NBS Special
Publication
480-38

The Role of Behavioral Science in Physical Security

Proceedings of the Third Annual Symposium, May 2–4, 1978

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
480-38

The Role of Behavioral Science in Physical Security

Proceedings of the Third Annual Symposium, May 2–4, 1978

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 Nuclear Surety 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.

U.S. DEPARTMENT OF COMMERCE,
Luther H. Hodges, Jr., *Under Secretary*
Jordan J. Baruch, *Assistant Secretary for Science and Technology*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

Issued DECEMBER 1979

Library of Congress Catalog Number: 79-600211

National Bureau of Standards
Special Publication 480-38
Nat. Bur. Stand. (U.S.), Spec. Publ. 480-38; 110 pages
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1979

For sale by the Superintendent of Documents,
U.S. Government Printing Office, Washington, D.C. 20402
(Order by Stock No. 003–003–02149–1; Price $4.25)
(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 third of a series, held on May 2-4, 1978, at the Hospitality House Motor Inn, Arlington, Virginia. The purpose of the symposium was to continue to define the contributions that behavioral science can make to the enhancement of all aspects of physical security systems. In response to the desire of those who attended the first two symposiums, four structured workshops were held; each co-chaired by a physical security specialist and a behavioral scientist conversant with the individual workshop topic.

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 Nuclear Security Directorate of the Defense Nuclear Agency, and attracted approximately 155 attendees from government and industry.

Mr. John Donaldson, on behalf of the Director of the National Bureau of Standards National Engineering Laboratory welcomed the attendees and introduced Vice Admiral Robert R. Monroe, the Director of DNA. The keynote speaker, Dr. Brian Jenkins of the Rand Corporation, expanded upon Admiral Monroe's concern for the threat to nuclear weapons posed by potential adversaries and terrorist groups, and the critical need to better understand human behavior, whether response force or adversary. Both Admiral Monroe and Dr. Jenkins charged the participants to explore innovative approaches and research objectives that would enhance all aspects of physical security systems and would improve the effectiveness of response force personnel. The attendees responded to the challenge through active participation and thought provoking discussions in the workshops; identifying numerous meaningful behavioral research studies that hold the promise of solving recognized problems in physical security.

The editor wishes to acknowledge the cooperation of the staff of the Defense Nuclear Agency, particularly Mr. Marvin C. Beasley and LTC Donald L. Richards. Special appreciation is extended to Col. Charles R. Linton, Director, Nuclear Surety, DNA and Colonel Herbert M. Dixon, Chairman, Physical Security Equipment Action Group, USDRE, for their participation in the panel discussion on new research thrusts as well as the program advisory 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, Nuclear Regulatory Commission; Jack Hennessey, Department of Energy; Daryl K. Solmonson, DNA; Dr. Harold P. Van Cott, and Dr. John V. Fechter, NBS Consumer Sciences Division.

Joel Kramer
Editor

ABSTRACT

This document contains the proceedings of the third annual symposium on, "The Role of Behavioral Science in Physical Security," held in May 1978. The symposium provided a forum for the exchange of information between specialists in physical security and behavioral science through the presentation of eight papers and four structural workshops: Human Sensory Capabilities/Limitations; Human Engineering of the Workplace; Human Motivation, Attitudes, Error/Reliability; Personnel Selection, Placement, Training. The symposium concluded with a summary and synthesis of the results of the workshops and a panel discussion on new research thrusts.

Key words: Adversary characteristics; animal research; behavioral science; biosensors; computer analysis; ergonomics; human engineering; human factors; human motivation; human reliability; personnel selection; physical security; physiological psychology; sensory capability; terrorism; threat analysis; training.

CONTENTS

BIOSENSOR FOR ASSESSMENT OF DEFENDER PERFORMANCE CAPABILITY

Dr. Thomas E. Bevan

Science Applications, Inc., Arlington, Virginia 22209

SUMMARY

A need exists for physiological assessment of defender performance capability. Security guards must maintain high levels of vigilance, in spite of long hours and extremely infrequent intrusion attempts. Physiological changes have been shown to occur during periods of decreased vigilance. Physiological monitoring of these changes could be used to diagnose conditions which contribute to vigilance decrements, and provide early warning of these decrements. Monitoring could also be used to detect when guards are out-of-action—a "physiological deadman" function.

Heretofore, on-the-job physiological monitoring has not been possible due to the cumbersome equipment necessary to transduce, amplify, record or analyze physiological signals. But with the advent of microprocessor technology, lightweight, highly reliable monitoring systems have been constructed and utilized for medical monitoring. The paper describes the state-of-the-art in ambulatory monitoring devices beginning with the Holter cardiac monitor.

This paper also describes two related devices which can be developed for security applications. The first device, a physiological cassette recorder, can be constructed from off-the-shelf components and can be used to diagnose conditions leading to decreased vigilance. The second device, a physiological analysis system, must be prototyped and tested. It consists of a lightweight, physiological transducer/microprocessor system which can be used for on-line, on-the-job monitoring. The cassette recorder will be used to develop the software algorithms used in the analysis system as well as to personalize the analysis system. Both hardware and software components of these devices are presented.

SAI has proposed to several government agencies that a research and development effort be started to utilize state-of-the-art physiological monitoring devices for various applications. EPA has offered to cost-share an effort to apply this technology to the problem of detecting physiological exposure to toxic chemicals. The paper describes the proposed R&D program and indicates the direct applicability of the program to security applications.

INTRODUCTION

In previous symposia, several problems relating to defender performance capability were discussed which may be addressed by the application of physiological monitoring devices. These are summarized in table 1. In last year's symposium these applications were described along with the physiological measures which reflect behavioral performance capability. This presentation gives a brief description of some of the physiological monitoring technology which presently exists or which can be developed, given existing electronic technology.

In particular, two devices will be described—one which is off-the-shelf hardware, the other which could be easily prototyped for physiological assessment. The first device is a lightweight physiological cassette recorder of which several versions are commercially available. The second device is an on-line analysis system which can be prototyped and developed, given the advent of today's microprocessor technology. The cassette recorder can be used to obtain physiological measurements in the work environment for diagnostic and research purposes. The on-line analysis system is primarily intended for day-to-day use as a device for detecting changes in the physiological state.

TABLE 1. *Proposed application of physiological assessment techniques*

Physiological Assessment of Defender Performance Capability

Problem	Application
Maintain vigilance information overload	On-the-job physiological monitoring of information processing load (EEG, EKG)
Assessment of exertion during penetration exercises	Monitoring of physiological correlates of physical workload (EKG)
Detection of guard out-of-action	Physiological "Deadman" (EEG, EKG)
Duress alarm	Detection of voluntary eye movement patterns to trigger alarm (EOG)
Exposure to toxic substances	Detection of abnormal physiological states (EEG, EKG)

STATE-OF-THE-ART IN AMBULATORY MONITORING

As shown in tables 2 and 3, there are both clinical (medical) and military/industrial applications to be considered in describing the state-of-the-art in ambulatory monitoring.

Ambulatory monitoring really began with the Holter [1][1] cardiac monitor which was developed to detect cardiac arrhythmias outside of the clinic. Improvements in this cassette recording system have made this type of monitoring a common technique. The same type of monitoring system was applied with limited success to blood pressure measurement by Pickering [2]. More recently, a cassette recorder for EEG (electroencephalogram) was developed by Ives and Woods [3]. Penry [4] developed a type of EEG recording system that involved analog to digital conversion before recording.

Several military/industrial applications of ambulatory monitoring have been made to on-the-job problems. Sem-Jacobson has performed electrophysiological recording of EEG and EKG for a variety of job functions and environments. In doing so, he developed a Vesta electrode for transducing heartrate from a chair cushion. NASA has performed physiological monitoring of astronauts on most missions and thus helped to develop electrode technology. However, they have had problems analyzing the huge volume of data which has been generated.

TABLE 2. *Clinical application of ambulatory monitoring*

State-of-the-Art Physiological Monitoring in the Field

Clinical Applications

- Holter - EKG
  - Medilog
  - Arrhythmia Detection Circuits
  - Digital Processing
- Pickering - Blood Pressure
- Ives and Woods - EEG
  - Analog Recording
- Penry - EEG
  - Digital Recording

[1] Figures in brackets indicate literature references at the end of this paper.

TABLE 3. *Industrial/military application of ambulatory monitoring*

State-of-the-Art Physiological Monitoring in the Field

Industrial/Military Applications
Sem-Jacobson - Vesla Electrode
North Sea Divers - EEG, EKG
Military Commanders - EEG
Aircraft Pilots - EEG
Sealab - EEG, EKG
Physiological "Deadman"
NASA
Data Reduction Problems
Electrode Technology

BIOSENSOR COMPONENTS

Before discussing the two biosensor configurations, cassette recorder and online analyzer, we will discuss the system components listed in table 4 since each configuration consists of two combinations of these modules. It should be noted that electrode technology has been stimulated from NASA programs and there does exist good quality, comfortable electrodes which are reusable (Beckman) or disposable (Cardiotronics). Although preamplification can be accomplished by electronics mounted on the electrode, for most applications it is not necessary. Low-voice (electrical) wire can improve signal quality by reducing movement artifact.

The core of an electrophysiological recording system is amplification of the signal from the micro-or millivolt ranges to the volts range. Four-channel amplification is currently built into off-the-shelf cassette recording systems. After amplification, microprocessor-based on-line analysis systems can be used to detect changes in physiological measures. The microprocessor system can also be programmed for a decision algorithm which might involve several physiological measures. This algorithm would determine when an auditory or radio-telemetry alarm is appropriate.

TABLE 4. *Biosensor components*

Electrodes
Beckman, Cardiotronics, NASA
Preamplifiers
Low-Noise Wire
Amplifier
4-channel
Analysis
Activation Measure Chip
FFT Microprocessors
Microprocessors - ROM and Custom-Made
Decision Algorithm
Microprocessor
Alarms
Auditory
Telemetry

TWO BIOSENSOR CONFIGURATIONS

A diagram for the two biosensor configurations is provided in figure 1. The cassette recorder device involves at least two electrodes, preamplification, amplification and recording the signal on tape. Such a configuration is exemplified by the MEDILOG recorder system. The on-line analysis system involves a microprocessor module to analyze the physiological data. Several physiological statistics could be generated by such a module.

Figure 2 shows a preliminary configuration of the hardware for an on-line analysis system. After amplification, the physiological signals can be analyzed directly by fast fourier transform processing or converted to digital form. Several statistics could be generated by such a system depending on the physiological measure: activation measure (EEG), interbeat interval (EKG), spectral characteristics (EEG, EKG, EOG) and frequency of response (EKG, EDR, EOG). The activation measure is a simple statistic comparing signal frequency with amplitude. The microprocessor could be supported by programmable read-only memory for statistic generation or decision algorithm processing. The microprocessor could trigger auditory or telemetry alarms or alerts.

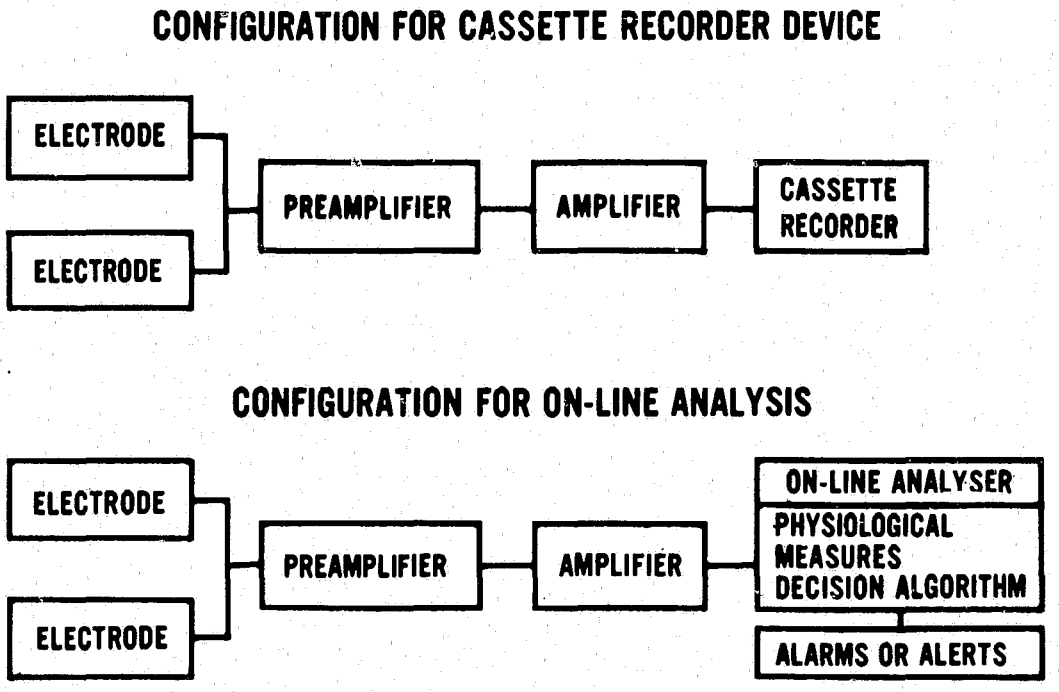

FIGURE 1. *Design configurations for biosensor devices.*

PRELIMINARY CONFIGURATION FOR ON-LINE ANALYSIS SYSTEM

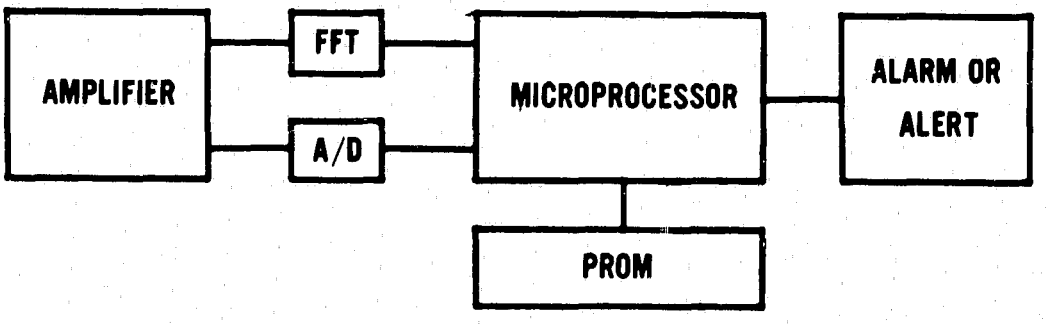

FIGURE 2. *Preliminary on-line analyzer configuration.*

SAI PROGRAM

SAI has planned an R&D program for developing both configurations of the biosensor as shown in table 5. The construction of a prototype recording system requires only minor changes to existing off-the-shelf equipment. A research program is needed to develop potential algorithms based on analysis of physiological signals. This research program will involve correlation of physiological with behavioral data. For each of the previously mentioned applications, experimentation will be performed.

After research to develop the algorithms and discover physiological correlations with behavior, either or both of the two configurations can be developed and field tested. The cassette recorder, by providing a baseline, may be used to personalize each device before wearing. After field testing, the biosensor systems can play an important role in solving the problems inherent in assessing defender performance capability.

TABLE 5. *SAI R&D program outline*

Configure Prototype Recorder
Research to Develop Algorithm(s)
- Laboratory testing
- Field testing and data collection
- Data analysis
Potential Algorithms
- Detection of abnormal physiological states
- Spectral analysis (EEG)
- Activation measure (EEG)
- Interbeat interval (EKG)
- Frequency EDR
Field Recorder System
Develop On-line Analyzer
Research for Personalizing On-line Analyzer
Field Test On-line Analyzer
Field On-line Analysis System

REFERENCES

[1] Holter, N. J. (1961). New method for heart studies. *Science,* **134**, p. 1214.

[2] Richardson, D. W., Honaur, A. J., Fenton, G. W., Stott, F. D., and Pickering, G. W. (1964). Variation in arterial pressure throughout the day and night. *Clinical Science,* **26**, p. 3.

[3] Ives, J. R. and Woods, J. F. (1965), 4-channel, 24 hour cassette recorder for long-term EEG monitoring of ambulatory patients. *Electroencephalography and Clinical Neurophysiology,* **39**, pp. 88-92.

[4] Sato, S., Penry, J. K., and Dreifuss, F. E. (1976). Electroencephalographic monitoring of generalized spike-wave paroxysm in the hospital and at home. *Quantitative Analytic Studies in Epilepsy,* pp. 237-251.

NEUROPHYSIOLOGICAL OPERANT AND CLASSICAL CONDITIONING METHODS IN RATS IN THE DETECTION OF EXPLOSIVES

Dr. Sidney Weinstein, Mr. Curt D. Weinstein

NeuroCommunication Research Laboratories, Inc., Danbury, Connecticut 06810

Mr. Raymond V. Nolan

Countermine Laboratory, MERADCOM, Fort Belvoir, Virginia 22060

INTRODUCTION AND OBJECTIVES

A major premise of the research reported herein is that biosensors (e.g., rats) may be useful as explosives detectors. In his book, The War Animals, Lubow [9][1] describes Bionics as a "technology that attempts to develop new, artificial systems based on the functions and principles found in living organisms." Our approach and that of Lubow was to use the entire organism as a simple tool whereas bionics seek to emulate the biological function. In one reconnaissance project, Lubow employed the pigeon and trained it by reinforcing its behavior with food rewards. Similarly, our project employed an entire organism (the rat) in the task of detecting TNT, and our reinforcement was the use of electrical brain stimulation (EBS) in one of the positive reward centers.

The scientific literature in the area of explosives detection, although not extensive, is from a diversity of sources and demonstrates rather clearly that animals (usually dogs) have had a quite respectable record in the laboratory, in the field, and even on the battlefield as explosives detectors. Indeed, several authors believe them to be the single most valuable asset in this regard.

Lubow's [10] report is typical: "We completely endorsed the biosensor approach to letter-bomb detection. There is no system that can match its speed, sensitivity and reliability." He further indicates that "for all practical purposes, the ability of a dog trained to detect the odor of an explosive cannot readily be jammed by the addition of other odors."

In view of the well-established ability of dogs as explosives detectors one might ask why we embarked on the study of rats and why we studied the potential use of neurophysiological methods.

The reasons, as we shall point out, are rather empirical: (a) *Size.* Dogs are several orders of magnitude larger and heavier than rats. (b) *Ease of maintenance.* Dogs require large cages and in domiciliary (troop) areas. Rats occupy small cages and produce little waste. (c) *Cost.* Dogs cost substantially more to purchase and feed than rats. (d) *Ease of training.* Dogs prefer individual trainers as masters, whereas rats can be trained in operant procedures routinely and impersonally. If a dog's master is not available, there may be problems in having him respond efficiently to a handler with whom he is unfamiliar. Rats do not require personal care, since their training and actual use in detection is controlled by electronic equipment. Man-hours in training large numbers of rats are only a fraction of those required to train dogs. (e) *Noise and Appearance.* Dogs are difficult to silence and hide and they may produce social problems in crowded areas such as airports. Rats are quiet, and should be entirely covert when in use as detectors. (f) *Transmission of Results.* Dogs are trained to "point" and "sit" when they detect explosives. Such gross responses may be confusing, especially if the dog is distracted by noisy crowds, oestrus females,

[1] Figures in brackets indicate literature references at the end of this paper.

and provocative males. Neurophysiological responses from the rat's brain are immediate, and there can be no ambiguity of the electronic response, e.g., a red light or a buzzer.

Among the problems encountered in the use of animals as biosensors is the question of type of reinforcement used in the training. The usual form of reinforcement is rapid feeding of the dog after it makes a response. This procedure requires having a handler with the animal, observing the correctness of the response, and dispensing the reward appropriately. In an actual search for concealed explosives, this reward cannot be offered, since the handler has no knowledge of the correctness of the response, and rewarding incorrect responses would serve only to negate the conditioned behavior necessary for efficient detection. In recognition of these practical problems, Lubow [11] suggested that "it may also be possible to use signals that are delivered to small electrodes implanted in the brain." In discussing the need for "short delay of reinforcement," Lubow [12] again suggested that "this argues strongly for the investigation of new procedures, such as electrical brain stimulation" (i.e., as a form of reinforcement to replace the traditional food reward).

The issue of how the animal transmits information back to the control has usually been resolved by training it to make a simple behavioral response, e.g., "pointing." Lubow [13] points out that "the report response can be either active or passive. In the first case, it may make use of a response that is not a part of the (animal's) normal behavior." An example he provides is to have a pigeon peck at a microswitch. "A passive response" (he continues) "does not require an overt muscular act." He provides examples such as changes in heart rate, respiration rate, blood pressure, and galvanic skin response; however, he did not list changes in brain waves.

Among studies employing active responses is one we conducted in which a rat pressed a bar when it detected a contaminant in water, and refrained from bar pressing when the water was pure [32].

METHOD AND PROCEDURE

The purpose of this experiment was to determine whether rats can differentially detect the presence of odors emanating from small quantities of TNT. Two methods were employed for the detection of the TNT: (1) operantly conditioning the rat to press a bar only when TNT was present, or (2) classically conditioning a change in the pattern of brain waves when TNT was present in contrast to other, nonexplosive (NTNT) control odorants. The TNT was granular and about 10 gm was employed over the one year during which the study was conducted.

Subjects. Twenty-two male albino rats, weighing from 250 to 600 gms, were employed. They were individually caged and provided with Purina Rat Chow and water ad libitum. They were housed in a ventilated colony room on a 12-hour light-on (9 AM to 9 PM), 12-hour light-off schedule.

Surgical preparation. The rat was anesthetized (I.P.) with chloral hydrate and sodium pentobarbitol (Chloropent) with the following dosages: 250 gram rats (.75cc), 300 gram rats (.88cc), etc. to 600 gram rats (1.77cc). Supplementary injections (15% of original dose) were administered as needed to keep the animal anesthetized. The ears were clipped in the usual laboratory scheme for identification, and the head was shaved. Mineral oil was applied to the eyes to keep them moist, and tincture merthiolate was applied as an antiseptic to the shaved scalp.

The rat was placed in a Kopf Small Animal Stereotaxic Instrument (Model No. 900). Each ear bar was placed firmly into the appropriate auditory meatus, the teeth were placed over the incisor bar, and the nose clamp tightened. The ear bars were centered, and fixed, keeping the head centered, level, and rigid.

The incision was made lateral to the midline and the coordinates for the skull landmarks (Lambda and Bregma) were obtained. Following the drilling of the skull holes the dura was penetrated and the stimulating electrode (stainless steel, bipolar, insulated to the tip, approximately 1 cm in length) was inserted to the proper depth in the medial forebrain bundle (MFB). Cortical Screws (080 stainless steel) were placed in far left anterior and far right posterior

holes, and leads from bipolar steel electrodes, stripped of insulation were affixed to each screw. The electrical cap, consisting of the stimulus electrode mount and a quantity of dental acrylic was positioned on the skull at the proper electrode penetration depth. When the acrylic adhesive had solidified, two or three stitches (00 surgical silk) were used to close the wound, and antibiotic ointment (Bacitracin or Mycitracin) was applied to minimize possibility of infection. The rat was allowed 5-7 days to recover before training.

There was thus, a bipolar stimulating electrode in the MFB and two transcortical surface cortical electrodes, positioned anterior and posterior.

Training procedures. "Shaping" is the term for training an animal to make the desired final response. It consists of continually rewarding partial, or approximate responses until the final desired response is obtained. The "reward" to the rat for these "spiral approximations" to the ultimate desired response is an electrical brain stimulation (EBS) delivered to the FMB by the experimenter. When the rat makes the desired response (i.e., pressing a bar) he then self-stimulates. The purposes of shaping are: (1) to determine whether, by causing the rat to self-stimulate, the electrode was correctly placed in the FMB, and (2) to have a *behavioral* index from the rat that he has learned to distinguish the TNT from NTNT.

"Shaping" was begun 5-7 days postoperatively. Stimuli were delivered by a Nuclear Chicago Constant Current Stimulator (Model 7150), or by a 60 Hz sine wave stimulator (built in house). The Nuclear Chicago Stimulator delivered a square wave stimulus with the following parameters: 0.2 msec (+), 0.2 msec (0), 0.2 msec (−), equally spaced at 100 presentations per second. The stimulus was delivered at a specific amplitude and duration. Amplitudes ranged from 50 μA to 600 μA, and the duration was usually 250 msec, with two exceptions (200 msec, and 500 msec). The sine wave stimulator delivered a constant current (no delay) 60 Hz sine wave stimulus, ranging from 50 mV to 400 mV, and was used only in shaping. The Nuclear Chicago Stimulator was used in all positive reinforcements during the actual conditioning.

Shaping procedures were started with stimuli set at 50 μA for 250 msec. A stimulus was delivered to the rat when it first approached, (or faced) the bar. Current was raised as necessary (if the animal disregarded the stimulation), until an orienting response was elicited while it was engaged in grooming. The subject was reinforced for approaching the bar, for touching it, and finally for pressing it. This procedure took from one 5-minute (rarely) to several 30-minute sessions. The animal soon developed a steady routine that enabled him to get the greatest number of stimulations per unit time. When the rat pressed the bar at least 10 times/minute for five consecutive minutes, for two successive days, shaping was terminated and prerecordings were taken prior to initiation of conditioning.

RECORDING PROCEDURES:

Prerecordings. EEGs were recorded from each rat prior to initiation of conditioning procedures. The subject was placed in the testing chamber with no bar for pressing available and allowed to become accustomed to the air being emitted from the pure (NTNT) air delivery tube for 3 to 5 minutes. He was then exposed to air which had passed over TNT granules contained within the odorant delivery tube; during this time EEGs were recorded. Finally, the NTNT (control) air was presented for 10 to 20 seconds and EEGs again recorded. Presentation of odorants was given at random for each rat. The EEGs were recorded between the two transcortical electrodes in contact with the cortex. The signals were amplified by a Grass (Model 7P 3A AC) Preamplifier and a Grass (Model 7 DAB DC) Driver Amplifier, and filtered at 0.3 to 500 Hz. They were recorded on either an Ampex (SP 300) or a Honeywell (7600) Tape Recorder at 1-7/8 i.p.s. with a voice mark and a trigger signal.

Postrecordings. Techniques varied according to the conditioning procedure used. In general, the EEGs were recorded in the manner described for prerecordings immediately following each conditioning session during which the rat received stimulation while it was exposed to the TNT vapor. Recordings were made without EBS during the last few trials of a chosen session. Instrumentation and techniques were identical to those described for prerecording.

CONDITIONING PROCEDURES:

During the year-long course of the experiment, several changes in procedure and technique were made in conditioning. Before we changed to a classical conditioning paradigm, behavioral (operant) conditioning was tried as an index of when the learned association occurred. These various procedures are outlined below.

Behavioral conditioning overview. The rat was placed in the testing chamber containing a "self-stimulus" press bar, and exposed to the TNT odor for the entire duration of the TNT trial, and also exposed to the NTNT odor for the entire duration of the NTNT trial. These trials were separated by a 10 second intertrial interval (ITI). A devised circuit allowed the rat to receive an EBS only if he pressed the bar during the TNT trial. An exhaust fan, which was continuously on, evacuated TNT-vapor laden air from the test chamber during the ITI. (The test room in which the test chamber was housed, also had an exhaust fan operating continuously to minimize the likelihood of odor contamination.) A timer controlled the length of each trial and ITI. Data (responses and number of trials) were recorded on both digital counters and cumulative recorder chart paper.

Air delivery system. This system evolved during the experiment as follows: (a) Initially, one positive pressure air delivery system was used to present the rat with TNT or NTNT odorants, each of which was contained in closed-end copper tubes perforated to allow passage of air. The experimenter manually switched the tubes during the ITI, placing them beneath the cage (in the test chamber). (b) This procedure was soon replaced by a dual positive pressure (dual-push) system, with one tube for each odorant. The odorants were now switched automatically by a logic circuit and probability generator, which presented the odorants randomly. (c) A vacuum system was then set up such that the tubes were double-ended, with air entering through one end and a vacuum pulling on the other end. During a TNT trial, air would blow through the TNT granules, and the vacuum would simultaneously pull on the NTNT tube. This process was reversed during the NTNT trial. During the ITI, vacuums would exhaust both tubes eliminating both TNT and NTNT simultaneously. (d) The final system that evolved was a dual push-pull system, in which both vacuum and air tubes were attached at one end of the odor tube, and the other end was open, leading to a small opening in the test chamber at nose level. The logic and probability generator were the same as before. In all systems, pressures of 1 psi or less were used, and all odorants were exhausted outside the laboratory building. For each conditioning session, the air and vacuum tubes were switched so that any specific clicking sound associated with a given solenoid valve could not be associated by the rat with the odor to be presented next. The NTNT (control) odorants employed were asphalt granules, pine sawdust, room air from the animal colony, and infrequently, instant coffee applied to wood chips.

