly terrorist acts directed toward personnel or facilities of the Department of Defense. The second part of the paper reviews the changing character of terrorist operations and capabilities. A third section addresses the contributions of the behavioral and social sciences to meeting the challenge of terrorist violence. Finally, the paper concludes with some suggestions for organizational changes and an agenda for further research on terrorism.

TRENDS IN TERRORIST ACTIVITY SINCE WORLD WAR II

The use of dramatic acts of violence to achieve political ends (whether as an isolated act or as part of a campaign of actions) is hardly a new phenomenon. Terrorism has been used for many years by widely varying groups to achieve major policy reorientations, changes in incumbent leaders, or changes in the basic nature and character of the political system. What is new is the *scope of terrorist activities* and the *increasingly international occurrence* of these activities. This section presents some information on terrorist actions since 1945 from two perspectives. First, it presents materials on all publicly identified terrorist incidents from 1946-1973. Second, it considers some basic information on a set of incidents from 1946-1975 in which facilities and/or personnel of the Department of Defense were the target of attacks.

EXAMINING TERRORISM OVER TIME

Figure 1 plots the occurrence of terrorist activities identified from open sources for all countries since 1946. As the graph clearly shows, acts of terrorism are not new to the international system. What is new is the scale of occurrence since the late 1960's. With the exception of 1946-1948 (when the United Kingdom was the target of a widespread terrorist campaign in Israel), 1956 and 1964, far fewer than 50 terrorist incidents occurred annually until 1969. From 1969 onward, however, the number of terrorist incidents increased dramatically, and over 350 terrorist incidents were reported

*Sections of this paper contain information gathered in connection with U.S. Government Contract No. N0004-76-C-0454. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the U.S. Government.

in public sources for both 1970 and 1971. After a drop to under 200 incidents in 1972, more than 230 terrorist attacks were reported in 1973, the last year for which complete data have been collected.

As table 1 suggests, specific countries have often been the target of terrorist actions at specific periods in what we shall later refer to as terrorist campaigns. In part, these campaigns have been used in struggles for national independence or political separation in countries such as Israel, Cyprus, Algeria, Ireland, and at certain times in Vietnam. At other times, they have been used to change the political system from within by installing new leaders with new policies (as in Uruguay). Finally, they have been used by competing political groups to wage violent political competition outside of the political system (as in the right wing-left wing battles in Argentina).

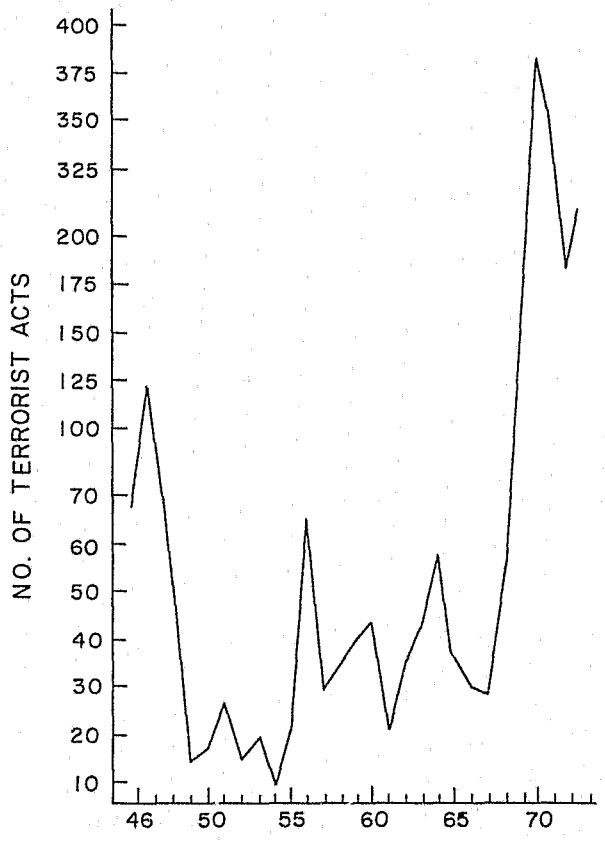


FIGURE 1. *A plot of terrorist acts from 1946-1973.*

TABLE 1. *Frequency of terrorist attacks on personnel or property of specific countries*

	United States	France	United Kingdom	Latin America	Israel
1946-1950	16	5	77	13	17
1951-1955	9	11	9	11	3
1956-1960	24	49	41	49	7
1961-1965	66	42	4	31	3
1966-1960	272	1	17	110	49
1971-	343	9	70	114	33

TERRORISM DIRECTED AT FACILITIES AND PERSONNEL OF THE DEPARTMENT OF DEFENSE

Over 14 percent of the terrorist acts directed toward the United States since World War II have been aimed at the personnel or facilities of the Department of Defense (DOD). Again using only open sources, CACI has identified 103 terrorist attacks since 1946 on DOD personnel and facilities.[1] Figure 2 displays these incidents over time. Defense facilities and personnel were infrequent targets between 1946-1969. After 1969, particularly in 1970 and 1971, the Department of Defense was a more commonly chosen target for terrorist actions. Terrorist actions directed toward DOD personnel and facilities numbered 30 in 1970, 33 in 1971, and 13 in 1973. Together, these three years account for almost 75 percent of all terrorist incidents directed at the Defense Department.

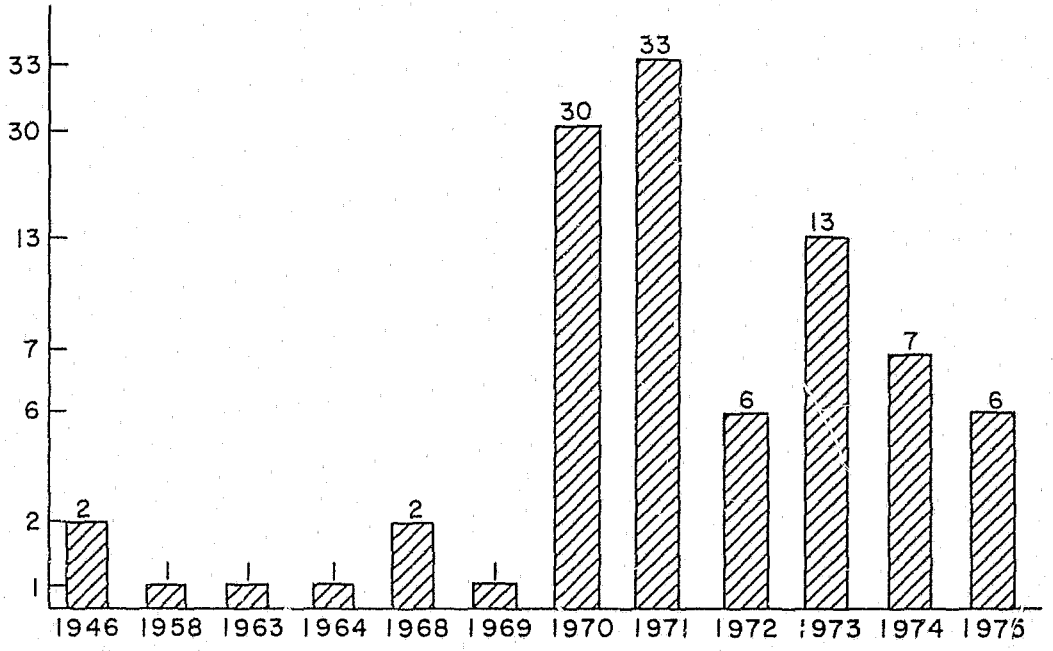


FIGURE 2. *Distribution of terrorist attacks against the Department of Defense over time.*

Table 2 breaks down the terrorist attacks against DOD by geographical region of occurrence. North America and Western Europe—where the majority of defense personnel and facilities are located—have been the site of the vast majority of terrorist incidents. Bombings outnumber the other types of terrorist incidents directed at DOD personnel and facilities by a substantial number (table 3). Firebombings are the second most common type of terrorist incident. Attacks against personnel—such as shootings and kidnappings—account for around 20 percent of the total number of incidents, while terrorist-sparked riots were the last identifiable incident type.

Table 4 presents information from the two previous tables in a different format, showing the most commonly encountered (modal) types of terrorist activity in each geographic region. North America, Western Europe, and South Asia are most commonly the site of bombings or firebombings. In the Middle East and Central and South

[1] These figures are subject to revision. For instance, there have been indications of at least 20 additional attacks against DOD targets in 1975.

TABLE 2. *Distribution of terrorist acts against the Department of Defense*
1946-1975

North America	38
Western Europe	37
Middle East	13
Central and South America	9
South Asia	6
	103

TABLE 3. *Terrorist acts, by type, against the Department of Defense*
1946-1975

Bombing	46
Firebombing	26
Kidnapping	13
Shooting	10
Riots	3
Miscellaneous	5
	103

TABLE 4. *Modal types of terrorism against the Department of Defense*
1946-1975

Region	Incidents
North America	Bombing, firebombing
Europe	Bombing
Middle East	Kidnapping, shootings
Central and South America	Kidnapping
South Asia	Firebombing

TABLE 5. *Location of terrorist attacks against the Department of Defense*
1946-1975

Government sites	59
Private residents	15
College campuses	9
Miscellaneous	20
	103

America, personnel are the more common focus of attacks. Kidnappings or shootings were the most likely incident in the Middle East. Similarly, kidnappings were the most frequent type of incident in Central and South America.

Finally, the data show that most of the acts occurred on government sites, as one would expect from the large number of bombings and firebombings in the cases studied. But private residences of military personnel in foreign countries are the second most common location struck by the terrorists. The third identifiable category, the college campus, is hopefully a passing phenomenon associated with the anti-war movements of the Vietnam era.

SUMMARY

These basic descriptions of the kinds of terrorist incidents that have occurred since 1946 and the kinds of incidents directed toward the Department of Defense indicate that terrorism is not a new type of activity but only one that has gained new popularity in recent years. The data also show that even basic analyses of the types and frequencies of events may yield useful information to organizations charged with physical security.

Most of the incidents directed toward the Department of Defense since World War II have been bombings or firebombings. While these are not actions that are to be dismissed as unimportant out of hand, they are not usually the kinds of actions that involve the attentions of high level policy makers for extended periods of time. But there is some scattered evidence in the writings and recent actions of terrorist groups that these individuals and groups have begun to shift tactics toward actions with potentially greater public impact. To plan and execute such attacks, terrorist groups must have greater capabilities and resources. Hence, the next section of the paper focuses on the changing character of the terrorist threat.

THE CHANGING CHARACTER OF TERRORIST OPERATIONS AND CAPABILITIES

A review of terrorist activities over the past 10 years shows some striking changes in the methods of operation used by international terrorist groups to achieve their stated objectives. In part, these new methods of operation reflect changes in the environment in which the terrorists operate. In part, they represent the development of a more experienced cadre dedicated to planning and executing dramatic acts of terror in several different industrial or developing countries. This section of the paper deals with the changing character of the operations and capabilities of the modern terrorist, focusing specifically on four major areas.

- The use of new technologies and communications to further the terrorist's aims.
- Increased sophistication in planning and training for terrorist acts, including international cooperation and funding between terrorist groups and certain governments.
- The problem of nuclear threats.
- The problem of biological, chemical, and precision-guided weapons.

The airplane is a prime example of how new technologies have advanced terrorist capabilities. Two or three persons can now hold up to hundreds of others hostage, destroy millions of dollars of property and disrupt a major form of transportation. In the extreme case, one well-placed explosive can end hundreds of lives. As a result, many airports around the world spend substantial sums on security apparatus.

Television, radio and press reports provide terrorists with instantaneous, worldwide coverage of their operations, fulfilling one of their primary objectives—publicity for their cause. The media also provide up-to-the-minute information on terrorist techniques and operations, facilitating a contagion effect in terrorist techniques. For example, in October of 1970, members of the French Canadian terrorist group, the FLQ, were reportedly traveling in New Mexico when word flashed over the radio of the kidnapping of British Trade Commissioner James Cross by other members of their organization. They immediately returned to Canada to kidnap Quebec Minister of Labor, Pierre La Porte, threatening to kill him if the demands of Cross's kidnappers were not met. La Porte's body was found in a car trunk on October 18.

These same advances in communications technology that have permitted the demonstration effect of terrorist actions to spread worldwide have also, together with the generally freer movement of peoples across national boundaries outside of Communist countries, facilitated the development of international terrorist groups that openly cooperate with one another in training for, planning, and executing dramatic acts of political terror. For example, Palestinian camps in the Middle East have been used to train foreign terrorists from Western Europe, Africa, Latin America, Asia, and North America, including groups such as the Japanese Red Army, the Irish Republican Army (IRA), elements of the Black Panthers, the Turkish People's Liberation Army, the Eritrean Liberation Front, and the West German Baader-Meinhof Group. Palestinian groups have also formed working relationships with terrorists in Argentina, Uruguay, Peru, Venezuela, Nicaragua, and other areas.

The exchange of personnel in actual terrorist operations has also been documented. During the 1970 Palestinian attempt to capture an El Al airliner in London, Israeli security guards killed Nicaraguan terrorists. The bodies of an Eritrean and a Turk were found among those of Palestinian Liberation Organization (PLO) infiltrators ambushed in the Jordan River Valley, and the 1972 Lod Airport massacre was carried out by the Japanese Red Army for PLO. Many examples of such cooperation exist, and trans-national relationships among terrorist groups are generally thought to be increasing.

Terrorist groups are also reported to receive substantial financial support from national governments. For example, Libya and Syria are reported to strongly back the Popular Democratic Front for the Liberation of Palestine. Libya is also strongly suspected of contracting the services of an international collective of terrorists in last year's incident with the Organization of Petroleum Exporting Country (OPEC) ministers in Vienna. Moreover, citizens in one country—such as the United States—are reported to have assisted terrorists in other countries (such as Northern Ireland).

Modern weaponry also has enhanced the potential capability of today's terrorist. For example, the Soviet SA-7 heat-seeking equivalent of the U.S. Redeye—a weapon that is easily portable by one man and capable of bringing down commercial aircraft—has appeared in terrorist arsenals. Two of these weapons were captured along with Arab terrorists at the end of a Rome airport runway in 1973. It should be emphasized, however, that modern weaponry is no substitute for ideological commitment and willingness on the part of the terrorists to sacrifice. There are also many examples of terrorists' procurement of advanced weapons systems which proved impossible for them to master or impractical for them to use.

But even without modern weaponry, today's terrorists are capable of inflicting greater destruction than ever before by virtue of the hundreds of vulnerable targets that characterize modern society. Besides large aircraft, such targets include conventional power generation plants and grids, computerized information systems, oil and gas lines, microwave transmitters, off-shore drilling structures, supertankers, nuclear plants and other facilities that characterize our technologically complex and interdependent society. Some of these targets of opportunity in modern society—including nuclear power plants—have already been attacked by terrorist groups. Other such attacks are likely in the future.

The threat of nuclear action by terrorists has been widely discussed in government and public forums. The terror implicit in such scenarios might be attractive to a few radical groups. Undoubtedly the possession of even the crudest nuclear device would allow a terrorist group unprecedented bargaining leverage and publicity, while causing far-reaching effects on a public that is already uneasy about many nuclear-related issues. Threats involving nuclear materials and facilities can be expected to increase in the future—if only for their dramatic publicity value. It is not at all clear that any terrorist group would ever reach the level of desperation required to execute a nuclear threat.

Although it may be well within their capability, mass-murder is an option that terrorists have not selected because of its counter-productive potential. Biological and chemical devices have long been available for such a purpose, but the point of terrorism is to frighten the audience and achieve goals through symbolic actions. But while mass-murder may be avoided, there may be situations where it will become impossible to positively discredit the credibility of a terrorist hostage threat involving biological, chemical, or nuclear materials. Crisis managers will then have to be prepared to make some very difficult decisions. Another remote possibility is the use of these special weapons by socalled "lunatic fringe" groups without explicit constituencies—such as the Japanese Red Army.

Nevertheless, it is clear that the *potential* for the use of special weapons—including nuclear and non-nuclear materials—is present and real. Advances by the United States in weapons design undertaken to reduce their size or increase their stability (such as the binary chemical munition) may paradoxically increase the magnitude of the terrorist security problem. Furthermore, the impact of demonstration or suggestions of capability on other groups should not be underestimated. Thus, one can only wonder whether concern over the terrorist potential in these areas may also be increasing the interests of terrorists in these weapons. For example, a recent search of Middle Eastern publications undertaken to discover if any terrorist groups were

contemplating such nuclear related activities revealed only one reference to the subject. A touring American scientist had suggested in an interview that terrorist groups were not capable of nuclear activity.

SOME CONTRIBUTIONS OF THE BEHAVIORAL AND SOCIAL SCIENCES TO MEETING THE TERRORIST THREAT

The research tools and findings of the behavioral and social sciences provide useful guidance on ways to confront the terrorist threat and actions to avoid in responding to the terrorists. Additionally, these sciences have developed research tools that can be used to gain additional insight into the most useful ways to confront various combinations of terrorist tactics. In this section of the paper we shall consider the contributions that the behavioral and social sciences can make to meet the terrorist threat in three areas: prior to the occurrence of terrorist incidents; in response to the single (apparently isolated) terrorist incident; and during the terrorist campaign.

PRIOR TO THE TERRORIST INCIDENT

The Problem

Highly visible dramatic acts of terrorism have become endemic in Western societies. Individuals and groups seeking publicity, personal fulfillment, and redress of perceived grievances have turned to physical assault on public order and authority. Some of these acts have been problems since the organizaton of society (assassination and kidnapping); others are products of civilization (bombings and skyjacking); while still others (nuclear blackmail) are primarily future dangers. Advances in weapons technology and the increasing interdependence of modern society have increasingly made it possible for a small group or even a single individual to inflict great property damage or cause many deaths.

For those charged with defense and security functions, these terrorist acts are a constant danger and a growing problem. A variety of factors make it increasingly difficult to foresee and prevent attacks on public order. First, there are many possible motivations for the attacks and potential sources of them. Emotionally unstable individuals seeking attention for their problems or recognition because they are unable to resolve the problems of living in modern society are one potential source of attack. Ideological or ethnic groups seeking to dramatize their causes, arouse groups of potential recruits, or damage the image of public authority are another source of danger. Of course, some members of these groups are also emotionally unstable. Hence, terrorist actions may be carefully planned attacks by well-organized groups, the ill-conceived actions of a disturbed mind, or something in between.

The problems of preventing and planning for terrorism are further complicated because of the small number of individuals usually involved in an event. These small groups seldom have records of major criminal involvement, so normal networks of informers and police surveillance are unlikely to be of value in locating them.

Faced with this situation, defense and security officials have increasingly adopted passive, reactive, and publicity-oriented postures toward terrorism. One set of responses is passive—establishment of physical security measures for popular or vulnerable targets. Physical barriers, trained guards, airport security procedures, all fall in this category. Reactive measures include vigorous investigation and prosecution when terrorist acts do occur. Publicity-oriented responses include tough negotiating positions when dealing with kidnappers and skyjackers, publicizing the effectiveness of detector systems for finding weapons, and other measures designed to deter attacks by making them appear hopeless. Some "active" measures, such as developing assassin "profiles" are also used. When information about terrorist intentions does exist, vigorous investigation is often undertaken.

Several key decisions must be made in the defense and security agencies to determine the level of security against terrorism and the cost of that security. They are made by experienced personnel based on the best information available to them:

- How much security is necessary?
- Where should security forces be located?
- When should enhanced security procedures be implemented?
- How long should they be maintained?

Given the occurrence of a terrorist attack on public order:

- What policies should be followed when dealing with terrorists who hold hostages or threaten large scale destruction?
- What outcomes should be sought or avoided?

These questions are of world importance, since the potential for terrorism exists in many locations. Moreover, terrorism appears to have a "contagious" influence—decisions made in one incident may have implications thousands of miles away. Finally, the "patterns" in terrorist actions can be revealed only through a coordinated effort, since the terrorists operate in so many countries.

Some Tools for Analysis

Effective application of social science research tools could provide systematic information on terrorist attacks on public order. This information would be directly useful for:

- Allocating resources—deciding when and where security forces are needed.
- Identifying periods of greatest likelihood of attack on public order so that enhanced security measures can be implemented.
- Estimating the extent of contagion from terrorist acts to determine the length of time during which extra security may be needed.
- Identifying policies which are effective in deterring terrorism.
- Identifying outcomes likely to cause or inhibit further terrorist attacks.

These kinds of information can be produced because terrorist acts are amenable to statistical analysis.

- The events are highly publicized, making their identification possible.
- The major categories of events—assassination attempts, bombings, and so forth—can be easily distinguished.
- There are enough events to meet the assumptions of powerful statistical techniques.

The Occasion of Terrorism. Terrorist acts coming without prior warning are the most likely to do serious damage. Prediction of the precise times and places of these attacks is virtually impossible. Emotionally disturbed potential assassins become confused and arrive late to political rallies. Random factors intervene: bombs fail to go off; or the unexpected presence of a uniformed policeman causes the cancellation of a plan. Moreover, organized groups plan very carefully to strike at unexpected times and places.

It should be possible, however, to determine the conditions and locations in which terrorist attacks are most likely to occur. Based on this information, it should be possible to determine the regularities in dramatic violent acts, and to plan and allocate resources accordingly. Because of its motivation, terrorism should be associated with social stress and social strife. When social pressure and the pace of modern life are greatest, emotionally disturbed people become more and more likely to lash out and seek recognition or relief through public violence. Hence, the analysis should include

linkages between measures of social stress in a city, state, or region and the occurrence of terrorism. A number of these indicators—unemployment, bankruptcies, suicides—are available and can be explored to identify those which are predictors of a climate of terrorism.

Terrorist groups are often rational and calculating. In many ways they are potentially more dangerous than individuals since they have greater capability to acquire sophisticated weapons and the technology to carry out mass destruction. They come into being and turn to violence not because of social stress, but because of social conflict. Projecting the likelihood of dramatic attacks by these groups requires examination of the level of civil strife within a locality. Political activism, strike violence, police/civilian incidents, riots, ethnic disturbances, and other indicators of social conflict should be associated with violent acts to produce predictors of dramatic violent activity along this dimension.

Since it is seldom possible, and would never be economical, to double the overall size of a security force or security agency every time the probability of terrorism reached a danger level, it is vital that the analyses produce indicators of the likely *locations* of terrorist actions. Increased security can then be allocated rationally and the burden on personnel and the costs of security can be held to a minimum. All cities, states, and regions are different. Moreover, the target of violence—particularly if it is inspired by social conflict—will be chosen at least partly because of its relationship to the perceived grievances and issues in the conflict. Here, again, no firm answer is likely. It should be possible, however, to produce a *profile* of likely targets. This profile would be similar to those now is use for identifying likely assassins in a crowd or skyjackers at an airport. Experienced security personnel, familiar with their own facilities, localities, and situations, should be able to use the profile to determine the key locations where security forces should be located.

The construction of a profile would again be a task of theoretical analysis and empirical validation by tracing patterns of association. First, a list of likely profile attributes would be constructed. These might include ease of access, value of the target to society, level of existing security, proximity to secure areas for preparation and escape, and presence of large numbers of people, among other things. A large number of different terrorist events would then be coded for all these variables. Associational and clustering techniques could then be applied. They would produce information on the likely *combinations* of attributes present in targets. Separate analyses of different types of violence and trend analyses would also be useful. The result would be a straightforward profile describing likely targets. Taken together, the likelihood indices for actor, type of violence, and target will provide powerful decision aids to security officials around the world.

Contagious Violence. Terrorist attacks on public order are among the most newsworthy of all events. Assassination attempts, bombings, skyjackings, and kidnappings are given wide coverage in the media, particularly in a free society. This publicity is attractive to many emotionally disturbed individuals and to politically organized groups. Police departments come to expect large numbers of false confessions to dramatic crimes. Similarly, individuals seeking attention or relief from emotional pressure or groups seeking increased prestige may be moved to action by media reporting of dramatic terrorist acts. Since control of the media is neither legal nor desired in a free society, security forces must expect and be prepared for "contagious violence." Four key questions must be addressed when the potential for contagious violence exists:

- What is the *scope* of the contagion—where should security be increased?
- What is the *length of time* the contagion should be expected to last?
- What *policies* can be pursued to discourage contagion?
- What outcomes should be sought?

Each of these questions is amenable to systematic analysis.

The scope of contagion should be related to the type of terrorist act, the extent and distribution of media coverage of the event, and the existing conditions for violence discussed in the preceding section. The same analyses used to study scope can be used to determine the length of different contagion cycles.

The *policies* utilized and the *outcomes* of events have related, but not identical effects on contagion. Policies are sets of rules determining actions. Authorities decide to negotiate, provide food, pay ransom, provide automobiles or aircraft, attempt to shoot a kidnapper, and so forth based on policies. Every such action is reported in the media and may have influence on the contagion effect. Outcomes—whether the terrorist escapes, is killed, is arrested peacefully, is captured only after a dramatic chase—refer to the results of those actions. Outcomes are at least partly beyond the control of security officials. Outcomes, too, have a profound effect on other potential lawbreakers. Escape and wide publicity are generally assumed to produce high contagion. Some non-obvious patterns also emerge, however. The killing of skyjackers, for example, has been shown to cause more attempts, apparently because the psychological desire to die is a characteristic of some skyjackers. Associations between police policies, publicity, outcomes and contagion should, therefore, be reviewed. Research on the impact of different policies should be undertaken using the tools of modern social science.

THE TERRORIST INCIDENT

The behavioral and social sciences have also begun to contribute to the assessment of the terrorism threat and the management of such crises in specific instances of terrorist action. As members of local, state and federal task forces, behavioral scientists are often involved as consultants to crisis managers. From information concerning the modus operandi of a terrorist group, such as the type of attack, weapons used, type of demands, the amount of planning implied, group size, ideological commitment, communication styles and training, behavioral scientists can help guide the responses and suggest the likelihood of success of particular counteractions. Information concerning past interactions of a group with a local government—including their willingness to negotiate, compromise, allow deadlines to pass or take violent action when provoked—can be useful to behavioral consultants attempting to analyze the probability of success of specific tactics. In short, systematic examination of the range of information available using the tools of social statistics can greatly assist in the realistic evaluation of terrorist threats.

The capability of the terrorists to engage in prolonged negotiations, the age, sex, nationality or ethnic origin of the terrorists and hostages and of course any information on the past history of individual perpetrators are additional pieces of information that can be systematically analyzed. The perpetrators' demands can often provide useful information on the identity, motivation, capabilities, and real intentions of the terrorists. For instance, the greater the evidence that the author of an extremely destructive threat is acting alone and is communicating an extremely difficult demand in an irrational manner, the greater the decline in his credibility. Political terrorists in single incidents have generally limited themselves to immediately satisfiable demands such as the release of prisoners or cash—rather than to policy changes that are more subtle and time consuming. Most serious groups will be well-enough acquainted with their targets to realize the impossibility of many types of demands, such as the resignation of elected officials, and will limit their demands accordingly.

Another mark of the serious political terrorist is whether the target is offered a means of communicating and negotiating. The terrorist threat itself may also be a guide to the nature of the group. The amount of financial investment, technical skill, logistic support and personnel necessary to complete a particular threat may diminish the

credibility of many groups. This is clearly true for threats that involve nuclear weapons or precision-guided munitions.

The threat may be accompanied by various forms of proof such as claims of responsibility for past incidents or diagrams that can further characterize the perpetrators. Other clues might be available from explanations of the choice of victims, target of demands or the presence of manifestos to be published.

In short, analysis of the specific incident from two perspectives can contribute greatly to a realistic evaluation of the terrorist threat. First, the incident or threatened incident can be evaluated against existing profiles of groups and assessments of stressful conditions measures as suggested in the previous section. Thus, the group's capacity to execute the action can be evaluated or the group can be identified through a search of the group profiles. Second, behavioral science can assist in the bargaining and negotiation that might occur before, during, or after an incident. The guidance of clinical psychology can be very helpful to the successful conduct of these negotiations.

THE TERRORIST CAMPAIGN

While the previous section discussed the contributions of the behavioral and social sciences to preventing or dealing with the single terrorist incident, this section considers the terrorist campaign and government responses to the campaign. By terrorist campaign we mean the repeated and systematic application of acts of violence by one or more groups, working separately or together, to force a change in the government leadership, in the policies of the government, or in the nature of the political system. Examples of terrorist campaigns include the activities of the Irish Republican Army in Northern Ireland, the Japanese Red Army in Japan and elsewhere, and the Baader-Meinhof Gang in the German Federal Republic.

Action-Reaction Cycles

Studies by a number of authors have considered political violence generally and political terrorism particularly as an action-reaction cycle between the terrorists and government authorities in which the pattern of exchanges often creates a dynamic that has far reaching implications for both sets of participants. Thus, terrorists may undertake a campaign expecting authorities to overreact in ways that will contribute to the ultimate goals of the terrorist group. Alternatively, government authorities may select their responses to minimize the chances of the terrorist organization growing by attempting to contain the campaign, by applying so much force that the terrorists are forced to change tactics, or by moving to reduce popular fear of the terrorists by some other set of policies. In each case, the action-reaction cycle may produce a series of unanticipated consequences, as the terrorists may not be able to traumatize the society and further their cause or the government may overreact and partially legitimize the aims of the terrorists. In short, within the action-reaction (as fig. 3 suggests) is the potential dynamic for the unanticipated—the escalation of acceptance of the terrorists or the destruction of the group.

In the action-reaction cycle, terrorists and government enter a series of exchanges in which each attempts to outbid the other in a struggle for public support. Using such a conceptualization, the participants can analyze the effects of their actions on the other, and particularly examine the impact of violence and counterforce on public sentiment.

The action-reaction cycle can be illustrated as follows. At the outset, terrorist operations are usually designed to accomplish training, logistics, propaganda, recruitment, financial, and other organizational goals. The bank robbery is the classic example of an operation designed to attain these goals. During this period the terrorists are a strictly criminal gang with political ends in mind. But the attention of government

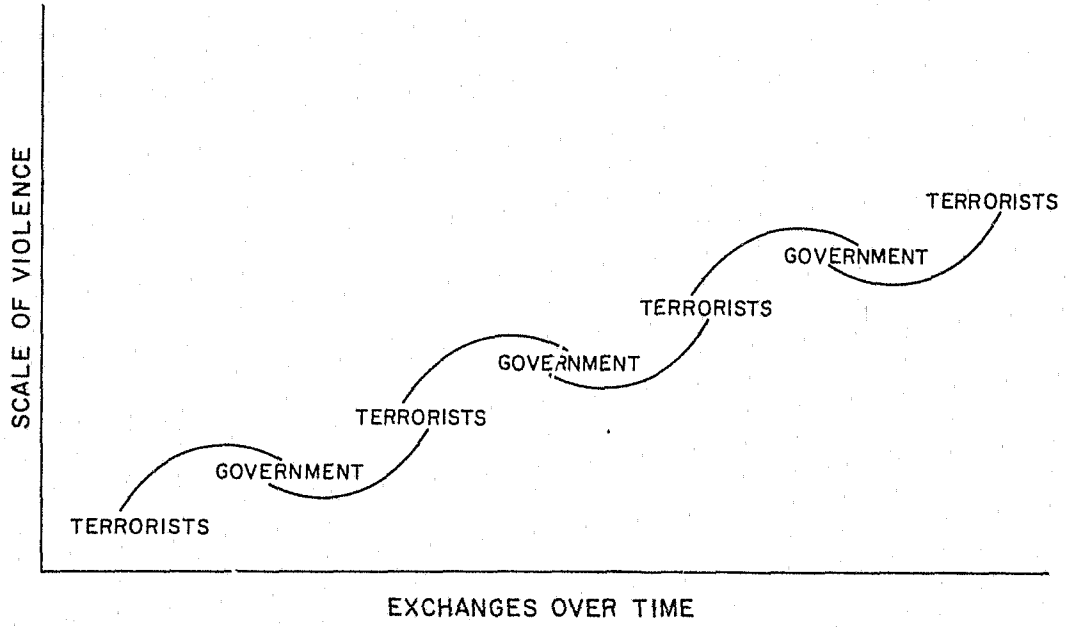


FIGURE 3. *Example of a hypothetical action–reaction cycle.*

decision-makers and the public usually becomes focused on the terrorists after they feel confident enough to begin a violent psycho-political offensive.

The long-term goals of the politically serious terrorist organization often involve modifying or replacing an existing political system. Specific issue-oriented terrorist campaigns may not directly involve these radical goals and their tactics and impact are usually limited to a specific societal target rather than aimed at causing widespread fear in society as a whole. Because they operate from a position of tactical and political weakness, an attack on the political system must be accomplished by producing strong, consistent, and widespread stress on key societal structures. One of the primary foundations of the relationship between a country's political leadership and those they govern is an agreement that the former are responsible for guaranteeing the physical security and safety of the latter. This is the foundation that terrorists often target to destroy or discredit.

Applying stress to these societal foundations takes many violent forms. Thus, bombings at public places, the deaths of bystanders, and the taking of innocent hostages for political ends may all aim at convincing the public that its leaders are incapable of protecting it from violence. While the mechanisms that control the speed with which this public fear spreads, when it does spread, are not completely clear, there is some evidence that social contagion processes are at work. Some observers believe that combinations of activities also produce closer public identification with the terrorists. Anger at political leaders for failing their primary responsibility definitely seems important. Government overreaction to terrorist episodes is also a major cause of shifting public sentiment and isolation of the government.

Another common characteristic of terrorist campaigns is the necessity for the terrorists to continually escalate the levels of their violence to maintain an atmosphere of fear. Situations which at their outset may produce extreme stress in populations can be adjusted to in time. But, by continually escalating levels of violence for this purpose, terrorists may also exceed the bounds of what society will tolerate, regardless of the popularity of their ideological goals. Decision-makers should be prepared to exploit opportunities resulting from exessive terrorist violence.

Under the stress induced by terrorist campaigns the citizenry often attribute the success of terrorism to the government, a source that should be instrumental in preventing the danger. The greater the public's feeling that the government should be capable of preventing terrorism and protecing them from it, the greater will be the anger at and alienation from the political leadership. The stage is then set for increased public identification with the aggressing terrorist group.

Of course, public authorities cannot prevent terrorist attacks or protect every citizen or public place. However, to preserve the foundations of society, at least in principle, they may be forced to limit civil liberties, risk international ostracism, and divert significant resources to defeat the terrorist campaign. But such extreme reactions risk alienation of the public, greater support for the terrorists, and political attack from the less conservative elements of society. On the other hand, preservation of democratic liberties and avoidance of more effective measures risks further terrorism, loss of public faith and political attack from some "law and order" elements of society.

The results of these pitfalls have been demonstrated in Uruguay (1971), Turkey (1971), Brazil (1971), and Northern Ireland (1974), where terrorism caused the creation of new and more politically repressive regimes. In these cases the terrorist strategy seems to have backfired, or worked too well, at least in the short term.

The Federal Republic of Germany is one country that has successfully balanced between repression and over-tolerence. Its anti-terrorist campaign included the organization of disciplined and trained anti-terrorist forces. Extremely good intelligence on the movements of suspected terrorists and excellent communication with the public, including logical explanations for moderate government actions, were other key ingredients of German success.

Behavioral Observations

Psychologists and sociologists have conducted limited case studies of terrorist-decision-maker interactions to examine their impact on public sentiment. They conclude that the application of some basic behavioral concepts to the formulation of anti-terrorist policy can be extremely cost-effective, and failing to consider the psychological factors that influence the motivation and impact of terrorism can be an extremely expensive mistake. The following examples of behavioral observations of terrorist-decision-maker interaction could be very useful to crisis managers confronted with a serious terrorist challenge.

Initial terrorist activity seems to occur when there is a perceived categorical rejection of potential terrorist demands by the government. Terrorism is an extremely serious business and potential terrorist groups will exhaust conventional and unconventional channels to decision-makers before resorting to violence. Even after civil disobedience and armed resistance to objectionable government policies or regimes, the use of terrorist violence remains a quantum leap in tactics. After continued rejection of their demands has resulted in terrorist violence, government offers of access to decision-making machinery or other concessions are likely to be rejected, even though they might have been accepted before the acts of terrorism. Successful government counter-offers must compensate for the increased ideological commitment, political emotional expenditure,and sacrifices made as the group attempts to succeed.

The ideological commitment of the terrorist group heavily influences its resolve and tactics. Individually, group members who more readily accept the high personal risks associated with terrorism are also more likely to believe that their actions will contribute to the accomplishment of their ideological goals. Such commitment verging on fanaticism may easily compensate for the lack of modern weaponry and funding. A well-developed strategy characterized by concrete planning and group member identification with the perceived need for particular actions will contribute to individual

resolve. Ideological commitment is also manifested in the extent to which members reject acts that create risks for the group as opposed to individuals.

Authorities should be extremely careful not to underestimate the power of an ideological cause. Risks perceived as non-rational by the outsider may seem logical to the dedicated terrorist. Thus, offering a terrorist his or her life in a bargaining situation may be ineffective. This ideological rejection of acts endangering the cause has resulted in extreme behavior, such as the execution of over-zealous terrorists by members of their own group. Decision-makers may be able to cause internal disruptions among groups divided on the question of the appropriateness of certain terrorist practices by emphasizing the counter-productivity of radical attacks. Moreover, the degree of ideological commitment of a terrorist group will directly affect tactics as well as group solidarity. Ideologically committed groups will view their terrorist activity strictly as a means for furthering political objectives. Targets may be carefully selected for symbolic value and excessive and indiscriminate casualties will be avoided. Groups that highly value public support will be strongly disposed towards public explanations of their actions. But greater perceived isolation of a terrorist group or their rejection by other societal factions is likely to reduce the extent to which precautions will be taken to avoid excessive casualties within those factions.

