NBS Special Publication 480-32

The Role of Behavioral Science in Physical Security

Proceedings of the Second Annual Symposium, March 23-24, 1977

Law Enforcement Equipment Technology

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards

ACKNOWLEDGMENTS

This document 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
480-32

The Role of Behavioral Science in Physical Security

Proceedings of the Second Annual Symposium, March 23-24, 1977

Edited by
Joel J. Kramer
Center for Consumer Product Technology
National Bureau of Standards

Sponsored by the
Law Enforcement Standards Laboratory and
Consumer Sciences Division
National Bureau of Standards
Washington, D.C. 20234
and the
Intelligence and Security Directorate
Defense Nuclear Agency
Washington, D.C. 20305

This work was supported by the Defense Nuclear Agency, Robert R. Monroe, Vice Admiral, USN, Director, under Subtask Code P99QAXDE910, Work Unit 27.

Issued June 1978

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, *Director*

Library of Congress Catalog Card Number: 77-600058

National Bureau of Standards
Special publication 480-32
Nat. Bur. Stand. (U.S.), Spec. Publ. 480-32, 93 pages
CODEN:XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1978

For sale by the Superintendent of Documents,
U.S. Government Printing Office, Washington, D.C. 20402
Stock Number 003-003-01950-0 Price $2.75
(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,* the editor or the Law Enforcement Standards Laboratory, National Bureau of Standards, Washington, D.C. 20234.

Jacob J. Diamond
Chief, Law Enforcement Standards
Laboratory

*Points of view or opinions expressed in this volume are those of the individuals to whom they are ascribed, and do not necessarily reflect the official positions of either the National Bureau of Standards or the Defense Nuclear Agency.

PREFACE

These proceedings are the result of a symposium, the second of a series, held on March 23-24, 1977, at the National Bureau of Standards. The purpose of the symposium was to continue defining the contributions that behavioral science can make to enhance physical security systems and to share information and ideas among the participants and other interested parties.

This symposium was jointly sponsored by the Law Enforcement Standards Laboratory (LESL) and the Consumer Sciences Division of the National Bureau of Standards (NBS) and the Intelligence and Security Directorate of the Defense Nuclear Agency, and attracted approximately 140 attendees from Government and industry.

The editor wishes to acknowledge the cooperation of the staff of the Defense Nuclear Agency, particularly Mr. Marvin Beasley and Capt. Daryl Solomonson. Special appreciation is extended to Dr. Lawayne Stromberg, Director, Armed Forces Radiobiological Institute, 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; William Immerman and Dr. Robert Mullen, Nuclear Regulatory Commission; Jack Hennessey, Energy Research and Development Administration; and Dr. Harold P. Van Cott, NBS Human Factors Section.

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

ABSTRACT

This document contains the proceedings of the second annual symposium on "The Role of Behavioral Science in Physical Security," held in March 1977. The symposium provided a forum for presenting and discussing continuing current behavioral science contributions to physical security. Nine papers were given; timely questions and challenges were explored in an open discussion session at the end of the first day; and the symposium concluded with a panel session devoted to a synthesis of the material presented and a discussion of future research directions.

Key words: Adversary characteristics; animal research; behavioral science; collusion; ergonomics; human factors; human reliability; physical security; physiological psychology; threat analysis; terrorism; training.

CONTENTS

THE INADVERTENT ADVERSARY TO NUCLEAR SECURITY—OURSELVES

Don D. Darling

Don D. Darling and Associates, El Segundo, CA 90245

INTRODUCTION

When I was asked to present this paper, the concepts of "tell it like it is" and "shake up the troops with a bit of truth" were considered. My thirty years experience in actively fighting institutional inertia and resistance to change in the average Government agency has made quite clear several human factors which are worthy of study and correction. The "Don't make waves; don't rock the boat; I only have a few years to retirement" syndrome is probably the worst. Second is the "We have done it this way for twenty years," which is followed closely by the "Not invented here" (NIH) philosophy. There are a number of other resistance-to-change tendencies which would be disclosed by a competent human factors study.

The morale deadening process in Federal service begins early in the employee's career, when even the most well-conceived idea for improvement, reform, or elimination of waste, unnecessary manpower or expense is met with disdain from well-entrenched higher authority. Even the highly publicized Government Beneficial Suggestion Program is affected by the "syndromes" noted above, and the number of "Your suggestion shows much merit, but..." letters are legendary. Initiative is further stifled when that same suggestion comes out as agency or department policy at a suitable later time, with only the name of the author changed. The final blow comes when the signator suggestor of the plagiarized material is given an award or promotion for his or her "original thinking."

This is particularly true in the field of Government security, which is volatile and constantly changing in both technique and technology. Unfortunately, no matter how brilliant the individuals may be as Government security officials, well over ninety percent of them are engaged solely in compliance assurance surveys and inspection against outmoded government security policies and regulations. They conduct their daily work as do any other "quality assurance" inspectors, much like tire inspectors or electronic parts inspectors. The same holds true for their counterparts in the nation's defense industries.

This leads to self-perpetuation of the breed without improvement, and all of the upgrading of qualifications, additional training, and seminar attendance leads only to greater outlays for the same mediocre levels of performance. Worse yet, and to prove the point, the perpetuation of the breed in this manner results in a quantum jump in the proliferation of policy, regulation and operational instruction paperwork to the degree that the security personnel become slaves to the paper mill and neglect, by direction, the real world of security to be found only in direct and continuing field experience in the "real world."

Omphaloskepsis has become a way of life and the philosophy of a substantial part of the security field. If you sit and contemplate your navel long enough, the answers to all of the problems in the world will pass before your eyes. What good does having all of those answers do anyone, if nothing is done to implement them? Presented in the following sections are several specific examples of the way in which we and the Government are, indeed, the inadvertent adversary to nuclear security.

PERSONNEL SECURITY CLEARANCE VULNERABILITIES AND COMPROMISE POTENTIALS

The basic and primary safeguard in any classified endeavor is the assured integrity and loyalty of those employed in that endeavor. Without that assured integrity and continuing loyalty of the personnel involved, all of the fences, locks, guards, alarm systems and any other physical security safeguards are absolutely worthless.

Government security requirements, in general, state: If a vulnerability or a security deficiency is believed to exist, it must be presumed to actually exist until it can be proven, beyond any reasonable doubt, that the vulnerability does not exist, or that a security violation could not possibly have occurred. Another law that tends to supersede all other laws applicable to the field of security is Murphy's Law, which in essence states, "What can happen, will happen."

The fundamental and inescapable, brutal fact is that the entire Government Personnel Security Clearance Program has been vulnerable to penetration and compromise for well over 25 years. The program has, in fact, been successfully penetrated, as is proven by numerous news articles.

These reports indicate beyond a shadow of a doubt that anyone with reasonable intelligence, an ulterior motive, and a certain degree of determination can obtain a false, but legally valid security clearance through existing loopholes in the system. Therefore, it is logical to conclude that there is no assured security in the Government's multi-billion dollar security program.

It is suggested that this problem area be given the highest national priority for both immediate corrective action and the conduct of research to develop an "idiot-proof," fail-safe system that cannot be sabotaged by so-called human error, thus resulting in positive identification of cleared personnel "from cradle to grave."

To illustrate this point—is there anyone reading this paper who can prove beyond any reasonable doubt that the author is the same individual to whom an original personnel security clearance in his name was issued? How many people in Government, the Military and the Defense Industry have transferred from job-to-job, station-to-station, simply on the basis of a single form without a fingerprint recheck to establish positive identification? Remember that what can happen, will happen, and documentation is available to substantiate that it has, in fact, happened.

As to recommendations for immediate corrective action within our available resources, it is suggested that we begin by:

(1) The fingerprinting and reinvestigation of every individual in Government who is an authorized security clearance authority. The clearance determinations in these vital positions should be assigned to a committee of at least five highly-placed individuals with top secret and ERDA clearances, who must *all* agree independently and unanimously as to the eligibility of those individuals submitted for clearance, with qualified alternates available to stand in when any member disqualifies himself because an applicant is personally known to him;

(2) Concurrently, refingerprinting all personnel who have access to nuclear weapons, nuclear fuels, or nuclear material of any kind and quantity; rechecking those fingerprints with those on file from the original security clearance; and, when this is impossible, conducting a full background reinvestigation of that individual from "day one"; and,

(3) Initiating a nationwide recheck of fingerprints from cleared personnel at all levels, without regard for rank or position, beginning at the top levels and working down from top secret through confidential clearance.

From the psychological deterrent standpoint, publicize the intent and purpose of this fingerprint recheck program whether or not a single verification recheck is ever made. We might be surprised at the number of people who would just resign or disappear for one reason or another, rather than be subjected to reinvestigation and possible compromise or exposure.

Unless and until this is done, an obvious and continuing vulnerability, a potential for penetration, and an open invitation to subterfuge and fraud can be presumed to exist. These affect

both the entire Government and its industrial, classified contractor complex, and is also extended through the "Visit Clearance Program" to our foreign allies.

Quite possibly, a "penetration testing" of these vulnerabilities is in order to validate the premises of this paper. If these test penetrations are successful, and such incidents have been reported a number of times to the highest levels of Government, there may well be evidence of misfeasance or calculated non-feasance in public office worthy of investigation by the heads of the agencies or departments involved, and/or referral for prosecution under our judicial system.

With respect to future areas of research, it is suggested that much work, both privately and governmentally funded, has been done by North American Aviation, a Division of Rockwell International and others on automated fingerprint and handprint systems to the point where such systems not only exist, but are technically and economically feasible. Quite possibly, a data base presently exists that can be used in developing the "cradle-to-grave," computer-based, positive identification system so badly needed in the nuclear energy and weapons fields, as well as in the Government security program as a whole.

To illustrate my strong personal feeling about this matter, when I was unable to get the problem corrected within regular command channels in March 1959, I resigned as the head of an Air Force office administering and inspecting for compliance the security programs of Defense Research and Development contractors performing over one-half billion dollars in R&D contracts in the 11 Western States. Rather than remain a party to an obvious fraud and delusion, 20 years of career status and 10 points preference went out the window as a sacrifice to the deficiencies of our "not too secure" Government personnel clearance system.

POLYGRAPH AND VOICE STRESS ANALYZER USE IN PERSONNEL SECURITY

A "security clearance" is not a constitutionally guaranteed or God-given right, but a privilege extended to those individuals who, by their sustained and demonstrated loyalty and integrity, continually justify the trust placed in them by their Government. Since this is a condition of continuing employment, there appears no valid reason not to consider the use of the polygraph and/or voice stress analyzing devices and techniques, under appropriate controls, as a means of validating that continuing loyalty and integrity. This was done successfully in the early years of the Atomic Energy Commission. Security forces at all levels and the custodians of both nuclear weapons and fuels might be primary candidates for periodic test and re-test. The words "UNDER APPROPRIATE CONTROLS" are emphasized to minimize infringement on civil and personal rights, with the questions confined to the individual's knowledge and/or participation in violations of statute, or security regulations or requirements.

SECURITY AND RESEARCH VULNERABILITIES AND LIMITATIONS AND CAUSE THEREOF

It is difficult to understand how any meaningful research into our security problems can be conducted under current conditions, particularly in the nuclear power and weapons fields. The nuclear power and weapons fields are inseparable insofar as security is concerned. Since May of 1969, there have been ten attacks on U.S. and European nuclear installations or facilities involving bombs or weapon fire. During this time period there have been 99 threats or acts of violence at licensed U.S. nuclear facilities. During the same time period, at least twelve nuclear facilities have been the victim of vandalism or sabotage, one facility has been the target of seven separate arson attempts, and there is documentation that uranium has been stolen from at least one European facility. As further evidence of poor security practices, it should be noted that twelve facilities licensed by the U.S. Nuclear Regulatory Commission were fined for non-compliance with security regulations during the period from June 1974 to January 1976.

The problem stems from the multiplicity, fragmentation, and differences of Government agencies in their command and control responsibilities, inspection procedures, survey techniques, penetration testing, and command direction of corrective action. These differences have undoubtedly been a major contributing factor to the perpetuation of many vulnerabilities which for years have been known by professionals in the security field. The deficiencies which continue to threaten the fundamental integrity of the entire Nuclear Security Program can only be corrected by the institution of a single, responsible Nuclear Security Control Agency which cuts across all command channels and derives its authority under a security program mandated by highest authority. All source and fissionable materials and weapons should come under a single control and accountability program wherein it becomes possible to identify, analyze, qualify and quantify vulnerabilities; establish acceptable risk levels; implement corrective action; develop countermeasures; and determine those areas requiring further research and development in both physical and personnel security.

A single "Nuclear Security Agency" should be mandated at the highest levels of Government under appropriate Congressional controls. This new agency should have unequivocal, broad, "across-all-agency and departmental channels" authority to command, rather than negotiate, correction of vulnerabilities, and a charter to gather all available data on all aspects of security so that the data base requisite for meaningful research is available to researchers from a single source. In other words, let's consider going back to the old Atomic Energy Commission concept, under a new, more viable plan of security program management that can operate under a single security command, control and inspection system, with a single set of standards, so that when we make a mistake nationally it will be a common mistake, correctable by a single agency action. Obviously, this recommendation is bound to evoke cries of opposition and resistance from those agencies which may feel their autonomy and command prerogatives are being threatened or invaded, but as things now stand, it is often found that the right hand doesn't know what the left hand is doing.

IN SUPPORT OF A CONTINUING PROGRAM OF PENETRATION TESTING OF NUCLEAR SECURITY BY "BLACK HAT-WHITE HAT" TEAMS

I express the opinion, as a member of the original "bad guy/good guy team," that if the specially selected three Special Forces troops, the Government, civilian, and the independent security consultants had been granted "carte blanche" and not forbidden overt or covert team action, the debriefing of the commander of a storage site and his staff could well be conducted with the supposedly protected material lying on the conference room table.

Pursuant to one possible scenario, the first facility assigned for the penetration survey would have been reduced to a pile of rubble with heavy, if not total casualties to the defenders and the adjoining military base; the nuclear storage area would have been left in such a condition that it is highly unlikely that anyone would be able to determine the number of weapons extracted by the invaders, even if authorities could have entered the area after the attack.

It is suggested that all facilities and installations which contain nuclear weapons or fuels be subjected to a continuing program of penetration testing by teams composed of military and civilian "black and white hats," and that such facilities be monitored by operations research personnel. There is nothing like a walk in the middle of the night through the woods and over the fence to begin your day, and nothing more refreshing than lying in a snowdrift for a few hours finding out where the cookies are stored and how the security systems work. So that there is no misunderstanding, let it be clearly understood that every single facility surveyed met or exceeded existing security requirements, right down to the man with an M16 at the fence line, imposed by all levels of command.

The humans were right on. The Government's own security policies and requirements are wrong. In spite of all directed corrective action since that time, it is strongly suspected that we still have a long way to go before we can say with any degree of certainty that our Government,

military or defense contractor facilities and personnel can today successfully defend against even a small overt or covert guerrilla or dissident type of operation. This is particularly true of facilities and installations where the possibility of "in place" assistance exists, deliberately infiltrated, and made feasible through the vulnerabilities of the Government Personnel Clearance Program.

MANAGEMENT MOTIVATION, ALL LEVELS

A comprehensive human factors study should be undertaken to determine the steps that must be taken to motivate those at command levels, authors of policy, and at the field regulation-making levels to leave their "chairborne" positions in comfortable offices two or more times a year and get out in the field to installations and facilities under their jurisdiction to obtain first-hand experience, and to evaluate the environmental and morale conditions which actually affect the field forces, prior to signing off on significant policy and regulation decisions that could affect the lives of the defense forces and the capabilities of their installations to survive a guerrilla attack. Reliance on field reports from subordinate command levels, and the inspection and survey reports of field inspectors which evaluate only compliance with existing rules and regulations, is no substitute for actual field observation and experience.

MILITARY ASSIGNMENT, ROTATION, AND DISCHARGE POLICIES FOR DEFENSE FORCES

A human factors study should be made of this vital area because the armed forces have rotated many thousands of military personnel through nuclear sites, with most of the assignees ultimately being discharged back to civilian life. In many instances, due to the volunteer military concepts, many of these individuals who have been assigned to isolated sites and installations have become totally familiar with the sites' defensive capabilities, manning tables, equipment capabilities and limitations, response forces capabilities and limitations, and the vulnerabilities of the site to guerrilla warfare attack. They, in effect, become "walking encyclopedias" capable of planning and executing a successful attack on the facility if the motivation is sufficient. This applies equally to both enlisted men and officers since, in many cases, their assignment to the nuclear site is a "tombstone assignment" prior to retirement or discharge and could be very much resented. Concurrently, a human factors study should be conducted to determine the ways and means of motivating and rewarding those serving in these positions to the degree that assignment to a "hardship station" would be sought after instead of being avoided at all costs.

SUMMARY

In my opinion, the physical security of our Nation's nuclear storage and processing facilities can be improved by changes in procedure and regulations of the type described. When the overall security requirements are investigated, we must not lose sight of the people that are assigned to protect nuclear weapons and materials. I urge the testing of the security of such facilities through actual penetration exercises.

In addition, our role as the inadvertent adversary extends to many other aspects of physical security. In one respect, our unwillingness to employ lethal force and countermeasures against an intruder limits the ability to defend against him. I personally see no reason why mine fields should not be employed inside of the perimeter fence. Similarly, our Nation's concern with ecology is often in direct conflict with good security practices. I feel that it is mandatory to have a sufficient clear zone around a perimeter fence. To refrain from cutting down trees because of environmental impact is clearly placing the patrol at a disadvantage. There is no excuse for providing protective cover for the adversary only ten meters from a fence.

Finally, I feel that the physical security equipment used and installed in nuclear facilities and weapons storage facilities should be improved. In my opinion, the existing physical security is obsolete and quite vulnerable to attack should an adversary choose to do so.

A BEHAVIORAL ANALYSIS OF THE ADVERSARY THREAT TO THE COMMERCIAL NUCLEAR INDUSTRY—A CONCEPTUAL FRAMEWORK FOR REALISTICALLY ASSESSING THREATS

Phillip A. Karber and R. W. Mengel

BDM Corporation, McLean, VA 22101

Behavioral science has played a less than significant role in the field of physical security and security systems. There are some notable exceptions such as airport security, but on the whole the effort to apply behavioral science has not been monumental and its impact spotty. In part, the lack of application of behavioral science to physical security is a direct reflection of a clientele who does not understand or appreciate the role that behavioral science might play in solving security problems. The form and substance of behavioral science, requiring a multi-disciplinary approach, is beyond the average layman in most cases. The result of this reluctance to accept behavioral science as a viable approach to defining security requirements has been the infrequent use of this valuable tool.

The value in a behavioral approach to physical security issues lies in the very aspect that has limited its use, its multi-disciplinary nature. Critics of the behavioral approach stress that the behavioral sciences cannot solve security problems, failing to provide a real-world perspective. These same critics use the intuitive approach to security, emphasizing those factors related to the physical aspects and the application of resources to deterring, preventing, and responding to malevolent activity. Many of those that spurn the behavioral approach are also those that maintain that physical security systems can provide 100 percent assurance against any attack. In reality, there is no circumstance that will ensure 100 percent physical protection.

The behavioral approach provides a methodology by which physical security might be examined across the range of subjects that impact upon its success or failure. Combining systems analysis and behavioral approaches, one is able to examine physical security from the requirements definition phase through test and evaluation and implementation of a security system. The behavioral approach provides a methodology which is flexible enough to explore not only system vulnerabilities but also adversary resources and adversary motivations in terms of their inner relationships in a particular environment.

Over the past several years, the professional staff at BDM has been developing various aspects of the behavioral approach to physical security. In a recent contract for the Nuclear Regulatory Commission's Special Safeguards Study, the BDM project team developed and used a behavioral methodology to arrive at the terrorist threat to the commercial nuclear industry. In fact, this methodology provides a basic framework within which any threat analysis might be undertaken. This presentation offers a conceptual framework within which threats might be assessed realistically regardless of the environment. In applying this methodology to the nuclear industry it became apparent that its utility went far beyond that particular industry or the environment within which that industry is currently operating. In order to provide an operational setting to discuss a behavioral methodology, this presentation uses the nuclear industry to provide substantive examples.

METHODOLOGICAL FRAMEWORK

The basic framework for this behavioral approach to assessing threats is founded on seven questions which, when examined, provide a complete threat assessment. Each of the seven

questions requires the application of one or more of the behavioral disciplines in order to arrive at conclusive answers, the extent to which any one is used depending on the specific threat being analyzed and the availability of information. When each of the seven questions has been answered individually, an overall analysis is undertaken to arrive at a composite threat assessment. The seven questions to be addressed in this behavioral framework are as follows:

(1) What are the identifiable characteristics of groups viewing nuclear facilities as targets and special nuclear materials (SNM) as potential weapons?

(2) What are the courses of "nuclear action" likely to be pursued?

(3) What are the likely objectives of a group and their correlation with possible courses of "nuclear action?"

(4) Considering past terrorism, what force level, knowledge, sophistication, etc., can be expected in an attack?

(5) Are the tactics, force levels, etc., likely to be used consistent with "nuclear action" objectives, tactics, etc.?

(6) What are the means for demotivating groups from nuclear violence?

(7) Why have there been no theft or sabotage attempts against licensed plants?

In the subsequent discussion each of these seven questions will be examined in terms of the approach taken and the types of conclusions that might be drawn.

QUESTION 1: WHAT ARE THE IDENTIFIABLE CHARACTERISTICS OF GROUPS VIEWING NUCLEAR FACILITIES AS TARGETS AND SNM AS POTENTIAL WEAPONS?

The approach to Question 1 involves three steps. First, a review of nuclear related activities was undertaken to include a comprehensive analysis of actual malevolent actions, an analysis of a selected set of threats against the nuclear industry and an evaluation of statements of expressed nuclear interest which, in this case, consisted of a content analysis of over 200 terrorist publications. Second, each of these activities was examined in light of the three primary identifiable characteristics, group, target, and type of attack. Third, the activities and the identifiable characteristics were correlated with comparable analyses of non-nuclear incidents. The purpose of this latter step is to derive any pertinent information that might be available from analogous threat situations.

The review of the events themselves does not merit further discussion at this point, but some of the insights that were derived from an examination of the three primary identifiable characteristics of the incidents are important for understanding the utility of a behavioral framework. The following insights are indicative of the range of salient information that might be derived from this first step in the conceptual framework.

(1) Insider assistance is critical to covert theft.

(2) Individual motivations are difficult to determine, while in many instances specific group motivations or objectives can be ascertained.

(3) There is high interest in low casualty-potential materials, while there appears to be less interest in high casualty-potential materials.

(4) The nuclear mystique affects individual behavior but fails to appear in any of the literature reviewed.

(5) Opportunities for casual theft are available to personnel with access to materials.

(6) Out of three protest type attacks, in two instances the attacking group cited opposition to nuclear energy programs.

(7) Transnational criminals have been contracted to steal nuclear material.

(8) There is no evidence that terrorists have undertaken any actions to fabricate nuclear weapons or dispersal devices.

Although the illustrative insights offered above indicate that it is possible to draw a wide range of initial conclusions, there are limitations to this initial step, particularly when dealing with nuclear data. In the first place, one cannot extrapolate into the future from the nuclear data base, as the environment will undoubtedly change; new groups with different motivations and resources will arise; and in the future, there will be more opportunities to attack nuclear targets as the industry expands. Additionally, there is an incomplete data base of past incidents/threats and literature. To date, there is no significant "history" which might be analyzed and conclusions drawn. Recognizing these limitations with nuclear data, it then becomes necessary to go beyond purely nuclear activities and explore those malevolent actions which might be analogous either in terms of the target or the potential outcome for such an attack. For the nuclear industry there are four analogies on which one might base further analyses. Figure 1 depicts the elements of the conventional-nuclear analogy. With this as a basis, it is possible to look at other activities and industries and derive germane conclusions. This type of approach, that of determining analogous situations, has utility in any threat assessment endeavor.

Type of salient characteristic	Analogy to nuclear installations	Method of analysis	Examples
High technology targets	A. Valuable or irreplaceable equipment B. Complex scientific apparatus C. Symbolic of modern technology	Collect and analyze violent acts perpetrated against computer centers, scientific laboratories, communications networks, etc.	Mass bombings of microwave transmission towers in U.S. Western States in 1960's
Energy systems	A. Produce public power B. Salient target for those interested in disruption outside the plant	Collect and analyze violent acts perpetrated against public power plants, dams, waterworks, and fuel depots	Mass bombings against public utility plants in California 1970-1972
Protected	A. Plants protected by fences B. Armed guards on duty C. Critical areas with controlled access	Collect and analyze violent military bases, banks, and guarded shipments	Arms thefts during early 1970's
Characteristics of past attacks	A. Types of groups committing acts in the past are likely to continue a trend of violence B. Inclination toward inflicting indiscriminate mass casualties	Review past behavior of known terrorists, criminals, avenging persons, dissident employees, etc., to identify propensities toward nuclear action	Inability of U.S. left-wing protestors to inflict mass casualties on the U.S. population during 1960's

FIGURE 1. *Elements of conventional-nuclear analogy.*

At the foundation of this behavioral approach to threat assessment is the determination of the relationship between the key variables and the questions which compose the basic framework. Figure 2 provides a graphic illustration of the relationships which exist between the key variables and the questions which are the heart of the methodology. In analyzing each of the questions, the triangular relationship between the key variables must be borne in mind. In taking a total approach to the problem of threat assessment, it is important to keep in mind that neither target vulnerability nor motivations nor resources/capabilities are stand-alone factors. Rather, it is necessary to examine all of these variables in such a way that the contribution of the multi-disciplines of the behavioral sciences are brought to bear on the question.

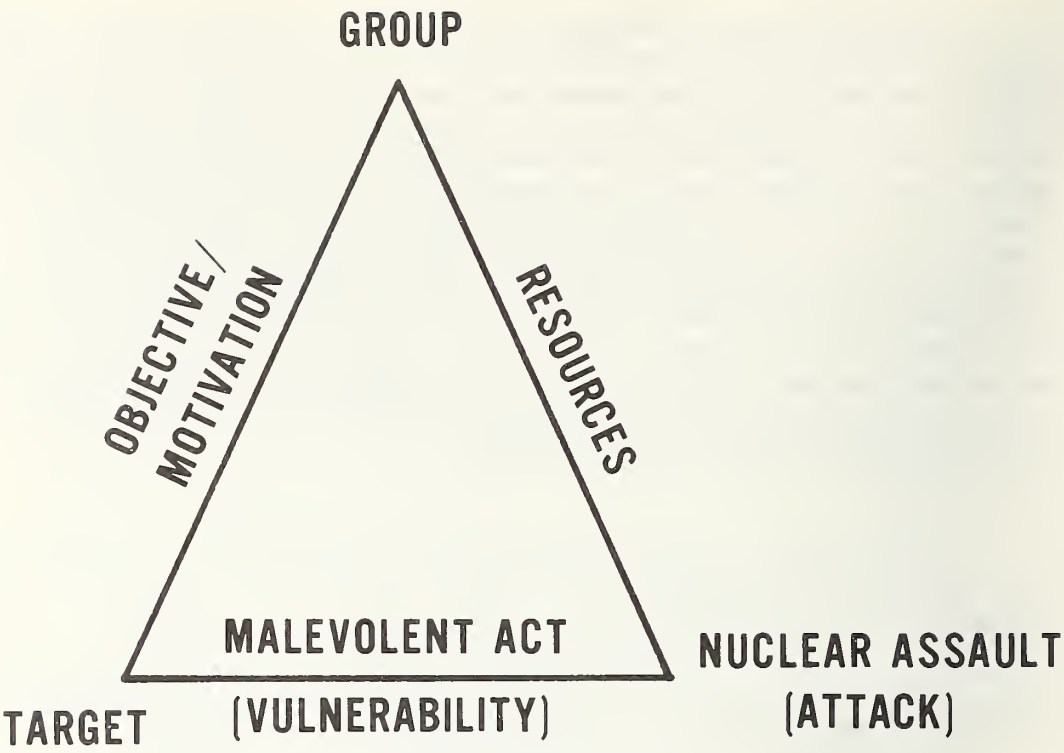


FIGURE 2. *Key analytic relationships.*

By way of explanation of figure 2, a brief description of the relationships between the various points and connecting lines of the triangle is desirable. The type of attack and the target are related by the vulnerability of that target. In other words, the type of attack necessary to overcome the target and achieve desired objectives is, in the main, determined by the vulnerability of that target. The relationship between target and group focuses on the motivation of that group. In order for a target to be attractive to the group, the target must offer a means to an end or help the group in achieving its objectives. The relationship between the group and type of attack is one of resources or capabilities. For example, if the group does not have weapons and ammunition available to it, the likelihood of an armed attack is very low.

The fifth question, which focuses on correlating motivations, resources and target vulnerabilities, will provide insights into the overall range of threats and the relative likelihood of any point on that range actually occurring. Questions 6 and 7 derive data from the relationships which are established between the key variables and, thus, depend upon the various facets of a multi-disciplinary approach to arrive at those elements which might demotivate potential attackers and arrive at an understanding as to the causes behind any current or past malevolent activities against a specific industry or set of targets. In this case, there was a desire to ascertain the means of demotivating individuals or groups from attacking the nuclear industry and ascertaining why there have not been any attacks of significance to date.

The empirical basis upon which BDM conducted this threat assessment to the commercial nuclear industry is a data base of approximately 5,000 malevolent acts collected for the period 1965 through 1977. This data base, consisting of 148 variables, primarily focuses on U.S. domestic and international terrorist activities. The data collected are multi-disciplinary in nature to include variables which depict motivation, resources, tactics, group characteristics, target characteristics, literature content, and profiles of known terrorists. This data base provided empirical support to the threat assessment, removing much of the analysis from the subjective/intuitive and placing it in the realm of the objective.

QUESTION 2: WHAT ARE THE COURSES OF "NUCLEAR ACTION" LIKELY TO BE PURSUED?

Question 2 focuses on the likely courses of nuclear action, i.e., acts of nuclear terrorism, likely to be followed by terrorists or other malevolent actors. Thus, this question attempts to identify the range of threats against the nuclear industry. In the past, three alternative approaches have been commonly used by those who have studied and postulated ranges of threats to the nuclear industry. Many practitioners of threat assessment have chosen the intuitive approach which permits a heuristic look at the range of threats. However, inherent in the intuitive approach are the disadvantages that there is a tendency to invent the maximum threat; non-explicit assumptions are made; internal inconsistencies between various levels of threat usually abound; and there is generally no evidential basis for the various threats. Second, the empirical approach attempts to identify key characteristics and establishes relationships between these characteristics. This approach, based on empirical data, tends to dispel myths which occur in threat assessments. The disadvantages of the empirical approach are that the past may not be a prologue to the future and is not predictive; there is a possibility that the sample might be biased and the validity of any subset questionable; and the majority of the data are overwhelmingly conventional, not nuclear. The third approach, the one which this conceptual framework is based upon, is behavioral analysis. This approach permits the manipulation of characteristics and the extrapolation from past data into future contingencies. The disadvantages of the behavioral approach tend to dissipate when they are combined with empirical and intuitive research. In essence, it is recognized that any behavioral effort cannot do without empirical data or the subjective judgments which form the basis for substantive conclusions.