Conditioning. Trials were presented manually at 100 one minute trials/session and 1 session/day. 10 Hz clicking sounds were presented to a small speaker in the test chamber to signal the presence of TNT (and thus the availability to the rat of the EBS). White noise (hiss) was delivered over the same speaker as a "punishment" if the rat pressed the bar for EBS during a NTNT trial. Only one rat was successfully operantly conditioned with this system.

The system was then automated with the logic and timers mentioned above: solenoid valves for the air, and a probability generator to change the odorants randomly. The air system used was the dual push-pull system. Rats were divided into five groups, with varying trial times, punishment, and visual and auditory cues (see table 1). Punishment took the form of white noise (hiss) over the speaker or a yellow light flash if he pressed the bar during a NTNT trial. It was later determined that the white noise was the more effective punishment. The Rf (reinforcement) schedule approximated FR (2); that is, the rat was reinforced approximately for every other (correct) press. A light used to indicate an ITI proved unsuccessful because the rats cued to its offset rather than to the odorants themselves. A flashing bright yellow light was used to signal the end of a TNT trial. Ten or 1,000 Hz clicks were used to signal the presence of TNT. It was found that several rats learned the clicks, but their accuracy deteriorated as the intensity of the clicks

TABLE I

April 1976

	Group A n=4	Group B n=4	Group C n=4	Group D n=4	Group E n=4
ITI time	10 sec	10 sec	10 sec	10 sec	10 sec
Trial time	50 sec	20 sec	50 sec	20 sec	20 sec
TNT	50%	50%	50%	50%	50%
NTNT	Asphalt 50%	Asphalt 50%	Asphalt 50%	Asphalt 50%	Asphalt 50%
Punishment	No	No	1 second yellow light flash	1 second yellow light flash	Hiss
R_f Schedule	FR (2)	FR (2)	FR (2)	FR (2)	FR (2)
No. Trials/Session	60/hr	60/½ hr	60/hr	60/½ hr	60/½ hr
Sessions/Day	1	1	1	1	1
Days/Week	5	5	5	5	5
ITI signal	Dim Yellow	Dim Yellow	Dim Yellow	Dim Yellow	Dim Yellow
Intro w/click = TNT	Yes	Yes	Yes	Yes	Yes
End TNT trial	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)

* Air-vacuum tubes were switched each day, to minimize predictability of solenoid sounds and specific odors.

was "faded" (attenuated to "wean" them). Hence the click approach was abandoned, and the simple air delivery of the odorant was considered a sufficient cue (see table 1 for a summary). We then established a system such that the rat had to learn the clicks first (pass at a level of $p<.01$); they were then "faded," and the rat was considered conditioned if it passed with no auditory cues (at $p<.01$). No rats passed this procedure.

The groups were then expanded and modified. New additions included: (1) A 2 to 3 second delay in clicks to allow the odorant to be presented first. (2) A "classical" group in which there was no bar, and each rat's own prerecorded preferential rate of bar pressing was delivered to him while stimulated by TNT.[2] (3) A new "continuance" trial group. If the rat responded within 20 seconds he was rewarded or punished (depending on the odorant) with a trial extension to 60 seconds. If he did not respond within 20 seconds, the trial was ended. (4) Rats were given 8 days (maximum) to pass each stage (clicks and clicks fading). Those who did not pass were rejected. (See table 2.)

[2] It was observed that the rats functioned better in the first 30 minute session than in the second 30 minutes, and the number of groups was reduced to four: Three operant and 1 classical conditioning group. We scheduled them as follows: 2 operant groups with 30 min/session, (1 group run twice and 1 group once daily); 1 operant group with 15 min/session, (run twice daily); 1 classical group run as described above.

TABLE 2

May 1976

	Group A	Group B	Group C	Group D	Group E	Group F	Group G	Group H (classical)
ITI time	10 sec	10 sec	10 sec	10 sec	10 sec	10 sec	10 sec	10 sec
Trial time	50 sec	20 sec	50 sec	20 sec	50 sec	20 or 50 sec	50 sec	20 sec
TNT	50%	50%	50%	50%	50%	50%	50%	50%
NTNT	Asphalt 50%	Asphalt 50%	Asphalt 50%	Asphalt 50%	Asphalt 50%	Asphalt 50%	Asphalt 50%	Asphalt 50%
Punishment	No	No	Hiss	Hiss	–	Hiss	Hiss	–
R_f Schedule	FR (2) final stage	FR (2) final stage	FR (2) final stage	FR (2) final stage	FR (2) final stage	FR (2)	FR (2)	–
No. Trials/Session	60/1 hr	60/½ hr	60/1 hr	60/½ hr	15/¼ hr	15/¼ hr	15/¼ hr	60/½ hr
Session/Day	1	1	1	1	2	1	1	1
ITI signal	Dim Yellow	Dim Yellow	Dim Yellow	Dim Yellow	Dim Yellow	Dim Yellow	Dim Yellow	
Intro w/clicks = TNT	Yes	Yes	Yes	Yes	Yes	No	No	No
End TNT trial	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)	Bright Yellow (1 sec)	–

The next modification involved the introduction of a 3-second delay in reinforcement. Thus, in order to permit the rat time to detect the odorant, EBS was not delivered during the first 3 seconds of each TNT trial. Any bar-presses during this time were considered as ITI presses. Continuance trials were then adapted to each rat according to its own optimal rate of responding determined during the "shaping" process. The faster the rate of responding, the shorter the time he was given to press the bar, and therefore the shorter the trial. Two rats (S004 and S020) learned behaviorally ($p < .001$) on this system, and we believe that this test is the one to use in behavioral conditioning of this type.

The final switch was made to classical conditioning. This system produced 18 rats who were trained to a statistically significant degree to demonstrate differential brain activity to TNT versus NTNT odorants.

General Procedure—Classical Conditioning

1. Shape (described above).
2. *Rate-Intensity Function.* Starting with the lowest parameters of the EBS with which a rat will press, his press rate (per minute) is taken over 5 minutes with increasing intensity, until the rate levels off or drops. This provides the optimal electro-stimulus intensity.
3. The rat's rate of bar-pressing is recorded on magnetic tape for 45 minutes at his optimal EBS intensity to obtain his optimal rate of response.
4. During the actual conditioning procedure the EBS is run at an intensity somewhat lower than the individual's optimum. The circuit is prepared so that the subject's recorded rate (constantly channeled through an audio threshold detection relay—Scientific Prototype 761-G) triggers the Nuclear Chicago Stimulator to stimulate the subject during all TNT trials. The entire system is prepared with the final air system and probability generator as follows:
   a. 20-second trials; 10-second ITI; 60 trials/session; 1 session/day; 3-second delay in reinforcement.
   b. Rf schedule: 100 percent until the trial before post-recordings, then 50 percent.

The final recording is of the EEGs of the last trials (TNT and NTNT) of each session.

ANALYSIS OF EFFECTS:

Behavioral. Subjects were considered behaviorally conditioned if there were statistically significant different distributions of their likelihood to bar-press during TNT and NTNT trials.

The tests used were one-tail Chi-Square, with four cells: response and nonresponse for TNT and NTNT. The cell entries for a trained rat are high for "response to TNT" and "nonresponse to NTNT."

Classical. Data were recorded on either an Ampex FM Recorder (Model SP300) or a Honeywell FM Recorder (Model 7600). Data were identified by voice and by a trigger signal on separate channels. Once the location on the tape was established via verbal identification, the tape speed was switched from 1-7/8 ips to 15 ips (1.8 time compression) and data were automatically collected. A timing circuit was triggered by the first trigger and at least 1,000 msec of compressed time was analyzed. A rectifier and Schmitt trigger unit accepted voltages of at least 0.1 V and baseline crossings of at least 8 Hz were converted into time intervals. The time intervals were converted into a histogram by the CAT mnemotron (Models 400B, 600, 522A, 520) in the H program. The H program digitally prints out histograms, and 26 bands of frequencies were formed by combining proper CAT addresses. The range of the 26 frequencies was from 1.2 Hz to 35.5 Hz. (These are midpoints between the upper and lower frequency of each band.)

We employed a filter set at (0.5, 32.0) [Hz –3dB pts @ –24 dB/octave roll off]. This procedure detects the frequency of simple wave forms such as sine waves well. However, we noted (visually) complex waves (summed sine waves of different frequencies) in the EEG and took measures to separate them. We first filtered for 1-6 Hz and 6-36 Hz; then decided upon 1-2 Hz, 2-4 Hz, 4-8 Hz, 8-16 Hz, and 16-38 Hz. Data collected outside the filtered band were not recorded.

a. $100\ C_i / \left[F_i \sum_{j=1}^{26} (C_j / F_j) \right]$

b. $50\ C_i/(F_i t)$

C - Counts in band$_i$

F - midfrequency (Hz) of band$_i$

t - time of data sample

These formulas are theoretically equivalent for simple waves, but formulation "b" accounts for data outside the bands which were analyzed. Pre- and postrecordings were always consistently analyzed (i.e., both according to "a" or to "b").

Wilcoxon's or Friedman's statistical tests were used to verify the hypothesis of differential occurrence frequencies across all bands. Limited band Wilcoxon's were also performed on the higher frequencies. Correlations were taken pre-exposure to conditioning and, at various times, postexposure: t-tests were performed to determine whether conditioning had occurred. When this was observed, the rat was considered conditioned as a TNT-detector.

STATISTICAL ANALYSES:

For each rat, Pearson Product Moment Correlations (r) were computed between the cortical frequency spectra (CFS) [i.e., the percentage time of EEG activity in each of the 26 bands] obtained during exposure to TNT and NTNT both before and after conditioning. We reasoned that unrewarded odorants (NTNT) should have no effect on the CFS, and thus there should be no change in the CFS recorded prior to the following exposure to totally indifferent (to the rat) odorants. On the other hand, there should be a significant change in the CFS recorded prior to and following exposure to an odorant (TNT) which was rewarded with EBS. These correlations were then statistically compared by t-tests. If they were significant at $p < .05$ it was concluded that the CFS had changed to a significant extent and that the rat was conditioned to the odor of TNT.

The following sets of correlations were computed:

a. *Experimental*

(1) Post TNT versus Post NTNT
(2) Pre TNT versus Post TNT
(3) Pre NTNT versus Post TNT

b. *Control*

(4) Pre TNT versus Pre NTNT
(5) Pre NTNT versus Post NTNT
(6) Pre TNT versus Post NTNT

The experimental correlations compared *Post TNT* to: Post NTNT, Pre TNT, and Pre NTNT; the control correlations compared Pre TNT to both Pre and Post NTNT; and Pre NTNT to Post NTNT. The three experimental r's (1, 2, 3) were each compared to t-test to each of the control r's (4, 5, 6). The resulting 9 t's were evaluated for statistical significance.

RESULTS

There were 12 rats who were subjected to operant conditioning by means of one of the procedures described above. Four reached statistical significance (1 by behavioral index above, 1 by neurophysiological index alone, and 2 by both indices).

There were 23 rats subjected to classical conditioning, including some who had previously received operant conditioning. Of these, 18 reached statistical significance. Thus, there were a total of 21 rats with neurophysiological indices of conditioning to detect TNT. Since decrease in the experimental correlations (1, 2, 3) was employed to determine conditioning, we tallied the number of rats for whom the lowest correlation was one of the three experimental correlations (1, 2, 3) *and* control correlations (4, 5, 6). Of the 21 rats, 16 met this criterion; of the remaining 5, 3 conformed to either of the above conditions. The means of the six correlations were also computed.

When the correlations means were ranked, the most critical experimental correlation (#1, between TNT and NTNT post conditioning) was the lowest (.67), and the most critical control correlation (#4, between the two preconditioning conditions) was the highest (.81). These findings conformed to our hypothesis that conditioning modifies the CFS.

DISCUSSION AND CONCLUSIONS

It is clear that both the operant and the classical conditioning approaches are effective in producing rats as TNT detectors. Even the early phases of the operant conditioning, in which various procedures were attempted, eventuated in several successful rats. The most effective training procedure apparently was the classical conditioning approach which yielded 21 successful rats.

It is interesting to note that even in the classical conditioning approach, in which the rats were not trained to respond behaviorally (e.g., to press a bar), the overt behavior soon clearly indicated when the rat had become conditioned. Even the untrained observer (following a sufficient number of sessions) could soon see that the rat placed his nose adjacent to the nozzle from which the air stream came when TNT was being delivered, and remained essentially motionless during the several seconds when the TNT vapor was being delivered. Conversely, when the clicking sound indicated that another trial was imminent, the rat ran to the muzzle, and if the odorant was a control (asphalt, pine sawdust, or room air), the animal left that area of the test chamber and continued grooming itself for the duration of the session. Indeed, we had a naive observer tally those trials in which the rat oriented to the tube, and those in which he sauntered off; the χ^2 test was highly statistically significant, showing that even subjective observation could determine which rats were conditioned, and at which part of the conditioning this occurred.

It is important and of practical as well as theoretical significance that EBS is an effective reinforcement and can replace traditional reinforcements such as food and water. Another insight

which emerged from this study is that either operantly or classically conditioned rats show behavioral, neurophysiological, or both indices of training.

The many questions which still remain unanswered concern methods for utilizing this technique in the creation of standard systems both for efficient training and for the accurate detection of the neurophysiological changes which occur with a specific exposure to an explosive.

More basic and applied research is needed in this field. However, it is abundantly clear that the described approaches are effective in creating a biosensor for TNT, as well as potentially for all other explosives, which may be quite effective in a variety of situations which require the rapid detection of explosives.

REFERENCES

[1] Berryman, G., Churchman, D., and Yallop, H. J., "The Detection of Explosives by Dogs-Feasibility Study." RARDE Memorandum 33-71. Royal Armament Research and Development Establishment, Port Halstead, Kent, England, October 1971.

[2] Carr-Harris, E., Eibert, L., Thal, C., and Thal, R., "Mine, Booby-Trap, Trip-Wire Detection Training Manual." Contract No. DAAD05-69-C-0234. Behavior System, Inc., Raleigh, North Carolina, September 1969.

[3] Carr-Harris, E. and Thal R., "Mine, Booby-Trap, Trip-Wire and Tunnel Detection. Final Report." Contract No. DAAD05-69-C-0234, U.S. Army Limited War Laboratory, Aberdeen Proving Ground, Maryland, January 1970. AD867-404L.

[4] Department of the Army Field Manual, FM-20-32: Landmine Warfare. August 1966.

[5] FBI Bomb Data Program. "Use of Dogs to Find Concealed Explosives—Update." General Information Bulletin 76-1. January 1976.

[6] Halligan, W. A., "Evaluation of Familiarization and Training in Aircraft and Airport Environment for Dogs Trained in Explosive Detection Measures. Internal FAA memo to S. Maggio, Chief, Air Transportation Security Div. October 1971.

[7] Knauf, H. and Johnston, W. H., "Evaluation of Explosives/Narcotics (EXNARC) Detection Dogs." Report 2102. U.S. Army Mobility Equipment Research and Development Center, Fort Belvoir, Virginia. May 1974. AD787-308.

[8] Kraus, M. "Explosives Detecting Dogs." Technical Report No. 71-11. U.S. Army Land Warfare Laboratory, Aberdeen Proving Ground, Maryland. September 1971. AD736-829.

[9] Lubow, R. E., *The War Animals*, New York: Doubleday, 1977 (p. 61).

This reference listing contains additional reports dealing with the use of animals as biosensors for explosives.

[10] Lubow, R. E., op. cit., (see Item 9) p. 225.

[11] Lubow, R. E., op. cit., (see Item 9) p. 91.

[12] Lubow, R. E., op. cit., (see Item 9) p. 92.

[13] Lubow, R. E., op. cit., (see Item 9) p. 97.

[14] Lubow, R. E., "Use of Biological Systems to Detect Explosives." Progress Report, 1972-73, Israel Ministry of Police.

[15] Lubow, R. E., "Weapons Detection Study Using Dogs." Final Report. Submitted to Israel Ministry of Defense, July 1971.

[16] Lucero, D. A., "Monthly Report of Marine Corps Mine Detection Program," 1 April 1970. Headquarters, 3rd Military Police Battalion, Force Logistic Command, Fleet Marine Force, Pacific, FPO San Francisco, April 1, 1970.

[17] Morgan, P. M., Robinson, G. A. N., and Yallop, H. J., "The Detection of Explosives by Dogs-Trials in Aircraft." RARDE Memorandum 29/73. Royal Armament Research and Development Establishment, Port Halstead, Kent, England, December 1973.

[18] National Bomb Data Center. General Information Bulletin 78-4. Picatinny Arsenal, Dover, New Jersey. March 13, 1974.

[19] National Bomb Data Center. General Information Bulletin 75-5. Picatinny Arsenal, Dover, New Jersey. June 12, 1975.

[20] Nolan, R. V. and Gravitte, D. L., "Mine Detecting Canines." Report 2217, U.S. Army Mobility Equipment Research and Development Command, Fort Belvoir, Virginia, September 1977.

[21] Phillips, R., "Training Dogs for Explosives Detection." Technical Memorandum. No. LWL-CR-01B70. U.S. Army Land Warfare Laboratory. Aberdeen Proving Ground, Maryland, October 1971. AD 733-469.

[22] Romba, J. J., "Tactics in the Development of Mine Detection Dogs." U.S. Army Land Warfare Laboratory. Aberdeen Proving Ground, Maryland. 1970. AD 713-577.

[23] Rolls, E. T. and Mogenson, G. J., *Brain Self-Stimulation Behavior*, Chapter 8, in Mogenson, G. J., *The Neurobiology of Behavior*, Hillsdale, New Jersey: L. Erlbaum Associates, Publishers, 1977.

[24] Southwest Research Institute. "Objectively Evaluate the Performance of Dogs Trained to Perform Various Militarily Significant Tasks," For U.S. Army Mobility Equipment Research and Development Center, Fort Belvoir, Virginia. December 1972. AD 909-955L.

[25] Southwest Research Institute. "Olfactory Acuity in Selected Animals Conducted during the Period June 1972-September 1974." Contract No. DAAK02-72-C-0602 with U.S. Army Mobility Equipment Research and Development Center, Fort Belvoir, Virginia. September 1974. AD 787-495.

[26] Thal, R., Thal, C., and Lubow, R. E., "Mine Detector Dogs." Final Report. Contract No. DAAD05-70-C-001. U.S. Army Limited War Laboratory, Aberdeen Proving Ground, Maryland. August 1970, AD 874-794L.

[27] U.S. Army Limited War Laboratory. "Mine, Booby-Trap and Trip-Wire Detecting Dog Handler Teams." Operating Manual. U.S. Army Limited War Laboratory. Aberdeen Proving Ground, Maryland. April 1969 (b).

[28] U.S. Army Limited War Laboratory. "Tunnel and Trip-Wire Detecting Dog-Handler Teams." Operating Manual. U.S. Army Limited War Laboratory, Aberdeen Proving Ground, Maryland. April 1969 (a).

[29] U.S. M. C. Project 90-69-01 Final Report. "Dog Detection of Mines/Booby-Traps." From: Commanding General, Marine Corps Development and Education Command, Quantico, Virginia. To: Commandant, Marine Corps (Code Ax), Washington, D.C., May 7, 1971. AD 883-469L.

[30] Weinstein, S., "Investigation of Neurophysiological Procedures for the Detection of Explosives." Final Technical Report, Contract No. DAAG-53-76-C-0020, September 30, 1976. (Fort Belvoir, Virginia).

[31] Weinstein, S., "Further Investigation of Neurophysiological Procedures for the Detection of Explosives." Final Technical Report, Contract No. DAAG-53-76-C-0020, December 30, 1977. (Fort Belvoir, Virginia).

[32] Weinstein, S. and Weinstein, C. D., "Development of Neurophysiological Procedures for the Detection of Organic Contaminants in Water." Final Report, Contract No. DAMD 17-77-C-7008, February 15, 1978. (Fort Detrick, Maryland, U.S. Army Medical Research and Development Command).

[33] White, B. W., Jr., LT COL ACTIV 60th Infantry Platoon (Scout Dog) (Mine/Tunnel Detection Dog). Final Report. Project No. ACG-65F, December 1969.

LINK ANALYSIS OF THREATS AND PHYSICAL SAFEGUARDS

Mr. Douglas H. Harris

Anacapa Sciences, Inc., Santa Barbara, California 93102

INTRODUCTION

Link analysis is a systematic behavioral approach to defining and describing relationships among entities (individuals, organizations, and locations). As such, it is a tool that can be employed in the analysis of organized threats to physical security and in the evaluation of physical safeguards employed against the threats defined. This paper presents recently developed computer-based link analysis techniques and illustrates the potential application of these techniques to threat analysis and safeguards evaluation. In addition, suggestions are provided for needed research and development to enhance the usefulness of link analysis for these purposes.

LINK ANALYSIS

Link analysis has proven to be a useful tool in behavioral science. Probably the earliest formal application was by Gilbreth and Gilbreth (1917) [5][1] who evolved a system for machine layout based upon distances traveled during shop operations. Fitts, Jones, and Milton (1950) [3] employed a link analysis approach to study the eye movements of aircraft pilots during instrument landings. Channell and Tolcott (1954) [1] used the method to define and rank communication links in a Navy command and control system. Haygood, Teel, and Greening (1964) [9] developed and used a computer-based link analysis technique to resolve conflicts in equipment placement. Harris and Chaney (1969) [8] illustrated the application of link analysis to the design of complex electronic test equipment. Recently, link analysis techniques were developed and applied in support of the criminal intelligence process within law enforcement agencies (Harper and Harris, 1975; Harris, 1978) [6]. The general acceptance and use of link analysis by behavioral scientists is further reflected by descriptions of the approach found in human factors reference books (Chapanis, 1969; McCormick, 1970; Van Cott and Kinkade, 1972) [13].

PHYSICAL SECURITY ANALYSIS

Both organized threats and physical safeguards lend themselves to assessment by link analysis. Developing an understanding of potential threats depends upon establishing the relationships that exist among the entities which constitute a specific adversary and defining the relationships that exist among different adversaries. Furthermore, the identification of these relationships must typically proceed from fragmentary information collected through intelligence efforts. Within this framework, link analysis can help assemble the best picture possible of a potential threat from whatever information is available. For example, command structures of adversaries can be defined; patterns of infiltration can be exposed; sources and flows of goods (money, weapons, and explosives) can be delineated; and the interrelationships that exist among potential adversaries can be described. In short, link analysis can be employed to piece together a description of an adversary which, together with other information, can serve as the basis for assessing the nature and magnitude of a threat.

[1] Figures in brackets indicate literature references at the end of this paper.

Link analysis can also be applied, in a different manner, to help evaluate physical safeguards. For example, a facility such as a fuel fabrication plant can be analyzed to identify the most vulnerable pathways for the possible diversion of strategic nuclear material through the facility and its associated safeguards. The entire facility can be defined by potential access entities (doorways, gates, hatchways, and fences) and by links (the safeguards that must be successfully overcome to pass through the access entities—such as guards, alarms, and monitors). By specifying the probability of successful passage through each link in the safeguard system, one can produce an ordered listing of the most vulnerable pathways for both penetration and escape.

COMPUTER-BASED TECHNIQUES

Computer-based link analysis techniques, developed originally for the analysis of criminal intelligence, are applicable to the behavioral analysis of both adversaries and safeguards. These techniques facilitate the organization and manipulation of available information to highlight the meaning. To this end, they: (1) aid the selection of information relevant to analysis, (2) provide a system for obtaining needed analytical products, and (3) overcome the problems typically associated with the manual application of link analysis by increasing flexibility, reducing time and effort, and enhancing analytical precision.

The fundamental information needed is a description of the link between two entities; the data base upon which the link analysis program operates is simply the collection of these fundamental descriptions. In this way, the program can proceed from the most fragmentary and incomplete information toward complex products of the types discussed earlier. Since links among entities can be of different types and strengths, and since their existence is likely to be based on information at different levels of estimated validity, a link description consists of four different kinds of information—entity, linktype, strength, and validity.

Entities are persons or things that might be linked one to another in some way. Any name of 20 characters or less can be entered into the program as an entity.

Linktypes are descriptions of the relationships (links) that connect one entity to another in some way. Any name of 10 characters or less can be a linktype. (For example, a link based on the flow of money from one entity to another might be called 11. MONEY; a link based on a criminal association between two persons might be called CR ASSOC.)

Strength is an estimate of the strength of the link between two entities; each link is assigned a value ranging from a low of 0 to a high of 99 corresponding to the particular scale of values defined for links of that type.

Validity is the likelihood that the link between entities of the specified strength actually exists as described. Validity is also measured on a numerical scale (ranging from a low of 0 to a high of 99) corresponding to the probable validity of the information.

Program routines act upon the four types of information at the analyst's direction to generate several different analytical products. The analyst has great selectivity and flexibility in producing the desired products, in focusing on selected entities, and in emphasizing networks of specific linktypes. For example, an analyst interested in determining if members of a specific group have links to known sources of explosives or weapons can obtain link networks consisting only of EXPLOSIVES and WEAPONS linktypes. Samples of two of the various analytical products that can be produced by the program are illustrated below with the context of sample applications.

APPLICATION TO THREAT ANALYSIS

Non-military adversaries, such as organized criminals and terrorist groups, can present more difficult analytical problems than military adversaries. Information for analysis is less readily available, and what is available is often more difficult to obtain. For example, the very existence of an adversary might not become known until after a major action is executed, and often not even then. Whereas the objectives, functions, and makeup of a military adversary are logically structured, such may not be the case for these other potential adversaries. Consequently, the

importance of intelligence efforts is as great or greater for the non-military as for the military adversary. Intelligence efforts are needed to produce, organize, and integrate information in a way that will facilitate the development of useful and valid inferences about the attributes and capabilities of a potential adversary.

The computer-based link analysis program produces link networks which integrate and summarize adversary information. A link network can be obtained for any selected entity or group of entities in the data base. The network shows the strongest paths of links between the selected entity and all other entities with which it is associated. A sample link network is shown in figure 1; the network was produced for R. GORMAN, suspected head of a potential adversary organization, and shows the paths of links between GORMAN and other entities.

The basic network is provided by the hierarchical structure at the left side of the figure. Entities linked directly to each other are located in adjacent columns. For example, GORMAN is shown linked directly only to SAVIO, OMAKE, and MUNLY. Other than the direct link to GORMAN, OMAKI is shown linked directly only to one other entity—SMIFE. Link paths are defined when both direct and indirect links are considered. For example, GORMAN is linked to BENTZ indirectly through OMAKI and SMIFE.

A special type of entity was included in the sample network; entities of this type are identified with an asterisk in figure 1—*NARCOTICS, *PHYSICS, and *DEMOLITION. They operate like tags to add further information and meaning to the network. In the sample network, for example, they tell the analyst that SAVIO and LA CROIX have criminal records for narcotics trafficking; that BENTZ and WARNELL have skills in physics; and that MUNLY has skills in the use of explosives for demolition. The entities are excluded from the computations by which link paths are generated.