One of the most important and relevant behavioral observations made is the continued need by terrorist groups for reinforcement. According to one study, unanticipated and undesired consequences for the terrorist may produce cognitive disonance. Repeated disappointments—including doubts of ultimate victory—may breed disillusionment and a change in terrorist tactics. Hence, assessments of terrorist threats can be aided by strong intelligence action to determine the exact purpose of the terrorist acts in order to avoid reinforcement and aid evaluation of the effects of proposed countermeasures.

AGENDA FOR THE FUTURE: ORGANIZATIONAL AND RESEARCH IMPERATIVES

This paper has examined the nature of threats posed by international terrorist groups to industrial societies generally and facilities and personnel of the Department of Defense specifically. Two sets of recommendations—organizational and research oriented—are presented in this section to conclude the discussion.

ORGANIZATIONAL IMPERATIVES

At the present time, the efforts of the U.S. Government to prepare for and meet the threat of international terrorism are fragmented through a large number of agencies and departments, including the Departments of State, Justice, Defense, and Treasury, the Federal Bureau of Investigation, the Central Intelligence Agency, and other major organizations.

Beginning in 1972 an attempt has been made through the Cabinet-level Committee to Combat Terrorism (and its Working Group) to coordinate the efforts of the U.S. Government in protecting the property and lives of its citizens and organizations.

Despite the diligent efforts of representatives of a large number of concerned departments and agencies, relatively little progress has been made in developing a coherent, realistic policy stance on terrorism, on coordinating information that can be used to combat terrorism and evaluate the terrorist threat, and on establishing crisis management procedures that can be employed when or if a major terrorist incident occurs. While there are many reasons—organizational and otherwise—why these goals have not been met, we shall merely note one aspect of the problem: the jurisdictional limitations of the existing agencies and the existing demands on the time of the major participating groups.

As noted in previous sections, modern terrorist organizations that can mount sustained, credible threats against U.S. citizens and U.S. Government facilities and personnel often are reinforced by international cooperation, training, and funding. At the same time, organizations in the U.S. Government that must collect, collate, and analyze information on the activities of these groups are limited by law in the kinds of materials that they can collect and evaluate. Domestic intelligence responsibilities reside with the Department of Justice and the FBI as its agent. International collection and analysis responsibilities rest with the CIA as the center for the production of finished international intelligence products. To this point in time, these agencies have not coordinated their efforts. Considerable information that would contribute to a systematic assessment of threats posed by groups that operate both internally and internationally is not completely collated and analyzed because no single organization is charged with carrying through such analyses.

Additionally, the information for effective policy formulation on terrorism is only one small part of the information that these agencies must provide. At the present time, the information requirements in that area are given (for obvious reasons) a considerably lower priority than is the acquisition of information on Soviet strategic weapons, the activities of organized crime, etc. Hence, terrorist information acquisition and analysis suffers from the need to divert resources to other tasks.

If terrorist activities are to be examined systematically and subjected to realistic threat analyses, additional information collation is mandatory. This information must come from domestic and international sources. It must be examined jointly as part of a single, unified inquiry into the threats posed by terrorists and the means to respond to those threats that are identified as credible. Accordingly, consideration should be given to the creation of a single group or task force—perhaps modeled after the Drug Enforcement Administration—that has complete responsibility in the area of terrorism. Such an agency would not necessarily need its own collection machinery. It would need access to the information collected from existing sources in a timely manner so that the collation and analysis of domestic and international materials could be undertaken rapidly by trained threat analysts.

In addition, the Department of Defense must recognize that it too—along with the Department of State, the FBI, and the CIA—has a unique role to play in the identification and response to terrorist threats. No other organization has so many facilities located worldwide that present such attractive targets for serious terrorist groups. The Department of Defense has begun to increase physical security at a number of these locations. These efforts are to be applauded and encouraged. Yet additional vigilance at particular locations seems to be required. Terrorist groups have already been connected with major weapons thefts from U.S. Government facilities. Should terrorists decide to seize precision-guided munitions, binary chemical weapons, nuclear devices, or other special weapons, it is clear that isolated Department of Defense storage facilities will be prime targets. Given this vulnerability, increased interest by the Department of Defense in both expanded physical security and the contributions of systematic threat analysis to the optimal deployment of these physical security devices is vital to the protection of DOD personnel and facilities.

RESEARCH IMPERATIVES

There is a need, now, to begin a major program of research into the conditions associated with dramatic attacks by terrorists on public order. The application of existing analytical techniques could provide new valuable systematic information relating to the occurrence of this type of violence. This information is needed both because this type of illegal activity is becoming endemic in industrial societies and because traditional security procedures have been stretched as far as they can, given the existing resource constraints. The development of six specific tools is suggested.

- *An index which forecasts the likelihood of terrorist acts by emotionally disturbed individuals based on indicators of general social stress*. This index will alert security forces when to take the types of action likely to deter attack—visible police presence, enhanced security of public buildings, and so forth.
- *An index of social conflict which projects the likelihood of attacks on public order by terrorist groups motivated by ideological or ethnic considerations*. This analysis will also produce a typology of groups likely to engage in terrorism and may, when validated, serve as a guide to determine when surveillance techniques and information collection are warranted.
- *A profile of likely targets of terrorism*. This profile, in the hands of experienced security personnel familiar with a locality, will allow identification of events, locations, and persons likely to be targets of dramatic terrorist violence. Day-to-day security measures can be reviewed in this light, including allocation of resources and existence of security and alarm systems. Contingency plans can be developed for periods when enhanced security will be required. Crisis decision-making can also be informed by this type of profile.
- *Projections of the scope and duration of contagious terrorism*. These data will help law enforcement officials across the country by alerting them when enhanced security precautions are wise or necessary. They will also allow efficient use of resources by providing likely boundaries beyond which this enhanced security is unnecessary.
- *Policy guidance for a variety of different kinds of terrorism*. Relatively few security officials have extensive experience in dealing with terrorist attacks on public order which involve protracted interactions with terrorists. Kidnappers, skyjackers, and trapped terrorists provide a newsworthy event. Government actions are almost always focused on the immediate problems of public safety, ending the confrontation, and apprehending the guilty. Little thought is given to the possible effects of policies on other potentially violent individuals and groups. But these policies do have implications for other people. Systematic analysis of past policies can be expected to provide guidelines for decisionmakers in these critical situations.
- *Information on the impact of different outcomes of terrorist incidents*. The results of violent acts, perhaps even more than police policies during confrontations, can be expected to influence the likelihood of contagious violence. Systematic analysis of the effects of different outcomes on subsequent terrorist acts can be expected to produce important information of use to policy makers.

Dramatic terrorist violence is an international problem. Development and implementation of effective tools for projecting, preventing, and controlling this type of crime is vital. The policy aids suggested in this paper are not a panacea. They would, however, be of great help in reducing the incidence of dramatic terrorism directed at the public order. Research to develop these tools should be undertaken now and pursued with vigor.

DISCUSSION

MS. JANE PRATT, Mitre Corporation: You have tabulated terrorist acts in different places in the world. Would you speak for a moment about methodology—how do you define a terrorist act? What sources do you use to get the information?

MR. HAZLEWOOD: I will defer that to my colleague, Mr. Shaw, who was very active in doing the tabulation.

MR. SHAW: The sources ran the gamut from the *New York Times* to chronologies put out by various government groups that are available through a group called the Cabinet Committee to Combat Terrorism in the State Department. There have been other studies by various research organizations, including your own and many others.

MR. GEORGE HAUGEN, Stanford Research Institute: You have mentioned in discussing several of the statistics, particularly the firebombings in South Asia, an attack on an Agency for International Development (AID) mission there. But you also mentioned that the statistics were based on attacks on Department of Defense installations. I wondered whether you have, for the purposes of compiling those statistics, defined AID missions as Department of Defense (DOD) installations?

MR. HAZLEWOOD: We have excluded AID missions and attacks on embassies, consulates, and legations from our set. The 103 incidents we have been talking about involved DOD armories, facilities or personnel. Included in this category are DOD armories, individuals who are identified as working for the Department of Defense such as military attaches, an individual assigned to part of a military aid mission such as those who were assassinated in Iran while part of the military assistance group there, and attempted or actual thefts and bombings carried out on defense facilities. We excluded the other U.S. Government categories. They are tabulated separately. The incidents that I was talking about here, the 103, are clearly Department of Defense.

MR. JOHN ALBERTSON, Army Intelligence Agency: You were talking about developing and studying group capability profiles in your agenda for the future. How can you do it in DOD and be legal?

MR. HAZLEWOOD: Within the Department of Defense you cannot. One of the first things that I mentioned was that we think that there is an organizational need for some group to take charge of getting and collating the available information that the Federal Bureau of Investigation (FBI) has gathered, that legitimate inquiries within the Department of Defense have gathered, that the Central Intelligence Agency (CIA) has gathered, as well as information from a number of other sources. This would call for a change in the law, either through executive order or legislation, to set up some new organization. I fully understand the legal limits on DOD at this time. One of the reasons for evaluating only DOD incidents outside the United States is because DOD is under extreme limitations on the kind of information it can get.

MR. ALBERTSON: We're working on that right now and that's our problem. Actually, we've only got two groups that we can collect from as far as the Army is concerned. I don't know about other agencies.

MR. HAZLEWOOD: There is substantially greater latitude at the CIA and they have been gathering some very useful information.

MR. ALBERTSON: But they cannot, in turn, give it to us. That's our problem. We're going to defend or try to protect a DOD facility, such as where you store nukes and other materials. You can't collect information on an outfit that's working right beside you. The FBI can give you this information and, legally, it has to go in one ear and out the other.

MR. KRAMER: General Cappucci may address this issue later this morning. I don't

know if there are any answers, but we'll hear a little bit about it later.

MR. GENE BROWN, U.S. Air Force: You indicated that certain types of terrorist acts were prevalent in certain areas of the world. I wonder whether you can conclude from this that the kinds of acts resulted from availability of either facilities or personnel; for example, in firebombing, bombing, shooting or kidnapping.

MR. HAZLEWOOD: Clearly, at least one of the reasons that more incidents are concentrated in North America and Western Europe, if you're talking about incidents directed at the Department of Defense, is that's where DOD facilities tend to be concentrated. It may well be the case that, in addition to the physical concentration in those regions, there is something deeper. For example, the easiest way to attack DOD facilities may be with a bomb. On the other hand, if you're going to attack personnel, maybe a communications station in Asmara is so isolated that you can grab personnel. There are clearly dynamics between the availability of targets and the varying capabilities developed to counter terrorists. What we are attempting to suggest is that you can at least draw some profiles that would say, if you're in this kind of area, you must be more concerned about certain kinds of security than other kinds.

FEDERAL AVIATION ADMINISTRATION'S BEHAVIORAL RESEARCH PROGRAM FOR DEFENSE AGAINST HIJACKING

Dr. Evan Pickrel

Federal Aviation Administration, Washington, DC 20591

A gross overview of the hijacking problem and the behavioral contributions to our boarding gate and in-flight defenses will be presented. This will be followed by an examination of our hijacking data to identify the effects of a psychological deterrent, a publicity campaign to discourage potential hijackers. Finally, our profiling methodology will be looked at in somewhat greater detail for possible application to meet other threats.

The problem of aircraft hijacking started almost as soon as the introduction of scheduled flight. In fact, the French experienced hijackings immediately following World War I when establishing air service across the Sahara, and Pan Am experienced hijackings in the early 1930's in South America and in the Far East.

But only in recent years did hijacking frequency become a problem in the United States. We can see that, for the many years from 1930 to 1967, only 12 hijackings were on record in the United States. Yet in 1968, 22 hijackings were recorded, and the problem continued to escalate after 1968. As this problem continued to escalate, there was much wringing of the hands and many people tried to introduce controls. Congress did what it could. Other agencies attempted solutions, and then the Federal Aviation Agency (FAA) finally set up an interdisciplinary team.

In 1968, then, an interdisciplinary team was set up by the FAA to attack the problem. This team was headed by the Deputy Federal Air Surgeon, and included such disciplines as security, law, medicine, management science, public information, electrical and aeronautical engineering and psychology.

The defense requirements they identified included: (1) convincing potential hijackers not to try the act, (2) creating defenses to keep those who try and weapons off the plane, and (3) defeating those who get on board to discourage others who might think about playing the game.

When one thinks of the various disciplines cited, and how they might contribute to each of these defense requirements, and this was a task assigned to each of those disciplines, public relations was certainly involved, including journalism and psychology in an effort to convince potential hijackers not to try. With respect to defenses to keep those who try and weapons off the plane, our legal people became involved in terms of making the act illegal and making it illegal for anyone to carry weapons on board the aircraft. These are a few examples of these various specialties and how they might contribute to meeting these defense requirements.

The team gathered whatever information they could find on past hijackings to give them a base of data for use in resolving future hijackings. They gathered all the historical information they could find from newspaper and magazine files, the New York Times as an example. In 1968, they then established procedures for gathering additional information by means of the FAA interviewing all participants after a hijacking. The FBI, Airline Pilots Association and the airlines were involved. They didn't restrict their interviewing to those involved in the hijacking itself. They went to those who knew the hijacker prior to the event, parents and friends, to gather any information they might have with the hope that this information could be useful in deterring future hijackers.

What kinds of information did they gather? For flight information, they gathered information on the kind of airplane. At one moment in time, the 727 airplane was one of the most popular for the parachute extortionist. Information related to the kind of aircraft, where it was taking off from and where it was headed was collected. The earlier hijackings (1968 and 1969) were generally in the area approaching Cuba. They also gathered operational and maintenance information on the aircraft.

Information related to the interaction or the interface between the crew and the hijackers, as the interface might involve physical injury, and anything else that could lead to control over the hijacker, was collected. Hijacker personal history data such as age, employment record and schooling were gathered to learn more about him/her.

What were the uses for all the information? They will be discussed in greater detail later, but those which are specificaly cited are profiling and the development of tactics for defense against hijackers. Typical analysis questions asked against the information base, in terms of the hijacker, would include: what kinds of people do it, why did they do it, how did they do it and what might have been done to prevent it? Questions asked related to the hijacking activity would consider: (1) the weapon, (2) the threats and their weakness or strength, (3) familiarity with the aircraft and its limitations, and (4) familiarity with the weather and other operational restrictions.

The problem, as it was escalating in 1968 and 1969, initially appeared to be hopeless. The airlines themselves felt that search at a boarding gate would negate their ability to keep their flight schedules. They felt that nothing really could be done in this fashion to control the problem of hijacking. Dr. John Dailey, the psychologist on the team at that time, suggested that they only search the hijackers, those who gave them the threat. A now retired Navy captain who was on that team as an operational man said that Dr. Dailey's suggestion was senseless. But Dr. Dailey pointed out that all one needed to do was search a high risk group that could include many good guys; if one could identify a high risk group which contained most of the hijackers, that part of the problem would be controlled. So his suggestion, then, was that the search be restricted to potential hijackers or a high risk group that approaches the boarding gate.

He proceeded to sort out information that had been gathered prior to that moment in time. He compared the normal air travelers to the hijackers and found that the normal air traveler is a businessman or successful member of society. Hijackers as a group were failures. There were a great many different kinds of hijackers including homesick Cubans, mentally ill, extortionists, political terrorists and even fleeing felons shooting their way on board. But despite the diversity among the hijackers, Dr. Dailey managed to create a behavioral profile which identified less than two percent of the air travelers as members of a high risk group that would need closer scrutiny, because most hijackers would be among its members.

This ratio seemed small enough to make boarding gate search possible, but the airlines really weren't interested at that moment in time. If you were Western Airlines and weren't experiencing nor had you experienced a hijacking prior to that date, would you be interested? The hijackings tended to be restricted to those airlines whose planes went to or near Florida. There were, therefore, a few airlines that were interested and some started to use the behavioral or psychological profile at the boarding gate. While they were few, it meant that Dailey could gather data for further research. The success of this effort was evidenced with the first sample I drew, for all of 1970 and the bulk of 1971. The prediction accuracy was 87 percent, i.e., the portion of the hijackers who fit the profile. In terms of identification ratio, therefore, the effort was quite successful.

As indicated, the airlines really didn't want to use the profile, but when the parachute extortionists became more of a problem, other airlines expressed their interest. The action of the FAA in January 1972, was to require that the profile be used, but it was not required that those who fit the profile be searched. Finally, in August 1972, the FAA required that search itself take place. All who fit the profile had to be

searched as of this date. The cumulative curve of hijackings prior to this was climbing at a rather steep rate, but, as soon as the requirement was established to search all selectees, it flattened out. There were a few more hijackings after the search requirement was established including three gang hijackings, but, when law enforcement personnel were at the boarding gate to search those who fit the profile, the primary step had been taken to solve the problem.

FAA and industry engineers designed the metal detector and manufacturers were soon producing detectors in sufficient quantity. As of January 1973, it was required that they be available at the boarding gates, a requirement, therefore, for a 100 percent search of all those who board our scheduled domestic air carriers. Finally x-ray equipment was required for searching carry-on baggage/luggage as an additional means for keeping weapons off the aircraft.

Dr. Dailey gave me two assignments when I joined the FAA in February 1971. One of them was to evolve more profiles; the other was to evolve operational tactics for flight personnel to use for those hijackers or other suspect individuals who do get on board the aircraft, as we didn't expect to stop everybody at the boarding gate.

As was stated earlier with respect to the gathering of information, files were established and we continued to collect information on every hijacking, not just domestic but international as well. We went back to those files and gathered all of the hijackings up to and including 1970. For available domestic hijacking, to oversimplify, those cases in which the hijacker won were placed in one stack; those cases in which the defensive people were successful in defeating the hijacker were placed in another stack. Then, using an analytical procedure somewhat similar to war gaming, the behaviors of the crew that led to stopping the hijacker were identified. However, the criterion was not supposed to be stopping a hijacker since the FAA's mission is to increase safety of flight for all involved. Thus, using the criterion of safety of flight, the behaviors and tactics that were used to stop hijackers could be sorted out.

A simple example is to obtain the release of the passengers on board. This would increase safety for them, a good behavior as contrasted to taking off with a degraded aircraft, with maintenance problems on the aircraft or an injured crew. The latter would be wrong and unsafe practices.

These tactics were given titles to describe their general content with examples from these past hijackings selected to show any student how past crews had used them successfully. These were, therefore, operationally tested tactics. Though these tactics were readily available in early 1971, again, the airlines weren't ready to use them. The training of crews was and still is costly. For cockpit personnel, it's roughly about $75 an hour per crew for training, paid for by the airlines. Also at that time Red Skelton and others were still treating hijacking as a lark: "It's a free ride to Cuba, a little vacation." That was the atmosphere; the airlines were not ready yet to train their personnel in ways to stop hijacking.

In early summer of 1971 a command center was created at headquarters FAA to help those who were hijacked as they were willing to accept help during the hijacking itself. At that moment in time, they would listen to us and we could have direct contact by way of our air traffic control centers, direct contact with the cockpit of the aircraft.

The center was set up much like a volunteer fire department. We were all on call to go down and help during the hijacking, daytime, nighttime, or on weekends. Management of the command center was assigned to our security people. Air Transportation Security was the title given to our group. The group was an available, interdisciplinary team including public relations/information people who manned the telephones when newsmen might call and ask about the hijacking, and persons who knew the specific kind of aircraft involved, its range, performance capabilities and maintenance requirements and capabilities. The group had operational experts, electrical engineers, bomb demolition expertise, if such a hazard existed, and medical

people. As a behavioral type, I was a participating member of the team from the tactical background standpoint as I knew what had happened in prior hijackings and how it might be applied.

One of the functions of our group was coordination. From a legal point of view, the airline was the parent of the kidnapped child and the aircraft was the kidnapped child. The FBI was in charge when the aircraft was on the ground, so it was part of our network. DOD provided chase aircraft if we had a parachute extortionist or assisted if the aircraft got out of range of our ground-based radar. The State Department was involved as well, if the plane was headed for a foreign land. There had to be communication among the embassies. The group fielded questions from the news media and proceeded to communicate with the cockpit of the hijacked aircraft. This worked only to a degree, for if the hijacker was in the cockpit of the aircraft, we certainly couldn't get too far.

Our real need was to train the crews so they knew prior to that moment of stress how to treat this emergency and what to do. Finally, one of our U.S. carriers, an international carrier, asked us, in the fall of 1971, if we'd train their crews for them. Then, one week before our scheduled date to appear and help them train their crews, a ticket agent in Portland sold a ticket to a passenger by the name of D.B. Cooper—they lost $200,000. This was just a week before training was to start; this certainly motivated them to pursue that which they had wanted, the training program.

The airline didn't have boarding gate defenses yet but they were willing to train their flight personnel. Since they wanted training to take place simultaneously at two points 1,500 miles apart, the tactics were placed on videotape. A team was sent to each of the locations. The team used the videotape for the the structured portion of the program but also responded to the questions that were asked by the personnel. These questions were then used in recorded form to upgrade our training program.

Their personnel were interviewed as soon as they completed the training program. One of their Captains, during the first week after the D.B. Cooper affair, said that too much had been thrown to him in a short period of time but that his team would be ready. They were hijacked not more than 2 weeks after training had taken place. Their parachute extortionist wanted $300,000; they stopped him. So, it was almost like a straight man in a shill operation from an outsider's point of view—without training they lost $200,000; with training they saved $300,000.

This got the rest of the airlines interested in the training program. Videotape training programs were delivered and conducted for our major airlines. Stewardesses responded to this program by complaining that there wasn't anything oriented toward cabin tactics. There were plenty of data available to warrant separating cabin tactics from cockpit tactics and to put the cabin tactics on 35 mm slides and tape cassettes for many airlines. We distributed them as quickly as we could to all U.S. air carriers and these tactics became a required part of their emergency flight training. We also distributed them to other government agencies as needed and, at present, to some 40 or 50 foreign air carriers.

What was the success of the training program? It can be seen in figure 1 that the number of defeats of those who were attempting the hijacking increased considerably in 1971 (summer) as the command center had been created, the training programs distributed, and as the FBI participated actively in stopping those hijackers who did get on board. The defeated curve dropped down to virtually none as the number of hijackings dropped in similar fashion.

In a more detailed sense, one of the first acts of the FAA task force formed back in 1968 was to start a vigorous campaign to discourage potential hijackers from trying to hijack an aircraft. This was accomplished in two ways. First, posters were evolved to communicate to potential hijackers that such acts are illegal and to describe potential punishments that could be invoked for attempting to hijack an aircraft. These posters were placed in all of our passenger terminals. Second, a vigorous campaign was

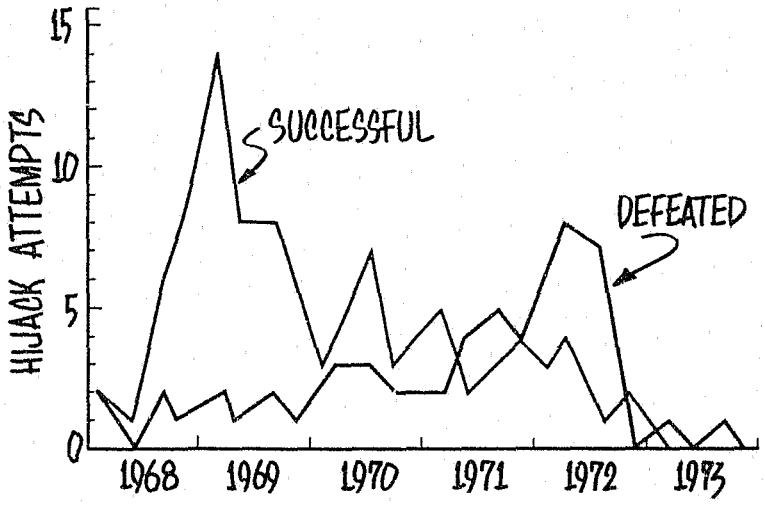


FIGURE 1. *Domestic hijackings by quarter-year.*

undertaken in the newspapers to describe what happened to those hijackers who went to Cuba (Castro was generally not very happy with them). It appears that, as a function of these actions, there was a considerable drop in the number of attempted hijackings in 1969-70.

The government's hijacking program has been called a thicket of obstacles. The first step was to try to convince potential hijackers not to play the game—to never appear at a boarding gate. The next step was the boarding screen; many potential hijackers were being stopped at the boarding gate during those early stages. If they got through the boarding gate, then we hoped to stop them in the cabin (about half of those who did get on board were being stopped in the cabin). For those who still got through to the cockpit, the hope was that they could be stopped by the cockpit crew so that the FBI and others wouldn't have to become involved. But a few still did succeed in reaching their destination. Other steps had to be and were taken very successfully to stop the hijackers. Work is presently continuing toward improvement of this program and increasing its usefulness.

A request has been made to provide some detail on the methodology used to create our profiles. After listening to the first presentation, most people here should be familiar with most of the techniques of profiling. However, starting with an oversimplification, the concept is simply to compare good guys to bad guys. To make it more complex, all available information is used to identify whatever the distinguishable differences between these two groups might be; those distinguishable differences then form the basis of the profile. This profile is then used to identify other potential bad guys before they misbehave (commit the crime).

My first introduction to this comparative kind of a game was about 30 years ago when I helped develop a differential aptitude battery for assigning airmen to technical school. At that time, the Air Force had been created, and one of the tests in the experimental battery was called a biographical inventory. The inventory for airmen contained a multitude of questions about their past experiences. Since the Army General Classification Test (AGCT) was still the means of assigning individuals to technical schools, personnel were followed through school. Their scores on these differential aptitude tests were observed and their response to questions on the biographical inventory were recorded for comparative analysis.

Items that related to success in each school such as jet engine mechanics were identified in this biographical inventory. They were later used in a composite for

selecting future candidates for aircraft and engine mechanic school or other similar technical schools. To relate this back to the preboard screening problem, a taxonomy has been created. It is a classification system which describes the nation's air travelers.

It's rather complex, but we have a variety of air travelers. During the week, businessmen are generally doing the traveling; our weekends are for pleasure. Furthermore, the kind of traveler on a short commuter flight from Washington National to LaGuardia generally is different from one who travels from Las Vegas to Hollywood/Burbank; yet the flights are of similar length. In Alaska, where surface travel generally is hard to find, most who are air travelers include those who would ride buses in Nebraska. The taxonomy is, therefore, our biographical inventory. Using it, a variety of profiles can be provided, profiles to sort out just the good guys or those who resemble our past hijackers. The profiles are not misused; they are not biased toward any particular sex, religion or race; they've been so tested in the courts. They are designed and used only to help provide safe travel for the general public.

DISCUSSION

Question: Did you ever examine your media treatment of hijackings; the amount of attention a hijacking incident receives; the quality or the characteristics of it; perhaps, feedback from the hijacker himself if he had seen similar incidents?

MR. PICKREL: While examples could be provided, this is not the appropriate time.

MR. HERB LEEDY, U.S. Army: How were the profile data obtained?

MR. PICKREL: By sitting at the boarding gate with videotape equipment and gathering all available information.

MR. KRAMER: This probably involved unobtrusive observation.

Question: You do have questionnaires on some of your flights. I've filled out some of them myself, rather detailed questionnaires, voluntarily.

MR. PICKREL: Those were airline specific, but that's another source.

Question: Don't they feed back into the FAA?

MR. PICKREL: When they are asked for.

Question: With respect to developing profiles in your analysis, did any day of the week stand out?

MR. PICKREL: For a long period of time the parachute extortionist was seeking gold just like a '49-er. He wanted to return back to the place he came from. At that moment and for that group, Friday was a very popular time. They would hope that, as they left work Friday, they could accomplish this act and go back to work Monday. For other groups and types of hijackers the day of the week would not make much difference, but it did for this group.

Question: Did the airlines take this into consideration?

MR. PICKREL: Yes, we had our key cities and established the effect. The question is how responsive can you be at that moment in time?

Question: Has any thought been given as to how long the present procedures will remain in force, or have they become a way of life?

MR. PICKREL: Three years ago, it seemed unnecessary to pursue our use of metal detectors and x-ray equipment any further. At that time, when the idea was tossed out as a "feeler" in the trade journals, the editorial pages of newspapers all came out saying: you got something that works, keep it; we did. The procedures and equipment don't cause slippage of flight schedules. They are established and working now. With a similar attitude from the general public, our intent is to continue.

MR. JOHN HAVEN: One of the recommendations that was turned in by Dr. Reighard's task force was that, as long as carry-on baggage is permitted to go through the gate using metal detectors, the program would not succeed. Why did it take so long to implement active searching of passenger carry-on luggage?

MR. PICKREL: Whatever is done affects the general public. Certainly the general public had to accept it and the airline didn't want to lose passengers. They could have had their electronic game by using evolving x-ray equipment, which could damage film while still permitting that kind of passive screening. All of these factors are involved. It's not a binary issue—now it does or doesn't work. It's those things that do work and how you can enforce them.

MR. KRAMER: Hasn't the same approach been utilized developing profiles for the airport bombing threat, actualized in New York recently?

MR. PICKREL: Much of the burden falls on three specialties, using a

multidisciplinary approach. I'm actively engaged, the FBI is, and others with a security background are as well.

Question: Didn't they recently, at National Airport, instigate x-raying of checked baggage? They said they were going to begin the program at five major airports in the United States.

MR. PICKREL: The answer, although it isn't a direct answer, is that there now is 100 percent screening of all checked baggage. As to how that screening is accomplished and what portion of it involves x-ray equipment, a trial has started at those airports to look at the application of x-ray equipment which does not differ substantially from the equipment you are familiar with in the carry-on luggage area. Equipment availability and need are being looked at now.

PERPETRATOR ATTRIBUTES IN THREAT ANALYSIS

Allan Fine

Sandia Laboratories, Albuquerque, NM 87115

INTRODUCTION

Sandia has a study contract with the RAND Corporation in which the attributes of potential threat perpetrators to nuclear facilities or materials are to be determined. This paper describes the current status of this work.

Sandia Laboratories is a prime contractor to the Energy Research and Development Administration in the field of nuclear weapon research and development. In this work, Sandia has gained experience in the areas of weapon command and control and in protective technology applicable to weapons programs. Experience in these areas led to Sandia having a major role in the field of physical protection and nuclear safeguards. This task involves the study, research, and development of physical protection elements and systems applicable to the protection of nuclear facilities and materials. Both fixed-site facilities and transportation methods fall within the purview of this task. The effort also includes the need to develop concepts applicable to new protection systems and to find means to assess capability and adequacy of existing and proposed systems. Sandia's goal is to achieve a balance in the use of personnel and technology in order to optimize protection. In-depth protection, another part of the objective, can be attained by the proper combination of barriers, sensors, alarms, people, and procedures.

In discharging the Sandia responsibility for evaluating current and proposed protection systems, new methodology is required to provide a means to assess various aspects of the systems. Several analytical techniques are under development. One method used to provide insights into protection system relative effectiveness involves computer simulation which, in turn, requires attribute specification for potential adversaries and for existing or proposed defensive system parameters. Definitions of various element capabilities such as barrier delay times, alarm functional probabilities, sensor successes and false alarm rates, and various personnel responses are needed as input to the model. In addition, detailed attributes of adversaries in terms of armament, training, dedication, transportation, and other such task-specific areas of interest are also needed as model input data.

Fortunately, there have been very few incidents in the world involving threats or attacks against nuclear facilities or materials. This precludes accumulating an extensive data base of adversary attributes containing information from nuclear-related incidents. However, we would prefer to have a data base for adversary attributes based on historically accurate incidents taken from realistic episodes of adversary action. It has become necessary, therefore, to achieve a data base by looking to alternative sources of incidents which could be transferred as potential threats to nuclear programs as analogs.

STUDY APPROACH

Sandia has contracted with the RAND Corporation to research and prepare a data base of analog incidents applicable to potential threats to nuclear programs. Brian Jenkins is RAND's principal investigator for this task. The basic tasks of the RAND work are to: 1) Determine a set of attributes of potential threats (see fig. 1) (covering a spectrum of threat models to nuclear programs by using analog incidents as data

sources), 2) accumulate a data base of incidents, and 3) estimate target attractiveness and relative likelihood of attacks over the threat spectrum derived from the data base. There is no intention to develop a probability model or to pattern this "soft science" study after the probabilistic type of study such as the reactor safety study headed by Prof. Rasmussen. We do expect some ranking of targets, threats, and combined likelihoods of attacks but on a relative, rather than an absolute, scale.

The data base for the RAND work covers a variety of incidents ranging from criminal activities to international terrorist attacks. To assimilate the wide variety of information types in the data base, RAND has accumulated a team possessing multidisciplinary skills of data collection, interpretation, and analysis. Both physical and behavioral sciences are represented on this team which includes persons in fields such as history, mathematics, physics, political science, psychology, psychiatry, and military intelligence.

The adversary attribute data will serve as input of the assessment techniques being developed at Sandia. In the simulation model mentioned earlier, the model pits an external attack force against a facility defense system with the adversary attribute data being an input. Relative vulnerability of a facility under varying conditions of both adversary and defense system characteristics is an output. This is one of several assessment techniques which utilize Monte Carlo computer simulation to provide a series of results from adversary-defense confrontations for relative values of facility vulnerability. The adversary attribute data base will be used to permit us to define mean values and limits of specific attributes for our simulation efforts. We recognize that computer simulation does not completely represent the real world and that difficulties do exist. Our use of this simulation technique is intended to yield insights, on a relative basis, into how changes in both adversary and defense attributes and characteristics affect the design of security systems. We plan to exploit promising avenues revealed in the design considerations of future systems.

Data base lacking
- Nuclear attacks rare
- Need alternate source of data base
- Desire historical record for data base

Rand study contract
- Objectives: To describe a spectrum of potential representative threats to nuclear facilities
  To acquire a data base of representative threats
  To estimate comparative likelihood of attack occurrence for each type of representative threat within the spectrum of threats
  Not Rasmussen study of probabilities
- Approach: Identify analogous incidents to be used as potential threats
  Collect detailed information on incidents found
  Classify perpetrators
  Use multidiscipline team to analyze data
  Break out categories of perpetrator attributes

FIGURE 1. *Adversary attributes*

ANALOGS

To acquire the adversary attribute input data for effectiveness evaluation, the RAND study covers the types of events shown in figure 2. A brief description of each of the analogs follows.

The first item shown is not really an analog; rather, it represents a compilation of actual incidents against civilian or military nuclear facilities or the illicit use of nuclear materials. There have been very few of these incidents, but those which have been documented are included in our list for completeness. This list includes such events as the raid against the Atucha reactor in Argentina, two attacks against French reactors, and the dispersal of a radioisotope throughout a European railway train. None of the attacks against reactors led to the release of radioactive material or to any public hazard.

The first type of analog in our listing is the accumulation of data regarding historical, non-war events in which the production of large numbers of casualties was an objective. The analog here is the threatened use of a nuclear explosive device, either stolen or fabricated from stolen material. There are not many of these incidents for our consideration; a search back to the turn of the century has revealed very few incidents which would be usable as "modern" data for our analog record. The LOD airport massacre is one of the few recent examples of this analog. In order to have any reasonable compilation for analogs of this category, it was necessary to reduce the number of casualties in the "large" category from around 100 to about 25.

Large scale extortion in which mass hostages are seized or use of weapons is threatened in another analog category. The example of the skyjacking of four passenger jet aircraft to Jordan, the threat of death for hundreds of passengers, and the subsequent destruction of the aircraft is an example of the use of extortion as an analog of interest to our study.

Sabotage of facilities—particularly industrial sabotage—is an analog which could be extended from conventional industry to the nuclear industry. Work in this area has just begun so there are few items to report for this analog category. However, this analog links closely to a similar one involving symbolic destruction. The analog of symbolic destruction represents a relatively low level nuclear threat although such threats or actions could lead to adverse circumstances for specific installations. An example of this type of incident is the 1974-1975 power line tower destruction in northwestern United States. The symbolic destruction analog is that of potential opposition to nuclear programs, whether the programs relate to weapons or power.

- Direct nuclear incidents
  - Few known incidents
  - Threats against nuclear facilities (or penetration)
  - Threats involving nuclear material use
- Large number of casualties (weapon use/radiologic
  - LOD Airport massacre
  - Search back to 1900
- Large scale extortion (mass hostages—threat of weapon use)
  - Hijacking of aircraft (Jordan)
  - Hostages involved in one-fifth of international terrorist activities
- Sabotage (facility disablement, shut-down)
  - Labor strife
  - Environmental
- Symbolic destruction (opposition to society, the establishment, nuclear programs, etc.)
- Terrorist attacks (threats against nuclear facilities)
- Sophisticated crimes (successful attack; indicators of well-planned operations)

FIGURE 2. *Analogous events (non-war)*

One of the more direct analog threats to nuclear programs is that of terrorist attacks. Although we are primarily interested in the potential for terrorist attack within the United States by indigenous groups, we cannot disregard international or transnational terrorism as analogs, particularly since organization, training, techniques, motivation, and goals can carry over from one set of terrorist organizations to another. The RAND Corporation has done extensive research in the field of terrorism and much of this work can apply to our project.