The approach taken within the conceptual framework to examine Question 2 has been to, first, review the hypothesized attacks which have resulted from previous intuitive and empirical analyses. This created certain problems with identification of the range of threats in that only the worst threats were completely evident; it was difficult to rank the threats on a continuum, and there was no way to establish the likelihood of occurrence. From this review, it became obvious that a different approach to the question was required. From this initial review of hypothesized attacks, it was determined that the first step was to differentiate the various acts of nuclear terrorism. Once this was accomplished, it was then possible to rank these attacks according to their severity in terms of consequences to the general public. Following this ranking, it became necessary to develop the attack sequence in order to define the relative likelihood of any one occurrence. Once this attack sequence had been developed, it was then possible to identify the generic tasks involved in an attack. Drawing the above steps into a final phase, a comparison of the nuclear attack to analogous conventional malevolent actions was undertaken.

The different acts of nuclear terrorism were determined using past experience within the nuclear industry, the hypothesized attacks reviewed earlier, and a general analysis of the types of actions that might be undertaken against the nuclear industry. The different acts of nuclear malevolence are outlined and ranked in terms of attack severity in figure 3. This severity was measured in terms of the consequential public casualties for each of the acts undertaken. Although highly judgmental in nature, the determination of public consequences on a relative basis provided a means of analyzing and ranking severity.

In a separate but related step, the sequence of the attack was developed, examining the degree of penetration which was required to perpetrate the various acts of nuclear malevolent actions. The facility was generically drawn with the respective barriers indicating a level of penetration. Each of the acts of nuclear malevolent action was in turn evaluated against the schematic to arrive at a necessary and sufficient level of penetration for each act (fig. 4). Once this had been accomplished, the number of generic tasks involved in each attack was differentiated. This provided a basis for drawing conclusions concerning the attack sequence and its relationship to the nuclear industry. These conclusions include:

(1) The deeper the penetration into the facility, the greater the number of generic tasks that are required.

(2) The deeper the penetration, the greater the variety of generic tasks that are required.

(3) The deeper the penetration, the greater the number of concurrent tasks that are required.

(4) Thus, the deeper the penetration, the greater the resources required in terms of personnel, knowledge, and equipment, and the greater the degree of motivation (dedication).

There are a series of conclusions that can be drawn from the examination of the courses of actions likely to be undertaken by a malevolent actor. First, over 95 percent of the incidents examined in the nuclear industry would fall within the purview of industry, rather than posing a general safeguards problem to the public. Second, there are no incidents recorded which substantiate the establishment of any relationship between venting, dispersal and fabrication and conventional attacks in terms of public consequences. Third, in those instances when the danger to the public is consequential they are acts which involve hostage, theft and damage situations. By comparison, the number of situations of this type is extremely low.

- Hoax—dupe or trick
- Threat—expression of intent
- Harassment—limited to exterior facility
- Disruption—interruption of facility operation
- Hostage—disruption by hostile presence
- Damage—significant destruction of key facility component
- Venting—release of radioactive material on site
- Theft—material diversion outside facility
- Dispersal—release of radioactive material into public domain (off-site)
- Fabrication—development of a nuclear device with the threat to endanger public safety

FIGURE 3. *Range and rank ordering of malevolent actions.*

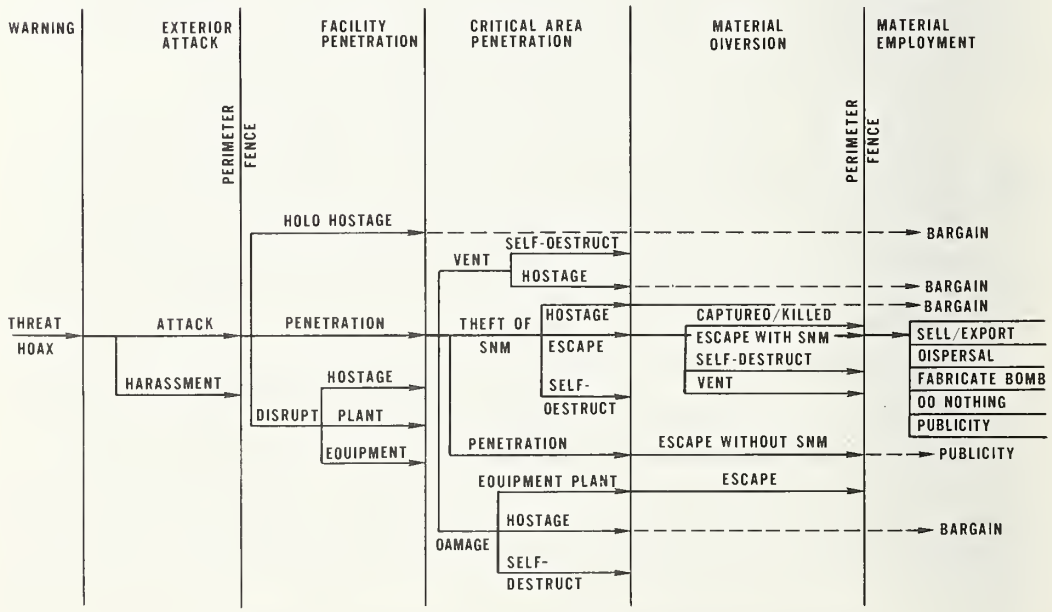


FIGURE 4. *Sequence of facility penetration and range of malevolent actions.*

QUESTION 3: WHAT ARE THE LIKELY OBJECTIVES OF A GROUP AND THEIR CORRELATION WITH POSSIBLE COURSES OF "NUCLEAR ACTION"?

Since any discussion of objectives of acts and motivations must, in and by itself, be highly detailed and involves complex studies of both group behavior and individual psychology, it is the intent of this discussion to merely highlight the approach taken to this question and provide some of the conclusions which were derived from the analysis of the nuclear industry. The approach to Question 3 is essentially twofold. In the first instance, a typology of violence approximating the objectives of likely attacks on nuclear facilities was constructed. This typology included a general violence classification which was theoretically based; a description of private versus public objectives; and an analysis of the forms of terroristic violence. The second step in this approach to motivation is the establishment of the relationships of the forms of violence to types of attack (courses of nuclear action), targets, groups, and environment.

The forms of violent behavior can be divided into two general categories with respect to motivations. On the one hand are the private motivations which include criminals, avengers, psychopaths, and vigilantes. In the other instance are those forms of violent behavior which are ascribed to public motivations and include terrorists, protesters, psychopaths, and paramilitary organizations.

In analyzing the forms of terroristic behavior, one finds that there is a relationship between target selection and the motivations/objectives of the perpetrators. Specifically, figure 5 depicts the relationships between instrumental and affective behavior and random or selected targets. In the case of randon and selected targets, they might further describe these as either discriminate (selected) or indiscriminate (random) targeting. One can see from this paradigm the relationship between target selection and the instrumental or affective objectives of the group. As the objective of the group becomes more severe in terms of societal consequences, the targeting tends to move

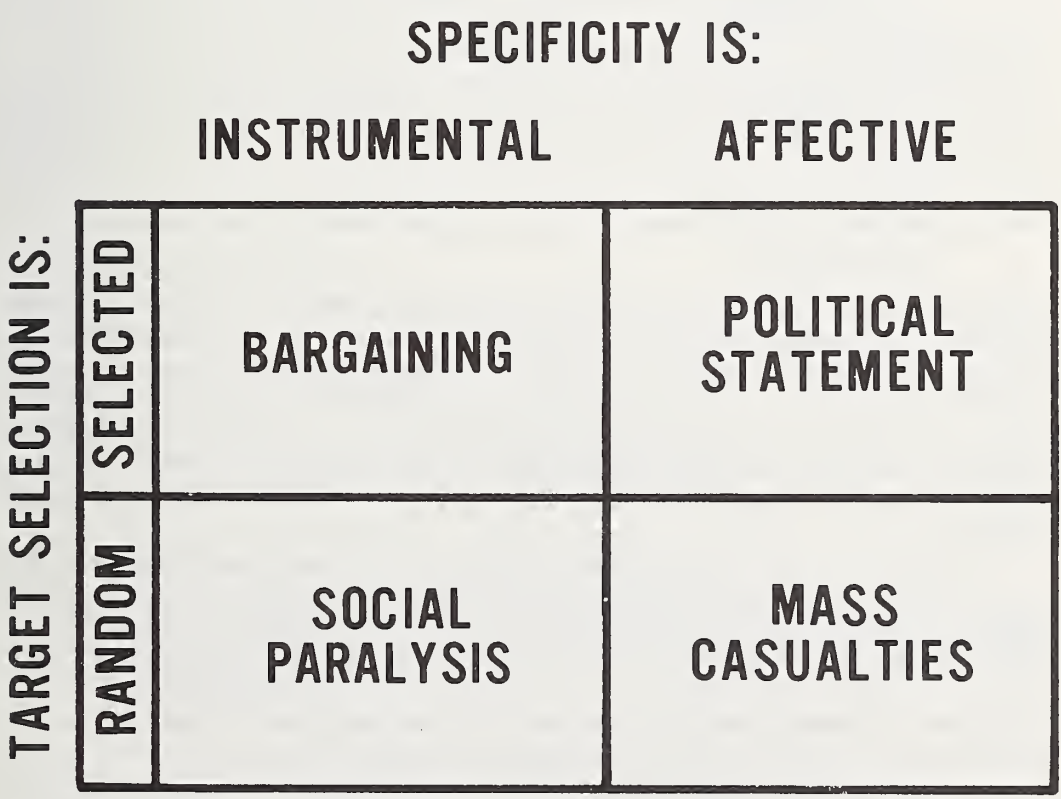


FIGURE 5. *Typology of terrorist behavior motivations.*

from discriminate and instrumental to indiscriminate and affective. For the nuclear industry the significance of this analysis lies in either the presence or the absence of the professed objectives which would tend to fall in the indiscriminate affective end of this violence paradigm.

In the course of studying motivations and possible nuclear actions several conclusions were drawn. The most significant conclusion is that generally groups have not been motivated to inflict mass casualties. This has a direct correlation and relationship to the nuclear industry. Second, individuals and groups tend to avoid confrontation which could result in death to the attacker. This is reflected in the high number of discriminate instrumental target attacks which have a low possible consequence for the attacker. Third, groups have not been motivated to attack high technology targets such as nuclear power plants, refineries and chemical complexes. Rather, groups have concentrated on highly symbolic targets such as governmental and military installations which convey a message related to the objectives of the group. Fourth, for one or two individuals engaged in violence the primary motivations have been revenge. For larger size groups, the primary motivations have been disruption, protest or simple demonstration.

QUESTION 4: CONSIDERING PAST TERRORISM, WHAT FORCE LEVEL, KNOWLEDGE, SOPHISTICATION, ETC., CAN BE EXPECTED IN AN ATTACK?

An equally important aspect of threat assessment focuses on the nature of resources available and the modus operandi of malevolent actors. Resources are one of the key components in the analysis of any threat and when correlated with motivations and target vulnerability provide the broad base necessary for complete and incisive threat assessments. The approach taken to this question is predicated on three prerequisites for a successful attack. These prerequisites are organization, training, and level of force. Specific sub-categories under each of these are depicted below:

- Organization
  - discipline
  - detailed planning
  - knowledge of target
- Training
  - tactical weapons
  - sophistication
- Level of Force
  - people
  - weapons
  - special equipment

Using these three prerequisites to a successful attack, empirical indicators of resources have been developed. For organization such items as motivational commitment, previous similar experience, and inside collaboration are useful as indicators. For measuring training as a resource one can look at the types of task involved in attacks and previous evidence of number of tasks, different tasks, and concurrent tasks in malevolent activities. With respect to level of force it is possible to empirically measure that resource by examining the number of personnel involved in previous attacks, the types of weapons and equipment used and access to and utilization of special equipment.

A few of the findings from the nuclear industry threat assessment merit mention at this point. In reviewing the frequency of attack sequences, it was found that in 70 percent of the attacks only a primary task was accomplished. For example, the placing of a bomb against a window or door outside a building involves only one primary task. In 25 percent of the cases, there were secondary tasks involved, such as entry into a building and then the placement of a device. In only 40 percent of the cases were there three tasks involved and in less than 1 percent four major tasks involved. Equally revealing are the empirical indicators related to personnel resources used in attacks. In over 95 percent of the incidents examined, three or less perpetrators were involved. This indicates that in the majority of the attacks there was a relatively small force

to be dealt with. The data on frequency of equipment usage in attacks reveals that small arms and explosives are used in the vast majority of all incidents while the occasions in which automatic weapons, crew-served weapons or communications equipment are found is limited to less than 5 percent of the cases.

From this analysis of resources it became evident that there are restraints on resources which impact on the ability of a perpetrator to undertake an attack. Specifically, the environment may limit the availability of resources to an individual or group. Second, a target may be invulnerable to overt attack because of the restraints on resources to a specific group or individual. Third, there are a series of invariant characteristics of a group which, in and by themselves, are limiting in terms of resources: there is a finite limit of force which can be brought into any one organization; the level of force is easier to change than the level of training of the perpetrators; the level of training is easier to change than the organizational structure necessary to accommodate an increase in force beyond a certain level.

A series of conclusions concerning resources was arrived at with respect to the nuclear industry. These conclusions are summarized below:

(1) Very few groups, particularly those engaged in terrorism, have the organization, training, or level of force necessary to carry out an attack against the nuclear industry with major societal consequences.

(2) Those terrorist groups that have the resources to attack a nuclear target, such as a number of international groups, have not operated, to date, in the U.S. socio-political environment.

(3) There are a number of non-terrorist groups potentially capable of operating in the U.S. that have the requisite resources to successfully attack nuclear targets and include a group of insiders, organized criminals, and military adventurers.

QUESTION 5: ARE THE TACTICS, FORCE LEVELS, ETC., LIKELY TO BE USED CONSISTENT WITH "NUCLEAR ACTION" OBJECTIVES, TACTICS, ETC.?

Question 5 provides the basis for exploring the correlations between the respective primary variables in the framework: resources, motivations, and vulnerability. The approach to this element of the framework consists of a series of seven steps through which the information derived from the initial questions were further analyzed. Specifically, the seven steps are as follows:

(1) Identify the key relationships or malevolent actions between nuclear facilities and nuclear actions (Question 2).

(2) Correlate those malevolent actions with the range of attack—objectives identified in Question 3.

(3) Evaluate those malevolent actions in terms of consistency with resources identified in Question 4.

(4) Examine interaction between resources required and nuclear actions to determine whether they are sufficient to achieve a desired attack objective.

(5) Project the interrelationships between nuclear action and the conventional type of attack which would be employed against the nuclear industry.

(6) Identify the range of potentially threatening types of groups which could possess the resources and have the objectives (motivations) required to undertake a terrorist type attack against a nuclear facility.

(7) Rank order those types of groups most likely to conduct terrorist type actions against the commercial nuclear industry or nuclear terrorism against the public.

The result of evaluations conducted through these seven steps should establish the key relationships between the types of malevolent action and nuclear facilities, the interactions

between resources and nuclear actions that affect the desired attack objective and the ultimate determination of the range of potential threatening groups and their rank ordering in the present social/economic environment.

In determining the key relationships between malevolent action and nuclear facilities, it was determined that nuclear power plants are likely to attract malevolent action which entail the facility serving as a hostage; the venting of radioactive material; or damage to the energy production capability. With respect to fuel fabrication plants the most likely malevolent actions are to be occupied to serve as hostage and to effect the theft of SNM. In analyzing reprocessing plants, it was determined that the likely malevolent actions include occupation in order to serve as a hostage and for the theft of SNM. Finally, transportation means are likely to attract malevolent action in order to effect the theft of SNM.

In viewing the interaction of resources and nuclear actions as they affect the desired attack objective, one finds that several conclusions can be drawn. First, if the attack objective is to gain publicity, it is likely that the attack will be upon the exterior, involving minimum resources in organization, training and level of force. Second, if the attack objective is to protest in some way, it is also likely that the attack will be upon the exterior of the facility and involve minimum resources in terms of organization, training and level of force. Third, in bargaining situations a penetration of the facility would be required, calling for an attack force of more than three persons and levels of equipment which would include explosives and small arms. These three examples are indicative of the types of analyses and resultant conclusions that would take place in determining the interaction of resources and nuclear actions in order to achieve a desired attack objective.

Given the present social/political environment within the United States, a rank ordering of potentially threatening groups is illustrated in figure 6. As can be seen in the rank ordering presented in figure 6, organized criminals are the most threatening group in terms of resources, capabilities and motivations. Following criminal groups are dissident employees, which is indicative of the target knowledge and target access that employees would have. Following the criminals and dissident employees in order of perceived threat are the transnational terrorist groups followed by domestic issue-oriented groups and domestic terrorist groups. Figure 7 provides a graphic portrayal of the attributes necessary to pose a safeguards problem. This same methodology might well be used in assessing any set of threats to any industry. Paramount in this assessment of the three primary attributes, motivation, target vulnerability as reflected in past targets attacked, and resources, is the ability to bring to bear the full range of behavioral sciences to include psychology, sociology, political science and human factors.

- Organized criminals
- Dissident employees
- Foreign/transnational separatists
- Foreign/transnational revolutionaries
- Issue-oriented
- Black revolutionaries
- White revolutionaries
- Right-wing extremists

FIGURE 6. *Rank order of potentially threatening groups in the present socio-political environment.*

Characteristic		Target characteristics				Resources				
Type of group	Motivation	Mass casualty	Protected	Hi-tech	Energy	Training	Organi-zation	Knowledge	Force	Remarks
Criminal			X			X	X	X	X	If market is established becomes primary threat-theft
Dissident employee	X		X					X	X	Most immediate threat because of inside position
Foreign separatist		X	X			X	X		X	Lacks motivation to attack U.S. nuclear industry
Foreign revolutionary			X		X	X	X		X	Lacks motivation to attack U.S. nuclear industry
Separatist		X	X				X		X	If motivated, mass casualty potential may make nuclear industry a target
Revolutionary			X				X		X	Motivation and overall resources lacking today
Violent issue-oriented				X			X	X		No motivation to create a safeguard danger
Reactionary extremist						X	X		X	No motivation to attack industry, no common threats
Sociopathic										No threat
Ad hoc	X				X					May be industry threat
Individual	X		X		X					Industry threat
Anarchist										No data on this type of group in the U.S.

FIGURE 7. *Attributes necessary and sufficient to pose a safeguard problem.*

QUESTION 6: WHAT ARE MEANS FOR DEMOTIVATING GROUPS FROM NUCLEAR VIOLENCE?

The question of means available for demotivating groups and individuals that are in pursuit of nuclear violence must focus on the full range of the behavioral disciplines. It is not satisfactory to state that target protection will be increased to the point that the target is invulnerable to attack. In most situations this approach is totally inadequate and unrealistic. The fact of dollar constraints forces those persons responsible for physical security to do a cost-benefit analysis in terms of what can be protected against realistically versus what can be afforded. Demotivation in a dollar constrained environment takes on even greater significance as it might be cheaper to demotivate than to spend recurring dollars on physical security. The basic approach to Question 6 is to determine what elements in the triangular relationship can be altered to enhance the opportunities for enhancing target protection. This does not necessarily mean that target security must be physically enhanced, but rather, those segments of the triangular relationship which can impact upon motivation and availability of resources must be identified and acted upon.

The key variables of resources, motivations and vulnerabilities can be altered in order to achive demotivation. In looking at each of these variables, examples of demotivating changes can be cited. In the case of motivation/objectives it is possible to exercise adaptation, alienation, legitimization of demands and actual educational campaigns. In the case of resources, it is possible to infiltrate the group with informants, establish weapons control systems, improve personnel security systems, and establish critical equipment controls. In terms of demotivation through changing the vulnerability variable, it is necessary to improve physical security to the point that outside attackers will view the situation as having a greater risk than potential attractiveness.

A series of conclusions can be reached concerning demotivation and countermeasures. First and foremost, the most difficult linkage to break in the triangular relationship is motivation. In order to alter the motivation of a group, one must primarily rely on altering the group's perception of risk versus attractiveness. Second, resources cannot be denied malevolent groups or individuals in general, but certain resources critical to handling of SNM can be monitored and perhaps restricted. Third, 100 percent target invulnerability is not possible, but systems that contain repetitive security measures, or security in-depth will deter most attackers. Fourth, intelligence must be able to provide information on the unanticipated threat and changed environment. Although most difficult in today's milieu of enhanced personal privacy and expanded freedom of information, intelligence is still a key variable in preventing and deterring threats.

QUESTION 7: WHY NO THEFT OR SABOTAGE ATTEMPTS AGAINST LICENSED PLANTS?

As a final step in this conceptual framework, it is necessary to ask the question, why have there been no attempts of theft or sabotage of licensed nuclear facilities? This same question might be posed in any threat assessment, either to determine the level of threats that have occurred to date and ascertain why that level has been reached or to explore why there have been no previous threats. In either case, the results of this question should provide the analyst with some idea as to the future potential for threats and the level to which these threats might rise.

The approach to this question is to hypothesize, using analogies and social indicators, the environments which might be favorable to an attack. As a second step, one should project the groups or individuals that are most likely to mount an attack. As a third step, it is necessary to project the objectives, resources, and consequences of an attack. In doing this, one must be able to postulate and examine the types of attack that are likely and the consequences of those attacks. At the final step in the approach to resolving Question 7, it is necessary to generate the variables that are representative of the projected environments. The accomplishment of this fourth step will permit the threat analyst to identify those variables which are primary and secondary in future environments.

By way of illustration, for the nuclear industry, five specific environmental variables were identified and the motivations, resources and consequences of an attack were examined in terms of each. These five environmental variables included:

- Group antagonism environment
- Domestic environment
- Interstate environment
- Interstate nuclear environment
- Nuclear technology environment

Each of these in turn was examined in terms of the change in the environment which must take place and the potential type of malevolent action which might result should a group undertake an attack. In answering Question 7, one has, in essence, examined the range of potential future threats to the industry.

BEHAVIOR AND MISBEHAVIOR OF TERRORISTS: SOME CROSS-NATIONAL COMPARISONS

D. Jane Pratt

The Mitre Corporation, McLean, VA 22101

> Our world today is full of violence...our society, despite its claims to peaceableness and justice, is in fact one of the most violent societies in the history of the world.....the issue of violence is to this generation what the issue of sex was to the Victorian world.
>
> —Kenneth Keniston
> Young Radicals, 1968

We are all exposed to the threat and/or use of violence in our daily lives, from the threat of mass "technological death" from nuclear war to terrorism and street violence, which are reinforced and even sensationalized by media coverage. Vicarious violence is so prevalent that by the age of 14, the average American child has witnessed 11,000 murders on television.[1] Our world today is not just full of violence; our world, while still disapproving, has come to accept violence. Megadeath, "ordinary" violence, and vicarious violence combine to produce a climate in which some people need to act violently in order to discharge their own excited rage (Keniston, 1968).

This discussion is concerned with one type of violence: terrorism. More specifically, the concern for the potential terrorist threat to nuclear facilities—a special form of terrorism that would combine the technological threat of mass violence with the apparent irrationality of the terrorist. We are trying to discover the differences between a violent person and a terrorist, and between an "ordinary" terrorist and the nuclear variety.

The responses terrorists seek are the creation of terror itself, and the subsequent alteration of behavior under actual or threatened duress. It would be desirable to have the National Bureau of Standards define a "standard nuclear terrorist" for us in much the same way as they define a standard meter, kilogram or teaspoon. Unfortunately, terrorists can be described only by attributes that are much less precise than physical standards.

CHARACTERISTICS OF TERRORISTS

This paper discusses the analytic approach and empirical evidence required for a thorough study of the terrorist threat posed by domestic insurgents. The first step for analysts is to determine which specific people or groups are likely to behave violently. Identification of particular types of violence-prone individuals would, it is hoped, permit the development of techniques and systems for preventing their antisocial behavior.

Within the group of those who are violence-prone, it is next important to distinguish those who could and would engage in terrorism, defined as the use of politically motivated violence by individuals or small groups directed against established authority, and often directed specifically at symbolic targets. Individual fanatics, non-political violent groups and even money-motivated sophisticated criminals are interesting departures for a study because some of their techniques and organizational structure could be copied by organized terrorists. They also contribute to a heightened climate of violence, which has led to "imitative violence."

[1]According to the National Citizens' Committee for Broadcasting, 1977.

However, it would be dangerous to use the analogies as more than a departure for characterizing potential nuclear terrorists. Some of the characteristics of analogous groups clearly do not apply to potential nuclear terrorists. Empirical studies show that bank robbers attempt to avoid violence, for example (Fine, 1976), while terrorists do not. Further, the disruption of a nuclear facility or theft of special nuclear materials (SNM) would require special skills and knowledge in addition to those possessed by most of the analogous groups. To overcome existing security systems and safeguards would require an understanding of nuclear engineering, knowledge of plant design and security systems, coordination between several individuals, and most probably, inside help to gain access. Special equipment and techniques may also be required, such as weapons, explosives handling equipment and communications systems.

Because no single individual is likely to possess the necessary combination of knowledge, skills and access, it is hypothesized that the primary terrorist threat to nuclear facilities would be from a well-organized group with sophisticated planning and operational capabilities. Because it is further assumed that the nature of the operation requires a very high level of motivation, it is also assumed that potential nuclear terrorists would be politically or ideologically motivated.

In a recent Mitre study of "The Threat to Licensed Nuclear Facilities" (MTR-7022, 1975), the characteristics of members of a number of groups possessing capabilities that represent a credible potential for terrorism against nuclear facilities were analyzed. It was concluded that the types of terrorists most likely to possess the required combination of skills and motivations are foreign intelligence agents and domestic insurgents who are ideologically motivated and have received paramilitary and ideological training over a period of years.[2]

As a result of the study, the foreign intelligence agent was characterized as follows:

(1) The psychology of foreign intelligence agents operating in this country is clear. They are pragmatic. To them, international affairs are like a chess game, in which their task is to obtain information of an economic, social, political, military, scientific, industrial, and technological nature.

(2) Strongly patriotic, most would rather die than defect. They are secretive by nature, quiet and unobtrusive in demeanor, and clandestine in their efforts. They are rational. They have specific assignments and explore every avenue to collect the information necessary. They are constantly alert to opportunities to exploit any individual they may convince, dupe, or coerce into aiding them. They are objective about the risks in their jobs.

(3) Frustrations do not unsettle their mental composure. They are optimists, confident that setbacks are only momentary and will not upset their scheme of things. They are working toward long-range successes they see as inevitable, and they derive personal satisfaction from their contributions toward that end. In short, they are very much in control of their emotions and psychologically are stable individuals, because they live and operate within a framework of personal conviction and dedicated discipline.

The responsibility for identifying, studying, monitoring, and controlling subversive acts by foreign intelligence agents rests with the CIA and the FBI. Because of similarities in organization, training, and operations, studies of foreign intelligence operations can also tell us something about the domestic insurgent. However, it was found that the domestic insurgent has many distinctively different attributes:

(1) The violent revolutionary in our society is equally dedicated; however, he is frustrated. He is convinced no legitimate channel exists through which he can change a system he sees as repressive, corrupt, and decadent. He claims protests and marches have failed, and that the only alternative is violence.

(2) He looks upon himself as a soldier. He is part of a group that has declared war on the enemy—the system. He is affiliated with a still larger army—the revolutionaries throughout the world, who fight for "liberation."

[2]It should be noted that domestic insurgents need not be U.S. citizens. They may be members of the informal brotherhood of transnational terrorists.

(3) He sees himself as playing a unique and important role. He is living within the enemy's camp. Therefore, he must use his wits and clandestine methods to avoid capture. Surrounded as he is, he often becomes paranoid.

(4) He obtains guidance and inspiration from the revolutionary leaders abroad. His ideology is a mixed blend of anarchist, Marxist-Leninist and Maoist concepts. His views emerge in the form of generalizations, rhetoric, and plagiarized revolutionary expressions.

(5) He is more an activist than a thinker. He depends more on passion and instinct than logic and rational analysis. He feels duty bound to strike out against all the symbols of repression, in order to let the enemy know that the forces of resistance have not given up.

(6) For some, the ultimate act is martyrdom. He will make his mark on the pages of history. His name will be recorded alongside those revolutionary heroes who have died for the cause throughout the world. This is in contrast to the espionage agent, who is content to work without the reward of fame.

(7) The psychological motivation of such individuals is as important to the selection of targets and choice of weapons as are external events. Certainly another situation raising mass public dissent like the Vietnam War would raise the likelihood of either a foreign or domestic group attacking a licensed nuclear facility or engaging in terrorism with a nuclear device. Plans for sabotage developed by foreign intelligence agents would then assume increased importance.

The domestic insurgent is a distinctive type, and it would be useful to know how to identify such individuals, how they are recruited and trained, how they are organized and how they operate.

Most American dissent is open, and as long as it remains so, concerns us only peripherally. When direct confrontation with authorities or sinister motivations drive opposition underground, however, it becomes more dangerous. Terrorist activities by domestic insurgents are more likely to emerge from small, secret groups than from public, mass movements. American insurgent groups, however, tend to be fragmentary, shortlived and incompletely formed; legal restrictions have also limited the collection of information on these groups, so that they have not been fully studied.

Most domestic insurgent groups, however, have emulated the examples of foreign revolutionary organizations employing terrorists, such as the Vietnamese National Liberation Front (NLF), the Palestinian Liberation Organization (PLO), and the Cuban-style groups. Certain characteristics are common to the most successful of these; and it is even hypothesized that these characteristics are sufficient if not necessary in running a successful operation. Because the NLF represents a fully articulated, successful and highly imitated organizational model for violent domestic insurgents, and has been extensively studied,[3] this model and its applicability to the American terrorist potential is the focal point. Note that this model need not apply to other potential threats to nuclear facilities such as foreign agents or individual fanatics, who are beyond the scope of this discussion.

A MODEL OF TERRORIST ORGANIZATION AND OPERATION

For terrorists to launch an attack against a nuclear target would require a combination of institutional opportunity, appropriate "objective conditions" (a term by which Marxist-Leninists refer to current events), and the existence of a trained, dedicated team of individuals with a specialized mix of skills. From previous experience with terrorists of this sort, it may be fairly certain that such a plan is not likely to originate with the people who are responsible for carrying it out. Rather, the planning and decision to launch a coordinated attack against a nuclear facility is more likely to originate at the top echelons of an organized, ideologically committed, extensive network of cadre. Having assessed "objective conditions" to be ripe, the leaders would commit selected individuals in the organization to execute the action.

[3] e.g., Pike, 1966; Pratt, 1975; The Rand Corporation, 1965.

There are a number of groups, both domestic and foreign, whose characteristics fit the model just described. Typical organization of the most threatening subversive groups is likely to be based on the principle of a strict hierarchy with authority flowing from the top down. Individual members are frequently organized into three-member cells, and strict secrecy is maintained, particularly with terrorist squads. Communications between cells is limited and based on "need to know." An act of nuclear terrorism would most probably be decided upon, planned and ordered by the highest levels of such an organization; the operation, however, is more likely to be carried out by specially selected individuals at other levels, who may well be unaware of the identity of those who plan the action.

The organizational principle of the three-member cell may be extended into a general principle of triadic structure for operations. The taking of hostages in three separate locations, or the simultaneous attack on three different targets, for example, are based on this principle. Multiple targets increase the likelihood of success by severely constraining the response available to authorities. It is reasonable to assume, therefore, that a terrorist attack on a nuclear facility may be launched against more than one nuclear target; or, major non-nuclear attacks may be launched simultaneously or just prior to a nuclear attack to divert and disperse security forces.