LINK NETWORK FOR /GORMAN, R./ 1 MAY 1978

	LINKTYPE	SOURCE
GORMAN, R. 100		
' SAVIO, S. 92	CONTROL	1055
' ' *NARCOTICS 90	CR RECORD	916
' ' LA CROIX 72	MONEY	76
' ' ' *NARCOTICS 22	CR RECORD	1922
' ' ' TAGER, R. 14	MONEY	674
' OMAKI, M. 86	CONTROL	1196
' ' SMIFE, Z. 61	PO ASSOC	302
' ' ' BENTZ, B. 43	PO ASSOC	550
' ' ' ' *PHYSICS 19	SKILL	1025
' ' ' ' WARNELL, C. 36	PO ASSOC	791
' ' ' ' ' *PHYSICS 22	SKILL	259
' ' ' ' ' RAYBIRD, K. 5	PO ASSOC	812
' MUNLY, D. 98	CONTROL	191
' ' *DEMOLITION 92	SKILL	1072
' ' IRVIG, J. 87	EXPLOSIVES	338
' ' ' FREEBE, M. 43	EXPLOSIVES	334
' ' ' ' CAPSITE CORP. 12	EXPLOSIVES	277

FIGURE 1. *Sample link network.*

The number to the right of each entity is the strength of the link path from the selected entity (GORMAN in the example) and that entity. For example, the strength of the link path between GORMAN and WARNELL is shown in figure 1 to be 36. In calculating path strength, the strengths of the direct links in the path are converted to decimal fractions (74 becomes .74) multiplied and then reconverted to whole numbers. Thus, the path strength calculated from direct link values of 90, 80 and 50 would be 36. Because of the arbitrary basis for their calculation, path strengths have little meaning in an absolute sense; however, they do serve to show the relative strengths of all link paths between the selected entity and all other entities in the data base to which that entity is linked, directly or indirectly.

The two right-hand columns show, for each direct link in the network, the linktype and the serial locator of the information of that link. For example, in figure 1, the direct link between OMAKI and SMIFE is based on a political association (PO ASSOC); the basis for this link can be found in Paragraph 302 of the raw information. Other systems of source identification and location can be employed (file locator, document number and page number). Thus, the link network can direct the analyst to the ultimate information source if a detailed review of the original sources should be required, or should amplification and assessment of specific link paths be desired.

APPLICATION TO SAFEGUARD EVALUATION

Link analysis is employed as a component of several safeguards evaluation techniques which have been developed in recent years. The TRW model (TRW, 1976) uses link analysis techniques to assess the probability of penetration into a facility which is described in terms of a network of grid points. Progress of penetration is monitored from grid point to grid point. The SAI model (Kendrick et al., 1975) defines an exhaustive set of adversary action sequences by enumerating all possible geometric paths (links between safeguards). Computer simulation runs generate probability distributions to estimate the likelihood of adversary success. The Sandia model (Chapman, 1975) uses link analysis methods to abstract a facility into barriers connected by links to represent the optimum paths an attacker can take between barriers. Computer simulations generate data for estimating the potential success of alternative adversary action sequences.

The use of link analysis in the evaluation of safeguards is illustrated here by means of the computer-based link analysis program described earlier. However, it is not suggested that this approach is necessarily representative of the approaches which were taken in the three models just referenced. Link analysis is used in the illustration to identify adversary paths which, if taken, provide the greatest risk to physical security—that is, those paths in which the probability of successful passage through the safeguards is greatest. The algorithm employed makes it possible to calculate path probabilities without the necessity of enumerating all possible paths.

Any facility can be represented by entities (areas within the facility), links (safeguards inhibiting the passage from one area to another) and strength (the probability of successful passage through the link). Then, at the direction of the analyst, path descriptions can be obtained and listed in order of decreasing vulnerability. Also, the analyst can alter the safeguard conditions and determine the impact of these alterations on path vulnerability. For example, through modification of the strength values of one or more specific linktypes, the analyst can assess the impact of changes in the effectiveness of certain safeguards. If an adversary has developed a capability of rendering a specific type of safeguard 50 percent less effective than before, the analyst can quickly assess how this might affect the overall security system.

In the sample path listing presented in figure 2, the analyst obtained a listing for covert escape from the plutonium vault. Paths are listed in the order of their strength from the perspective of an adversary—the path listed first has the highest probability for successful escape (P=.09).

The sample was based on a relatively simple algorithm which can be augmented in several ways. An important augmentation would provide for variation in link strengths as a function of time to permit the incorporation of security force response time, timed locking of doors and windows, and similar defensive reactions. In this manner, success probabilities and path listings could be provided as a function of time.

```
PATH LISTING FOR COVERT ESCAPE

LINK PATHS BETWEEN PLUTONIUM VAULT AND ESCAPE

STRENGTH        PATH

   9            /PLUTONIUM VAULT       /VAULT SIDE PVLT DOOR /
                /COR SIDE PVLT DOOR    /MAIN CORRIDOR        /
                /COR SIDE COR AIR OUT  /P A SIDE COR AIR OUT /
                /PROTECTED AREA        /P A SIDE OF FENCE    /
                /OUTSIDE FENCE         /ESCAPE

   6            /PLUTONIUM VAULT       /VAULT SIDE PVLT DOOR /
                /MAIN CORRIDOR         /COR SIDE LIQ INTAKE  /
                /OUTSIDE LIQ INTAKE    /

   2            /PLUTONIUM VAULT       /VAULT SIDE PVLT DOOR /
                /COR SIDE PVLT DOOR    /MAIN CORRIDOR        /
                /COR SIDE COR AIR OUT  /P A SIDE COR AIR OUT /
                /PROTECTED AREA        /P A SIDE WST EXIT    /
                /WST SIDE EM EXIT      /WASTE + SCRAP TREATMT/
                /WST SIDE LIQ OUTL     /OUTSIDE LIQ OUTLT    /
                /ESCAPE

   1            /PLUTONIUM VAULT       /VAULT SIDE PVLT DOOR /
                /COR SIDE PVLT DOOR    /MAIN CORRIDOR        /
                /COR SIDE SNM REC PT   /REC SIDE SNM REC PT  /
                /SNM REC RM            /CONTROLLED CORRIDOR  /
                /P A SIDE SEC ALARM ST/OUTSIDE SEC ALARM ST /
                /ESCAPE                /
```

FIGURE 2. *Sample path listing.*

IMPLICATIONS FOR BEHAVIORAL RESEARCH

Beyond the immediate value of link analysis techniques for purposes of threat assessment and safeguards evaluation, link analysis provides a structure for highlighting related behavior research needed on physical security problems. These research needs include:

- *Improved link analysis methods.* Many refinements in methodology appear to be possible if some effort were devoted to answering questions such as: What is the best structure of link analysis outputs for defining the attributes and capabilities of an adversary? What is the best way of assigning strength values to links when describing a terrorist organization? How should the time variable be incorporated into safeguard path analysis? How should path strength be computed?
- *Human performance data.* Safeguards evaluation now depends on relatively gross assumptions and estimates about the human performance of both adversaries and defenders. This is particularly true of attack modes involving stealth and deceit. Success probabilities and time requirements for passage through links are largely dependent upon human performance. What is the most useful form of human performance data for link analysis application? What level of precision and detail is required of the data? What methods should be employed for obtaining valid data?
- *Intelligence emphasis.* Because of the limited resources available for intelligence operations, priorities need to be established for collecting and analyzing information on the attributes and capabilities of an adversary. What are the most important linktypes to employ in defining the internal structure of an adversary? What types of entities should be emphasized? What criteria should guide the selection and production of analytical products?

REFERENCES

[1] Channel, R. C. and Tolcott, M. A., Arrangement of equipment. In supplement to *Human factors in undersea warfare.* National Academy of Sciences, National Research Council, Washington, D.C., 1954.

[2] Chapanis, A., *Research techniques in human engineering.* Baltimore: Johns Hopkins Press, 1969.

[3] Fitts, P. M., Jones, R. E., and Milton, J. L., Eye movements of aircraft pilots during instrument landing approaches. *Aeronautical Engineering Review,* **9**, February 1950.

[4] Chapman, L. D., Fixed-site physical protection system modeling. Sandia Laboratories, December 1975.

[5] Gilbreth, F. G. and Gilbreth, L. M., *Applied motion study.* New York: Sturgis and Walton, 1917.

[6] Harper, W. R. and Harris, D. H., The application of link analysis to police intelligence. *Human Factors,* 1975, **17**, 157-164.

[7] Harris, D. H., Development of a computer-based program for criminal intelligence. *Human Factors,* 1978, **20**, 47-56.

[8] Harris, D. H. and Chaney, F. B., *Human factors in quality assurance.* New York: John Wiley and Sons, 1969.

[9] Haygood, R. C., Teel, K. S., and Greening, C. P., Link analysis by computer. *Human Factors,* 1964, **6**, 63-70.

[10] Kendrick, H., et al., Approach to the assessment of safeguards system effectiveness. Science Applications, Inc., December 1975.

[11] McCormick, E. J., *Human factors engineering.* New York: McGraw-Hill, 1970.

[12] TRW. TRW safeguards assessment model. March 1976.

[13] Van Cott, H. P. and Kinkade, R. G. (Ed.), *Human engineering guide to equipment design.* New York: McGraw-Hill, 1972.

AN OVERVIEW OF THE M.A.I.T. ANALYSIS SYSTEM*
(Machine Analysis of the Internal Threat)

Dr. James R. NiCastro

Lawrence Livermore Laboratory, Livermore, California 94550

Dr. B. Woolson and Dr. J. Glancy

Science Applications Inc., La Jolla, California 92138

INTRODUCTION

The M.A.I.T. system is a data analysis system for use by security analysts. The intent of the method is to objectively record and manipulate data. The analysis critically depends on the opinions and insights of the security analyst and the format is constructed to accommodate them.

One of the prime concerns related to the internal threat is the opportunity for collusion among insiders attempting theft or sabotage. The purpose of the present study is to conduct a systematic examination of the issues involved in collusion and the ways that work rules can be structured to reduce the opportunity for adversary activities.

The internal *threat* specifically being addressed involves employees from either the contract security force or the site work force who may or may not be operating in cooperation with an outsider. The *objective* of these adversaries is either theft, diversion or sabotage. In this regard, the safeguards being analyzed are those that function to prevent unauthorized personnel access, to prevent unauthorized Special Nuclear Material (SNM) removal by persons or in equipment and packages, and to prevent introduction to contraband.

The adversary *tactics* specifically being addressed are collusion or the illicit use of access privileges. Other tactics such as force, stealth and deceit are not necessary where authorized access or safeguards control exist. In limiting the scope of these tactics, this study is distinguished from others attempting full evaluations of safeguards effectiveness. Obviously, any full evaluation must consider all tactical options including detailed considerations of force, stealth and deceit. The method uses the following information about the facility and the safeguards system:

Facility Geometry. Site, facility, and floor plans are divided into a suitable mesh size. The facility is then "unfolded" to yield a simpler diagram more useful in safeguards analysis. From this "unfolded" diagram an "adjacency array" is completed. This array defines, for each of the meshes (geometry elements), all units adjacent to it.

Facility Safeguard. All safeguards within the facility are described, their function identified and their location determined. A "safeguards location array" is completed to define all safeguards located at each mesh unit or geometry element. A "safeguards discriminator" is also completed and can be used to select, from the total set of all safeguards, only those that perform a certain function, e.g., detect SNM.

Work Rules (Access and Control). For control over the functioning of the safeguard security and work force personnel are grouped into distinct classes according to their authorization for access. Two separate arrays are then completed. The "safe-guards access" array defines, for each safeguard, the single person(s), or person pair(s) in the event of a two-man rule, authorized access through the safeguard. The "safeguards control" array similarly defines, for each safeguard, the

* Work sponsored by the Nuclear Regulatory Commission and performed at Science Applications Inc.

TABLE 1. *Insider analysis system*

Interview and Analysis Inputs	M.A.I.T. Analysis	Output Assessment
. Facility Description	. Threat Description	. Vulnerability by combinations of personnel for various adversary objectives.
. Safeguards	. Dynamic Path Generation	. Construction of all paths and relevant safeguards.
. Working Rules	. Path related data base of Safeguards	. Examination of all paths for entry combinations of personnel in the facility.
	. Formulation of working rules arrays	
	. Matrix Analysis of vulnerability	

Redesign
. Review working rules associated with identified individuals or groups for which vulnerability exists.
. Redesign working rules to eliminate vulnerability.
. Strengthen critically recurring safeguard elements

person(s) or pair(s) authorized control over the safeguard, whether the control is by operation, inspection, or maintenance.

Application of the method involves three distinct and useful steps: preparation, analysis, and assessment (table 1). The key part of the preparation step is the interview at the facility where the arrays described above are completed. The analysis consists of a computer code that generates all paths or event sequences using the "adjacency array" and "safeguards location array." The code then computes, for each path, the safeguards removed through either access or control by every insider. This step is performed using the "safeguards access" and "safeguards control" arrays. The problem to be analyzed is defined by selecting a starting and ending point for path generation (e.g., outside the facility to inside the vault) and an adversary objective, or conversely, a safeguards function by using the "safeguards discriminator."

The technical approach has been designed to yield the following types of results:

- The event sequences or paths that are most susceptible to collusion;
- The pair(s) of colluding insiders who are the greatest threat because of their access and control authorization;
- Insights into work rules and procedures that can reduce collusion opportunities; and
- Insights into safeguards equipment and equipment operating procedures that can reduce collusion opportunities.

The results are assessed in a stepwise fashion. A summary printout of results shows paths that are completely vulnerable and paths with only a few safeguards remaining. The results are then printed at a more detailed level for each of these paths, showing the insiders who can collude to defeat the safeguards system. Finally, the few safeguards remaining can be identified so that the security specialist can judge the degree of protection remaining. It would be difficult in a short paper to convey all of the detailed procedures in both the construction and the use of the arrays indicated. Central to the success of the method was the reduction of three issues to a form suitable for data processing in a computer code. These issues were:

- A method for recording mathematically the *control* of safeguards and *access* to locations protected by safeguards for any combination of people in the facility.
- A method of *discriminating safeguard* elements as to their intent and function.

- A method of *defining the capability* to be ascribed to the adversaries during any evaluation of the system.

These issues will be highlighted in the subsequent sections. The complete analysis procedures and an application to an existing facility safeguard system have been documented in reports submitted to the Nuclear Regulatory Commission [1].[1]

THE FORMAT OF THE ACCESS AND CONTROL ARRAYS

At the heart of the analysis involving collusion and illicit use of access are the control and access working rules. An effective means of expressing them is required. The use of arrays to accomplish this is done for two reasons:

- When interviewing at a facility and determining the working rules, it presents the security specialists with a simple and comprehensive format.
- The arrays (matrices) are consistent with the overall format of the problem and an enormous amount of specific detail can be easily summarized and manipulated.

There are two separate arrays in the analysis: one for access and another for control. Both, however have the format of the array, as indicated in figure 1. Suppose for discussion there were four employees in the facility labeled P_1, P_2, P_3 and P_4 and five Safeguards S_1 through S_5. Each column of the array is labeled by one of the safeguards. The labeling of the rows is somewhat more complicated. In order to examine the vulnerability of the system under all combinations of individuals P_1 through P_4, the access and control that comes under one and two man rules must be indicated. Functions might be exercised under "higher man rules." In this example, we will presume that there are no access and control working rules involving more than the two man rule. For this case, only single individuals and individual pairs need be considered. Referring again to figure 1, the first four rows are labeled by the four individuals; the subsequent rows are labeled by the various possible combinations of these individuals.

[1] Figures in brackets indicate literature references at the end of this paper.

	S_1	S_2	S_3	S_4	S_5
P_1	1	0	1	0	1
P_2	1	0	1	0	1
P_3	0	1	0	1	0
P_4	0	1	0	1	0
P_1P_2	0	1	0	1	0
P_1P_3	0	0	0	0	0
P_1P_4	1	1	1	1	1
P_2P_3	1	1	1	1	1
P_2P_4	0	0	0	0	0
P_3P_4	1	0	1	0	1

FIGURE 1.

In order to demonstrate how the array is read, a set of 1's is indicated in the figure. Suppose for specificity that figure 1 is the access array. (Control array is interpreted similarly with the phrase *control exercised* interchanged with *access permitted.*) Suppose further the Safeguards S_1-S_5 are applied at locations in the facility to control the flow of personnel. Indeed the safeguard system does more than this and this is discussed under the section entitled discrimination of safeguards. Referring to the figure, P_1 can enter the location controlled by safeguards S_1, S_3 and S_5 by himself. While P_2 can do this, P_3 and P_4 cannot. P_3 and P_4 can be admitted individually to the location controlled by S_4 and S_2. P_1 and P_2 in a two man rule configuration can be admitted to the location controlled by S_2 and S_4. P_1 and P_4 together or P_2 and P_3 together can be admitted under a two man rule configuration to locations controlled by any of the safeguards, through the type of procedure indicated above, two arrays record in simple data format all of the possible combinations of one man, two man or multi-man rules for access and control.

The situation is actually more complicated. Safeguards not only regulate the movement of people but may also regulate the movement of people carrying SNM.

DISCRIMINATION OF SAFEGUARDS

A given safeguard measure in the safeguard system does not necessarily contribute to counteracting every threat. In examining the vulnerability of a safeguard system to a given threat, we must provide some functional method of selecting all system safeguards that are germane to that particular threat. This selection inevitably involves some judgment and opinion. The format of this analysis is completely flexible to accommodate various "opinions." If we do not discriminate safeguards, the facility will appear *less* vulnerable. Thus the use of detailed discrimination results in a more *conservative analysis.*

One objective of the analysis is to construct and test working rules. If working rules are structured to be effective for a subset of discriminated safeguards, they are ipso facto at least as effective for the larger group of safeguards.

In a sense, defining the subset of the safeguards that are pertinent for a particular threat is tantamount to refining the "definition" of the *threat.* Since the definition of words like theft, are analytically *soft,* there is apt to be some discussion as to the meaning of terms.

In this study it is sufficient to separate safeguards into two major categories[2]: regulation of the flow of personnel and materials (table 2). The flow of materials is further subdivided into materials flow linked to personnel and that linked to equipment. Materials are divided into two categories: SNM and contraband or other items. An example of a safeguards measure is indicated in each category. The breakdown is based on the somewhat elementary idea that relevant

TABLE 2. *Safeguards categories*

Regulate Personnel Flow			Regulate Materials Flow			
			Applied to Personnel		Applied to Equipment	
Category	Ingress	Egress	SNM	Contraband & Other	SNM	Contraband & Other
Example Safeguard Measures	ID Badge Sign-in sheet	ID Badge Sign-out sheet	γ- ray scan of person passing	Physical search for a gun	γ-ray scan off a waste barrel	Vehicle search

movement involves personnel and material, and that material must be moved with or by personnel or machine. It is necessary, furthermore, to relate the relevant categories of safeguards to the threats of interest. Table 3 summarizes a set of security analysts opinions about threats and

[2] Further categories can be structured by the analyst if necessary; this simply represents an increase in the size of a matrix.

TABLE 3. *Threat categories*

		Flow of Personnel		Flow of Materials			
		Control of Access		Applied to Personnel		Applied to Equipment	
Category:		Ingress	Egress	SNM	Contraband	SNM	Contraband
Adversary Action	Branch						
Theft	IN	X					
	OUT		X	X			
Diversion	IN	X					
	OUT		X	X			
Sabotage	IN	X					
	OUT						

safeguards. Theft should consider safeguards that *control access* on the In and Out segments[3] (note: this need not be the case if one assumes the thieves decide to depart in a purely overt mode) and regulate the flow of SNM carried by personnel during the out branch. A similar configuration is indicated for diversion. Analysis in the study is not concerned with a pure overt assault that does not utilize insider resources. Thus, for sabotage, ingress safeguards coming under the control of the insiders are relevant.

By using the information in tables 2 and 3 every safeguard in the facility is discriminated as to its relevance for each path segment of every adversary activity threat under consideration. A threat safeguards array can be constructed. It is this array that is used in the analysis. What is relevant is not the "dictionary word designation" for the threat such as "theft," "diversion" or "sabotage" but the subset of the safeguards that are involved in counteracting the threat. Thus, many more threats can be configured than there are reasonable words in the dictionary to define them. It is in this array that alternative opinions by the analyst or security specialists are ultimately best expressed.

Once figure 2 is agreed upon by the security analysts, the user need only specify to the computer the threat (theft, diversion, sabotage), the start point, target point and the finish point. All other items are processed internal to the analysis.

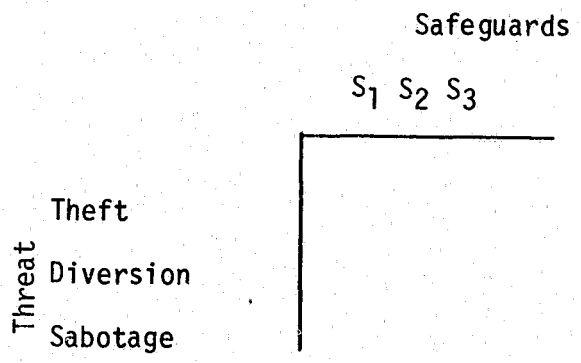

FIGURE 2. *Threat safeguards array.*

[3] Inevitably a personnel or material path is involved in the analysis consisting of an In and Out segment.

THE ADVERSARY CAPABILITY PROBLEM

Within the code segment that computes the vulnerability of the paths to individual collaborators, there exists any number of evaluation options relating to the capabilities to be ascribed to the adversaries, the *runner* (the one who in any pair executes the scenario) and his *accomplice*. The evaluation does not only depend on each pair of colluders, but on what actions are taken by members of the pair. In general, the action can vary from one path segment to the next. In this problem we will distinguish only the *in* and *out* segments. Suppose we are evaluating a path. Let P and Q represent two people (guards or workers), then table 4 summarizes some of the capability options.

What each adversary colluder is capable of contributing to the successful execution of the scenario is his *access capability* and his *control* capability. The question addressed by table 4 involves the possible combinations of capability for each adversary pair P and Q. In table 4 we assume that P executes actively the major *in* or *out* segment and Q is his collaborator.

Option 1 includes the access capability of P, the runner, and the control capability of the accomplice. In Option 2, the access capability contributed is again due to P alone, while the presumed control capability is due to Q under the one man rule and P and Q under any existing two man rules. Option 3 is the maximum control capability of the adversaries and Option 4 is the maximum *total capability*. There are many other capability options that can be ascribed to the adversary. The few options indicated span the range of adversary capabilities and were chosen because of this. Changing them represents no problem or adding new ones presents no difficulty.

The more capability you ascribe to your adversaries, the more conservative the evaluation of the facility will be. We have not stipulated whether P and Q are worker or security force. In terms of the option selections, this is irrelevant since in the code, all combinations of people are analyzed.

The safeguards controlled by the P, Q adversary pair under any option is determined from the facility path analysis and the access and control arrays indicated in the previous section.

TABLE 4

	Access	Control
1	P	Q
2	P	Q+ QΩP
3	Q	P+Q+QΩP
4	P+Q+QΩP	P+Q+QΩP

SUMMARY

The problem of the internal threat epitomized by the tactics of collusion and illicit use of access has been structured into a data processing format. The format procedures and analysis are objective, the flexibility of the method allows the security analyst to input his judgment and opinions into the code. By so doing he can interact and determine the effects of interacting with the safeguard system.

REFERENCES

[1] NiCastro, J., Woolson, B., and Glancy, J., *Internal Threat Analysis* SAI-77-947-LJ.

[2] NiCastro, J., *Application of the MAIT Analysis System(s).* SAI/LJ77:1164.

STRATEGIES OF COUNTER-NUCLEAR TERRORISM: THEORY AND DECISION ON THE FRONTIERS OF LAW ENFORCEMENT AND CRIMINAL JUSTICE

Dr. Louis René Beres

Associate Professor of Political Science, Purdue University, West Lafayette, Indiana 47907

Lenin once remarked: "Without a revolutionary theory, there is no revolutionary practice." The same relationship applies between the theory of counter-nuclear terrorism and effective counter-nuclear terrorism in practice. Without the former, the latter is impossible. Therefore, this paper proposes further research to construct a theory of counter-nuclear terrorism from which viable strategies, should they ever be needed, could be systematically derived.

INTRODUCTION

On August 22, 1977, I submitted a report to the United States Arms Control and Disarmament Agency (ACDA) on the subject of nuclear terrorism.[1] This report, "Terrorism and International Security: The Nuclear Threat," was commissioned by ACDA in April 1977, and represents the product of one summer's research effort. The report identifies effective means of preventing nuclear terrorism (deterrence) and limiting nuclear terrorism if prevention fails (situation management). These means are derived from a rudimentary theory of counter-nuclear terrorism which: (1) is founded upon an awareness of differences between terrorist groups on the balance of risks that can be taken, and (2) correlates deterrent and remedial measures with the characteristic risk calculations of the different types of terrorist groups.

THE NEED FOR FURTHER RESEARCH

With these facts in mind, this paper proposes further research to refine and expand this theory with particular reference to the construction of a decision-making taxonomy suitable for use by policy-makers in crisis or pre-crisis situations. This taxonomy, in which strategies of counter-nuclear terrorism would be differentiated according to the particular category of risk-calculation involved, could provide a rationally-conceived behavioral technology for dealing with terrorist nuclear threats.

The need for such a behavioral "technology" is underscored by the following two points: (1) the central task of effective counter-nuclear terrorism lies in distinguishing contingencies of reinforcement according to the particular type of terrorist group in question, and (2) at the present time, scholars and policy-makers continue to expend all of their efforts on the search for a mechanical "fix" to the prospect of nuclear terrorism, with no concern for the truly crucial *behavioral* aspects of the problem. Nuclear terrorism cannot be prevented solely by additional guards, higher fences, and other protection devices. Sooner or later, a determined terrorist group will be able to by-pass these measures and gain access to fissionable materials, assembled nuclear weapons, or nuclear power plants. What *can* work to prevent nuclear terrorism (or at least offer *some* hope of successful deterrence) are strategies that are directed toward affecting the behavior of terrorists. The search for such differentiated strategies defines the theoretical and public-policy "core" of the needed research.

[1] Nuclear terrorism is defined as the use of nuclear explosives, radiological weapons, or nuclear reactor sabotage by insurgent groups.

WHY STRATEGIES OF COUNTER-NUCLEAR TERRORISM? RATIONALE OF THE NEEDED RESEARCH

From the end of the eleventh century, when a Muslim sect known as the Assassins (a translation from *Hashishaya*) willingly sacrificed their own lives in pursuit of what they considered to be righteous and salvation, special difficulties have been involved in dealing with terrorists. Not until very recently, however, have these difficulties entailed the prospect of nuclear catastrophe. Today, the failure of counter-terrorist strategies can give rise not only to locally destructive acts of rage and violence, but to enormously damaging events triggered by nuclear weapons.

The reason for this state of affairs lies largely in the fact that the ability to acquire and use nuclear weapons has now passed into the hands of private individuals and groups. Coupled with the orientation to violence of terrorists, their relative insensitivity to orthodox threats of deterrence, and the growth of inter-terrorist cooperation, this ability signals a perilous drift toward nuclear insurgency. A brief look at this situation follows. *A detailed explanation of these four factors which, taken together, suggest a compelling need for the proposed research can be found in Appendices A and D.*

PRECIS OF THE PROBLEM

° The increasingly easy access of terrorists to nuclear weaponry (either by theft of assembled systems from military stockpiles or by self-development from plutonium that has been pilfered from nuclear power plants) and nuclear reactors.

Compelling evidence now exists that nuclear weapons storage areas can be penetrated successfully; that fissionable materials needed for the fabrication of fission bombs or radiation dispersal devices are inadequately protected; that the design and manufacture of a highly-destructive nuclear weapon is no longer a difficult task technically; and that sabotage of nuclear reactors can be accomplished.

° The indiscriminate use of violence by terrorists.

Today's terrorists are *sui generis* in one important respect: they no longer operate according to a code which defines a sense of proportionality in the use of force, or which distinguishes between combatants and non-combatants. Viewed from the standpoint of nuclear terrorism, the random exercise of unrestrained violence suggests that the amount of suffering to be inflicted is limited only by the availability of weapons resources.

° The relative insensitivity of terrorists to ordinary retaliatory threats.

Today's terrorists are typically insensitive to threats of retaliatory destruction, either because of the preeminent value which they attach to certain goals, or because of the difficulty that is involved in locating them. As a consequence of this insensitivity, the essential dynamics of deterrence that lie at the heart of international security processes are immobilized. They do not work. From the standpoint of the threat of nuclear terrorism, this suggests that where diplomatic forms of persuasion prove useless, strategies of preemption may have to be taken seriously.