The last analog event of our study effort is one which has received the initial attention and one for which some detailed information can be provided. This analog concerns burglaries and robberies in the realm of sophisticated crimes. As an analog, this is important because it represents successful actions against high-value targets which are protected by means of some of the same types of elements considered for nuclear protection systems—barriers, alarms, vaults, guards, and response forces. These incidents are considered to be directly transferable to nuclear program concerns from the standpoint of technical skills, but not necessarily from the aspect of motivation.

Before providing details on the work to date in the area of sophisticated crimes, it is necessary to touch on an area of commonality of all the incidents going into our data base. Each candidate item found in the various analog categories, whether it is found in newspaper accounts, books, historical records, or any of the many other sources of data, is examined to determine if it can or should be included in the data base. As a guide to whether or not the item is worthy of continued consideration, a series of questions has been prepared as a "check list" for general application to all potential data base items. This listing is shown in abbreviated form in figure 3. The list covers the major headings of 15 general areas which are of interest to data base items in this study; more detailed questions under each major heading are asked about each item, but the detail is not warranted here. Figure 4 is a subset of the listing shown in figure 3 and was configured as a checklist to aid in coding the data base questions for initial tabulation and analysis.

In order for a candidate incident to be selected for our data base, sufficient detailed information about the incident must be available to provide answers to a substantial number of the questions on our selector listing. Not all questions are relevant nor can they be answered for all incidents; however, we do need answers to most of the questions. We hope to have a total data base of several hundreds of incidents for further analysis.

- Type of incident
- Political, social, economic context
- Perpetrators
- Specific objective or intended outcome of the action
- Intended effects in terms of any broader objectives
- Planning and preparation
- Resources required
- Description of any device used
- Description of target
- Execution of the operation
- Actual results of the operation
- Nature of the threat and any associated demands
- Response to the threat and associated demands
- Consequences of the incident and ultimate fate of the perpetrators and/or their organization
- Publicity and public reaction

FIGURE 3. *Data base questions*

Numbers
- ° Number of people independent of other factors

Equipment
- ° Hand tools
- ° Power Tools
- ° Explosives
- ° Heavy equipment
- ° Specialized

Arms
- ° Small arms
- ° Explosives
- ° Automatic weapons
- ° Tanks

Transport
- ° Foot
- ° Car or truck
- ° Aircraft
- ° Special

Knowledge
- ° Casual
- ° Public research
- ° Criminal
- ° Intelligence and insider

Dedication
- ° Casual
- ° Discomfort
- ° Injury
- ° Loss of life

Training
- ° Planning level
- ° Degree of training
- ° Tactics

FIGURE 4. *Adversary attributes*

SOPHISTICATED CRIME ANALOG

The analog category of sophisticated crimes has more than 40 incidents included as part of the data base. Among the incidents included are the Boston Brinks robbery, the "Great Train Robbery" of Great Britain, and other similar incidents in which high-value materials or cash were the object of a criminal act. The inital source of most of the sophisticated crime basic data was newspaper accounts—chiefly in New York and California newspapers. Follow-up data for application to the list of questions came from a variety of sources such as court records, police interviews, and public accounts of activities. Court records proved to be a valuable source of data. While many crimes have made headlines, recent ones may not have sufficient information regarding planning, execution, motivation, financing, etc. to be of value to our data base. The data accumulation is dynamic and is a continuing area of interest; however, years may be required before sufficient data become available on some promising items. Acquiring data is difficult today in view of laws protecting privacy. This is one reason for using "solved" crimes for our data base so that public and open sources of data are available for scrutiny.

Figure 5 contains summary information regarding 42 incidents of sophisticated crimes which have been analyzed. These incidents are not to be considered as a statistical sample of all serious crimes; however, they are considered as representative of the class of sophisticated crimes applicable to our analog data base.

In figure 5, it is shown that for the incidents analyzed, approximately two-thirds involved four to seven perpetrators. Also, about two-thirds of the listings were burglaries; the remainder concerned robberies and a couple of prison "break-ins." These latter crimes involved attempts to free prisoners and, while the techniques were similar to those of robberies and burglaries, the objectives were obviously different. Highly valued items such as cash and securities accounted for nearly half of our sample incidents. Three-quarters of the incidents occurred in the United States, and the others occurred in either Canada or the United Kingdom.

For the attribute involving the number of perpetrators, detailed investigations revealed that the general rule appeared to be that the right number of people to do the job was the number used. Fewer people could leave part of the tasks uncovered; a surplus of people meant a lesser "split of the loot" for those involved. Also, by limiting the number of people to just those needed, the security of the operation was better maintained.

Number of participants	
1 to 3	24%
4 to 7	64%
8 and more	12%
Types of crimes	
Burglary	62%
Robbery	29%
Other	9%
Targets	
Cash and securities	48%
Jewels and precious metals	19%
Art works	17%
Other	16%
Data base	
United States	76%
Overseas	24%
Total of 42 incidents	
Equipment used	
Special tools	36%
Hand and portable power tools	31%
No tools in evidence	33%
Inside help	
8 cases	19%
Communications	
Commercially available	
Access	
Armed assult (13)	30%
Barrier penetrated (25)	50%
Deception used (5)	12%
Insider (3)	7%
Alarms disabled (15)	36%
Legitimate access (4)	10%
Barrier bypass (10)	24%
Types of weapons used	24%
Handguns	7%
Shotguns	5%
Machine guns	5%
Bombs and grenades	5%
Antitank weapon	50%
No arms apparent	
Casualties	2%
One pistol-whipped employee	
Preparation	
Casing (36 cases; 3 with rehearsal)	86%

FIGURE 5. *Sophisticated crime data.*

The percentages do not add to 100 percent on all attributes. There are some attributes for which more than one answer applies—for example, in some cases access to a target may have been gained by disabling an alarm and also by penetrating barriers.

Equipment used (fig. 5) in these activities (basically burglaries) was about evenly split among special tools, hand and portable power tools, and no obvious use of tools. Special tools included items such as a crew-served anti-tank weapon which was used to blast into a bank vault. The sound of firing 31 rounds was muffled by the use of blankets.

One very interesting and important attribute was the use of inside help. In one-fifth of the incidents studies, there was evidence of some degree of inside help such as door left open, alarms turned off, and similar functions of aid to the overt perpetrators. The one-fifth value is a minimum determined only from those incidents in which such aid was clearly evident. It is believed that more incidents involved inside help, but this is conjecture and not in evidence from the data available for review.

Communications presented no problems to perpetrators of the sophisticated crimes. Where necessary, hard wire lines between "inside" and "lookout" personnel were used. Walkie-talkie radios were in use; often these were stolen items, usually taken from construction sites.

Access, as our adversary attribute, refers to the method(s) perpetrators used to reach the area of their targets. In some instances they entered premises (such as a bank) in legitimate fashion as an apparent customer; sometimes they gained entry through stealth, at other times they either had to disable alarms or use force to enter premises. The percentages shown under the category "ACCESS" in figure 5 add to more than 100. This results from the overlap of access methods when more than one happened to be used in a particular escapade.

In half of the incidents analyzed, no evidence of weapons use was found (fig. 5). The perpetrators may have had weapons but either found no need to use them or had no desire to display them. Handguns were the most prevalent type of armament used. However, the use of shotguns, machine guns, bombs and grenades, and a crew-served anti-tank weapon was noted in the incidents studied.

Little desire to inflict injury was displayed in the sophisticated crimes studied. In only one incident was a victim injured: an employee of a target company was pistol-whipped by the perpetrators.

A substantial degree of preparation and planning was evidenced for the sophisticated crimes. In 86 percent of the incidents covered in this analog attribute, there was direct evidence of casing. In some instances, this was coupled with rehearsal of the plan of attack. Thorough planning was, therefore, a dominant characteristic exhibited by perpetrators of sophisticated crimes.

As a summary of information obtained from the study of sophisticated crimes as analogs to potential threats, the following are preliminary conclusions:

- Violence was avoided whenever possible during the execution of crime.
- Good leadership and organization were generally employed, and ingenuity and a talent for improvisation often existed when the need arose.
- Alarms and signal systems were often successfully bypassed or circumvented by skilled personnel in the criminal team.
- Detailed preparation, including reconnaisance and rehearsal, was typical of this analog category.
- No particular problems arose in acquiring weapons, tools, skilled personnel, or special equipment needed for the execution of the criminal action.
- Diversionary maneuvers were used in several incidents; when used, they were always successful in providing the effect desired by the perpetrators.
- The number of perpetrators rarely exceeded seven.
- The incidents were characterized by having high potential rewards.

- Planning for the incidents stressed thoroughness and low risk for the perpetrators.
- The incidents were not typical of spontaneous crimes of opportunity.

FUTURE ACTIVITIES

We hope to conduct examinations of the other analog incidents similar to those exhibited for the sophisticated crimes analog. The RAND Corporation will continue gathering of data and making analyses in the coming year. If time and funding permit, we hope to investigate some of the psychological aspects of potential nuclear program adversaries as well as study physical attributes of the type discussed here.

DISCUSSION

MR. AL MASON, USAF: The 40 crimes analyzed were mostly burglaries and robberies. Approximately how many were burglaries and how many were robberies? What other crimes are included?

MR. FINE: Sixty percent were burglaries. Break-ins or break-outs of prison, and similar events, in which the target was people rather than objects accounted for about 9 percent.

MR. MASON: Were the cases which were analyzed only the failures, i.e., those in which arrests were made?

MR. FINE: Thus far, these are the only ones for which information is readily available. The obvious limitation is recognized. For example, while preliminary information may be obtained relative to how many people were directly involved in the recent Montreal armored car incident, details of the planning of the incident or involvement of others than the direct perpetrators are not yet known. It appears that a great deal of professional planning was involved. Even though there appears to be a direct connection between this incident and a television program covering this type of crime, shown about a week before the incident, all indications show that planning was started long before the television program was shown. Actual confirmation of proposed theories regarding the planning and execution of the incident may require the apprehension and trial (and conviction) of the perpetrators before details are available.

Question: It appears that this study is limited to domestic cases. Is that correct?

MR. FINE: No. For example, nearly 25 percent of the crimes in our analog sample were committed outside the U.S.; Canada, and the U.K. were the main outside sources of data. There is enough crosscorrelation from these non-U.S. sources to provide useful information.

Question: The question was asked because one is prohibited from dealing with drug cases unless access to non-domestic sources is available and granted.

MR. FINE: That certainly could be part of the reason for drug case omission. While they weren't omitted for any overt reason, information availability may have been a factor. Also, the resources of the program are not unlimited. Much of the funding goes for data collection and that is a complex part of the problem. Newspaper reports for initial listings of potentially applicable incidents are heavily relied upon, as well as cross references in open publications. Some of these, as well as personal contacts of the investigators, often dry up or turn out to be dead ends. Data gathering for a meaningful data base is a difficult problem but certainly not insurmountable.

Question: What proportion of the total crimes of this kind does the sample represent?

MR. FINE: I don't have an answer to that. We do not know the total number of crimes committed during the period covered by this analog. However, sophisticated crimes as an analog should cover 10 to 15 percent of our entire data base of all analog events of 400 to 500 incidents.

Question: What is the proportion of unsuccessful to successful events? Over the time period that 40 unsuccessful instances were collected, how many total incidents were there?

MR. FINE: At this time, the question can't be answered. The sample used represents the more spectacular or publicized crimes written up in east and west coast newspapers. We have no idea how many others were committed which did not fall into our investigator's purview. When considering a worldwide arena, the question will probably never have an answer.

Question: Is this enterprise promising or not?

MR. FINE: We believe it is, although we must wait for a full data base analysis before we can answer the question with any degree of assurance.

MR. RAY MOORE, NBS: Is the Sandia simulation model the same as, or in addition to, the air base defense model also used out at Sandia?

MR. FINE: Are you referring to the BISS (Base Installation Site Security) program?

MR. MOORE: Yes.

MR. FINE: There's commonality, but perhaps my colleagues here can give you more specific answers to your question.

The simulation program is applicable to general confrontations between defense and adversaries so BISS work can be applied if definitions of the system elements are made compatible with the needs of the simulation program.

I would like to re-emphasize that several of the analytical techniques under development at Sandia are used to assess *relative* vulnerability of fixed-site security systems. These models are, primarily, design tools which have as their principal virtue the capability of providing quantitative results for comparing alternate physical security systems. It must be, and is, recognized that the calculated measures of system performance from these tools and techniques are not absolute. However, they do provide useful information and guidance which can be used in judging the adequacy of a physical system.

MR. MARVIN BEASLEY, DNA: Are you soliciting inputs from any of the group attending today relative to known cases that Sandia may or may not be aware of and, in turn, will your slides be made available for inclusion in the proceedings? Where should the solicited case information be sent?

MR. FINE: Please forward such information to me. If anyone here today has any cases believed to be of interest we would be happy to hear about them. We have to judge incidents by the amount of information we can discern from our list of questions. While many questions on our list are not applicable to all incidents, we prefer to have incidents in which as many as possible of the questions can be answered by available hard data.

Question: Do any of the burglaries or robberies include incidents involving DOD weapons armories or facilities?

MR. FINE: As best as I can recall, no. Perhaps some of these may show up in updated listings but they have not yet been included. Possibly, their omission indicates that the crimes have not been solved.

Question: Would they be interesting in terms of analogy?

MR. FINE: That's a very good point; have the perpetrators been caught yet?

Reply: For the incident, all the people have been apprehended. One insider and an outside professional stole the weapons. The individuals involved in the incident last week and the one the other night haven't been caught yet.

MR. FINE: At the time the tabulations for our analog incidents had been made, some 7 months ago, these events were not included.

MR. BEASLEY: Is there some reason for omitting the targeting of the drug factors, that is, the smuggling incidents? There's some commonality in the methodology in planning and carrying out these crimes. Some of these very important crimes have been broken and they may be quite useful in Sandia's study.

MR. FINE: It was not intentional. The cases included were those for which sufficient detailed information was available from which good inferences could be derived. There was no direct reason for excluding the case of drug thefts. The incidents used are generally high-payoff crimes; some of the drug thefts may be high-payoff, others may not be.

MR. BEASLEY: Some of the attendees have such closed cases. They could be made available and would be quite applicable within the threat spectrum of Sandia's program. Is there interest in such cases?

MR. FINE: My first inclination is that there is interest, although it could be qualified because I'm not certain how the information from such cases could or would be fed into or relate to the program.

PROFILES OF COMPUTER CRIMINALS

Susan Nycum

Chickering and Gregory, San Francisco, CA 84104

In computer abuse, the perpetrators tend to shy away from violence. In 375 cases of computer abuse only one was found in which there was a loss of life, and that was peripheral. A leading university's computer center was blown up several years ago and an innocent researcher's life was taken. The perpetrators of computer abuse are more typical of white collar criminals, who do not usually get involved with physical confrontation.

Computer abuse can be defined as those acts in which there has been an incident involving the computer in which a perpetrator did or could have received a gain and/or a victim could have or did suffer a loss. In certain of these situations, particularly those involving sabotage, the gain to the perpetrator isn't at all clear unless one gets inside his/her mind. The perpetrator may have gotten some sort of kick from what was done, but there was no monetary advantage.

The data base of 375 incidents, while trivial compared to all the incidents of general white collar crime, can be classified as follows: (1) abuse to computers themselves, hardware and systems, (2) abuse to the assets which happen to be stored in the computer such as the programs and data, either proprietary programs, data constrained by the Privacy Act of 1974, or other personalized information, (3) the computer itself as the perpetrating device, and (4) the computer as a symbol. In the last classification, the computer may or may not really be involved, but it has served as the symbol of the abuse.

While the number of cases is small, it is the opinion of many including ourselves that they represent the tip of an enormous iceberg, because most of the exposures have come about by accident. Based on this feeling one can wonder how many other incidents are going on. It has been suggested that we may have uncovered about 15 percent of the total number of actual acts involving computer abuse. While a percentage cannot be calculated without knowing the total sample size, this guess is offered in the spirit of stimulating the development of more definitive data.

At this point, it seems worthwhile to elaborate somewhat on the types of incidents of computer abuse which have occurred to gain a better understanding of and appreciation for the problems and how they might relate to situations in your own area, where a need for designing and implementing improved physical security has been or can be identified.

In terms of abuse to computers themselves, there have been several cases in which disgruntled individuals have fired either shotguns or handguns at the computer. For the individual, these actions have only contributed to a release of tension. These acts have accomplished a great deal more in terms of putting the computer out of commission until the responsible parties have been able to replace it. An even more bizarre and devastating type of behavior has been the firebombing of computers. This was carried to the extreme in Wisconsin by taking the computer hostage to bring the institution to its knees. The nerve center of the institution thus became under the direct control of the perpetrators. Since the early 1970's, the student population has seemed to calm down with respect to their unhappiness with the establishment and, for the most part, these actions haven't continued. It now appears that a few others have gotten the same idea. On occasion, a rival will sometimes blow up a competitor's computer. This

happened in Los Angeles about a year ago and the proceeding was followed through the trial. Therefore, these actions still occur, although for different reasons than in the past.

Hardware is one problem; systems software is a different one. In this instance, the computer is left unscathed, but the operating system is somehow compromised. This category of system abuse generally includes such actions as system oversaturation in which excessive data input has overloaded the system to the point where no useful work can be done. In one instance, someone gained control of certain system commands by means of a telephone connection and was in the process of erasing the volume table of contents. We were able to catch the individual in time, saving at least $50,000 in replacement costs. The local sheriff and telephone company were called to determine legal recourse. The answer was that an obscene or harrassing telephone call had been placed, a misdemeanor in that state. This is something that lawyers refer to as cold comfort, but very illustrative.

In a similar example, some disgruntled customer engineers had sabotaged a customer's data center by the following means. The central site of an insurance company had the host computer. At all the branch offices there were terminals which collected all the information during the day. At night, the host computer would poll them via telephone lines. The terminals responded by sending the information across the lines. The engineers obtained the sequence that initiated the polling. By first using just a pay phone and later using more sophisticated techniques, they called these various stations at random and had the initiation sequence started, without having the host computer listen at the other end. When the real computer called, no data were transferred because the terminal tapes had been unwound. This continued over a period of several months, with both the customer and the computer vendor spending a great deal of money trying to determine who the perpetrators were and why they did it. The laws in that state are such that we again have the case of the obscene or harrassing, but expensive telephone call.

The second area of abuse to the assets in the computer concerns theft of trade secrets or software. There is also a separate issue here involving the people who are concerned about protecting patents, trademarks, copyrights and the like from the legal point of view. There is the technical issue of how to protect this sort of material from being taken in the first place, as this appears to be one of the more exciting areas for the commercially useful but he/she is also spared all development costs.

One can literally get rich overnight. In a case recently settled in Chicago, they were fortunately able to prove that the perpetrator had been sufficiently unclever by copying everything such that if the tapes were held up to the light, they would match precisely. The judge had no difficulty seeing what had transpired. With a little more cleverness, the potential for gain is great.

Within the privacy area, particularly at the federal level now, there is concern for loss of data which is personal information. Government agencies are responsible for ensuring that such information and data do not fall into the wrong hands. The possibility of penetration to get such data is also viewed as computer abuse.

Use of the computer as a perpetrating device is fascinating. One of the computer criminals who showed up in the profile didn't use the computer at all to steal. Instead, he modeled his thefts from the company involved so that he would be sure that he would get just the right amounts of money which wouldn't cause an exception report to be printed or an alarm bell to go off. He was so successful that he finally had to get himself caught in order to get out of it. He had made enough money; but didn't have a way of terminating the activity. He wanted to retire. While perpetrator profiles will be discussed shortly, these individuals are not dull.

The last area in which the computer is used as a symbol amounts to only about 9 percent of the total number of cases. Examples include the computer dating bureaus popular several years ago, where you'd find the answer to your prayers; going

to a computer school for four months to guarantee getting a high paying job; bills produced by computers are always correct because computers don't make mistakes; the inevitability of computer predictions such as going out of business in so many years because the computer so predicts. There are a host of other political or policy uses of computers which seem to be symbolic, even though the computers themselves may not be involved at all.

Who are the perpetrators of computer abuse and what are they like? While the sample is small and sophisticated analysis has not been undertaken, such analysis should be done by individuals skilled in appropriate techniques and methods.

We have talked with the computer perpetrators who have been identified. On occasion, even though it is certain that the act took place, the individual(s) may not be available. Yesterday, only the lawyer and victim were available because the perpetrator had fled to Canada. In 15 cases we've talked with the perpetrators, some for as long as 20 hours at a stretch. The word "stretch" is used advisedly because sometimes they had to be visited at non-appealing locations such as federal and state penal institutions. In any event, a lot of time has been spent talking with these individuals about their motivation as well as making empirical observations concerning what they did to determine whether they are different from other white collar criminals.

The first thing noticed was their age; they are younger than most white collar criminals. They tend to vary from 18 to as high as 46, but with a mean age of 29. In fact, one of the most successful, who now has a computer security business, is still under 25.

Their skill level is usually very high. They are mostly computer programmers who have formal education in some cases, but in all cases they seem to have a high intelligence quotient. There is a close relationship between what they do for a living and what they do for criminal reasons. All but one of the perpetrators committed the crime while in the course of their employment. This one was the individual who, as an outsider, successfully impersonated telephone company employees for a profit of about $1 million. At the time he was 20 years old and a part-time college student, but he successfully performed an incredibly sophisticated con job. Although he knew the technology, he actually demonstrated on television last year how to break a computer system without knowing anything about the technology. He simply cajoled a young woman on the other end of the phone line into giving him the information he wanted. This and similar instances can be represented by a concept called "steel doors and paper windows" in which highly sophisticated technical restraints are in place, yet the person who answers the telephone may be convinced that the caller has a right to know certain information just because he/she is displayed as being the type of person who should get it.

The modus operandi also includes perpetrators who both use the computer the way it was designed to be used and also play with the input-output materials. The biggest example of this was the equity funding case in which false insurance policies were created and those policy numbers were put into the computer, resulting in a profit of $2 billion. The computer program was just designed to keep control of the numbers; the perpetrators changed those numbers. Another example is the case of a keypunch operator who was responsible for inputting all the traffic tickets from her own small town. She decided to leave out her friends' traffic tickets. Therefore, it is not necessary to be a major crook to perform such acts. It is sometimes just a nice person who ends up being fired.

In contrast, there are people who steal software and misuse the passwords of a legitimate user. At the very sophisticated level, computer control is achieved by covert program alteration; it is extremely difficult to catch these individuals.

Mr. Fine of Sandia indicated earlier that as many as seven individuals are typically involved in sophisticated crime incidents. While collusion is very high in

computer abuse, groups as large as seven have not been found outside of Equity Funding. Computer abuse frequently requires more than one individual because a combination of knowledge, skill and access are needed. Modern computer systems are such that it is extremely difficult for one person to perpetrate an act successfully. Sometimes only one insider is required, but an outsider may also be needed, someone who can draw money out of an account. An insider manages to put all the money into one bank account, but he/she can't be seen taking the money out.

From discussions with the perpetrators, the reasons for committing acts of computer abuse appear to be largely personal gain, with profits ranging from about $1,400 to as high as a million and a half. The benefits may accrue over a period of time, such as a year or a year and a half until the perpetrator is caught or voluntarily stops and tells someone what has been done.

Other reasons include the "I'm going to show them" type of situation, characterized by people who are disgruntled for one reason or another. A differential association syndrome is at work here and is generally typical of white collar crime; i.e., from the viewpoint of society, there is very little difference between what these people do rightfully and how they twist it ever so slightly to be wrong. There is also the Robin Hood syndrome. A lot of these people wouldn't take your wallet if they found it lying on the floor, but they think nothing of taking a million dollars from the telephone company. The attitude is that there is nothing immoral about stealing from either a huge organization or from a machine, which, if placed in front of a huge organization, removes all moral compunctions whatsoever. But while these individuals take from the rich, they have yet to be observed giving to the poor.

There is also the game playing idea. It's neat to see how well one can beat the "infallible" computer. Some of these people just enjoy beating the machine; it's like a chess game for them. They will often leave notes saying they've done it. Some of them will actually confess if they are not caught fast enough.

In terms of the disposition of these people, nine of the people interviewed received felony convictions for this crime. This is fascinating from the legal point of view. Many fit into the normal process; one was hired by the victim, and this represents the spread of what has gone on. Interestingly enough, only one had ever had a prior conviction, and that was for a youthful marijuana episode.

In one situation everybody thought the perpetrator was a nice guy including the prosecutors, investigators and jailers. Everybody liked him, but he was sentenced. A hardened criminal who had seen him perpetrate the act and had said at that point, "You've got an accomplice now," for some odd reason, got off completely. No one was ever able to figure out why.

With respect to personal characteristics, these individuals don't like to get caught. They are white collar criminals who are in great fear of being discovered. Other than that, their backgrounds and the like are similar to yours and mine. Most of them are bright, very highly skilled men.

It is important to know that this situation is permitted to exist essentially due to functional vulnerabilities and vulnerabilities of particular places. Most of the acts take place at the input-output phase of data. There are problems here and in other functional areas associated with a lack of separation of functions and a lack of double supervision functions.

Sometimes there is a lower level person being supervised by a crook who has a greater amount of access. The separation of functions didn't exist at that higher level, even though it existed perhaps at the lower level.

There has been a tradition in the computer area of people walking freely back and forth. If one separates all the employee functions, who are left to walk back and forth? Janitorial types may possibly get the best information out of the wastebasket. In fact, this is what the telephone company impersonator did. Vendor personnel who repair

machines and do other sorts of checking back and forth may go from your site to nother site. They may represent the most marvelous company in the world, but may be personally corrupt. They may be on the payroll of one of your competitors. So, it can be the old English mystery in which nobody noticed the postman or the butler. It isn't always your own easily identifiable employees or the outsider who obviously doesn't belong there. It may be just this invisible person that should be watched for.

It is also necessary to have physical and technical access restrictions. Access to software, terminals and communication devices should be controlled with appropriate provision of audit trails so that if something does happen, the event can be reconstructed very quickly to see who was involved, how the act was perpetrated, and at what time.

It has been observed that physical security in the sense of access to the door of the computer/machine room is generally poor. Many times I have seen someone in a machine room who didn't belong there. Because the person acted like he/she belonged there, the operator or other individual in charge did not question him/her. If the person is warned, vigilance will probably last a day and a half to a week, and then that natural tendency to not question the person who appears to have authority steps in again.

The manager of security at IBM ran a study of badges with pictures on them. The best person payed attention to 400 badges in a period of a day, but most people could not pay attention to more than about 200 badges.

There has also been concern about computer terminal operating procedures. There is a requirement for backup, which may or may not be true in other areas. With backup it is possible to replicate the situation should any loss occur.

There is a weakness in business ethics in this area. There seem to be two things that can go wrong. First, the general business ethic may be very lax. One perpetrator had been corrupted because he saw everybody else in this large corporation stealing; he finally decided to steal as well. Second, there is the "peninsula ethic" which affirms that computer programmers think that there is absolutely nothing wrong with taking someone else's software program because the program is viewed as being in the public domain or crashing another person's system to see how it works because this is something called reverse engineering. Aided by the attitude of many grade and high schools to encourage children to learn as much as they can, real problems are posed by sharing passwords and getting their father's passwords onto somebody else's machine. Such attitudes do not foster the development of moral responsibility at early ages.

It is recommended that the level of the ethical standards be raised both in computer technology and in our educational institutions. Particular attention should be given to control functions, proper use of programs and access to time sharing systems. The impact of time sharing systems is becoming more widespread with the development and expanded implementation of electronic funds and international transfer systems. Simple procedures such as keeping magnetic tapes well-labeled and sequestered can be quite effective.

Finally, based on what is known about computer criminals, a major effort should be undertaken to remove temptation. If such acts can't be performed conveniently, and if the individuals are kept reasonably happy in their jobs, a lot may be accomplished at a reasonably low price. From a technical standpoint, it is far better to start with the things that can be afforded, perhaps sacrificing costly sophistication to avoid situations like designing an impregnable front door without considering that the back door only takes 30 minutes to get through.

SOME HUMAN FACTORS THAT INFLUENCE RELIABILITY OF SIGNAL DETECTION AND IDENTIFICATION IN SURVEILLANCE SYSTEMS

Dr. Robert Mackie

Human Factors Research, Inc., Goleta, CA 93017 93017

The purpose of this paper is to describe some human capabilities and limitations that significantly influence the overall performance of surveillance systems. First, factors that influence the ability of human operators to maintain high levels of attention for critical signals or events that may occur very infrequently or unexpectedly will be discussed. This is the area of human behavior generally known as vigilance. Second, consideration will be given to some of the factors associated with signal interpretation where the recognition of characteristics that differentiate a signal of interest from system noise or other background signals is of paramount importance. This is the very complex area of pattern recognition. Both signal detection and signal interpretation are elements of most surveillance systems and each poses very significant problems in designing the most effective possible surveillance system.

DEFINITION OF VIGILANCE

Any discussion of vigilance performance requires consideration of both central nervous system functions associated with alertness and the manifestation of that activity as seen in externalized human behavior. In 1923, Sir Henry Head defined vigilance as the global responsiveness of the nervous system to exteroceptive or proprioceptive stimuli, exphasizing that consciousness was a continuous function of the level of vigilance in the higher centers of the brain, This definition is accepted today by most physiologists (O'Hanlon, 1970). On the other hand, psychologists have preferred to define vigilance in a more behavioral sense; that is, as an unspecified function of the central nervous system that enables man to respond effectively to the infrequent and uncertain occurrence of specific, often low intensity stimuli (signals) in a monotonous environment. Today, it is widely recognized that insights into vigilance performance and monotony tolerance clearly demand both viewpoints, i.e., a psychophysiological approach.

Various kinds of behavioral responses are usually employed to indicate trends in cerebral vigilance. However, the averaging of behavioral responses over a period of time can lead to the misconception that changes in cerebral vigilance are typically slow and progressive. Actually, the work of Oswald (1962) and others has shown quite the opposite: cerebral vigilance normally fluctuates widely, on a moment-to-moment basis. There are, however, long-term trends that are very important. What may be considered a classical change in performance over time is shown in figure 1. Performance (ordinate) at the start of the watch is shown under alerted conditions where the operators are ready for the watch to begin and a relatively large number of signals is presented. As time goes on (abscissa), it can be seen that there is a performance decrement which generally levels off somewhere after 30 to 60 minutes.

Then, if a relatively large number of signals is again presented at the end of the watch, performance usually goes back up to the level near where it started, demonstrating that the operators' average level of performance was substantially below their achievable maximum. There are many research studies that show typical vigilance or performance decrements of this general type.

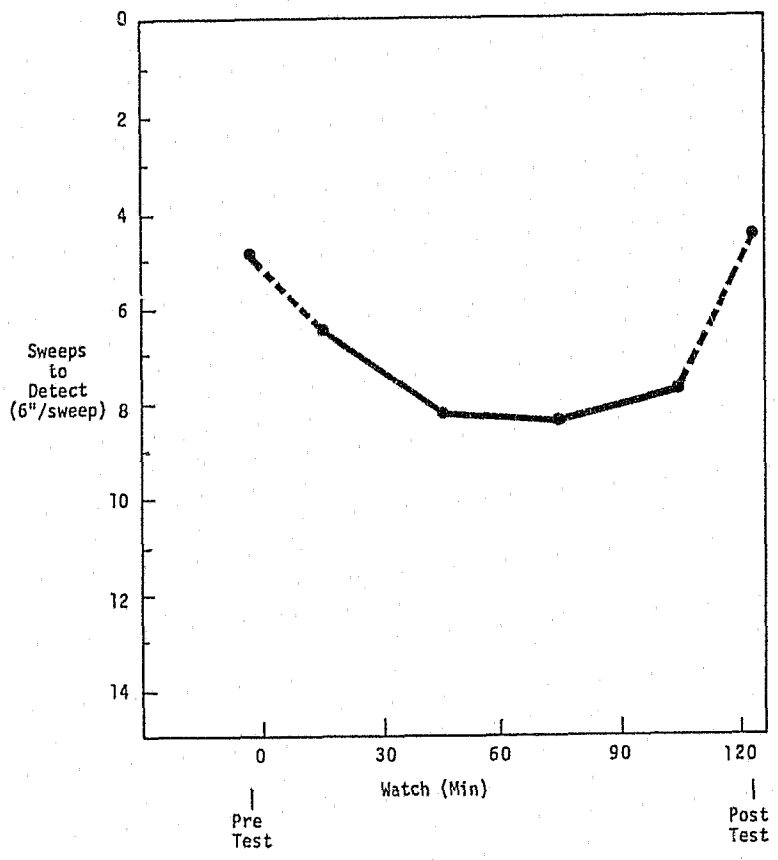


FIGURE 1. *Classic vigilance decrement (from O'Hanlon & Beatty, 1976).*

THE PROBLEM OF MAINTAINING VIGILANCE

Research interest on the vigilance decrement can be traced historically to the introduction of assemblyline methods in industry, and as early as 1932, performance trends in visual inspection tasks were the subject of study. The development of strong interest in vigilance research is generally attributed, however, to studies of performance decrements of ships' lookouts and airborne radar operators during World War II. The task of these operators fully embodied the essential vigilance features of long waiting with signal uncertainty. American and British investigators independently determined that radar operators did not perform at peak detection efficiency for long periods of time, even when their failures could have serious operational consequences. Detection performance appeared relatively good at the beginning of a watch, but often deteriorated progressively as the watch wore on. Years later, Baker (1962) reviewed British wartime records and estimated that "if all radar watches had been only one-half hour long, enemy submarine detections would have increased by 50 percent."

The beginnings of research on vigilance in controlled settings are generally ascribed to N. Mackworth (1948) who was probably the first to take the real-world operational problem of sustained attention for low probability events into the laboratory. Since then, an enormous amount of research on vigilance has been conducted. Attention has been directed toward the influence of such variables as signal duration, intensity and frequency, the interval between signals, the type of non-signal background stimuli,

task complexity, task duration, knowledge of results provided to the operator, sensory modality, sensory restriction, various personality characteristics of the operators, and the influence of environmental stressors such as noise, heat, and vibration. This flurry of interest in vigilance research spanning a period of approximately 20 years has led to the development of various theories of vigilance behavior, some of which will be considered briefly in this paper.

There has been some criticism of vigilance research, particularly that performed in the laboratory, because the vigilance task posed for the subjects typically involves very simple conditions, such as the detection of intermittent increases in the intensity of a periodic flashing light, or intermittent increases in the intensity or quality of an auditory signal, under long-term watchstanding conditions whose monotonous effects cannot be denied. Under these circumstances, investigators almost always obtain a performance decrement of the type shown in figure 1. Results of this kind have been challenged by critics such as Teichner (1972) who, after a review of laboratory vigilance studies, asserted that "the decremental function itself is more presumed than established" and that "more complex situations, those that involve multiple targets and/or extraneous or noisy elements, tend to be less susceptible to decrement with time on watch." Thus, Teichner has challenged the two main assumptions that underlie vigilance research: (1) that an operationally meaningful decrement in vigilance can or does occur, and (2) that it occurs in performing operationally meaningful tasks.

Others, for example Kibler (1965), have contended that technological change has reduced the number of tasks having characteristics approximating those typically employed in laboratory vigilance research. Kibler asserts that:

1. The weak, brief duration signals as typically employed in the laboratory vigilance studies are rarely encountered in applied monitoring tasks.
2. The human monitor typically is required to keep watch over multiple information sources, and frequently more than one type of target or information class is the object of his vigil.
3. The signals are often complex and multidimensional rather than simple and uni-dimensional events such as those typically employed in laboratory studies.
4. In most monitoring tasks, determining the appropriate response to a signal event entails a decision process much more complex than those required in laboratory vigilance studies. Situations which at one time may have required a simple, well-defined response to an unambiguous signal can be, and often are, accomplished entirely by machines.

In terms of vigilance theory, there are good reasons to expect that the vigilance decrement would be less severe under conditions where the human operator is required to monitor multiple channels (assuming his information processing capacity is not exceeded) and where signals are complex rather than unitary. In fact, if the signals to be detected are as simple and well-defined as Kibler suggests they might be, we would argue that machines should be employed for the detection task since machines are not susceptible to a vigilance decrement. The problem, however, is that many surveillance systems detect signals that are not of interest as well as those that are. Further, the signals are often highly complex, occur in a background of noise that is not random, and their discrimination requires a highly sophisticated type of pattern recognition that is very difficult and expensive to automate without the consequence of either: (1) failure to detect some highly significant targets or (2) an extremely high false alarm rate that keeps the system in a more or less constant state of alarm.

Despite the doubts expressed by Teichner and Kibler, there is ample evidence, unfortunately, that the vigilance decrement occurs even under highly complex stimulus conditions and even in the face of circumstances that are very consequential for the

operator. Perhaps the most dramatic evidence of this fact comes from the field of highway safety research. Fatigue, with its attending loss of alertness, is a major contributing factor to the incidence of traffic accidents. In a recent survey of interstate motor carrier accidents resulting in death, injury, or extensive property damage, it was found that about 40 percent were attributable to the driver either being drowsy or actually asleep at the wheel (U.S. Dept. of Transportation, 1970). Loss of alertness is also responsible for a large share of automobile accidents. This is particularly obvious for single-vehicle accidents. For example, (Baker, 1963) has shown that about 30 percent of all single-vehicle accidents are caused by the driver either falling asleep at the wheel or becoming so drowsy that he is unable to effectively control his vehicle.