Tactics of terrorist groups aim at high visibility for their (public) operations for the terror is itself an end, demonstrating the weakness and vulnerability of the system, creating chaos and distrust of the government's ability to provide basic security for its citizens, and undermining the most fundamental basis of government authority.

The nuclear terrorist is most likely to be a member of an established group or organization, rather than a newly created group. Members most likely to be employed in sabotage or violence are the hardest to detect within such organizations, for they are generally kept hidden until told to act. Great care is exercised to keep such individuals isolated from public activities; they do not, as a rule, participate in overt propagandizing but may be associated with those who do. Such associations explain the official alarm that arose when it became known that a physics professor in Germany had friendly ties to associates of the Baader-Meinhof gang.

RECRUITMENT TO THE ORGANIZATION

Within Marxist-Leninist, Maoist and Cuban-style revolutionary organizations, recruitment follows a guided strategy, everywhere relevant to and consistent with general ideological considerations. An examination of the selection process, therefore, can tell a great deal about the type of individual who becomes a terrorist.

A terrorist is unlikely to be involved directly in any but the final stages of the process of recruiting new members. Rather, the initial and intermediate phases of the process are usually undertaken by members with less sensitive functions.

According to a former Communist Party member who served the Vietnam National Liberation Front as a propaganda and education cadre:

> Yes, there are norms. Whenever they are looking for new memberships, and this does apply to all people's organizations, they have principles to stick to. There are inquiries to be conducted, propaganda works to be done, there are training courses, there are trials before they accept new members. Inquiries, propaganda, training, trials, organization. These are the five phases, all of them mandatory, which lead to memberships. They have called them the five steps of the recruitment process.

The NLF exercised definite and regular preferences with regard to the type of person targeted for recruitment. In general, it was the Party that selected the recruit, and not vice versa: "The Front has a political network with experienced cadre, and they have the responsibility for selecting, for contacting the students. The students don't need to look for them, but they will look for the students," according to a former Party member. As a general rule, particular attention was paid to the potential target's mental attitude; but doctrine also required that the inquiry focus on class origins and current class affiliations.

A former professor of Marxism-Leninism at the University of Hanoi stated categorically in an interview:

> The priority for recruitment comes from the worker's families. Because according to Marxism-Leninism, this class really hates—they are the most miserable class of the society, and for this reason they're very displeased with the present government. And [as a contrast] take me, for example. Even though I know very well Marxism-Leninism, because I don't come from this class, it's very difficult to motivate people like me! For that reason, in North Vietnam, it's usually the children from the poorer, the peasant class who are selected to be sent to Russia for training; and the children of the rich people are not allowed to go abroad.
>
> But I also have to tell you this. What Marx said in his written work is that when the ideology penetrates the public, it will convert into a material force. And in the present circumstances, because of this, the intellectual class can be considered as a basic class too. For that reason, the Communist cadre carry out their propaganda with the intellectual class, and that's something very important.
>
> Such is the Communists' angle, even though a student comes from the rich class of society, if he has changed his mind already, sure he will be accepted to be a Party member—but with all the precautions.
>
> I have to stress this point. The objectives are to take students and school children into the organization. Then, the basic elements here are those with good political inclinations—the intellectual people they have called the progressive intellectuals. You see, such elements have realized the slogan, "Unite farmers, workers and small capitalists." Basic elements in students' organizations do not need to come from the basic social classes. The Communists are very flexible with tactics! [Emphasis added.]

The conclusion, then, is that the NLF, for ideological reasons, preferred when possible to recruit new members from the "basic classes"—the workers' class and the poor peasants' class. In practice, however, the true working class is small and the poor farmers unsophisticated, while students are eager, willing and capable. The result was that—for students at least—"basic class" meant students who had an appropriate mental attitude, and this amounted to little more than rationalizing in ideological terms the very sensible practice of selecting those who were already predisposed towards the movement and its aims.

The same practices have been employed by groups in Latin America, where membership in terrorist organizations often consists of an otherwise unlikely combination of students, workers, and peasants. Liberalism and strong anti-government views suggest predispositions suitable for potential recruits. Further, youth itself is almost a prerequisite, for all such groups prefer to train individuals whose beliefs are incompletely formed. Individuals with strong religious ties are not considered suitable for selection. However, high moral standards are considered necessary; for corrupt, immoral members are generally considered untrustworthy for sensitive operations.

Who is recruited varies somewhat among countries and groups. Within the model being described, however, selection criteria tend to be quite consistent, so that it is possible to describe a characteristic type for many groups. As noted earlier, for example, activist students recruited in the U.S. in the mid-60's were frequently children of liberal or leftist parents whose only outstanding complaint about the older generation was that they did not act out their beliefs. Many of these activists were recruited as students in leading universities, a large proportion were actually "self-recruited," participating in open protest before being driven underground. They were of predominantly liberal, middle- or upper-middle-class families, good students, and disproportionately Jewish—perhaps reflecting the strong intellectual tradition of a large segment of American Jewry (Keniston, 1968).

It is quite certain that thefts of significant quantities of SNM have occurred. It is equally certain that nuclear facilities are vulnerable to a determined terrorist attack, and that opportunities exist, as do trained individuals to carry out instructions for attack. Although existing security systems and safeguards do serve the function of making nuclear targets less attractive, the fact that no major attack has yet been aimed at disrupting an operating facility in the United States does not prove security systems effective. Equally, the lack of an attempt could be due to an assessment by terrorist leaders that "objective conditions" are not yet suitable or that more promising targets exist elsewhere.

Fortunately, a change in objective conditions may be as perceptible to would-be preventors as to would-be perpetrators of a terrorist attack on nuclear facilities. Because of the organizational imperative of groups such as those described in this study, it is even probable that the existence and extent of a heightened threat would be signaled in advance:

(1) Increased attacks by terrorists on nuclear facilities abroad would...signal an immediate need for tighter security here. Whether by design or imitation, these activities often follow a pattern: skyjacking and political kidnappings serve as an example. The recent attacks on operating nuclear power plants in France are likely to be a precursor of a series of such attacks, in France, and perhaps, in other Western European countries.

(2) Expanded contacts between organized crime here and supporters of terrorist groups abroad would also raise significant questions. For example, published reports have indicated that Colonel Qadhafi of Libya has offered millions of dollars for strategic quantities of plutonium. These large sums of money could attract the attention of organized crime.

(3) Any movement which organizes very large demonstrations at nuclear sites might attract extremists to the cause. Such demonstrations could escalate, either by accident or design, to confrontations and clashes with police forces. Increased militancy of a clandestine nature, including the use of explosives, might follow.

(4) Further indication might be found in the underground press. In the past, such publications not only supplied the drum beat but also pointed the way for those marching with destructive intent on government and corporate structures.

Given warning of an increased danger, increased security and surveillance could lessen the chances of terrorist success.

Because the consequences of a successful terrorist attack against a nuclear facility are potentially catastrophic, the problem of identifying and characterizing potential terrorists is urgent. We must also begin immediately to focus on how to deal with the ones who have, and will, get through the preventive screens; and we can learn how to do this only by learning what they teach us about themselves.

REFERENCES

Brennan, C.D., et al., 1975. The Threat to Licensed Nuclear Facilities, the Mitre Corporation, MTR-7022, McLean, VA.

Fine, Allan, 1977. Perpetrator Attributes in Threat Analysis, in *The Role of Behavioral Science in Physical Security*, National Bureau of Standards, NBS Special Publication 480-24, Washington, DC.

Keniston, Kenneth, 1968. Young Radicals, Harcourt, Brace and World, New York, NY.

National Citizens Committee for Broadcasting, 1977. Newsletter, Washington, DC.

Pike, Douglas, 1966. Viet Cong, The Massachusetts Institute of Technology Press, Cambridge, MA.

Pratt, D. Jane, 1975. Student Political Activism in the Vietnam Conflict, unpublished Ph. D. dissertation, Department of Political Science, MIT, Cambridge, MA.

ATTRIBUTES OF POTENTIAL ADVERSARIES TO U.S. NUCLEAR PROGRAMS[1]

Allan M. Fine

Sandia Laboratories, Albuquerque, NM 87115

INTRODUCTION

Sandia Laboratories, in its activities as a prime contractor for ERDA, has been heavily involved in the research and development of physical protection elements and systems applicable to the protection of nuclear facilities and materials. A part of this effort has involved the characterization of potential threats to U.S. nuclear programs. The Rand Corporation, under contract to Sandia Laboratories, has investigated several hundred incidents which involved activities that could serve as analogs of potential threats to U.S. nuclear programs. This paper summarizes the data used by Rand and provides a listing of potential adversary attributes derived from a historical-incident data base. The attributes are expressed in terms of the capabilities of a composite adversary group.

DATA BASE INFORMATION

In the United States, no nuclear installation has been attacked, seized, or effectively sabotaged; no nuclear weapons have been diverted or illegally detonated; no nuclear materials have been stolen or taken by force or used for blackmail or made into an explosive device; and no radioactive materials have been maliciously released. Although there have been telephoned bomb threats to many U.S. commercial and governmental nuclear installations, some minor industrial sabotage related to labor problems, and some accidents resulting from poor training or inferior procedures, no major incidents concerning U.S. nuclear programs have occurred.

Outside the United States, more serious events involving nuclear materials and facilities have occurred: political extremists have sabotaged reactors in France; urban guerillas have seized control of a nuclear power plant in Argentina; and a mentally disturbed individual has spread radioactive materials on a train in Europe. While these events are serious, they have not occurred in sufficient numbers to permit extrapolation to adversary attribute characterization for use in describing potential threats to U.S. programs. However, inclusion of these types of incidents in a more general data base of information can yield insights into the *modi operandi* of perpetrators of such actions and provide utility in characterizing U.S. program needs.

While it is fortunate that no major incidents involving U.S. programs have occurred, conversely security analysts have little hard information on the basis of which to postulate potential adversary characteristics. Because of this factor, it has been necessary to go outside the nuclear program realm and to examine incidents which could provide data on potential adversaries in terms of analogous events which have characteristics transferable to potential nuclear incident perpetrators. Rand analysts have used this approach to provide a set of analog incidents—historically based, factual, and detailed—to accumulate a data base. This data base is intentionally limited in scope and is capable of providing information from the incidents chosen for a relatively

[1]This work supported by the U.S. Energy Research and Development Administration.

select group of questions relating to perpetrator attributes observed or determined from the action incident. The attribute list for which the data base incidents have been chosen includes:

- Number of attackers
- Armament
- Knowledge (technical, operational)
- Training (technical, operational)
- Equipment used
- Transportation modes
- Dedication to mission
- Planning for mission
- Overall resources available

The various types of events used as analogs are:

- Sophisticated crimes: Robberies and burglaries by groups against high-value, protected targets for monetary gain.
- Symbolic bombings: Bombings by groups of political dissidents for material damage.
- Terrorist attacks: Seizures of facilities and/or hostages; group action for political gain.
- Sabotage: Actions by individuals or groups to damage facilities.
- Large scale extortion/hostages: Group actions for massive political or economic gain by threat of wide-scale damage.
- Mass casualties: Historical use of weapons or acts to kill large numbers of people for political gain.

  Wartime incidents of dedicated groups attacking defended targets.

SPECIFIC ANALOG PROFILES

Rand analysts have completed work on several analogous incident reports and have others in process. In order to provide a listing of attributes, several analogous incidents were selected for concentrated study. The data base for these contains nearly 200 incidents covering sophisticated crimes, terrorist assaults, and bombings. These events were selected because their characteristics approximate the intentions and capabilities believed to be required for attacking or penetrating a nuclear facility by stealth or force of arms for the purpose of seizing hostages, sabotage, or theft. For each of these analogous incident types, a profile of typically displayed attributes has been compiled and a general profile of the typical attributes—based on a combination of the specific profiles—has been derived.

PROFILE 1. TASK FORCE CRIMES OR "CAPERS" (ROBBERIES AND BURGLARIES)

The data base in this category comprises crimes committed by groups of people, some of whom are highly specialized and skillful. The perpetrators assemble for the specific operation and form "task forces" organized for assaults on well-protected objectives such as bank vaults and museums. The prizes sought are substantial, and the adversaries display some high-level capabilities. Specialists involved may include but not be limited to safecrackers, electronics experts and communications experts. The current data base of nearly 200 incidents includes 46 such crimes. Of these, about three-fourths were committed in the United States and one-fourth abroad, primarily in Canada. Most are burglaries (involving surreptitious, forced, or illegal entry); the remainder are armed robberies, such as the famous Brinks robbery in Boston, or attempts to release prisoners. One of the prison breaks and an arsenal robbery involved members of political extremist groups; none of the other task force crimes had political overtones.

Almost all of the cases examined were successful. The adversaries evaded or overcame the security measures and escaped with the goods. It would be instructive to examine failures as well

as successes, but information on these is hard to obtain. The professional criminals involved appear unwilling to assume major risks; confronted with high risks of failure or apprehension, they are likely to abort the operation. Of course, failures generally are not as well publicized as spectacular successes, making it difficult to even know about them; unless the perpetrators are apprehended, there are few means of determining what resources they had assembled for their attempt. Figure 1 is a listing of the task force crimes profile.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
				"ROBBERY"				
3-6	Handguns, shotguns	Hand and power tools	Foot, commercial vehicles	Mid	Mid	Information	Mid	Mid to high
				"BURGLARY"				
2-4	Usually not displayed	Explosives, and power tools	Foot, commercial vehicles	High	Mid	Information	High	Mid to high

FIGURE 1. *Task force crimes profile.*

PROFILE 2. ASSAULTS

This portion of the data base includes 32 terrorist assaults. Of these, 23 were related to the conflict in the Middle East: eight took place in Israel, four elsewhere in the Middle East, seven in Europe, three in Asia, and one in Latin America. The targets of 14 of these incidents were Israeli assets, including El Al offices, aircraft, diplomatic posts, and personnel outside Israel. Arab assets (e.g., embassies) were the targets of two incidents; U.S. assets or citizens were the targets of six incidents, including an Amman hotel seizure in 1970, the Lod airport attack in 1972, the seizure of the Bank of America in Beirut, and attacks on two parked aircraft in 1973. Three assaults took place in Latin America and six took place elsewhere: the seizure of a train and of the French embassy in the Hague and the seizure of the U.S. embassy in Kuala Lumpur, an assault on the German embassy in Stockholm, and an attack on a San Francisco police station. Although the risks involved in the terrorist assaults exceed those involved in the task force crimes, for the most part these were assaults on soft targets; the assailants could expect at least to seize control of the facility or hostages without running into serious armed resistance. Figure 2 is the profile of attributes of the "typical" terrorist assault.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
3-6	Handguns, automatic weapons	High explosives	Foot, commercial vehicles, air	Mid	High	No	High	Mid to high

FIGURE 2. *Typical terrorist assault profile.*

PROFILE 3. BOMBINGS

The current data base consists of 108 bombings which occurred between 1965 and 1976 in the United States. The targets were about evenly divided between commercial facilities (e.g., corporate headquarters and banks) and government facilities (e.g., office buildings and consulates). However, a few residences were involved. The bombings were mainly of soft targets; attacking them presented little risk to the perpetrators. Most had minimal or no security system. The bombers were motivated by political extremism, personal animosity, anger at particular corporations, and anger at or resentment of public officials or the acts of public agencies. The total casualties of the bombings were four dead and 69 injured. Figure 3 is the typical bombing profile.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
1-2	Explosives	Hand tools	Foot, commercial vehicles	Mid	Low	No	Mid	Mid to high

FIGURE 3. *Typical bombing profile.*

PROFILE 4. COMPOSITE FOR U.S. ACTIONS

By combining the attributes of the analogous incidents shown, a composite model, figure 4, of attributes has been developed. The composite is based on typical values from each of the contributing profiles. An adversary group adhering to this composite might exhibit the following characteristics: three to six perpetrators armed with hand guns, shotguns, and automatic weapons; access to and egress from a target by almost any type of commercial land vehicle; tools used could be hand-held, portable power tools, and there could be limited use of high explosives. The group would have the benefit of good planning for the mission and would exhibit sufficient ingenuity, technical and operational skills to provide for proper execution of the operation. Group members would be sufficiently dedicated to the group and its mission to risk capture or injury. Assistance or information from an insider could help the group complete its mission.

It is important that the composite profile not be misconstrued or misrepresented. It represents the typical profile of potential adversaries as derived from other profiles of selected incidents believed to be analogous and transferable to potential adversary activities relating to U.S. nuclear programs. The composite is *not* a description of "the threat to U.S. nuclear programs," nor is it intended to describe "the current threat" to any facility. It is a description of typical values of

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
3-6	Automatic weapons, grenades, shotguns	Hand tools, power tools	Foot, commercial vehicles	Mid to high[1]	Mid to high[1]	Information or other assistance from one "insider"	High	Mid to high

[1]Generally not seen together at high levels.

FIGURE 4. *Composite for U.S. actions.*

characteristics of adversaries observed in the perpetration of malevolent actions. The insights gained in the description of these characteristics are intended to provide a basis for consideration of adversary threat characteristics to any security system.

There is nothing in the "typical" profile to preclude individual attributes from taking different values from those listed; in fact, the episodes used for data base information in formulating profiles contain items in which many of the attributes of the typical profile are exceeded. An interesting tabulation can be constructed by combining the high levels of attributes found in the various analog incidents and making a "high level" analog composite. Such a tabulation is an artificially constructed one because the higher level attributes represent values not seen in the basic data as combined high-level attributes, but rather as an individual high value within a given analog incident.

A high-level composite profile based upon high levels of attributes from the analog incidents is shown in figure 5. For this high-level composite, the number of perpetrators is increased to a range of 12-20, armament is enhanced to include crew-served weapons, transportation includes aircraft, and other related attributes are all at the high level.

Number of perpetrators	Weapons	Tools	Transport	Criminal and military skills	Dedication (risk)	Inside assistance	Planning	Ingenuity and imagination
12-20	Anything up to and including crew-served weapons	Explosives, power tools	Foot, commercial vehicles, air	High	High	Information and possible active help	High	High

FIGURE 5. *High-level composite profile.*

Analysis of the data base incidents by Rand analysts indicated that many of the attributes listed at the high level do not generally appear at a high level within sets of analog types of incidents. As an example, figure 6 shows a generalized plot of two of the attribute characteristics—dedication and technical sophistication. At the high level of dedication (risk of capture, injury, or death), one finds many perpetrators of terrorist assaults; at the high level of technical sophistication appear perpetrators of sophisticated burglaries. These characteristics are found as extremes in two different types of activities, while in the high-level composite profile (fig. 5) they appear together (upper-right region of fig. 6). The high-level composite calls for the combination within a group of diverse characteristics which leads to the conclusion that such a combination is of low likelihood and thus contributes to the artificiality of the high-level composite profile as a derivative of the analog data.

There is no reason to believe that a group of adversaries could not contain large numbers of people, could not use aircraft or helicopters, could not have crew-served weapons, and could not possess all the high levels of attributes in areas of skills, planning, and dedication. There is no justification to believe that such an adversary group could not exist; however the data from historically-based perpetrator incidents have not indicated that such a group has existed outside of wartime, nationally-sponsored, military experiences. For the non-war, sub-national, potential U.S.-based adversary, a group possessing all the attributes of the composite high-level profile would be expected to be extremely rare.

Analysis of the analog incidents, profiles, and composites has led to the tentative conclusion that physical attributes do not appear to be the most critical for an adversary. The high-level composite was constructed to show some degree of criticality in attributes for a potential adversary, that is, those attributes which appear critical to an adversary to assure the success of a mission. It

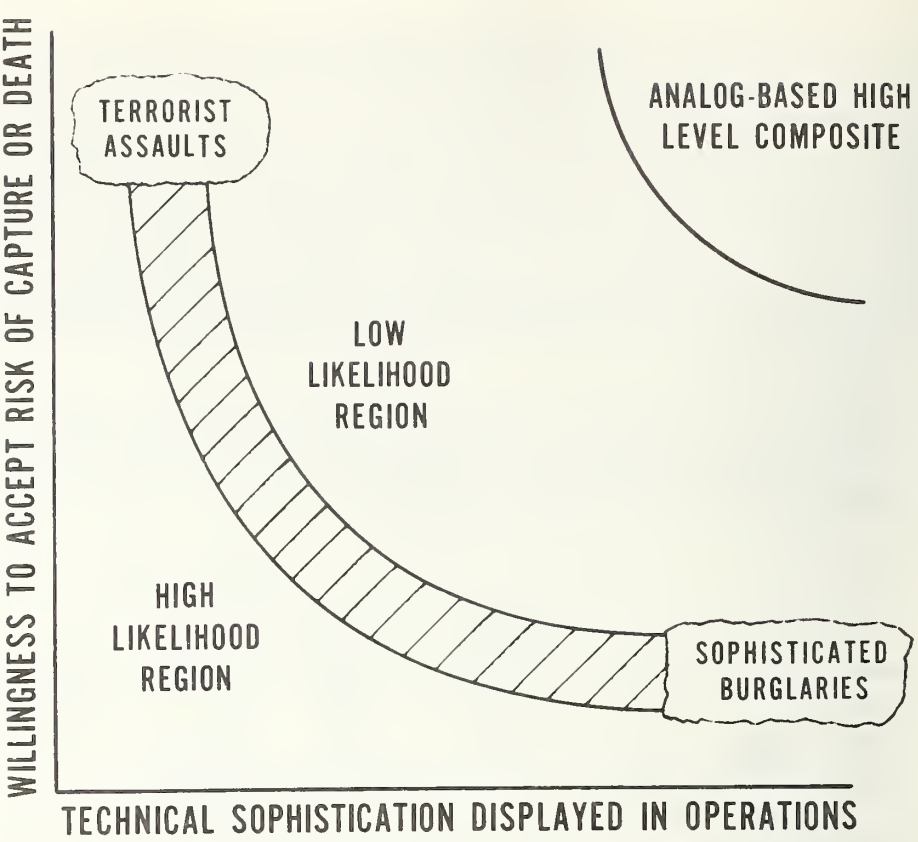


FIGURE 6. *Dedication vs. sophistication.*

appears that human factor type attributes, in combination, may be the most critical ones for a potential adversary group to possess. In the United States today, it is not difficult to obtain arms, ammunition, explosives, tools, equipment or specially skilled people for a specific task. Given that these physical attributes are available, other factors appear as critical constraints to potential adversaries. The critical factors which quite often decide the success or failure of a mission include:

- Imagination and ingenuity
- Criminal and military skills
- Technical knowledge and capability
- Dedication (willingness to risk capture, injury, or death)
- Fostering or cultivating inside assistance for a mission target

SECURITY SYSTEM IMPLICATIONS

The use of analog incidents and attribute profiles provides a means to generalize the needs of generic security systems in terms of defending against an adversary group possessing the given characteristics. Two aspects of physical security arise in consideration of the attribute listings: physical attribute defeat and human factor deterrence.

A security system should extract some minimum "price of entry" from an adversary in terms of requiring the adversary to possess the high levels of physical attributes. The more a security system tends to force a potential adversary toward the difficult-to-obtain high-level composite attribute list, the more severe will be the requirements for the adversary to assure a successful mission. Barriers, fences, alarms, guard forces, surveillance, and vaults are among the security related items which can contribute toward forcing an adversary to high, possibly detectable, levels of resources.

In terms of thwarting the critical attributes of a potential adversary, a security system should pose danger and risk to adversaries; it should possess features which are "mysterious" or unknown to outside (and many inside) personnel; it should promote change in appearance, tactics, and routines just for the sake of change; and it should utilize updated equipment to the degree necessary and commensurate with the material or facility to be protected. The combination of elements useful in thwarting potential adversary capabilities may vary from facility to facility, but the general theme is to create conditions which attack those attributes of skill, knowledge, dedication, and planning capability, and either deter the adversary group directly or force the group to go to extremes to provide the resources for a mission.

FUTURE WORK AREAS

The adversary attribute study by the Rand Corporation is continuing. Attribute description and data base information are in preparation and will be updated throughout the year.

In addition, the program has started to include an investigation of individuals and groups in relation to the motivation and intent of perpetrators of malevolent actions. Coupled with this will be a study of target attractiveness and operational planning factors relating to the individuals and groups studied. A report covering the combined physical and motivational attributes of potential adversaries to security programs will be provided as the terminus of the currently funded program. Future work is expected to include the updating and expansion of the data base for all attribute types contributing to potential threat characterization.

SOME IDEAS ON STRUCTURING THE PROBLEM OF COLLUSION[1]

James NiCastro and Hugh Kendrick

Science Applications, Inc., La Jolla, CA 92138

The objective of this study is to provide a cursory investigation of the vulnerability of a facility to collusion from members of the security force.

INITIAL REMARKS

Collaboration with another individual may be brought about by a variety of means as indicated in figure 1. The considerations given in this paper pertain to voluntary collusion.[2]

Voluntary collusion is a tactic of two or more people acting in concert to accomplish an objective. The relevant implication is the need to establish knowledge and familiarity between individuals involved. In the process of constructing safeguard systems immune to collusion this "requirement," while observationally trivial, is paramount. A bond of "trust" must be established before collusion can be used as a viable tactic or the adversary risks exposure. Figure 2 indicates graphically the intuitive relationship between familiarity, knowledge and risk of exposure.

The extent of the knowledge of another individual judged to be sufficient by an adversary depends on his concern with risk of exposure.

A BASIC CATEGORIZATION OF SAFEGUARDS MEASURES

The safeguard system should protect against:

(1) Premeditated, planned collusion prior to hiring, and

(2) Possibility of collusion occurring after employment, in particular with others in sensitive locations.

Two general kinds of activities are conducted to accomplish this:

(1) Prevent unnecessary or potentially deleterious common bonds that form a basis for collusion, and

(2) Detect collusion and defeat its utilization as an effective tactic.

Representative examples of safeguard measures are drawn to illustrate this in figure 3. Due to different attributes of a safeguard measure, it may contribute to more than one category. Thus rotation may be useful in B1 and B2.

WORK RULES IN THE MODE (B1)

A variety of work rule options are possible; some of these are indicated in figure 4. Each X indicates a possible work rule. The usefulness of rotation and its "variations" are bounded by the number of people in the facility. An alternative may be to confine rotating groups to specific areas; thereby requiring a smaller number of skills. This semi-insularization also limits the knowledge of security practices in other areas. For a given facility some optimum combination of the configurations of "rotation" and "insularization" might exist. The latter discussion is not limited to an individual working alone. Additional options are generated by introducing the two-

[1]Work sponsored by the U.S. Nuclear Regulatory Commission.

[2]As distinguished from "involuntary collusion" which involves some coercion.

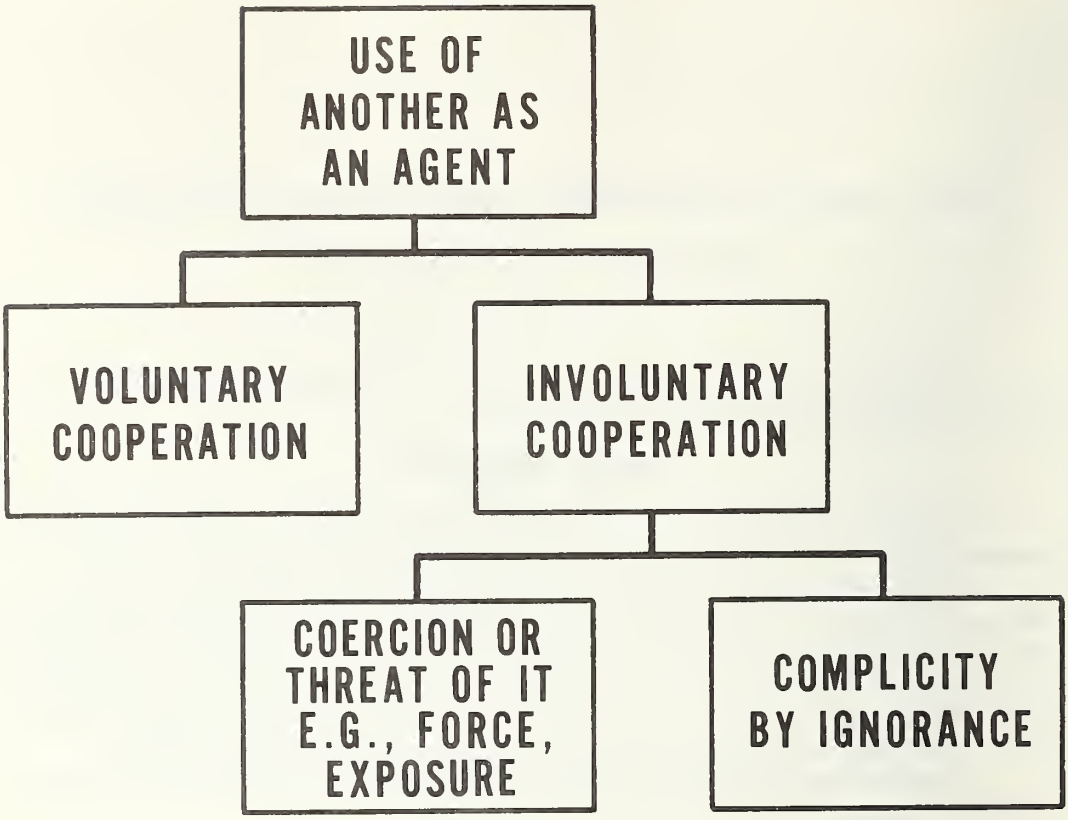


FIGURE 1.

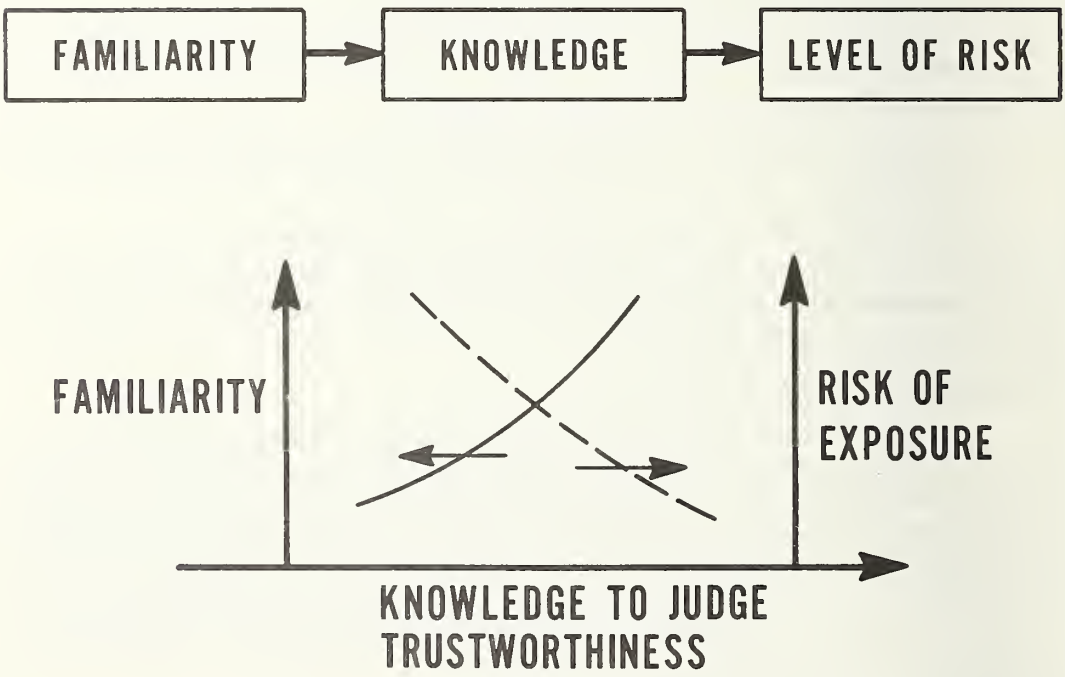


FIGURE 2.