° The trend toward growing cooperation among terrorist groups.

Today's terrorists are engaged in increasingly high levels of intergroup cooperation. The implications of such cooperation for nuclear destruction by terrorists are at least four in number: increased opportunities for acquiring nuclear weapons; the proliferation of "private" nuclear weapons throughout the system; the spread of expertise in handling nuclear weapons; and the growth of reciprocity in such areas as forged documents and safe havens.

PHASES OF THE NEEDED RESEARCH

To create the decision-making taxonomy, I propose the following two basic phases of research:

Phase I

An in-depth exploration of the six critical conditions which determine terrorist stance on the balance of risks that can be taken in pursuit of particular objectives. These conditions are as follows:

- Terrorist perceptions of the utility of nuclear violence.
- Terrorist alignments with states.
- Terrorist alignments with other terrorist groups.
- Terrorist receptivity to positive cues or sanctions as opposed to negative ones.
- Terrorist perceptions of patterns of counter-terrorist cooperation among states.
- Terrorist perceptions of sympathy and support from others in the *intra*national and *inter*national milieu.

PRINCIPAL RESEARCH QUESTIONS

To accomplish the proposed exploration of these six basic conditions, the research must address the following principal questions:

- To what extent, if any, are the risk-calculations of terrorist actors affected by the belief that increasingly-destructive modes of insurgency are gainful (i.e., in their own best interests)? In this connection, special attention must be directed toward understanding ways in which such a belief might be reversed.

  Historically, many violent acts of terrorist groups have alienated popular support and been counter-productive to political objectives. As examples, we may point to the Stern Gang (especially the murder of Lord Moyne in Cairo in 1944, which inspired the Jewish Agency to launch a counter-terrorist campaign); the *Front de Liberation Quebecois,* FLQ (especially the killing of French-Canadian Cabinet Minister LaPorte); the Malayan Terrorists of the 1950's; the OAS in Algeria; the Turkish People's Liberation Army; the U.S. Weathermen; and the Netherland's South Mollucan terrorists.

  It is worth pointing out, however, that the practice of terror and cruelty can occasionally elicit support and admiration as well as revulsion. In writing about the history of bandits, for example, Eric Hobsbaum has indicated that bandits have often become heroes not in spite of their terrible cruelty (cruelty, incidentally, beside which some examples of modern terrorism pale into insignificance), but *because of it.* The hero image stems not from their presumed ability to right wrongs, but to *avenge.* In describing the Colombian *violencia* during the peasant revolution of the years after 1948, Hobsbaum points out that bandits who chopped prisoners into tiny fragments before whole villages and ripped fetuses from pregnant women became instant heroes to the local population [15].[2]

  What this suggests, from the point of view of effective counter-nuclear terrorism, is that the ability to convince terrorist groups that nuclear violence is apt to be self-defeating may be impossible in certain contexts. In such cases, where resort to nuclear terror may actually generate admiration and support, efforts to prevent this terror must center on the other bases of deterrence.

[2] Figures in brackets indicate literature references at the end of this paper.

° To what extent, if any, are the risk-calculations of terrorist actors affected by alignments with state actors? And how, therefore, can we use what we know about such effects to devise an effective counter-nuclear terrorist strategy?

It would appear that such alignments encourage terrorist inclinations to nuclear violence in two ways: (1) by direct assistance from state allies, in the form of weapons, material aid, and safe havens; and (2) by the progressive alteration of international power configurations in favor of terrorist actors.

° To what extent, if any, are the risk-calculations of terrorist actors affected by geographic dispersion among, the intermingling with, state actors? Since terrorists do not occupy a piece of territory in the manner of states, they are not susceptible to orthodox threats of deterrence. The proposed research, therefore, must examine how effective counter-nuclear terrorist efforts might be reconciled with the reality of geographic dispersion.

Terrorist intermingling with state actors may (1) give rise to alignments between states that are dedicated to counter-terrorist purposes; (2) inhibit the formation of contemplated alliances where split sympathies between states are in evidence; or (3) fractionate existing alignments that are cross-cut by such a split. While the first possibility would appear to put a damper on terrorist adventurism, the other two possibilities seem fraught with opportunity for terrorists to wreak havoc with impunity. In this connection, it is important to point out that the effects of the second and third possibilities could conceivably include some fundamental realignments of power between states; indeed, they might produce a genuinely realigned global structure.

° To what extent, if any, are the risk calculations of terrorist actors affected by their relations with "host" states? Since terrorist actors operate within the framework of individual states, the character of the relationship between "visitor" and "host" may affect the viability of counter-nuclear terrorist measures. The proposed study, therefore, must ask: How might we exploit what is known about such relationships in curbing the threat of nuclear terrorism?

Terrorist groups, of course, do not occupy a piece of territory in the manner of states, but necessarily operate from within states. Where the targets of terrorist attacks are located within their own states (*intra*national insurgency), the terrorist organization is anathema to its own government and enjoys no protection from the principle of sovereignty. However, where the terrorist target is located within another state (*inter*national insurgency), it may enjoy both the blessings of its "host" state and safety from acts of retaliation.

The effect of the second condition, i.e., terrorist targets located in other states combined with a supportive host state, is to embolden terrorist behavior. Here, since counter-terrorist measures necessarily require infringements upon the sovereignty of host states, these measures inevitably impinge upon delicate international legal concerns. Hence, unless the target states of terrorists are willing to turn their backs on legal/jurisdictional niceties, and initiate pre-emptive or retaliatory strikes on terrorist bases, it is these states—rather than the terrorists—who are put on the defensive.

° To what extent, if any, are the risk-calculations of terrorist actors affected by their relations with other terrorist groups? And how might we exploit what we know about such ties to devise an effective strategy of counter-nuclear terrorism?

Some of the evidence here is genuinely startling. Links have now been established between such groups as the various Palestinian organizations, the Tupamaros, the FLQ, the IRA, the Basque Liberation Front, the Baader-Meinhof group, the Turkish Popular Liberation Front, and the Japanese Red Army. Occasionally, joint operations are staged, as was the case with the Lod Airport Massacre in May 1972, which was carried out for the PFLP by Red Army Agents that had received training in Syria.

° To what extent, if any, might the decisional calculations of terrorist actors be receptive to positive cues or sanctions as opposed to negative ones, and exactly which rewards seem to warrant consideration? In this connection, special attention must be directed to studies of child rearing, which indicate with overwhelming regularity that positive sanctions (rewards) are generally far more effective than negative ones (punishment).

The reasonableness of such a strategy is also enhanced by its probable long-term systemic effects. Just as violence tends to beget more violence, rewards tend to generate more rewards. By the incremental replacement of negative sanctions with positive ones, a growing number of actors in world politics, terrorists as well as states, are apt to become habituated to the ideology of a reward system, and to disengage from the dynamics of a threat or punishment system. The cumulative effect of such habituation is likely to be a more peaceful and harmonious world and national system.

Some of the problems associated with such a strategy in a world system founded upon the principles of *realpolitik*—problems to be dealt with in the proposed research—concern the appearance of "bribes." Even if a strategy of positive sanctions is worked out that looks exceptionally promising, the public reaction to it may be exceedingly unfavorable. Matters of honor and courage, therefore, may mitigate against the operation of positive sanctions in counter-nuclear terrorist strategies.

Another problem associated with the operation of positive sanctions in such strategies centers on the possibility that some terrorists who display the self-sacrificing value system of *Fedayeen* thrive on violent action for its own sake. They are unconcerned with the political object or matters of personal gain. Here, we are up against a brick wall, the *reductio ad absurdum* of deterrence logic, since the only incentives that might be extended to deter acts of violence are the opportunities to commit such acts.

And then there is the "blackmail" problem. The habitual use of rewards to discourage terrorist violence is apt to encourage terrorists to extort an ever-expanding package of "gifts" in exchange for "good behavior." Here, we must confront the prospect of terrorism as a "protection racket" on a global scale.

° To what extent, if any, are the risk-calculations of terrorists affected by inter-state patterns of counter-terrorist cooperation? And how, therefore, might such patterns be created? In principle, the surest path to success in averting nuclear terrorism lies in a unified opposition by states to terrorist activity. Yet, at least in the immediate future, this kind of opposition is assuredly not forthcoming. It is sometimes argued that an effective international agreement among all states to combat terrorism is practicable, since all states share a common interest in obstructing terrorism. This argument rests on the mistaken assumption that all states will always value the proper functioning of the international diplomatic system more highly than any other preference that might be obtained through terrorist activity. It is, therefore, an erroneous and dangerous argument, very much like the argument that all states will agree to halt the proliferation of nuclear weapons since it is clearly in their common interest to do so. Regrettably, everything that is known about the *realpolitiker's* paradigm of foreign policy behavior mitigates against accepting the assumption that states will risk significant cooperative ventures in an anarchic world system. The proposed study, therefore, must ask: What cooperative patterns between *particular* states can cope with the problem at hand?

In this connection, special attention must be directed toward such options as exchange of intelligence data concerning terrorist groups; bilateral agreements on extradition; mutual judicial assistance concerning acts of terrorism; multilateral infiltration of terrorist organizations to gather information; improved border checks; expanded use of the media to publicize terrorist inclinations and inter-group ties; and separate negotiations with selected groups to fractionate their bonds and atomize their operations. International cooperation could also take the form of highly limited and particularistic

acts, e.g., the willingness of Kenya to allow Israeli planes to refuel during the Entebbe mission, and the assistance of three ambassadors from Moslem states during the Hanafi Moslem siege of Washington, D.C. in March 1977.

° To what extent, if any, are the risk calculations of terrorist actors affected by the degree to which their policies evoke sympathy and support from others? Since almost all acts of terror are essentially propagandistic, it is important to understand their desired effects on selected publics in order to prevent escalation to a nuclear option.

Sympathy and support of terrorist groups in the international community suggests an opportunity for such groups to increase their strength and step up their activities with minimal fear of interference. Unless the trend toward such support is quickly and surely altered, it will certainly convince terrorists that policies of violence will be rewarded rather than punished.

SUMMARY OF PRINCIPAL RESEARCH QUESTIONS

By considering these basic questions, the proposed research can begin the search for a "behavioral technology" to reduce the chances of terrorist nuclear violence. As with all other groups of human beings, terrorists acquire a repertoire of behavior under the particular contingencies of reinforcement to which they are exposed. The "trick" is to understand this repertoire and to use it to inform the differential reinforcement of alternative courses of action. Once this is done, the spectre of nuclear terrorism can be confronted with counter-measures that are grounded in a systematic body of theory.

SUMMARY OF PHASE I METHODOLOGY AND RESEARCH STRATEGY

The proposed Phase I research must be informed by hypotheses that represent tentative explanations of the eight principal research questions. These hypotheses must link the risk-calculations of terrorist actors (as dependent variables) to corrective steps (as independent variables) which might be expected to affect these calculations. To investigate these hypotheses, a number of appropriate analytic models must be created wherein the stipulated connections that are presumed to obtain between independent and dependent variables can be explored. In effect, these analytic models would represent different configurations of world policy processes which vary according to the precise pattern of remedial steps involved.

Paralleling the major research questions and their respective hypotheses, these models must focus upon such policy processes as the following: steps to convince terrorist actors that nuclear violence would generate broad-based repulsion rather than support; steps to curtail "heterogeneous" alignments between terrorist and state actors; steps to discourage states from offering "hospitality" to terrorist actors within their borders; steps to fractionate bonds between terrorist groups; steps to develop strategies of "positive sanctions" to apply to terrorist actors; steps to create workable patterns of counter-terrorist cooperation between states; and steps to impair sources of public sympathy and support for terrorist excesses.

The mode of investigation must reflect strict adherence to the basic canons of empirical-scientific inquiry. This means that conclusions about the dependent variables must be derived in conformity with the requirements of logical consistency, and that the value-maximizing properties of the models must be rigorously deduced before they are subjected to the tests of correspondence with empirical materials.

After the analytic models have been suitably explored Phase II study must get underway, and recommendations must be offered for the consideration of policy-makers. In arriving at these recommendations, attention must be directed to both the desirability and feasibility dimensions of the proposed remedies. This two-part concern derives from the understanding that the chances for implementation of particular strategies define a criterion of reasonableness that is every bit as important as the inherent attractiveness of these strategies.

Phase II

This phrase seeks to develop a decision-making taxonomy which rests upon the findings of Phase I research, and which differentiates strategies of counter-nuclear terrorism according to the particular category of risk-calculation involved.

To accomplish such development, I propose the identification of six principal types of terrorist group according to the group's position on two primary dimensions: (1) Degree of Commitment to Political Objectives, and (2) Utilization of Criminal Tactics (i.e., robbery or "expropriation" to secure funds).[3] Since the first dimension would have three possible forms (High, Moderate, or Low) and the second dimension would have two possible forms (Criminal or Non-Criminal), six basic types of terrorist group would be considered. Each type would display a distinctive stance on the balance of risks that can be taken in pursuit of particular preferences.[4] The following chart lists the six basic types of terrorist group that would be used in the decision-making taxonomy:

Group type	Degree of commitment	Utilization of criminality
1	High	Non-criminal
2	High	Criminal
3	Moderate	Non-criminal
4	Moderate	Criminal
5	Low	Non-criminal
6	Low	Criminal

These six types range from what might be termed "pure altruism" (Group Type Number 1) to what comes very close to being "pure criminality" (Group Type Number 6). Psychopathic or nihilistic terrorism can fall under the heading of either Group Type Number 5 or Group Type Number 6. To create the decision-making taxonomy from these six basic types of terrorist group, I propose (1) an exploration of the various forms of counter-nuclear terrorist strategy that appear appropriate to each particular type. The resultant decision-making taxonomy would represent a theoretically-informed plan that correlates each of the six group types with a highly-detailed set of recommendations and prescriptions. *A detailed summary of these six terrorist group types can be found in Appendix B.*

To clarify these proposed operations of Phase II research, let us very briefly consider Group Type Number One. This type of terrorist group is characterized by a high degree of commitment to political objectives and by an absence of criminal activity. Hence, the self-sacrificing value system of *Fadayeen* is in evidence, and the group does not secure needed funds through "expropriatory" activities.

In view of the particular ordering of preferences associated with this particular type of terrorist group—an ordering which assigns far greater value to political objectives than to personal safety—the task would be to identify and probe a range of deterrence options that focuses upon threats to obstruct political objectives. Such options would include: (a) ways of convincing the group that its resort to nuclear violence would mitigate against political objectives because such violence would stiffen incumbent resolve and alienate vital bases of popular support, and (b) the use of positive sanctions, whereby certain rewards or concessions which relate to political objectives are promised in exchange for the non-use of nuclear violence. The possible use of positive sanctions has been left out of existing studies of counter-terrorism; yet, it might prove to be one of the most worthwhile ways of affecting the decisional calculations of terrorist groups.

[3] While all terrorist groups are, of course, "criminal" in the broad meaning of the term, as it would be used in the proposed taxonomy that term would apply to only *ordinary* criminal tactics used to secure funds. Hence, groups that do not utilize such ordinary tactics would be characterized as "non-criminal."

[4] With the introduction of a number of "intervening variables" into the basic types or models (e.g., group types utilizing ordinary criminal tactics could be subdivided according to *particular forms* of such tactics), several subsidiary types of terrorist group could also be considered.

Indeed, since we now live in a world wherein the execution of certain terrorist threats could have genuinely calamitous effects, responsible authorities can no longer always afford to take a hard line position against making concessions. Such concessions, however, should be based upon a systematically-formulated hierarchy of concessions that has been worked out in advance of a particular incident or crisis, rather than upon ad hoc judgments. Recognizing this, the proposed study must include the development of a such a hierarchy, ranging from the most easily satisfied financial demands to the most sweeping transformations of government policy and personnel. With such a hierarchy in hand, responsible officials could enter into a protracted bargaining situation with prospective nuclear terrorists, pursuing a concessionary policy that is consistent with predetermined calculations of tolerable losses.

In reference to the investigation of the other five group types, the proposed research must also focus upon deterrence options that involve: (c) ways of exploiting the ordinary criminal characteristics of certain terrorist groups; (d) threats of mild punishment[5]; and (e) orthodox threats of physically punishing retaliation. Where a particular group type is expected to value the violent act itself more highly than any alleged political goals, strategies of "prophylaxis" must be examined together with deterrence measures. Here, however, special attention must be directed to the possible effects of such preemption strageties on essential human and citizen rights, since the requirements of effective counter-nuclear terrorism strategies must always be tempered freedoms. *A detailed explanation of the threat to civil liberties posed by certain strategies of counter-nuclear terrorism can be found in Appendix C.*

CONCLUSION

Taken together, Phases I and II of the needed research define a coherent plan for (a) increasing our understanding of the threat of nuclear terrorism, and (b) identifying differentiated strategies of prevention and response that are organized into a set of theoretically-informed, yet specific, policy recommendations. At the present time, students of the problem of nuclear terrorism continue to expend almost all of their efforts on the search for a technological "fix" to what is inherently a social-psychological and political problem. The research that is recommended in this paper would shift scholarly and governmental attention to the essential *behavioral* underpinnings of the problem, and provide a theory of counter-nuclear terrorism from which viable strategies could be systematically derived. In this way, the needed research would contribute to the improvement of national and international security through the power of theoretical and policy-relevant scholarship.

[5] Threats of mild punishment may have a greater deterrent effect than threats of severe punishment in certain instances. From the vantage point of the terrorist group's particular baseline of expectations, it would appear that such threats may prove less likely to elicit the high levels of anger and intractability than can impair rationality and override the inhibiting factor of expected punishment. Moreover, threats of mild punishment may be less likely to support the contention of official repression—a contention that is often a vital part of terrorist group strategies.

APPENDIX A—Factors Which Suggest a Compelling Need for Counter-Nuclear Terrorism Research

1. *Terrorist Access to Nuclear Weapons*

Terrorists can now gain access to nuclear weapons either by theft of assembled systems from military stockpiles and production facilities or by self-development from pilfered nuclear materials. To acquire an assembled weapon, terrorist operatives might direct their attention to any one of the tens of thousands of nuclear weapons now deployed across the world in national arsenals. In the future, such terrorists are likely to have a significantly enlarged range of possibilities for stealing nuclear weapons. This is the case because the number of national members in the so-called "Nuclear Club" is growing steadily.

To fashion their own weapons from basic nuclear materials, terrorist groups would require both the materials and the expertise to create an explosive device or radiation dispersal implement. However, it would not be difficult for them to fulfill these requirements since increasingly large amounts of fissionable materials are being produced by the nuclear power industry, thus, providing the terrorists the opportunities to exploit the manifestly catastrophic skyrocketing possibilities that lie dormant in nuclear fuel.

How difficult would it be for terrorists to actually get their hands on fissionable materials? According to Mason Willrich and Theodore Taylor, co-authors of a special report to the Energy Policy Project of the Ford Foundation, the extant system of safeguards in this country is so inadequate that it is only a matter of time before terrorists are able to surreptitiously remove the essential fissionable materials from nuclear power plants [23]. Although significant improvements in American safeguards have taken place since this appraisal was offered, parallel improvements have not always been implemented abroad. This situation has portentious overtones since American safeguards do not secure us against nuclear weapons fashioned from materials stolen elsewhere. To be genuinely worthwhile, the protection of nuclear materials from terrorist groups must be *global* in scope.

Regrettably, the amount of fissionable materials present in other countries which might become the target of terrorists is likely to expand at an alarming rate. Together with India's manufacture of a nuclear device with technology supplied by Canada, the West German-Brazilian and French-Pakistani deals involving pilot reprocessing plants to extract weapons grade plutonium from spent reactor fuel rods and the continuing development of fast-breeder reactor plants by Japan, the Soviet Union, France and West Germany signal very dangerous conditions. Unless immediate and effective steps are taken to inhibit the spread of plutonium reprocessing and uranium enrichment facilities to other countries, terrorist opportunities to acquire fissionable materials for nuclear weapons purposes will reach very high limits.

To fabricate its own nuclear weapons, a terrorist group would also require expertise. According to Willrich and Taylor, "The design and manufacture of a crude nuclear explosive is no longer a difficult task technically, and a plutonium dispersal device which can cause widespread radioactive contamination is much simpler to make than an explosive."[6] Since as early as 1954, declassification and public dissemination of information about the design of fission weapons has been extensive. As a result, such widely-publicized cases as the one involving the 20-year-old MIT undergraduate who put together a devastatingly accurate technical design for a nuclear explosive—a case documented in the NOVA science series on public television, March 9, 1975—assume a high degree of credibility.[7]

[6] A crude nuclear explosive made from pilfered plutonium would probably have a yield in the range between several hundred and several thousand tons of high explosive. If such an explosive were detonated in a crowded metropolitan area, as many as 10,000 people might be killed directly while tens of thousands might suffer severe fallout problems (also see reference number 24).

[7] More recently, there is the case of the 21-year-old undergraduate physics major at Princeton, John A. Phillips, who designed an atomic bomb in four months with information obtained entirely from public documents. The point of his design, said Phillips, "was to show that any undergraduate with a physics background can do it, and therefore that it is reasonable to assume that terrorists could do it, too." (See also reference number 20.)

The fact is that such cases are not really all that remarkable. According to Willrich and Taylor:

> Under conceivable circumstances, a few persons, possibly even one person working alone, who possessed about ten kilograms of plutonium oxide and a substantial amount of chemical high explosive could, within several weeks, design and build a crude fission bomb. By a "crude fission bomb" we mean one that would have an excellent chance of exploding, and would probably explode with the power of at least 100 tons of chemical high explosive. This could be done using materials and equipment that could be purchased at a hardware store and from commercial suppliers of scientific equipment for student laboratories.[25]

What would happen if such a bomb were made and exploded? Since a nuclear explosion yields deadly penetrating radiations (gamma rays and neutrons) as well as blast wave and heat, even a "small" nuclear weapon could generate terrible destruction. Consider the following examples provided by Willrich and Taylor:

> A nuclear explosion with a yield of ten tons in the central courtyard of a large office building might expose to lethal radiation as many as 1000 people in the building. A comparable explosion in the center of a football stadium during a major game could lethally irradiate as many as 10,000 spectators. A nuclear explosion with a 100-ton yield in a typical suburban residential area might kill perhaps as many as 2000 people, primarily by exposure to fallout. The same explosion in a parking lot beneath a very large skyscraper might kill as many as 50,000 people and destroy the entire building.[20]

A terrorist group might also choose to use its plutonium in the form of a radiation dispersal device. In this case, the plutonium would be transformed into an aerosol of finely divided particles that could be distributed uniformly into the intake of a large office building's air conditioning system. According to Willrich and Taylor, only three and one half ounces of this extraordinarily toxic substance (its toxicity is at least 20,000 times that of cobra venom or potassium cyanide) would pose a lethal hazard to everyone in such a building.

How would such a weapon work? Consider the following scenario:

> A criminal or terrorist group distributes only three and one half ounces of plutonium aerosol into the air-conditioning intake system of a large downtown office building. Such a small amount could prove a deadly risk for all of the occupants. Death by lung cancer would probably come to anyone inhaling between ten and one hundred *millionths* of a gram. Death due to fibrosis of the lung would be the probable fate of those who retain a dose of about a dozen *thousandths* of a gram.[25]

What makes this scenario particularly macabre is that the building occupants who absorb lethal but not massive doses of plutonium might not know of their poisoning for weeks, or months, or perhaps even years. One can only imagine the reaction of thousands of office workers to the disclosure that they have been lethally irradiated. The concrete human implications, the social and economic dislocations, and—last but certainly not least—the political implications are staggering.

Plutonium might be dispersed in still other ways. One scenario that has been considered at the Nuclear Regulatory Commission office in Washington, D.C. is described as follows:

> During what appears to be a normal day at the Pacific Coast Stock Exchange, a large beaker filled with boiling liquid is noticed in the window of a nearby hotel. Police investigate, but it is too late. The boiling acid in the beaker has been dissolving and dispersing half a pound of plutonium, enough to expose everyone within several city blocks to a high risk of lung cancer.[17]

Rather than use plutonium for nuclear explosives or radiation dispersal, terrorists might also find it agreeable to sabotage nuclear plant facilities. Such sabotage could yield extensive death and

property damage via radiation release. Although the chances of accidental reactor meltdown are generally believed to be extremely small, the case is quite different with respect to deliberate reactor meltdown. Consider the following scenario, another in the collection of the Nuclear Regulatory Commission's Office of Nuclear Material Safety and Safeguards:

> Under the cover of night a dozen men storm the gates of a nuclear power plant, killing the two guards and taking the operating staff hostage. After placing charges of high explosives next to the plant's critical cooling systems, they phone the mayor of a nearby large city. Send $5 million, they demand, or we will blow the plant, sending radioactive particles drifting over the city's neighborhoods.[19]

Such acts could pose monumental problems for the appropriate authorities. Although a great many steps have already been taken to diminish the vulnerability of nuclear power plants in this country, successful sabotage is certainly not out of the question. By penetrating the physical barriers between themselves and the fission material in the reactor, and by disabling the cooling systems to the reactor core, saboteurs could cause the reactor to melt through its protective shielding and release deadly radioactivity into the atmosphere. Alternatively, since today's nuclear plants are unable to withstand the impact of large aircraft, a kamikaze-type plane crash into a nuclear plant could create a calamitous reactor core meltdown. Comparatively speaking, however, it would be more difficult for terrorists to "pulse" a nuclear reactor core to destruction than to make a radiological weapon or crude fission bomb.

2. *Terrorist Orientations to Violence*

Today's terrorist groups typically share an orientation to violence that has been shaped largely by the preachings of Bakunin, Fanon, and Sorel. All too frequently, these groups operate without a code of honor that distinguishes between combatants and non-combatants. As a result the imperative to create limits to violence is ignored, and terrorist anger is vented almost randomly. At the same time, the level of adopted violence is constrained only by the limits of available weaponry. These facts imply an unacceptably high probability of nuclear terrorism should access to weapons or power plants be realized.

To a certain extent, this orientation to violence stems from the conviction that the absence of inhibitions to apply maximum force to virtually any segment of human population is expedient. Since war is still the *ultima ratio* between states, so, it is argued, must internal war be the final arbiter within states. Such "gun-barrel" thinking is often taken as an adaptation from the aphoristic philosophy of Mao Tse-tung.

To another extent, this orientation derives from the romanticization of violent action exemplified by Bakunin's dictum that "The passion for destruction is a constructive passion." Fused with the categories of Sorel and Fanon, and the existential idea of Sartre that "irrepressible violence. . . is man recreating himself," such romanticization breeds a cathartic view of violence. The *reductio ad absurdum* of this view is the slogan of the Spanish Civil War, "*Viva la Muerte.*"

Finally, today's terrorist orientations to violence stem, in part, from the presence of psychopaths and sociopaths who enjoy carnage for its own sake. Here, the complete inversion of Judeo-Christian notions of conscience and compassion flows not from any means-end calculation or from devotion to the "creativity" of violence, but from a purely psychotic motive. Where such a motive is present among terrorists who are suicidal schizophrenics, the problems of effective counter-terrorist action are greatly exacerbated. This is the case because terrorists—whose incentive is to use violence nihilistically rather than politically—are apt to regard the threat of death as a stimulus rather than as a deterrent.

As we have just seen, the viability of deterrent threats against terrorist actors may be undermined when these actors are impelled by psychotic motive. It must now be pointed out that the ability to deter violent behavior by terrorists is in doubt with *all* categories of terrorist, including those whose actions spring from purely political concerns. Since a great many modern terrorists place a higher value on the achievement of certain political and social objectives than

they do upon their own lives, these groups are essentially insensitive to orthodox threats of retaliation. Faced with an international actor for whom the "deadly logic" of deterrence is immobilized, states bent upon an effective counter-terrorist stragegy are at a significant disadvantage.

Consider the following examples of terrorist "rationality":

- Arab terrorists, in April 1974, seized an apartment building in Northern Israel, and ultimately accepted death rather than capture.
- SLA members, during the widely-publicized California shoot-out in May 1974, preferred death to incarceration.
- Two Red Army terrorists, during their attack on Israel's Lod International Airport in May 1972, killed themselves.
- Holger Meins, of the Baader-Meinhof group, succumbed to self-inflicted starvation in 1974.