Moreover, single-vehicle accidents, including those caused by sleeping drivers, tend to be very severe. Baker's nation-wide survey revealed that single-vehicle accidents resulted in 36 percent of the fatalities while constituting only 21 percent of the total number of accidents. In California, single-vehicle, run-off-the-road accidents on freeways account for 55 to 60 percent of the total number of fatalities on those highways.

It is easy to speculate, and there is some experimental evidence as well, that the modern, beautifully engineered, lengthy, straight freeway which covers the shortest distance between points A and B may be conducive to the kind of monotonous stimulation that is likely to produce a loss of alertness on the part of human operators. It should be noted that this can happen despite the fact that, from an information processing point of view, the total stimulation impinging upon the central nervous system of the motor vehicle operator is undeniably complex.

SOME THEORETICAL CONSIDERATIONS

To understand some of the suggestions that will be made later in this paper concerning the systems design implications of human vigilance performance and signal interpretation, it is desirable to briefly introduce a few theoretical considerations. Moruzzi and Magoun (1949) demonstrated that the major information processing area of the brain, the cerebral cortex, ceases to function normally in the absence of constant neural input from the midbrain reticular formation. It is now generally believed that it is the reticular formation that mainly sets the level of cortical arousal. Activity within the reticular formation is itself determined by: (1) neural imputs arriving from collateral fibers of the classic exteroceptive or proprioceptive sensory tracts, (2) impulses arriving from numerous feedback systems within the brain, and (3) from the direct stimulating action of various circulating hormones, notably adrenaline.

In supporting the importance of the reticular formation in maintaining optimal cortical arousal, Hebb (1955) has pointed out that every sensory impulse has two functions. As the impulse passes from a sense organ through a sensory tract to its cortical projection area, the impulse serves a "cue" function, conveying information about the stimulus to the organism. As the impulse passes through collaterals from the sensory tract to the reticular formation, it also serves an "arousal or vigilance function," activating the reticular formation, which arouses the cortex to deal with the incoming information.

INVERTED "U" HYPOTHESIS

Having perhaps identified the center of brain activity most responsible for level of alertness or arousal, we now turn our attention to a number of theoretical considerations concerning the relationship between cortical arousal and performance. Most fundamental and possibly most generally accepted is the "inverted U" relationship probably first suggested by Duffy (1934). This hypothesis states that there is a certain optimal level of arousal for every type of response or learning: under-arousal causes

inattention and a sluggish response; over-arousal causes distraction and irrelevant or uncoordinated responses. Figure 2 depicts these relationships as conceptualized by Hebb (1955).

In addition to the physiological hypothesis, there are a number of behavioral science or psychological theories that will be described briefly.

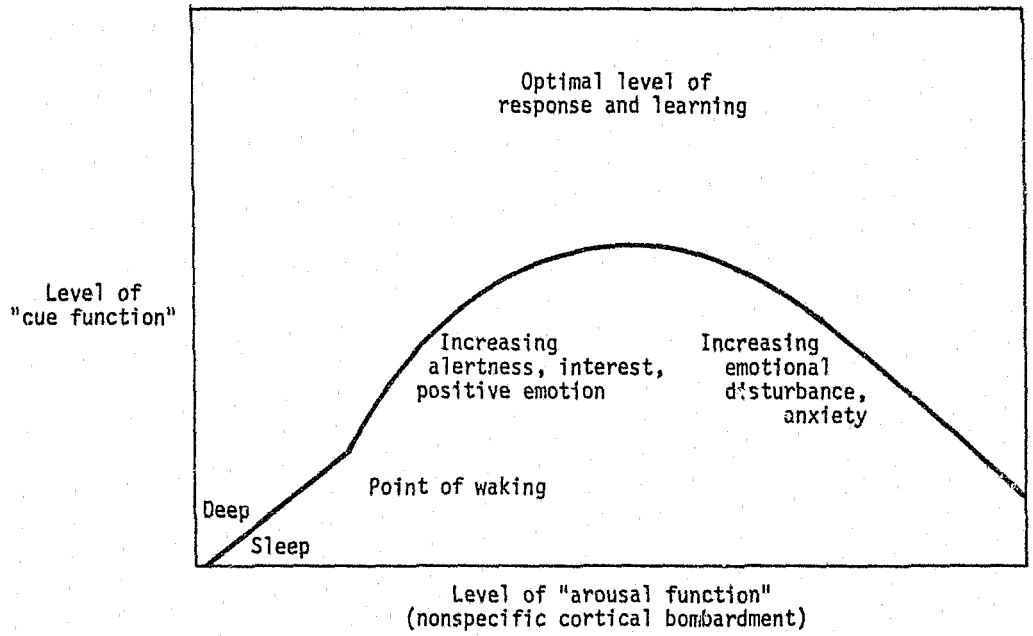


FIGURE 2. *Inverted U hypothesis (after Hebb, 1955).*

INHIBITION THEORY

J. Mackworth (1969) has proposed that the performance decrement found in the course of a wide variety of somewhat monotonous decision-making tasks is related to the physiological phenomenon of habituation. According to this view, active inhibition of neural responses to repetitive stimuli makes various kinds of responses less likely, or reduced in speed or accuracy. Vigilance tasks usually present many "unwanted" background or non-signal events for each wanted signal. According to inhibition theory, the decrement in detection performance is attributable to habituation of the neural responses to the many unwanted background events, from which the signal must be discriminated. According to this view, decrements will occur not only in passive monitoring tasks but also in more active tasks, such as tracking, which require a positive response to every repetitive event.

Habituation has been defined as a decrease in an innate response as a result of repetition of the stimulus. A stimulus only captures an individual's attention when it is new, unexpected, or difficult to interpret (Mackworth). These factors produce the arousal response. As these properties disappear with repetition, the response habituates. Therefore, a stimulus that is repeated many times produces a gradually decreasing response.

REINFORCEMENT THEORY

Reinforcement theory falls within the theoretical framework of operant conditioning. The basic assumption is that detection of a signal serves as reinforcement for making observing responses. If detections are rare, the frequency of observing responses will diminish, the probability of missing infrequent signals will increase, thus leading to a further lack of reinforcement and a continuing decrement in performance. Conversely, reinforcement theory postulates that the detection of a signal is in itself a rewarding experience, and will serve as an inducement to further vigilance.

FILTER THEORY

Filter theory is based on the assumption that because of the limited capacity of the human perceptual system, a selective filter device in the nervous system passes only certain incoming information on to the perceptual system. According to this view, it is impossible to respond adequately to more than one part of the total stimulus situation at a time. As with inhibition theory, it is assumed that stimuli of the greatest physical intensity, biological importance, or novelty have the highest probability of being attended to, but repeated observation of a stimulus reduces the novelty of that stimulus and results in a greater probability of detection for other, task-irrelevant stimuli. This results in a hiatus in the intake of task information and these interruptions, although short, tend to occur more frequently as time on the task increases (Stroh, 1971). Thus, the operator experiences a series of temporary distractions of attention that reduces the probability that critical signals of short duration will be detected.

EXPECTANCY THEORY

Several investigators have employed the term "expectancy" in explaining the results of vigilance experiments. Expectancy theory suggests that: (1) one is more likely to detect a signal if it occurs when it is expected; (2) it is easier to determine when to expect a signal if the other signals have occurred at fairly regular and small intervals; and (3) if a signal occurs at a time when it is not expected, the observer is more likely to miss it.

AROUSAL THEORY

It was noted earlier that Hebb felt that a stimulus serves the dual functions of providing a cue for guiding goal-directed responses and a basic arousal function at the level of the reticular formation. It was his opinion that a state of alertness could not be maintained under conditions of monotonous sensory stimulation. Related to this view is the contention that reduction in stimulus variation of any kind may be responsible for decrements in vigilance performance. Thus, a major prediction from arousal theory with respect to vigilance performance is that the greater the variety of either task-relevant or task-irrelevant stimuli (within limits), the smaller the vigilance decrement should be. This prediction has been supported by a good deal of research.

An important point to remember is that arousal theory says nothing at all about the effects of stimulus frequency, except as it relates to novelty. The more often a stimulus is repeated, the less novel it becomes. From this it follows that even in a very complex task, such as motor vehicle driving, the operator is susceptible to the vigilance decrement. The case of driving in rural areas at night versus city driving during the daytime provides an example. At night, the total visual input is considerably less rich and varied than it is in daylight. Accident data involving drowsy drivers strongly support the notion that night driving may be less arousing in the sense implied by arousal theory. However, this is not the whole argument; there are other fundamental

physiological facts related to arousal which tend to make night operations more hazardous. These will be discussed later.

SIGNAL DETECTION THEORY

An interesting theoretical viewpoint that is quite different from those so far described is that of signal detection theory. According to this theo[illegible]crements in operator detection performance over time are not necessarily the resu[illegible] of changes in operator proficiency but rather reflect a change in the operator's criterion of what constitutes a signal. When this change is in the direction of greater conservatism, fewer faint signals will be detected. It is also contended that fewer false alarms will occur but this prediction only follows if the background noise is random and if the operator's detection performance involves a good deal of guesswork. However, in many surveillance systems, nontarget signals are encountered which meet many of the physical criteria of target signals; the operator's task, therefore, becomes one of responding to subtle differences between target and non-target signal patterns. Thus, there must be concern for maintaining vigilance not only for the detection of faint signals but for discriminating subtle differences between wanted and unwanted signals which may be clearly suprathreshold.

Swets et al. (1961) have noted that monitoring tasks involve not only discrimination but also decision. Signal detection theory handles this dual aspect of performance very nicely. Calculations based on signal detection theory yield two independent scores: d′, which is a measure of the sensory capabilities of the observer, or of the effective signal strength; and β, which is a measure of the observer's cautiousness, and reflects such things as signal interpretation skill, attitudes toward false alarms, and motivation. The location of the optimal decision criterion (β) is determined by the particular balance of operational probabilities desired. For example, it is generally desirable to maximize the probability of detecting a true target signal, but a consequence of this may be a very high false alarm rate. This trade-off consideration may lead the operator to adopt a more conservative decision threshold.

Several researchers have found evidence to support the proposition that the apparent vigilance decrement is often the result of increased caution on the part of the operators. It should also be noted, however, that a decrease in the subject's basic sensitivity to faint signals has been observed in some cases. Finally, research performed by Wylie and Mackie (1974) have shown that a high degree of command attention can both increase the number of valid detections and decrease the number of false alarms. This was reflected by increased values in both d′ and β and, it should be noted, directly supports reinforcement theory.

In leaving this brief introduction to theoretical positions on vigilance, it should be noted that the research community generally endorses parts of all of these theories and that considerable effort has been directed toward developing a unified theoretical viewpoint.

INDIVIDUAL DIFFERENCES IN PERFORMING MONOTONOUS TASKS

A major and very consequential finding from many studies of vigilance is that there are large individual differences among operators in ability to sustain performance in the face of monotonous conditions. At the beginning of a work period, there may be relatively small differences in detection performance among a group of randomly selected personnel but, as the watch continues, these differences typically become larger. Figure 3 depicts the range of individual variations in the study by O'Hanlon and Beatty referenced earlier, as well as the performance of the 25th, 50th, and 75th centile operators. Obviously, such differences in performance could be operationally significant. There are evidently both physiological and psychological reasons for these differences.

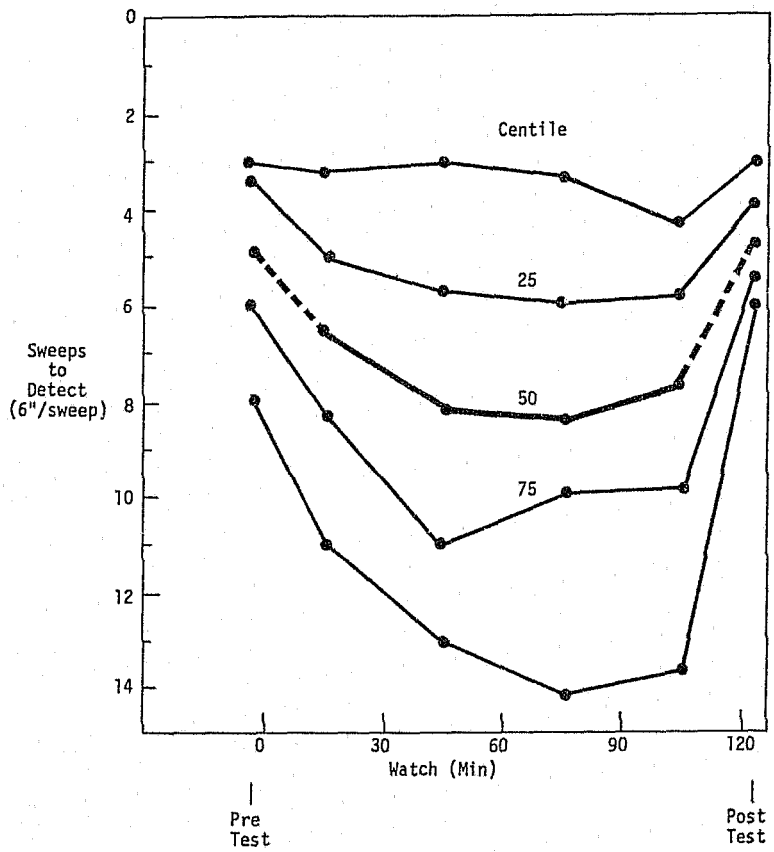


FIGURE 3. *Individual difference in detection performance (from O'Hanlon & Beatty, 1976).*

PHYSIOLOGICAL FACTORS

Perhaps the most direct physiological correlate of sustained attention and vigilance performance is the level of circulating catecholamines, adrenaline and noradrenaline, in the blood stream. O'Hanlon (1970) has shown that there is a high correlation between circulating adrenaline levels and detection performance in watchstanding tasks. He has shown that when the operator is alerted, the average adrenaline level quickly rises from its resting level; but, if signals are infrequent and the watchstanding conditions are otherwise monotonous, the level of circulating adrenaline progressively declines in a manner which closely parallels poorer performance in signal detection.

A second physiological measure that appears to be closely related to state of alertness is variability in the inter-beat intervals of the heart. Heart rate generally increases during periods of high arousal and the interval between beats becomes highly regular. Under monotonous watchstanding conditions, as well as under prolonged driving conditions on the highway, it has been shown that the variability in the inter-beat interval of the heart progressively increases. This increase has been shown to be related to increased time to detect target signals on radar and sonar displays, and by decreases in the automobile driver's ability to maintain smooth tracking performance on the highway. In some cases, the driver's performance shows inadvertent drifting from the intended traffic lane which, it may be speculated, can eventually result in the drowsy driver either running off the road or into an opposing traffic lane.

Another physiological index of level of central nervous system arousal is the distribution of energy in the several frequency bands of the electroencephalogram (EEG). EEG signs of waning arousal, in particular, an increasing abundance of theta activity (3 to 7 Hz) over the posterior cortex, has been correlated with poor monitoring performance and behavioral indications of drowsiness. Mackie, O'Hanlon, and McCauley (1974) showed that increasing driver drowsiness and poor lane tracking performance was associated with increasing percentage of EEG energy in the lower (delta and theta) bands relative to the higher frequency bands (alpha and beta). In an ingenious experiment, O'Hanlon, Royal, and Beatty (1976) trained subjects utilizing biofeedback techniques to proficiently self-regulate (minimize) the amount of brain wave energy in the theta band while simultaneously engaging in a radar monitoring task. Theta suppression was associated with stable and superior target detection performance. When theta was suppressed by means of the biofeedback technique, experienced radar operators were able to perform detection tasks with no degradation in performance over a 3-hour period. Without this biofeedback, they showed a linear decline in target detection efficiency over time.

INTROVERSION/EXTROVERSION

Research on vigilance performance in a variety of contexts has repeatedly shown that individuals who are basically introverted in their personality structure tend to do better in performing monotonous tasks than individuals who are basically extroverted. According to Eysenck, the typical introvert is quiet, retiring and reserved. He tends to plan ahead and distrusts the impulse of the moment. He does not like excitement, keeps his feelings under close control, seldom behaves in an aggressive manner and does not lose his temper easily (Eysenck and Eysenck, 1968).

The extrovert, in contrast, tends to be outgoing, impulsive and uninhibited. He is social, needs to have people to talk to and does not like sedentary activities. He craves excitement, takes chances and tends to be impulsive. He prefers to keep moving and doing things, tends to be aggressive and is not always reliable. Few people, of course, are introverted or extroverted in all aspects of their personalities. Nevertheless, vigilance research data tend to confirm the observation that people with introverted tendencies do better at sedentary tasks than do those who are extroverted.

We have noted that, according to signal detection theory, some aspects of vigilance performance can be explained in terms of changing levels of operator cautiousness. In terms of the definitions of extroversion and introversion just presented, one can readily speculate that individual differences in personality types may very well be related to such critical system performance parameters as false alarm rate and missed detection opportunities.

WORK/REST CYCLE

The work-rest cycle itself is an important consideration in maintaining vigilance. Obviously, individuals who engage in extended operations without adequate periods of rest may suffer a vigilance decrement. Perhaps not so obvious is the fact that displaced sleep has equally or perhaps even more serious effects on performance than occasional loss of sleep. Displaced sleep means that the individual is forced by circumstances to obtain his sleep at markedly different times with respect to the 24-hour clock from one day to the next. All of us have experienced the disruption of normal sleep patterns associated with the shift of time on the 24-hour clock occasioned by travelling across a number of geographic time zones. Time-honored military, watchstanding procedures, for example, those followed aboard Navy ships at sea, which call for an individual to stand a night watch during a different period of time on each successive night, necessarily

produce sleep displacement and almost ensure adverse consequences in terms of vigilance.

Perhaps the most fundamental consideration with respect to work/rest cycles and vigilance, however, concerns the natural daily variations in level of psychophysiological arousal. These are variously referred to as diurnal rhythms or circadian biorhythms. There is evidence that these circadian biorythms affect not only the primary physiological functioning of various organs associated with arousal level, but also human behavior under operational stress. Klein (1970) has shown marked correlations between circadian rhythms of physiological functioning and performance in a variety of tasks including flying in flight simulators. Some of his data are shown in figure 4 where it can be seen that both physiological indicators of arousal and task performance show a very pronounced decline in the early morning hours, from midnight on.

Results from controlled laboratory studies have been substantiated by field research to underscore the significance of circadian biorhythms on vigilance. Working with longhaul truck and bus drivers, Harris and Mackie (1972) have continuously tracked a number of physiological variables related to arousal as the drivers engaged in extended operations, day and night. The arousal measures show a marked depression during the hours between midnight and 6 a.m. For those drivers who had engaged in extended driving periods and were *concluding* their trips in the early morning hours, the arousal signs were particularly depressed. The operational significance of these findings is attested to by analyses of accidents involving drivers who were judged to have dozed at the wheel or actually to have been asleep just prior to the accident. The number of such accidents occuring in the time frame between midnight and 6 a.m. is approximately three times the number of such accidents occuring during all of the remaining hours of the day combined. This occurs despite the greatly reduced traffic density during those early morning hours, and thus, to some extent, the reduced level of exposure to accident-producing circumstances.

Therefore, in terms of arousal theory, there are at least two major variables operating to magnify the vigilance decrement during nighttime operations: (1) the natural decrease in biochemical stimulation of the central nervous system; and (2) the relative paucity of non-monotonous stimulation from the operating environment.

ENVIRONMENTAL STRESSORS

A considerable amount of research has been directed toward the effects of such environmental stressors as noise, heat, and vibration on vigilance performance. While we are perhaps conditioned to think of such stressors as adversely affecting human performance, it should be noted that the inverted U hypothesis discussed earlier would predict that performance under moderate amounts of stress may well be superior to that obtained if the individual is either understressed or overstressed.

There are some research results that support this prediction. For example, in sonar watchstanding, target detection performance has been shown to be somewhat better in a mildly noisy environment than in a quiet one, provided that the noise source does not actually mask the auditory signals to be detected. On the other hand, there is some evidence that human perceptual processes are adversely affected by noise when it is intense. With respect to temperature, Mackie et al. have shown that high combinations of heat and humidity adversely affect the performance of individuals engaging in prolonged driving. However, similar performance effects have not been found for various levels of whole-body vibration. This is not to say that extended exposure to vibration might not have other adverse effects on human operators.

Considerable caution must be exercised in drawing conclusions about the effects of various environmental stressors on vigilance performance since they are likely to be very specific to the intensities and other characteristics of those stressors. It can

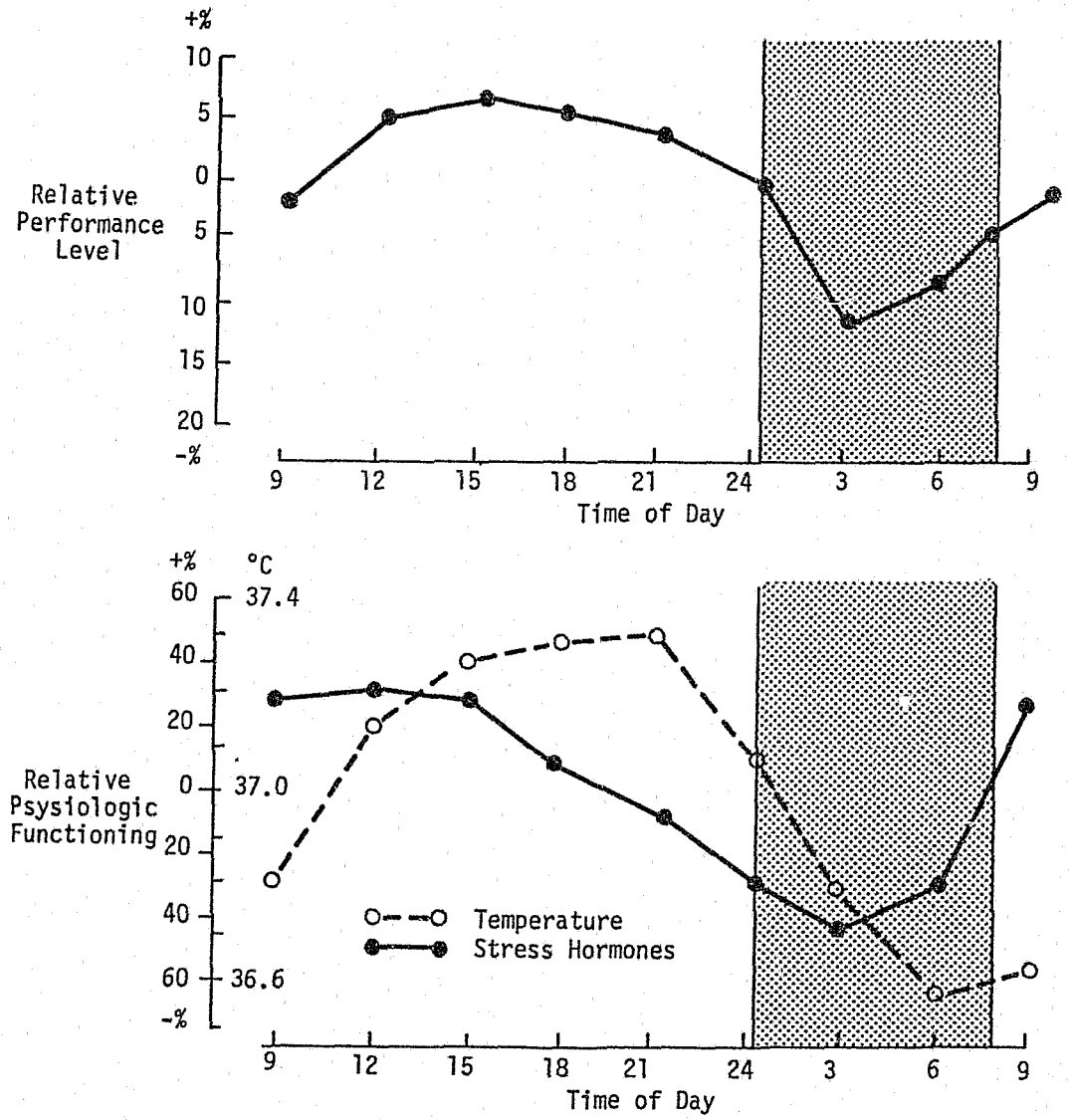


FIGURE 4. *Circadian rhythms of behavioral and physiologic functioning (in percent of the 24-hours-mean; body temperature in °C). (After Klein et al., 1975).*

probably be concluded, however, that mild stressors, in whatever form, are likely to have a beneficial effect on maintaining alertness for many operational tasks.

SIGNAL INTERPRETATION

Thus far, the more elementary aspect of the surveillance system operator's task has been described, i.e., the simple detection of a signal in the system. It has been noted that "noise" from which signals of interest are to be differentiated in many surveillance systems is far from random. Thus, the operator has a continuing requirement to differentiate signals that are of interest from those that are not. This may involve fairly elementary perceptual processes such as discriminating the size or shape of an object or its representation on a cathode ray tube (CRT) display, or it may involve fairly high-level cognitive processes, including inferences about the target's nature or

behavior from a variety of displayed cues. Thus, in most surveillance systems the act of target detection includes elements of what is properly considered target identification. The problem of maintaining alertness for target identification is strongly influenced by many of the same variables that have been discussed earlier in connection with detection performance. Virtually all of the theories of vigilance have a bearing on the process of target identification. For example, if the total stimulus field that must be monitored at a given time is very complex, filter theory would suggest that stimuli of the greatest physical intensity and novelty would have the highest probability of being detected. This might occur at the risk of increasingly large numbers of attention lapses for those areas of the monitoring display which regularly produce nothing but routine, nonthreat signals.

Filter theory clearly ties in closely with expectancy theory in this connection. "Expectancy" can operate in two ways to adversely affect signal detection and identification. In case of detection, if the operator's expectancy for encountering a significant target is low, momentary lapses of attention are likely and the vigilance decrement will be more severe as measured either by missed detection opportunities or latency of detection. In the case of signal identification, it has been shown in the context of sonar operations that operators will perceive cues in ambiguous stimuli that relate to targets of the type they "expect" to encounter. This can have favorable effects when there is advance intelligence that a target of a particular type may be encountered. It can have negative effects when, on the basis of past experience, the operator expects to encounter only targets that are not operationally significant.

With respect to arousal theory, it should be clear that prolonged encounters with non-significant targets, even if they occur very frequently, will serve to reduce activation of the arousal centers in the central nervous system. For this reason, in surveillance systems where targets of interest are a very *infrequent* event, and non-interesting targets occur very frequently, it may be imperative to resort to artificial signal injection on a carefully programmed basis to maintain operator performance at a high level.

Both signal detection theory and reinforcement theory suggest that it is absolutely imperative for operators of surveillance systems to have feedback concerning the adequacy of their performance. By the very nature of their jobs, most of their time is spent screening out signal inputs that are not operationally significant. There is little inherent reward in this process and there may be negative rewards for reporting signals that turn out to be false alarms. In many surveillance systems, false alarming is distracting, disruptive, and possibly even embarrassing to the operational command. This tends to produce a basic conservatism (β in the signal detection theory sense) in target reporting, and may prove costly in terms of latency of detection, or even completely missed opportunities to detect valid targets. Most surveillance systems are not designed to provide inherent feedback concerning these two aspects of performance. In fact, by their very nature, the system may be totally unaware of missed opportunities for valid detections. To maintain a high level of alertness and motivation for the task, as well as to adjust the operator's decision threshold to that level most desired in view of the system's objectives, requires that a means be established to feed back information to the operators concerning the success and failures in their performance. This, too, often argues for a careful program of injected target signals.

SOME SYSTEM DESIGN CONSIDERATIONS

One final problem having to do with both signal detection and signal interpretation merits discussion. The various ways in which human performance may fall short of perfection in detecting and identifying the presence of significant signals in a surveillance system have been emphasized. The frequently proposed engineering solution to such human deficiencies is to totally automate the process. To do this for

many surveillance systems requires computer algorithms that will effectively handle some extremely subtle and complex pattern recognition problems. Many millions of dollars have been invested in attempts to do just this in certain military surveillance systems. Typically, the disappointing result has been that when the detection threshold of the computer is adjusted sufficiently low so as to minimize the probability of missing significant targets, the system has been overwhelmed by a corresponding high false alarm rate. The reasons are complex, but basically concern the complexity of automatically extracting a great variety of very subtle target cues.

There is little doubt that machine algorithms can be designed that are more sensitive to faint signals in noise than is man and that do not, under circumstances other than catastrophic breakdown, suffer a vigilance decrement. These advantages of machines might well be capitalized on in the design of new surveillance systems. However, human perceptual and cognitive processes are sorely needed later in the process, where discrimination must take place between signals that meet only some of the criteria for targets of interest and those that meet enough of them so that a genuine alert should be called. This implies that the most effective surveillance system for a given application will be achieved only if the system is designed to take advantage of the unique capabilities of both man and machine and care is taken to avoid the limitations of both. In this process, attention should be directed, as a minimum, to the following:

1. Selection of personnel who are resistant to the vigilance decrement
2. Display designs that will minimize the effects of momentary lapses of attention
3. Design of operator tasks so that they are not oversimplified; augmentation, if necessary, with nondistracting, extra-task stimulation
4. Means of avoiding long intervals of time during which no signals of interest are presented
5. Means of providing performance feedback to the operators
6. Means of adjusting system operating procedures for the best achievable compromise between missed detections and false alarms
7. Special provisions for maintaining alertness during periods of reduced psychophysiological arousal
8. Watch schedules that will minimize such problems as displaced sleep
9. Watch environments characterized by conditions that are neither so overstressful nor so benign as to adversely influence vigilance performance.

REFERENCES

Baker, C. H., *Man and radar displays*, New York: MacMillan Press, 1962.

Baker, S. J., *Single vehicle accidents: A summary of research findings*, Washington, D.C.: Automotive Safety Foundation, 1968.

Duffy, E., Emotion: An example of the need for reorientation in psychology, *Psychological Review* **41**, 184-198, 1934.

Eysenck, H. J., and Eysenck, S. B. G., *EITS Manual: Eysenck Personality Inventory*, San Diego, Educational & Industrial Testing Service, 1968.

Harris, W., and Mackie, R. R., *A study of the relationships among fatigue, hours of service, and safety of operations of truck and bus drivers. Final report, Phase I & II* (Tech. Rep. 1727-2), Goleta, Calif.: Human Factors Research, Inc., 1972.

Hebb, D. O., Drives and the C.N.S. (central nervous system), *Psychological Review* **62**, 243-254, 1955.

Kibler, A. W., The relevance of vigilance research to aerospace monitoring tasks, *Human Factors* **7**, 93-99, 1965.

Klein, K. E., Bruner, H., Holtmann, H., Rehme, H., Stolze, J., Steinhoff, W. D., and Wegmann, H. M., Circadian rhythm of pilots' efficiency and effects of multiple time zone travel. *Aerospace Medicine* **41**, 126-132, 1970.

Mackie, R. R., O'Hanlon, J. F., and McCauley, M. E., *A study of heat, noise, and vibration in relation to driver performance and physiological status* (Tech. Rep. 1735), Goleta, Calif.: Human Factors Research, Inc., 1974.

Mackworth, J. F., *Vigilance and habituation*, Middlesex, England: Penguin Books, 1969.

Mackworth, N. H., The breakdown of vigilance during prolonged visual search, *Quarterly Journal of Experimental Psychology* 1, 6-21, 1948.

Moruzzi, G., and Magoun, H. W., Brain stem reticular formation and activation of the EEG, *EEG and Clinical Neurophysiology* 1, 455-473, 1949.

O'Hanlon, J. F., *Vigilance, the plasma catecholamines, and physiological variables*, (Tech. Rep. 782-2), Goleta, Calif.: Human Factors Research, Inc., 1970.

O'Hanlon, J. F., and Beatty, J., Catecholamine correlates of radar monitoring performance, *Biological Psychology*, 1976, in press.

O'Hanlon, J. F., Royal, J. W., and Beatty, J., Theta regulation and radar vigilance performance. In *Biofeedback and behavior: A NATO symposium preliminary proceedings*, J. Beatty (Scientific Director), Munich, Germany, 27-30 July 1976.

Oswald, I., *Sleeping and walking*, New York: Elsevier, 1962.

Stroh, C. M., *Vigilance. The problem of sustained attention*, Toronto-New York: Pergamon Press, 1971.

Swets, J. A., Tanner, W. P., and Birdsall, T. G., Decision processes in perception, *Psychological Review* 68, 301-340, 1961.

Teichner, W. H., *Predicting human performance III: The detection of a simple visual signal as a function of time of watch* (NMSU-ONR-TR-72-1), Las Cruces, N.M.: New Mexico State Univ., 1972.

U.S. Department of Transportation, U.S. Bureau of Motor Carrier Safety, *Analysis and summary of accident investigations: 1969*, 1970.

Wylie, C. D., and Mackie, R. R., *Attack decision making in surface ship ASW: Historical, theoretical, and experimental d...* (U), (Tech. Rep. 1721-2), Goleta, Calif.: Human Factors Research, Inc., 1974 (CONFIDENTIAL).

DISCUSSION

Question: On the subject of nuisance signals, what sort of time frame are those taken over? For example, if a person were exposed to nuisance signals over a period of 6 months, would one expect a decrement?

DR. MACKIE: By nuisance signals, you mean signals that are normally injected to keep the system alert? I think the answer to your question depends on how it's handled. In many surveillance systems, I see no reason why the injected signal can not be indiscriminable from an actual one, and, therefore, the operator would simply be doing his/her job. If the signal is regarded as a source of nuisance, then my prediction would be that the response to it will adapt out, or at least some other kind of response mechanism will be adopted to defeat the purpose of having such signals in the first place. But, in many surveillance systems where the targets of interest appear extremely infrequently, it does not seem that there is any other solution than to inject signals which need full processing. They may actually alert the system, and only somebody farther up the line is aware of the fact that this is a signal that has been injected.

To the extent that the operator's task involves analysis of the signals as well as its initial detection, the injected signals should be of such a level of sophistication as to require the operator's full attention to all of the detailed cues and all other things included in facing the real situation.

Operators deserve and need feedback on their performance. Other investigators have suggested that operators of surveillance systems should actually acquire, over a period of many watches, norms on their own performance, so that not only are they getting feedback, but their command is getting feedback on their performance as well.

Question: Which of the senses is most valuable in signal detection?

DR. MACKIE: That is difficult to answer; I'm not sure how many researchers would agree. The auditory channel has the advantage of requiring nothing comparable to voluntary visual search. There are many problems with visual search and displays, primarily associated with the fact that human operators do not tend to search very systematically. In general, the more sensory channels that can be stimulated the better. Reinforcing one channel with another is the best practice.

In many cases, there is no choice other than using a visual display, sometimes a fairly large one. In this case, techniques which force the operator's visual search pattern to be more or less systematic may be needed. A number of such display techniques has been developed.

Question: Has much attention been given to the optimal man-machine design mix; have you done much work on this?

DR. MACKIE: There has been a great deal of concern for the allocation of functions between man and computer in surveillance systems. The generalization defended the most is that the automatic part of the system is by far the better element of the system to rely on as far as detecting signals in noise are concerned, but, when it comes to identifying complex signal patterns that sometimes change depending on environmental conditions, it may be very difficult for a computer algorithm to do this because of the large amount of computer capacity which is necessary to process a signal track that may be changing dynamically. When tradeoffs like this are involved, it is probably better to put man back into the system.

With surveillance systems, the single, largest problem by far has been that the computer algorithms have difficulty extracting visual cues; for that matter, either one. If the cues can be extracted, then they can be put together with logic very nicely. Humans are good at the extraction process, getting information out of a very complex, time varying signal, provided that they are given proper training in the task.

Question: Has any effort been made to include non-humans in surveillance studies, e.g., dogs and birds?

DR. MACKIE: I have not in my research. I understand there is some work going on with animals, but I do not feel qualified to speak on this subject.

HUMAN RELIABILITY FACTORS

Joseph J. Cappucci

Operational Systems, Inc., Arlington, VA 22209

A continuing problem in both government and industry has been the search for a dependable method of measuring the reliability, loyalty, stability, and suitability of persons being considered for employment in sensitive and critical positions. For many years, the methods utilized in government to determine a person's suitability have consisted of various forms of background investigations, national agency checks, local agency checks and combinations of all three. These do provide highly informative data on a person's past reliability, and security clearances are granted on the premise that, if a person has been loyal, reliable and stable in the past, then it can be presumed he will be so in the future. For the vast majority of people this has apparently proven correct, but for some it has not, perhaps because there were no obvious clues in their past activities to indicate how they would react to a new situation.

The problem with people is that they act like human beings, and human beings are subject to stress, temptations, emotions and other factors which have some impact upon their behavior. Measuring or predicting the effect of these impacts on a person has been and still is a problem. Of the people in the armed forces who have been apprehended for criminal acts and disloyal activities, the majority had been given some form of security clearance. They had a good past and there was no apparent reason to deny them a clearance. However, in many cases it was found that, subsequent to being cleared, these persons were exposed to new opportunities and temptations for criminal or disloyal acts as a result of a geographical or job assignment change, or both, or some new emotional factor entered their lives.