Time \ Function	1 (prevent)	2 (deter)
A/(Before hiring)	No family members hired	Polygraph Q, clearance
B/(While working)	Random rotation, 2-man rule, isolation. Variations of above	Reliability checks Spot inspections SSNM area sweep

FIGURE 3.

Position configuration \ People involved	Single	Two man	Remote two man	Remote overlap
Isolation	X		X	X
Rotation				
random	X	X	X	X
defined	X	X	X	X
Insular with rotation	X	X	X	X
Rotator/stator		X	X	X

FIGURE 4. *Work rule options.*

man rule. A variation of the two-man rule might be a remote second man or a collection of remote second men who are monitoring activities in which there is a random overlap. Still a further alternative is to have a fixed (stator) group and a rotating group. The rotating group might be more highly trained and continually cleared, serving the function of administrative monitors in the two-man rule configuration.

VARIATIONS USING ROTATION

The objectives associated with the possible use of rotations are twofold: to avoid people knowing each other well enough to collude; and to require many colluders or many acts of collusion with a long interim time to successfully execute an adversary sequence.

The benefit, if any, to be derived by rotation of individuals working alone (fig. 5) would be to make it difficult to string together a sequence of acts in an adversary sequence utilizing different work positions. While considerable arbitrariness in work location can be achieved by maximizing rotation, any benefit might be weighed against the possible decrease in working efficiency. Additional variations result if rotation is used between shifts.

With the introduction of a second person (two-man rule), the variations are of course even richer. In this case the safeguard features would generally require an act of collusion before an adversary act could be committed at a particular site. Figure 6 indicates the combinations for a particular shift.

Unless the individuals are distinguished in some way $Y_iX_j = Y_jX_i$ there are five distinct rotation work patterns indicated. A similar array could be constructed for rotations through varying shifts.

Variation within a shift	Fixed shift		Variation between shifts	Varying shifts	
Random	O	X	Random	X	X
Defined	O	X	Defined	X	X
None	X	O	None	X	X
	same location	different locations		same location	different locations

FIGURE 5. *Rotation work patterns for a single individual.*

Individual Y	Individual X None	Defined	Random
None	Y_1X_1	Y_1X_2	Y_1X_3
Defined	Y_2X_1	Y_2X_2	Y_2X_3
Random	Y_3X_1	Y_3X_2	Y_3X_3

FIGURE 6. *Rotation work patterns for the two-man rule, fixed shift.*

NEEDS FOR COMPOSITE TREATMENT OF SAFEGUARD MEASURES

° Example of the appearance of a problem

This discussion is directed at indicating the need for considering more than a single isolated safeguard component in estimating its value. Consider a system consisting of two physical locations. These might correspond to the material access portal in the manufacturing building and the boundary perimeter portal. Postulate an individual removing material by a non-specified physical path passing through these locations. As a subverting tactic, the individual adopts collusion with the monitor guard at each location. Rotation is part of the guard force program. If P is the probability of successfully passing through a given portal without collusion then the trees indicated in figure 7 and table 1 summarize the options.

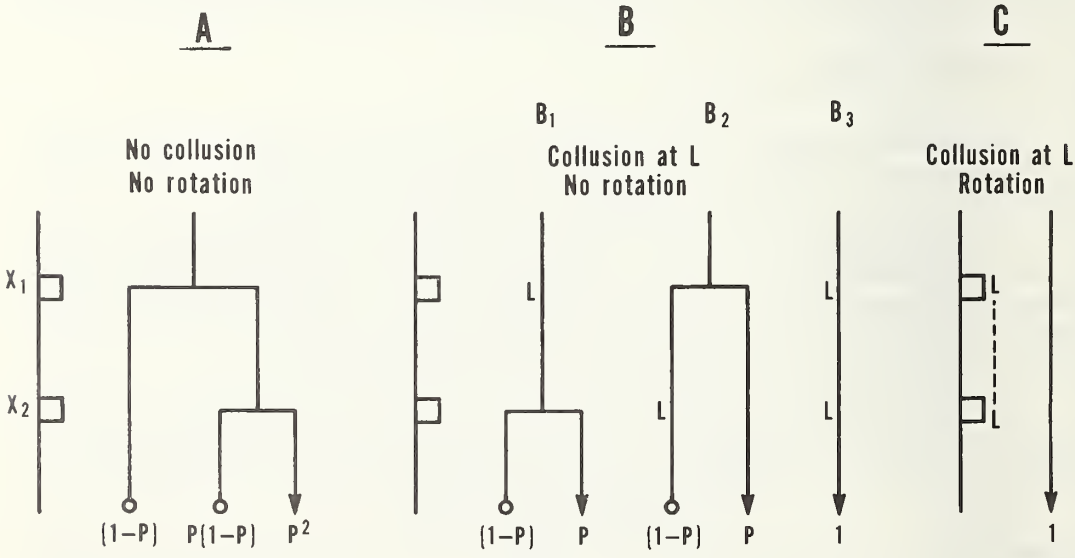


FIGURE 7.

TABLE 1

Graph	Number of colluders	Collusions	Probability of success
A	0	0	P^2
B_1	2	1	P
B_2	2	1	P
B_3	3	2	1
C	2	2	1

° Reconciliation of the problem

The graphs in figure 7 indicate a result that appears to be counter-intuitive and one suspects something is wrong. An important aspect of the problem has been ignored. Random or designated rotations involve some type of time sequence. The individual following option C can not elect to work through the system at any time. Between the time the colluding partner moves from post X_1 to X_2 in graph C the material must be stored. While success might be achieved with configuration C there is a penalty in removal time. Despite this, however, the benefit derived from rotation seems offset by its enhancement to successful utilization of collusion. Considered alone, rotation may not be beneficial.

As a supplement to the work option of rotation, an additional feature consisting of a programmed area search for SSNM at given intervals may be added. Under this situation graph C (fig. 7) becomes either C_1' or C_2' (fig. 8), depending on the time the theft of material occurs, i.e., whether one or two storage times are required.

The probability of success in graph C_1' is not unity but $(1-P_d t_d)$ where P_d is the probability of detection per unit time and t_d is that time for the rotation process to move the colluder from X_1 to X_2. If the theft is not timed optimally, then graph C_2' applies and the indicated probability is appropriate. The additional branching is a direct result of the requirement to store material

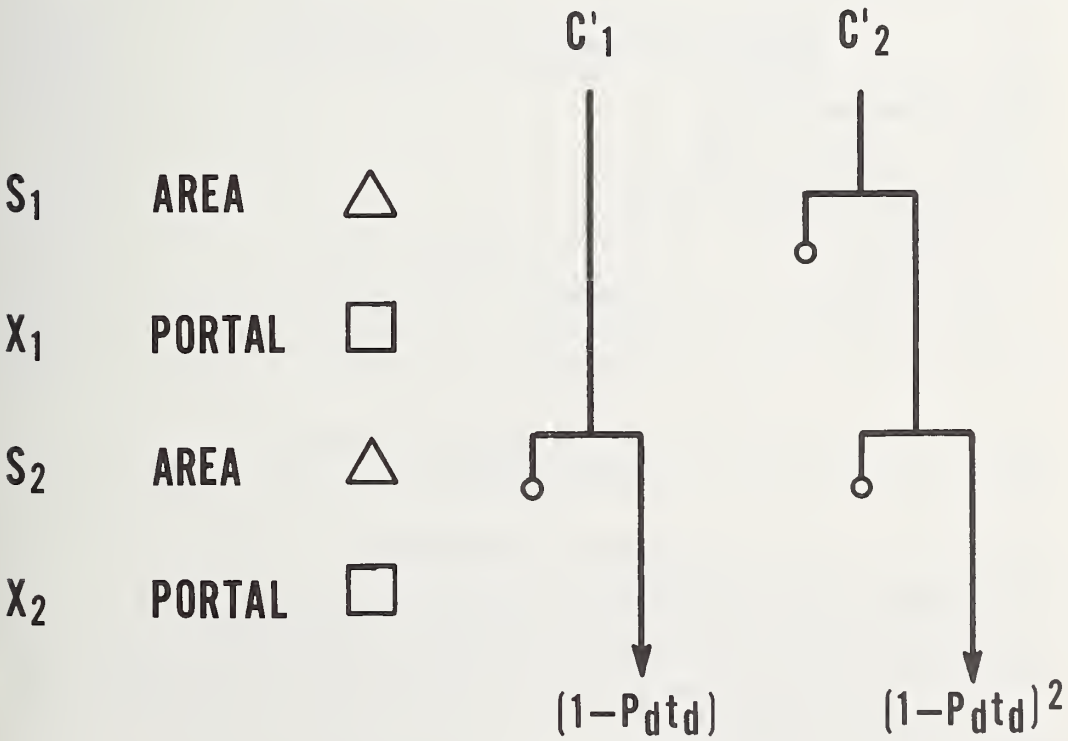


FIGURE 8.

between rotations, and that during this time there is susceptibility to being detected by the sweep procedure. Rotation alone can reduce personnel contact and increase the time required for removal if less than the maximal number of colluders is available. It becomes a valuable procedure in conjunction with programmed area searches.

° Consideration of the role of reducing the probability of the occurrence of colluders

The previous example assumed colluders exist, but, in fact, that probability is reduced by the level of effectiveness of the measures used in all the categories of figure 3.

This is an additional aspect of the problem that has not been taken into account. A probability might be ascribed to each element in figure 3 characterizing the level of effectiveness of the appropriate set of safeguard measures, from which the possibility that a collusion occurs at all might be formulated. Corresponding to Al, A2, Bl, B2, let the probability of success of the safeguard system be P_{A1}, P_{A2}, P_{B1}, P_{B2}. Then the probability that a colluding adversary exists might be represented conceptually by the expression:

$$\rho = [(1\text{-}P_{A1}(\ \cap\ (\ 1\text{-}P_{A2})] \cap \cup\ [(1\text{-}P_{B1})\ \cap\ (1\text{-}P_{B2})].^{3}$$

It would be completely spurious to assign numerical values, but it is clear that this difficulty to the adversary needs to be taken into account.

Taking the above items into account, table 1 is superseded by table 2, where the probability column refers to successful adversary action.

TABLE 2

Graph	Colluders	Collusions	Probability
A	0	0	ρ^2
B_1 & B_2	2	1	$P\rho^2$
B_3	3	2	ρ^3
C_1'	2	2	$(1-P_d t_d)\ p^2$
C_2'	2	2	$(1-P_d t_d)^2\ p^2$

GENERAL THOUGHTS ON SAFEGUARDS

SAFEGUARDS OBJECTIVES

First: To prevent a problem

Second: To deter, given a problem

° Rotation

° Q clearance

° Etc.

° Develop worker esprit de corps

° Reduce the feeling of management suppression

° Do not treat workers as if they were untrustworthy

° Develop supplementary programs to handle problems

CLOSING COMMENTS

° Orwellian tactics have been the focus of attention in safeguards studies.

° The most important link in any system is the individual and how he feels about it.

° Our understanding of safeguards measures should be broadened to include humanitarian as well as Orwellian tactics.

[3] $\cup$ = logical "or"; $\cap$ = logical "and." The formula is symbolic and not to be interpreted in a numerically literal sense.

RESPONSE FORCE SELECTION AND TRAINING

Stephen L. Galloway

Operational Systems Incorporated, Arlington, VA 22209

This paper addresses an extremely complex, serious problem throughout the entire government/private security sector: response force selection, training and motivation. Security managers concerned with behavorial problems do not have definitive solutions for these problems. The areas which affect the private security sector, specifically the nuclear industry portion, are covered briefly. Nuclear security response forces are those forces considered to be already on the nuclear facility, and are part of the integral facility security organization.

The past few years have seen a tremendously increased awareness of the necessity for upgrading security levels at nuclear-related facilities. Behind this effort there have been essentially three interrelating factors, i.e., environmentalists, legislative mandates, and the increased threat from various groups or individuals bent on gaining illegal access to a nuclear facility. Responding to these factors, the Nuclear Regulatory Commission has undertaken an extremely energetic effort over the past year directed at physical security, electronic systems, and human factors aimed at improving security conditions for private industry.

Previously published papers, symposia and studies have addressed the problem of constantly maintaining personnel interest in normally routine security functions which have extremely serious ramifications for failure. Numerous procedures, ideas and concepts have been tried: training, both formal and informal; testing; periodic field exercises; rotation of personnel throughout the security complex and the often used standby of job loss for failure to perform. Needless to say that none of these either in part or whole have provided the answer. The basic problem remains one of creating a response force able to respond to that one "real" incident occurring at the least likely time, place and, most certainly, without much or any prior warning.

The Federal Government has developed, to an extensive degree, a wide variety of selection processes, methodologies, and means of determining the preferable match of a security individual to a given position. The success of this is evidenced at missile sites, submarines, aircraft weapons parking areas, and other sensitive control areas. It is realized that a response effort is in large part reflective of group dynamics, but it is still comprised of people who have three factors influencing their reactions. The first is personal qualities, encompassing such items as initiative, courage, and motivation. The second is action prescribed by existing regulations and policies. The last is the degree of training. The security system which these factors place into active response are based upon: numbers, capability, and reaction time.

Again, the nuclear power sector is now being made abundantly aware of the requirement for increased security. The expressed requirement is that the civilian security component is now going to be required to have essentially the same type security level and training as expected of the government, with none of its assets or research base.

The civilian security industry is faced with several constraining influences. Traditionally, security departments have drawn little of the budget and most certainly little of whatever corporate prestige exists. Security budgets are inherently constrained and this, as we know, affects the quality of the individuals hired. Training is reserved for last because, for the most part, training is all too often last in most security budgets. The majority of security departments hire personnel with prior Government or police backgrounds to overcome these limitations. At first glance, this appears to be a satisfactory solution to all three of our response force areas of concern; however, except for isolated instances, the training given at the point of hire is virtually all the individual

ever receives, in some cases, for his entire career, and is often not even relevant. Private security personnel firms hire by the skill and, like cars, lease them on the same basis to the user.

The nuclear sector is now discovering that being "penny-wise" is "pound-foolish." This will be a difficult problem when dealing with an escalated threat requiring specialized skills and continuous, very expensive training. All of these obstacles are surmountable but have an impact upon the eventual selection of security personnel. When looking at the basic question of recruitment it can be seen that, legally, the use of the polygraph, certain psychological tests and security agency checks serve to constrain proper initial screening. When applied to the limited manpower base available to nuclear plants, this constraint decreases the number of suitable candidates. Legislative actions concerning private security forces are even further restrictive; however, at present, no single licensing criterion exists, although a model statute has been proposed.

Basically, the solution and the problem for response force personnel are identical—qualified people. These people must have a purpose. Almost any purpose will do, but they must accomplish an identifiable task and be rewarded for it. There are just so many SWAT actions, hostages, snipers, and bombers running around. Unfortunately, from the viewpoint of criteria or standards for keeping response forces up to readiness, these actions are few and far between and are unlikely to occur at the same site with any reliable frequency to justify continued training.

When an elite or any type of "special" element is created, as is the case with the response force concept, there is the difficulty of what to do after an optimum training peak is achieved. If there is no realistic mission for the force's talents, the unit quickly deteriorates. Although the loss is more psychological than physical, the competitive edge is nonetheless lost. After a while constant "motivation" training is just so much training.

Selection involves a multitude of problems. Pre-employment screening by law must be job-related. However, for security work this may not be a valid generalization; therefore, if the individual is to perform a specialized assignment, the screening procedures may reflect a need for a security position. Psychological testing of a job applicant, particularly for response forces, tends to be realistically valid only upon initial screening. After that point, on-the-job performance, peer evaluation and other factors will of necessity be more useful. National agency checks (NAC's) are becoming more restrictive with respect to what a police department or indeed any agency will release. Therefore, what used to be an effective management device when properly utilized is no longer valid. Previous job performance used to be checked; again, with recent court rulings, this is not the case today. If the individual desires to have certain references excluded he can. In many instances, a desire not to have a check made is cause for genuine suspicion. But there are circumstances in which the individual has a legitimate reason for not consenting to any reference check. The use of Civil Service-initiated clearances are a help, but extremely long backlogs even for routine checks are normal.

The oral interview is becoming very prevalent because the employer gets some opportunity to see the applicant before the final decision is made. Techniques for upgrading its use should be improved. An employment probationary period is often used for blue collar employees, a category encompassing security forces. With the expense of security clearances and relocation, this alternative is unavoidable.

Many security guards and response forces in particular have chosen to seek this type of work because of the masculine image projected by the addition of a weapon, i.e., the "cop image." In the Government, this can be cured by reassignment but in the private sector this means loss of work. If an individual is selected with the ultimate purpose of being able to use a weapon, then we had best be prepared for him to use it. Deadly force is a requirement at nuclear facilities and the constraints are totally undefined.

In the Government, an individual is relatively easily removed or reassigned if there is a mismatch or his services are no longer required, and this can often be accomplished with little difficulty. Also, the manpower base is large, diverse and able to respond to specific needs for specific talents. In the private security sector, in particular nuclear power facilities, this is often not the case. For many reasons such facilities are not located near a large metropolitan area and

management naturally seeks to keep operating costs down. At the top management level salaries, fringe benefits and other factors are very comparable to any other segment of the management sector. However, at the operational level the lowest pay rate prevails.

In many cases, the supervisor/manager is the only one with any prior background in any security field. The problems of an 800 million dollar facility are enormous and complex, but it is not surprising to find some individuals who occupy positions for which they have no real background. To those people in the security field who do not fit this description I apologize, but they are as well aware of the glaring gaps as anyone. As previously stated, prior security experience of any sort will get a person hired. The reason in most cases is the additional expense which training represents. Training is a formal procedure. In the private sector, the Government provides some of the training. The majority of private security response forces are patterned directly after the military. The police also draw from the military. Now this is not to cast stones at the military; but rather to state that the protection of a nuclear weapons depot or offensive actions against enemy divisions are not in many ways the same as guarding a warehouse of spent fuel rods. What represents a legitimate act by a FEDERALIZED FORCE is not always legitimate with a CIVILIAN one, but unavoidably this is often lost sight of.

Training is an issue of great importance because it can and does substitute for preparation against actual events. Response forces require a combination of formalized on-site and off-site schooling, exposure to realistic threats, on-going specialized courses, and certification to minimum Federal standards. However, the basic drawback is the low budget status and the lack of reputable civilian security training. At present, many of the worthwhile and necessary levels of instruction are Federal or State sponsored and not available to private sector elements. That which is available is at exorbitant fees, aimed at management. Trying to train even on a small scale requires training aids and as is known, a book without the experience in a functional occupation is sometimes worse than worthless. Such problems are not unsolvable, but rather indicate that, if a uniform standard is to be applied across the board to achieve basic Federal minimums, more than a piecemeal effort must be planned and conducted.

How do we motivate a person or group to perform a given task? A response force requires special care in that its mission will be to ultimately go into what is a crisis event. The fact that a response force will inherently be comprised of more thoroughly screened personnel than would normally be encountered in routine activities automatically makes its members more aware that they are different. Screening and training serve to eliminate misfits and the untrainable, and enforce a standard performance measure. However, nothing can produce that inherent element of determining the individual who can function under stress.

Much is said about leadership as a motivating factor. Leadership in a security force role is normally displayed in its traditional forms. The first, appointed by rank, function, or seniority, is to a large degree uncontrollable. The second, natural leadership which comes to the front in a crisis or unusual situation and often remains hidden until such an event occurs. Both have advantages and weaknesses. Testing can provide a listing of leadership traits but these very frequently disappear when it comes down to the performance of an individual when the risk is real, other than in a training scenario.

An area of major motivating concern for civilian security forces is that the private security individual has relatively little to look forward to if he does not totally immerse himself in identifying with the facility he works at. Traditionally, it is very rare for lower and middle echelon personnel to leave once hired. Seniority is often a union contract condition and, no matter how good you are, that alone will serve to stifle continued motivation in terms of performance. The majority of sites are located in remote areas and hence the lure of the big city with its attendant attractions are missing. In other words, there is a captive audience with outsiders reluctant to come in. By virtue of plant size, there is little rotation of duties. Again seniority and rank determine who does what. Advanced, specialized training is quite low and unless the company is forced into it, or a rare individual comes along who recognizes the need to prepare subordinates for higher responsibility, it is not likely to occur. Management is the exception; the manager gets the first pick of what is available. If such training is not passed on it is worthless. Security work is

regarded as a blue-collar trade. To the plant employee with a Ph. D. he is muscle, or somebody to call upon to start a car on a cold day. Now, however, the times have changed. Modern plants and their requisite security systems are expensive, demanding, and require continuous input from all employees if they are to function in any manner.

RECOMMENDATIONS

Having indicated the negative aspects of motivation, training, and selection, how can the situation be improved? First, it must be acknowledged that the security of a nuclear facility is a total responsibility. Response forces, by virtue of the size of a facility, cannot constitute a separate group. They must be part of the existing organization. The knowledge gained from small-unit, military operations is extremely valuable. For, like their civilian counterpart, they are by mission, objective and selection necessarily lean in numbers, highly trained in purpose, selected for skills and motivated towards their mission.

The team concept must be totally instilled, with each member fully aware of each other's strengths, weaknesses, capabilities, and responsibilities. There must be total involvement in every aspect of facility security. Cross training cannot be a separate function but a complete component of the overall organization. Again, this is possible because the facility force will have a low attrition rate after the first year and if included into pay-promotion packages it will be doubly meaningful. The use of frequent, in-service training and periodic, off-site specialty courses will continually raise the level of expertise. Off-site training affords the individual, in the case of a response force, the opportunity to learn free of the work environment. Such training molds, shapes, and returns to the site a group very confident and ready to implement what they have learned. Field training and command post exercises require input from the Federal level. Law enforcement coordination exercises can vary greatly in scope and dimension. The introduction of security-related lesson plans, books, lectures, and continuing education will produce a measureable result. The facility gets a force trained, equipped, and motivated, which can respond to a variety of threats. The force is pressure-tested, job-oriented, recognized as trained professionals, and educated in their selected profession. Units which act and react as an elite force are not simply established. Behavioral scientists, who have to understand group behavior, must recognize that every issue discussed here is obtainable. If we fail to make available to the private sector the results of our efforts, and do not insist upon appropriate standards, the objectives of physical security will not be realized.

DISCUSSION SESSION

"Adversary Attributes/Characteristics—Problems and Future Research"

Moderator: Herbert Susskind
Brookhaven National Laboratory

Discussants: D. Darling
R. W. Mengel
J. Pratt
A. Fine

MR. RAY MOORE: I'm doing some work for DNA on a computerized site security monitoring and response system. One of the concepts that we've had is that there are attributes of guard force activities or performance that may be, in some subtle way, indicators or triggers of impending collusion. What sort of activities and attributes could be monitored or sensed using equipment? How could these activities be interpreted? Is there any work that's going on, or planned, that could provide information which would be useful in expanding on this concept?

MR. DONALD DARLING: With nuclear power reactors and particularly at the storage sites for nuclear fuels, it calls for using an awful lot of detection equipment that will monitor everything going out—from the garbage to personnel—to make certain that no significant quantities of nuclear materials are leaving the premises. Of course, we do have the problem which is inherent at such sites of somebody pushing the panic button, indicating a radiation spill. All the gates open and everybody leaves. We are working on this problem now.

In the nuclear weapons area, I would suggest that primary consideration be given to target attractiveness, which means from the guerrilla standpoint that the most likely and logical devices are those that are man-portable. There's been quite a bit of work done recently with respect to isolating them in a useful configuration where they can be readily delivered when needed, and using well-trained, highly motivated military personnel to safeguard them. Does that partially answer the question?

MR. MOORE: I don't think that I made my desired objective clear. I am well aware of the various types of sensors that can be used to detect the movement of materials and things of that sort. What I had in mind is the guard who has decided to sell out to the adversary. He is going to unlock a padlock, or let someone in a gate, or do some other thing in collusion with this adversary that will enhance the likelihood of the adversary's success. I'm raising the question: are there attributes of guard performance or guard activity that may be amenable to automatic observation and interpretation to provide an insight or indicator that collusion is either impending or actually taking place? And if so, what are such attributes of activity and performance?

MR. DARLING: This morning I mentioned that consideration be given to using periodic polygraph examination or the new voice stress analyzer. I am not qualified to comment on the validity and reliability of such equipment, except as having been on the receiving end. They kept me pretty honest. If the examination is prepared properly and given periodically, there would be no infringement on the rights that employees have; quite possibly, it might be a significant deterrent.

After security checks have been made, a tremendous amount of security is based solely on reliance upon the two-man rule and having your buddy turn you in. From practical experience we know

that, unless there is a particular grudge to bear, most likely a turn-in system will not work as it should.

We have done detailed profile studies and analysis on everything known to man to come up with some way of pinpointing precisely when a good individual goes sour. For this reason alone, we have seen the tremendous interface between man and equipment. But as yet there is no profile or attribute study that works. Your problem is like the needle in the haystack. The problem is going to be ongoing forever.

Question: I wonder if periodic psychological testing would have any impact here?

MR. R. W. MENGEL: There appears to be one basic problem with any kind of test. That is, the standardization of application in the field, where there are a number of facilities involved and the test is somewhat subjective in nature. Subjective interpretation can produce a wide variety of results which in fact will tend to degrade the usefulness of the test.

Question: The discussions of terrorism and some of the other covert activities at a nuclear site of any type would seem to indicate that the perpetrators that we are looking for are the more sophisticated brand, of what's perhaps been known as a surrogate terrorist group, or perhaps, as Dr. Pratt suggested, an actual part of an intelligence organization.

But one thing Dr. Pratt mentioned was that the climate was not yet right, or presently hasn't been right. Would you give us some scenarios or perhaps some suggestions of what a right climate would be? Is this really why there haven't been attacks?

DR. JANE PRATT: I think so; I'd agree with Mr. Darling that the capabilities exist today. I have interviewed individuals in other countries who have the capabilities. Such individuals exist and are motivated.

All it would take was a decision to go against a nuclear facility. I believe that the only reason why this hasn't happened is that other targets of opportunity are more easily available, perhaps more directly relevant to issues that these groups are presently concerned with. The political climate is not currently appropriate for this.

I'd like to just mention something in passing that occurred to me on the last question and that is that one of the things that we've looked at with in-plant security systems, and one of the problems that we've had, is that while you could administer tests to a response force inside a plant, one of the places where you're most likely to detect a change of heart on the part of one of your security force guards is outside the plant.

One of the things that has restricted us in getting at these individuals outside the plant is our insistence on protection of civil liberties. You can't, under present circumstances, very easily routinely monitor individual bank accounts and personal associations.

This is one of the contributing factors to making detection so hard. What I'd like to see done is the kind of thing that Allen Fine of Sandia and Bryan Jenkins of Rand are doing. Identifying physical and behavioral attributes is absolutely crucial and the data bases they're using to extract such relevant information are worthwhile.

But we also need to do a second kind of thing. I didn't mean to be too critical of using analogs. The problem is that that kind of analog won't give you the behavioral attributes. In order to do this, you've got to do the kind of thing that Pickerel did with the airline hijackers, which was to go out and look at hijackers, and find out who are the people in guard or response forces who have failed to perform, and profile their attributes.

Comment: I'd like to maybe extend this a little further. It's too easy to obtain conventional materials, without the danger of getting caught or shot at. One of the worst scenarios that we developed was the extraction of several hundred gallons of highly radioactive liquid waste, putting them on a semi-tractor trailer truck, properly booby-trapping it, driving it into downtown Washington, dumping the trailer and letting the signs fall: Here it is, what are you going to do about it?

Waste you can get. It's wrong that our nuclear weapons storage sites are surrounded by conventional weapons storage sites which give the attacking forces the equipment to use against us.

Get the man-portable nuclear weapons out of where they are and start picking someplace where they can be properly guarded and delivered back in a reasonable period of time. If one wants to destroy the operations of a nuclear weapons system, concentrate on the computerized logistics systems. That will do more damage than stealing a nuclear weapon.

But, as a guerrilla, pick the targets that are soft, where the easy materials can be obtained, like a little van loaded with ammonium nitrate fertilizer. Park it in front of a computer building such as has been done back East. Result: fifteen-foot hole, computer gone and researcher killed. Why fool around attacking fairly well-guarded nuclear sites when you are going to have some losses? Why don't you do it the easy way?

If you're dealing with a single individual, you start with the assumption that this person has some reason(s) for the behavior. The person may be a psychopathic individual, in which case, if you're talking about the individual weirdo or nut, certainly the psychologist and psychiatrist can tell you a lot about screening for such individuals. The military does do psychological screening of individuals who are serving in the capacity of guarding a nuclear facility. I think you can find out a lot about individuals who are engaged in this kind of activity and get a very good handle on what some of the attributes of these individuals are.

MR. ALLAN FINE: The Rand people who are on contract to Sandia have become very interested in the lone psychopathic individual. They call him a flaming banana.

Part of the motivational analysis they're going to undertake for us will hopefully contain some of this information. However, the ultimate utility of such information is open to question. In our kind of society, you may never be able to detect who these individuals are beforehand. One may not be able to do very much about the lone individual who doesn't let anybody else know his plans, except perhaps identify some of the peripheral things that might set him off.

Comment: I'm wondering about the relative value or applicability of this data base, which is based on a lot of information generated overseas, to the American environment.

MR. FINE: It's one of the things that we have to put up with, because we don't have an American data base, fortunately.

DR. PRATT: One of the other points is that transnational terrorism is a widespread phenomenon, and it certainly is relevant to study foreign groups, because activities that are carried out on American soil don't have to be carried out by Americans.

Question: Dr. Pratt, in reference to your cross-national survey, you said that you had been to Vietnam and other places. In your interviews with these terrorists did you come across, detect, or are there any indicators to lead one to believe that some of these terrorists were really not so-called terrorists, but rather individuals who were working under the auspices of terrorism to cover up affiliation with some other country?

DR. PRATT: Yes, but they don't make that distinction. The individuals involved may have been trained in unconventional warfare anywhere in the world, or trained in many different places. Some of them were trained in Latin America and were operating in Asia, but they personally tended to feel unemotional about their activities that you describe as being terrorist in nature. They were not operating necessarily out of personal rage, but simply because it was their job and they were working toward the defined goal of disrupting a system and carrying on the revolution.

Question: Within the scenario of sabotage of an installation, has there been any work done regarding the possible use of a surrogate, or unwitting adversaries?

DISCUSSANT: There has been some work done on using surrogates to actually sabotage a facility unwittingly.

Question: Most suicides, whether they succeed or fail, are prone to telegraph their intention to someone, possibly someone close to them, or possibly to something like a Hotline service,

sometime before they actually attempt suicide. Has there been any work or research to indicate that people like psychopaths might telephone, communicate, or in some other way indicate that they intend to take some action? Could this be used as an indicator of what might happen, without getting into violation of civil liberties?

DR. PRATT: Your initial premise is that most of these people do communicate in advance, but you're still left with the "most." For some of these people, there's no way you're going to be able to tell in advance. We have no way of getting at them.