What are the implications of this particular behavioral characteristic of terrorist actors for the threat of nuclear terrorism? Quite plainly, the most significant implication is that should terrorists obtain access to nuclear explosives or radioactivity and calculate the prospective costs and benefits of use, the fear of retaliatory destruction might not figure importantly in this calculation. In effect, this means that traditional threats of deterrence might have little or no bearing on the terrorist decision concerning the use of nuclear force.

It follows that unless diplomatic or other forms of persuasion can prove successful, the only means left to prevent the threatened nuclear act would be a "surgical" or pre-emptive strike. In certain instances, of course, even this option might prove inappropriate or ineffectual.

3. *Cooperation Among Terrorist Groups*

- Venezuelan terrorist Illich Remirzed Sanchez receives weapons training from the P.F.L.P. in Lebanon.
- Members of the Japanese Red Army terrorist group receive weapons training in Lebanon.
- Joint training programs and arms transfers take place between the Turkish People's Army and Black September.
- Members of the American Weathermen, Northern Ireland's IRA, and Nicaragua's *Tandanista* movement are trained in Palestinian camps.
- Black September operatives demand the release of German insurgents who had been involved in the killing of German policemen.
- Liaison between P.F.L.P. and Japanese Red Army agents produces the Lydda Airport massacre; an attack on the American Embassy in Kuala Lumpur, Malaysia; the hijacking of a JAL flight; an assault on the Japanese Embassy in Kuwait; and a takeover of the French Embassy in The Hague.

These are only a few of the most glaring examples of a new phenomenon in world politics—systematic cooperation and collaboration between terrorist groups. Terrorists have always formed alignments with sympathetic state actors, but they are now also beginning to cement patterns of alliance and partnership with each other. The net effect of such behavior patterns is a mirror image of Trotsky's theory of "permanent revolution."

From the standpoint of nuclear terrorism, cooperation between terrorist groups is particularly ominous. Such cooperation greatly facilitates terrorist acquisition of nuclear weapons and their exchange between different groups. It also increases the prospect of shared expertise in the technology of nuclear destruction and enlarges the opportunity for reciprocal privileges which might be crucial to successful operations.

APPENDIX B—Summary of Terrorist Group Types

Group type	Degree of commitment	Utilization of criminality
1	High	Non-criminal
2	High	Criminal
3	Moderate	Non-criminal
4	Moderate	Criminal
5	Low	Non-criminal
6	Low	Criminal

Group Type No. 1

This type of terrorist group is characterized by a high degree of commitment to political objectives and an absence of criminal activity.[8] Here the self-sacrificing value-system of *Fedayeen* is in evidence, and the group does not secure needed funds through "expropriatory" activities. In view of the particular ordering of preferences associated with this type of terrorist group—an ordering which assigns much greater value to political objectives than to personal safety—it would appear that the deterrence efforts should focus upon threats to obstruct political objectives.

Such threats must be directed at convincing the group that its resort to nuclear violence would mitigate against political objectives because it would both stiffen incumbent resolve and alienate vital bases of popular support. Deterrence might also be based upon a strategy of positive sanctions,[9] in which certain rewards or concessions which relate to political objectives are promised in exchange for the non-use of nuclear or higher order weapons technologies. Prior to the advent of concern for nuclear acts of terrorism, the idea that governments would engage in substantive bargaining with terrorists which might lead to major concessions was widely criticized. Today, however, we must face up to the fact that the execution of certain terrorist threats could have genuinely system-destructive effects. Recognizing this, the "hard line" unwillingness to bargain and concede can no longer be regarded as a fixed and irrevocable position of responsible governments. Moreover, a willingness to offer certain concessions to terrorist demands need not be construed as a sign of weakness. Not only does it have the effect of buying time while other courses of action are explored, it is a reversible policy which does not necessarily signal continuing capitulation. It would appear that *under no circumstances should deterrence of this type of terrorist group be based upon orthodox threats of physically punishing retaliation.*

Group Type No. 2

This type of terrorist group is characterized by a high degree of commitment to political objectives and by the utilization of criminal tactics. Here, the self-sacrificing value system of *Fedayeen* is still in evidence, while the group secures needed funds through robberies of one kind or another. It follows that deterrence efforts should focus upon the same threats and promises associated with Group Type No. 1 *plus* efforts which exploit the criminal character of the group. It would appear that this second category of efforts should concentrate upon creating a "bad press" for the group among potential adherents and supporters by spreading the news about the group's ordinary criminal tendencies.

Group Type No. 3

This type of terrorist group is characterized by a moderate degree of commitment to political objectives and by an absence of criminal activity. Here, the group's primary rationale and concern

[8] The special meaning of "criminal" should be kept in mind.

[9] It is ironic that the mainspring of global security has always been the threat to punish rather than the promise to reward. After all, beginning with studies of child-rearing, the literature on behavior modification regularly underscores the idea that positive sanctions are more effective than negative ones, that—speaking metaphorically—we can influence more flies with honey than with vinegar. In reference to reducing the probability of nuclear terrorism, we must begin to look at some carrots as well as the usual sticks.

is still manifestly political, but there is no evidence of the self-sacrificing value. And the group does not secure funds through "expropriation."

In view of the particular ordering of preferences associated with this type of terrorist group—an ordering which values both political objectives and personal safety—it would appear that deterrence efforts should focus upon the same threats and promises associated with Group Type No. 1 *plus* an appropriate level of orthodox threats of physically punishing retaliation. The use of negative physical sanctions must always involve great care and subtlety, even where it is clear that the intended terrorist targets value personal survival and safety. Indeed, a great deal of sophisticated conceptual analysis and experimental evidence now seems to indicate that, in certain cases, the threat of physical punishment may actually prove counterproductive. [12-14] Such negative sanctions are needed to compensate for the diminished (vis-a-vis Group Types 1 and 2) level of political commitment.

Group Type No. 4

This type of terrorist group is characterized by a moderate degree of commitment to political objectives and by the utilization of criminal tactics. Here the group's political concerns mirror Group Type No. 3, but the group does secure funds through robberies and hold-ups. It would appear, therefore, that deterrence efforts should focus upon the same threats and promises associated with Group Type No. 3 *plus* efforts to broadcast and publicize the group's ordinary criminal activities. As in the case of deterrence efforts associated with Group Type No. 2, such efforts are designed to alienate the group from vital bases of potential support.

Group Type No. 5

This type of terrorist group is characterized by a low degree of commitment to political objectives and by the absence of criminal activity. Here the group's *raison d'etre* is only nominally political, and the group does not secure funds through "expropriation." Typically, this type of group looks upon violence as its own end rather than as an instrument. Moreover, violence is viewed as a romantic and creative force that is self-justifying. In view of the particular ordering of preferences associated with this type of terrorist group—an ordering which values the violent act itself more highly than any alleged political objectives—it would appear that deterrence should be abandoned altogether as a strategy of counter-nuclear terrorism. Since such groups exhibit traits that are best described as nihilistic or psychopathic,[10] preventive measures should focus upon "prophylaxis" via a counter-nuclear terrorism campaign which may or may not require preemption. And since personal safety figures unimportantly in this type of terrorist group's risk calculus, the application of negative physical sanctions must be at the highest reasonable levels, i.e., levels that are consistent with the society's basic commitment to decency and essential human rights.

Group Type No. 6

This type of terrorist group is characterized by a low degree of commitment to political objectives and by the use of criminal tactics. Here, the group's nominal political concerns mirror Group Type No. 5, but the group does secure funds through "expropriation." While this type of terrorist group may also exhibit nihilistic or psychopathic traits, its primary characteristics come closer to those of ordinary criminals or bandits. It would appear, therefore, that deterrence efforts should focus upon the kinds of threats that are used to counter orthodox criminality, and that these efforts must be augmented by the preventive measures associated with Group Type No. 5.

[10] Witness, for example, the case of Kozo Okamoto, the surviving terrorist of the Lydda Airport massacre, who stated that he experienced "a strange ecstasy" as unknown people fell to his bullets. It would be a mistake, however, to conclude that such individuals are incapable of having profound effects because of their condition. As Freud points out, "Fools, visionaries, sufferers from delusions, neurotics, and lunatics have played great roles at all times in the history of mankind and not merely when the accident of birth had bequeathed them sovereignty. Usually they have wreaked havoc. . . ."

The extent to which such preventive measures should be adopted depends largely on which primary features this type of terrorist group exhibit nihilistic/psychopathic rather than purely criminal traits.

APPENDIX C—The Threat to Civil Liberties

In seeking to identify a potentially effective configuration of counter-nuclear terrorism measures, the proposed research must also explore the effects of such measures upon civil liberties. Such exploration is suggested by the realization that, on occasion, effective counter-nuclear terrorist measures may be achieved only at considerable cost to certain basic democratic values, and that this cost must be included in the decisional calculations of governments contemplating the use of such measures. For government that is sensitive to preserving the basic fabric of civil liberties, the concern for effective counter-nuclear terrorist measures must always be tempered by a coequal concern for judicious respect of essential human rights.

Some of the prospective sanctions available to counter-nuclear terrorist strategies entail measures that might be injurious to such values as social justice and human rights within states. Of special interest in this connection are options involving:

- A total, no-holds barred military-type assault designed to eradicate the terrorist group(s) altogether; and/or
- A protracted, counter-terrorist campaign utilizing "classical" methods of informers, infiltrators, counter-terror squads patterned, perhaps, after Israel's *Mivtah Elohim* (God's wrath),[11] agents provocateurs, and selected raids.

The first option, however effective it might be, is apt to be most destructive of essential citizen rights. Hence, governments contemplating such an option must pay close attention to the necessary trade-off between efficacy and liberty that is involved. Since this option would almost certainly be repugnant to the most deeply-held values of liberal, democratic societies, governments, before resorting to this option, would have to be convinced that its prospective benefits were great enough to outweigh its probable costs. In fact, short of its use at the situational level where higher-order acts of terrorist violence have already taken place, it is unlikely that this option would be taken seriously in democratic states. Rather, we are likely to see its adoption only by the world's most blatantly authoritarian, anti-democratic regimes.

This no-holds-barred military option is problematic for another reason. Not only might it incite fears of military/police repression among the more liberal sectors of the population, it might also confer a genuine combatant status upon the terrorists. As a result; the terrorist group(s) would more likely acquire the cast of an underdog army than that of a criminal band.[12]

The second option is also apt to score high marks on the efficacy dimension, but its effects on essential citizen rights need not be as injurious. This is not to suggest that a protracted counter-terrorist campaign utilizing classical methods of apprehension and punishment would necessarily be any less repulsive to liberal, democratic societies, but that such a campaign might be conducted on a comparatively less-visible and clandestine basis. An additional virtue of such quiet operations would be the avoidance of sympathy-generating publicity for the terrorist group(s).[13]

In the final analysis, the problem of conflicting values which emerges from the consideration of harsh deterrent counter-measures can be resolved only by careful comparison of the costs and benefits involved. To the extent that the terrorist threat is believed to be of potentially "lethal"

---

[11] Despite the revulsion that is typically generated by the suggestion of assassination in liberal, democratic societies, there is a well-established tradition in political philosophy which regards it as permissible under certain circumstances, e.g., the writings of Cicero, St. Thomas Aquinas, and Sir Thomas More.

[12] Once it becomes focused upon the no-holds-barred military option, counter-terrorist measures generate a symbiotic relationship between opposing "armies," with each "feeding" upon the other. This development is contrary to the interests of the government, not only because it tends to fulfill the terrorist claims of repression, while boosting terrorist group morale and cohesion, but because it also creates incentives for escalation of violent action by both sides. An example of this point is the case of FLN terrorism in Algeria (1954-1962) and the "mirror image" response of the OAS.

[13] As in the case of the first option, it is essential that option 2 tactics be confined to the purpose at hand, lest they give rise to the sorts of right-wing vigilante groups that have run amok in Brazil, Argentina, and Guatemala.

quality to the state's very survival, Trudeau's "total war" message of October 14, 1970 may be regarded widely as perfectly reasonable:

> There are a lot of bleeding hearts around who just don't like to see people with helmets and guns. All I can say is, go on and bleed, but it is more important to keep law and order in the society than to be worried about weak-kneed people. . . . I think society must take every means at its disposal to defend itself against the emergency of a parallel power which defies the elected power in this country.[14]

On the other hand, where the terrorist threat is not deemed to be of such a precarious character, the prospective benefits of draconian measures may not be great enough to outweigh the resulting impairment of civil liberties and personal freedoms.

In general, the optimal counter-nuclear terrorist strategy is one in which effective counter-action leaves the prevailing network of citizen rights and privileges unimpaired. Barring this possibility, however, the requirements of effective strategies should be tempered, to the greatest extent possible, by the assurance of those freedoms which are basic to any democratic order.

In reference to the two options just outlined, it would appear to be better from the civil liberties point of view if their sanctioning methods could be replaced altogether by the use of positive sanctions; moderate, ad hoc acts of physical punishment; efforts at underscoring the orthodox criminality of terrorist activities; and sustained efforts to convince terrorists that higher-order violence would be counter-productive to their objectives. Indeed, it would surely appear to be a good idea for counter-nuclear terrorist planners to begin to exploit the psychological warfare tactics which go back to the fifth century B.C. and Sun Tzu's THE BOOK OF WAR. Recognizing that in most cases terrorist violence is not an end in itself, but an instrument for achieving desired personal/social/political change, certain terrorist groups might be deterred from nuclear violence to the extent that they believe such violence to be self-defeating. Unlike options 1 and 2, such tactics would recognize the primacy of ends over means in the preference orderings of most terrorist groups, and exploit this recognition by the establishment of reasoned counter-measures. This primacy of ends over means has also served to justify the use of totally random and highly destructive violence by terrorists. As long as terrorists believe that the overwhelming righteousness of their particular causes justifies any available means, governments must learn how to deal with what Hannah Arendt calls the "banality of evil" problem. This is the case because terrorists with an "ends justifies the means" stance on violence are capable of engaging in evil without experiencing it as evil. In fact, they are even capable of displacing responsibility for their own violent acts upon the victims of these acts, e.g., the statement by the leader of Black September terrorists concerning responsibility for the helicopter deaths in Munich: "No Israelis would have been killed if the Germans had not trapped the operation. No one at all would have been killed if the Israelis had released their prisoners." Hence, the terrorist reasoning disclaims responsibility because the Germans and Israelis had not agreed to blackmail. To counter this sort of thinking, counter-terrorist efforts must be geared toward communicating the need for "proportionality" between ends and means to terrorist groups (e.g., the statement included in the Report of the Ad Hoc Committee on International Terrorism of the General Assembly, New York, 1973: "Even when the use of force is legally and morally justified, there are some means, as in every form of human conflict, which must not be used; the legitimacy of a cause does not in itself legitimize the use of certain forms of violence, especially against the innocent.") Such efforts must also be augmented by steps designed to undermine the "psychology of the cell," a psychology which acts to submerge individual feelings of responsibility and consequently renders violent excesses more likely. These steps should be calculated to fractionate bonds between members of a terrorist group, so as to strengthen, rather than diminish, feelings of individual responsibility. The effects of the

[14] Canadian Prime Minister Trudeau's response to FLQ tactics of bombing and assassination, a response which was designed to put Canada on a genuine wartime footing against its internal insurgents, gave the government the power to do anything "it deems necessary for the security, defense, peace, order, and welfare of Canada" (War Measures Act, October 1970). While such a "broad net" strategy may actually be effective in dealing with the problem at hand, it inevitably generates new problems in the process.

psychology of the cell were perceptively revealed by James Cross of the British Trade Commission after his captivity at the hands of the FLQ in the winter of 1970. Together with the Uruguayan Tapamaros and the Algerian FLN, the FLQ best illustrates the clandestine cell structure of a terrorist group.

Such tactics, however, are intrinsically ill-suited to dealing with terrorist groups for whom higher-order acts of destruction are ends in themselves. In dealing with such groups, the previously stated options may circumscribe the government's only means of defending the citizens in its charge. It would appear that in such cases, the exigencies of survival may have to take precedence over the claims of libertarian values.[15]

REFERENCES

[1] Beres, Louis René, *Terrorism and International Security: The Nuclear Threat,* a Report to the U.S. Arms Control and Disarmament Agency, August 1977, to be printed in *Chitty's Law Journal,* Toronto, Canada, forthcoming.

[2] Beres, Louis René, "The Nuclear Threat of Terrorism," *International Journal of Group Tensions,* Vol. 6, Nos. 1/2, 1976, pp. 53–66.

[3] Beres, Louis René, "International Terrorism and World Order: The Nuclear Threat," *Stanford Journal of International Studies,* Vol. XII/Spring 1977, pp. 131–146.

[4] Beres, Louis René, "The Threat of Palestinian Nuclear Terrorism in the Middle East," *International Problems,* Vol. XV, Nos. 3/4, Fall 1976, pp. 48–56.

[5] Beres, Louis René, "Arab Terrorists May Use Nuclear Weapons," *Maariv* (in Hebrew, Israel), Saturday Magazine, April 23, 1976.

[6] Beres, Louis René, "Terrorism and the Nuclear Threat in the Middle East," *Current History,* January 1976, pp. 27–29.

[7] Beres, Louis René, "Guerrillas, Terrorists, and Polarity: New Structural Models of World Politics," *Western Political Quarterly,* Vol. 27, No. 4, December 1974, pp. 624–636.

[8] Beres, Louis René, "*Hic Sunt Dracones:* The Nuclear Threat of International Terrorism," *Terrorism:* An International Journal, forthcoming.

[9] Beres, Louis René, "The Ever-Violent Middle-East," in W. P. Lineberry, ed., *The Struggle Against Terrorism* (New York, The Reference Shelf, 1977), pp. 76–82.

[10] Beres, Louis René, "The Nuclear Threat of Terrorism," *International Studies Notes,* International Studies Association, forthcoming.

[11] Beres, Louis René, *Apocalypse: Nuclear Catastrophe in World Politics,* forthcoming.

[12] Berkowitz, Leonard, *Aggression:* A Social Psychological Analysis (New York, McGraw-Hill, 1962), p. 96.

[13] Buss, Arnold H., *The Psychology of Aggression* (New York, Wiley, 1961), p. 58.

[14] Gurr, Robert Ted, *Why Men Rebel,* Princeton University Press, 1970, pp. 241, 242, 259 and 274.

[15] Hobsbaum, Eric, *Bandits* (New York, Dell, 1969).

[16] Jenkins, Brian, *The Potential for Nuclear Terrorism,* The Rand Paper Series, May 1977.

[17] Jones, Robert R., *Nuclear Reactor Risks—Some Frightening Scenarios,* Chicago Sun Times, Friday, April 30, 1976, p. 12.

[18] *The Princeton Alumni Weekly,* October 25, 1976, p. 6.

[19] *The Princeton Alumni Weekly,* October 25, 1976, p. 12.

[20] *The Princeton Alumni Weekly,* October 25, 1976, p. 22.

[21] *The Psychology of Aggression,* (New York, Wiley, 1961), p. 58.

[22] U.S. Congress, Office of Technology Assessment, *Nuclear Proliferation and Safeguards* (New York, Praeger, 1977).

[23] Willrich and Theodore Taylor, *Nuclear Theft: Risks and Safeguards* (Cambridge, Ballinger, 1974), p. 115.

[24] Willrich and Theodore Taylor, op. cit., p. 1.

[25] Willrich and Theodore Taylor, op. cit., pp. 20–21.

[26] Willrich and Theodore Taylor, op. cit., pp. 24–25.

[15] However, even when survival itself is at stake, decent governments must resist descending to counter-terrorist policies of "prophylaxis" as they are practiced in the Soviet Union and other authoritarian societies. Such policies, having their historical roots in the arbitrary arrest provisions of the Law of 1793 during the French Reign of Terror, represent so great an assault on fundamental human rights that they destroy the very values which counter-terrorism is designed to protect.

POTENTIAL APPLICATION OF COMPUTER-BASED CRISIS MANAGEMENT AIDS TO PROBLEMS OF PHYSICAL SECURITY

Stephen J. Andriole and Judith Ayres Daly

Cybernetics Technology Office, Defense Advanced Research Projects Agency, Arlington, Virginia 22209

I. INTRODUCTION

Crisis management is one of the broader problems subsumed by the general topic of "The Role of Behavioral Science in Physical Security." Much research conducted under the rubric of crisis management is now or potentially relevant to other problems of physical security. Such problems include:

- need for and difficulties of quick response time;
- identification of patterns in past threats to physical security which might include the attributes and capabilities of adversaries, and the association of historical defender actions with successfully achieved objectives;
- the utility of scenarios for training and contingency planning;
- the impact of warning on enhanced crisis management.

This paper first describes two interactive, computer-based aids developed by the Advanced Research Projects Agency Cybernetics Technology Office's (ARPA/CTO) Crisis Management Program (CMP). The first is an executive aid for crisis management and the second is an early warning and monitoring system. Secondly, the paper suggests ways in which the concepts, methodologies and technologies of these two systems can be applied to problems of physical security. Finally, ways in which such computer-based systems can help solve the myriad problems associated with the behavioral aspects of physical security are suggested, including:

- alleviation of pressures of quick response time by computerized search for precedent defender actions and objectives and adversary attributes and capabilities in past threats to physical security;
- using computerized warning and monitoring scenarios for training of physical security managers and response forces;
- linking warning of threats to physical security to improved management of such events.

II. EXECUTIVE AID FOR CRISIS MANAGEMENT

The ARPA/CTO Crisis Management Program is an effort to develop, test and transfer technology in three areas:

- computer-based early warning and monitoring systems;
- computer-based executive aids for crisis management and;
- new quantitative methods for advanced warning, monitoring and management.

Under ARPA/CTO sponsorship, CACI, Inc. has taken the lead in developing the executive aid which can be used to:

- outline the history of U.S. crisis management problems since World War II;
- summarize crisis problems that the U.S. has faced in the past;
- identify recent trends in problems faced by U.S. crisis managers;
- search rapidly for historical precedents and analogies in the course of considering crisis options; and
- in non-crisis periods, serve as a training tool for crisis management personnel.

These capabilities are founded on the following definition of crisis:

> a period of increased military management activity at the national level that is carried on in a sustained manner under conditions of rapid action and response resulting from unexpected events or incidents that have occurred internationally, internally in a foreign country, or in the domestic United States and that have inflicted or threatened to inflict violence or significant damage to U.S. interest, personnel, or facilities. [1][1]

Based on this definition, 307 crises from 1966-1976 in which the U.S. was involved were identified. The crisis cases were coded according to major characteristics and three subsets of the 307 analyzed more extensively to produce data bases for special applications. These three data bases, of which the executive aid is comprised, are:

- 101 U.S. crisis operations from 1946-1976 which focus on U.S. actions and objectives;
- 41 crises from 1956-1976 presenting the major problems encountered by the U.S. in each; and
- descriptive information on 307 U.S. crises over the period 1946-1976.

The aid runs on a PDP-11/70 at ARPA/CTO's Demonstration and Development Facility (DDF) and is self-prompting, interactive and user-oriented. A sample output from the executive aid which fully demonstrates the capabilities of the system is shown in tables 1-8 and figure 1.

As demonstrated by the preceding sample output, the first section of the aid permits the rapid search for and correlation of U.S. actions and objectives in crises. The search can be conducted by actions, objectives, crises, or combinations of them as specified by the user. Use of the aid in a real-world crisis situation can decrease the speed of precedent search to a matter of seconds, allow the user to determine which crisis actions have historically been associated with U.S. objectives similar to those in the crisis he is currently facing, and greatly increase the number of actions and objectives considered beyond what the decision-maker is likely to generate under the pressure of a real-world crisis.

This component of the executive aid has several potential applications to physical security. Data on adversary and defender attributes and capabilities, as presented in the general framework for this conference, could be collected from past incidents of threats to physical security, coded, quantified, and installed in a computer-based aid similar in concept to the crisis management one described above. In addition to attributes and capabilities, past threats could also be coded for adversary and defender actions and objectives to allow those charged with physical security to rapidly search for actions taken by adversaries similar in attributes, capabilities and objectives to the ones they are currently facing. Such an aid for physical security would alleviate many problems associated with the necessity of quick response time—including the rapid generation of alternative actions and their selection. It would allow the association of historical defender actions with successfully achieved objectives, perhaps categorized by adversary attributes and capabilities.

[1] Figures in brackets indicate literature references at the end of this paper.

Table 1

```
THIS CRISIS MANAGEMENT SYSTEM IS DIVIDED INTO THREE SECTIONS:

SECTION I.

          HERE THE USER WILL FOCUS ON U.S. ACTIONS AND
          U.S. OBJECTIVES AND THEIR ASSOCIATION AS DERIVED
          FROM A STUDY OF 101 CRISES INVOLVING THE UNITED
          STATES BETWEEN 1956 AND 1976.


SECTION II.

          HERE THE USER WILL FOCUS ON MANAGEMENT PROBLEMS
          THAT WERE IDENTIFIED IN 41 CRISES INVOLVING THE
          UNITED STATES BETWEEN 1956 AND 1976.


SECTION III.

          HERE THE USER MAY EXAMINE 307 CRISES INVOLVING
          UNITED STATES BETWEEN 1946 AND 1976.  THESE
          CRISES ARE DESCRIBED BY THE TYPE AND DEGREE OF
          MILITARY MANAGEMENT ACTIVITY DURING EACH CRISIS
          PHASE AND BY A SELECTED SET OF 19 GENERAL CRISIS
          DESCRIPTORS.

DETAILED DESCRIPTIONS ARE PROVIDED WITH THE PROGRAMS.
WOULD YOU LIKE A SUMMARY OF ONE OF THE SECTIONS BEFORE CHOOSING ONE ?

           PRESS 'Y' OR 'N' AND 'RETURN'.
Y
ENTER 'I','II',OR 'III'.
I
```

Table 2

```
                        SECTION I.

THIS SECTION IS DESIGNED TO ASSIST DEPARTMENT OF DEFENSE
PERSONNEL IN EVALUATING PROPOSED COURSES OF ACTION AND
SETS OF U.S. OBJECTIVES BASED ON DATA FROM 101 CRISES
INVOLVING THE UNITED STATES BETWEEN 1956-1976.

THE USER IS GIVEN THREE LEVELS OF ANALYTIC ASSISTANCE:

    1. THE CAPACITY TO SEARCH FOR HISTORICAL CASES WITH
       SETS OF USER-SPECIFIED U.S. ACTIONS OR OBJECTIVES.

    2. THE CAPACITY TO IDENTIFY, ACROSS ALL CASES,
       THOSE ACTIONS THAT HAVE HISTORICALLY BEEN
       MOST STRONGLY ASSOCIATED WITH EACH OBJECTIVE
       SELECTED BY THE PROGRAM-USER;

    3. THE CAPACITY TO IDENTIFY, ACROSS ALL CASES,
       THOSE ACTIONS THAT HAVE HISTORICALLY BEEN MOST
       COMMONLY ASSOCIATED WITH SETS OF U.S. OBJECTIVES
       SELECTED BY THE PROGRAM USER.

FOR ADDITIONAL INFORMATION ABOUT THE SYSTEM, PRESS 'HELP'.

WOULD YOU LIKE TO SEE A SUMMARY OF ANOTHER SYSTEM SECTION ?

           PRESS 'Y' OR 'N' AND 'RETURN'.
Y
ENTER 'I','II',OR 'III'.
II
```

Table 3

U.S. ACTIONS

1 COMMIT LAND FORCES TO COMBAT
2 COMMIT SEA FORCES TO COMBAT
3 COMMIT AIR FORCES TO COMBAT
4 COMMIT SUPPORT SERVICES (LAND)
5 COMMIT SUPPORT SERVICES (SEA)
6 COMMIT SUPPORT SERVICES (AIR)
7 REPOSITIOION LAND FORCES
8 REPOSITION SEA FORCES
9 REPOSITION AIR FORCES
10 THREATEN NUCLEAR FORCES AS A DETERRENT
11 REDEPLOY NUCLEAR FORCES AS A DETERRENT
12 CHANGE ALERT STATUS OF NUCLEAR FORCES AS A DETERRENT
13 THREATEN NONNUCLEAR FORCES AS A DETERRENT
14 REDEPLOY NONNUCLEAR FORCES AS A DETERRENT
15 CHANGE ALERT STATUS OF NONNUCLEAR FORCES
16 REDEPLOY PEACEKEEPING FORCES
17 SHOW OF MILITARY FORCE
18 MILITARY BLOCKADE OR QUARANTINE
19 ISOLATED MILITARY CONTACT
20 MILITARY FORCES USED IN SEARCH AND RESCUE OPERATION
21 MILITARY INTELLIGENCE COLLECTION
22 MILITARY INTELLIGENCE DISSEMINATION TO AN ALLY
23 MILITARY INTELLIGENCE DISSEMINATION TO AN ANTAGONIST
24 MILITARY MANEUVERS OR TRAINING EXERCISES
25 IMPROVE, MAINTAIN FORCE READINESS
26 COVERT MILITARY OPERATION
27 MILITARY INTERVENTION BETWEEN COMBATANTS
28 AIRLIFT PERSONNEL AND/OR SUPPLIES AND EQUIPMENT
29 PROVIDE MILITARY ADVISORY ASSISTANCE
30 PROVIDE MILITARY TRAINING FOR COMBAT TROOPS

PRESS 'HOME/PAGE' TO CONTINUE.