For example, unless a person has, or can have, access to classified information, he is not a good candidate for recruitment as a spy. No spy recruiter wants him since he has nothing to sell. An espionage case is recalled in which the subject desiring money actually tried to be recruited as a spy overseas. But since he had no access to classified information at that time, he had nothing of value to sell. He was told to come back when he had access to something of value. These circumstances compelled him to remain loyal despite his intent. He was subsequently assigned to an area where he did have access to classified information. This provided him the opportunity, and he did get himself employed as a spy until he was caught. A person relocated to an area where narcotics are cheap and plentiful, for example, now has the actual opportunity to become involved in narcotics traffic for financial gain or other reasons. Many resist the temptation, but a few don't.

Since a background of good behavior does not always promise continued good behavior under new and changing conditions, a system of periodic updates of the background investigation has been and still is in-being as a method of rechecking reliability. An update may consist of just an agency check or a continuation of a background investigation where the previous one left off. However, this still consists of a report of past conduct, which is a good indicator, but obviously not fool proof, since there still is no way of knowing what temptations and situations the person will be exposed to during the ensuing years, nor how he will react to such exposures.

So how can the wrongdoers be found? Occasionally a person will report an approach from another to participate in a crime or a disloyal act to the authorities. Sometimes a report will be made after the first initial approach, other times when the

person becomes involved to some degree, and then becomes apprehensive about getting caught. Most would be learned about wrongdoers by other means, including good investigative techniques.

What are the temptations and the motives which could cause a person's reliability or integrity to waiver? They include: (1) The opportunity for easy money, with everything that money brings, (2) involvement in affairs with foreign espionage recruiters, and (3) in some cases, a misplaced desire to help bring peace to the world by sharing information. Some motivations might appear rather weak, and it may be wondered how anyone could succumb to the temptation. The fact remains that some do.

It is not very easy to know how you would react to a given situation until you face the reality of it. Everyone's reliable to some extent, and everyone has integrity when there are no opportunities or temptations to be anything else.

The question is, what would one do in a real situation? How would a particular person react to a real opportunity? Assume an actual offer of $100,000 in cash or twice that amount to conduct an espionage or sabotage act. At what point is the money offer such that some persons can't refuse? How does one judge a person's resistance to something real like that?

Some people are honest, because they're afraid they'll be caught if they aren't. Most are honest because they can resist the temptations. Consider real threats of blackmail or duress. What qualities does one need to refuse and bear the consequences? How can a person's resistance to real temptations be assessed. Primarily, there has been a dependence on a background investigation to judge a person's continued reliability, but background investigations alone obviously cannot provide the complete data base needed for a full evaluation.

In recent years, the scope or extent of a background investigation has continued to shrink with periodic limitations imposed on what subjects can be covered, (i.e., beliefs and associations cannot be checked). Additionally, legal questions arose as to the authority of security investigators to make FBI and police file checks to determine if a person had a criminal record. Many states now allow such checks only in connection with a current criminal case and not with a loyalty case. This can cause some clearance adjudication problems, mostly in Industrial Security cases. Then came the Privacy Act of 1974, and the Freedom of Information Act as amended, in 1974. Very briefly stated, the Privacy Act, among other things, provides certain safeguards for an individual against an invasion of personal privacy through the misuse of Federal records, and it provides that individuals shall be granted access to records concerning them which are maintained by Federal agencies. A record is defined as any item, collection, or grouping of information about an individual, including but not limited to, education, finances, criminal history and employment record. The Act authorizes some exemptions pertaining to access and disclosure, among which are: Certain criminal information used for law enforcement purposes, and investigatory material compiled solely for the purpose of determining suitability, eligibility or qualifications for Federal employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who provided it under an express promise the identity would not be revealed.

The Freedom of Information Act is generally similar to the Privacy Act except that it pertains to government records as opposed to a personnel record. The Act provides that any person has a right to access and copies of any document, file, or other record in the possession of any Federal agency or department, subject to about nine exemptions. With regard to security, the exemption is similar to the Privacy Act. Additionally, classified information is exempt, except that the classification can be challenged in court. Personnel references which constitute an unwarranted invasion of privacy are also exempt.

These two acts have had very little impact thus far on the usefulness of a background investigation. It is possible that some people interviewed during a background investigation on an individual may be reluctant about disclosing unfavorable information because they don't want to be involved or sued, in the event the subject of a background investigation finds out who divulged the information. However, thus far, it appears that these are much in the minority.

Since recent changes have had only minor impact on the value of information developed through a background investigation, a background investigation continues to be an important vehicle in the process of assessing a person's reliability. But even at best, is that sufficient to permit at least a fairly accurate assessment of a person's reliability and stability? For many jobs the answer could be yes, but for highly critical jobs it may not be enough. The background investigation should be augmented by some procedure which will, with some degree of accuracy, assure us that persons who are in a position to perform acts which will affect the national security, and our safety and welfare, are reliable and stable from the start, and that there is a good basis for believing they will remain so. This is where behavioral sciences can make a contribution. An appropriate mixture of background information plus some form of clinical testing or evaluation by competent professionals may be better for more accurately measuring reliability. The most important factor in any security system is the human factor, and at least as much effort and professionalism should be devoted to assessing human reliability as is expended in assessing the reliability of hardware, software and other segments of the security system. What is a particular person's weakness, and how can it be exploited? How will a person react in a real situation? What type of person will be an alert security guard where duties become monotonous and boring—when nothing may really happen for months or maybe years—then suddenly in seconds he has to respond to an emergency? How much stress can a particular person take in a certain critical job? What behavior patterns should be looked for to detect early indications of a decrease in reliability? These are just a few of a long list of questions which have a bearing on human reliability.

The best security system in the world is only as good as the people who implement it. Accordingly, more should be done to evaluate and assess the reliability of the people who are in a position to do us grave damage. *Background investigations report past history—behavioral science can help assess future conduct and reliability*. The science of human behavior can be a very important supplement to other security procedures in assessing the reliability of persons in critical positions, and it is hoped that this science will be utilized much more than it has in the past.

HUMAN ENGINEERING IN DECISION THEORY

Mr. Kenneth A. Plant

Science Applications, Inc., Arlington, VA 22209

This paper presents some very personal thoughts about the state-of-the-art in decision-theory, especially as it relates to the Department of Defense. In addition, some interesting basic research that is ongoing across the nation will be discussed and related to research that will be conducted in our laboratory being built in Rosslyn.

Figure 1 lists the essential ingredients of command and control. Sensors, communications, computers, facilities and decision aids form the classical tools that aid the decisionmaker. Automatic Data Processing (ADP) is emphasized because it pervades all the other ingredients today.

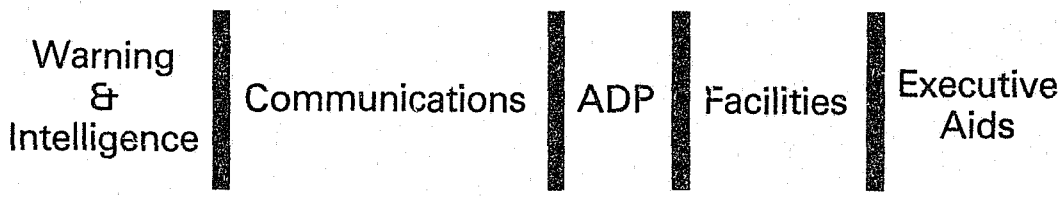


FIGURE 1. *Resources supporting information flow.*

One of our concerns is that, although great technological strides in each of these areas have been made, it is possible that the technology has driven the requirement. The hardware is sometimes driving the rate, the amount, and the accuracy of the data that flows through the information systems to the point where the individual and the function in the system may be confused, inundated and/or mislead by the data.

The individual is characterized in figure 2. The technology can be viewed as the inputs and the outputs depicted. It is not suggested that research for better technology or hardware should not be continued, but rather that research directed to the individual and his function in the information flow set can no longer be ignored or short-changed. An example of the problems follows:

The Secretary of Defense (SECDEF) might come to me, if I were in the data processing business in the Pentagon, and ask, "What is the status of the 7th fleet?" I would run downstairs, retrieve data from the WWMCCS computer and report back to the SECDEF. "There are two task forces, one in the eastern Pacific and one in western Pacific. There are carriers in each task force. The carrier Oriskiny is C-1 and the JFK is C-2. Each task force has a destroyer flotilla and they are C-1 and the support ships are

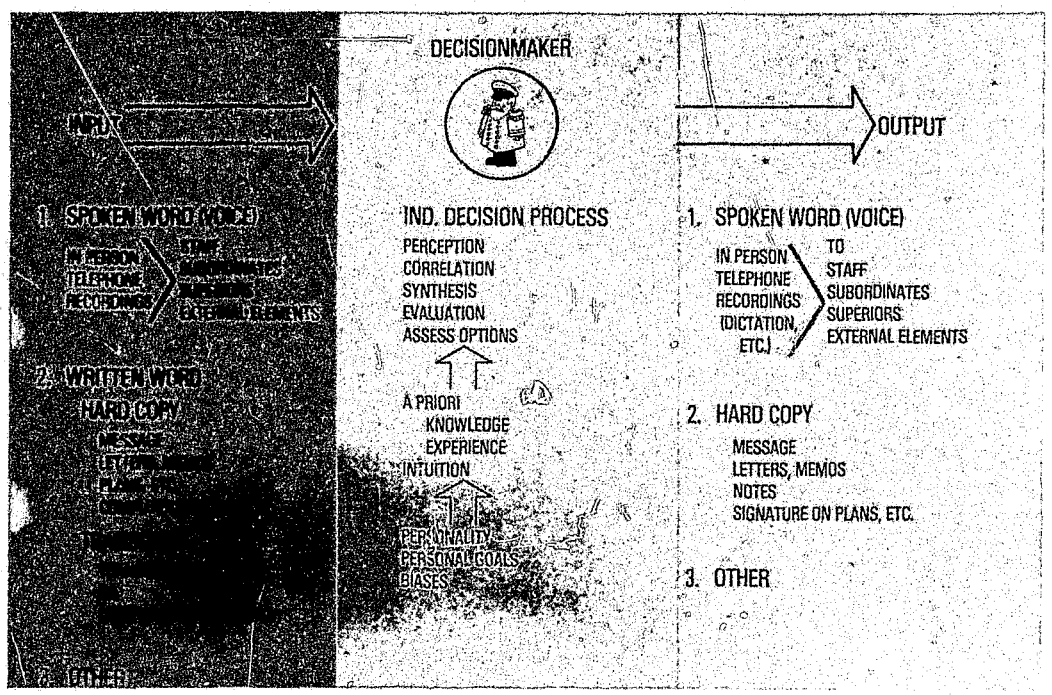


FIGURE 2. *C^3 decision theory single set.*

also C-1." The SECDEF might respond, "Gee, that's great! Where did you get the information?" "I got it out of the WWMCCS computer in the basement." "Expletive, you can do better that that, call CINCPAC in Hawaii and get the information from him."

This exchange happens more often than not and is indicative of an important institutional transfer problem. Technology does not always help! The tools required to improve the man/machine interface are not very effective in these cases. Why is this? Why doesn't the SECDEF accept this answer? His communications, ADP and facilities are currently the best we can provide! Yet he reacts the way his experiences, biases, training and motivations move him—whether or not this reaction is the way to obtain the best decisions.

Now, when CINCPAC is called to relay the SECDEF's question, three answers are likely: 1) the same answer given the SECDEF because CINCPAC's WWMCCS computer system, reporting system and communications links are more or less the same, 2) since CINCPAC has recently been testifying before Congress, defending the CINCPAC budget, the answer relates to this motivation, i.e., "The Soviet fleet is growing, my ships are more than 30 years old, the Pacific is a vast ocean area, etc., and the status of the fleet is lousy," 3) because he has been stumping to be the next Chairman of the OCS, the answer might be, "Despite the vast area of the Pacific, and the terrible equipment I have to operate with; and despite the growing threat, the status of the fleet never has been better." It is submitted that these latter two answers occur more often than the first. Why? Technological improvements currently shed little light on the reason why. We ought to be able to do better! The use of human factors technology may help.

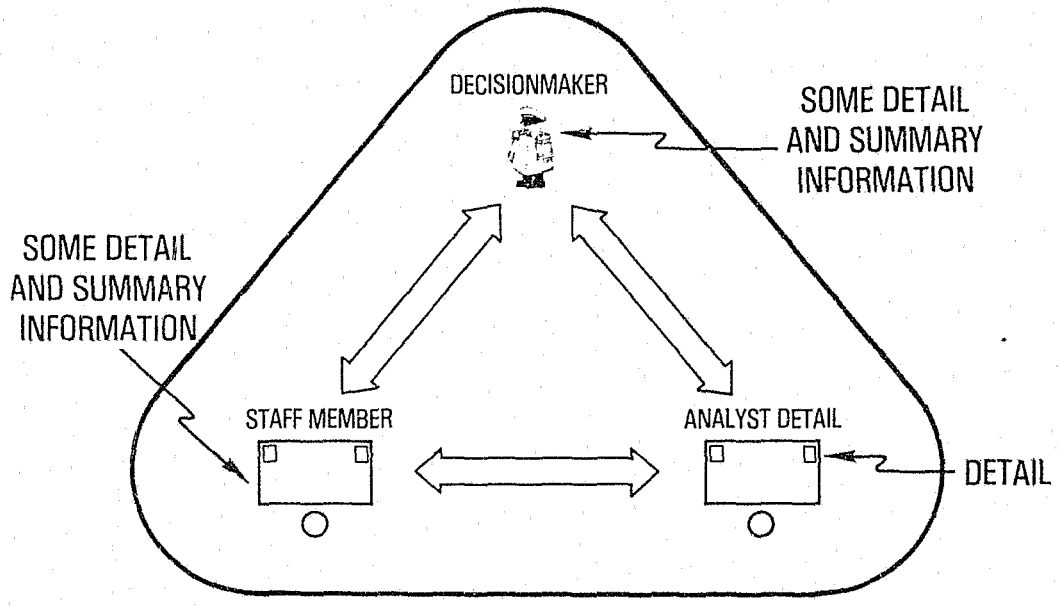


FIGURE 3. *C^3 decision theory multiple set.*

Figure 3 expands the single decision theory set to contain three individuals. It doesn't make any difference whether this is a management information system in industry, whether they're in a security system in the Defense Nuclear Agency, or in a high level White House situation.

Classically, they consist of three kinds of people. First, there is the decisionmaker (i.e., the commander, the manager, and/or the director). Second, there is the individual who treats raw information and data by collecting/gathering, making selections, compressing, summarizing and filtering it to a degree. Sometimes assessments are made, but supposedly, the person doesn't make decisions. For the sake of this paper let's call this person an intelligence analyst. Finally, there is the person who is like an operations staff officer in the military, but in any organization the one that sets the scenario/stage. This person determines whether things are normal, whether there's a crisis, when there's panic, whether and what staff have to work around the clock, or whether one works 4 hours a day. He/she asks and forms the questions. Using the assessment from the person manipulating the data, alternative answers/options are developed for the decisonmaker. The question is: who is really making the decision in this multiple C set? Is it the person who is working with the raw data? Is it the person who is forming the questions and the alternatives to the answer, or is it the person who finally makes the decision?

To make the point in a different manner, when one goes to the intelligence person in the set and asks him: "What's the status of the Seventh Fleet," he gets into the immediate role of indicating what has happened to the Seventh Fleet in the last 4 years. What have their routes been? What has the weather been at this time of the year? Where are they likely to go? What ports are they likely to visit? Can the sailors go on shore leave if they go to a certain port? What's the Middle East oil situation? Can they be refueled at port? Can they be refueled at sea?

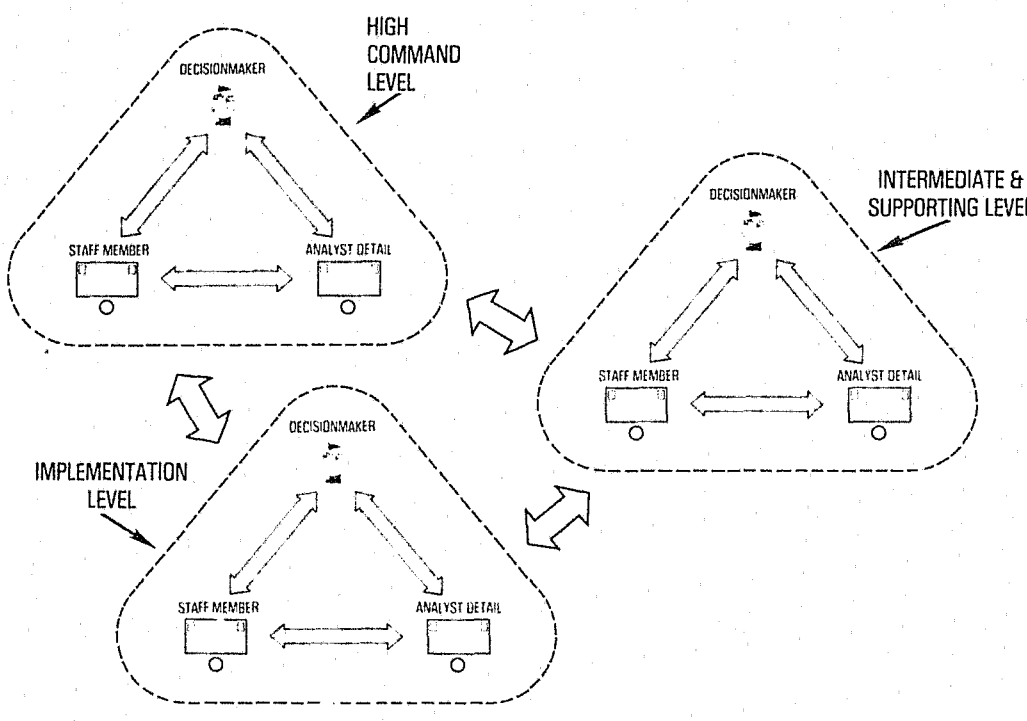


FIGURE 4. *C^3 decision theory hierarchical set.*

This may not be bad, but there's a very interesting systems application here. Is the system characteristic that we design for the intelligence analyst the same that we should design or might have desired for a decisionmaker? If the operations officer is asked: "What's the status of the Seventh Fleet?", he goes into a self-protective mode of operation. He gets more concerned with all the follow-on questions. He asks: "Why is the combat readiness status, C-2?" To the response of: "There were so many airplanes on the carrier that were not combat ready," he asks: "Are they ready for maintenance?" To the response of: "They need gear retraction tests," he asks: "Do they have retraction gear?" To the response of: "No, it has to be flown in with a helicopter," he asks: "What's the tail number for the helicopter and what's the time that it's going to be back into maintenance?" The operations type gets so involved with all the follow-on questions that the basic question: "What's the status of the Seventh Fleet" is forgotten. Perhaps it is the question that is wrong.

Shown in figure 4 is another interesting C^3 set, called the hierarchical set in which the same trained individuals, whether a decisionmaker, an intelligence analyst, or an operations person, each of the same rank, experience and training are placed at three different levels in the command chain, one at the national level, one at the commander-in-chief level, and one at a field level or unit. Now, ask them the question: "What's the status of your organization?"

All three individuals will treat, perceive, and respond differently to that question. Of greater importance, as we move to centralization of computer power and standardization of such equipment as displays, is the question of whether such centralization is realistic without a better understanding of the individual and his function. Should the same computers, communications and displays serve each of these individuals? Are the hierarchical levels of command proper? Too little attention is payed to these kinds of problems.

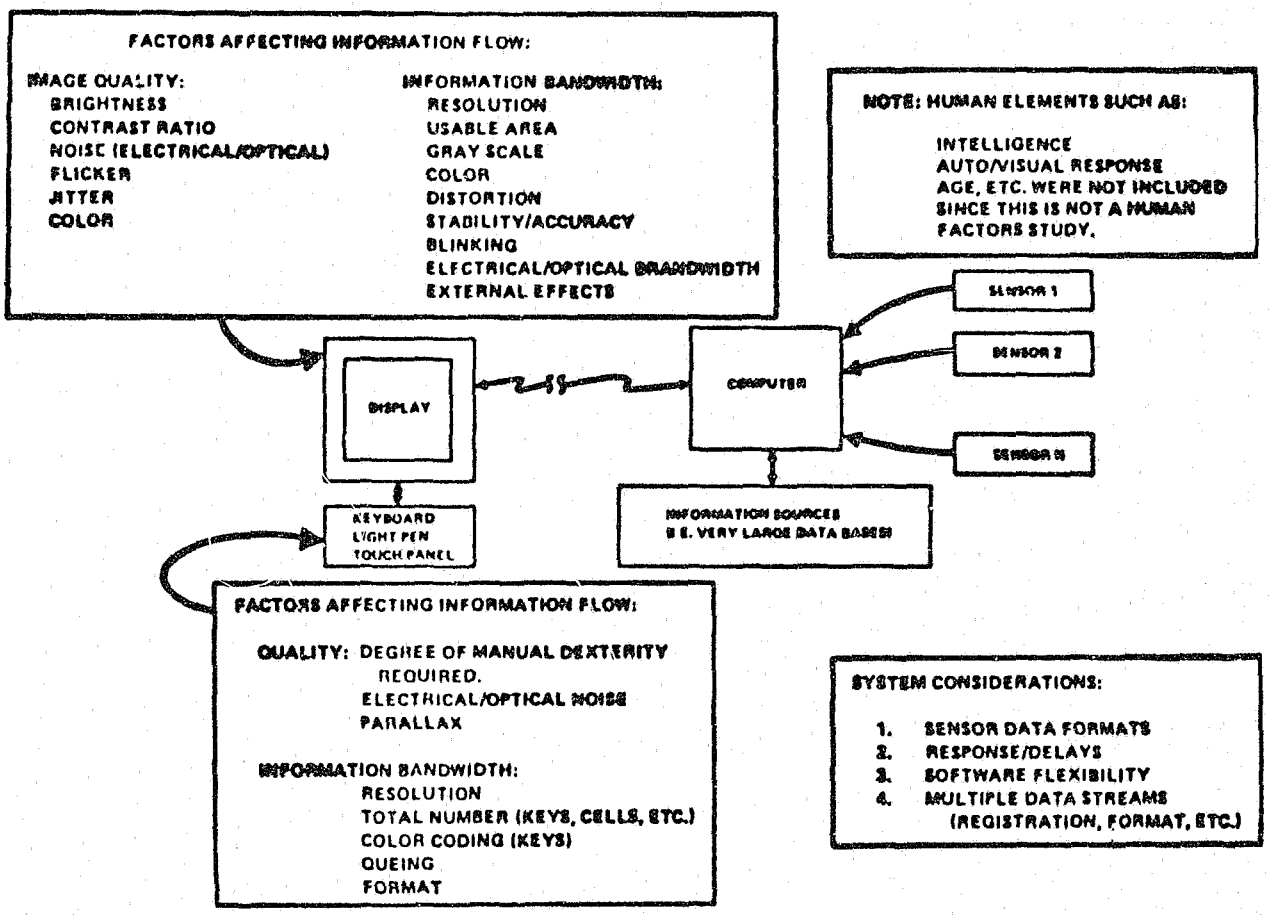


FIGURE 5. *Detailed man-machine interface model command and control displays.*

While somewhat out of context, figure 5 depicts an area in which we've been involved at Science Applications, Inc. (SAI). We've been building a large 25-in diagonal plasma panel gas discharge device for the Strategic Technology Office in the Defense Advanced Research Projects Agency (DARPA). Among the things which had to be done on this contract was a survey of the state-of-the-art in display technology (i.e., liquid crystal, light emitting diodes, cathode ray tubes, and free gas discharge devices). DARPA asked us: "What is the state-of-the-art today, and if we wanted a certain device in the future—through the year 2000—what technology can provide us that device?"

We went through that survey and came up with some answers. Tell us the brightness level desired and that reduced glare or glitter are wanted, and we can tell you what kind of a device will give you that capability. What we forgot is what does man need? What resolution and brightness criteria does he need? This hasn't yet been done to my knowledge.

SAI also has another interesting contract with DARPA, dealing with the role of the individual in a command center in a decision-theory process. Three tasks are involved. One is to do a comparative evaluation or an analysis of many command centers, looking at them from a human factors point of view. An example is that housewives in Sweden man their air defense radar sets. They do it at a much higher performing capability than U.S. airmen. Their fatigue and performance decrement

factors are much lower than those at similar sites in our country. In our country no one ever penetrates our air space, with few exceptions. The controllers get bored to tears; they hate their job; they're low ranking. They don't want to stay in their field. In Sweden, housewives who work 4 hours a day, 2 days a week, perform admirably.

Another task is to bring groups such as yourselves together to talk about the characteristics of a laboratory SAI is building. The final task is to conduct a series of mini-experiments. The following sections describe DARPA programs in human factors and biocybernetics.

The biocybernetics program, originally a 5-year program, is now a 3-year program. In addition there is a new 5-year Human Factors program in command and control. SAI will be involved in both of these programs. Some very interesting technologies are developing in the basic research. For those of you who know Manny Donchin at the University of Illinois, he's been using the P300 component of the electroencephalograph (EEG) evoked response to do some interesting work—predicting relevancy of information with interesting results. Using the electroencephalograph, and putting EEG electrodes on your skull, he can say whether you are confused or you're seeing relevant information.

Donchin is also modifying a link trainer so that if a flashing warning light comes on after placing a pilot in the trainer, he will be able to perceive the pilot's perception of that relevant rare event of the flashing, blinking light by means of this physiological measurement.

A long term application (15 to 20 years and beyond) of this EEG technology might involve interpretation of the pilot's perception of a blinking light to tell him that he's going through a prohibitive mach number; he's going to disintegrate. When this warning occurs, he is supposed to pull the throttle back, lower the gear and flaps and hit a couple of circuit breakers. He goes through maybe 12 items on his emergency checklist. If this is done in time, the catastrophy is averted. If the G-force prevents the corrective actions because he can't utilize his motor sensory capability, through the proper measurement of his P-300, he may be able to go through that checklist and perform those functions by converting the P-300 to computer driven actions. Figure 6 shows a normal, "nonrelevant" trace and the relevancy indication 300 msec after stimulus presentation.

Figure 7 relates to some interesting biocybernetics basic research going at UCLA. In this instance, the researchers have developed the ability to put electrodes on a man's skull and identify certain characteristic EEG signatures. For instance, one can characterize thinking right, left, up, down, on, off. Some very good signal characterization work is going on. An individual sits in front of a robot and thinks the robot through a maze. By thinking right, the EEG is transmitted in digital form to the driving computer. The robot raises its foot and turns to the right. It then walks on through the maze when appropriate EEG characteristic has been inputed. One other area of interesting work using evoked response measurements utilizing the EEG method is an attempt to characterize the semantic meanings of words.

Figure 8 reviews another area of EEG research. It is factually clear that the processing of linguistic information—like speech—is accomplished for the most part by the left hemisphere, at least for most right-handed individuals. An interesting experiment might be to present certain types of information to both hemispheres simultaneously. From EEG measurements, one might be able to discern improvements or confusion decrements in cognitive capabilities associated with such total—right and left hemisphere—processing.

Figure 9 depicts some interesting work going on in magneto-encephalograph (MEG) measurements. Whereas a main finding of the EEG work is the uniqueness of EEG signatures, and this uniqueness has promising applications in the safeguards areas, there is some evidence that EEG measurements on mice reveal group characteristics of

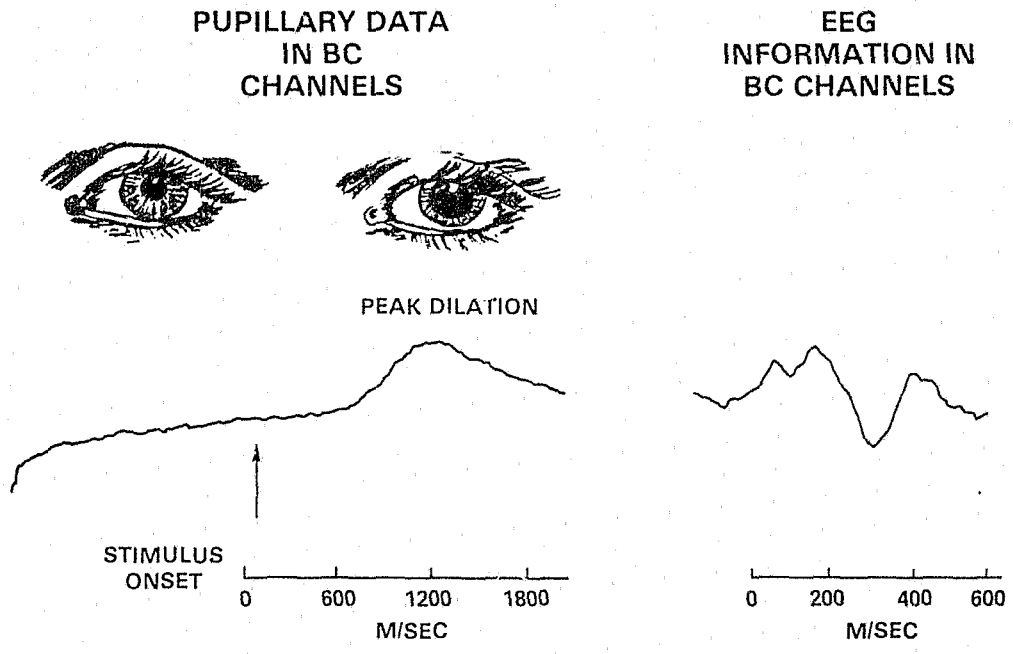


FIGURE 6. *The general concept of biocybernetic applications.*

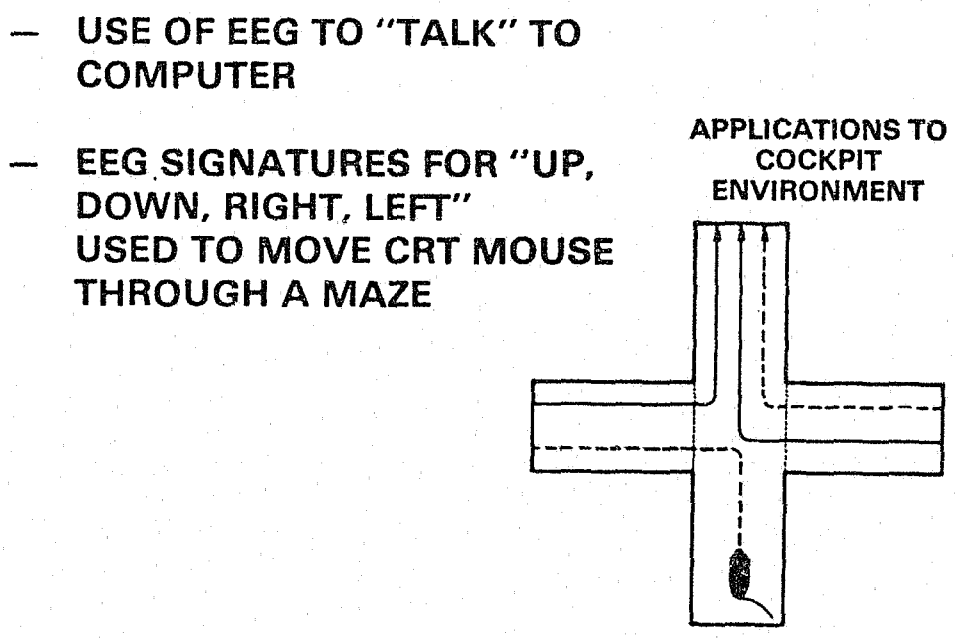


FIGURE 7. *UCLA Biocybernetics Research, D. Vidal.*

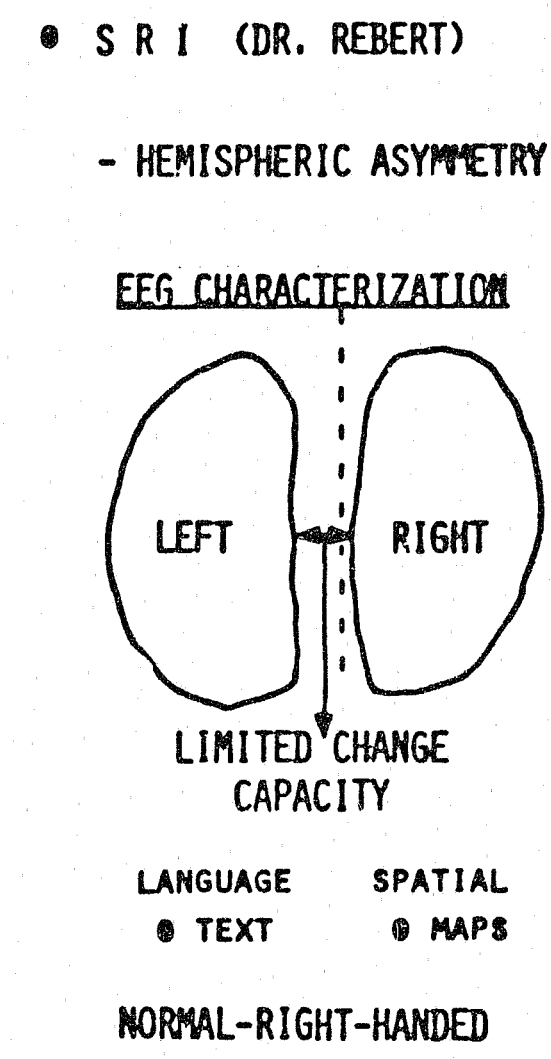


FIGURE 8. *DARPA Biocybernetic Program.*

° Magnetoencephalography - MEG
° Measurement emphasis
° Potential signatures

FIGURE 9. *MIT DARPA Biocybernetic Program (Dr. Cohen).*

the evoked response. If this characteristic proves to be repeatable and predictive, applications of this technique are truly exciting.

Figure 10 outlines a new program in human factors related to command and control. The program is sponsored by DARPA. SAI will be engaged in human factors mini-experiments.

Does the addition of a third, fourth or fifth color add to human cognition for specific decisionmaking functions? This question is typical of our scheduled experiments. In addition, Bolt, Beranek and Newman (BBN) and CACI have contracts in support of the human factors command and control program.

Figure 11 shows our laboratory. It has three rooms with good experimental stations. The computer room, using PDP 11/70's is rather respectable for the types of research that will be conducted.

From a human factors standpoint, if you were in the military, assigned a tour in a military command and control center, spent most of your life on either a destroyer or flying an airplane or in a tank, and then you advanced to a position of authority and responsibility involving building a command center, and someone came up to you and asked: "What kind of display do you want?," a typical answer might be the following: An individual in the Navy might say, "I want some plexiglass, and I want to write backwards." A person in the Army might say, "I want some butcher paper on a blackboard." And, an Air Force individual would say, "I want it three stories high, and it's got to be full colorgraphic and dynamic." Not quite that bad, but almost.