Comment: We've had one of the 12 publicized examples of this sort of thing happening, and if the person with whom that individual had been communicating had been aware of the possibility and had the ability to respond, the attempt on the President's life would not have occurred. The lady apparently wanted to be stopped; she communicated her fears to somebody in the police and FBI prior to her actual attempt on the President's life.

DISCUSSANT: Regarding Presidential assassinations, this apparently has been the only case where a threat was made and the individual actually tried to assassinate the President. In every other case, the individual who made the attempt did not make a threat initially.

Comment: When you deal with foreign threats and information, that's one thing. The difficulty in this country is legitimately acquiring and utilizing surveillance data gathered on U.S. individuals for identifying someone who is predisposed to shooting up a building, or attempting to blow up a nuclear installation.

Everything that's been stated here so far is identification after the fact. This is no problem—hindsight's always 20-20. But our problem is, how do we identify the people we know exist before they attempt to commit an act?

Under the current legislative atmosphere within the United States, we're trusting a great deal to luck. If an individual goes to a psychiatrist and says, "Listen, I'm going to blow up the White House tomorrow morning at 9:00," that psychiatrist has a tremendous problem with confidentiality of patient information.

Now, if this individual in the past made these claims every day, and he now turns it over to the Secret Service, or whatever, and that information is found to be blatantly false, you can see the problem. If, on the other hand, there is an attempt at a true act, then we are dealing with something else.

The whole underlying premise is in the current atmosphere of constitutional guarantees. The civil liberties people will jump all over you, and maybe that's the best end to this discussion.

Comment: I think the whole question is two-sided. The other side is, if you knew that the guy was going to do something, there is not a hell of a lot you can do about it.

Question: Dr. Pratt, you've implied that the primary threat was from organizations that are basically sponsored, supported and organized by foreign governments. If that's really the case, is it right to handle the problem by taking some direct action against that government?

DR. PRATT: I think the most credible threat comes from organizations that follow this model. Not all threats are organized and instigated by foreign governments, but many threats tend to be organized along these principles and have this kind of network and capability. I was trying to rule out the Hanafi Muslims, for example, as a credible threat to a nuclear facility. I think the other type of organization is a more serious threat.

Question: We've heard a good deal about data banks, both today and at last year's symposium, concerning the successes of adversary forces of various kinds and professional burglars. Is anybody doing analyses or creating a data bank on the successful actions taken by response forces? Such a data bank would be an important source of feedback information for the design of future systems and models.

DISCUSSANT: I think the Israelis probably have done this. They've had some worthwhile successes and some good things to record. I don't know where we stand on this.

USES OF ANIMAL SENSORY SYSTEMS AND RESPONSE CAPABILITIES IN SECURITY SYSTEMS

Robert E. Bailey and Marian Breland Bailey

Animal Behavior Enterprises, Inc., Hot Springs, AR 71901

For the past thirty years, our company has been concerned with applying the theories and knowledge of behavioral science to the practical control of animal behavior. Our company had its origins in a military project—some of us were engaged with B. F. Skinner in the "Pigeon in a Pelican" project designed to train pigeons to guide missiles to a target. It was during this phase that we realized that the theory of behavioral psychology was much better than most people realized, and that it could be put to practical use. Animal Behavior Enterprises began in 1947 in mixed fields of advertising and entertainment. Trained chickens, rabbits, and pigs were used to advertise farm feeds at fairs. These animals were sent out on the road with feed salesmen, usually completely unfamiliar with animal handling and training techniques. It was found that manuals could be written instructing these salesmen how to care for the animals and maintain their conditioned behavior. To our knowledge, this was the first comprehensive instruction manual for operant conditioning of animals. In 1955, the first scientifically oriented training program for dolphins and their trainers was designed at Marine Studies, now Marineland of Florida. The dolphin program was extended to Marineland of California in 1956, and, during the late 50's and early 60's, our programs were extended to many other avian and mammalian species.

In 1962, we were asked to become consultants to the Navy marine mammal program. This was our first, direct involvement in governmental research on a large scale; we directed the development of their training program for personnel. Over the years since then, our involvement with Government programs has expanded. Private research and commercial use of trained animals have also expanded. A word or so is needed with respect to the theories and information that have made all this possible.

Basically, the theories of operant psychology have been applied. These theories and the detailed expertise that has grown up around operant or so called "Skinnerian" theory have made it possible to condition species which were previously poor bets for traditional "animal training," to mass produce conditioned animal behavior and to condition the more traditional trainable animals in feats which were previously considered impossible. Most important of all, people were trained to train animals. To this basic framework, important information and methodology have been added from related disciplines—biology, and particularly from the ethologists, European zoologists specializing in animal behavior. Not only were specific useful bits of information acquired, such as the importance of the imprinting process and critical periods, but also the whole attitude of viewing each species as something distinct and unique in itself, and of the necessity of learning by close observation about each species' habits, capabilities and limitations—its way of doing business in the environment, in its own ecological niche. The control of animal behavior which has been possible within this practical and theoretical combination has created a virtual revolution in the animal training industry. What does this mean for security systems?

Our research and applications are divided into three basic systems: aerial, terrestrial, and aquatic. There are also possibilities of expansion into subterranean and space environments, although our firm has not been engaged in research in these environments. However, before getting into the specifics of each type of system, the general characteristics of an animal system should be understood.

Numerous animal species, including those commonly found over large areas of the globe and others of more restricted distribution, have sensory and response capabilities which would make them useful in security systems. Animal capabilities can be utilized successfully in systems where they can: (1) supplement human capabilities (including electronic or mechanical extensions thereof), (2) provide superior secrecy, and (3) provide sole sources of sensory information or response to information. It might be considered that the animal is a tool, an extension of our own sensory systems or our arms and legs, which, with the control behavioral science has made possible, can be used to extend our human capabilities. Thus, in addition to the land, sea, or air classifications, animal systems can also be categorized as to whether they are primarily sensory systems, primarily response systems, or a combination of both.

In the course of the discussion, a number of concepts and terms will be mentioned which should be defined for those not familiar with certain behavioral and biological terms. Reference will be repeatedly made to behavior or response. Behavior means anything the animal does—walking, swimming, climbing, vocalizing, manipulating objects, and so on. These behaviors may be those which occur normally in nature without human interference, or those which humans have somehow shaped or altered. Response means a small segment of this behavior which has been isolated for discussion, study, or control; it is usually a response or reaction to something in the environment or in the animal itself. This something is a change in the physical environment or a stimulus, often called a signal.

The technical jargon for training is behavioral conditioning, or just conditioning. One important part of conditioning is the formation of discriminations, where the animal is trained to make a response to a certain stimulus and not to respond to another, or to make one response to one stimulus and another response to a second.

Imprinting, another concept, is the process by which a very young animal, during a certain usually very short time period in its life, forms a close and often virtually irreversible attachment to another object—in nature its parent. A baby duck just hatched, will normally get up and follow its mother when she first moves away from the nest. However, if in the first few hours after hatching, the baby duck sees instead a human, it will become attached to humans. Thereafter, it will act toward the human as it would to its mother. From our standpoint, the important thing is that such an animal will be very tame around humans, and will seek to be with humans. Unimprinted animals of certain species are often worthless as experimental or mission-oriented animals—ravens, seagulls, cormorants are examples.

This imprinting must happen during a certain critical period in the young animal's life. By critical period, we mean a stage of life when an animal must go through certain experiences in order to develop normally. Imprinting is one of these. If it does not occur during the animal's critical period for imprinting, the animal will grow up abnormally—unable to form the social and sexual attachments which are necessary for normal life—and is usually very fearful and disturbed. The critical period for imprinting differs with different species.

In our later discussions the term "animal/hardware interface" will be used. In simplest terms, it means the relationship or interaction between the hardware or equipment and the animal. Millions of years of evolution have gone into the design of the animal—there is not much that can be done to redesign it to suit particular purposes. For speed and efficiency in pairing the animal and the hardware, it is best to start at the very beginning to design the hardware around the animal. If the animal is to be placed in a box, obviously the box must be the right size and shape. If an animal is required to pull a ring to release an object, the size of the ring must fit the animal's beak or mouth or hand (and whether it is a beak or a mouth may alter the design). The strength of tug required must be within the animal's capability.

AERIAL SYSTEMS

For about 15 years, our company has experimented with free-flying birds, mostly pigeons, crows, ravens and seagulls, and have conducted short-term programs with many other species—

starlings, large vultures, hawks and even albatrosses. Our subjects have included diving birds such as ducks and cormorants.

The experiments have included developing guidance techniques, establishing design criteria for hardware, including payloads and bird-hardware interfaces. Basic research has been performed on the sensory capabilities of some species. Some effort was spent designing transport and housing equipment as well as other support hardware. More basically, the natural history of several species was studied, including much field observation as well as library research. For some birds like ravens and albatrosses, special diets had to be developed.

The guidance of free-flying birds was of great interest and much of the effort was spent designing, developing and testing guidance systems. Some experiments were conducted with on-board guidance systems, but the obvious weight limitations and the difficulty of concealment made most on-board systems impractical. There were also behavioral and perceptual problems in attempting to guide a bird (in this case a pigeon) with on-board port and starboard lighting systems. While on-board guidance systems for avian species hold promise, there is still a need for considerable improvement in hardware and behavioral technology.

By far the simplest and most reliable way of directing birds to a specific location was to place the guidance information at or near the target. The bird simply homed-in to the signal, usually a small spot of light.

Under some conditions for some birds, a guidance system is quite superfluous. The raven, in particular, could be taught to recognize a particular object or structure and could generalize to a remarkable degree. If a raven were taught, for example, to fly to a desk top in a training room to perform a certain task, it would quickly learn, when confronted with a strange room, to seek out any flat table or elevated spot to "do its thing." Most species of birds were not so flexible and even the slightest change of the environment could cause confusion or panic.

The objectives of several of the research programs were to determine the physical and behavioral capabilities of birds—how much weight could the bird carry and what was the best means of attaching payloads; what were the manipulative capabilities of each species; how much individual variation was there within a species? It was in these areas that the studies of the natural history of each species really paid off. Our observations, and the reports of others, indicated that a bird like a pigeon has a smaller repertoire of behavior, is far less manipulative, and is less flexible in its food-getting behavior than is either the crow or the raven. The laboratory and field experiments quickly showed the crow and raven to be excellent at generalization, problem-solving and manipulating objects. The relatively few things the pigeon could do, it did very well, but the ravens were clearly among the geniuses of the bird world.

Pigeons can transport packages weighing up to 75 grams (2.6 ounces) (for the larger pigeons) on various types of harnesses, and can, with certain mechanical aids, pick up and deliver packages. They can be guided by visual stimuli for distances of 60 meters (200 feet) or more. However, their behavior tends to be rather rigid, specific and stereotyped. They do not generalize well and complicated chains of behavior are usually not practical.

Ravens, on the other hand, can manipulate objects in a number of ways. They can perform a number of tasks in sequence and can generalize to classes of objects. Their vision is even better than that of the pigeon and they respond very well to visual guidance signals. They are also more adaptable to new environments and can operate under more variable conditions.

Our birds were taught to carry objects of varying shapes, sizes and weights in their beaks. The birds learned to cope with some rather bulky packages with weights of well over 100 grams (3.5 ounces), even though 60 grams (2.1 ounces) is considered to be a practical limit for most experiments.

Once the bird arrived at the target area, the bird was to manipulate the payload in one or more specific ways. The bird had to push, pull, twist, or otherwise cause something to happen. In some instances, the bird had to perform multiple actions in a particular sequence.

Ravens were taught to scan a designated area of open ground for a particular class of objects. No particular guidance was involved under these circumstances. It was found that the

raven was quite efficient in establishing a search pattern and was usually able to find and retrieve the object in question.

Pigeons have been used for centuries for communications. Homing pigeons even saw action in World War II. While the pigeon has been extensively used by man for a long period of time, the mechanisms by which the pigeon finds its way back to the home loft are still not fully understood. It seems probable that at least part of the pigeon's remarkable homing facility is a highly developed ability to recognize visual patterns. The pigeon apparently develops a kind of "road-map" in its head during flights around its home loft. Whether the bird also makes use of celestial navigation, polarized light, magnetic fields or other information, is still not known in detail.

It is known that the pigeon has excellent eyesight and can recognize gross features, such as buildings, trees and even specific people. It also appears that pigeons have the visual acuity to detect small features such as seed grains on the ground (its main source of food). All the evidence points to the pigeon's excellent visual perception of the world around it.

In an effort to capitalize on the pigeon's good eyesight and excellent flight characteristics, the Army began the development of a biological ambush detection system. As the Army perceived the mission, a pigeon would fly out ahead of troops on the move and search for concealed forces in their path. As the mission finally developed, motorized convoys would be protected by a team of pigeons. These pigeons would be trained to land on or near any personnel concealed off the road at a distance of up to 50 meters (160 feet) from the road. The birds would ignore anyone standing or walking on the road. Surveillance would be monitored by radio link between the pigeons and the convoy. Each pigeon would carry a small radio transmitter which, when on, transmitted a steady tone which could be received by the convoy. The radio was turned on by a very sensitive air pressure switch. As long as the bird flew, the switch was depressed by the air flow. If for any reason, the bird stopped flying, the switch opened and the signal ceased. The air switch mechanism was very simple and proved extremely reliable. The bird was conditioned to fly out ahead of the convoy about 800 to 1,000 meters, (2600 to 3300 feet), the limit of the transmitter. Each bird could maintain coverage for up to several minutes, depending on convoy speed, terrain and transmitter range. The bird could be recalled using a very loud air horn.

A typical scenario was as follows: A four-truck convoy is traveling along a highway. Refugees and other non-hostiles are walking along the highway. Coming to a stretch of highway where an ambush is likely, the convoy maintains a speed of about 15 to 25 kilometers per hour (10 to 15 miles per hour) and launches the first pigeon. The pigeon outflight speed is about 35 to 40 kilometers per hour (20 to 25 miles per hour). The pigeon normally flies out 4 to 8 kilometers (2.5 to 5 miles) and then returns on its own. As soon as the first pigeon is recovered by the moving convoy, a second pigeon is released. The convoy never stops during launch or recovery except during a suspected detection. If, during an outflight, the signal from the pigeon-borne transmitter ceases, this cessation indicates a detection, a malfunction of the equipment, or that the pigeon has exceeded the limits of the radio link. When this occurs, the convoy stops and a second pigeon is released to confirm or deny a detection. If the second pigeon fails to detect a target, recall is sounded, both pigeons are recovered, and the convoy moves on. If target contact is verified, troops are sent ahead to search for hostiles.

This ambush system had a number of conceptual flaws and equipment handicaps. The pigeons' mission was ill-defined; there was no clear-cut ending on an outflight where there was no target. Since there were normally far more no-target runs than detection runs, the birds sometimes made an error and went too far. The bird really had to "make up its own mind" when enough was enough, unless it found a target or was recalled by our very powerful air horn.

The birds performed very well despite the shortcomings of the system. Troops quickly learned how to handle all elements of the system and, by the end of three weeks, we were no longer involved in its operation. It was very difficult for experienced Army personnel to hide from these birds and still be in effective ambush position. Tests were halted late in the evaluation period, when several of the birds were stricken with a contagious disease.

In 1967, work with seagulls started. It was clear from the natural history studies that imprinting of the gull chicks at an early age would be important. It was determined experimentally that chicks collected from 4 to 16 hours after hatching were most suitable. The chicks were hand-reared, some at our own training facility and some in the homes of friends and employees. These hand-reared birds made excellent training subjects.

Adult seagulls were also collected, but never proved reliable for anything other than very short flights. Even after several months of intensive work, the adult gulls never showed the same tractability displayed by hand-reared gulls.

It took 2 years to develop a satisfactory program for the field collection, hand-rearing and early training of seagulls. Particularly knotty problems were nutrition and development of the bird's flight capabilities. It was found that if a seagull does not have the opportunity to develop certain critical patterns of flight behavior, the bird never flies very well. In most birds, flight behavior and physiology are not so critical, and a bird's flight potential is not harmed noticeably if it is somewhat confined during early adolescence. Indeed, many birds learn the rudiments of flight by almost flying in place. Not so with the seagulls and some other birds. Flight involves, at least partially, a trial and error learning process. Also, physiologically, the wings must develop and be exercised by a certain time, about 90 days, after the hatching date, or the wings will be poorly formed. By about 6 months, the seagulls have achieved most of their full flight capabilities.

In some respects, the seagulls proved very good training subjects. The birds had ravenous appetites, and would work very hard for a small amount of food. The seagulls were not easily distracted from their work. However, the seagulls did have some handicaps. First, the gulls did not seem overly burdened with brains. They could readily master only simple chains of behavior. It was hard for them to change their behavior when the training procedures were changed. The gulls were not very clever at problem-solving and manipulative behavior, and often much time had to be spent teaching the bird simply how to search for an object and then how to handle it once it was found. Going around an obstacle rather than through it was a hard lesson for a gull to learn.

Most of the programs conducted with seagulls involved the bird's searching for some known object, responding to that object, and then returning for recovery. For example, a seagull had been conditioned to search for a person in the water. On sighting the person, the bird landed on or near the person and took a small ring from the person. The gull then returned home.

Very little gadgetry was involved in this particular program. It would have been possible to attach a radar transponder to the bird so that a flight track could be made. Very intense strobe lamps have been used to supply guidance information to the bird on its way back home, but it has been found that this is seldom necessary unless the recovery point is a long way from the initial launch point. The seagull has the persistence to go out and search over a large area for a very small, almost completely submerged object. Once the object has been found and the ring retrieved, the bird then begins a search for home, in most instances a small boat. Since the launch boat was often moved a considerable distance after sending the bird on its way, the bird had to do some scanning to get home.

The birds were required to make long searches under certain conditions of poor visibility. The gulls have made detections of targets more than 2 kilometers (1.2 miles) away in dense fog, when visibility was reduced to about 15 meters (49 feet). The total time of trials of this sort could be 30 to 45 minutes. There is little data on the flight pattern used by the birds during long range missions and those trials when vision was obscured. It was hard to see the bird at ranges of more than 400 meters (1300 feet). Also with other gulls and similar birds in the area the issue was further confused. For many theoretical and practical reasons, the establishment of monitoring stations at the target or elsewhere in the theatre of operation was avoided. As a matter of fact, most of the time, the personnel tending the launch boat did not know where the target was located. In many flights where the distance between the target and launch point was beyond one or two kilometers, the trainers at the launch point did not know if the bird had found the target until the bird approached their boat with the target ring in its beak.

Early in the work with seagulls, a healthy respect was developed for their persistence and single-mindedness in pursuit of their tasks. One should view the notion of an animal's "sense of

duty" with a jaundiced eye, and learn not to get too excited over the numerous "Lassie-Come-Home" stories found in popular literature.

Here is a remarkable example of "stick-to-itiveness" in anecdotal form that should be dear to the heart of any military field commander. A seagull had made a flight to a target some 800 meters (2600 feet) away and was some 400 meters (1300 feet) from the boat returning home. The training crew was tracking the bird with binoculars. Seemingly from nowhere, a bald eagle swooped down at the gull. It was not unusual to see them flying overhead during training sessions, but there had never been any attack prior to that time. The gull veered to one side to avoid the eagle and then corrected course back toward the boat. The eagle recovered and made another pass, this time forcing the gull to fly close to the water to avoid being hit. The eagle made a third pass, this time striking the smaller bird. By this time, the crew had fired up the outboard engine and was heading toward the beleaguered gull. The trainers saw the feathers fly when the eagle struck the seagull and the injured bird fell into the lake. The gull quickly became airborne again. It was here, at a range of some 100 to 150 meters (300 to 500 feet) that the trainers noted that the gull still had the ring in its beak. Shortly after taking off, and while the gull was flying very low and slowly, the eagle struck again, its fourth pass. This time, the obviously weak and struggling bird was driven hard into the water. The gull, still carrying the ring, never stopped moving in the water, and in the space of a few seconds, was taking off again. The trainers were within 50 meters (160 feet) by this time. The boat slowed down and turned broadside to receive the bird. As the bird landed on the recovery ramp, dropped the ring, and entered the safety of the recovery box, the eagle startled the trainers by making a final pass. One trainer almost hit the eagle with a short boat paddle, so close did it come to the boat on that last pass at our bird. The gull literally collapsed in the recovery box. When the bird arrived at the vet's, it was barely alive. The bird had suffered numerous serious lacerations to one wing and along the back and neck. One potentially lethal wound was discovered. One of the eagle's talons had penetrated completely through the gull, from the back and emerging through the breast. It had penetrated one lung and bright, frothy blood oozed with each breath. After considerable patching up, the bird was put on extended sick leave. This bird recovered, and several months later, performed very well during final field tests.

TERRESTRIAL SYSTEMS

An example of a terrestrial system is the use of dogs in land mine detection. Dogs have served the military services for many years, chiefly for sentinel duties. More recently, dogs have been useful as olfactory sensors for military and civilian agencies.

Some breeds of dogs combine good temperament, fairly high intelligence, a keen sense of smell and hearing and a natural curiosity. There is a long list of surveillance and detection duties which such an animal can be trained to perform. Today narcotics and explosive-sniffing dogs are commonly used by various law enforcement agencies. Most handlers of these animals never cease to be amazed by the sensitivity the dogs display.

In one project, golden Labrador retrievers were trained to search out very small, plastic anti-personnel mines buried up to 15 centimeters (6 inches) in the earth. Some of the mines the dogs detected had been buried and exposed to the elements for over two years.

In the course of the work with certain land animals, we developed a number of remote guidance systems. These guidance systems were used to direct the animal from Point A to Point B. There are a number of possible approaches to guiding the animal. One of the simplest is to have the animal home-in on some signal, either visual, olfactory, or acoustical. It is more difficult to condition the animal to respond appropriately to guidance cues located away from the target. However, a number of systems have been developed in which animals may be guided remotely.

AQUATIC SYSTEMS

An excellent aquatic example of combining extraordinary sensory abilities with special response capabilities is the Navy's Operation Quick-Find. Here, pinnipeds and cetaceans—

specifically, California sea lions, bottle-nose dolphins, pilot and killer whales—were trained to dive, locate, and retrieve or mark submerged objects, with the aim of recovering lost gear and weapons. The animals used whatever sensory systems were available to them, from visual inspection (where possible) to sonar inspection for targets in dark and murky waters. Sometimes the animal attached a "grabber" and towed the object back. Sometimes a marker was attached which floated to the surface and mechanical means were then used to retrieve the object. In any case, the dramatic part was the animals' ability to locate these submerged objects, and to dive to extraordinary depths to do so. The dolphins and sea lions were capable of routine dives of 150 to 180 meters (500 to 600 feet), the whales to depths of 300 to 480 meters (1000 to 1600 feet), with good indications that even greater depths can be achieved. Incidentally, experiments with these animals are of interest, not only because of these special mission capabilities, but because of the physiology of their deep diving mechanisms. This is of concern to those studying human divers—how can these animals accomplish these deep, rapid dives, without the many physiological problems which plague human divers?

The bottle-nosed dolphin *(Tursiops truncatus)* is well adapted to cope with its environment. It is capable of a fairly high rate of speed (probably in excess of 20 knots); it is large enough not to be intimidated by most other sea creatures. Its vision is excellent. The dolphin apparently can focus its eyes very well below the surface and fairly well above water. In addition to excellent vision, probably only of marginal use much of the time, the dolphin possesses a remarkable sonar system, as is well known, and high degree of intellect. Researchers have shown that dolphins are capable of learning complex chains of behaviors. Evidence indicates that dolphins can develop at least simple concepts.

Many systems employing dolphins require the dolphin to get from point A to point B. These points could be near or far apart. In most instances, the dolphin would be moving through waters completely unfamiliar to it, a difficult task for any animal. Wild animals are, for the most part, territorial and are uneasy about entry into unfamiliar areas. It is likely that the exact pathway a dolphin will have to follow to get to the target and return cannot be predicted in advance. Of course, if it were possible to lay down some kind of physical trail (e.g., markers, a cable, or some other recognizable trail) the solution would be simple. A dolphin, and many other animals for that matter, can be taught to follow a distinct path. In many, if not most instances in aquatic situations, the course cannot be laid out in advance. Somehow a guidance system must be built using the combined capabilities of man, machine and dolphin. Many such systems are possible and several have been tried with varying degrees of success. Those guidance systems that have been successful have had certain common features—the orientation information supplied the dolphin was unequivocal, more or less continuous, and very reliable.

In one of the research programs, dolphins were conditioned to carry loads of varied configurations and weights. Techniques and devices were developed to guide the dolphins over extended ranges in the open ocean.

OTHER SYSTEM APPLICATIONS

Designers of animal systems have been handicapped by a lack of basic information. A number of the programs have been designed to fill some of these information gaps. One of the projects attempted to establish physical criteria for the design of internal and external loads. Several species of birds and mammals were selected for study. An effort was made to use species representative of large classes of animals. Packages of various sizes, weights, shapes, and dimensions were attached externally and inserted internally. Different locations of both the internal and external loads were investigated. All surgical procedures were developed with the assistance of a veterinarian. External loads were attached with harnesses, jackets, and certain forms of adhesive. After loads were attached, the degree of deterioration of the animals' locomotion was measured objectively and judged subjectively. Other physical and behavioral responses to the loading were studied.

As a representative of small birds, the common starling was tested. A lightweight harness made of Velcro was used to attach external loads to the breast and back areas. It was not necessary to train the birds in any fashion. The starlings were simply placed in a large room and their flight patterns were observed. If a weighted bird could take off from the floor and easily reach a platform some 2 meters (6.5 feet) above the floor, the bird seemed to be able to fly without effort. Taking off from the ground and gaining altitude were the most critical factors of flight. Once airborne with a weight, flight was much easier. This proved to be the case in all of the tests with every avian species. If the maximum weight a bird could take off with and fly to an elevated point some distance away could be determined, this would establish the maximum practical weight-carrying capability.

For a starling, the external practical weight limit was 15 grams (0.5 ounce). A somewhat larger bird was a crow with an average body weight of 550 grams (19 ounces). Crows were harnessed, again with Velcro material. They were trained to take off from the ground and fly some 30 meters (100 feet) to a platform. The data indicate that 90 grams (3.2 ounces) is a safe maximum load limit, although the crow can carry more. As already mentioned, these birds can carry around 75 grams (2.6 ounces) in their beaks. Mallard ducks could easily take off with and carry about 100 grams (3.5 ounces). Since mallards are particularly fast flyers, the aerodynamic design of external packages is important. The common turkey vulture with a wing spread of about 2 meters (6.5 feet) could easily take off and fly with external loads of 250 grams (8.8 ounces).

Among terrestrial animals, the wild rat was tested. This presumably hardy animal was extremely susceptible to the emotional stress of captivity. Often, the wild rats died of simple, fear-caused stress. When they were successfully kept alive, they could easily carry about 25 grams (0.9 ounce) externally.

Two species of monkeys were tested, the specialized, tree-dwelling, spider monkey and the more generalized, stump-tailed macaque. A completely satisfactory harness or other means of attaching external loads to monkeys was never found. They possess powerful hands and feet and are clever and persistent at using them. The monkeys can easily carry 20 percent of their body weight around 1.5 kilograms (3.3 pounds) for a macaque or 0.65 kilogram (1.4 pounds) for a spider monkey .

The wild hog (the same species as the European wild boar), was the largest species tested in this particular program. The wild hog's unsavory reputation was well deserved—the pig destroyed all but the sturdiest of harnesses. The pig could carry whatever was kept on its back, up to 15 kilograms (33 pounds). Heavier loads shifted or tore the harness.

Some experiments were conducted to test internal load carrying capabilities of animals. In the course of these experiments field surgical techniques were developed. Small birds proved very delicate surgical subjects and the internal loads they could manage were low; volume rather than weight was the limit factor. The starling was limited to a volume of 12 cubic centimeters (0.7 cubic inch); the crow, 48 cubic centimeters (2.9 cubic inches); the duck, 66 cubic centimeters (4 cubic inches); the vulture, 75 cubic centimeters (4.6 cubic inches).

The very small wild rat was a difficult subject for implantation of packages. The rat could carry a volume of 33 cubic centimeters (2 cubic inches) and a weight of 50 grams (1.8 ounces) internally. The monkeys tested could carry approximately 100 cubic centimeters (6.1 cubic inches) in volume and weights of approximately 150 grams (5.3 ounces). Beyond these limits, internal injury could result in the course of the monkey's normal activity.

The wild pig could carry bulky objects up to 4 liters (4.2 quarts) in volume. Actually the pig could carry more volume; the load was limited more by incision size than by any internal restriction. Of course with large loads, density and weight become important. Large objects, three or more liters in size, should weigh no more than 2 kilograms (4.4 pounds) to prevent long-term tissue damage. If the load will be implanted for only a short time, several days for instance, the weight can be increased to about 3 kilograms (6.6 pounds).

In general, the experiments demonstrated that animals could be safely operated on under field conditions and that there are four prime factors in load design: volume, shape, weight and density. A relatively small package is much less critical in the shape and density categories, and,

all other factors being equal, it is better to have two or three smaller loads than one large load. Properly designed cables, which interconnected packages, caused no problems.

DESIGN CRITERIA FOR PRACTICAL BEHAVIORAL SYSTEMS

How does one go about designing and building a system that includes an animal (other than human) as one element? Experience has shown that the design techniques employed in developing hardware-oriented systems are applicable to animal oriented systems. In each case, animal or hardware, it is simply a matter of defining a problem and applying state-of-the-art techniques to solving that problem. If the technology is not good enough, a period of research and development must be undertaken to extend the state of the art. Just as in hardware engineering, biological or behavioral engineering requires a clear definition of the problem.

While it might seem simple to define a mission, on a number of programs months have been spent trying to pin down objectives. For a mission-oriented system, the questions that need to be answered most are: what, when, and where? What is to be done? When is it to be done and where will it be done?

The next step is to identify those unresolved issues critical to the development of the system. Sometimes, there will be only one that stands out; more often there will be two or three that need solution before the program can progress. If the kind of animal to be used has been selected by this time, and it is some exotic species, it is recommended that, before any major effort in any other area is made, at least a tentative study be made to demonstrate the feasibility of that animal as a subject for experimentation. The initial choice of animal may be unavailable, may not live well in captivity or, for some other reason, may be unsuitable. In this search, another animal even better suited than the original choice may be found. It is suggested that persons familiar with the problems of working with animals be contacted. They may be very helpful in pursuing your ideas and offering optional plans.

Once the critical areas are identified, before anything is constructed, and before any timetable is established, it would be worthwhile to develop a basic plan for achieving the defined mission. More than one plan may have to be formulated to allow for options and unknowns. Plan backwards from the objectives of the mission; think of the task that the animal is finally going to have to accomplish. The planning approach is basically the same, whether the animal will be performing its tasks in a small box or several kilometers out at sea.

In most of the systems studies, the animal element has been critical to the operational success of the system and the mission. Yet, in many, if not most programs encountered, the mission has been fixed and the equipment or hardware elements were conceived, designed and, in many cases, fabricated before the biological element has even been considered by persons familiar with the animal's possible requirements. The net result has usually been that the hardware constructed did not fit the animal and, 1) either the hardware had to be redesigned, 2) the system operated under a self-imposed handicap, or, 3) the system failed in its mission and what might have been a good idea was abandoned, with little chance for revival.