31 PROVIDE OTHER MILITARY TRAINING
32 DRAWDOWN MILITARY EQUIPMENT FROM U.S. UNITS
33 PROVIDE SUPPLIES FROM U.S. DEPOTS
34 PROVIDE SUPPLIES FROM NON-MILITARY SOURCES
35 PROVIDE MILITARY MAINTENANCE ASSISTANCE
36 PROVIDE OTHER MILITARY LOGISTICS ASSISTANCE
37 PROVIDE OTHER MILITARY ASSISTANCE
38 MAKE POL/ECO COMMITMENT IMPLYING NEW MIL MISSION
39 UNDERTAKE A NEW MILITARY MISSION
40 ACCEPT A NEW MILITARY COST
41 MODIFY AN EXISTING DEFENSE TREATY
42 MODIFY AN EXISTING BASE RIGHTS TREATY
43 MODIFY AN EXISTING STATUS OF FORCES AGREEMENT
44 SEEK ASSISTANCE IN DECISION-MAKING
45 TAKE NO MILITARY ACTION
46 EMPLOY DIPLOMACY
47 MEDIATE A DISPUTE
48 THREATEN TO, OR ACTUALLY, WITHDRAW SUPPORT
49 ADVOCATE/SUPPORT PEACEKEEPING EFFORTS
50 IMPROVE SCIENTIFIC/TECHNICAL CAPABILITIES
51 REAFFIRM EXISTING POLITICAL/MILITARY COMMITMENT
52 LODGE PROTEST(S)
53 OTHER
54 U.S. ACTS ALONE
55 U.S. ACTS WITH ONE OTHER NATION
56 U.S. ACTS WITH TWO OR MORE OTHER NATIONS
57 UNITED NATIONS INVOLVED

PRESS 'HOME/PAGE' TO CONTINUE.

Table 4

U.S. OBJECTIVES

1 DETER IMMINENT ATTACK
2 IMPROVE OR RECTIFY DETERRENCE POSTURE
3 PUT DOWN REBELLION
4 RESTORE A REGIME
5 REGAIN ACCESS TO ECONOMIC RESOURCES
6 RESTORE PEACE
7 RESTORE TERRITORIAL INTEGRITY
8 RESTORE MILITARY BALANCE OF POWER
9 RESTORE READINESS
10 PRESERVE READINESS
11 PRESERVE PEACE
12 CONFIRM OR RE-ESTABLISH PRESTIGE
13 PRESERVE TERRITORY AND/OR FACILITIES
14 PRESERVE REGIME FROM EXTERNAL THREAT
15 PRESERVE REGIME FROM INTERNAL THREAT
16 PRESERVE, RESTORE, OR IMPROVE ALLIANCE
17 PROTECT LEGAL AND POLITICAL RIGHTS
18 INDUCE MAINTENANCE OF CURRENT POLICY
19 DISSUADE FROM A NEW POLICY
20 PROTECT A MILITARY ASSET
21 SUPPORT A NEW GOVERNMENT
22 INDUCE NATIONAL REORIENTATION
23 INDUCE ADOPTION OF A NEW POLICY
24 BRING ABOUT THE FALL OF A REGIME
25 SUPPORT INSURGENCY
26 DENY POLITICAL ACCESS
27 DENY MILITARY ACCESS
28 ASSURE CONTINUED ECONOMIC ACCESS
29 PRESERVE OR REGAIN CONTROL OF THE SEA
30 PRESERVE OR REGAIN CONTROL OF THE AIR

PRESS 'HOME/PAGE' TO CONTINUE.

31 DENY SUCCESS TO TERRORISTS OR HIJACKERS
32 PROTECT HUMAN LIFE
33 PROVIDE SANCTUARY OR ASYLUM
34 SUPPORT CRITICAL NEGOTIATIONS
35 DISCOVER INTENTIONS OR ACTIONS
36 PREPARE FOR ALTERNATIVE MISSIONS
37 SUPPORT EFFORTS BY THE UNITED NATIONS
38 CONTAIN OPPONENT(S)
39 PREVENT SPREAD OF WAR
40 PRESERVE LINE OF COMMUNICATIONS
41 REGAIN TECHNICAL ADVANTAGE
42 RESTORE PRESTIGE
43 PRESERVE BALANCE OF POWER
44 PREVENT SPREAD OF COMMUNIST INFLUENCE
45 PREVENT NUCLEAR PROLIFERATION
46 INSURE SELF-SUFFICIENCY
47 AVOID DIRECT INVOLVEMENT
48 PRESERVE SECRECY

PRESS 'HOME/PAGE' TO CONTINUE.

Table 5

```
THE FOLLOWING ACTIONS/OBJECTIVES WERE SELECTED:

 16  PRESERVE, RESTORE, OR IMPROVE ALLIANCE

--------------------------------------------------------------------------------
THE FILE WILL BE SEARCHED FOR CRISES WITH THESE U.S. ACTIONS/OBJECTIVES.
PLEASE BE PATIENT; MATCHES WILL BE PRINTED AS THEY ARE FOUND.
--------------------------------------------------------------------------------
  4   1957 JORDAN SURVIVES DISMEMBERMENT; OUSTS EGYPTIANS
 15   1959 CUBAN FORCES INVADE PANAMA
 17   1959 INSURGENCY IN LAOS
 21   1960 FRANCE BECOMES A NUCLEAR POWER
 25   1960 NICARAGUA VS COSTA RICA
 30   1961 BERLIN BORDER CLOSED BY EAST GERMANS
 31   1961 "SANTA MARIA" INCIDENT; HIJACKING OF PORTUGESE AIRLINER
 33   1962 U.S. TROOPS TO THAILAND
 36   1962 FRANCE SEEKS "NUCLEAR CLUB" MEMBERSHIP
 48   1963 CYPRUS TROUBLE; GREEK-TURKEY WAR THREAT
 51   1964 FURTHER TENSIONS WITH USSR AND CUBA
 52   1965 INSURGENCY IN THAILAND
 54   1965 INDIA-PAKISTAN CONFLICT
 57   1966 FRANCE LEAVES NATO
 58   1967 ISRAELI "SIX DAY" WAR
 62   1968 SOVIET INVASION OF CZECHOSLOVAKIA
 64   1968 JAPAN DEMANDS RETURN OF OKINAWA
 67   1969 USSR/CHINA BORDER CLASH
 75   1971 INDIA-PAKISTAN WAR
 80   1973 U.S. WORLDWIDE ALERT
 85   1974 CYPRUS CIVIL WAR; TURK INVASION
 88   1975 U.S. ENDS AID; TURKS CLOSE U.S. BASES
 96   1976 GREECE THREATENS U.S. BASE RIGHTS TREATY
 97   1976 NATO RESPONSE TO WARSAW PACT BUILDUP
 98   1976 THE AEGEAN CRISIS
```

Table 6

```
THE FOLLOWING ACTIONS/OBJECTIVES WERE SELECTED:

  7  REPOSITION LAND FORCES
  8  REPOSITION SEA FORCES
  9  REPOSITION AIR FORCES

--------------------------------------------------------------------------------
THE FILE WILL BE SEARCHED FOR CRISES WITH THESE U.S. ACTIONS/OBJECTIVES.
PLEASE BE PATIENT; MATCHES WILL BE PRINTED AS THEY ARE FOUND.
--------------------------------------------------------------------------------

 34   1962 CUBAN MISSILE CRISIS
 65   1969 ANTI-U.S. RIOTS IN ISTANBUL
 72   1970 JORDAN/PALESTINE GUERRILLAS/SYRIA CONFLICT
 78   1973 MIDEAST WAR
 80   1973 U.S. WORLDWIDE ALERT
 99   1976 "PANMUNJON TREE" CRISIS

--------------------------------------------------------------------------------

THE SEARCH OF THE HISTORICAL FILE IS COMPLETED.

  6 MATCHES WERE FOUND.




PRESS 'HOME/PAGE' TO CONTINUE.
```

Table 7

```
U.S. ACTIONS
-------------------------------------------------------------------------
 89   1975 CAMBODIA SEIZES "MAYAGUEZ"
-------------------------------------------------------------------------

      2  COMMIT SEA FORCES TO COMBAT
      3  COMMIT AIR FORCES TO COMBAT
      4  COMMIT SUPPORT SERVICES (LAND)
      7  REPOSITION LAND FORCES
      9  REPOSITION AIR FORCES
     14  REDEPLOY NONNUCLEAR FORCES AS A DETERRENT
     17  SHOW OF MILITARY FORCE
     20  MILITARY FORCES USED IN SEARCH AND RESCUE OPERATION
     39  UNDERTAKE A NEW MILITARY MISSION
     40  ACCEPT A NEW MILITARY COST
     46  EMPLOY DIPLOMACY
     54  U.S. ACTS ALONE

-------------------------------------------------------------------------
        ENTER   NO. OF SELECTED HISTORICAL CRISIS (1-101).
```

Table 8

```
U.S. OBJECTIVES
-------------------------------------------------------------------------
 89   1975 CAMBODIA SEIZES "MAYAGUEZ"
-------------------------------------------------------------------------

     12  CONFIRM OR RE-ESTABLISH PRESTIGE
     19  DISSUADE FROM A NEW POLICY
     29  PRESERVE OR REGAIN CONTROL OF THE SEA
     32  PROTECT HUMAN LIFE
     35  DISCOVER INTENTIONS OR ACTIONS
     36  PREPARE FOR ALTERNATIVE MISSIONS

-------------------------------------------------------------------------

        ENTER   NO. OF SELECTED HISTORICAL CRISIS (1-101).
        ENTER '999' TO RETURN TO THE LIST OF PROGRAM OPTIONS.
999
```

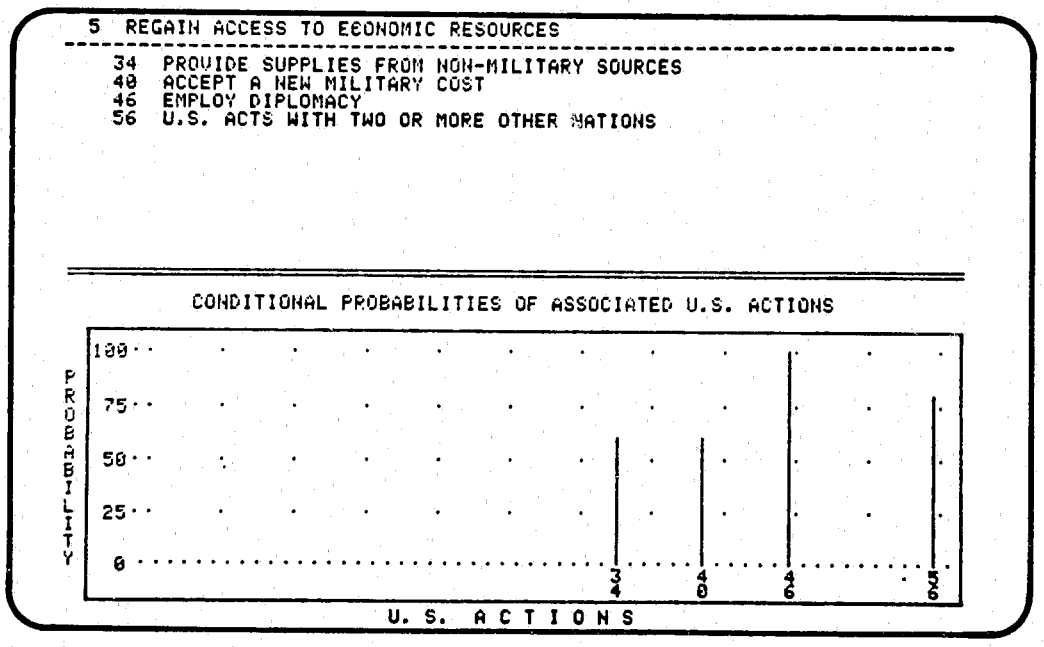

Figure 1

The second dimension of the Executive Aid is also relevant to problems of physical security. As shown in tables 9-14, the analyst is allowed to match 18 major problem categories with 41 crises and to access an in-depth description of the crisis management problems for any case.

If a data base for physical security existed and were organized like this section of the crisis management executive aid, it would have at least two uses. Such a physical security aid could be used to train new personnel, to familiarize them with problems they are likely to encounter. On a decision-making level, a computer-based physical security aid could be used for contingency planning as well as to generate and run scenarios and simulations for training of physical security managers.

The third section of the aid depicted in tables 15 and 16 allows the analysts to list historical crises by several criteria, e.g., geographic region and time period. Region could, of course, be replaced by criteria more relevant to physical security managers while the use of time periods would allow them to examine changes in the nature of threats to physical security over time.

The third section of the aid also provides a very detailed description of the problems in any of 307 crises of the user's choice. This is shown in table 17. Like the second section of the aid, this one could be used as introductory material for new personnel at all levels, as well as for contingency planning and more rigorous, scenario-based simulation training for physical security managers and response forces.

The relevance of the concepts, methodology and technology of the crisis management executive aid to problems of physical security should be clear. Potential application could occur even sooner than indicated above since there is currently under development an interactive aid for the management of terrorist incidents.[2] It too will be computer-based and will apply concepts, methodology and technology similar to those of the aid described above to the problem of terrorism. Conceivably, the terrorism management aid could be a salient topic at the next Conference on the Role of Behavioral Science in Physical Security.

Table 9

```
                    SECTION II.

THIS SECTION PERMITS A DETAILED EXAMINATION OF MANAGEMENT PROBLEMS
 ENCOUNTERED IN 41 SELECTED CASES (1956 - 1976).

MAJOR PROBLEM CATEGORIES ARE:

      1. SYSTEM-RELATED DELAYS IN DECISION-MAKING
      2. SYSTEM/PROCEDURAL CONSTRAINTS ON ACTIONS
      3. LEGAL ISSUES INVOLVED
      4. RESOURCES INADEQUATE FOR DECISION-MAKING/ACTION
      5. INTELLIGENCE FAILURES AT DECISION-MAKING LEVEL
      6. EMOTIONAL/IDEOLOGICAL ISSUES INVOLVED IN DECISIONS
      7. INTERPERSONAL FACTORS IN DECISION-MAKING
      8. PROLONGED CRISIS PROBLEMS
      9. PROBLEMS IN SELECTING ACTION PERSONNEL
     10. CONSTRAINTS ON OPERATIONS
     11. PHYSIOLOGICAL PROBLEMS FOR OPERATING FORCES
     12. INFORMATION FAILURES BY OPERATING FORCES
     13. FAILURES IN TAKING APPROPRIATE/TIMELY ACTION
     14. FORSTAT PROBLEMS
     15. PROBLEMS IN THE OPERATING ENVIRONMENT
     16. GENERAL PROBLEMS IN CRISIS PLANNING
     17. GENERAL PROBLEMS IN CRISIS HANDLING
     18. GENERAL PROBLEMS IN CRISIS TIMING

FOR ADDITIONAL INFORMATION ABOUT THE SYSTEM, PRESS 'HELP'.

WOULD YOU LIKE TO SEE A SUMMARY OF ANOTHER SYSTEM SECTION ?
          PRESS 'Y' OR 'N' AND 'RETURN'.
Y
ENTER 'I','II',OR 'III'.
III
```

Table 10

```
---------------------------------------------------------------------
 0 THE FORTY-ONE CRISES SELECTED FOR DETAILED STUDY ARE:
---------------------------------------------------------------------

(THE NOS. IN () ARE THE CASE ID'S USED IN SECTION I.)

 1  1946 CIVIL STRIFE IN GREECE
 2  1946 CIVIL WAR IN CHINA
 3  1948 BERLIN BLOCKADE
 4  1948 U.S. RAIL STRIKE
 5  1950 U.S. RAIL STRIKE
 6  1950 NORTH KOREAN ATTACKS
 7  1950 AID TO FORMOSA
 8  1952 GERM WARFARE CHARGES
 9  1952 KOJE-DO RIOTS
10  1952 U.S.INTEPCEPTS SOVIET FIGHTER
11  1953 EAST BERLIN RIOTS
12  1954 QUEMOY-MATSU
13  1955 COSTA RICA - NICARAGUA
14  1956 MIDEAST WAR; SUEZ CANAL CRISIS (1)
15  1956 HUNGARIAN REVOLUTION (3)
16  1957 LITTLE ROCK CRISIS
17  1957 USSR LAUNCHES SPUTNIK (8)
18  1958 U.S. MARINES SENT TO LEBANON (9)
19  1960 CUBA/U.S. DISSENSION (19)
20  1960 U-2 INCIDENT (23)
21  1961 U.S. INCREASES MILITARY SUPPORT TO RVN (28)
22  1961 BERLIN BORDER CLOSED BY EAST GERMANS (38)
23  1961 NUCLEAR TEST BAN
24  1962 CUBAN MISILE CRISIS (34)
25  1964 CANAL ZONE FLAG RIOTS (41)
26  1964 TONKIN GULF INCIDENTS (45)
27  1965 DOMINICAN REVOLT; U.S. INTERVENTION (55)
          PRESS 'HOME/PAGE' TO CONTINUE.
```

```
28  1966 U.S. DROPS FOUR H-BOMBS OFF SPANISH COAST (56)
29  1966 FRANCE LEAVES NATO (57)
30  1967 ATTACK ON USS LIBERTY (59)
31  1968 SEIZURE OF USS PUEBLO BY NORTH KOREANS (60)
32  1968 DR. KING ASSASSINATED
33  1968 SOVIET INVASION OF CZECHOSLOVAKIA (62)
34  1969 OPERATION "RED HAT"-MOVEMENT OF TOXIC MUNITIONS (69)
35  1970 NEW YORK CITY MAIL STRIKE
36  1973 MIDEAST WAR (78)
37  1973 ARAB OIL EMBARGO (79)
38  1974 COUP IN PORTUGAL (83)
39  1975 U.S. ENDS AID; TURKS CLOSE U.S. BASES (86)
40  1975 SEIZURE OF "MAYAGUEZ" (89)
41  1975 ANGOLA CIVIL WAR (90)

          PRESS 'HOME/PAGE' TO CONTINUE.
```

Table 11

```
YOU HAVE CHOSEN THE FOLLOWING PROBLEM CATEGORIES:
-------------------------------------------------------------------------

  1. SYSTEM-RELATED DELAYS IN DECISION-MAKING/ACTION
  2. SYSTEM/PROCEDURAL CONSTRAINTS ON ACTIONS
  3. LEGAL ISSUES INVOLVED
  5. INTELLIGENCE FAILURES AT DECISION-MAKING LEVEL
  6. EMOTIONAL/IDEOLOGICAL ISSUES INVOLVED IN DECISION-MAKING
 15. PROBLEMS IN THE OPERATING ENVIRONMENT
 17. GENERAL PROBLEMS IN CRISIS HANDLING
 18. GENERAL PROBLEMS IN CRISIS TIMING

THE CASES IN WHICH THESE PROBLEMS WERE PRESENT ARE:
-------------------------------------------------------------------------

 6  1950 NORTH KOREAN ATTACKS
21  1961 U.S. INCREASES MILITARY SUPPORT TO RVN (28)
24  1962 CUBAN MISILE CRISIS (34)
26  1964 TONKIN GULF INCIDENTS (45)
31  1968 SEIZURE OF USS PUEBLO BY NORTH KOREANS (60)
34  1969 OPERATION "RED HAT"-MOVEMENT OF TOXIC MUNITIONS (69)

          PRESS 'HOME/PAGE' TO CONTINUE.
```

Table 12

1 1946 CIVIL STRIFE IN GREECE

I. PROBLEMS AT THE NATIONAL DECISION-MAKING LEVEL

1. SYSTEM-RELATED DELAYS IN DECISION-MAKING/ACTION

Extensive Inter-agency Coordination Required for Action
Referral to International Agencies (U.S., NATO, OAS) Required
President Involved as Decision-Maker

2. SYSTEM/PROCEDURAL CONSTRAINTS ON ACTIONS

Consideration of U. S. Domestic Impact

6. EMOTIONAL/IDEOLOGICAL ISSUES INVOLVED IN DECISION-MAKING

Crisis Actions Affected by Ideological Issues

7. INTERPERSONAL FACTORS IN DECISION-MAKING

Multi-Lingual Problems

PRESS 'HOME/PAGE' TO CONTINUE.

Table 13

1 1946 CIVIL STRIFE IN GREECE

II. OPERATIONAL PROBLEMS

10. CONSTRAINTS ON OPERATIONS

Joint Operation-Language
Action in Friendly Country (Area)
Inadequate Communications for Operating Forces

15. PROBLEMS IN THE OPERATING ENVIRONMENT

Geography - Terrain - Climate

PRESS 'HOME/PAGE' TO CONTINUE.

Table 14

```
1  1946 CIVIL STRIFE IN GREECE

III. GENERAL PROBLEMS

 16. GENERAL PROBLEMS IN CRISIS PLANNING
No Appropriate Plans Ready for Crisis Contingency

 17. GENERAL PROBLEMS IN CRISIS HANDLING
Crisis Develops Despite Adequate Actions
Late U. S. Military Involvement

 18. GENERAL PROBLEMS IN CRISIS TIMING
Situation Develops Over Time Before Crisis Level Is Reached
Prolonged Crisis With Intermittent Peaks

PRESS 'HOME/PAGE' TO CONTINUE.
```

Table 15

```
E X E C U T I V E   A I D S   F O R   C R I S I S   M A N A G E M E N T

              SECTION III.  : EXAMINATION OF 307 CRISES
      TWO PROGRAM OPTIONS ARE AVAILABLE:

         OPTION 'A' WILL ALLOW YOU TO SELECT AND PRINT CASES BY :
                   o YEAR OF OCCURRENCE,
                   o LOCATION (ONE OF THE 10 JCS REGIONS), AND
                   o ANY SPECIFIED LEVEL OF ONE OR MORE OF THE
                     19 CRISIS DESCRIPTORS.

         OPTION 'B' WILL ALLOW YOU TO SELECT AN INDIVIDUAL CASE
                   AND PRINT ITS DESCRIPTION.

PLEASE CHOOSE ONE OF THE OPTIONS (ENTER 'A' OR 'B')
A
ENTER YEARS (AS '46-48'  OR  '46-46' FOR ONE YEAR)
75-76
ENTER ONE REGION CODE (0-9), OR
      'A' FOR ALL REGIONS (I.E. NO SELECTION BY REGION), OR
      'H' FOR DEFINITIONS OF THE REGION CODES.
H
1=NORTH AMERICA          / 2=CENTRAL,SOUTH AMERICA
3=W. EUR.,MED.,ATLANTIC / 4=E. EUR.,USSR
5=MID-EAST,N. AFRICA     / 6=SE ASIA,INDIAN O.,SUB-SAH. AFR.
7=PACIFIC AREA, E. ASIA / 8=POLAR REGIONS
```

```
9=SPACE                    / 0=MULTIPLE, WORLD

ENTER ONE REGION CODE (0-9), OR
      'A' FOR ALL REGIONS (I.E. NO SELECTION BY REGION), OR
      'H' FOR DEFINITIONS OF THE REGION CODES.
A
W O R K I N G
WOULD YOU LIKE TO SPECIFY ADDITIONAL SELECTION CRITERIA ?
('Y' OR 'N').
 N
('Y' OR 'N').
N
NO. CASES SELECTED =                  24
WOULD YOU LIKE TO DISPLAY THESE CASES ('Y' OR 'N')
Y
```

Table 16

```
------------------------------------------------------------------------
                        1975-1976 ALL REGIONS
------------------------------------------------------------------------
NOTE: THE ID. NO. OF ANY CASE INCLUDED IN SECTION I. WILL BE FOUND IN ()
.


284  1975 USSR REJECTS TRADING WITH U.S.
285  1975 U.S. ENDS AID; TURKS CLOSE U.S. BASES (86)
286  1975 TURKISH CYPRIOTS PROCLAIM STATE
287  1975 CAMBODIA SEIZES "MAYAGUEZ" (89)
288  1975 ANTI-U.S. DEMONSTRATIONS IN LAOS
289  1975 MRS. GANDHI PROCLAIMS EMERGENCY
290  1975 CIVIL WAR IN ANGOLA (90)
291  1976 MOROCCO-ALGERIAN DISPUTE
292  1976 CAMBODIA PROTESTS BOMBING OF SIEM RAP (93)
293  1976 SADAT ABROGATES SOVIET TREATY (94)
294  1976 U.S. THAI BASES CLOSED (95)
295  1976 GREECE THREATENS U.S. BASE RIGHTS TREATY (96)
296  1976 NATO RESPONSE TO WARSAW PACT BUILDUP
297  1976 FIRST LEBANON EVACUATION (APRIL-JUNE) (91)
298  1976 THE AEGEAN CRISIS (98)
299  1976 U.S. PLEDGES SUPPORT TO KENYA
300  1976 SECOND LEBANON EVACUATION (JULY) (92)
301  1976 "PANMUNJOM TREE" CRISIS (99)
302  1976 USSR DEFECTOR WITH MIG-25 (100)
303  1976 PANAMA CANAL TALKS STALLED
304  1976 NORTH KOREA PROPOSES NEW PEACE TREATY
305  1976 FRANCE WITHDRAWS TROOPS FROM GERMANY
306  1976 NAVY LOSES TOMCAT FIGHTER FROM CARRIER (101)

          PRESS 'HOME/PAGE' TO CONTINUE
```

Table 17

```
1975 U.S. ENDS AID; TURKS CLOSE U.S. BASES (86)
CRISIS LOCATION : W. EUROPE, THE MEDITERRANEAN, OR THE ATLANTIC
A. PRE-CRISIS PERIOD
--------------------

PRE-CRISIS ACTIVITY              : INCREASED READINESS.
DURATION OF PRE-CRISIS ACTIVITY : EXTENDED (>30 DAYS).

B. CRISIS PERIOD
----------------
CRISIS ACTIVITY                  : INTERNATIONAL.
NATURE OF THE CRISIS             : POLITICAL AND MILITARY.
DURATION OF CRISIS               : EXTENDED (>30 DAYS).

C. POST-CRISIS PERIOD
---------------------

CRISIS RESOLUTION                : EXTENDED (<<30 DAYS).
CRISIS OUTCOME                   : NEGATIVE.

D. CRISIS DESCRIPTORS
---------------------

AWARENESS OF CRISIS POSSIBILITY: ANTICIPATED.
THREAT TO U.S. INTERESTS       : SEVERE.
THREAT TIMING                  : EXTENDED (>7 DAYS).
DECISION TIME                  : EXTENDED.
U.S. AND SMALL POWER(S)        : LARGE POWER INTERESTS.
U.S. RESPONSE                  : CONFRONTATION.
U.S. OBJECTIVES                : STATUS QUO ANTE.
STRATEGIC IMPLICATIONS         : NON-NUCLEAR.
          PRESS 'HOME/PAGE' TO CONTINUE.
```

III. EARLY WARNING AND MONITORING SYSTEM (EWAMS)

As with terrorist incidents, it is much more difficult to forecast general threats to physical security than to provide warning of international political crises. However, it may be possible to monitor potential and on-going threats to physical security with a computerized system.