Again, the point is that we should be able to do better than that from a technological point of view. Displays with touch panels for retrieval and verbal retrieval may be one way to improve man-machine interactions. Equipment in the SAI laboratory will support these kinds of experiments. The equipment is ordered and should be delivered soon. Figure 12 identifies 10 of the 70 planned experiments. This summer's

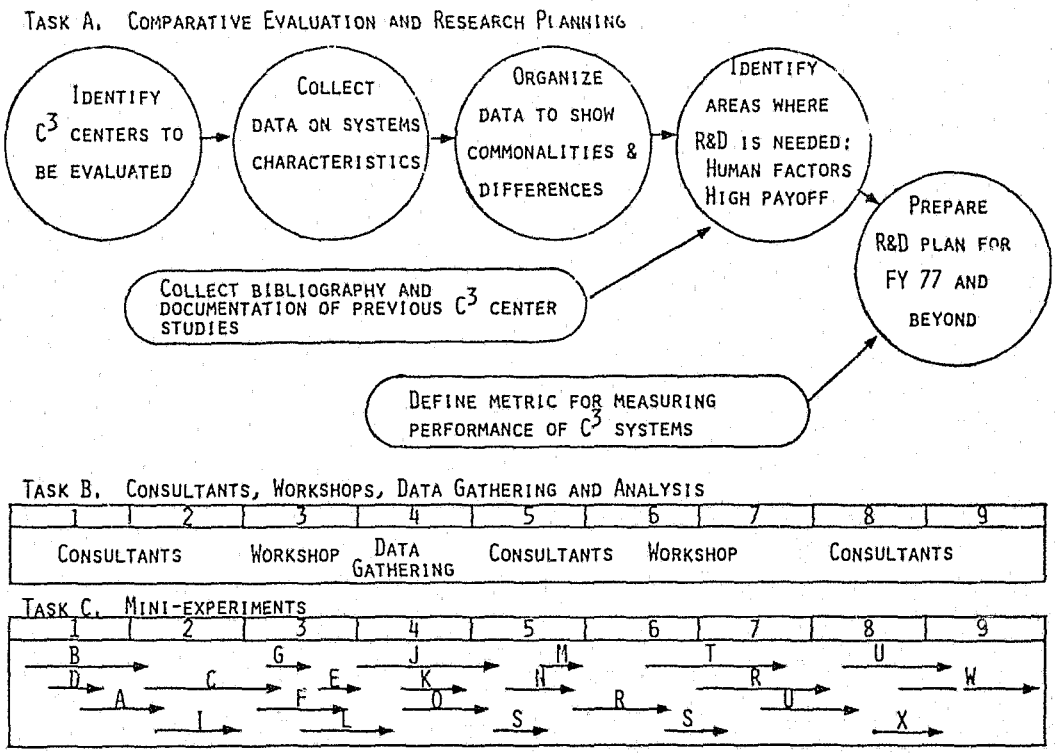


FIGURE 10. C^3 *analysis and research planning.*

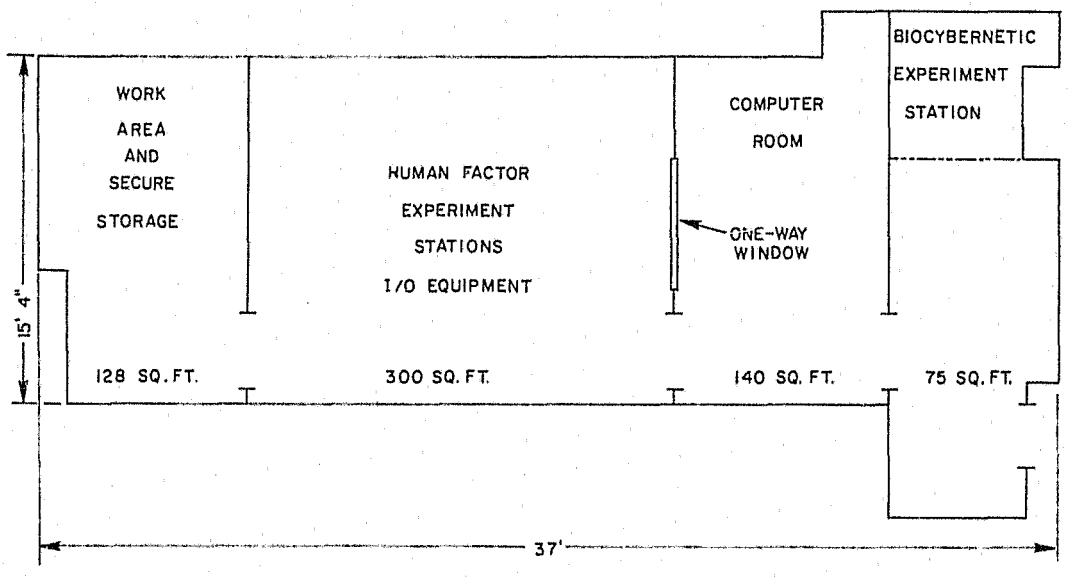


FIGURE 11. *SAI Human Factors and Biocybernetics Laboratory.*

activity will involve around 12 graduate students, and eight cognitive psychologists from the University of Maryland, Georgetown University and American University. These psychologists will be teamed with some information scientists, all doctoral candidates. These teams will act as independent researchers, conducting mini-experiments. From the 3 months' activity this summer, we'll take those experiments whose results look exciting and promising and we'll create longer term projects.

Going back to the biocybernetics side, many of the following concepts have been talked about by the preceding speakers in one form or another, but we would like to suggest a different context. We would like to do counter-intuitive experiments, which are aimed at reconsidering some general assumptions made over the last 20 or 30 years. Intuitive solutions are biased on certain parameters, but if the counter-intuitive research proves that we may have been wrong, the payoff would be extremely high. In this regard, two points should be made.

One concerns the use of color to provide information content on the decision theory side of displays. If all of the intuitive feelings we have, if all of the research has taught us that the red and yellow doesn't really provide the information we need, if there were some errors in previous experiments and we can now show that there are better ways to present data by using black and white or by some other technique like accessing through audibles, the savings to the government by providing black and white displays instead of color could be immense. Over a 10-year period, millions of dollars could be saved. This is what our counter-intuitive experiments are all about.

Second, we are concerned about fatigue and performance decrements. The inability to maintain a high state of alertness worries some of us. Some real-world experience I had with airborne controllers working 12-hour, on-station shifts in combat does not necessarily reflect the same kind of performance. It is possible that the type of functions being performed by the airborne controllers differ enough from the anti-submarine warfare (ASW) operators to make the comparison faulty. However, my observations indicate that controllers handling 600 sorties in a 12-hour period performed much better than controllers handling 20 or 30 sorties during a similar period. This low activity occurred when weather wiped out air-to-ground activities, for example. The fatigue decrements to me seemed more related to activity stimulation, rather than to stress.

Information dissemination
Individual decisionmaking
Advanced technology for group problem solving
Advanced technology for optimizing display design
Man–computer synergistics
C^3 Environmental factors
C^3 Performance evaluation methods
Improved information transfer
- ° Text comprehension
- ° Spatial memory
- ° Influence of context on memory
- ° Natural U.S. stylized language
- ° Highlighting

Improved data structures
- ° Personalized keys
- ° Personalized restructuring
- ° Spatial relationships

Data retrieval
- ° Using place memory techniques
- ° Using eye movement cues

FIGURE 12. *Areas Where R &D Is Needed*

Human factors research
- ° Optimal balance of sensory input channels for electronic guard console
- ° Security system credibility as a function of personal perspective
- ° Perceived criticality of signal absence vs. signal presence
- ° Adaptation effects during information overload

Biocybernetics research
- ° EEG manipulation of a security device
- ° Brain wave signatures as ID codes
- ° Covert alarm setting–eye movement
- ° Computer monitoring of guard's alertness
- ° Pupil dilation indicator of signal detection miss

Deception studies
- ° Nonverbal indicators of deception
- ° Qualities of deceptive verbalizations

FIGURE 13. *SAI Research Efforts Applicable to Physical Security*

Figure 13 suggests ways that human factors, biocybernetics and human engineering might help people concerned with security, protective forces and perpetrators. The problem in decision theory is that there's too much data available at a given moment. At least, too much that we don't know how to get in usable form to a decision maker, whether he be a commander, an intelligence analyst or an operations individual. In the past, problem solution has involved making computers bigger, faster, and more selective. Data have been compressed, performing top-down, structured program development. Better communications switching and sensors of all kinds have been provided. Hierarchical changes in organization, procedures and message formats have been attempted. However, too little has been done with tying the man into this whole sequence. How can the machine make him smarter than he is? What should the machine do? These are the filters we ought to worry about.

FINAL REPORT
JOINT SERVICES PERIMETER
BARRIER PENETRATION EVALUATION

Robert A. Fite and Stuart Kilpatrick

Evaluation & Application Division, U.S. Army Mobility Equipment Research & Development Command, Fort Belvoir, VA 22060

I. INTRODUCTION

The perimeter barrier penetration evaluation was divided into two separate evaluations. Phase I was conducted from 10 Dec. 74 to 24 Jan. 75 and was designed to determine how long various fence configurations could delay skilled, trained intruders, and also to examine various methods and procedures for penetrating fences and barbed tape barriers. The results of Phase I have been released in a report titled "Interim Report, Joint Services Perimeter Barrier Penetration Evaluation," and are also included in this final report.

Phase II was conducted from 3-26 July 1975 and was designed to verify the results of the Phase I evaluation in addition to determining the effectiveness of several new fence configurations that were designed as a result of the Phase I evaluation and also to determine the vulnerability of fences to explosive breaching techniques. During the Phase II evaluation new penetration aids and techniques were evaluated in an attempt to determine the minimum delay that can be expected from any fence configuration.

All of the non-explosive testing was accomplished at the MERADCOM outdoor perimeter test site located at the MERADCOM North Annex, Fort Belvoir, VA. The explosive testing was performed at Quantico Marine Base, Quantico, VA.

The Joint Services Perimeter Penetration Test was conducted by the Evaluation and Application Division of Lab 7000, MERADCOM in coordination with the Defense Nuclear Agency, Navy Material Command, and the National Bureau of Standards.

II. TEST OBJECTIVES

A. Primary Objectives

a. To determine the penetration time of skilled intruders against various standard and proposed barbed wire and barbed tape topped fences and barbed tape barriers.

b. To determine the difference in penetration time for various fence heights.

c. To determine the effectiveness of precast concrete sills to anchor the fence fabric.

d. To demonstrate the vulnerability of chain link fences to explosive breaching techniques.

B. Secondary Objectives

a. Observe whether enhancement of the perimeter fence with barbed tape degrades or improves the performance of the Fence Distribution Sensor (FDS) and other fence detection systems.

b. Determine the best procedures for installing the various barbed tape toppings.

C. Tertiary Objectives

Collect experimental data on the performance of developmental fence sensors of the BISS Program. This data will not be included in the written reports.

III. TEST FENCE DESCRIPTION

The test area consists of two parallel chain link fences separated by 50 feet with one fence 100 meters long and the other fence 300 meters long. Both fences were built to the Corps of Engineers Guide Specification CE-233, Fence Type FE-5 with various barbed wire and barbed tape toppings. Type FE-5 fence is a 7-foot-high chain link fence using 9-gauge, 2-inch mesh fabric attached to 2-3/8-inch steel posts set in concrete on 10-foot centers. In addition to the above fences, 30-foot sections of 6-foot and 8-foot-high fences and a 30-foot section of fence using 8-foot fabric on 7-foot posts so that 1 foot of fabric was above the top of the posts were also constructed. All fences were built with 9-gauge, 2-inch mesh fabric.

IV. INTRUDERS

The intruders were all active duty military personnel in good physical condition. Four men from the 437th MP Company, Fort Belvoir, VA, four men from the 5th Special Forces Group of the 1st Special Forces, Fort Bragg, NC and six men from the Marine Guard, Yorktown Naval Weapons Station, Yorktown, VA participated in Phase I of the test program.

None of the intruders were specifically trained to cross fence or barbed tape barriers, but most of them became very proficient after watching several training films and making a few practice intrusions. It was obvious that each individual intruder became more skilled and therefore made faster penetrations as the test progressed. Four men from the 5th Special Forces were the intruders for Phase II. Two of the four men had participated in Phase I and were already quite proficient. The two skilled intruders trained the two new men and therefore very little time was spent during Phase II for training purposes.

V. PENETRATION TEST RESULTS

A. General Comments

From a total of over 40 proposed fence configurations, 20 were selected for evaluation. In addition to the 20 selected fence arrays, various methods of stabilizing the bottom edge of the fence fabric, such as staking it to the ground, attaching it to buried, precast concrete sills, or anchoring it in poured concrete sills were also evaluated. Slight variations of some of the 20 selected arrays such as different methods of attaching or positioning the barbed tape on the fence, were also evaluated. The data is not shown separately for each variation of a basic fence array if there was no significant difference in penetration times.

The penetration test results are divided into the following four categories:

a. Climbovers
b. Penetrations under the fence fabric
c. Penetrations thru the fence fabric
d. Ladder assisted jumpovers

Unless otherwise noted, only one intruder penetrated the barrier during each test, although he might have been assisted by one to three other men who did not cross the barrier. In some cases the assistant(s) did nothing except throw a 20-pound pack over the fence. The pack simulated the weight of the anticipated material the intruder would

require to complete his mission after he crossed the perimeter barrier. Although the 20-pound pack was used for each intrusion in Phase I, it was observed that its use did not significantly increase the total penetration time, and therefore was not used in Phase II. Each intrusion attempt was started 30 feet from the fence and ended 30 feet on the other side of the fence to simulate a 30-foot clear zone on each side of the fence. Two times were recorded for each intrusion—the penetration time and the total time. The penetration time is the time from when the first man in the penetration team touched the barrier until the intruder(s) cleared the entire barrier. The total time is the penetration time plus the time required for the intruder(s) to cross the 30-foot clear zone on each side of the barrier.

Before each penetration attempt the intruders were told whether they had to go under, over, or through the fence and what aids they would be allowed to use. In most cases they were not told specifically what aids they could or could not use but were given only general guidelines, such as limited or unlimited aids. Limited aids were defined as anything that could be easily carried on their person such as cutters, wire hooks, canvas sheets, steps, etc. Unlimited aids were defined as bulky items such as ladders, sheets of plywood, rolls of carpeting, etc. The aids used in this test are described in table 1. All aids had to be carried across the first 30-foot clear zone but were left at the fence if they were no longer needed.

B. Climbovers

The fence arrays are listed in table 2, and the data for climbovers is shown in tables 3-5 and figures 19-37. The climbovers can be conveniently divided into two categories—limited aids and unlimited aids. The various aids used are listed in table 1 and the application of some of them is shown in figures 4-6 and 9-11. As shown in tables 3 and 4 the fastest penetration times for fences were usually achieved with the simpler aids. For fences without barbed tape toppings the fastest penetration times were achieved with no aids, but the use of aids generally improved the penetration times for barbed tape topped fences. The fastest penetration times for barbed tape topped fences were achieved when a piece of carpeting was thrown over the fence as shown in figure 8. The carpet was made by nailing the end of 4-foot-wide by 15-foot-long piece of heavy carpeting to a 5-foot-long 4x4 and then rolling the carpet around the 4x4. For some of the shorter fences two men could simply throw the rolled carpet over the fence, but for the taller fences they could not clear the fence and had to use two 8-foot-long 2x2's with a nail in one end to lift the carpet roll over the fence and drop it on the other side while a third man held the loose end of the carpet. Another method used to get the carpet over the fence was for the intruder to carry the rolled carpet up a ladder and toss it over the fence while another person held the loose end of the carpet. Using the carpet as described above it took the intruders only a few seconds more to penetrate the more complex fences than the time required to climb the simpler fences with only barbed wire toppings.

When only limited aids were allowed against barbed tape topped fences the most efficient aids were hooks to hold the barbed tape out of the way. The canvas sheet thrown over the barbed tape was not effective because it was too thin to provide adequate protection from the barbed tape.

Table 5 shows that for the combination barbed tape/fence barriers (arrays 25, 26, 27) the use of unlimited aids, such as sheets of plywood, considerably reduced the penetration times. The greatest reduction occurred for fences that had rolls of barbed tape on the inside (arrays 26 and 27) because the intruders could drop a sheet of plywood over the fence, as shown in figures 5 and 6, so that it landed on the barbed tape, and then jump from the fence to the plywood. Without the plywood over the barbed tape the intruder had to carefully climb down the inside of the fence and step

into the barbed tape to prevent getting entangled in it. Although it was not tried, a piece of carpeting thrown over the rolls of barbed tape would probably have been just as effective as the plywood against the combination barriers.

It is obvious that for some fence configurations the use of a ladder would have shortened the penetration time, but for these tests the ladder was used only to demonstrate the feasibility of jumping over the fence without activating any fence alarm systems. Table 9 compares the penetration times of climbovers with limited and unlimited aids for various fence configurations.

As can be seen from tables 4 and 5 when the barbed tape was cut from the top of arrays 14, 17, and 25 the penetration times were generally longer than for the other climbovers because of the difficulty of cutting the barbed tape and barbed wire, but as figures 7 and 10 show the barbed tape fell away from the fence and made the climbover easier and safer. For most arrays with a combination barbed wire and barbed tape topping the barbed tape was fastened only to the barbed wire and therefore when both the barbed tape and barbed wire were cut the whole topping would fall away from the fence. During Phase II a 30-foot section of array 17 was installed using modified "Y" brackets that allowed the barbed tape to be fastened to the top of the fence fabric. There was no significant difference in the penetration times between the two different installation methods.

Table 9 ranks all of the fence arrays tested in order of the time required to climb them. After the completion of the Phase I evaluation behavioral scientists from the National Bureau of Standards asked the intruders to rank the fences in order of difficulty to climb. Their rankings are shown in appendix A and compare very well with the rankings shown in table 9.

A factor that had considerable influence on the penetration times was the skill level of the intruders. The longest penetration times generally occurred early in the penetration attempts and were greatly improved upon when the same intruders attacked the same fence after they became more proficient. Also, as the intruders attempted to penetrate new barriers their first attempts were slower because they had to experiment to find the easiest method of attack. During Phase II selected fence arrays from Phase I were retested using the same penetration methods, and in all cases the penetration times were faster due to the improved skill of the intruders.

Each intruder made no more than seven climbovers per day and usually five or less, so fatigue did not become a signficant factor in the penetration times.

Although most climbovers were made using assistants that did not cross the fence it was observed that for fences without barbed tape toppings there was no signficant difference in the penetration times between assisted and unassisted penetrations because the assistant can only throw the pack over the fence or give the intruder a boost. A skilled intruder can make a faster penetration using his own momentum to vault over the fence rather than being boosted by another person. For the barbed tape topped fences the assistant(s) did improve the penetration times because they could help hold the barbed tape out of the intruder's way and thus make the penetration easier and safer. When bulky aids, such as sheets of plywood, ladders, pieces of carpeting, etc., were used the assistant(s) made a signficant reduction in penetration times and in some cases were indispensible.

C. Penetrations Under the Fence Fabric

The data for penetration under the fence is shown in table 6. To go under the fence, the intruders simply pushed a 10-foot-long pipe or 2x4 under the fence fabric and lifted it high enough to allow a person to crawl under. Going under the fence has the advantage of allowing the intruder to maintain a low profile and thus minimize the chance of being apprehended. As can be seen from table 6 the time required to go

under a fence is only slightly longer than the time required to climb a fence without a barbed tape topping but is significantly shorter than the time required to climb a fence with a barbed tape topping when only limited aids are used. It requires a minimum of two persons for a single intruder to get under the fence using this method, but once the fence fabric is lifted up any number of people can crawl under. Adding a bottom rail to the fence approximately doubles the penetration time because it forces the intruders to use two 10-foot pipes to lift the fence fabric. The first pipe is pushed through the fabric above the rail and is used to lift the fabric high enough to put the second pipe over the bottom rail but under the fabric and lift the fabric high enough to allow a person to go over the rail and under the fabric. Attaching barbed tape to the fence along the bottom edge of the fabric has little effect on the penetration time. If a single pipe is used to lift the fabric the penetration time is greater because the intruders have to use wire hooks to pull up the barbed tape and fasten it to the fabric. There is no increase in penetration time if two pipes are used to lift the fabric so that the intruder can crawl under the fabric between the two pipes.

A 30-foot section of fence with two pieces of fence fabric fastened to the outside of the fence posts and a 30-foot section of fence with a piece of fence fabric attached to each side of the fence posts were constructed to determine if this type of fence could increase the penetration times. The double fabric did not hinder the intruders from penetration under the fence fabric. The penetration time for the section with both pieces of fabric on the outside of the posts was greater because there was a slight rise in the ground inside the fence that made it difficult to push the pipes under the fence.

Precast concrete sills designed by the Corps of Engineers were installed along a 30-foot section of fence. Each sill is 8-1/2-feet-long, 10 inches high and 3 inches wide and has nine 3-inch-long reinforcing rods protruding from one side of the sill. Each sill was buried along the outside of the fence, between the posts, with approximately 3 inches of the sill above ground and the reinforcing rods through the fabric so that they could be bent around the fence fabric to securely anchor the fence fabric to the sill. The sills effectively stopped penetrations under the fabric because it takes considerably longer to free the fabric from the sills than it does to cut a man-size opening through the fabric or climb over the fence.

Anchoring the fabric in concrete would obviously make it impossible to go under the fence and would force the intruder to cut through or go over the fence.

D. Penetrations Through the Fence Fabric

The data for penetrations through the fence fabric is shown in table 7. After using several different sizes of bolt and wire cutters to cut the fence fabric it was found that the small 14-inch bolt cutters were the easiest and fastest. Tin snips were more effective than bolt cutters against the barbed tape.

Cutting through the fence has the obvious advantage of allowing the intruder to maintain a low profile and also does not require any assistance. Cutting through the fence takes longer than climbing a fence without a barbed tape topping but requires less time than climbing most fences with barbed tape toppings when only limited aids are used. Cutting through the fence requires more time than lifting the fabric and going under the fence.

If the bottom of the fence fabric is not securely anchored it takes only a single row of approximately 12 to 15 cuts to make a man size opening because after the fabric is cut it can be simply pushed back to form an inverted "V" opening. Anchoring the fabric in concrete approximately doubles the cutting time because the intruder is forced to make a double row of cuts to provide a large enough opening.

With a bottom rail attached to the fence it takes slightly longer to cut through because several more cuts are required to get over the rail. When a roll of barbed tape

is attached to the bottom of the fence fabric the easiest method of cutting through is to cut an inverted "V" in the fabric and then push the fabric down over the barbed tape. This takes slightly longer than cutting through fence fabric anchored in concrete. Three rolls of 24/30 barbed tape attached to the outside of the fence fabric (array no. 38) only slightly increased the penetration time because an assistant could simply pull the bottom roll up and out of the way while the intruder cut through the fabric. When the bottom roll was staked to the ground there was a significant increase in the penetration time because the barbed tape could not be moved and had to be cut out of the way.

A 30-foot section of fence with two pieces of fabric fastened to the outside of the fence posts and a 30-foot section with a piece of fabric attached to each side of the fence posts were constructed in an attempt to increase the amount of time required to cut through the fence. As expected, the penetration times were approximately double the times for a standard fence. When these special fence sections were anchored in concrete the penetration times did not increase significantly because two men cutting the fence simultaneously could make the required double cut in approximately the same amount of time as required for an intruder to make a single cut in the unanchored fence. There was no signficant reduction in penetration time when two people attempted to make a single cut in an unanchored fence because they tended to get in each others way.

E. Ladder Assisted Jumpovers

The data for the ladder assisted penetrations is shown in table 8. Using a step ladder to jump over the fence takes slightly longer than climbing the barbed wire topped fences but is considerably shorter than climbing most barbed tape topped fences using only limited aids. Using a ladder has the advantage of allowing an intruder to clear the fence without touching it and therefore not activating any fence sensors, although it does take one or two people to assist with the ladder. The 7-foot step ladder used in these tests was not of sufficient height for all of the fence arrays tested, but if a taller ladder had been used any of the fence arrays could have been cleared. With several rolls of barbed tape around the fence an intruder probably could not jump far enough with a step ladder to clear the barbed tape and would therefore need a more sophisticated arrangement such as shown in figure 11. This aid, made by hinging together the two sections of an extension ladder, allowed four intruders to cross the fence and three rolls of barbed tape in less than 5 minutes. Such an arrangement is cumbersome and easily detected by visual observation but it does allow the intruders to clear a barrier without activating any sensors that are attached to it. Another method of jumping over the fence without setting off any fence alarms was devised by the intruders. Two men crouched down with a 5-foot-long 2x4 held slightly above their heads while a third man balanced himself on the 2x4. The two men then stood up and lifted the 2x4 over their heads so that the intruder could jump over the fence. This method eliminates the need to carry cumbersome ladders to the fence, but cannot be used on taller fences.

VI. SENSOR PERFORMANCE

Sensor performance was not part of this evaluation but four types of fence sensors were already on the fence and were observed during all testing. A two count FTS was installed along the entire length of both fences and gave at least one alarm for every penetration except the ladder assisted jumpovers where the intruders did not touch the fence. Ten Air Force FDS sensors and 10 Inertiaguard Sensors were installed along a 100-foot section of the 100-meter fence. The Inertiaguard also detected every penetration except the ladder assisted jumpovers, but the FDS failed to detect cutting

through the fence in addition to missing the jumpovers. The MBT detected all aggressive penetrations but could be easily defeated.

The more complex fence configurations take the intruders a long period of time to penetrate and therefore increase their probability of being detected by fence sensors. During the Phase II testing an effort was made to defeat the sensors. The Inertiaguard and FDS were defeated by stripping the interconnecting wires and shorting out several sensors. This could be overcome by installing all wiring in conduit. An attempt was made to defeat the FTS by cutting the cable off the fence, but was not successful. The MBT could be defeated by attaching hooks to the fence fabric so that the sensor wires were not moved during the penetration attempt. This problem might be solved by adding sensor wires and switches above the fence fabric.

VII. EXPLOSIVE BREACHING

An 80-foot section of fence array 17 and a 70-foot section of fence array 5 were built at Quantico Marine Base to determine the vulnerability of chain link fences to explosive breaching techniques. The test can conveniently be divided into two categories—hand emplaced explosives and rocket and bazooka attacks. Marine Corp personnel performed all of the explosive work.

A. Hand Emplaced Explosives

Three basic types of explosive charges were used against the fences—bangalore torpedos, satchel charges and detonation cord. Figures 13-18 show the placement of typical charges and the results. As can be seen from the figures, the bangalore torpedo was the most effective device and was tested in three different positions. It was pushed through the fence fabric, placed along the bottom of the fabric, and fastened to a fence post. The charges placed through the fence fabric were the only ones that completely severed the fence. With the fabric anchored in concrete the bangalore torpedo placed through the fence completely took out the fabric between two fence posts, but when placed through the fabric of an unanchored fence it cleared a 30-foot section of fabric but did not take out the fence posts.

As shown in figure 17 a 20-pound satchel charge placed approximately 2 feet from the top of the fence did not completely sever the fence, but had it been placed slightly lower it might have been more effective. Two 10-pound satchel charges placed approximately 2 feet from the top and bottom of the fence fabric were more effective but again did not completely sever the fence fabric.

A chain of ten 2-1/2-pound blocks of C4 strung together with detonation cord was thrown over the fence and barbed tape topping as shown in figure 18. This was very effective except that the block of C4 closest to the bottom did not detonate and as shown in figure 18B did not sever the bottom of the fence fabric.

Various amounts of detonation cord was woven through the fence fabric, wrapped around fence posts, and attached to the fabric, but none of these tests were effective and did little more than bend one fence post.

B. Rocket and Bazooka Attacks

A number of light anti-tank assault weapons and 3.5-inch bazooka rounds were fired at the fence. As shown in figure 12 they were all relatively ineffective as they only made a 2 to 3-foot-diameter hole in the fence fabric.

VIII. BARBED TAPE INSTALLATION METHODS

The easiest installation method for the 18-inch barbed tape was for one person to hold the coil of barbed tape and pull it out as necessary while a second person attached it to the fence with stainless steel ties.

Two different installation methods were tried for the 24/30 barbed tape. For the first method the coil of barbed tape was stretched out on the ground. A long pipe was put through the entire length of the barbed tape so that it could be hoisted to the top of the fence with a crane mounted in the pickup. This method was only attempted using a 30-foot length of barbed tape and proved to be quite awkward. With the proper equipment this method might be easier. The second method tried also consisted of stretching out the coil of barbed tape on the ground and then six or seven people, each equipped with an 8-foot-long 2x2 with a nail in one end, and equally spaced along the length of the barbed tape lifted the entire roll of barbed tape and dropped it between the strands of barbed wire on top of the fence. This method proved to be the fastest and easiest of the two methods tried. After the barbed tape is in place it is secured to the top strands of barbed wire with stainless steel tie wires. A third method that was suggested but not tried was to build a platform on a truck so that a person standing on the platform would be directly above the fence and could simply dispense the barbed tape as the truck proceeded along the fence.

When the barbed tape is attached to the barbed wire in standard "Y's" on the fence there is a gap between the top of the fence fabric and the bottom of the barbed tape. A 30-foot section of fence was constructed using modified "Y's" that had been spread to form an angle of approximately 120° so that the barbed tape could be fastened to the top of the fence fabric and the barbed wire. There was no difference in the penetration time with the modified "Y's."

IX. CONCLUSIONS

A. General

a. A fence should not be considered a barrier, but should be used primarily to define legal boundaries.

b. Sensors or visual observation should always be used in conjunction with a security fence.

c. The addition of barbed tape to the fence makes penetration more difficult and time consuming and therefore increases the probability of detection of fence sensors.

d. Barbed wire and barbed tape toppings on fences equipped with fence sensors must be carefully and securely installed to prevent an increase in wind related false alarms.

e. The use of a ladder to jump over the fence defeats fence sensors and could be used to defeat buried or above ground line sensors if their exact location were known.

f. Some barbed wire and barbed tape toppings provide a psychological deterrence to the untrained or unskilled intruder; however, the trained intruder will select the appropriate aids and techniques and will not be deterred or signficantly delayed by the addition of barbed wire or barbed tape.

B. Climbovers

a. A standard 7-foot chain link fence with or without barbed wire topping provides only a 2 to 5-second delay against trained intruders.

b. Addition of 18-inch or 24/30 barbed tape to the fence increases the delay time to 7-54 seconds for intruders using only limited aids, but only increases the delay time to 5-10 seconds for intruders using unlimited aids.

c. The addition of barbed tape obstacles around the fence increases the delay time to 44-98 seconds.

d. The difference in penetration times for 6-, 7-, and 8-foot-high fences with no topping was insignificant.

C. Penetrations Under the Fence

a. Penetrations under the fence are difficult to detect visually because the intruders are able to maintain a low profile, there is very little damage to the fence to indicate the point of entry, and the time required to complete the penetration is very short.

b. Anchoring the fence fabric in concrete eliminates penetration under the fence.

c. The use of precast concrete sills to secure the bottom of the fence is a very effective deterrent because it takes considerably less time to cut through or climbover the fence than it does to free the fence from the sill and go under the fabric.

d. A bottom bar does not provide a significant increase in penetration time.

e. Using two pieces of fence fabric on single fence posts does not increase the time required to penetrate under the fence.

D. Penetrations Through the Fence

a. Penetration by cutting through the fence allows the intruder to maintain a low profile and provide an easy exit route upon completion of the mission, but clearly marks the point of entry.

b. Anchoring the fence in concrete approximately doubles the time required to cut through the fence.

c. Using two pieces of fence fabric on single posts approximately doubles the time required to cut through the fence.

E. Explosive Breaching

a. Explosive devices provide a large opening in the fence but obviously alert the reaction force.

b. Bangalore torpedos appear to be more effective and easier to place than satchel charges or other charges placed on the fence.

c. Detonation cord alone is not effective.

d. Rocket or bazooka rounds provide only a 2 to 3-foot-diameter hole in the fence.

TABLE 1. *Penetration aids*

Item	Description	How used
Canvas sheet	6' x 8' folded canvas sheet	Thrown over top of fence to aid climbing.
Cutters	Bolt cutters, wire cutters, or tin snips	To cut fence fabric, barbed wire, or barbed tape.
Steps	18" long iron rods bent to form a step	Hooked into fence fabric and used as steps to aid climbing. (See figs. 4 and 6.)
Wire hooks	6" to 12" pieces of stiff wire bent into hooks	To hold barbed tape to fence to aid climbing. (See figs. 4, 5 and 6.)
Long hooks	3' long rods bent into hooks	To pull down barbed tape toppings to aid climbing. (See fig. 9.)
Ladder	7' step ladder	To jump over fence. (See fig. 10.)
Extension ladder	20' extension ladder hinged in the middle to form an "A"	To crossover combination barbed tape/fence barriers. (See fig. 11.)
10' pry bar	10' 2x4 or 10' piece of 2" pipe	To lift fence fabric so intruder can crawl under fence.
Plywood	4' x 8' sheet of 3/8" plywood	To put over barbed tape barrier to aid crossing. (See figs. 5 and 6.)
Carpet	4' wide x 15' long piece of heavy carpet rolled up on a 5' long 4x4	Thrown over fence to aid climbing. (See fig. 8.)
2x2s	Two 8' long 2x2s with a nail in one end	Used to lift carpet roll over fence.

TABLE 2. *Fence arrays*

Fence Array No.	Fence height	Topping or enhancement
1	7′	None
2	7′	45° outriggers supporting 3 strands of barbed wire and pointing to outside of perimeter
2A	7′	45° collapsible outriggers supporting 3 strands of barbed wire and pointing to outside of perimeter
4	7′	45° outriggers supporting 3 strands of barbed wire and pointing to inside of perimeter
5	7′	"y" bracket supporting 6 strands of barbed wire
6	7′	"A" bracket supporting 5 strands of barbed wire
8	7′	Single roll of 18″ barbed tape attached to top, outside edge
14	7′	Array No. 2 with single roll of 18″ barbed tape attached to barbed wire
17	7′	Array No. 5 with roll of 24/30 barbed tape attached to the barbed wire
18	7′	Array No. 8 with a roll of 18″ barbed tape attached to the bottom, outside edge of the fabric
20	7′	Array No. 8 with a roll of 18″ barbed tape attached to the outside center of the fabric
25	7′	Array No. 17 with 4 rolls of 24/30 barbed tape laid on the ground outside and parallel to the fence
26	7′	Array No. 8 with 3 rolls of 24/30 barbed tape laid on the ground inside and parallel to the fence
26-25	7′	Arrays 26 and 25 spaced 50′ apart with array 26 to the outside
27	7′	Array No. 8 with 3 rolls of 24/30 barbed tape laid on the ground on each side of the fence
36	7′	Array No. 6 with 2 rolls of 18″ barbed tape attached to the top strands of barbed wire
37	4′	5 rolls 24/30 barbed tape, 20 rolls high, 2 rolls deep with 5th roll in center and and supported on each side with a 4′ high, 2 strand barbed wire fence
38	7′	Array No. 17 with 3 rolls of 24/30 barbed tape fastened to the outside of the fence fabric
42	6′	None
43	8′	None
44	8′	7′ posts with 8′ fabric so that 1′ of fabric extends above the posts

CONTINUED

1 OF 2

TABLE 3. *Barbed wire topped fence climbovers*

Array no.	Aids (see table 1)	No. men assisting but not crossing barrier	Fastest penetration time[1] (seconds)	Average times		
				Penetration time[1] (seconds)	Total time[2] (seconds)	No. of attempts
42	None	1	1.5	2.8	7.9	5
1	None	1	2	5.7	11.6	10
1	Canvas	1	6	9.8	15.1	6
43	None	1	4	4.7	8.9	4
43	Carpet	3	6	6.0	11.0	1
44	None	3	2.5	3.8	8.3	2
44	Carpet	3	7.0	7.0	14.0	1
2	None	1	4	4.3	9.7	3
2A	None	1	4	8.7	14.7	3
4	None	1	5	6.3	10.7	3
5	None	1	4	7.3	13.7	3
5	Steps	1	12	12.0	16.0	1
6	None	1	5	5.0	8.0	1
6	Steps	1	7	9.0	15.0	2

[1]Penetration time is the time for one man to cross the barrier.
[2]Total time is the penetration time plus the time to cross a 30 ft clear zone on each side of the barrier.

TABLE 4. *Barbed tape topped fence climbovers*

Array no.	Aids (see table 1)	No. men assisting but not crossing barrier	Fastest penetration time[1] (seconds)	Average times		
				Penetration time[1] (seconds)	Total time[2] (seconds)	No. of attempts
8	Wire hooks	1	16	16.0	22.0	2
8	Steps-canvas wire hooks	1	22	31.0	37.7	4
8	Carpet	3	5	5.0	11.0	1
14	Long hooks	2	10	10	17	1
14	Long hooks cutters	1	15	15	24	1
17	Long hooks	2	54	54	62	1
17	Long hooks steps	2	34	34	39	1
17	Long hooks steps-cutters	2	52	66	72.5	2
17	Carpet/2x2s	3	7.0	8.4	16.3	4
17	Carpet/ladder	3	9.5	9.5	15.0	1
38	Carpet	3	5.5	5.5	13.0	1
36	Long hooks	1	7.0	7.0	11.8	2
36	Carpet	3	4.5	5.8	9.8	2

[1]Penetration time is the time for one man to cross the barrier.
[2]Total time is the penetration time plus the time to cross a 30 ft clear zone on each side of the barrier.

TABLE 5. *Barbed tape/fence barrier climbovers*

Array no.	Aids (see table 1)	No. men assisting but not crossing barrier	Fastest penetration time[1] (seconds)	Average times		
				Penetration time[1] (seconds)	Total time[2] (seconds)	No. of attempts
27	Wire hooks steps	1	98	98	100	1
27	Wire hooks steps-plywood	3	55	55	62	1
26	Wire hooks steps	1	44	44	55	1
26	Wire hooks steps-plywood	3	25	32.0	38	2
25	Long hooks steps	3	50	50	57	1
25	Long hooks ladder-plywood	3	44	40	52	1
26-25	Plywood-ladder steps-cutters[3]	2	104	104	110	1

[1]Penetration time is the time for one man to cross the barrier.
[2]Total time is the penetration time plus the time to cross a 30 ft clear zone on each side of the barrier.
[3]Two men over both barriers.

TABLE 6. *Penetrations under fence fabric*

Bottom configuration of fence fabric	No. men assisting but not crossing	Aids (see table 1)	Fastest penetration time[1] (seconds)	Average times		
				Penetration time[1] (seconds)	Total time[2] (seconds)	No. of attempts
Tension wire	1	10' pry bar	7	7.3	14.0	3
Tension wire[3]	0	10' pry bar	11	14.6	21.2	5
Fabric staked to ground	1	10' pry bar	7	8.0	14.0	2
18" GPBT on bottom of fabric	1	Wire hooks 10' pry bar	28	28	32	1
Bottom rail	2	Two 10' pry bars	18	18	24	1
Fabric on each side of post-single tension wire	2	Two 10' pry bars	5	5.0	10.0	1
2 fabrics on same side of posts-single tension wire	2	Two 10' pry bars	14	14.0	19.0	1
3 rolls 24/30 GPBT on outside of fabric	2	Two 10' pry bars	5	5.0	10.0	1
Precase concrete sill	3	Two 10' pry bars & crowbar	76	76	80	1
5 rolls 24/30 GPBT supported by barbed wire fence (array 37)	0	None	9	9.0	13.0	1

[1]Penetration time is the time for one man to cross barrier
[2]Total time is the penetration time plus the time to cross a 30 ft clear zone on each side of the barrier.
[3]Two men under fence.