It is not surprising that the animal got little consideration in the early 1960's. There were few biologists who could converse with electronic engineers, physicists, systems analysts and others who populated the various committees exploring the use of animals in a systems context for military purposes. The psychologists were not much help either, since very few had experiences with animals other than pigeons, monkeys or rats and, even then, almost always in the confines of a laboratory. More recently, hardware designers, the military and psychologists have demonstrated a greater awareness of the animal and have sought to know the animal as an integral and critical part of the whole. Engineers are now asking what criteria should guide the selection of animal species for any given biological system.

There are really two problems here: 1) the selection of the species to be used, and 2) the selection of individuals within the selected species. With regard to the first problem, selection of species, the suitability for the task at hand needs to be considered. With respect to suitability, what are the performance characteristics of the animal—will it operate in the desired

environment? Does it fly, swim, or walk? Then, can it fly at the required speed, swim far enough, learn the required discriminations and perform the desired responses? If these requirements are met, what is the availability of the chosen animal? Can it be purchased from a regular laboratory supplier? Can it be trapped or collected at any time, or only in certain seasons? What are the special collection or trapping problems. Permits required? Special gear?

What are the maintenance characteristics of the species in question? Does it require special temperature housing and humidity conditions? Will there be contact with others of its species or close contact with other species? Is there a need for special diets? Are there any special requirements which might limit its usefulness in a security system?

What is the state of the art with regard to knowledge of the available response systems of the species in question and its sensory systems? What do we know about the ability of the animal to learn; which discrimination capabilities are within its repertoire?

Are there security considerations such as, how unusual is it to see a certain type of animal in a given area? If a certain animal is on a mission of some sort, is it apt to be in trouble simply because it is unusual in this particular environment?

Once the decision is made with respect to the species to be tested or employed, crucial work remains to be done with regard to the selection of individual subjects within this species. For example, in the work with pigeon ambush detection systems, pure-bred, line-tested, homing pigeons were needed in order to get the flight capabilities which were required. It is also important that individual subjects be properly selected and handled at the critical period for imprinting or socializing to human beings.

Often, at this stage, questions are asked concerning certain species which cannot be readily answered by library research or from familiar sources of information. For example, information regarding the sensory capabilities of a given species under field conditions may be needed. More often than not, if the animal has been studied at all, the studies were made in the controlled environment of an indoor laboratory. Often, data collected under these controlled conditions do not readily translate to practical application situations in an outdoor environment.

It has been asked whether certain birds can make visual discriminations of stimuli at a great distance and respond on the basis of these discriminations. Laboratory studies indicated that pigeons should have good distance acuity because they could discriminate fine-lined grids presented to them in the confines of a Skinner box. To test whether in fact a pigeon and other birds could respond to stimuli some distance away, an experiment was designed in which the pigeon was contained in a small box. The stimulus was located some distance away from this box and consisted of a black and white striped target. The bird's task was to discriminate whether the stripes were vertical or horizontal. The bird made its choice by pecking the appropriate key placed directly in front of its box. The target was moved further and further away from the bird. The visual acuity of the bird was determined by the distance at which the bird could discriminate the vertical from horizontal position of the stripes.

According to the information gathered under standard laboratory conditions, the pigeon should have been able to discriminate the vertical and horizontal stripes a considerable distance from the box. In the field tests, the pigeon's visual acuity was very poor. The bird's response broke down at a distance of only a few meters. It is probably not that the pigeon really had poor vision, but that the pigeon's natural behavior patterns made it difficult for it to make a close-up response to a distant stimulus. This difficulty of directly responding to a distant stimulus supported field observations made by the trainers.

The same visual discrimination test was made with ravens. Western and white-necked ravens had no difficulty in extending these distances considerably, up to 265 meters (865 feet).

This discrimination capability, of course, is phenomenal, indicating an acuity of 0.2′ of an arc, compared to the average human figure of 0.5′. These experimental results were consistent with the raven's superior field performance.

It should be mentioned that these experiments were conducted under conditions which were vastly different from those of the controlled environment in the laboratory. Although the bird was confined in a box, almost everything else varied as it would under natural free-flight conditions.

The weather changed, from light rain or mist to bright clear sunshine. Distractions occurred—cats, cows, and sometimes hawks appeared in the line of sight. Notations of these variables were made. Some variables were carefully controlled—drive or motivational level of the bird, operation of the control devices and training equipment, and the randomizing of the target presentation.

In addition to studying sensory processes of various species, the trainability, adaptability, response capabilities and handling methods were determined for a number of species. The tests have included strictly controlled, indoor laboratory experiments, as well as tests in the open environment. The out-of-door tests, although they are of necessity less strictly controlled, are often more applicable to an operational system, and they may be less costly as well.

A number of tests were developed to measure, to some degree, the question of species suitability for a given mission. These tests involved manipulating objects, locomotion problems and discrimination of stimuli. A behavioral profile for an unfamiliar species can be developed quickly. Incidentally, for many new species programs were developed for simply keeping them alive and growing—diets for infant albatrosses and special medication for the treatment of fungus disease for gannets.

Research, development and time requirements for a new animal system will vary considerably depending on the species involved and the tasks to be performed. It takes much longer to develop and test a system if the animal is a new species or the mission requirements are complex or difficult. There are similarities here with hardware systems development. Sometimes, a hardware system can be developed by experienced people using time-tested materials and already established techniques. The hardware may have been previously tested under the conditions that will be met during the mission. If the mission itself is also a familiar one, then system development will usually be relatively simple and straight-forward. If, however, one or more elements of the system or the mission is new, development becomes more difficult, time-consuming, costly and the outcome is less predictable.

What may development times for some hypothetical animal-oriented systems be like? Remember, systems development should include delivery of an operational unit plus data on reliability under specific environmental conditions.

First, consider a system that utilizes a common homing pigeon, where the pigeon does nothing more than discriminate and makes a simple response to a signal under non-stressful conditions. Such a system could take as little as one month to as long as five months, depending on the exact mission. The chances for success of the program would be reasonably good and the system would be quite reliable. Suppose the situation were complicated a bit, with the pigeon having to perform its tasks under some known environmental stress such as vibration or axis rotation. Assuming that the stress tolerance of the bird would have to be determined, system development time would increase from three months to six months. As expected, hardware costs to simulate mission conditions would go up significantly. While the mission demands have increased, a familiar animal is being used and it is already known that the animal will perform while undergoing the type of stress called for by the mission. The stress limits and reliability are all that need to be established—how much vibration and rotation the bird will take and still perform. Again, the outcome of the program should be successful and the animal will perform predictably—but the project will take longer and cost more.

Take a quantum jump with a more complex hypothetical pigeon system. Call it "Pigeon Impossible." A pigeon is to fly out and search for a specific object. This object, if it is there at all, may be anywhere in a specific 100 square kilometer (40 square mile) area. If the bird locates the target, the bird returns to a fixed point and taps out on a set of keys the coordinates of the target. The search pattern would be monitored by radar transponder. Breaking this mission down to its simple elements, the bird must first know what it is to be looking for; next, the bird must identify the search area; the bird must then set up some kind of a systematic search pattern in that area.

If the bird sees the specific mission object, the bird must orient the target within the search area. Once the bird identifies the coordinates of the target, it must return to a designated point to report. The bird is now obliged to encode the coordinates in such a way that it can be understood by humans. The bird must accomplish all of this with a brain weighing about 15 grams (0.5

ounce). Needless to say, this is beyond anything yet asked of a pigeon, well beyond the state of the art in animal training. There are many questions to be answered, both theoretical and practical. Additionally, a radar transponder small enough to do the job is not readily available now, so development would be involved here as well. All in all, such a program might take many years, because research, engineering, development, and production would necessarily be combined. The chances for success of such a system are probably not good. It is possible that a pigeon could be trained to do all of these things, but there are so many chances for error on the part of the pigeon that it is probable that the reliability of the system would be low. In summary, this would be a costly and risky system to attempt, with the present state of the art in hardware and in animal conditioning.

For another example, assume there was a need for a fresh-water dolphin to perform tasks in certain large lakes in foreign countries, much the same as the familiar salt-water dolphins which have been used. Actually, much of the behavioral and hardware technology already exists. Only modifications have to be made. In some respects, the job is simplified since normally the fresh-water environment is not as hostile as salt water. However, in spite of the head start in understanding of the mission and the hardware, it is likely that the development of a reliable, fresh-water dolphin system might be a couple of years in the making because very little is known of the fresh-water dolphins.

Nutrition, medical care, environmental tolerances, social and other needs are not yet well enough understood to assure success. A ready source of supply of suitable specimens to work with is not available.

It is best to try to solve a few problems at a time, rather than push hard in all areas at once. This is particularly true with the animal and animal/hardware interface elements. By painful experience, it has been learned that it is best to let the animal "tell" you its needs. It is best not to be too quick to fix a design until it has been tried by the animal in question. Too often, in contract work, too much emphasis has been placed on fixing the design of hardware elements at the very beginning of a program. In most instances, this is an attempt to shorten development time. There usually has not been enough program flexibility to allow for the inherent biological demands of an animal system. Such facts of life as maturation, learning, seasonal reproduction and other factors are sometimes not fully understood or appreciated by hardware-oriented engineers and contract administrators.

Such systems can be looked upon as "tool-like" extensions of our own sensory or response capacities. Very little is known concerning the senses of animals and even less about the general process of perception. Yet, it seems that one of the prime attributes of an animal, be it a cockroach, chicken or killer whale, is its ability to perceive and respond to its environment. Millions and perhaps billions of years have gone into developing the information sensors, storers, retrievers, correlators and all of the other components involved in the process of perception. A tiny mosquito is a flying carbon dioxide-sensing platform weighing a tiny fraction of a gram. A honey bee senses polarized light and its angle of incidence relative to its body. It also is somehow cognizant of the passage of time. Thus, a bee perceives where flowers are relative to its own hive and can transmit this information to its colleagues. Rattlesnakes possess a sensitive infrared sensor. The moth has the capability of locating its mate by perceiving a chemical that is in the air in a concentration measured in parts per billion. The moth collects the odor, detects it, determines which direction it comes from and pursues the target. And the total weight of the entire system is a fraction of a gram. The point is that biological perception systems are worth studying. The spin-offs from such studies can have potential military and security uses.

It is possible to somehow tap into an animal's nervous system and read the output from any given sensory system. Whether use of the information thus provided can be made, is something else. For example, it has been known for many years that by attaching electrodes to various parts of the hearing apparatus of various animals (dogs, cats, dolphins and humans), electrical potentials can be picked up and amplified. The animal, in effect, becomes a living microphone. We are able to hear what the animal hears.

Pursuing the topic of animal systems on a neuronal level, it has been shown that the effects of some conditioning can be detected in the output of certain cranial nerves. While the

relationship between conditioned and unconditioned behaviors is still not established, there is evidence that alteration or control of unlearned behavior can lead to changes in neuronal output. The persistence of such changes in the nervous system is not yet known. It is conceivable that information could be encoded and stored in an animal's nervous system using behavioral techniques. The animal's "memory" or perception of past events becomes a storage bank awaiting a triggering signal for readout through one or more nerve fibers. Continuing the trend of thought along microbiological avenues, biologists, physiologists, biophysicists and biochemists are studying the actual formation of memory and transmission of information along individual nerve fibers. Beyond this is the encoding of information on the surface of and in the interior of individual cells. The next decade may see an amalgamation of the behavioral and biological sciences on a cellular level and the emergence of a real understanding of behavior. This merging of disciplines could have dramatic impact on possible military and security applications.

It might be interesting to consider direct application of some additional animal systems of both sensory or response types. Certain hypothetical systems based on the present state of the art in hardware and our own experience in behavioral technology can be described.

One immediate application is the use of the olfactory capabilities of dogs or other animals. It may be possible to tag fissionable materials or other items deemed critical with a specific odor. Dogs could then be used to conduct personnel inspections, either on a spot-check or a continuous basis. A possible fringe benefit of such a system would be the resistance of the dog to bribery, blackmail or extortion.

Aquatic surveillance systems have been of interest for many years. It would be a simple matter to condition dolphins to perform sentry duty in aquatic environments, as dogs have been trained for terrestrial areas. The dolphins could remain in place and passively listen for those sounds associated with surface or scuba swimmers, or submarine transporters of various types. Such a system might be useful in guarding nuclear installations near seashores. The range of detection would depend on the ambient noise, the environmental acoustics and loudness of the intruder's activities. If a dolphin were permitted to swim the perimeter of a defense area, the surveillance area would be increased even further. In either case, once the dolphin detected a suspected intruder, the dolphin could make a specific response to a human handler nearby. It is best, for theoretical as well as practical reasons, to have this detection verified by another dolphin, or by the first dolphin repeating the detection procedure. Should the dolphin continue to report an intruder, a dolphin or a human swimmer can be sent to intercept the intruder. This particular system would be relatively simple to produce since it requires very little specialized hardware.

A dolphin could serve as an excellent vehicle to survey certain coastal waters and supply photographs. As previously mentioned, dolphins can be guided many kilometers to a precise point where they can perform one of several particular actions depending on the circumstances. Guidance information, data links and tracking information could be supplied by radar or radio channels. Less conventional guidance and information systems might include submarine transmission or earth satellite transmitters. Precise location fixes could be supplied with present technology, shore-based stations or satellite systems.

Consider something as simple as teaching a cockroach to run a maze—attached to the cockroach is a fine gold wire, finer than a human hair. A cockroach could pull many meters of such a wire through heating or cooling ducts. It is known that cockroaches are sensitive to vibration, temperature and other environmental factors. What would prevent us, or someone else, from tapping into the nervous system of a cockroach—the cockroach becomes a tiny, living transducer, transmitting information through the wire to a receiver.

A rat, trained to follow an odor trail, could be used as a live drop. A pouch, placed surgically beneath the skin, could be used to transport messages on microfilm.

Domestic farm animals, operating near a frontier, could be used to smuggle contraband. A cow could carry surgically over 30 kg of weapons, ammunition, explosives or other material implanted in its gut. The surgical procedures are simple, require little skill and would take less than 15 minutes per cow.

Consider that wild Eurasian boars abound in certain mid-East and African states. It would be possible to lay down an invisible odor trail for a given herd to follow between two feeding

stations. In a short space of time, an entire herd could be conditioned to travel from one point to another following this odor trail. Once this migratory pattern had been established, certain pigs could be stuffed full of contraband—more than 4 liters (4.2 quarts) in volume or 5 kilograms (11 pounds) in weight. The entire implant procedure would take less than 8 minutes per pig and could be done with commonly available tools and materials.

A large bird such as a vulture can carry a package and hover over a given station unsuspected for long periods of time. Such a system could provide valuable surveillance of areas which might be inaccessible to human patrols and in situations where deployment of aircraft was undesirable.

Again, a large bird could hover overhead, this time trailing an invisible, long, fine wire. A nearby low-powered transmitter could beam a message. A small receiver and tape recorder unit inside the bird could capture and store the message. A few hours later, in another location, someone could interrogate the system.

Since 1962, our company has been involved with Government projects, studying, training and evaluating a number of animal species—over 19 species of birds, 8 species of land mammals, and 9 species of aquatic mammals. At the same time, in our own private business, we experimented with another 30 or more different species for commercial purposes. The military work resulted in the development of several potentially useful systems, training programs and the acquisition of considerable useful information. The total level of effort for the behavioral work was quite low as Government programs go. Also, most of our programs were generally of short duration, a year or two at a time; sometimes less. Even a small country with limited resources could easily mount an effort of this scale, with results which could be highly useful to them and detrimental to us.

How could such an animal system be used to our disadvantage? Animals are ubiquitous and generally not subject to close inspection. It doesn't take much imagination to see how an animal, particularly a small bird such as a raven, or a small mammal such as a rat could be used to penetrate even a highly sophisticated security system. The use of animal systems in less-developed areas of the world would be particularly easy and probably rewarding. Security and intelligence agencies should be made aware of the potential of animal systems. Our own national posture seems to be that little military use will be made of biological systems. Other countries may not be so disposed, so it is in our best interest to know the capabilities of animal systems. Programs studying animal sensory capabilities, locomotion and other attributes both physical and behavioral, should be supported whenever possible; especially applied research programs oriented toward practical applications. By knowing the capabilities of animals, understanding animal sensor mechanisms and how they may be compatible with man-made instrumentality, it will be possible to assess potential uses against our country and also to develop necessary countermeasures.

PHYSIOLOGICAL CORRELATES OF INFORMATION PROCESSING LOAD—ONGOING RESEARCH AND POTENTIAL APPLICATIONS OF PHYSIOLOGICAL PSYCHOLOGY

Thomas E. Bevan

Science Applications, Inc., Arlington, VA 22209

INTRODUCTION

The three objectives of this paper are to describe:

- The process of identification of human factors problems for military command, control and communications (C^3) systems and how the same process applies to security systems,
- the nature of physiological psychological (or biocybernetics) experimentation and applications, and
- how physiological psychology methods might be applied to security problems.

SAI has been tasked by the Defense Advanced Research Projects Agency (DARPA) to identify human factors problems in the military C^3 environment, and to conduct psychological experimentation toward applications which would result in improvements in C^3 man-machine systems performance. This effort involved conducting task analyses at various C^3 centers, both here and abroad (e.g., SAC, NEACP, ANMCC, METRO, Sweden, Germany). The aim of task analysis is to identify the tasks, or specific behavioral sequences, which make up a specific job function. These tasks can then be analyzed from a psychological perspective to determine performance goals, hardware, software, and human factors problems associated with each task. The output of this process (as shown in fig. 1) was an R&D roadmap for the DARPA Human Factors and Biocybernetics (Physiological Psychology) Research Program. A human factors/physiological psychology lab has been constructed by SAI in Rosslyn, Virginia; this includes a PDP 11/70 computer, various I/O devices and physiological measurement equipment.

From the study of command centers, several human factors problems were identified. Experimentation began this year in human factors and physiological psychology (biocybernetics).

Human factors experimentation involves several important issues for improving C^3 systems:

- Highlighting to improve information flow

  A series of studies will be conducted to investigate the use of visual, temporal and auditory highlighting techniques for facilitating information processing.

- Human-computer credibility

  Studies will be conducted to determine those characteristics of man-computer and human interactions which influence the relative use of human and computer aids. Should differential use of human and computer aids be discovered, additional studies will be conducted to develop prediction equations for determining when computer aids will be rejected as unreliable. Other studies may also be pursued to investigate whether or not the use of a computer aid is task specific, how computer response characteristics affect mancomputer interaction, or the effect of "bad" data on the use of a computer aid.

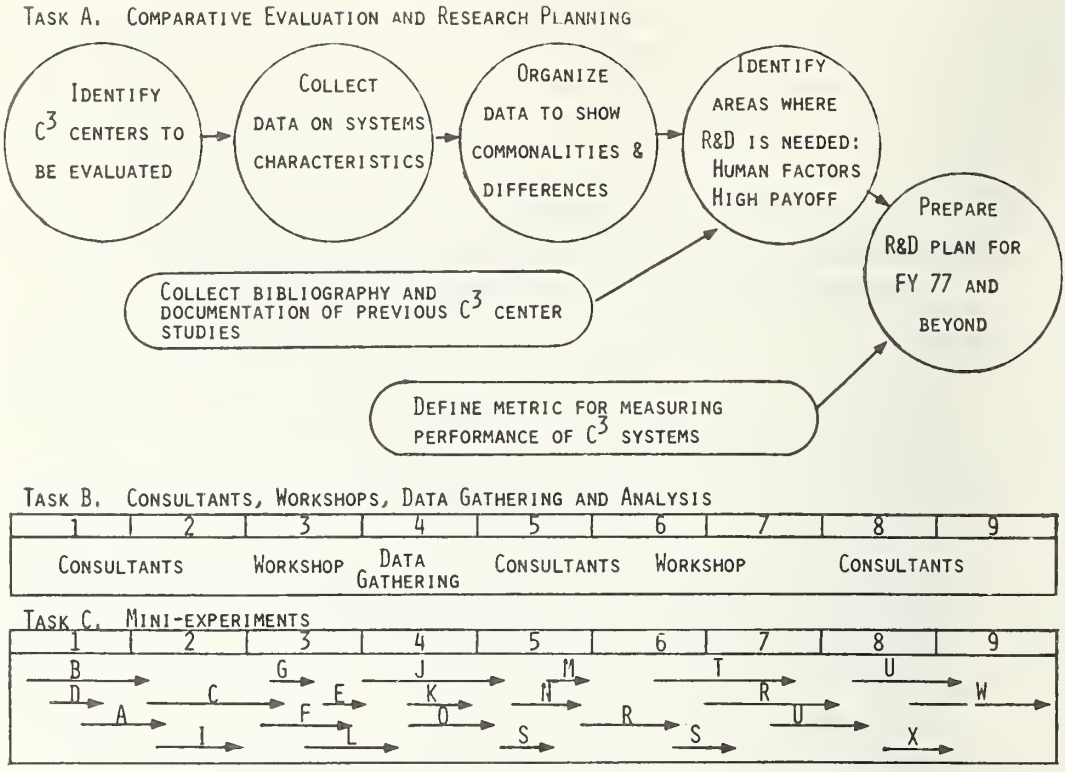


FIGURE 1. *Plan for human factors and biocybernetics research on C³.*

- Natural versus stylized language

  Studies will be conducted to evaluate grammatical English as an interactive language for retrieving information from a computer, especially as compared to stylized query languages. This should allow us to determine the utility of "natural" language for interacting efficiently with computers.

- Preferred and most effective rate for presenting speech

  Many people have preferred speaking and listening rates. When these rates must be changed to accommodate other people, the resulting discomfort may affect their ability to attend to the communication. Research is planned to investigate preferences for speaking and listening rates and their effects on comprehension of auditorially presented messages.

- Large versus small screen presentation

  What is the most appropriate size display for computergenerated text and graphics? We hope to empirically determine the display size requirements for these display types.

- Improve map symbology

  A series of studies will investigate the "innate" or cultural meaning of color for facilitating perception of military threat.

- Spatial memory

  Experiments will be conducted to continue our work in investigating the role of spatial cues in the recall of information.

° Picture-word processing and decision-making

This is the final experiment, in support of Kroll and Potter, DARPA-funded contractors, which investigates the use of visual, temporal and auditory highlighting techniques for facilitating information processing.

Experimentation is also being conducted in physiological psychology under the DARPA Biocybernetics Program. The concept of biocybernetics requires some explanation. Just as "cybernetics" deals with the science of mechanical and electrical feedback loops, biocybernetics deals with feedback loops involving biological information. In a cybernetic thermoregulatory system, a thermostat acts as a sensor to transduce temperature into an electrical control signal. In a biocybernetic system, a biological signal, such as "brain waves" (EEG) or pupillary dilation, is transduced into an electrical signal compatible with modern computer equipment. For both types of systems the goal is to maximize system performance. In the biocybernetic system an attempt is made to optimize man-machine performance.

Biocybernetics represents an advance over traditional man-machine systems. In the traditional system, I/O devices (teletypes, CRTs, keyboards, etc.) act as interfaces between man and machine. In a biocybernetic system this man-machine interface is augmented by the transmission of biological information from man to machine, in order for the machine to be more responsive, and thus improve system performance.

An example of the layout of an EEG biocybernetic system, shown in figure 2, reveals that a biological signal is transduced by EEG amplifiers. This signal is then converted from analog to digital information for use by a computer. A display and teletype make up the traditional man-machine interface. This layout is similar to those already present in EEG laboratories and the equipment and principles of operation are well understood. The biological information must be interpreted by the computer; an algorithm must be provided by the physiological psychologist.

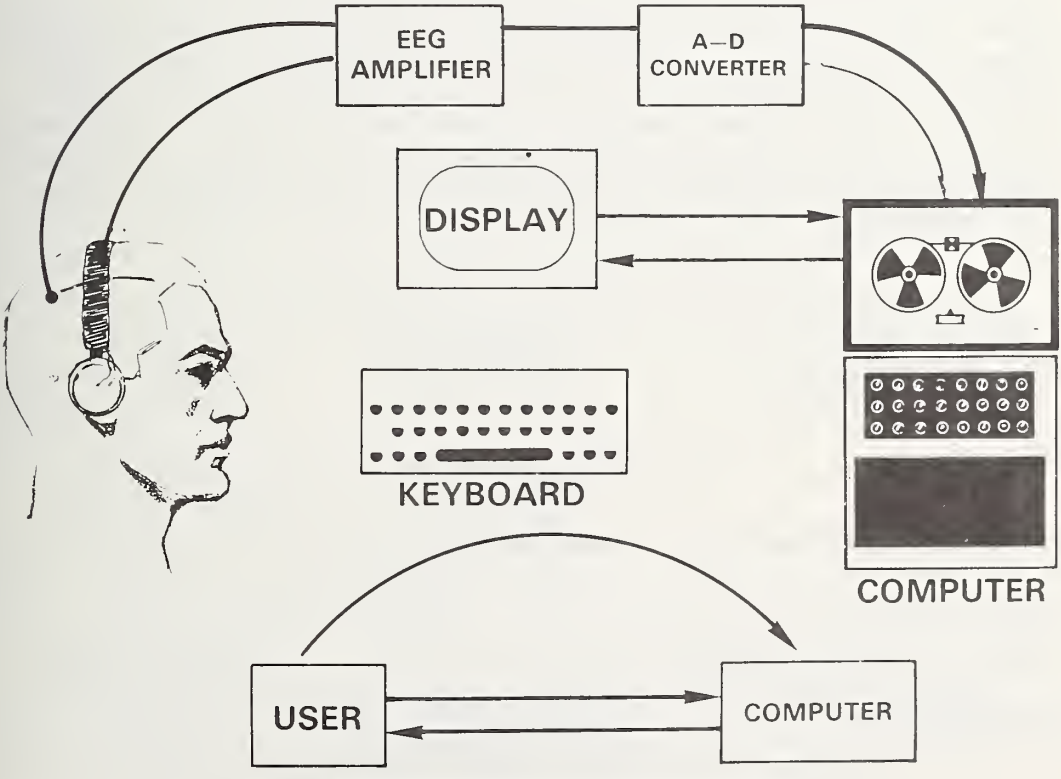


FIGURE 2. *How EEG information is used in a biocybernetic system.*

Several C^3 problems areas were identified in the DARPA study which might be ameliorated through biocybernetics technology:

(1) Message sorting often entails high information-processing loads (IPL). Many messages must be promptly and accurately routed. When on-line monitoring of a sorter indicates excessive IPL, the rate of message presentation can be slowed, or personnel can be rotated to prevent erroneous sorting.

(2) Conversely, IPL is too low in many indication and warning, and photointerpretation tasks. Given on-line detection of this user state, catch trials can be injected by the computer to bring up the user's level of arousal to an optimal state.

(3) Confusing messages, when detected, lead to excessive retransmissions for clarification and, when undetected, lead to immeasurable disruption of C^3 effectiveness. Biocybernetic measures of semantic meaning could be used in the message approval and message interpretation processes to prevent ambiguities.

(4) Decisionmakers and information analysts can be so inundated with decision-relevant information that they fail to comprehend and retain it completely. Biocybernetic indicators of IPL can be used to tailor the presentation of information to the decisionmaker so that he is exposed to it when fully receptive.

(5) Traditional human factors techniques for selecting among alternative systems and system element designs are costly, often subjective, relatively insensitive to users' internal states, and do not predict long-term user reactions. Biocybernetics measures hold the promise of alternative criteria on which to base such selections.

There are several biocybernetic technologies which have been developed under DARPA auspices (fig. 3). These involve essentially two types of biological information, the electroencephalogram (EEG) evoked response and the pupillometric dilation response. Both of these responses occur because a meaningful sensory signal is presented to a subject. When this evoked response systematically changes in response to information processing on another task, the changes can be used as an indicator or correlate of information processing load (IPL).

The first biocybernetics experiment to be conducted for DARPA by SAI concerns IPL correlates during a simulated message-sorting task. The performance of message sorters is degraded by both high and low IPL; this is particularly a problem for modern computer-communications systems. In the old systems, messages queued up at the end of the transmission line in terms of priority or classification labels. In modern computer systems, the messages are received by a high-speed computer at the end of the transmission line, but must be processed by a human message sorter for dissemination. This type of system is evolving at all of the C^3 command centers under study.

BC INFORMATION	ASSOCIATED CONSTRUCT	DARPA INVESTIGATOR
P300 N190 (EEG)	RELEVANCE, RARITY SURPRISE, IPL	DONCHIN U. OF ILLINOIS
MOMENTARY PUPIL DILATION	COGNITIVE LOAD (IPL) PSYCHOLOGICAL STRESS	BEATTY, UCLA
SEMANTIC EVOKED POTENTIALS (EEG)	SEMANTIC MEANING	CHAPMAN, U. OF ROCHESTER
EEG WAVEFORMS	"UP, DOWN, LEFT, RIGHT" MOVEMENTS IN CRT MAZE	VIDAL, UCLA

FIGURE 3. *The kinds of biocybernetic information abstracted from EEG and pupillary data*

The proposed solution to this problem, addressed by the first experiment, is to use physiological indicators of IPL to modulate message processing by the human "gatekeeper." Message presentation rate and message-sorting tasking or goal setting can be altered by computer algorithms which utilize EEG information.

In this message-sorting experiment, subjects are presented with messages (fig. 4) that must be sorted based on rules of various difficulty (fig. 5). The message is presented for a fixed time, after which the subject is prompted to respond with his/her answer. Auditory tones are used to trigger EEG evoked responses. Manipulation of IPL is accomplished by adding levels of decision-making to the task. EEG data analysis (fig. 6) includes background EEG analysis through activation measure and spectral decomposition. Evoked response data are analyzed through multiple stepwise linear discriminant analysis (MLDA) or principal components analysis.