ARPA/CTO has sponsored development of an interactive, computer-based system for the early warning of international political crises and the monitoring of international affairs. The design of the system consists of:

- quantitative political, military and economic indicators
- forecasting methods
- computer base

The most important output of this system is probabilistic crisis warnings. The data base of the current system includes the political actions and the interactions of all countries in the world from 1966 to the present. The data is updated every day so that EWAMS runs in a "real-time" mode. It runs on a PDP 11/70 at ARPA/CTO's Demonstration and Development Facility. Sample output from the system is presented in tables 18-32 and figures 2-9.[3]

The connection of this extant early warning and monitoring system to problems of physical security is more tenuous and less clear than that between the crisis management executive aid and physical security. This results from lack of data rather than conceptual or methodological inadequacies. Early warning of threats to physical security could possibly serve to avert them and would certainly enhance their management. Early warning would also provide time for action, selection, evaluation, and for mobilization of response forces. Even if there is insufficient data to forecast or warn of threats to physical security, the concepts and technology of the warning and monitoring system described above might be used to develop a system for *monitoring* threats. That

is, while there may not be sufficient data on such threats to generate probabilistic forecasts or warning, there may be enough to monitor them. Such a monitoring system would be of use in the following areas:

- contingency planning by physical security managers.
- scenario generation for simulation training of physical security managers and response forces.

Table 18

```
********** CRISIS EARLY WARNING PROTOTYPE SYSTEM **********
                    HISTORICAL VERSION

     THE CRISIS EARLY WARNING PROTOTYPE SYSTEM WAS DEVELOPED
FOR THE ADVANCED RESEARCH PROJECTS AGENCY'S CYBERNETICS TECH-
NOLOGY OFFICE BY DECISIONS AND DESIGNS, INCORPORATED (DDI).


     THIS VERSION OF THE SYSTEM IS DESIGNED TO SIMULATE HOW
QUANTITATIVE POLITICAL INDICATORS MIGHT HAVE CONTRIBUTED TO
THE U.S. DEFENSE COMMUNITY'S ABILITY TO FORECAST A NUMBER OF
IMPORTANT INTERNATIONAL CRISES.  IT IS ALSO DESIGNED TO ILLUS-
TRATE HOW THE GENERAL NATURE AND DIRECTION OF INTERNATIONAL
AFFAIRS MAY BE MONITORED USING POLITICAL INDICATORS.


     OTHER "REAL-TIME" VERSIONS OF THE SYSTEM SIMULATE HOW
ACTUAL TRACKING AND CRISIS FORECASTING MAY BE ACCOMPLISHED
USING MANY OF THE SAME, HISTORICALLY VALIDATED, POLITICAL
INDICATORS.


     FUTURE VERSIONS WILL SIMULATE HOW "REAL-TIME" TRACKING
AND FORECASTING MAY BE ACCOMPLISHED VIA A MULTI-TRACK INDI-
CATOR SYSTEM COMPRISED OF QUANTITATIVE MILITARY, POLITICAL,
AND ECONOMIC INDICATORS.

                    **********

PLEASE PRESS RETURN TO ACTIVATE THIS VERSION OF THE SYSTEM:
```

Table 19

```
xxxxxxxxxxxxx EARLY WARNING SYSTEM ACTIVATED xxxxxxxxxxxxx


THE FOLLOWING INTERNATIONAL CRISIS CASES ARE NOW AVAILABLE
ON THE DEMONSTRATION SYSTEM :

  1.  SINO - SOVIET BORDER CLASHES,
      JANUARY , 1967 AND MARCH , 1969

  2.  CZECHOSLOVAKIAN INVASION,
      AUGUST , 1968

  3.  INDO - PAKISTANI WAR,
      NOVEMBER , 1971

THE SYSTEM ALSO CONTAINS THE FOLLOWING OTHER CASES :

  4.  U.S. - SOVIET UNION,
      JANUARY , 1966 - DECEMBER , 1975

  5.  U.S. - PEOPLES REPUBLIC OF CHINA,
      JANUARY , 1966 - DECEMBER , 1975

  6.  SOVIET UNION - PEOPLES REPUBLIC OF CHINA,
      JANUARY , 1966 - DECEMBER , 1975

PLEASE SELECT ONE CASE NUMBER :  2
```

Table 20

```
xxx CZECHOSLOVAKIAN INVASION , AUGUST , 1968 xxx

    PRIMARY ACTORS :
        SOVIET UNION (USR)
        CZECHOSLOVAKIA (CZE)
    OTHER ACTORS :
        UNITED STATES (USA)
        PEOPLES REPUBLIC OF CHINA (CHN)

PLEASE SELECT TWO ACTORS :(E.G. XXX,YYY )USR,CZE

SPECIFY ACTIVITY FLOW :
    0. ONE WAY (USR )>> CZE)
    1. ONE WAY (USR <<( CZE)
    2. TWO WAY (USR <-) CZE)2

SELECT TIME INCREMENT :
    1. MONTHLY
    2. QUARTERLY
    3. YEARLY      1

SET TIME PARAMETERS (JAN66,DEC75) :JAN68,DEC68

DO YOU DESIRE 30 DAY PROBABLISTIC FORCASTS (Y OR N) : Y
                  . . . P R O C E S S I N G . . .

NUMBER OF EVENTS FOUND :    217
```

Table 21

MONTHLY PROBABILITY
JAN, 1968 - DEC, 1968

*** USR <<<>>> CZE ***

DATE	PROBABILITY
JAN 68	.10
FEB 68	.50
MAR 68	.70
APR 68	.70
MAY 68	.80
JUN 68	.40
JUL 68	.70
AUG 68	.60
SEP 68	.40
OCT 68	.05
NOV 68	.01
DEC 68	.01

Table 22

MONTHLY ACTIVITY
JAN, 1968 - DEC, 1968

*** CZE <<<<<< TWO-WAY FLOW >>>>>> USR ***

DATE	TOTAL ACTIVITY NUMBER	Z-SCORE	PROB	COOPERATIVE ACTIVITY NUMBER	Z-SCORE	PROB	CONFLICTUAL ACTIVITY NUMBER	Z-SCORE	PROB
JAN 68	1	1.95	.10	1	1.95	.01	0	0.00	.01
FEB 68	2	3.89	.50	2	3.89	.10	0	0.00	.01
MAR 68	5	8.12	.70	5	8.12	.40	0	0.00	.01
APR 68	0	7.01	.70	4	3.32	.05	4	0.00	.01
MAY 68	21	11.38	.80	12	9.09	.40	9	11.72	.80
JUN 68	12	2.55	.40	8	2.87	.05	4	1.97	.10
JUL 68	37	7.79	.70	13	4.31	.10	24	12.41	.80
AUG 68	48	5.83	.60	20	5.37	.20	28	5.88	.60
SEP 68	41	3.33	.40	28	5.51	.20	13	1.66	.10
OCT 68	21	1.24	.05	16	2.03	.01	5	.38	.01
NOV 68	11	.41	.01	4	.10	.01	7	.67	.05
DEC 68	10	.32	.01	8	.71	.01	2	-.18	.01

Table 23

MONTHLY TENSION AND UNCERTAINTY
JAN, 1968 - DEC, 1968

*** USP <<<<<< TWO-WAY FLOW >>>>>> CZE ***

DATE	TENSION	Z-SCORE	H-REL	Z-SCORE
JAN 68	0.0	0.00	0.000	0.00
FEB 68	0.0	0.00	0.000	0.00
MAR 68	0.0	0.00	.431	0.00
APR 68	50.0	0.00	.561	6.57
MAY 68	42.9	4.35	.420	2.93
JUN 68	33.3	2.51	.603	3.76
JUL 68	64.9	4.66	.774	4.00
AUG 68	58.3	3.10	.772	3.17
SEP 68	31.7	1.26	.575	1.92
OCT 68	23.8	.80	.483	1.41
NOV 68	63.6	2.88	.531	1.54
DEC 68	20.0	.45	.352	.78

DO YOU WANT EVENT FREQUENCIES (Y OR N)Y

Table 24

MONTHLY COOPERATIVE ACTIVITY
JAN, 1968 - DEC, 1968

*** USR <<<<<< TWO-WAY FLOW >>>>>> CZE ***

DATE	YLD	CMNT	CNSL	APPR	PRMS	GRNT	REWD	AGRE	ROST	PROP
JAN 68	0	0	0	1	0	0	0	0	0	0
FEB 68	0	0	2	0	0	0	0	0	0	0
MAR 68	0	1	2	1	1	0	0	0	0	0
APR 68	0	0	2	1	0	0	1	0	0	0
MAY 68	0	1	10	1	0	0	0	0	0	0
JUN 68	0	0	2	1	3	0	0	2	0	0
JUL 68	2	0	6	1	1	0	0	0	2	1
AUG 68	3	0	6	2	2	0	0	6	0	1
SEP 68	3	1	18	0	0	1	0	4	1	0
OCT 68	1	1	12	0	0	1	0	0	1	0
NOV 68	0	0	0	0	0	1	0	2	1	0
DEC 68	0	0	6	0	0	1	1	0	0	0

Table 25

MONTHLY CONFLICTUAL ACTIVITY
JAN, 1968 - DEC, 1968

*** USR <<<<<< TWO-WAY FLOW >>>>>> CZE ***

DATE	RJCT	ACUS	PROT	DENY	DMND	WARN	THRT	DEMO	RDUC	EXPL	SEIZ	FRCE
JAN 68	0	0	0	0	0	0	0	0	0	0	0	0
FEB 68	0	0	0	0	0	0	0	0	0	0	0	0
MAR 68	0	0	0	0	0	0	0	0	0	0	0	0
APR 68	0	2	0	0	0	1	0	0	1	0	0	0
MAY 68	0	7	0	1	0	1	0	0	0	0	0	0
JUN 68	0	1	1	2	0	0	0	0	0	0	0	0
JUL 68	3	8	1	1	4	2	0	3	2	0	0	0
AUG 68	1	12	1	1	2	2	1	4	3	0	4	0
SEP 68	0	0	1	0	2	0	0	0	1	0	1	0
OCT 68	0	2	0	0	2	0	0	1	0	0	0	0
NOV 68	0	4	0	0	0	0	0	2	0	0	0	1
DEC 68	0	2	0	0	0	0	0	0	0	0	0	0

Table 26

********** CRISIS EARLY WARNING PROTOTYPE SYSTEM **********
"REAL-TIME" VERSION

THE CRISIS EARLY WARNING PROTOTYPE SYSTEM WAS DEVELOPED FOR THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY'S CYBERNETICS TECHNOLOGY OFFICE BY DECISIONS AND DESIGNS, INCORPORATED (DDI).

THIS VERSION OF THE SYSTEM IS DESIGNED TO SIMULATE HOW A COMPUTER-BASED CRISIS WARNING SYSTEM COMPRISED OF QUANTITATIVE POLITICAL INDICATORS MIGHT BE USED BY INTELLIGENCE ANALYSTS IN A "REAL-TIME" MODE TO TRACK INTERNATIONAL AFFAIRS AND FORECAST INTERNATIONAL CRISES.

ANOTHER, HISTORICALLY ORIENTED VERSION OF THE SYSTEM SIMULATES HOW THE SAME INDICATORS MIGHT HAVE CONTRIBUTED TO THE U.S. DEFENSE COMMUNITY'S ABILITY TO FORECAST A NUMBER OF IMPORTANT PAST INTERNATIONAL CRISES.

FUTURE VERSIONS WILL SIMULATE HOW "REAL-TIME" TRACKING AND FORECASTING MAY BE ACCOMPLISHED VIA A MULTI-TRACK INDICATOR SYSTEM COMPRISED OF QUANTITATIVE MILITARY, POLITICAL, AND ECONOMIC INDICATORS.

****

PLEASE PRESS RETURN TO ACTIVATE THIS VERSION OF THE SYSTEM:

Table 27

```
************** CRISIS WARNING SYSTEM ACTIVATED **************

                    REGIONAL OPTIONS:

1.    NORTH AMERICA
2.    CENTRAL AND SOUTH AMERICA
3.    WESTERN EUROPE-MEDITERRANEAN ATLANTIC
4.    EASTERN EUROPE-SOVIET UNION
5.    MIDDLE EAST AND NORTH AFRICA
6.    EAST ASIA AND PACIFIC
7.    SOUTH ASIA AND SUB-SAHARAN AFRICA

                  CROSS-REGIONAL OPTIONS:

8.    MAJOR POWER INTERACTIONS
9.    ALL INTERACTIONS
10.   SPECIAL PURPOSE INTERACTIONS

  SELECT ONE REGIONAL OR CROSS-REGIONAL OPTION:  5

  SPECIFY REGIONAL FOCUS:

1.  REGIONAL ACTORS <-> REGIONAL ACTORS
2.  REGIONAL ACTORS <-> WORLD                    1
```

```
********** 5. MIDDLE EAST AND NORTH AFRICA **********

WOULD YOU LIKE A LIST OF ACTORS WITHIN THIS REGION (Y OR N):  Y
```

Table 28

```
********** 5. MIDDLE EAST AND NORTH AFRICA **********

ALGERIA (ALG)                          LEBANON (LEB)
BAHRAIN (BAH)                          LIBYA (LBY)
ERITREAN LIBERATION FRONT (ELF)        MOROCCO (MOR)
ETHIOPIA (ETH)                         MUSCAT AND OMAN (MOM)
IRAN (IRN)                             SAUDI ARABIA (SAU)
IRAQ (IRQ)                             SOUTH YEMEN (SYE)
ISRAEL (ISR)                           SUDAN (SUD)
JORDAN (JOR)                           SYRIA (SYR)
KURDISTAN (KUR)                        TUNISIA (TUN)
KUWAIT (KUW)                           UNITED ARAB EMIRATES (UAE)
```

Table 29

```
PLEASE SELECT TWO ACTORS
OPTIONS:
ALL REGIONAL ACTORS VS. ALL REGIONAL ACTORS  (ALL-ALL)
ONE REGIONAL ACTOR  VS. ALL REGIONAL ACTORS  (XXX-ALL)
ONE REGIONAL ACTOR  VS. ONE REGIONAL ACTOR   (XXX-YYY)  UAR-ISR

SPECIFY ACTIVITY FLOW :
    0. ONE WAY (UAR >>> ISR)
    1. ONE WAY (UAR <<< ISR)
    2. TWO WAY (UAR <-> ISR)  2

SELECT TIME INCREMENT :
    1. MONTHLY
    2. QUARTERLY
    3. YEARLY                 1

SET TIME PARAMETERS (MMMYY-MMMYY) :  JAN67-DEC67

DO YOU DESIRE 30 DAY PROBABLISTIC FORECASTS (Y OR N) : Y

. . . P R O C E S S I N G . . .

NUMBER OF EVENTS FOUND :    110
```

Table 30

MONTHLY PROBABILITY
JAN, 1967 - DEC, 1967

*** UAR <<<>>> ISR ***

DATE	PROBABILITY
JAN 67	.01
FEB 67	.01
MAR 67	.01
APR 67	.01
MAY 67	.80
JUN 67	.60
JUL 67	.70
AUG 67	.01
SEP 67	.05
OCT 67	.05
NOV 67	.61
DEC 67	.01

Table 31

MONTHLY ACTIVITY
JAN, 1967 - DEC, 1967

*** ISR <<<<<< TWO-WAY FLOW >>>>>> UAR ***

DATE	TOTAL ACTIVITY NUMBER	Z-SCORE	PROB	COOPERATIVE ACTIVITY NUMBER	Z-SCORE	PROB	CONFLICTUAL ACTIVITY NUMBER	Z-SCORE	PROB
JAN 67	0	-.87	.01	0	-.29	.01	0	-.74	.01
FEB 67	0	-.81	.01	0	-.28	.01	0	-.69	.01
MAR 67	0	-.76	.01	0	-.27	.01	0	-.66	.01
APR 67	0	-.72	.01	0	-.26	.01	0	-.63	.01
MAY 67	13	15.28	.80	1	1.75	.01	12	15.89	.80
JUN 67	18	5.36	.60	4	7.23	.40	14	4.46	.50
JUL 67	39	7.41	.70	3	2.52	.05	36	8.27	.70
AUG 67	5	.09	.01	4	2.96	.05	1	-.30	.01
SEP 67	18	1.46	.05	0	-.51	.01	18	1.69	.10
OCT 67	10	.53	.05	0	-.49	.01	10	.65	.05
NOV 67	5	-.01	.01	1	.27	.01	4	-.05	.01
DEC 67	2	-.33	.01	0	-.50	.01	2	-.28	.01

Table 32

MONTHLY TENSION AND UNCERTAINTY
JAN, 1967 - DEC, 1967

*** ISR <<<<<< TWO-WAY FLOW >>>>>> UAR ***

DATE	TENSION	Z-SCORE	M-REL	Z-SCORE
JAN 67	0.0	-.81	0.000	-.43
FEB 67	0.0	-.76	0.000	-.41
MAR 67	0.0	-.72	0.000	-.39
APR 67	0.0	-.68	0.000	-.38
MAY 67	92.3	1.28	.575	7.14
JUN 67	77.8	.88	.558	3.27
JUL 67	92.3	1.14	.393	1.62
AUG 67	20.0	-.41	.162	.30
SEP 67	100.0	1.28	.352	1.28
OCT 67	100.0	1.20	.305	.96
NOV 67	80.0	.73	.431	1.57
DEC 67	100.0	1.12	.224	.42