TABLE 7. *Penetrations through fence fabric*

Bottom configuration of fence fabric	No. men assisting but not crossing	Aids (see table 1)	Fastest penetration time[1] (seconds)	Average times		
				Penetration time[1] (seconds)	Total time[2] (seconds)	No. of attempts
Tension wire[3]	0	Cutters	17	21.5	28.0	2
Tension wire	0	Cutters	11	18.6	44.2	5
Bottom rail	0	Cutters	14	14	19	1
Fabric anchored in concrete	1	Two cutters	21	24.0	28.0	2
Fabric anchored in concrete	0	Cutters	22	22	26	
Fence arrays 26-25[3]	0	Two cutters	71	71	78	1
Fabric on each side of posts-single tension wire	1	Cutters	29	29	33	1
Fabric on each side of posts anchored in concrete	2	Two cutters	34	34	39	1
2 fabrics on same side of posts-single tension wire	1	Cutters	28	28	33	1
2 fabrics on same side of posts anchored in concrete	2	Two cutters	30	30	35	1
3 rolls of 24/30 GPBT on outside of fabric	3	Hooks Cutters	22	22	28	1
3 rolls of 24/30 GPBT on outside of fabric with bottom roll staked to ground	3	Hooks Cutters	63	63	69	1

[1] Penetration time is the time for one man to cross barrier.
[2] Total time is the penetration time plus the time to cross a 30 ft clear zone on each side of the barrier.
[3] Two men through fence.

TABLE 8. *Over barriers with ladders*

Array No.	Aids (see table 1)	No. men assisting but not crossing barrier	Fastest penetration time[1] (seconds)	Average times		
				Penetration time[1] (seconds)	Total time[2] (seconds)	No. of attempts
6	Ladder	2	7	8.0	12.0	2
8	Ladder	2	8	8.0	13.0	1
1	2x4 held overhead by 2 men	3	4.5	6.2	11.4	3
26[3]	Extension ladder	0	280	280.0	296.0	1

[1] Penetration time is the time for one man to cross the barrier.
[2] Total time is the penetration time plus the time to cross a 30 ft clear zone on each side of the barrier.
[3] Four men over fence.

TABLE 9. *Summary of penetration times for fence climbovers*

Array No.	Penetration time with limited aids (seconds)	Penetration time with unlimited aids (seconds)
26-25		104
27	98	55
25	50	44
26	44	25
17	34	7
8	16	5
14	10	
36	7	4.5
6	5	
4	5	
5	4	
2A	4	
2	4	
44	2.5	7
43	4	6
1	2.0	6
42	1.5	

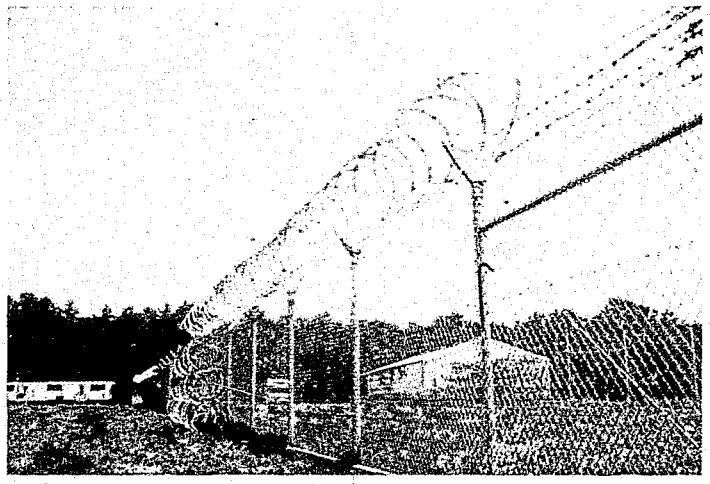


FIGURE 1. *Fence Array Nos. 17 and 38.*

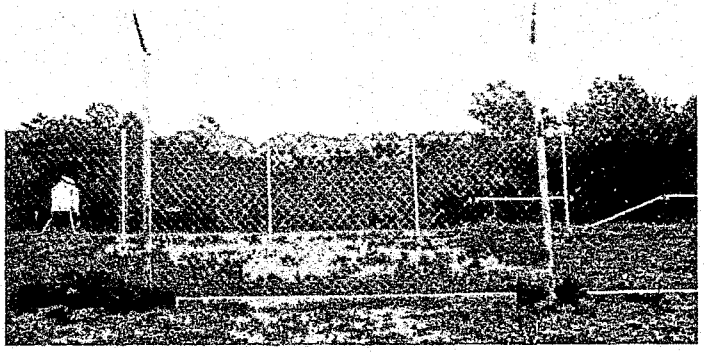


FIGURE 2. *Fence Array No. 17.*

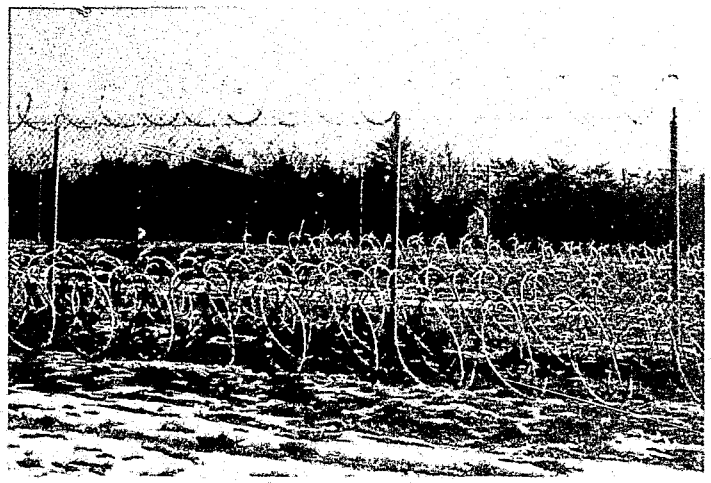


FIGURE 3. *Fence Array No. 27.*

FIGURE 4. *Fence Array No. 27.*

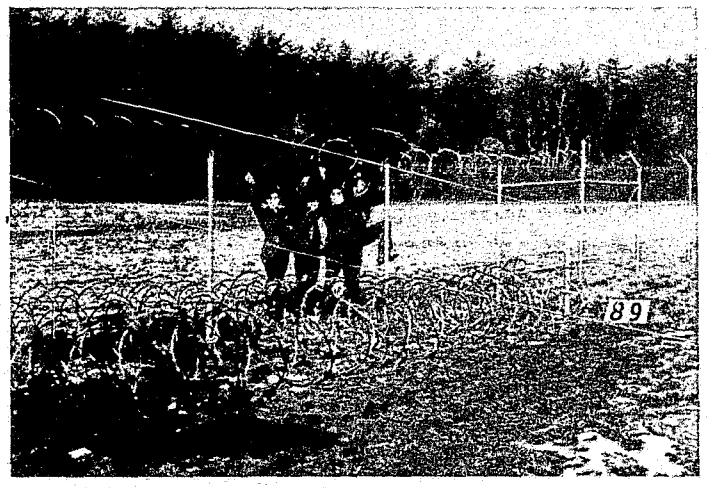


FIGURE 5. *Fence Array No. 27.*

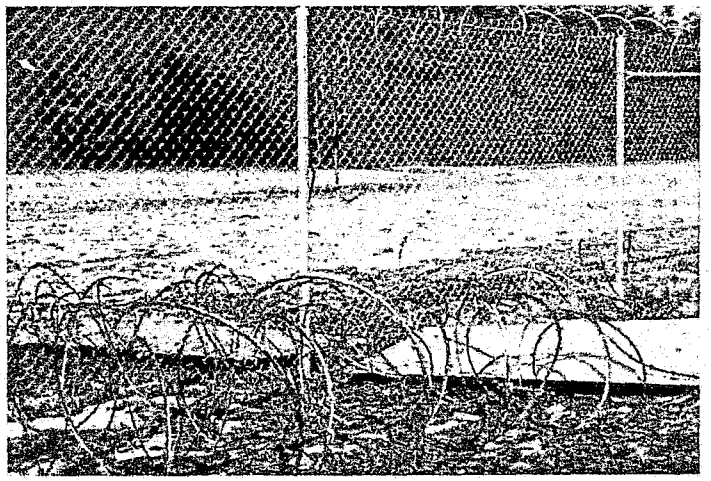


FIGURE 6. *Fency Array No. 27.*

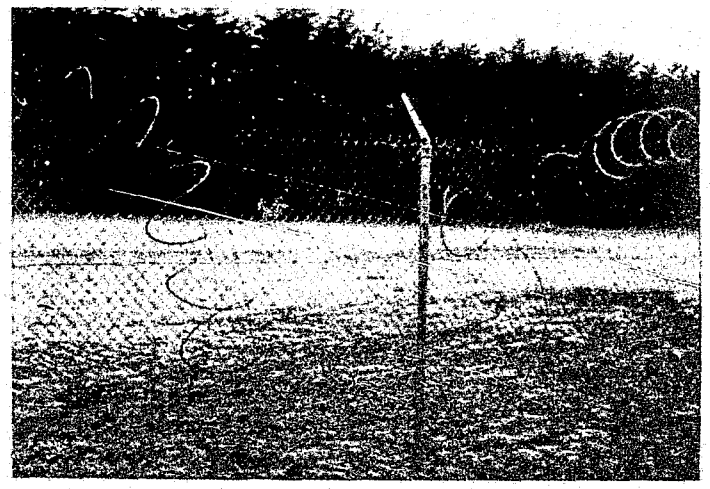


FIGURE 7. *Fence Array No. 14.*

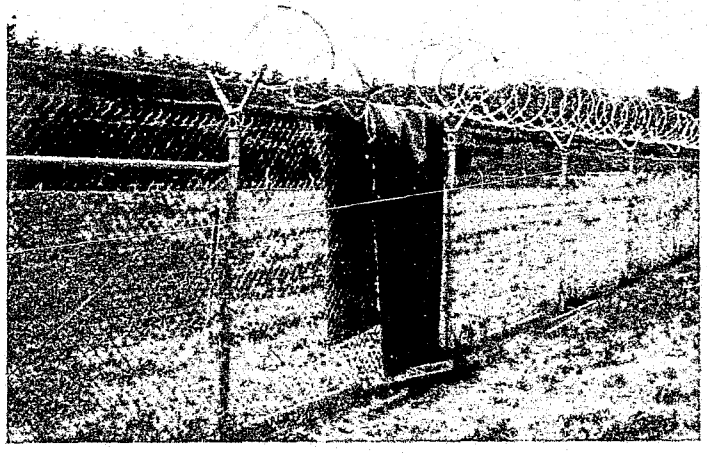


FIGURE 8. *Fence Array No. 17.*

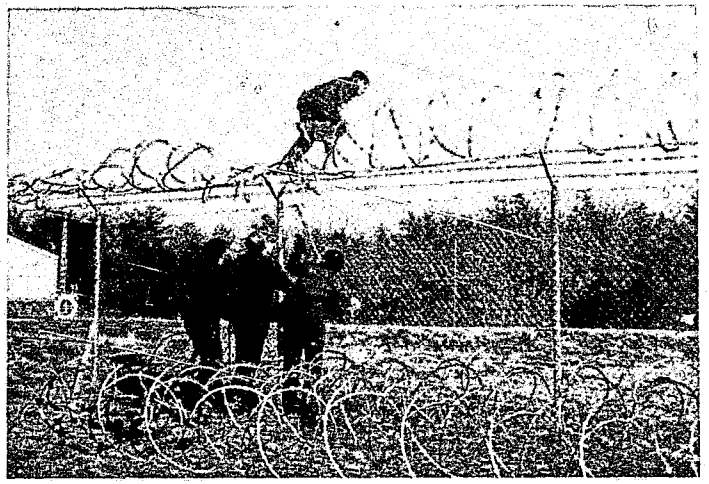


FIGURE 9. *Fence Array No. 25.*

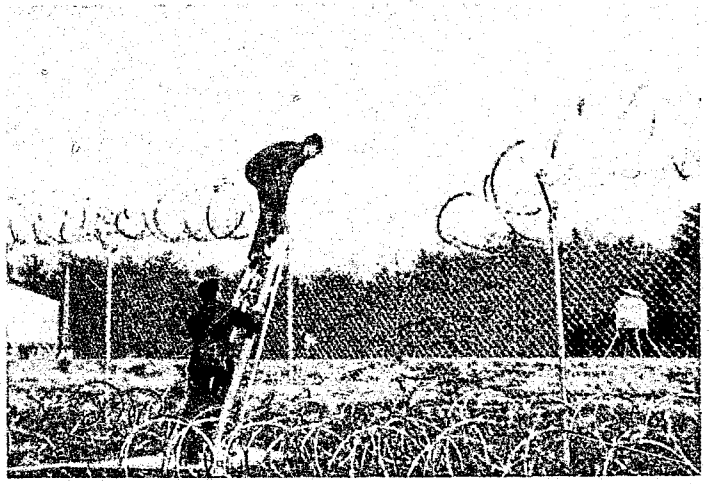


FIGURE 10. *Fence Array No. 25.*

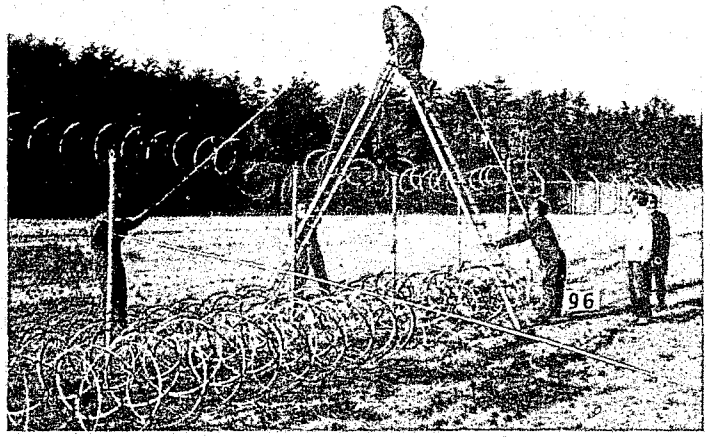


FIGURE 11. *Fence Array No. 26.*

FIGURE 12. *Damage caused by rocket attack.*

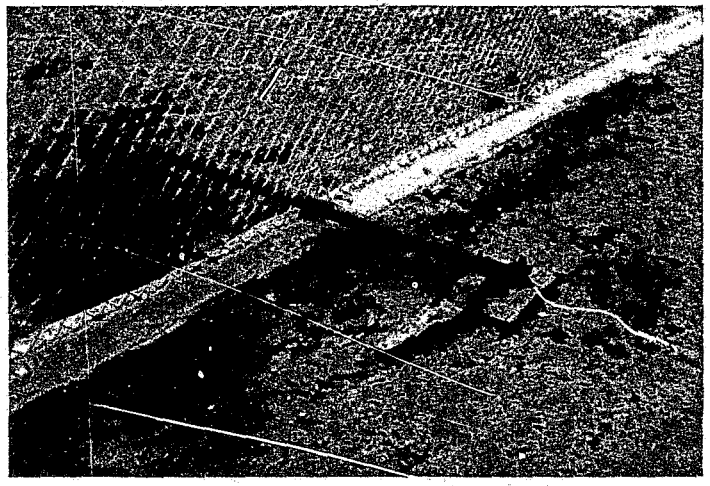


FIGURE 13A. *Bangalore torpedo.*

FIGURE 13B. *Damage caused by bangalore torpedo.*

FIGURE 14A. *Bangalore torpedo.*

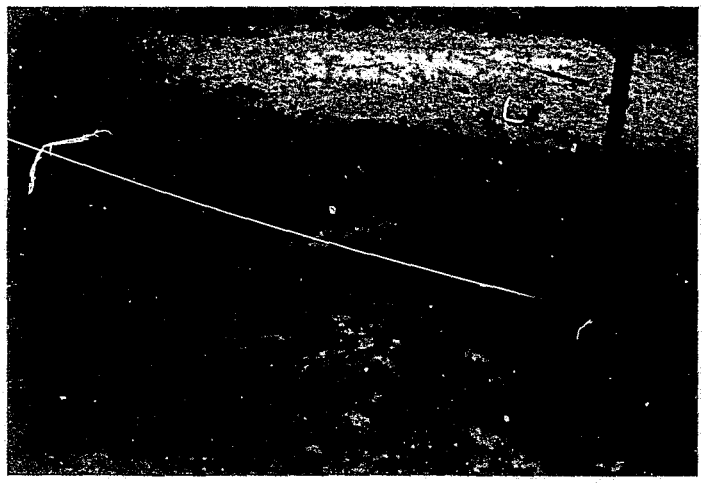


FIGURE 14B. *Damage caused by bangalore torpedo.*

FIGURE 15A. *Bangalore torpedo.*

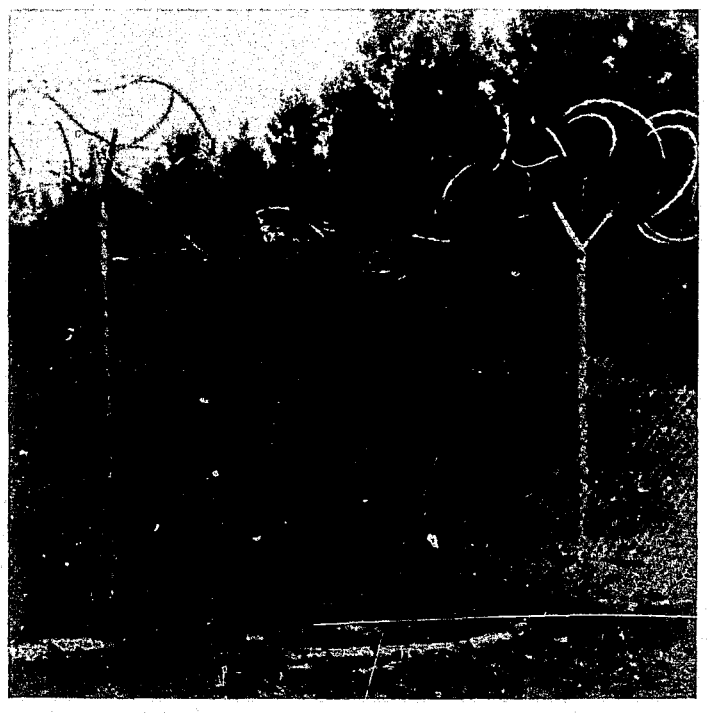


FIGURE 15B. *Damage caused by bangalore torpedo.*

FIGURE 16A. *Bangalore torpedo*.

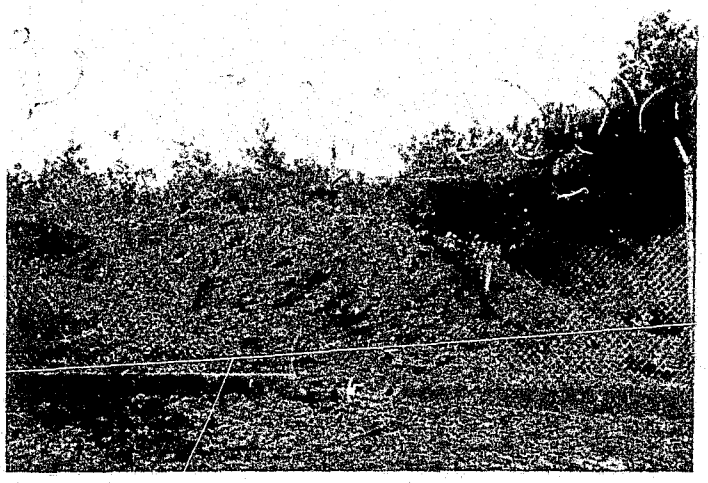


FIGURE 16B. *Damage caused by bangalore torpedo*.

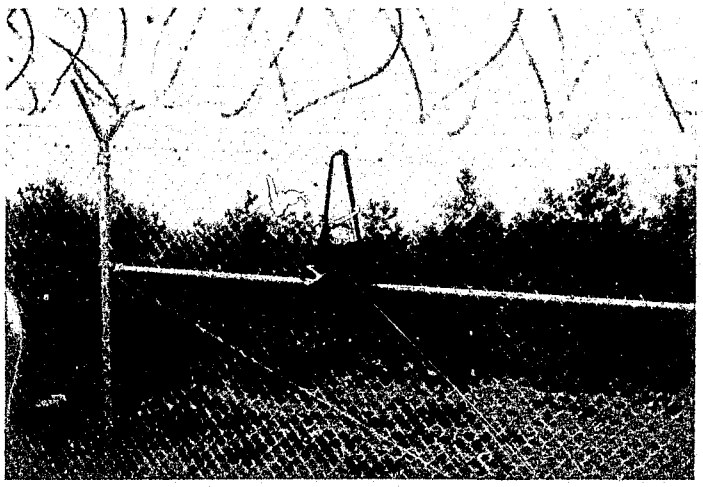


FIGURE 17A. *20-lb satchel charge.*

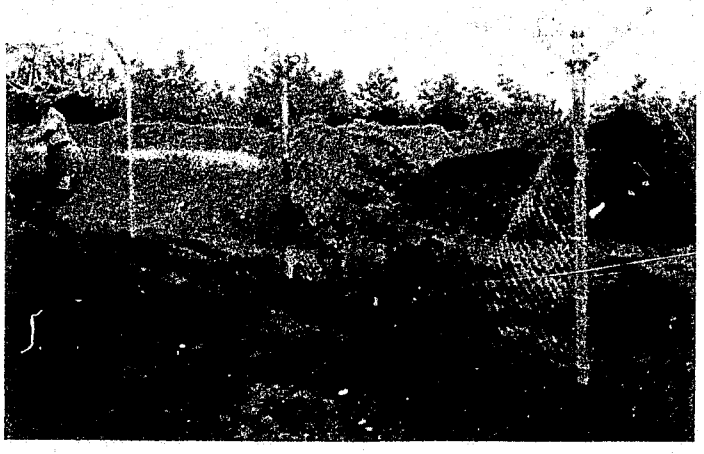


FIGURE 17B. *Damage caused by satchel charge.*

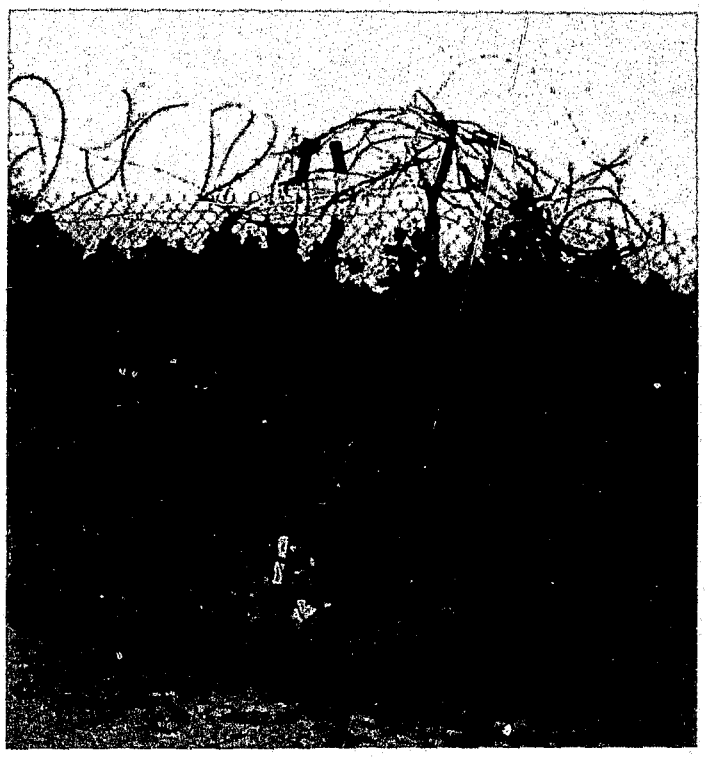


FIGURE 18A. *Chain of C4.*

FIGURE 18B. *Damage caused by C4.*

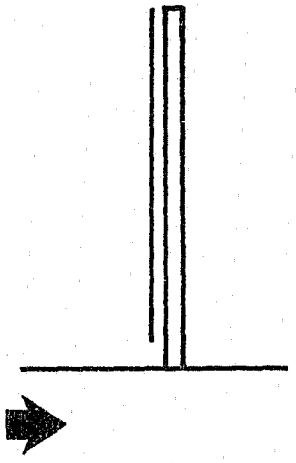


FIGURE 19. *Fence Array No. 42 (6 ' fence).* The fastest unassisted penetration time was 3 seconds without the use of aids; the fastest penetration time with one man assisting, without the use of aids, was 1 1/2 seconds.

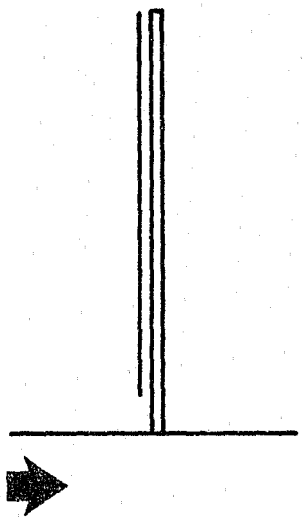


FIGURE 20. *Fence Array No. 1 (7 'fence).* The fastest penetration time with one man assisting, without the use of aids, was 2 seconds; the fastest penetration time with one man assisting, using canvas as an aid, was 6 seconds.

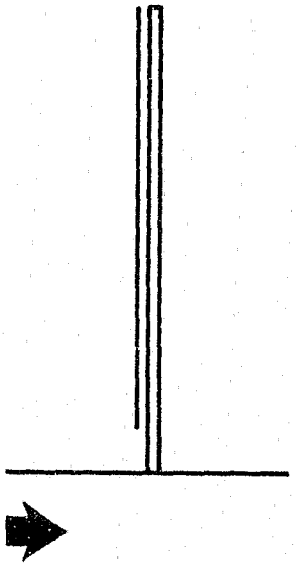


FIGURE 21. *Fence Array No. 43 (8 ' fence).* The fastest penetration time with one man assisting, without the use of aids, was 4 seconds; the fastest penetration time with three men assisting, using carpet as an aid, was 6 seconds.

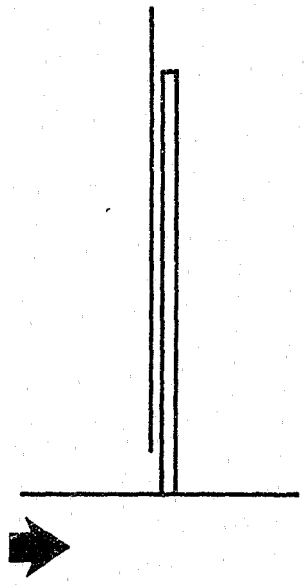


FIGURE 22. *Fence Array No. 44 (7 'posts, 8 'fabric).* The fastest penetration time with three men assisting, without the use of aids, was 2 1/2 seconds; the fastest penetration time with three men assisting, with carpet as an aid, was 7 seconds; the fastest penetration time unassisted, without the use of aids, was 5 seconds.

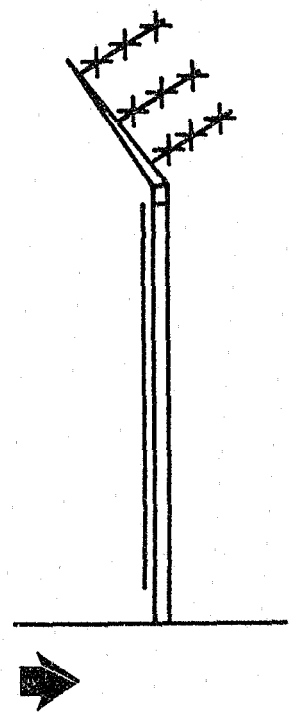


FIGURE 23. *Fence Array No. 2.* The fastest penetration time with one man assisting, without the use of aids, was 4 seconds.

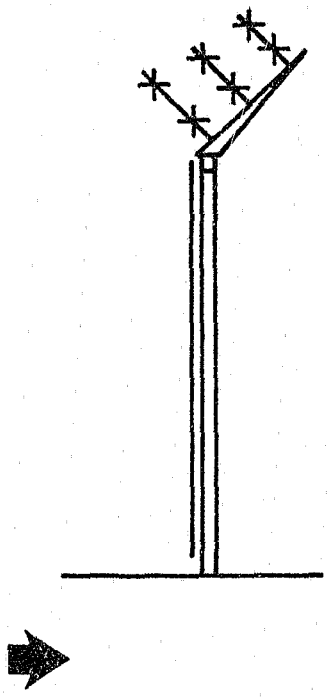


FIGURE 24. *Fence Array No. 4.* The fastest penetration time with one man assisting, without the use of aids, was 5 seconds.

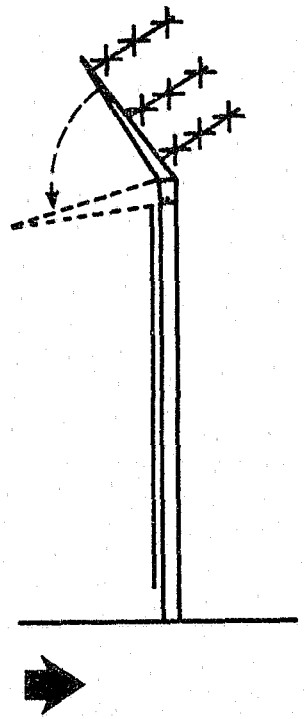


FIGURE 25. *Fence Array No. 2A (same as No. 2, but with collapsible outrigger).* The fastest penetration time with one man assisting, without the use of aids, was 4 seconds.

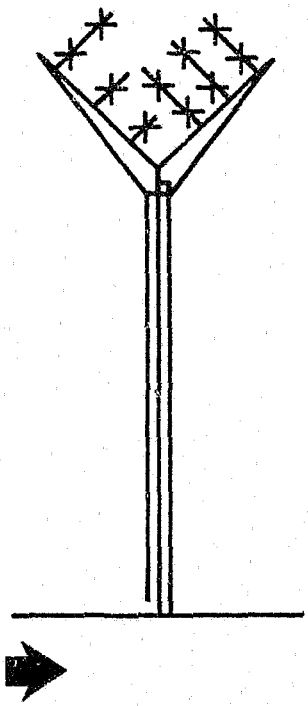


FIGURE 26. *Fence Array No. 5.* The fastest penetration time with one man assisting, without the use of aids, was 4 seconds; the fastest penetration time with one man assisting, using steps as an aid, was 12 seconds.

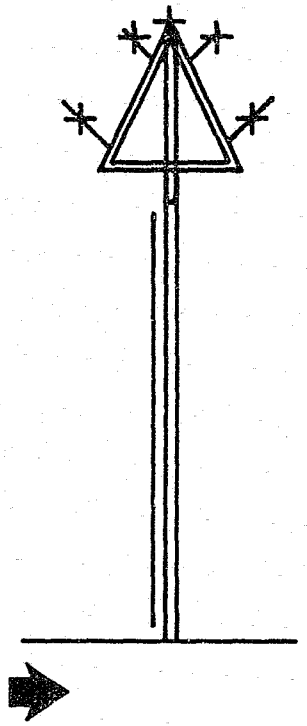


FIGURE 27. *Fence Array No. 6.* The fastest penetration time with one man assisting, without the use of aids, was 5 seconds; the fastest penetration time with one man assisting, using steps as an aid was 7 seconds.

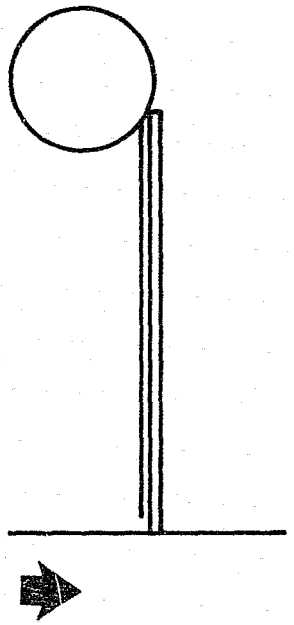


FIGURE 28. *Fence Array No. 8.* The fastest penetration time with one man assisting, using wirehooks as an aid, was 16 seconds; the fastest penetration time with one man assisting, using steps-canvas and wire hooks as aids, was 22 seconds; the fastest penetration time with three men assisting, using carpet as an aid, was 5 seconds.

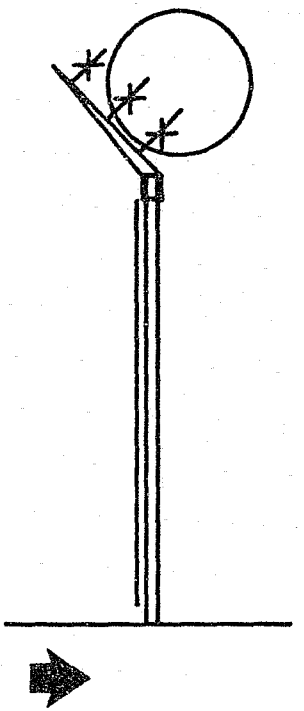


FIGURE 29. *Fence Array No. 14.* The fastest penetration time with one man assisting, using long hooks and cutters as aids, was 15 seconds; the fastest penetration time with two men assisting, using long hooks as aids, was 10 seconds.

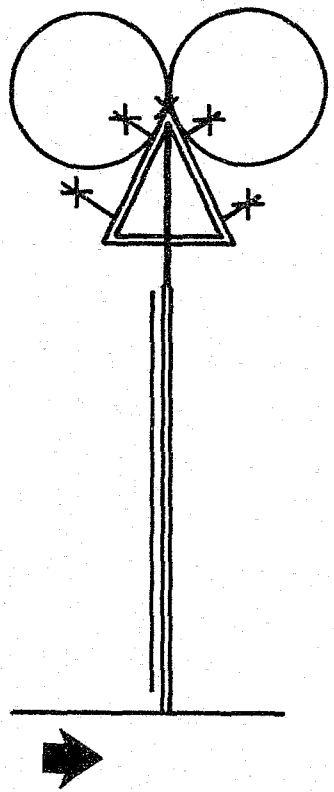


FIGURE 30. *Fence Array No. 36.* The fastest penetration time with one man assisting, using hooks as aids, was 7 seconds; the fastest penetration time with three men assisting, using carpet as an aid, was 4 1/2 seconds.

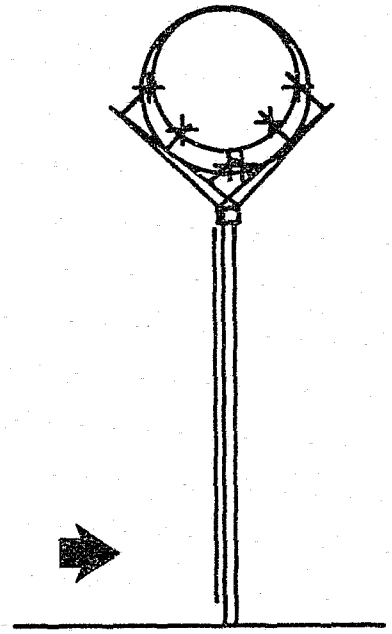


FIGURE 31. *Fence Array No. 17.* The fastest penetration time with two men assisting, using long hooks as aids, was 34 seconds; the fastest penetration time with two men assisting, using long hooks, steps, and cables as aids, was 52 seconds; the fastest penetration time with three men assisting, using carpet with 2x2s as an aid, was 7 seconds; the fastest penetration time with three men assisting, using carpet and ladder as aids, was 9 1/2 seconds.

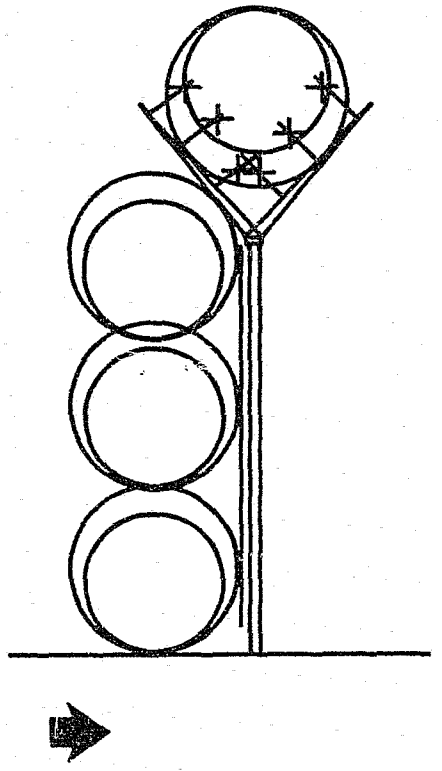


FIGURE 32. *Fence Array No. 38.* The fastest penetration time with three men assisting, using carpet with 2x2s as an aid, was 5 1/2 seconds.