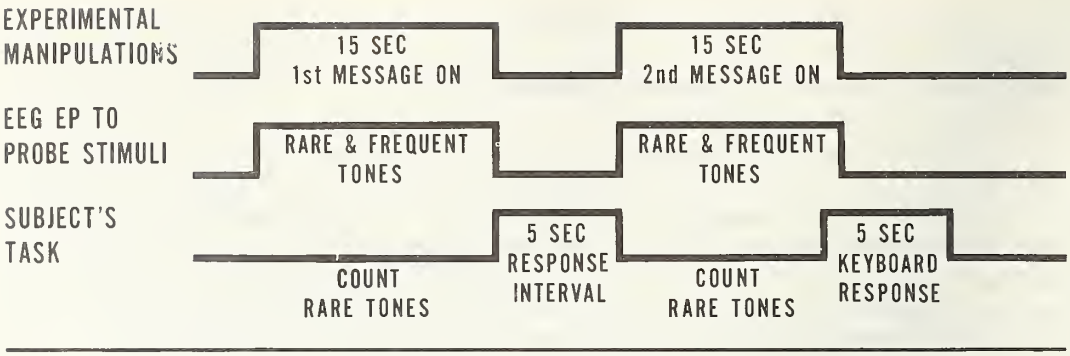
EEG indicators of IPL may also be useful as tools for human factors design of displays or other output devices. These physiological indicators can be measured with minimal interference to behavioral tests, are potentially more objective than rating-scale techniques and may result in R&D savings in time and cost. Hardware and software designs of displays may be selected on the basis of combined behavioral and physiological measurements.

```
  ***
 S
BULLETIN #001
REFS: BULLETIN #362
FROM: CALIFORNIA STATE ENERGY COMMISSION/
      COMMISSIONER RATCHFORD
TO  : UPI
DATE: 1449
SUBJECT: REFRIGERATOR ENERGY STANDARDS

     THE CALIFORNIA ENERGY COMMISSION ANNOUNCED TODAY THAT
TWO MAJOR NATIONAL MANUFACTURERS HAVE VOLUNTARILY ADOPTED
THE CEC'S REFRIGERATOR ENERGY STANDARDS.
     BOTH PHILCO AND WESTINGHOUSE PLAN TO BEGIN PRODUCTION
OF THE NEW MODELS WHICH COMPLY WITH THE COMMISSIONS STANDARDS.$$
***
 M
BULLETIN #002
REFS: BULLETIN #374
FROM: U.S. MARINE FISHERIES SERVICE, WASH DC/
      INFO DIRECTORATE
TO  : US ARMY CORPS OF ENGINEERS, UPI
DATE: NOV 11, 1976
TIME: 1053
SUBJECT: BAN ON PORPOISE KILLS

     A BAN ON KILLING OF PORPOISES BY U.S. TUNA FISHERMAN OR
AS A BYPRODUCT OF ENVIRONMENTAL ALTERATIONS FOR FLOOD CONTROL
OR OTHER PURPOSES WAS ANNOUNCED YESTERDAY BY THE NATIONAL MARINE
FISHERIES SERVICE.  THE BAN WILL LAST UNTIL THE YEAR'S END.  A
QUOTA OF 78,000 DEAD PORPOISES WAS SET FOR THIS YEAR.$$
```

FIGURE 4. *Examples of messages used in message-sorting experiment.*



MANIPULATION OF IPL

LEVEL I:
INTRA-REGIONAL OR EXTRA-REGIONAL SOURCE

LEVEL II:
ADD GOVERNMENT, NON-GOVERNMENT SOURCE DECISION

LEVEL III:
ADD PERSON AGENCY SOURCE DECISION

FIGURE 5. *Message-sorting experiment.*

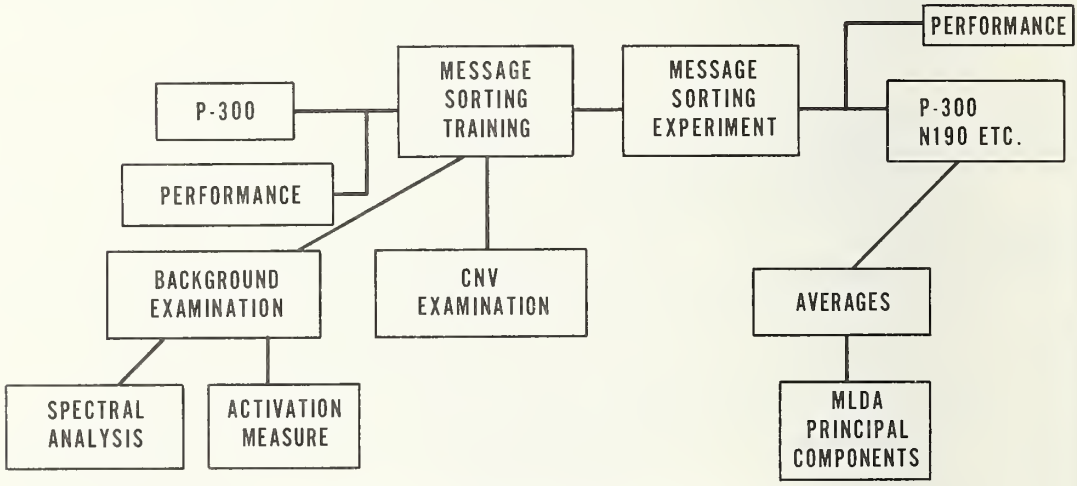


FIGURE 6. *Message-sorting experiment data analysis.*

Biocybernetics technology and physiological psychology have applicability to security problems in at least three areas:

- Correlates of IPL can be utilized to assess the performance capabilities of guards performing vigilance tasks.
- EOG (electrooculogram) correlates of eye movements could be utilized in a covert EOG duress sensor system. Recorded EOG signals indicate that characteristic EOG signals, when voluntarily produced by guards, could be used to send a duress alarm.
- Physiological changes in speech production due to stress could be used to determine if security personnel are under threats or intend collusion.

TOWARD THE COLLECTION OF CRITICALLY EVALUATED ERGONOMICS DATA

Harold P. Van Cott and Joel J. Kramer

National Bureau of Standards, Washington, DC 20234

INTRODUCTION AND OBJECTIVES

The importance of critically evaluated data has long been recognized by the physical sciences, engineering and the high technology sectors of commerce and industry. Today, collections of selected and evaluated numerical data on the properties of substances and materials are being developed in data analysis centers around the world. These centers systematically extract, evaluate, organize, and publish data from scientific literature on many topics, ranging from the properties of neutrons and crystalline substances to information on alloys and chemicals. When gaps in data exist or available data are of poor quality, arrangements are made to obtain the needed data by conducting appropriate research. Evaluated data are then made available to users in the form of monographs, journal articles, printed tables and computer tapes. Access to these data saves time when searching for needed information and reduces the likelihood that erroneous or inaccurate data will be used or that research will be unnecessarily repeated.

The activities of these data centers are an intrinsic part of science and technology. They not only retrieve and process information; they also create new information. They are an important aspect of industrial research and development. In short, critically evaluated data are of vital importance to the nation's economy.

Except for a few handbooks and other specialized compilations, systematically developed and evaluated data collections do not exist in ergonomics or behavioral science.[1] None of these compilations can claim to rely on evaluation criteria more stringent than the subjective process of peer review for critical evaluation. As a result, far more complete, precise, and accurate information exists on the electrical conductivity of tungsten than exists on human hearing, vision, or other basic human performance characteristics. There are fewer systematically developed data on the physical dimensions and strength of the human body than on the properties of sodium bromide. Yet data on each of these topics play a critical role in the design of physical security systems, safe efficient consumer products, systems, and home and work environments. It is not our purpose to speculate why this is the case. Rather, the objectives of this paper are to:

- Examine the requirements for a collection of critically evaluated ergonomics data.
- Stimulate the discussion and planning needed to develop such a system.

SCOPE

In a broad sense, "numerical data" from the field of ergonomics encompass an enormous amount and variety of quantitative information. Therefore, the initial consideration of an ergonomics data collection must be restricted to critically evaluated data for which there are urgent and widespread needs and an adequately developed measurement methodology. These data—relatively simple measures of human characteristics—provide the building blocks for studying

[1] "Ergonomics" is the study of human capability and psychology in relation to the working environments and the equipment operated by the worker. *McGraw Hill Dictionary of Scientific and Technical Terms.* McGraw Hill, New York, 1974, p. 505. The term is credited to W. Jarzebowski who first used it in an article appearing in *Nature and Industry* in 1846. The roots are Greek: "Ergon" to work and "nomos" meaning natural laws.

human behavior as a complex system. Of particular interest to the National Bureau of Standards are ergonomic data about people as consumers. Such data are needed to make scientifically-based recommendations for designing appliances, furniture, housewares, physical security hardware, and other products.

Our colleagues in other Federal agencies, industry, and the research community who are concerned with consumer products and the human engineering of communications, housing, transportation, space, military, and physical security systems need similar data. Examples include: the body dimensions of the U.S. population—needed for sizing clothing, shoes, protective equipment, furniture, workplaces, and other applications where a close physical match between a person and his environment is important; the sensitivity of the eye and ear at different ages—needed for designing signals, symbols, displays, and printed and other auditory and visual information; threshold values for tolerance to such environmental conditions as temperature, humidity, noise, and ambient illumination; the muscle strength of children, adults and the handicapped—needed to relate the breakaway strength of materials to the forces expected to be applied to levers, controls and other objects.

The data represented by these examples can be expressed as quantitative values of relatively well-defined and easily measured anthropometric and performance characteristics. In other cases, the current state of measurement methodology has not progressed to the point where quantitative characterization is as easily accomplished, e.g., human problem solving, risk-taking, or motivation. Immediate attention, therefore, must be given to the best characterized and readily expressed values of well-defined properties.

BACKGROUND

The notion that peoples' sensory attributes, performance capacities and physical dimensions are related to their ability to function in the world is an ancient one. Folk norms about the size and properties of hand tools, furniture and building design date back before Biblical times. These norms matched the anthropometric properties of the user. Similarly, the design of bow sights and other implements took the visual and other performance capacities of the user into account. Not until much later did an interest develop in actually measuring body dimensions. This interest was in part due to the need for better-fitting body armor.

The first systematic attempts to measure the performance and anthropometric characteristics of large samples of people began in the 19th Century. One of the more notable of these attempts was begun by Sir Francis Galton in 1883.[2] He established a measurement laboratory at the London Health Exposition. In a period of 5 years he amassed detailed, quantitative measurements on the sensory, cognitive and anthropometric capabilities of over 9,000 exposition visitors. Although Galton foresaw the technological applications of these data, not until 1945 was a systematic survey actually made (by Hooton[3]) for a specific technological application. Hooton measured 3,867 adult men and women in Boston and Chicago railroad stations to obtain data for designing railroad seats. However, real interest in the general application of data on human characteristics did not occur until World War II, when dozens of research studies were made on selected samples of military personnel to establish dimensions for uniforms and special clothing and for the characteristics of controls and displays, the reach envelopes for cockpits and tanks, and the properties of the countless other items that required a close physical and performance match at the "man-machine" interface.

Unfortunately, comparisons among or within sets of these data, their aggregation or extrapolation are nearly impossible because individual investigators used different measurement methods to quantify the same characteristics. Attempts were made early in the 20th Century to standardize anthropometric measurement, but to this day insufficient significant progress has been

---

[2]Galton, F. et al. Final report of the anthropometric committee. *Report of the British Association for the Advancement of Science,* 1883, 253-306.

[3]Hooton, E. A., *A Survey in Seating,* Heywood Wakefield, Gardner, Mass., 1945.

made.[4] Furthermore, it is difficult to assess the precision, accuracy or current validity of the data that do exist in light of the effects of improved diets, physical exercise, and other factors on body size, weight, and performance.

Nevertheless, several important current forces generate a mounting pressure for developing comprehensive, critically evaluated ergonomics data. These forces are: the mass markets for consumer products which must be designed to match the characteristics of product users; the national emphasis on the protection of consumers from unsafe and inefficient products; and the skyrocketing costs of research that make it increasingly prohibitive to conduct studies or surveys when results intended for a specific application are not generalizable to other applications. These practical concerns are a stimulus to examine the need for a comprehensive ergonomic data collection system. An additional impetus for the development of a data collection system comes from the Senate passage of the Metric Conversion Bill of 1975 (S. 100). This bill calls for the Federal Government to help plan and coordinate metric conversion in the United States. It is of interest that this bill refers specifically to the possible need for a "study of body sizes and shapes as they are affected by metric conversion."

A single example illustrates the problem created by the absence of a data base. For many years the apparel industry has relied upon trial and error or upon anthropometric data collected in 1939-1940 by the Department of Agriculture to size clothing. In 1973, industry concern over the lack of up-to-date, accurate sizing data led to a meeting on the subject in Washington, DC. At that meeting participants representing 50 leading designers, quality control experts, and officials of commercial, governmental and professional organizations pointed out deficiencies in existing data and the economic consequences of these deficiencies. They highlighted the urgency of obtaining accurate, comprehensive information in formats that would encourage use early in product design.

Following that meeting, the participants sent letters to the Director of the National Bureau of Standards (NBS) expressing their interest in a nationwide anthropometric survey and asking for assistance from NBS. These letters led to a brief pilot study of the feasibility, scope, and costs that such a survey would entail.

After the pilot study was completed, the interested parties were told that the Bureau did not possess the capabilities required to carry out a study of such magnitude and that there was little possibility that critical NBS manpower or funds could be diverted for such a survey. However, the Bureau offered to provide technical assistance if some other vehicle, such as a trade association, could be employed to spear-head the effort.

Since that time the problem has remained unsolved. The Department of Agriculture, which had conducted the 1939-1940 body size survey, is no longer staffed, equipped, or funded to collect the needed data. Although the U.S. Center for Health Statistics at the Department of Health, Education and Welfare is staffed and equipped to conduct representative surveys of the U.S. population, its present mission is concerned with measures that are indicators of health and not with the additional measurements needed for clothing, product, and system design.

Since that time new programs have been initiated at NBS that require access to ergonomics data for designing consumer products, law enforcement equipment, buildings, and environments. Staffing, facilities, and funding have been acquired for these programs. In view of these recent developments, the present and emerging needs of other Federal agencies whose programs involve ergonomic considerations, and the continued need by many sectors of industry, it is appropriate to reconsider the need for critically evaluated ergonomics data and a system for making it available to its many users.

A MODEL SYSTEM

Is there a model for an Ergonomics Data System? In 1963 the Federal Council for Science and Technology asked the National Bureau of Standards (NBS) to assume primary responsibility in

[4] Hrdlička, A. *Practical Anthropometry*, The Wiston Institute of Anatomy and Physiology, Philadelphia, 1952, reprints the "Report of the commission appointed by the Fourteenth International Congress of Anthropometry and Archeology at Geneva (1912), to supplemeot the work commenced by the Thirteenth Congress in the session at Monaco (1906)," translated by W. L. H. Duckworth, the Anthropological Laboratory of the University, New Museums, Cambridge, 1912.

the Federal Government for promoting and coordinating the critical evaluation of numerical data in the physical sciences. The program was envisioned as a decentralized but nationwide effort with funding coming from a number of Federal and private sources, but with NBS being responsible for the overall planning and coordination. When NBS accepted this responsibility for what was called the National Standard Reference Data System (NSRDS), it established an Office of Standard Reference Data to manage the program and for funding projects within NBS and in other Government and university laboratories to perform critical evaluation.

Today, the Office of Standard Reference Data at NBS promotes the compilation of evaluated physical and chemical data; coordinates related work done under the auspices of other Government agencies; establishes criteria for the quality of all products used in the system; develops standards, measurement methodology, and other related activities necessary to assure compatability of all units of the system. In performing these functions, the expertise of NBS in specific substantive areas is also brought to bear, along with NBS' unique competence in measurement methodology and standards development. Guidance to the NBS Office of Standard Reference Data is provided by a series of advisory committees of the National Academies of Science and Engineering.

The selection, evaluation, compilation, publication, and dissemination of existing data from the published literature is performed by data analysis centers throughout the United States. The products of these centers are made available to the public at a nominal cost. In those rare instances when gaps in coverage or quality are identified, NBS may help arrange for necessary research to be done by grants or contracts to colleges and universities. Funding for these efforts comes from several sources: the NBS budget, the budgets of other Federal agencies, industries with interests in specific types of data, and fees from the sale of copyrighted NSRDS publications.

THE FUNCTIONAL REQUIREMENTS OF AN ERGONOMICS DATA COLLECTION

It is apparent from an examination of the NSRDS model that several conditions must be met to achieve a collection of critically evaluated ergonomics data. These include the following at a minimum (table 1):

(1) There must be a community of users with identifiable data needs. These needs must be definable in terms of required measurements, precision, accuracy, and priority.

(2) There must be a governance representative of the user community to establish policy, priorities, and procedures for the system.

(3) There must be a national focal point or secretariat to manage the development of the system and to implement the guidance of its advisory committees.

(4) There must be one or more data analysis centers to interpret, synthesize, evaluate, and repackage data from existing data sources. These centers will contain the subject matter specialists who will produce critical reviews, state-of-the-art monographs, data compilations, and otherwise respond to user inquiries.

(5) There must be public or private research organizations to perform the research where gaps in substantive areas or data quality exist.

(6) Finally, there must be standards for measurement units, measurement procedures, measurement instrumentation, and data presentation.

Because of the magnitude of effort required, it must be assumed that funds for these efforts will be met by cost-sharing among those organizations in the Government and industry that have similar ergonomic data needs. The burden would be too great for any single organization or agency to assume.

CURRENT EFFORTS

In January 1977, the Human Factors Section of the Center for Consumer Product Technology, Institute for Applied Technology at NBS, received funds for a small project to

TABLE 1. *The functional requirements for an ergonomics data collection system*

User community	- Define data needs and determine priorities; specify precision/accuracy/population requirements
Governance	- Set policy, priorities, procedures
Secretariat	- Coordinate and implement policy
Data analysis	- Process, evaluate, and disseminate data
Research organizations	- Obtain missing or more accurate data
Standards	- Develop standard measurement methods, procedures, and instrumentation
Funding	- Support all elements

conduct a 9-month pilot study of the need for and feasibility of establishing a collection of critically evaluated ergonomics data. This study was motivated by the recurring needs of the Center for critically evaluated data on the performance and anthropometric characteristics of human beings—data that could be used in developing consumer products, product safety standards, and informative product labels for consumer guidance at the point of sale. It was recognized that the data required would be of two types: (1) Data unique to a given problem that was so specialized that they would not be used for any other than a single application, and (2) data of a more generic nature that while they have immediate application to a specific situation, could also be used for other consumer product problems or by other persons or organizations for other related problems. It was this second class of data need that prompted the Center to pursue the project that is now underway.

USERS AND USER NEEDS

The first and most important step in the project was to meet with representatives of NBS, other Federal agencies, and industry to identify the extent and nature of needs for ergonomic data. To this end, meetings were held early in 1977 with members of the Mail Order Association (representing such large firms as Sears, Roebuck & Co., J. C. Penney, Montgomery Ward, and Spiegels); members of the apparel industry at its American Apparel Manufacturers Association—Technical Forum III; persons from the Department of Defense, General Services Administration, Defense Nuclear Agency, U.S. Postal Service, and other Federal agencies; and behavioral scientists from other units within NBS.

At these meetings, each group was asked to address the following issues: (a) the needs of its members for ergonomic data, (b) the types of data that are needed, and (c) the interest of its participants in contributing to and using a national ergonomics data system. We anticipate that additional meetings will be held in the future to obtain more detailed information and to help insure that inputs from a spectrum of potential users and contributors have been obtained from the Government, industry, and research communities.

While it is not envisioned that these informal meetings with potential user groups will be definitive, the preliminary findings are helping us to validate the concept of a need and to isolate parameters of interest. The frequency of occurrence of given measurement domains among the

organizations represented will also help provide an initial basis for establishing program priorities, content, and the probable costs of obtaining the information from existing sources or from new research. Based on these preliminary findings, we hope to conduct a more definitive survey of more specific data needs in FY-78.

A REPRESENTATIVE GOVERNANCE

A second focus of the present study will be to devise a set of alternative concepts for a participative governing structure through which the needs and interests of potential user groups can be expressed and appropriate policy guidance can be generated.

A NATIONAL FOCAL POINT

Whereas a governance will be needed to establish policy and priorities for the Ergonomics Data Collection System, a national focal point or secretariat will be necessary to coordinate the program. One potential analog is the NSRDS model in which coordination is performed by the National Bureau of Standards. The Bureau's leadership role in the development of measurement methodology and standards and its mission in the area of consumer product safety and performance are positive factors for suggesting that it serve as an interim or sustaining secretariat for the Ergonomics Data Collection System. Other organizations that merit consideration include the National Science Foundation and the Department of Health, Education and Welfare, existing scientific, technical or trade associations, or a new, not-for-profit organization formed for this purpose. Without further interchange of ideas, it would be premature to identify which of these several alternatives would be most suitable.

DATA ANALYSIS CENTERS

A number of organizations exist in the university and not-for-profit sectors that qualify in terms of mission, staff, capabilities, and facilities to accept data analysis and critical evaluation functions. Some also have the capability to publish and disseminate critically evaluated data and information. It is envisioned that candidate organizations for performing the data analysis function can be selected when specific data needs have been identified.

NEW DATA SOURCES

It is envisioned that there will be the need to conduct one or more large-scale surveys and a number of more specific, limited studies to obtain needed ergonomic data. One of the most obvious of these needs is for a *nationally* representative survey of body dimensions and basic performance characteristics. Although such a survey is undoubtedly a large and costly effort, it may be the only basis on which a number of industry needs can be met. Accordingly, one aspect of the present pilot project will be to examine the sampling, instrumentation, and other requirements for such a survey, with a view to estimating technical feasibility and cost boundaries.

Several organizations in the U.S. are qualified to undertake nationwide surveys or components of surveys. It is not envisioned, therefore, that NBS would itself attempt to conduct the national ergonomic survey. For additional studies leading to data collection on specific data needs, many organizations including NBS, are qualified to undertake specific research.

STANDARDS

One of the shortcomings of current ergonomic survey and research efforts is the lack of adequately defined and accepted standards for measurement, instrumentation, measurement units, and data reporting. Accordingly, in any ergonomic data program a key element will be a community-wide effort to develop these standards. While the standard adoption process is viewed as being a voluntary rather than a mandatory process, NBS could make a major contribution, as it has in the past, to standards development coordination, evaluation, and dissemination.

APPLICATION OF AN ERGONOMICS DATA SYSTEM FOR PHYSICAL SECURITY

Critically-evaluated, quantitative data related to human characteristics, capabilities and limitations, and various aspects of human performance appear to be essential for designing, operating and maintaining the current, complex and sophisticated physical security systems under consideration in many nuclear and non-nuclear applications, whether governmental or industrial in nature. An application of such ergonomics data is described below within the contexts of nuclear weapons and materials for illustrative purposes only. The relevance or generalizability to other contexts and applications should be obvious.

Security personnel, i.e., guards and response forces, are a major component of both nuclear weapon and material physical security. An understanding of their individual and collective characteristics, capabilities and limitations from an ergonomics viewpoint can lead to enhanced physical security. For example, consider the design of control/monitoring rooms for the varied and complex intrusion detection hardware/systems currently available. The performance of personnel given the responsibility for monitoring and responding to alarms and other information input will be improved if the following classes of ergonomics data were made available and utilized early in the design of such facilities:

(1) *Static Anthropometric Data* (body measurements) as related to work space layout (proper location and sizing of display/control panels).

(2) *Dynamic Anthropometric Data* (reach, strength and force characteristics) as related to operating knobs, switches, dials, levers and other controls.

(3) *Human Visual and Auditory Acuity Data* for not only illumination, color coding and other related design requirements, but also for direct visual surveillance of intruders or potential intruders.

(4) *Human Detection, Identification and Recognition Capabilities* as related to the surveillance function.

(5) *Human Vigilance and Information Processing Performance* from the standpoints of information overload and performance decrement.

All of the above provide key input to the formulation of personnel selection and training requirements.

SUMMARY AND CONCLUSIONS

There is presumptive evidence of the need for a system of critically evaluated data related to human characteristics and performance. The need exists at all levels of Government, industry and the research community. The National Standard Reference Data System is one model of such a system. Capabilities currently exist which could be structured to match this model and to carry out the activities required by it. However, before any serious consideration can be given it will be necessary to:

- Survey users and their needs.
- Use this information to further define the content and methods for obtaining the needed data.
- Initiate a serious dialog with interested participants.
- Develop detailed objectives, plans, budgets, schedules, and other mechanisms that will be required to move ahead.

To do all of this will require patience, careful analysis and active participation in the form of personnel time and resources from interested persons and organizations. Let us now start the constructive dialog that will be our first step together.

PANEL SESSION—"SYNTHESIS AND FUTURE DIRECTIONS"

Discussants:

Dr. H. Wallace Sinaiko
Smithsonian Institute

Dr. Preston S. Abbott
Preston Abbott Associates

Dr. Harold P. Van Cott
National Bureau of Standards

Mr. Joel J. Kramer
National Bureau of Standards

Mr. Marvin C. Beasley
Defense Nuclear Agency

DR. SINAIKO: What I would like to do first is run through some of the papers very quickly and give my personal reactions to them and what I think some of their implications are. I hope the speakers, particularly yesterday's speakers, are here because what I have to say is in some cases quite critical of them, and I would like them to have the opportunity to respond.

Mr. Darling had many provocative things to say. His notion of using black-hat penetrators as a means of testing security systems is a very good one. I have been involved in that sort of thing with the FAA's anti-hijacking profiling system. The black-hat notion provides very important reinforcement for a serious problem—the issue of vigilance, which has come up over and over again in the last couple of days. The issue as I see it is how to maintain vigilance for highly critical situations, namely, the detection of an extremely important event which has a terribly low probability of occurrence.

I have some problems with the practicality of Mr. Darling's concept of an idiot-proof, cradle-to-grave security system. Partly, my problem concerns civil liberties, and that's a very important issue that I want to raise separately at the end of my remarks.

I don't share Darling's doomsday views, and I think my reason for this is that, as far as I can tell (taking a citizen's viewpoint rather than a scientist's) I think the U.S. security system has been very effective. At least, I'm not aware of catastrophes or near catastrophes.

I'm concerned about the role of the media. I have some clippings that I've gotten just in the last few days from such widely diverse newspapers as the New Orleans Times, the Boston Globe and the Chicago Tribune, all of which deal with the variations we're talking about here. And I'm concerned that maybe, as a case in point, the Chicago Tribune's article on terrorists gearing up to attack some of the nuclear power generating facilities in Illinois might serve to stimulate that kind of activity. However, I have no evidence to support my concern.

I think Darling's favoring of polygraphy and voice stress analysis poses some problems. I was quite impressed with what Dr. Bevan had to say this morning, at least about voice stress analysis, but I think that Dr. Abbott and Dr. Van Cott are much better qualified to comment on some of these physiological things. I would remind all of you that there are some classic examples of people who have been subject to polygraphy and who have done some pretty horrendous things.

I think there's a need for data. I heard the question that was asked yesterday; it was not answered; it was addressed of Mr. Darling. He was asked to support his assertion that there have been falsely obtained security clearances. I'm sure that's happened in a few cases, but anecdotes are not satisfactory answers to that kind of question. I think we simply have to know whether it is a real

problem or just one of these aberrations that we as a nation are going to have to live with and risk. There was an amusing anecdote in this morning's paper. The White House sent the name of the wrong brother for clearance, and the wrong guy almost got appointed; so it can happen at very high levels.

Mr. Mengel of BDM talked about a classification scheme that doesn't deal with the loner or the disgruntled welfare recipient, the very kind of person that seems to be giving the public so much trouble today. I have some difficulty calling his data base a data base. Incidentally, the term data base tends to be used very loosely, implying a sense of accuracy, precision, or mathematical excellence that generally doesn't exist. What I'm afraid of is that a lot of people we work for are being misled by some of these notions; I hope we can dispel some of them.

Mr. Mengel said that terrorists are not generally suicidal. I would have to question this statement based upon the newspaper articles I have read. There have been some terrorists abroad who have clearly gone into situations where they knew they wouldn't survive and they didn't survive. Also, I still don't really understand why BDM's data base excludes the experiences in Ireland, Israel, and Lebanon.

Dr. Pratt stated, I believe that, by the age of 14 or early adolescence, the average American kid has seen 11,000 murders on TV. Well, I did some quick arithmetic; that would mean, by my calculation, that every day, from the moment that child was born, he/she sees 2.15 murders a day. Is this really credible? These kinds of scare assertions, particularly when they're so patently wrong, tend to diminish the credibility of other things that some of us may have to say.

I thought Dr. Pratt's characterization of the foreign agent and how he operates was good. While I can't vouch for the accuracy of the characterization, intuitively it made a lot of sense to me. I was particularly interested and impressed with her dispelling the myth of the generational conflict, the fact that young dissidents and activists are in fact not so different from their parents, that they share the same values and perpetuate them. I think there's an implication for the security world here, and I'll get to that a little later.

Dr. Pratt stated twice, I believe, that the only reason that an attack hasn't come from foreign agents is that objective conditions haven't been right. I just don't understand this; I would prefer a more parsimonious explanation; perhaps our security system works, and, in spite of whatever the conditions were, people like you and others have prevented those attacks.

I strongly support her closing remarks which urged researchers to go out and talk with the terrorists, particularly those who have been apprehended, as she has done in Vietnam. However, there are always problems in attempting to extrapolate from foreign experience to our own.

To illustrate my point, I spent a year in London and travelled in Europe in the late 60's. There still was a tremendous amount of interest at that time in the John Kennedy assassination. Over and over again, Europeans and other people on both sides of the Iron Curtain asked me whether or not I really believed the findings of the Warren Commission.

I don't think they were really interested in my personal belief, but they wanted to know why Americans accepted the notion that a single assassin could have done anything like that. To them this was just obviously wrong.

In the European tradition, there is a tremendous amount of conspiracy. President De Gaulle had four to six attempts on his life, all by conspirators. So here is the case of a very strong cultural difference. Europeans, in my limited sample, simply didn't believe the fact that an individual, acting alone, could have assassinated the President; they prefer to think of Oswald, or whoever the assassin was, as being part of a larger conspiracy.

Alan Fine's presentation was well-balanced. I thought that his conclusions about the relative unimportance of perpetrator physical attributes, in contrast to the high importance of psychological factors, make a lot of sense. What he didn't say, but implied, was that, as is almost always the case, the psychological problems are the toughest ones to deal with. Dr. Van Cott just illustrated this by indicating how little we really know about human motivation, learning, and cognition. Anybody who purports to be a behavioral scientist, psychologist or sociologist, who tells you he

has answers in all of these areas, should be very carefully evaluated before such pronouncements to the contrary are accepted.

I liked some of the suggestions that Fine made about improving security. His notions of increasing the price of entry and forcing risks made sense to me.

Mr. Kendrick talked about collusion. As he went on with some of his rather eloquent equations, I wanted to retitle his talk "Games Physicists Play." With all respect to him, I think he illustrated best what I've seen over and over again for many years, the typical engineering/operations research approach to behavioral issues.

With all of its eloquence, the modeling approach somehow just never takes account of such things as—and I think Marian Bailey brought this up in one of her questions—the price one pays for these kinds of gatekeeping activities. What about the deleterious effects on productivity or morale? Modelers only rarely recognize that there are people who are being manipulated and rotated within shifts or between shifts.

Turbulence of this sort is very costly in many ways. Those of you who have had military careers or are presently in the military will recognize what I'm talking about. Rotation, whether on a daily basis or on an every-three-year basis, is just terribly expensive not only in terms of getting up to speed, but also in terms of maintaining efficiency and learning new tasks. One of the dangerous things about Mr. Kendrick's proposal is that it would work to destroy individuals' trust in the system, each other and their employers.

A notion was advanced that family members should not be employed in security operations, sort of a nepotism rule to minimize collusion. I'm aware of at least one agency headquartered in this city that has just the opposite rule. That agency makes the assumption that this is cost-effective. Hiring preferences are given to the children of people who have been cleared. Once you've established the loyalty or the security status of an individual, and, in line with what Dr. Pratt said yesterday, if we will accept the fact that generational differences do not really exist, having such a nepotism rule just doesn't make sense.

The response force problem Mr. Galloway dealt with is a very difficult one. Maintaining the morale and alertness of response force members is a serious problem. There are no easy solutions. His suggestion of going to command post exercises and constant alert-type training will help, but is extremely expensive. A great deal can be learned by security people from the military training world; there's a lot of expertise there (some of it is personally represented in this room). More of this expertise should be utilized in the future.

Mr. Galloway and others see a lot more in psychological testing and screening than most bona fide psychologists would lay claim to. Dr. Pratt said yesterday that psychologists and psychiatrists can screen out psychopaths. A bit of caution is urged here; this is not quite as easily done as implied.

As always, I was impressed with the Baileys' work. They presented a number of useful principles and concepts. First, the importance of training the trainers. Incidentally, while the Baileys were talking about animals, they were talking about us and our world as well. Next, their emphasis on the value of observation is very important. When they described animal-machine systems, the Baileys were really describing good human engineering principles-human engineering, not just animal engineering. I don't think that they have to apologize to the traditionalists about whether or not their work is science; it's science and it's good science.

One final thing I would like to say about the work of the people from Animal Behavior Enterprises is that the cost is low. It's interesting to see how much good work can be done by a few bright people with not many resources; I hope some of you who are sponsoring this meeting and work in this area keep this in mind. You don't have to have great electronic cathedrals and multimillion dollar laboratory facilities to do good work. Some of our heavily-invested efforts may be counterproductive, because such efforts force most of us as psychologists or whatever we are to tend more to the electronics than to the behavior we're trying to understand and predict.

I was quite impressed with Dr. Bevan's comments; the area he's working in has great promise. I'm sorry there wasn't time this morning to discuss what he alluded to at the end of his presentation,

the problem of lack of communication. The lack of communication between the polygraphers on the one hand and the physiologists on the other was very delicately put. This gets to an issue I would like to mention in a more general sense; it is the two-culture problem. There's a serious communication problem among what, for simplistic reasons, I'll call the two cultures represented in this room. Whitehead or some other philosopher referred to the simple-minded versus the muddle-headed.

On the one hand, there are the pious scientists—like some of us on this panel. On the other hand, there are the harassed, overworked, overburdened, and sort of hopelessly involved security people. On the scientific side, there's a lot of talent, knowledge, and ability to size things up and to look at problems in a hopefully useful manner.

I think security people, on the other hand, can't afford to wait. They're under the gun; their world consists of a lot of pressure. Unfortunately some of them want instant solutions; they want a magic pill; they want the scientists to tell them how to screen bad guys out and screen good guys in. As I've tried to explain this afternoon, I don't know good ways of doing this.

Since a greater sense of community is needed, I propose that there be more frequent, less formal meetings. I think that it would be useful, for example, if a group met quarterly for a half-day, instead of every year. The reason for this suggestion is that I think there's a need for us to establish trust, confidence, communication and continuity—to begin to understand each other and know who we are. It would be possible to have, but not necessarily on a continuing basis, other kinds of expertise represented that would have been very useful here. For example, I would have liked to have heard somebody with expertise in civil liberties law, because the issue kept coming up over and over again. I'd like to see greater representation and involvement of the intelligence community.

Finally, I've alluded several times to the issue of civil liberties. It seems to me at least that this is the new scapegoat that has emerged in the last two days. Over and over again, I heard people lay their problems at the feet of civil liberties. They said that if we didn't have a Bill of Rights to contend with, the physical security problem would be easy to deal with.

My answer to this is, nonsense! I have some stronger notions. Reflect a moment on the public disclosures about the Army's intelligence programs in which civilians were investigated and dossiers compiled or about the FBI's long surveillance of the Young Socialist League and some of its programs; I'm not aware that these programs were effective. As a consequence, I don't think civil liberties is what's keeping you from doing your job as security officers, and I wish you'd get off that kick.

DR. ABBOTT: We have done work in terrorism, but more on the negotiation end and not on physical security. While I do know a little about the physical security problem, I share Dr. Sinaiko's frustration associated with not knowing the extent of the security problem. I do not deny that people will try to penetrate, but I think it's very hard to sit at a meeting like this and have people give covert glances to one another, or say, "But I can't talk about that." It's difficult to deal with a problem if it must be kept to so few. If we are going to talk about physical security, perhaps we all need higher security clearances, or we need to discuss the problems at a different level.

There have been studies by the intelligence community and in other communities that are terribly relevant to some of the papers presented during the last two days. Such studies were not alluded to, either because of classification level or a lack of knowledge.

There were gaps in several of the presentations, because the presentations were not built on the total literature that exists. This tended to make the program somewhat fragmented. Having an audience that is somewhat fragmented as well, gives me a feeling that we're really not attacking the security problem in a systematic way.

I am concerned also about the systems approach and the data bases. I found very little system orientation. Certainly, the data base phrase has been overused, as Dr. Sinaiko indicated.

In contrast to Dr. Sinaiko's views on the matter, there are contributions to be made by conducting psychological analyses related to terrorism. There has been some excellent work in this area.

Major contributions can be made in at least obtaining a better understanding of certain behavior and behavior under stress. Little of this was related to the attribute discussions.

I would like to know more about how the profiles which were discussed were arrived at; the depth of some of the interviewing techniques; what kind of sampling was employed. Are we taking the word of one interviewee to come up with attributes; what is the extent and depth of the data base(s)?

I wanted to hear Dr. Pratt speak in detail on methodology. There needs to be further work on cultural effects on terrorism. I think she may have inadvertently left the impression that, since that's our only data base, we're shading cultural differences. We can make some horrible mistakes doing this. I think that a lot of good data are available and cultural effects should be stressed more. There are also transnational influences in the training, participation, philosophy, and communications of terrorists. There are differences and we must be careful of them.

We are possibly doing an injustice to the analysis when we refer to loners as "crazies," "banana-heads," "psychopaths" and "sociopaths." This is a very imprecise use of language. If we're going to understand behavior better, I would hope that we could adopt better categorizations or terminology.

If the civil rights issue is a stumbling block, instead of what we have been hearing regarding the ambience and attitudes toward this issue, I suggest we look for other ways around it; there are many. I don't mean by subverting rights. There are other techniques for observation. There are certainly better interview techniques that can yield much more legitimate data.

I was surprised to hear so little concentration on or reference to training. Mr. Galloway may not have left this impression with me purposely, but it seemed as though he indicated that all training possibilities for guard or response forces had been explored. We have some extremely experienced psychologists and trainers who I would like to hear respond to some of these training questions and the adequacy with which training has been considered. While training is not the answer to everything, enough attention was not given to it in yesterday's program.

DR. VAN COTT: I've been associated in the past with military problems in the areas of command and control. As a relative newcomer to the field of physical security, let me make my comments from the point of view of an outsider coming into a field which I've been reading much about, and, perhaps, offer a somewhat different perspective.

It strikes me that the whole field of physical security as a science or a technology is still in a very preliminary stage, not unlike many new sciences or technologies when they first get started. Physical security reminds me of the computer field. At the very beginning, there was little agreement upon terms; there wasn't really a systems approach; the emphasis was on hardware. The word "software" wasn't invented until well after hardware had been developed. There was little in the way of theory, an unevenness of development in various areas, a tendency to concentrate on the engineering aspects, and, because of a lack of a systems and theoretical orientation, a tendency to think in terms of various kinds of components. Certainly, physical security must start somewhere, and it's necessary to start talking about the various elements of a system, but we really don't have a system yet.

With respect to behavioral science contributions, my observations from what I've read and heard at this meeting are that there are some areas with higher payoff than others for applying behavioral science to physical security problems.

Selection and training of defense forces represent high payoff areas. The techniques utilized in animal behavioral research as indicated by the Baileys are also applicable to the training of people. There's a great deal that we know about training technology that's come from the military. We know about vigilance in security operations—there's a great deal of research and a body of information that can be applied. There are human engineering and man-machine interface data and principles related to the interfacing of guards and sensing equipment. There's potential payoff in further development of incident data bases. A great deal needs to be done in this area to be able to codify various categories of incidents. Incidents should be segregated with respect to

culture and the particular individuals involved in the incidents characterized on the basis of various kinds of demographic and other descriptive variables.

There may be a lower payoff in the area of comprehensive profiling of adversary forces. I'm just not sure what we can learn from such efforts, because each incursion may be such a unique event that there may be very few generalizations which can be made about the kinds of individuals that would penetrate secure areas.

I think that there is a conflict of values in the security field, a tendency to either take the position that we've got to come up with a completely secure system (with all the costs that are involved), versus one which faces up to the problems of civil liberties. And along with this, the notion that total security is impossible.

There are some limits to the application of behavioral science. There are some things that it's just not going to do for physical security. Prediction of individual or small group behavior, no matter how much information we have on other individuals or small groups, can only be done in a statistical sense. To the extent that we get good, detailed data on the people that we're dealing with, simple behaviors are obviously more easy to deal with than complex ones. In the field of physical security, particularly with terrorism, we're dealing with extremely complex behaviors which are difficult to characterize in a definitive sense.

I would also like to congratulate the Bailey's on their work. I'm surprised at the low level of Government support that their work has received compared to what would appear to be a high potential payoff, particularly when one thinks of the billions of dollars that have been spent on hardware in this and other areas.

MR. KRAMER: I have a basic problem of not knowing which data to believe in the area of adversary attributes. By way of example, we established for 1977, based upon an almost unanimous agreement in 1976, a secret level of clearance. As a matter of fact, one of the presenters was a previous presenter. Another individual who made a presentation in 1977 was in attendance in 1976 and pretty much insisted upon the need for having a classified forum to foster more worthwhile discussion of adversary attributes.

The presentations I heard provided little, if any, new data. Was our clearance level too low? Was there not enough time to prepare presentations? Or, perhaps, is it because no one really knows any more than has already been conveyed? If the state of the art in adversary attribute modelling and characterization is in fact what it appears to me to be, it may be a waste of time from a behavioral standpoint. Physical security specialists should realize that prediction and prevention may be impossible to achieve, particularly prediction, unless we completely monitor every individual in the world.

I'm now going to turn the discussion over to Marvin Beasley of DNA; without his support, interest and enthusiasm in the behavioral area we wouldn't be here. Marv, where do we go from here as far as DNA is concerned, and what are your reactions to what you've heard?

MR. BEASLEY: I enjoyed the presentations. I hate to differ with the other learned panel members, but I found a great deal of competence reflected in the papers. Let me say in all candor that, if I had a certain size budget, I would certainly invest some of it on some of the thoughts, ideas and identified needs for further research that I've heard expressed by our speakers. Being a professional security man, I would like to explain to Dr. Van Cott that we haven't yet claimed to reach his level of science and technology; we're still calling physical security an art. Maybe we should be calling it modern art, or perhaps an even more fitting adjective would be grotesque.

We have come a long way since 1974 when some of us met at NBS in an attempt to determine what to do about the people factor(s) in physical security. By 1975, the number had increased to seventeen. Last year we invited 50 people to the first symposium and some 70 to 80 people showed up. With the recent gains we've made, we haven't done too badly, considering the competition of other meetings scheduled at the same time.

We did structure this symposium somewhat loosely, extending our invitations to a rather broad segment of the community that we like to consider as those people concerned with security. A

large part of our audience has been performers from industry and Government—that is, people who are contributing either to the problem, its solution or both. We have also had a few customers, the people who earnestly are seeking the answers, the people who really need some help and guidance. I'd like to list myself among that group.

But then there was a third group here; we call them interpreters. These include program officers who somehow manage to get their hands on some money and try to find out what the customer needs and what the performer can do. The interpreters attempt to put the needs and capabilities together. I'd like the audience to think of the members of this panel as interpreters. That's what we were trying to do.

I appreciate the contributions made by each one of them. I did enjoy their candor, and I think that's what we're here for. I would like to know from the audience whether or not tax dollars should be spent to continue having annual symposia. I do like the suggestion of having more frequent meetings and that we also make public as much of this information as is in the public good.

From a number of the questions asked and some side discussions that went on in the hall, I have identified a number of individuals who have some rather novel approaches to the question raised. If you think you might have an approach to answer some of the questions raised, (if you think you might have an identifiable research project that is worthy of consideration), I will guarantee that you will have a friendly ear to listen to what you have to say. I'd like to now return the discussion to our chairman, Dr. Sinaiko, for your reactions or questions and comments from the floor.

MR. RAY MOORE: I recall a town called Jericho that had some walls around it. What were they for, if not physical security? What about all those castles in medieval Europe? They had moats around them. Weren't they for physical security? What about those suits of armor? Wasn't this all physical security? I think physical security is something the human race has been concerned with for most of recorded history. We're still learning; I don't think it's something new.

Comment: The terrorist is a very potent force that we can't afford to ignore. I was on the first task force that the FAA had to develop the profile of the skyjacker. I thought this effort was relatively successful. I can't see why terrorist profiling, at least in a limited sense, would not be successful.

DR. SINAIKO: I'm not speaking for Dr. John Dailey of the FAA, but I think what he did was very imaginative, innovative, and useful. However, so much was happening in the world at the time—the peak of the airline hijacking in 1970, with the Middle Eastern episode in particular—and so many frantic things were tried by the Government, the Sky Marshall program for one, the mandatory use of magnetometers, and now x-ray surveillance. It's really, therefore, very difficult for me or anybody to say that the Dailey and Pickrel work was specifically what turned the skyjacking situation around. We simply don't know whether the change was due to changing politics, a change in the nature of the threat, or other different events. I'm simply saying this to mitigate the difficulty and sometimes the disappointment that we as scientists have of knowing whether what we've done made any difference, when so much else happened.

DR. BILL McCLELLAND: I have a constructive suggestion for the Program Committee, that there be a somewhat more refined concentration of focus if there is to be another session of this sort. This may mean a smaller group or much smaller or more restricted area of interest. There were enough topics presented (I don't know about content). In the future, you could have one or two sub-sessions which would integrate the findings of diverse research in each topical area.

MR. KRAMER: In 1976 we concentrated on one particular area. The consensus at the conclusion of the first symposium was to broaden the scope for the 1977 symposium. But your comment is well taken. The issue is simply where to draw the line in terms of limited versus expanded scope. Each has its advantages and disadvantages.

Comment: I appreciated the comments of the panel and think there's a real need, in any meeting like this, to have criticism on papers. However, I perceive from many of the comments made that there needs to be some smaller group discussion(s) among the people who are in the physical

security business, the people who are the managers of the resources and the people in the behavioral sciences area in order for each to fully understand the problems that the others have. We too frequently start with the assumption that we all start out the same, and that's not always valid.

It seems to me that the physical security business essentially involves risk management and analysis. During any given day, month or week, there will be various risks; these risks have to be perceived on a daily basis. We have to manage resources to minimize these risks.

One of the problems we face every day is aberrent behavior, both inside and outside. This is one of the risks that has to be managed. So from that point of view, and supporting what Ray Moore said about all the moats and all the castles, it's a battle for survival and for the continuation of what the organization is supposed to be doing; we have to minimize all risks. This is the business of physical security.

DR. ROBERT MACKIE: You've said some things that I heartily agree with, and most of what I was going to say. This is my second year here. Last year I gave a paper on vigilance, thinking that since physical security involves surveillance systems, vigilance must be important. I still think vigilance is important, but what I feel I lack is the operational managers' side of the problem. What is their day-to-day problem as they see it? I don't think any behavioral scientist is going to make much of a contribution until that day-to-day operation is understood.

I find it curious that we're speculating at this point about whether or not the airplane anti-hijacking program has been successful, because I'm sure that system is producing data every day which will tell us. There must be data on the number of positive idents; there must be false ident information.

I asked the question yesterday about whether anybody was preparing a data bank on the successes of physical security systems. I hope somebody is, because I suspect that a lot of the people are doing the job very well, but we just don't yet have any data.

Comment: I appreciated the panel's wrap-up. It brought into perspective a lot of conceptions and pains I've had over the last couple of days. In a sense, I'm an observer who's becoming involved.

With respect to the need for achieving a greater sense of community, I got the feeling that there's a certain amount of dogmatism and narrow-mindedness associated with physical security among vendors, contractors, bureaucrats, and consumers. I thought there was a certain degree of unnecessary antagonism, both formally in terms of the presentations and in the halls. I got the impression that there are many people here who feel they have the answers to many or all of the problems, whatever they may be. If we're going to have a greater sense of community, perhaps we could have more one-on-one informal meetings in the future. Coupled with this is the workshop concept, where I as a bureaucrat get with the behavioral scientists in a group interaction involving 10 to 15 people. We could include some engineers, professors, or academicians and get at interpersonal relationships, share ideas and be more candid. In summary, I thought that the symposium was very beneficial and future sessions can be even more productive.

LIST OF ATTENDEES

Mr. Edward A. Abbott
Naval Research Lab.
Code 4171E
Washington, DC 20375

Dr. Preston S. Abbott
Abbott Associates, Inc.
300 N. Washington Street
Alexandria, VA 22314

Mr. Kenneth Adams
Sandia Laboratories
Div. 1758
P.O. Box 5800
Albuquerque, NM 87115

Mr. Ward A. Albro
Department of the Army
USA/IMDSO/EWL
Bldg. 4524D
Fort Meade, MD 20755

Mr. Francis E. Armbruster
Hudson Institute, Inc.
Quaker Ridge Road
Croton-on-Hudson, NY 10520

Dr. Marvin C. Atkins
DDST
Defense Nuclear Agency
Washington, DC 20305

Dr. Marian Breland Bailey
Animal Behavior Enterprises, Inc.
4800 Albert Pike
Hot Springs Nat'l Park, AR 71901

Mr. Robert E. Bailey
Animal Behavior Enterprises, Inc.
4800 Albert Pike
Hot Springs Nat'l Park, AR 71901

Mr. Louis A. C. Barbarek
IIT Research Institute
10 West 35th Street
Chicago, IL 60616

Mr. Robert L. Barnard
U.S. Army MERADCOM
Attn: DRXFB-X
Counter Det. Div.
Ft. Belvoir, VA 22060

Mr. Marvin C. Beasley
NSSO
Defense Nuclear Agency
Washington, DC 20305

Ms. Louise E. G. Becker
Congressional Research Service
The Library of Congress
Washington, DC 20540

Dr. Warren W. Berning
Stanford Research Institute
1611 N. Kent Street
Arlington, VA 22209

Dr. Thomas E. Bevan
Science Applications, Inc.
1911 N. Fort Myer Drive
Arlington, VA 22209

Mr. Richard F. Blackmon
U.S. Nuclear Regulatory Commission
Mail Stop EW 359
Washington, DC 20555

Mr. Rexford G. Booth
Department of the Army
U.S. Army MERADCOM
Laboratory 7000
Fort Belvoir, VA 22060

Mr. Robert J. Bosco
Department of the Navy
(Code 6161)
Naval Ship Engineering Ctr.
Washington, DC 20360

Mr. Stephen E. Brucker
TRW Systems
2425 Alamo Ave., SE
Albuquerque, NM 87106

Mr. Ralph W. Busch
Honeywell Information Systems
7900 Westpark Drive
McLean, VA 22101

Charles J. Bushey, Maj, USA
Defense Intelligence Agency (RCI-1)
Washington, DC

Winston G. Campbell, Maj., USA
U.S. Army Nuclear Agency
Bldg. 2073, North Area
Fort Belvoir, VA 22060

Mr. Robert Carpenter
National Bureau of Standards
Technology Bldg., Room A219
Washington, DC 20234

Mr. Donald F. Coffey
National Security Agency
Ft. George G. Meade, MD 20755

Mr. William T. Conner
National Security Agency
Office of Security
Ft. George G. Meade, MD 20755

Inspector Douglas A. Cooper
Royal Canadian Mounted Police
"P" Directorate, Vedic Bldg.
H.Q. Division
Ottawa, Ontario, Canada

Mr. Henry B. Cranford
Armed Forces Radiobiology Research Inst.
Bethesda, MD 20014

Mr. Aloysius D. Dady
Honeywell, Inc.
7900 Westpark Drive
McLean, VA 22101

Mr. John M. Dailey
U.S. ERDA
Division of Safeguards & Security
Washington, DC 20545

Mr. A. Barry Dalinsky
U.S. ERDA
Office of the Asst. Admin. for
National Security A-330
Washington, DC 20545

Mr. Don D. Darling
Don D. Darling & Associates Consultants
Box 216
El Segundo, CA 90245

Mr. John J. Davidson
U.S. Nuclear Regulatory Commission
SGCP
Washington, DC 20555

Mr. Charles P. Demos
U.S. Nuclear Regulatory Commission
Division of Safeguards T & E
Washington, DC 20555

Mr. Jacob J. Diamond
National Bureau of Standards
Physics Bldg., Room B150
Washington, DC 20234

Quensel K. Diamond, LCD USN
NSSO
Defense Nuclear Agency
Washington, DC 20305

Bruce Dipiftrantonio, Sgt., USA
AFFRI/Security
Bethesda, MD 20014

H. M. Dixon, Col, USA
ODDREE Rm. 3D1028
Pentagon
Washington, DC 20301

Mr. Ronald C. Dobbyn
National Bureau of Standards
Materials Bldg., Room B120
Washington, DC 20234

Mr. Clarence J. Douglas, Jr.
Decisions and Designs, Inc.
Suite 100, 7900 Westpark Dr.
McLean, VA 22101

Mr. Lawrence K. Eliason
National Bureau of Standards
Physics Bldg., Room B150
Washington, DC 20234

Mr. Warner A. Eliot
The Mitre Corporation
1820 Dolly Madison Blvd.
McLean, VA 22101

Mr. John Ewashko
Canada's Atomic Energy Control
Board
P. O. Box 1046
Ottawa, Ontario
Canada K1P 5S9

Dr. John Fechter
National Bureau of Standards
Metrology Bldg., Room A353
Washington, DC 20234

Dr. Craig Fields
Defense Advanced Research Projects
Agency
Washington, DC 20301

Mr. Allan M. Fine
Sandia Laboratories Div. 1758
P. O. Box 5800
Albuquerque, NM 87115

Mr. Brian H. Finley
Sandia Laboratories
Org. 1222
Albuquerque, NM 87115

Mr. Stephen L. Galloway
Operational Systems, Inc.
Suite 201
1600 Wilson Blvd.
Arlington, VA 22029

Mr. Richard L. Goheen
General Services Administration
18th & F Streets, NW
Washington, DC 20405

Mr. Karl Goodwin
National Bureau of Standards
Rad. Physics Bldg., Room C229
Washington, DC 20234

Mr. Robert Griner
Tracor, Inc.
1600 Wilson Blvd.
Arlington, VA 22209

Mr. Brian S. Gunderson
The BDM Corporation
7915 Jones Branch Dr.
McLean, VA 22101

Mr. John Haben
U.S. NSWC/WOL
Washington, DC 20350

Mr. Ralph E. Hannan
Raytheon Service Co.
Spenser Laboratory
#2 Wayside Rd.
Burlington, MA 01803

Mr. Alfred J. Hartzler
U.S. Arms Control and
Disarmament Agency
Washington, DC 20451

Dr. John E. Hennessey
U.S. ERDA
Washington, DC 20545

Mr. Ronald Henry
Naval Weapons Support Center
Crane, IN 47522

Ms. Cheryl L. Herrin
System Planning Corp.
1500 Wilson Blvd.
Arlington, VA 22209

Mr. John W. Hockert
U.S. Nuclear Regulatory Commission
Mail Stop 881-SS
Washington, DC 20555

Mr. William H. Immerman
U.S. Nuclear Regulatory Commission
Division, Safeguards, Fuel Cycle, &
Environment Research
Mail Stop 1130-SS
Washington, DC 20555

Mr. Evert S. Johnson
Defense Logistics Agency
Alexandria, VA 22314

Mr. James L. Johnson
Raytheon Service Co.
Spenser Laboratory
#2 Wayside Dr.
Burlington, MA 01803

Mr. Harvey B. Jones, Jr.
U.S. Nuclear Regulatory Commission
Mail Stop 881-SS
Washington, DC 20555

Mr. Philip A. Karber
The BDM Corporation
7915 Jones Branch Dr.
McLean, VA 22101

Dr. Hugh Kendrick
Department of Energy
Mail Stop G 434
Washington, DC 20585

Mr. Alfred L. Koenig
National Bureau of Standards
Technology Building, Room A219
Washington, DC 20234

Mr. Joel Kramer
National Bureau of Standards
Metrology Bldg., Room A359
Washington, DC 20234

Dr. Herbert B. Leedy
Department of Army
U.S. Army Military Personnel Ctr.
Alexandria, VA 22332

Mr. Justin T. Long
U.S. Nuclear Regulatory Commission
Mail Stop 881-SS
Washington, DC 20555

Dr. Robert R. Mackie
Human Factors Research
6780 Cortona
Goleta, CA 93017

Mr. Thomas B. Mancinelli
DIA
USA Mil Pers Ctr.
Alexandria, VA 22332

Theodore W. Manduca, CDR, USN
Defense Nuclear Agency
Washington, DC 20305

Mr. Frank Martin
U.S. ERDA
Washington, DC 20545

Mr. Edward E. Mayer
The BDM Corporation
7915 Jones Branch Dr.
McLean, VA 22101

Dr. William A. McClelland
Human Resources Research Organization
300 North Washington Street
Alexandria, VA 22314

James T. McDaniel, Lt Col, USAF
Code NSSO
Defense Nuclear Agency
Washington, DC 20305

Ms. Mary J. McGuinness
U.S. Nuclear Regulatory Commission
Mail Stop 881-SS
Silver Spring, MD 20555

Mr. R. W. Mengel
The BDM Corporation
7915 Jones Branch Dr.
McLean, VA 22101

Mr. Edward Mickolus
Office of Regional & Political
Analysis, CIA
Washington, DC 20505

Mr. John J. Miller
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Mr. Don W. Minium
OACSI, DA
Washington, DC 20301

Dr. Bert Mogin
Stanford Research Institute
1611 No. Kent Street
Arlington, VA 22209

Mr. Patrick H. Moore
Armed Forces Radiobiological
Research Institute
Bethesda, MD 20014

Mr. Raymond Moore
National Bureau of Standards
Technology Bldg., Room A217
Washington, DC 20234

Mr. David C. Morrison
Navelex HQ
Attn: PME 121-3
Washington, DC 20360

Dr. Robert K. Mullen
U.S. Nuclear Regulatory Commission
Mail Stop 881-SS
Washington, DC 20555

Mr. Patrick J. Murphy
IOSD, Inscom, Rm. 1J073
Forrestal Bldg.
1000 Independence Ave., S.W.
Washington, DC 20314

Thomas F. Niedbala, CDR, USN
Special Panel #3-Room 1132
Navy Special Discharge Review Board
Ballston Towers No 2
801 N. Randolph St.
Arlington, VA 22203

Mr. Thomas P. Noe
CIA
Washington, DC 20505

Mr. Raymond V. Nolan
U.S. Army MERADCOM
Attn: DRXFB-X
Ft. Belvoir, VA 22060

Mr. Robert W. Oliver
Universal Systems, Inc.
2341 Jefferson Davis Highway
Arlington, VA 22202

Louis Okyen, Col, USA
OAIS
Defense Nuclear Agency
Washington, DC 20305

Mr. Lawrence R. Paggeot
Motorola, Inc.
P. O. Box 8788
Baltimore-Wash. Int'l Airport, MD 20240

Mr. Robert W. Payton
Motorola, Inc.
P. O. Box 8788
Baltimore-Wash. Int'l Airport, MD 20240

Mr. Kenneth A. Plant
Science Applications, Inc.
1911 N. Ft. Meyer Drive
Arlington, VA 22209

Mr. James E. Plummer
Armed Forces Radiobiological
Research Institute
Bethesda, MD 20014

Dr. Jane Pratt
Mitre/Metrek
Westgate Research Park
McLean, VA 22101

Dr. Tawfik Raby
National Bureau of Standards
Reactor Bldg., Room A148
Washington, DC 20234

Ms. Linnea Raine
DIBA/IWG
Room 3814-B DOC
Washington, DC 20230

Robert R. Reddick, Maj, USA
USANA
Ft. Belvoir, VA 22213

Donald R. Richards, LTC, USA
NSSO
Defense Nuclear Agency
Washington, DC 20305

Kenneth W. Robinson, Maj, USA
HQ USAINTA/MII-OSOP
Ft. Meade, MD 20755

John W. Ross, Jr., LTC, USA
Defense Logistics Agency (DLA-T)
Cameron Station
Alexandria, VA 22314

Mr. Jerry A. Sawyer
Science Applications, Inc.
8400 West Park Drive
McLean, VA 22101

Mr. Hans B. Schecter
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Mr. John C. Schleter
National Bureau of Standards
Radiation Physics Bldg., Room C229
Washington, DC 20234

Mr. Eric D. Shaw
CACI, Inc.
1815 Ft. Meyer Dr.
Arlington, VA 22209

Mr. Edgar L. Shriver
Kinton Inc.
104 Prince St.
Alexandria, VA 22314

Mr. Morton D. Sims
Institute for Defense Analyses
400 Army-Navy Drive
Arlington, VA 22202

Dr. H. Wallace Sinaiko
Smithsonian Institute
Washington, DC 20560

Michael Skotzko, LTC, USA
HQ USAINTA
Ft. Meade, MD 20014

Ronald H. Smiley, LTC, USA
OAPO
Defense Nuclear Agency
Washington, DC 20305

Mr. Odel F. Smith
U.S. Nuclear Regulatory Commission
Physical Security Licensing Branch
Washington, DC 20555

Mr. Lewis C. Solem
U.S. Nuclear Regulatory Commission
Office of Standards Development
Washington, DC 20555

Daryl K. Solomonson, CPT, USA
NSSO
Defense Nuclear Agency
Washington, DC 20305

Dr. Carl Sontz
Tracor Sciences and Systems
P. O. Box 2572
EADS Station
Arlington, VA 22202

Mr. Gordon N. Spies
U.S. Nuclear Regulatory Commission
Mail Stop 881-SS
Washington, DC 20555

Mr. Milton E. Stevens
OALG
Defense Nuclear Agency
Washington, DC 20305

Mr. John B. Stewart
Nuclear Regulatory Commission
Washington, DC 20555

Dr. Lawayne Stromberg, CPT, USN
Commander, Armed Forces Radiobiological
Research Institute
Bethesda, MD 20014

Dr. Herbert Susskind
ERDA, Brookhaven
Brookhaven National Lab.
Upton, NY 11973

Mr. Robert P. Teetz
Department of the Army

Mr. John P. Thomas
Hudson Institute, Inc.
Quaker Ridge Road
Croton-on-Hudson, NY 10520

Mr. Gerald K. Tomlin
U.S. Nuclear Regulatory Commission
Contingency Planning Branch
Washington, DC 20555

Mr. James Torrence
National Bureau of Standards
Reactor Bldg., Room 137
Washington, DC 20234

Mr. Joseph F. Trainor
Security Section Rm. 6531
Department of Justice
Washington, DC 20530

Mr. Marshall J. Treado
National Bureau of Standards
Physics Bldg., Room B150
Washington, DC 20234

Mr. Amado A. Trujillo
Sandia Laboratories
Albuquerque, NM 87115

Dr. Harold Van Cott
National Bureau of Standards
Technology Bldg., Room A127
Washington, DC 20234

Mr. William J. Ward
U.S. Nuclear Regulatory Commission
Office of Inspection & Enforcement
Washington, DC 20555

Dr. Stanley I. Warshaw
National Bureau of Standards
Center for Consumer Product Technology
Polymers Bldg., Room A355
Washington, DC 20234

Mr. John R. Williams
Motorola, Inc.
4710 Auth Place, S.E.
Suite 350
Washington, DC 20023

Mr. Rudolph Williams
National Bureau of Standards
Metrology Bldg., Room A359
Washington, DC 20234

Mr. James F. Wimpey
Science Application Inc.
8400 West Park Drive
McLean, VA 22101

Mr. Casper L. Woodbridge
The Mitre Corporation
1820 Dolly Madison Blvd.
McLean, VA 22101

Mr. C. Dennis Wylie
Human Factors Research
6780 Cortona
Goleta, CA 93017

Dr. H. Thomas Yolken
National Bureau of Standards
Physics Bldg., Room A329
Washington, DC 20234

Mr. Robert W. Young
Armed Forces Radiobiological
Research Institute
Behavioral Sciences Dept.
Bethesda, MD 20014

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-538)

☆ U. S. GOVERNMENT PRINTING OFFICE : 1978 O - 258-795

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

SPECIAL FOURTH-CLASS RATE
BOOK