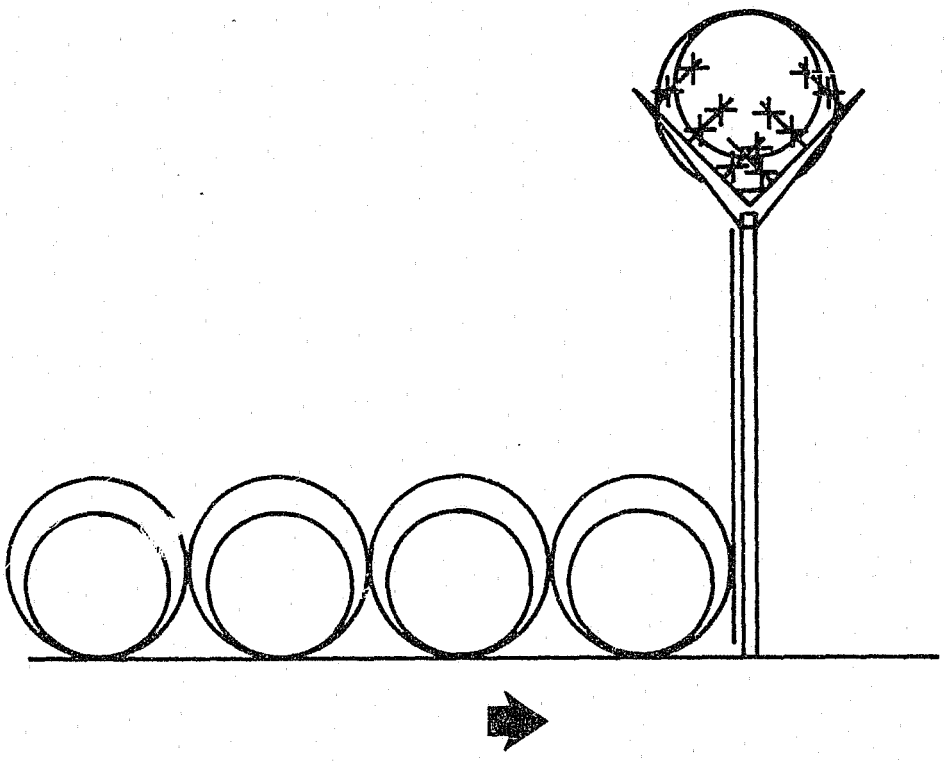


FIGURE 33. *Fence Array No. 25*. The fastest penetration time with three men assisting, using long hooks and steps as aids, was 50 seconds; the fastest penetration time with three men assisting, using long hooks, a ladder, and plywood as aids, was 40 seconds.

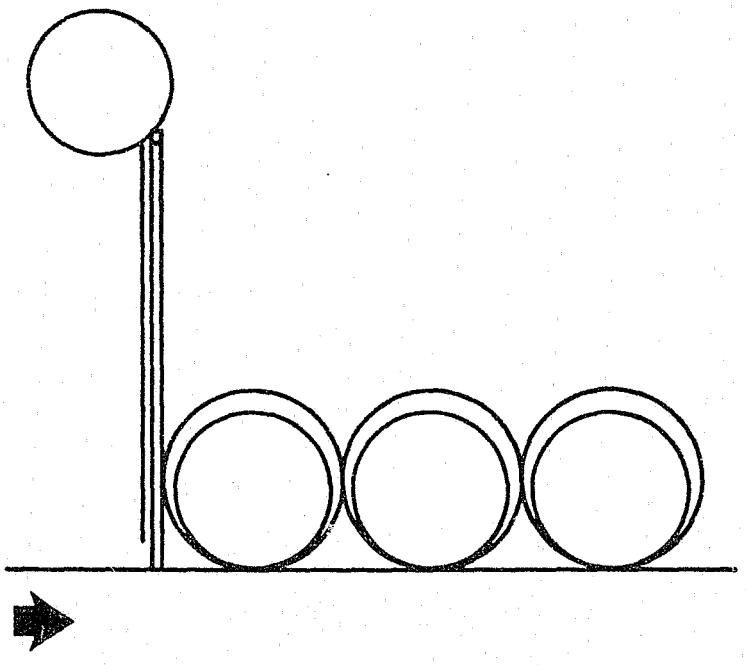


FIGURE 34. *Fence Array No. 26*. The fastest penetration time with one man assisting, using wire hooks and steps, was 44 seconds; the fastest penetration time with three men assisting, using wire hooks, steps, and plywood as aids, was 25 seconds.

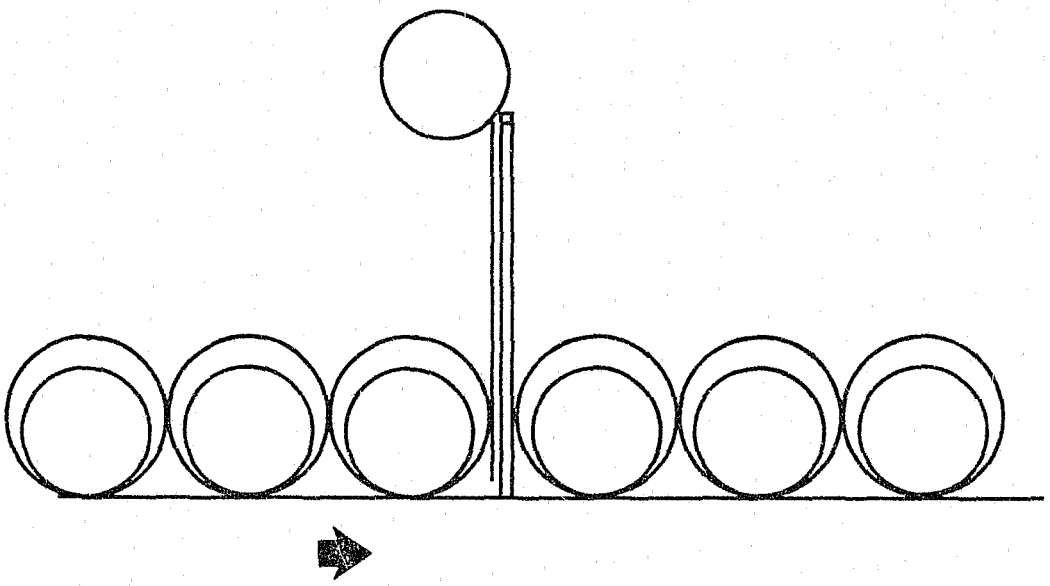


FIGURE 35. *Fence Array No. 27.* The fastest penetration time with one man assisting, using wire hooks and steps as aids, was 98 seconds; the fastest penetration time with one man aiding, using wire hooks, steps and plywood as aids, was 55 seconds.

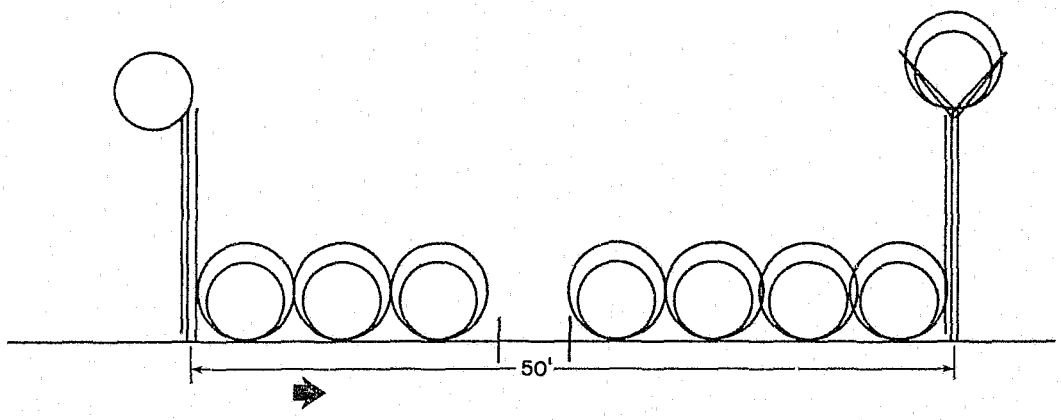


FIGURE 36. *Fence Array No. 26–25.* The fastest penetration time with two men assisting, using plywood, ladder, steps, and cutters as aids, was 104 seconds.

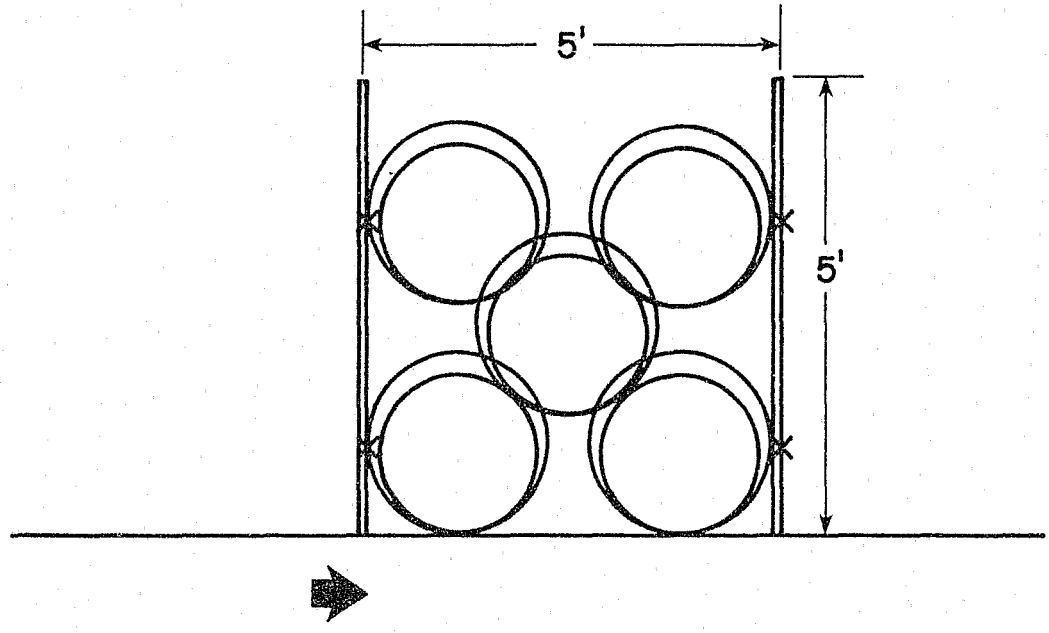


FIGURE 37. *Fence Array No. 37*. The fastest penetration time with three men assisting, using plywood as an aid, was 2 1/2 seconds.

APPENDIX A

Behavioral scientists of the National Bureau of Standards (NBS) observed Phase I of the Barrier Penetration Evaluation and also interviewed and held informal discussions with the four MPs and four Special Forces members acting as intruders. NBS has concluded that the configurations tested offer no psychological or physical deterrence value to individuals or groups intent on making a penetration.

Although individual interviews with each intruder at the end of the exercises would have been preferred, time constraints permitted only one group interview. This group interview consisted of four members of the Army's Special Forces and was conducted on 24 January 1974. The questions presented and the answers obtained are given below. It should be noted, however, that the final question entailed rank-ordering the configurations from hardest to easiest. The rank-ordering were done on an individual basis.

I. In penetrating a plain chain-link fence, what is your first, second and third choice in terms of *over*, *under* or *thru*?

1. Three said UNDER (assuming two intruders) and one said OVER.
2. Three said OVER—one said UNDER.
3. THRU (all four).

With barbed tape or barbed wire on top of the fence, all four would choose to go UNDER if possible, otherwise they'd go THRU.

II. Which tools (aids) were most useful for cutting thru:

Fence: 15-in bolt cutters were best. The 18-in bolt cutters were not as easy to handle as the 15-in ones—handles were too long and each cut took longer to make.

(In going under the fence a metal pipe about 8 feet long and 2-1/2 or 3 inches in diameter was found better than a wooden 2x4 because the pipe didn't break).

Tape: Tin shears were best. Aviation shears would also be good but none were available.

Wire: 15-in bolt cutters. Even shorter ones would be easier to use (10 in was mentioned).

III. How effective were the techniques used? What would you have done differently? What other tools would you have used?

They would not have used some of the techniques except that they were required by the test plan and materials at hand. Instead of 4-ftx8-ft plywood sheets they would use 2-ftx8-ft sheets which are easier to handle. Also, they did not like the specially designed ladder. Although the idea is good and provides a method for getting over the fence without setting off the fence alarm, they would redesign the ladder to make it more stable and easier to handle. As mentioned above, they would like smaller bolt cutters and aviation shears.

IV. What suggestions do you have for improving the outer perimeter fence? Inner fences?

They felt that in view of the cost, the outer fence should not be too elaborate but enough to keep out nonterrorists; in other words, a fence with sensors. Inner fences should be made hard to go over and impossible to go under to force going thru to set off the alarms. Inner defenses should rely more on visual surveillance by armed guards and TV monitors.

V. When you first saw these different fence configurations did they look imposing or threatening to you?

One of the men said, "The fences were not particularly 'scary.' This was just a job we had to do. We.ve seen things like this before." The others all agreed.

VI. Rank-order the 13 fence configurations from hardest to easiest in terms of difficulty of penetration.

The following table shows the results of these rankings in descending order of difficulty (hardest to easiest) for the four Special Forces intruders. The numbers in the table are the fence test array identifiers listed in the USAMERDC Phase I Test Plan, dated 19 December 74.

Intruders			
A	B	C	D
25-26	25-26	25-26	25-26
27	27	27	27
26	25	26	26
25	26	25	25
14	4	17	17
17	5	14	14
2A	17	8	8
5	6	6	6
6	2A	5	5
8	14	2A	4
4	8	4	2A
2	2	2	2
1	1	1	1

NOTE: Configuration 2A is the same as configuration 2 except that the outrigger arms are hinged. As can be noted in the above table, there is consensus agreement as to the first 4 configurations and the last 2. For arrays in between a consensus was not obtained.

PRELIMINARY OBSERVATIONS OF COMPLEX FENCE AND BARRIER ASSAULTS—PHASE II

Joel Kramer and Patrick Meguire

National Bureau of Standards, Washington, DC 20234

1. INTRODUCTION

The Defense Nuclear Agency (DNA) initiated a research effort to evaluate the vulnerability of complex fences and barriers in December 1974, shortly after formal execution of interagency support DODAAD Number HD 2001. The National Bureau of Standards (NBS) Law Enforcement Standards Laboratory (LESL) was asked to assign behavioral scientists to act as observers throughout the test program at Fort Belvoir, in an effort to obtain a preliminary evaluation of the behavioral impact of a variety of test configurations upon volunteer attack teams.

NBS participation was intended to provide only preliminary observations of behavioral impact, and to serve as the basis for future participation in the design of experimental evaluations of Forced Entry Deterrent Systems (FEDS) presently under development by DNA.

An earlier report (Phase I report dated February 1975) covered a total of 27 intrusion barrier test configurations which were erected and tested on a test range at Fort Belvoir U.S. Army Mobility Equipment Research and Development Center (USAMERDC). This Phase I test program was initiated with preliminary fence climbs during the second week of December 1974 and ended with assaults upon complex fences and barriers on January 24, 1975. The responsibility for the direction of this program was assigned to the Countermine/Counter Intrusion Department of USAMERDC.

2. PHASE II TEST PROGRAM

Between July 14 and July 25, 1975, 10 additional intrusion barrier test configurations were tested at USAMERDC. These configurations are described in table 1, and the more complex are illustrated in figures 1-3.

Behavioral scientists from the Consumer Behavior and Information Section, Product Systems Analysis Division of NBS were present to observe the penetration tests against the 10 barrier configurations. The assult team attacked each barrier configuration, some of which were protected by alarm sensors, using a variety of tools and penetration aids. Upon completion of the tests the NBS personnel conducted a debriefing session with the four U.S. Army Special Forces members who acted as intruders. The debriefing consisted of (1) a questionnaire filled out on an individual basis by each intruder, and (2) an informal group discussion (taped) with all four intruders present. The major subject of interest in the discussions was the "psychological deterrence value" of the 10 barrier configurations tested.

3. NBS ASSAULT OBSERVATIONS

None of the 10 barrier configurations tested offered any significant psychological or physical deterrence protection against the four man assault group (see USARMERDC test report for their performance data). It must therefore be concluded that these 10 barrier configurations would offer little, if any, deterrence value in terms of envisioned worst-case threats.

TABLE 1. *Barrier configurations*

Barrier Configuration Number	Description
1	7 ft chain link fence
1A	6 ft chain link fence
1B	8 ft chain link fence
1C	8 ft chain link fence with 7 ft support poles (top 2 feet of fence fabric not attached to poles)
1D	7 ft chain link fence with 24"/30" General Purpose Barbed Type (GPBT) on top, and bottom of fence fabric attached to concrete sill.
34	7 ft chain link fence with fabric attached to both sides of support poles.
35	7 ft chain link fence with 2 layers of fabric on same side of support posts (second fabric section offset to give effective mesh size of 1 in)
36	7 ft chain link fence with barbed wire and GPBT on top (fig. 1)
37	Five rolls of GPBT (fig. 2)
38	7 ft chain link fence with 3 rolls of GPBT on outer fence surface, and 1 roll GPBT on top (fig. 3)

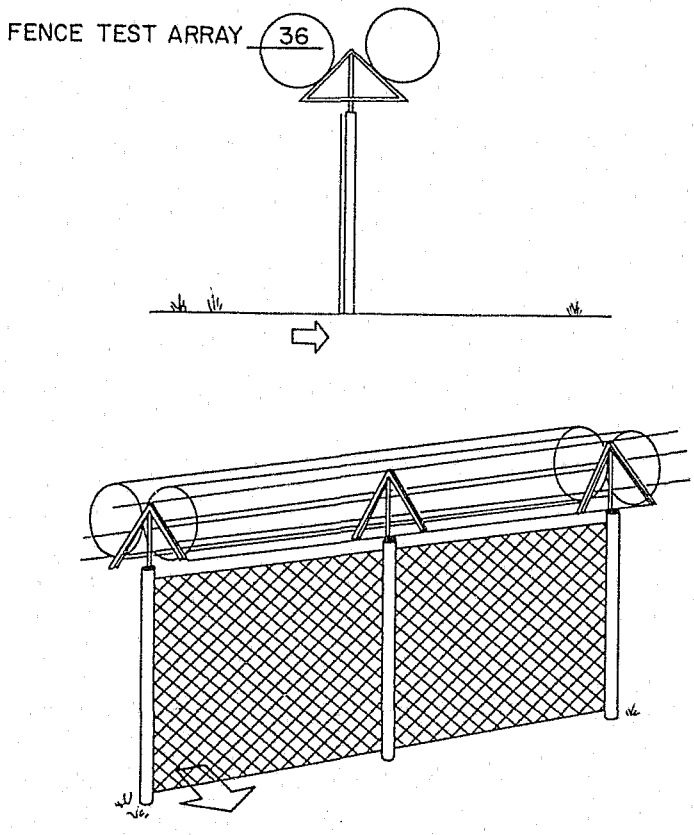


FIGURE 1.

FENCE TEST ARRAY 37

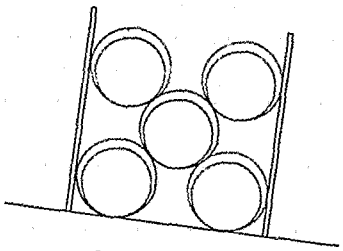
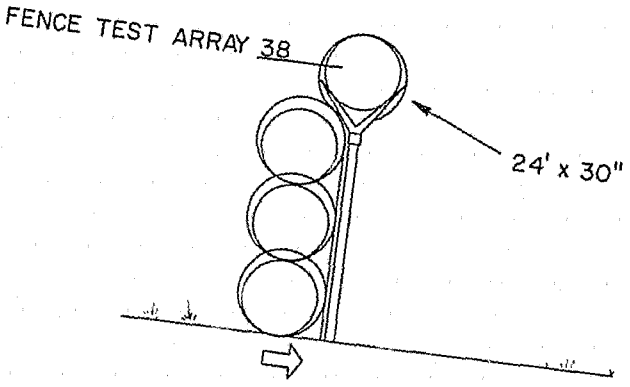


FIGURE 2.



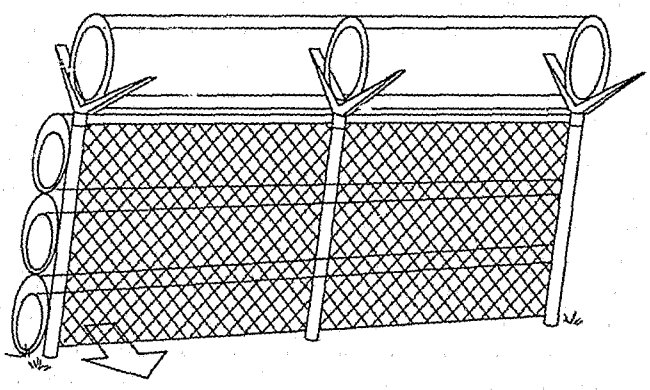


FIGURE 3.

4. RESULTS OF QUESTIONNAIRE STUDY

A questionnaire dealing with the "psychological deterrence value" of the 10 barrier configurations was administered to each of the four intrusion team members. For each of five hypothesized scenarios (see below) they were asked to: (1) rank order the barriers in terms of "perceived likelihood of achieving a successful penetration," (2) indicate their preferred method of barrier penetration, (3) indicate their preferred choice of aids for the penetration, and (4) make any comments relevant to the specific barrier/scenario condition under consideration.

General assumptions for all five scenarios were provided to the assault team members as follows:

1. A *covert assault* is planned: you must avoid visual detection by patrolling security forces and/or sensors at all costs.
2. A *four man assault team* is planned; only one member of the team is required to penetrate the fence.
3. The penetration must be accomplished in *3 minutes or less*.
4. The following *aids* are available:

Concealable aids:	a. wire and/or bolt cutters
	b. climbing hooks
	c. short (3 ft) pipe or 2x4
	d. rope and/or wire
Unconcealable aids:	e. long (8 ft) pipe or 2x4
	f. 4 ft x 8 ft plywood sheet
	g. rug or heavy canvas and "lifting poles"
	h. stepladder

5. The penetration must be accomplished by one of the following *methods:*
   a. under fence
   b. through fence
   c. over fence

Specific assumptions for the individual scenarios were:

SCENARIO 1	A.	No sensors on fence
	B.	Concealable aids only may be used
SCENARIO 2	A.	No sensors on fence
	B.	Concealable and/or unconcealable aids may be used
SCENARIO 3	A.	Sensors are on fence (you must avoid setting off sensors; deactivation of sensors not permissable)
	B.	Concealable aids only may be used
SCENARIO 4	A.	Sensors are on fence (you must avoid setting off sensors; deactivation of sensors not permissable)
	B.	Concealable and/or unconcealable aids may be used
SCENARIO 5	A.	Sensors are on fence (deactivation of the sensors is permissable)
	B.	Concealable and/or unconcealable aids may be used

4.1. Ranking Task: Results and Conclusions

Table 2 summarizes the results of the questionnaire ranking task for each of the 10 barriers and 5 scenarios tested. The barriers are ranked from most (1) to least (10) difficult based upon the mean ranks obtained from the four intruders for each barrier.

TABLE 2. *Results of the barrier ranking task*

Scenario No.: Rank	1	2	3	4	5
1	38(4)	38(4)	38(1)	38(2)	38(2)
2	36(4)	36(4)	36(1)	36(2)	36(2)
3	34(4)	34(4)	37(1)	37(2)	37(2)
4	35(4)	35(4)	1C(3)	1C(3)	1C(3)
5	37(4)	37(4)	1B(3)	1B(3)	1B(3)
6	1D(4)	1D(4)	1D(3)	1D(3)	1D(3)
7	1C(4)	1C(4)	34(3)	1A(3)	34(3)
8	1B(4)	1B(4)	1A(3)	34(3)	1A(3)
9	1A(4)	1A(4)	35(3)	35(3)	35(3)
10	1(4)	1(4)	1(3)	1(3)	1(3)

intrusion attempt *under the conditions postulated* is depicted in parentheses next to the barrier configuration number. Mean ranks were based only upon the rankings of the "willing" intruders.

In comparing the five scenarios, it is evident that the barrier ratings of scenarios 1 and 2 are identical, as are the barrier ratings of scenarios 3, 4, 5. The differences between these two fundamental groups (sensors vs. no sensors on barriers), however, are considerable. Thus, without sensors, all four intruders felt they could successfully penetrate every barrier configuration tested, while with sensors, at least one intruder felt he would not attempt a penetration for each configuration tested. Hence, it may be concluded that barriers with sensors are perceived to be significantly more likely to lead to an unsuccessful intrusion than are barriers without sensors. In addition, rank ordering of the barriers within scenarios are considerably different between the sensor vs. no sensor groups. Thus, barrier nos. 37, 1C and 1B were ranked higher (more difficult) within the sensor scenarios, while configurations 34 and 35 were ranked higher (more difficult) in the no sensor scenarios. We may thus conclude that the application of sensors has a bearing upon the perceived *relative* difficulties of various barrier configurations.

4.2. Preferred Methods: Results and Conclusions

Table 3 summarizes the results of the preferred method portion of the questionnaire. The preference frequency for each of the three possible methods (over, under, or through) is presented for each barrier configuration and scenario.

Again there is a large difference between the sensor and no sensor scenarios. With sensors present, the *only* feasible method of intrusion *under the conditions postulated* is to go *over* the barrier without making contact with it, while with no sensors present, the preferred method of intrusion varies as a function of the aids available and the specific configuration to be penetrated. In general, going over the barrier is still the most commonly preferred method. When only concealable aids must be used, *through* is more often the preferred than *under*; when unconcealable aids may be used, *under* is more often preferred than *through*.

4.3. Preferred Aids: Results and Conclusions

The preferred choice of aids varied considerably between the four intruders, especially for the no sensor scenarios. In general, a long pipe or 2-inx4-in was the preferred aid associated with going under the barriers, while a bolt cutter was the preferred aid for going through the barriers. Where the preferred method was over, a

TABLE 3. *Preferred methods of penetration*

Scenario No.:	1			2			3			4			5		
Barrier Configuration Number	Over	Under	Through	Over	Under	Through	Over	Under	Through	Over	Under	Through	Over	Under	Through
1	3	0	1	3	0	1	3	0	0	3	0	0	3	0	0
1A	3	0	1	3	1	0	3	0	0	3	0	0	3	0	0
1B	2	0	2	1	3	0	3	0	0	3	0	0	3	0	0
1C	2	0	2	1	3	0	3	0	0	3	0	0	3	0	0
1D	2	0	2	4	0	0	3	0	0	3	0	0	3	0	0
34	4	0	0	3	1	0	3	0	0	3	0	0	3	0	0
35	4	0	0	3	1	0	3	0	0	3	0	0	3	0	0
36	1	1	2	1	2	1	1	0	0	2	0	0	2	0	0
37	1	0	3	3	0	1	1	0	0	2	0	0	2	0	0
38	1	0	3	2	2	0	1	0	0	2	0	0	2	0	0
Total	23	1	16	24	13	3	24	0	0	27	0	0	27	0	0

variety of aids were preferred, including climbing hooks, a short 2-inx4-in, rug, plywood, and ladder. Typically, the simpler the barrier was perceived to be, the fewer and less complex were the aids required.

In the sensor scenarios, sensor deactivation aids were mentioned, but were felt to be inappropriate for the general assault conditions postulated (especially the 3 minute time limit). The preferred aids for going over a barrier with sensors were ladders and a short 2-inx4-in (presumably to be used for lifting one intruder high enough to enable him to jump over the barrier without making contact). All four intruders mentioned that the presence of sensors would greatly increase the difficulty of making a covert penetration, but if an overt penetration was planned, or if the sensors could be deactivated, the barriers would present no penetration problems.

5. RESULTS OF GROUP INTERVIEW

During the group interview, five specific questions were presented by NBS personnel for discussion. The questions and discussion were taped, and a synopsis including major conclusions is presented below.

Question 1: Is General Purpose Barbed Tape a psychological deterrent? Why?

Conclusion: If the motivation and capabilities of the potential intruders are sufficiently high, General Purpose Barbed Tape offers no psychological deterrence value. It will not influence a "go-no-go" decision, but may influence the time and effort spent during the assault planning stage. For intruders with low motivation and capability, a standard 7-foot chain link fence with the bottom of the fabric embedded in a concrete sill, and either barbed wire or barbed tape on top, *will* offer some psychological deterrence value.

Question 2: What was your reaction when you first saw General Purpose Tape? Your present reaction?

Conclusion: When seen from a distance on film, barbed tape looks somewhat "foreboding," but after closer inspection, and especially after some experience with it, all apprehension disappears. It may continue to look foreboding to poorly motivated and unskilled individuals.

Question 3: Can you think of any other barrier configuration that might achieve psychological deterrence for the worst-case threat?

Conclusion: No barrier by itself will completely deter the worst-case threat. The best deterrent would probably be a barrier with reliable sensors and a well-armed "ready force."

Question 4: Do you think that sending a single individual either over, under or through a barrier is a realistic procedure for the worst-case threat?

Conclusion: It is highly unlikely that the worst-case threat would plan on sending one person into a Nuclear Weapon Storage Area. Many more individuals would probably be used in a wide variety of roles, both inside and outside the barrier perimeter. In situations where a single individual can be put across the barrier, there should be no problem in getting more across. The number of persons to be put across may influence the choice of penetration method.

Question 5: On the basis of what you have seen and done, how much of a commitment should be made to improve barriers for enhancing nuclear weapon security?

Conclusion: Cost-effectiveness is the biggest problem. Money would best be spent on improving *sensors* (constant visual surveillance might be even better), and "ready force" capabilities. Even sensors could be avoided or neutralized by intrusion forces given enough time and practice.

SUMMARY OF THREAT ANALYSIS WORKSHOP

The second day of the symposium was designed to achieve the following objectives: (1) to conduct a workshop session on threat analysis and (2) to plan for future symposia. The threat analysis workshop featured impromptu discussion and a lively interchange of information and ideas between panel members and interested attendees. There was considerable reluctance on the part of all concerned to deal with the specifics of perpetrator attributes and the details of psychological profiling activities in an open, unclassified forum. The workshop session resulted in a consensus conclusion that the development of a meaningful data base and a substantive interchange of relevant information could only be achieved in a classified forum. Attendees stressed the critical need for a more reliable, valid, and comprehensive data base in the area of threat analysis.

Based upon the results of the workshop session, preliminary plans were formulated for the Second Annual Symposium. Instead of concentrating exclusively on the area of terrorism, the scope of the Second Annual Symposium would be expanded to include adversary characteristics for the entire threat continuum, with a classification of up to and including SECRET required for both attendance and presentation. Attendees and panel members indicated that it was premature in this first symposium to draft definitive statements concerning the role of behavioral science in physical security systems. It was generally agreed that this should be the product (objective) of the next symposium. With near unanimity, the attendees expressed the sentiment that the symposium was worthwhile and informative and encouraged DNA and NBS to sponsor and conduct future symposia and workshops to define the needs for behavioral contributions to physical security and to demonstrate behavioral capabilities.

LIST OF ATTENDEES

AFRRI
Armed Forces Radiobiology
Research Institute
ATTN: Robert W. Young (BHSE)
Lt. Col. J. L. Mattsson, USAF
Bethesda, MD 20014

AMERICAN INSTITUTE OF ARCHITECTS (AIA)
John F. Albertson
8305 Tamarac
Wichita, KS 67606

AIR FORCE
USAF/SPOL
ATTN: Gene Brown
Maj. Allan Mason
Bolling Air Force Base
Washington, DC 20332

ARMY
Commander
Military Personnel Center
ATTN: DAPC PMP-T (Dr. Herbert Leedy)
2461 Eisenhower Avenue
Alexandria, VA 22331

HQ DA (DACE-HRE)
ATTN: Col. Lowrey
Washington, DC 20301

HQ DA
Law Enforcement Division
ATTN: Mr. Klekner
Washington, DC 20310

Chief, Lab 7000
U.S. Army Mobility Equipment &
Readiness Command
ATTN: Stuart Kilpatrick
Fort Belvoir, VA 22060

Dr. John P. Farrell
U.S. Army Research Institute
1300 Wilson Boulevard
Arlington, VA 22209

Colonel James Hill
HQ DA (MONA-SU)
Bldg. 2073, North Area
Ft. Belvoir, VA 22060

BDM
The BDM Corporation
ATTN: Arnold E. Dahlke
Brian S. Gunderson
1920 Aline Avenue
Vienna, VA 22180

CACI
CACI Inc.—Federal
ATTN: Dr. Don Harris
Dr. Leo Hazlewood
Eric Shaw
1815 North Fort Myer Drive
Arlington, VA 22209

C& G
Ms. Susan H. Nycum
Chickering and Gregory
San Francisco, CA 94104

DDI
Decisions and Designs, Inc.
ATTN: Jack Levell
Dr. Judith Selvidge
Suite 600
8400 Westpark Drive
McLean, VA 22101

DIA
Director
Defense Intelligence Agency
ATTN: Maj. Charles J. Bushey
Washington, DC 20301

DNA
Director
Defense Nuclear Agency
ATTN: Marvin C. Beasley
Robert Benedict
Charles Blank
Ray Cadorette
Robert Carson
Bruce DiPietrautonio
Earl Eagles
Allen Futral
Cpt. S. G. Galing, USN
Herbert L. Gurnee, General Counsel
Ltc. R. H. Martin, USA
Cdr. J. P. Neyland, USN
Ltc. George Norwood, USAF
Col. R. A. Peshkin, USAF
Col. O. B. Smith, USA
Milton E. Stevens

DOD CONSULTANT
Willard Shankle
1670 Pine Valley Road
Milledgeville, GA 31061

DLA
Defense Logistics Agency
ATTN: (DLA-T) John Ross
Cameron Station
Alexandria, VA 22314

ERDA
Division of Safeguards and Safety
U.S. Energy Research &
Development Administration
ATTN: Barry Rich
Washington, DC 20545

FAA
Office of Aviation Medicine
HQ, FAA
ATTN: Dr. Pickrel
800 Independence Avenue
Washington, DC 20003

HFRI
Robert H. Macki
Human Factors Research Inc.
Goleta, CA 93017

IACP
International Association of
Chiefs of Police, Inc.
Eleven Firstfield Road
ATTN: Robert Miller
Gaithersburg, MD 20760

LLL
University of California
Lawrence Livermore Laboratory
ATTN: Roy Adams
P.O. Box 45 (808)
Mercury, NV 89023

MITRE CORP
MITRE Corp.
Westgate Research Park
ATTN: Dr. Jan Pratt
1820 Dolley Madison Boulevard
McLean, VA 22101

NAS
Dr. George A. Lawrence
National Academy of Sciences
2101 Constitution Avenue
Washington, DC 20037

NAVY
Commanding Officer
Naval Weapons Support Center
ATTN: Ron Henry
Crane, IN 47522

Commander
Naval Facilities Engineering Command
ATTN: Herb Lamb (CODE 032E)
Alexandria, VA 22332

Deputy Chief of Naval Operations
(Logistics)
Physical Security Branch
ATTN: NOP-403 (CDR Tom Neidbala)
Washington, DC 20350

Naval Investigative Service
ATTN: Richard Cook (27B)
Earl J. Jamison (27B)
Hoffman Building
2461 Eisenhower Avenue
Alexandria, VA 22331

Naval Surface Weapons Center
ATTN: John Haben (CODE WR43)
Silver Spring, MD 20910

Office of Naval Research Branch Office
ATTN: Dr. Eugene Gloye
1030 East Green Street
Pasadena, CA 91106

Office of Naval Research
ATTN: Dr. John Nagay (CODE 452)
800 North Quincy Street
Arlington, VA 22217

NBS
U.S. Department of Commerce
National Bureau of Standards
ATTN: Bob Carpenter
Lawrence Eliason
Alfred Koenig
Joel Kramer
Patrick Meguire
Ray Moore
John Schlater
Washington, DC 20234

NRC
U.S. Nuclear Regulatory Commission
Office of Inspection and Enforcement
ATTN: Loren L. Bush
Owen Chambers
William J. Ward
Washington, DC 20555
MAIL STOP EW-359

U.S. Nuclear Regulatory Commission
Office of Program Development
Division of Safeguard
ATTN: Dr. Robert Mullin
Joe Yardumian
Washington, DC 20555
MAIL STOP 9609

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
ATTN: Dr. Thomas E. Shea
Washington, DC 20555
MAIL STOP 1130SS

U.S. Nuclear Regulatory Commission
Office of Standards Development
ATTN: Dr. Frank A. Constanzi
Michael Gailanis
Jim Prell
Washington, DC 20555
MAIL STOP NL-5650

OSI
Operational Systems Inc.
ATTN: Joseph J. Cappucci
1600 Wilson Boulevard
Arlington, VA 22209

RDA
R & D Asscciates
ATTN: Dr. Lynn Gref
P.O. Box 9695
Marine Del Rey, CA 90291

R.V. WARD LTD
Ralph V. Ward LTD
Technical Security Consultant
1309 Oberon Way
McLean, VA 22101

SAI
Science Applications, Inc.
ATTN: Kenneth A. Plant
Dr. Carol A. Keegan
1911 North Fort Myer Drive
Suite 1200
Arlington, VA 22209

McLean/Science Applications, Inc.
ATTN: Dr. Hugh Kendrick
1651 Old Meadow Road
Suite 620
McLean, VA 22101

SANDIA
Systems Analysis & Engineering
Division
Facility Protection Department
Sandia Laboratory
ATTN: Allan Fine
Albuquerque, NM 87115

Sandia Laboratory
ATTN: James Kaiser
Brian Finley
P.O. Box 5800
Albuquerque, NM 87115

SRI
Stanford Research Institute
ATTN: George Hagn
Burt Mogin
1611 North Kent Street
Arlington, VA 22209

* U. S. GOVERNMENT PRINTING OFFICE : 1977 O - 244-848

ANNOUNCEMENT OF NEW PUBLICATIONS ON NATIONAL CRIME AND RELATED SUBJECTS

Superintendent of Documents,
Government Printing Office,
Washington, D.C. 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued on the above subjects (including this NBS series):

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-351)

END