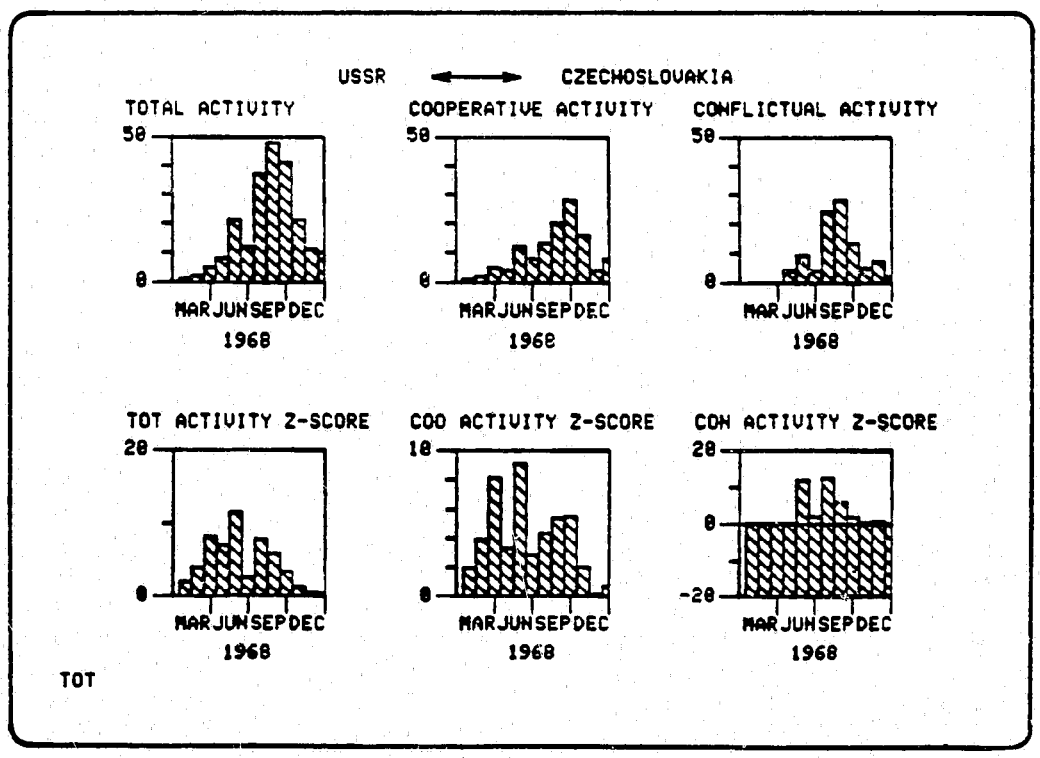

Figure 2

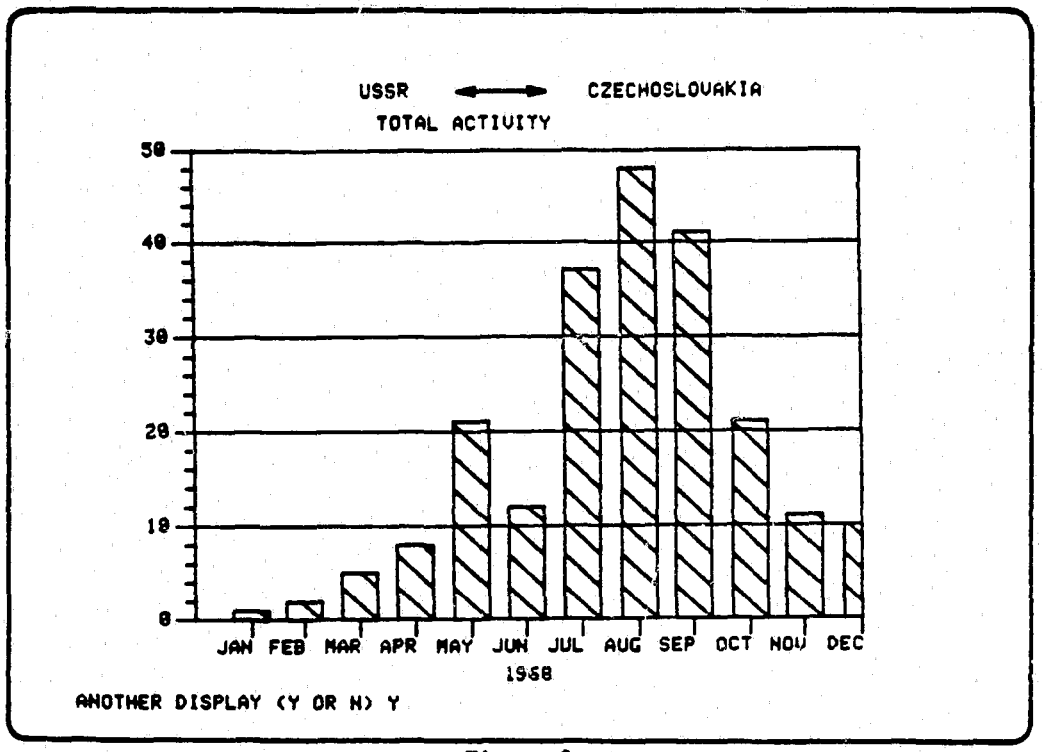

Figure 3

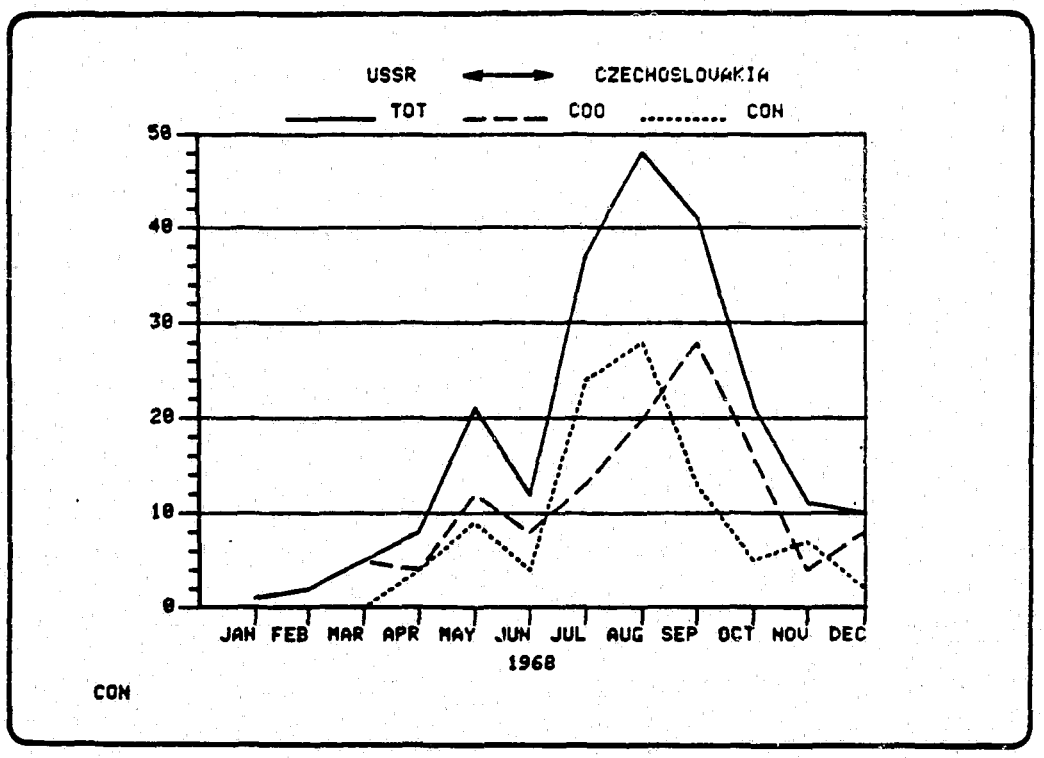

Figure 4

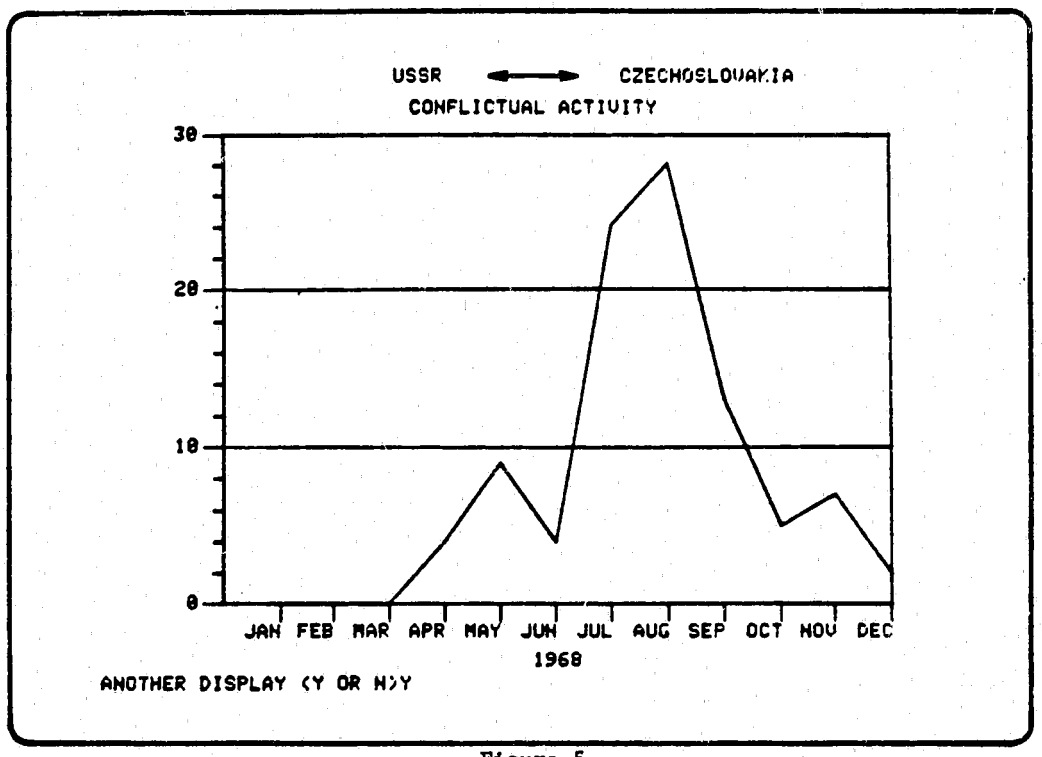

Figure 5

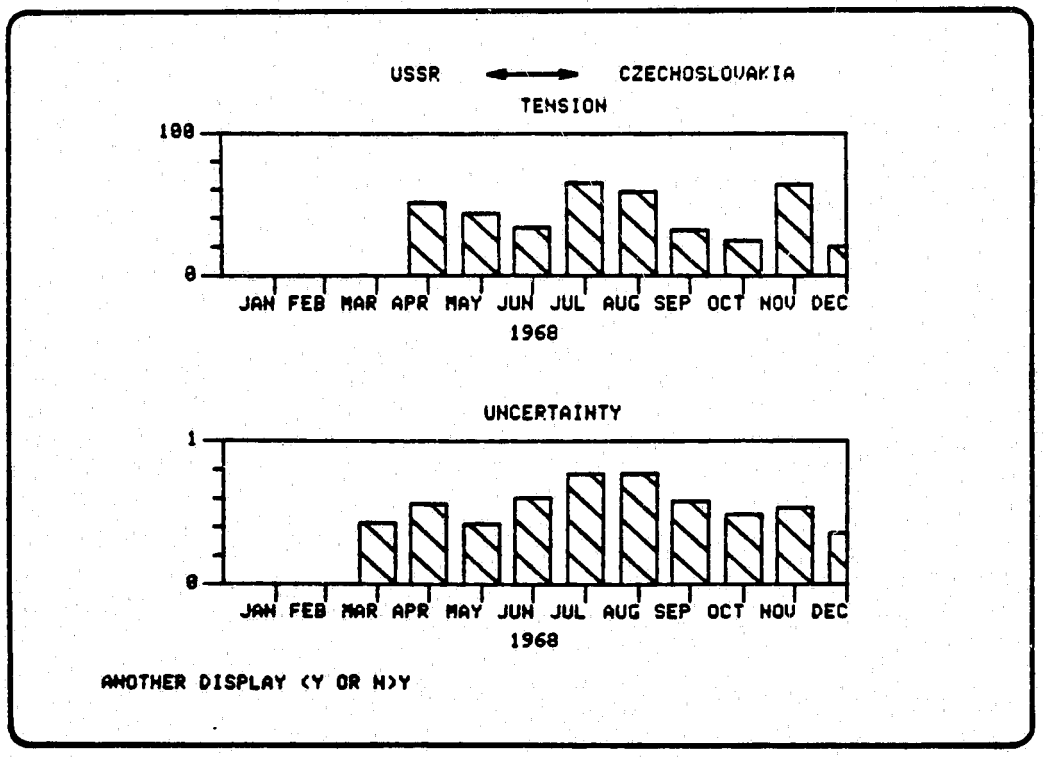

Figure 6

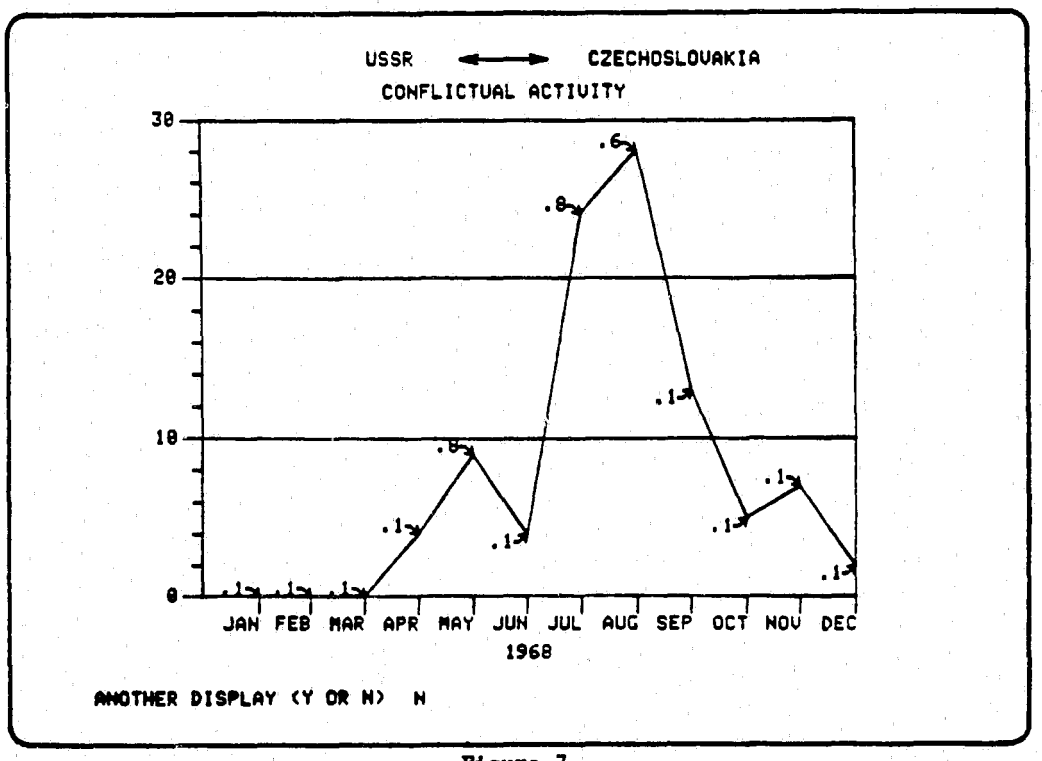

Figure 7

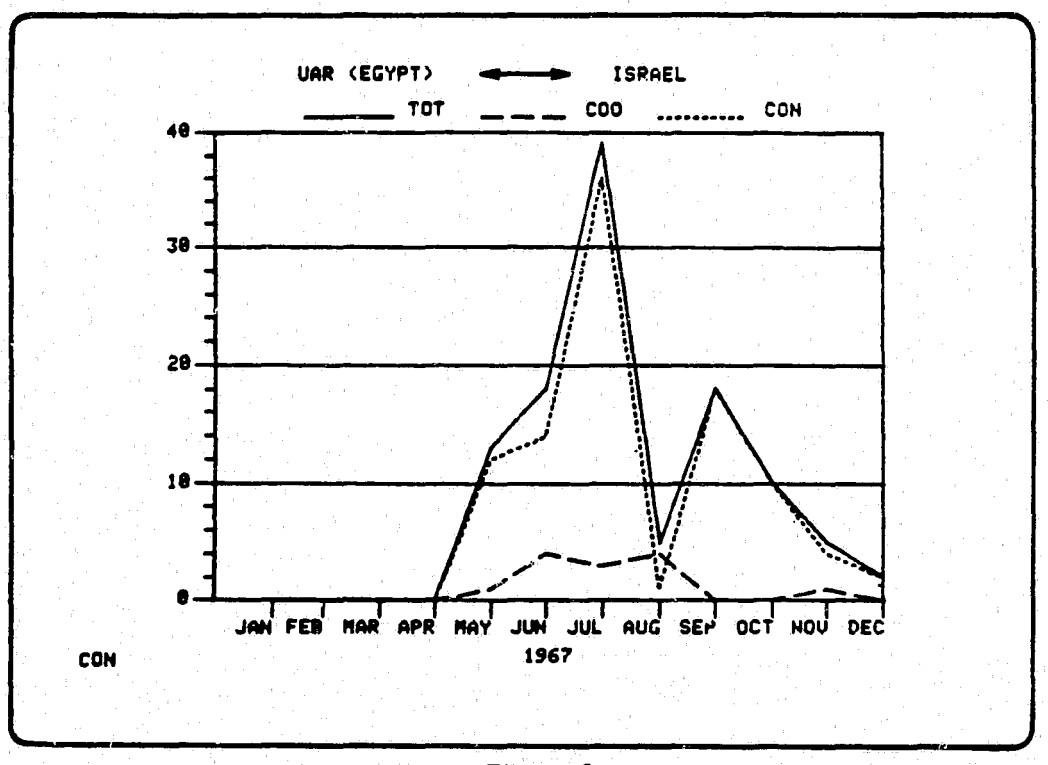

Figure 8

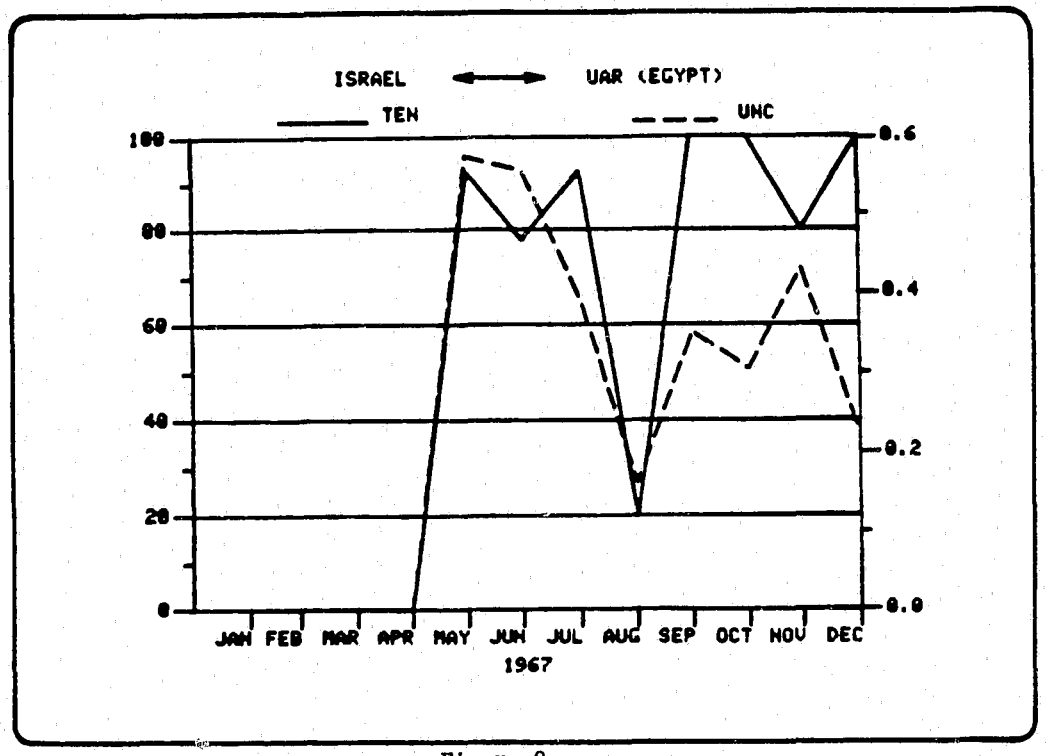

Figure 9

IV. CONCLUSIONS

Two interactive computer-based aids, one for crisis management and the other for early warning and monitoring, have great potential utility in alleviating problems of physical security. Just a few of the problems to which the aid's concepts, methodology and technology, might be addressed are: need for and difficulties of quick response time; identification of patterns in the attributes, actions, objectives, and capabilities of adversaries in past threats to physical security; associating defender objectives with successful actions; optimizing training; improving contingency planning; linking warning and monitoring of potential threats to physical security to better management and identification of specific problems likely to be encountered in different types of threats to physical security.

Potential solutions to physical security problems suggested by the crisis management and early warning and monitoring aids include: alleviation of pressures of quick response time by computerized search for precedent defender actions and objectives and adversary attributes and capabilities; using computer-based management, warning and monitoring scenarios for training of physical security managers and response forces; use of the same scenarios for contingency planning; to the extent potential physical security threats can be forecasted or monitored, the management of such threats will be facilitiated.

REFERENCES

[1] CACI (1977a) *Final Technical Report to Executive Aid for Crisis Management: Phase II,* Arlington, VA: CACI, Inc., and CACI (1977b) *User's Guide to Executive Aid for Crisis Management: Phase II,* Arlington, VA: CACI, Inc.

[2] CACI, Inc. (January 1977) *Research Gaps on Crisis Management of Terrorist Incidents,* Arlington, VA.

[3] For details on EWAMS, see: Stephen J. Andriole (1976) *Progress Report on the Development of an Integrated Crisis Warning System.* Technical Report 76-19, Decisions and Designs, Inc., McLean, VA, December; Thomas R. Davies and Judith Ayres Daly, *The Early Warning and Monitoring System: A Progress Report,* Mineo, March 1978; DDI (1978) *Early Warning and Monitoring Prototype System: Sample Output,* McLean, VA; Thomas R. Davies (1978) Users Manual for the Early Warning and Monitoring System, Mineo.

BRAIN WAVE AND BIOCHEMICAL RESEARCH FINDINGS

Dr. Karel Montor and Mr. Douglas Afdahl

United States Naval Academy, Annapolis, Maryland 21402

INTRODUCTION AND OBJECTIVES

Personnel selection of security guards can benefit from a variety of techniques both physiological and psychological in nature. Kent in discussing "the brains of men and machines" has noted that "the brain and the computer have both developed in an evolutionary manner, with survival of the fittest determining what features were retained and what were discarded."[1][1] Whether we are dealing with a potential known adversary or the evaluation of a guard in whom we entrust our security, it follows that their ability is a result of their physiological makeup as modified by their education/training and experiences. From the standpoint of the guard we are concerned with his level of attention to the dangers that may exist. Beatty has found in a series of experiments using pupillometric and electroencephalographic measures that a close relation is observed between the psychological processes of attention and the physiological indications of increased phasic activation.[2]

Another thesis of this paper is that there is a direct relationship between human physiological factors and observed psychological performance. While the years ahead will determine the specifics as well as cause and effect relationships, it is now possible to show that there are correlational indicators that suggest performance differences can be related to human physiological differences. Raher for example has found a significant correlation between a measure of physical fitness for Navy enlisted men enrolled in Underwater Demolition training, and their serum lactic acid concentrations.[3] Giannitrapani, studying the relationship between Schizophrenia and EEG Spectral Analysis, has found that the EEG autospectra shows correlates to a portion of the patients having the primary diagnosis of schizophrenia.[4]

While I could continue at length as to what others have been doing and have found in areas related to this meeting's interests, it seems to me that I must have been invited to share with you what we at the Naval Academy have found that might be worthy of your consideration. It is important to note that we have been using standard, off-the-shelf equipments for all our analyses. We have avoided the development of procedures which require advanced medical training of someone to determine results. All our experiments and studies are repeatable with outcomes numerically measurable. It is also important to note that my use of the word "we" does not come from a sense of modesty but rather is directly linked to the involvement of students and faculty at the Academy. Without the contributions of Midshipmen Gilbert, Olson, Bush, Hill, Woods, Enochs, Gray, and Walsh over the years there would be no results to report. If it were not for the wave analysis expertise of Dr. Bruce Johnson, who along with the writers have advised these young men—there would also be no results to report.

Using long-established signal processing techniques and applying these methods to neurological analysis suggests a method of possibly differentiating between "normal" and "not-normal" individuals. The suggestion is thus being made that, by determining the physiological parameter differences between competent and incompetent security guards, a profile might be developed so that it can be used in future security personnel selection. Further, it is suggested that our preliminary results may have permitted the development of physiologically reliable predictors of performance in "normal" individuals.

[1] Figures in brackets indicate literature references at the end of this paper.

We have found that attention level differences can be determined by looking at activity in the 8 to 13 Hz region related to a 10 microvolt level. An individual's concentration on a particular task results in a greater internal voltage drop in the brain at these frequencies. By determining the individual baseline for the person it is then possible to establish when the individual is no longer concentrating on the assigned task.[1] The application to security guards is a concern to make certain that they have not gone to sleep nor are daydreaming excessively, a parameter that can be established and monitored exactly. Equipments for measuring and telemetering brain waves have been developed by Ensign Paczan and circuit diagrams are available from the authors. Hughes has developed techniques for brain wave monitoring that can withstand severe head impact with relatively high frequencies (up to 13 Hz/sec) being seen during conditions of great anxiety and anticipation.[1]

Thus with the combination of an attention level monitor and EEG FM transmitter it can be seen that monitoring of security guards is possible and that if they are interfered with in their duties, third parties could be instantly notified. With respect to the adversary there are also techniques for detecting his presence. Superconducting Technology of Mountain View, Calif. has developed a highly sensitive superconducting quantum interference device as a magnetic field detector which can detect the heart's magnetic field from a distance of 15 feet. Thus an intruder in an area designated as free from human interference will be instantly detected and an alarm will sound. Brenner has found that brain waves may also be magnetically detected several cm from the scalp [7] and our findings at the Academy indicate specific, repeating, reactions of an individual to a flashing light. Thus looking into the future it is not hard to predict that a security area might have a low-level flashing light environment producing a known and specific reaction in the brain of the security guard which is constantly monitored by a micro computer AND that this pick-up will NOT require wiring of the guard. D. Cohen's work at the MIT Magnetics Laboratory involved almost $250K of special equipment and shielding. Within 5 years the price was down to $25K without shielding being required. It is reasonable to expect that the future technological developments in this area will make remote brain wave pick-up possible from yards away and thus with the microcomputer programmed to recognize our friendly guard—it will also be able to recognize the difference in brain waves of an intruder, even without a flashing light.

This capability to baseline individuals neurologically could also be used in transferring security personnel from one location to another so that imposters could be spotted. The Academy has not, and is not working in this research area.

Figure 1 shows the patterns we record for both heart and neurological data. These presentations have been known for decades to the neurological community. The major fault with this approach is that the analysis of these patterns requires the skill of an experienced neurologist to determine defects that are only apparent with monitoring many feet of pen and ink paper recordings. Figure 2 is a summary of 32 seconds of data. However, it could also represent several hours even though such long time averaging would mask individual events. Figure 2 could also represent activity over 1/2 a second or less. Figure 3 illustrates a technique originally developed by Dr. Bickford to present a lengthy series of spectral plots thus enabling the viewing of a changing reaction from seconds to hours.

Figures 7 and 8 indicate results found when spectral patterns were "not-normal." Figure 4 shows a normal comparison of left and right cross correlations with figure 9 indicating results found with "not-normal" individuals. Figure 10 is an indication of results found with averaging evoked potential responses over a period of time with the strobe frequency varying from one rate to another (12 to 28 Hz) rather than the averaging of one frequency (14 Hz) as in figure 4.

Our experience includes the measuring of more than 1750 midshipmen including 99 percent of the 1980 Class. Figures 5 and 6 show a technique that has been developed, but not yet applied to our brain wave tape recordings. The amount of potential research on these 1227 tape recordings is probably unlimited, especially when one considers the longitutional research that can be done several decades from now with respect to the possibility of determining advance predictors of disease states.

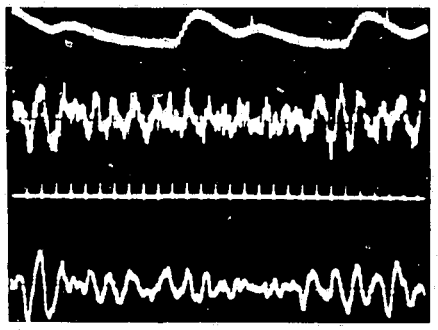

FIGURE 1. *Time Domain Data*
Ch 1-Heart *Ch 2-Left (01-C3)*
Ch 3-Strobe *Ch 4-Right (02-C4)*

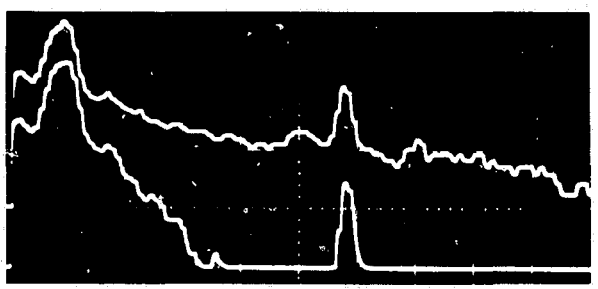

FIGURE 2. *Left) Spectral plots with Right) 60 Hz filter out.*

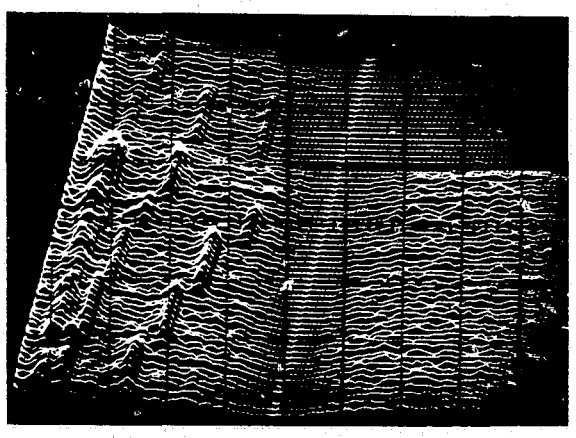

FIGURE 3. *Waterfall display of multiple spectral plots showing evoked potential changes with varying visual stimulation and 60 Hz filter in.*

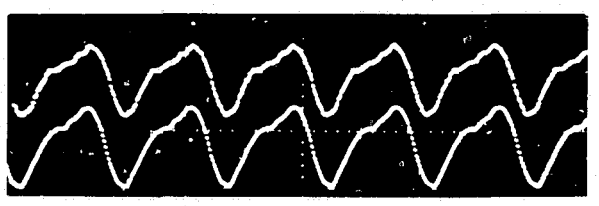

FIGURE 4. *Left) Cross correlation of Right) brain wave vs. strobe.*

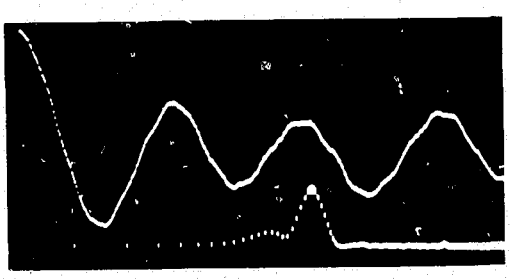

FIGURE 5. *L/R Cross correlation of brain waves and L/R cross spectrum analysis indicating power of common frequencies (mode 11 Hz).*

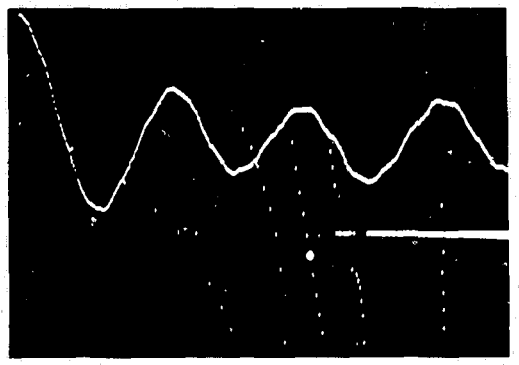

FIGURE 6. *L/R cross correlation and L/R phase angle difference indicating 38.16 degree difference at 11 Hz.*

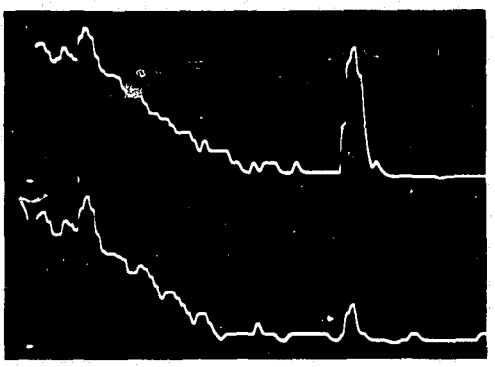

FIGURE 7. *Midshipmen with low frequency response during strobing were found to have significantly (.05) lower grades in Naval Science, Chemistry, Computers, Calculus, and Physical Education.*

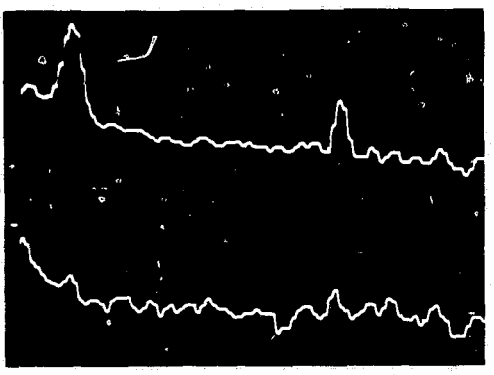

FIGURE 8. *Where the right hemisphere (bottom trace) mode frequency was found to be depressed the individuals had significantly (.05) higher grades in English and History. In those cases with left modes depressed, or both modes depressed the individuals had significantly (.05) lower grades in Naval Science.*

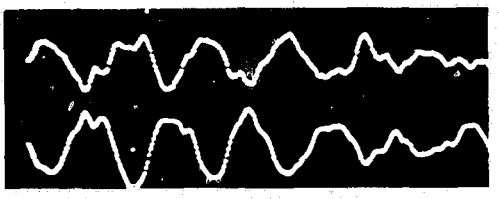

FIGURE 9. *With the left and right hemispheres 180° out of phase, as measured during strobing, significantly (.05) lower grades were earned in English, Naval Science, Chemistry, Computers, and in Military Performance.*

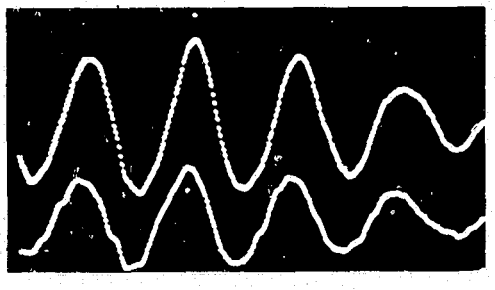

FIGURE 10. *An example of being able to determine hemispheric dominance by evoked potential amplitude. This individual writes right handed, although the right hemisphere is dominant as indicated by the lower amplitude. The person remembers being switched in childhood.*

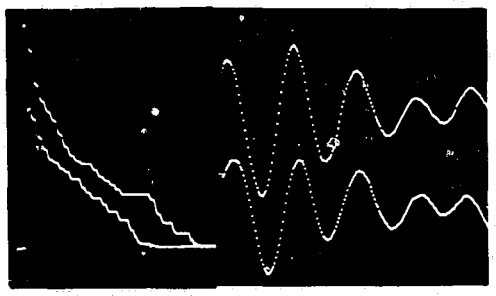

FIGURE 11. *Combination scope display of spectral plot (w/o strobing) and evoked potential from strobing of an individual who expired ten hours later. While the EEG was essentially flat - portions of the brain did not respond to the light.*

Applying these techniques to security guard selection suggests that screening for normalcy may be in order, assuming that the studies previously suggested do not differentiate between those who are and those who are not good at their jobs. It may also be in the best interest of the guard to know if there is something neurologically "wrong." However you are cautioned to realize that we do not yet know what the "not-normal" reaction may indicate, although we do have evidence that midshipmen with such irregularities do not do as well in our measurement system as those without such deviations.

Additional research outside the neurological area has been conducted. In addition to brain wave measurements on the Class of 1980 there was also the taking of blood from those who were willing to volunteer for that aspect. Over 1000 midshipmen volunteered and the blood was analyzed on both the Technicron SMA 12/60 and the Programachem 10/40 analyzers. The midshipmen with normal values in the following areas did significantly better, at the .05 level, than those with values above or below the normal amounts of Protein, Albumin, Cholesterol, Uric Acid, Creatinine, and Serum Glutamic Oxalic Transaminase. It should be noted that the findings of military performance was higher in those midshipmen with normal protein levels, high calcium levels, and normal uric acid levels. (Significant at the .07, .09, and .05 levels respectively.) One set of data indicated that higher conduct grades of the same midshipmen were achieved in those with high protein levels, and low calcium levels, thus suggesting that further research is required.

The concept of color psychology has been studied throughout modern history. In 1947, Max Luscher proposed a theory which attributed the selection preference for eight solid colors to conflicts and tensions that were inhibited in the personality.[8] In accordance with Luscher's Theory, a normal, mentally-at-ease person would reject the dull, drab colors (otherwise known as the auxiliary colors—maroon, brown, black and neutral grey). This was found to be the case in the majority of midshipmen tested over a period of several years. It was also found that there were significant differences in brain waves between those who preferred the color yellow rather than red, and that in general midshipmen had personality differences related to their color preferences.

Other findings have indicated that those with residually higher Vitamin C levels, after 12 hours of Vitamin C deprivation, perform "better" at the Academy than those with lower levels. The finding was the same when we compared performance of smokers to non-smokers; the smokers did significantly poorer in almost all areas of measurement.

It is apparent from the foregoing that we are in the midst of an extensive study from which the findings have been quite diverse. We have found for example that those with a neurological hemispheric processing speed difference of more than 7 msec seem to have reading problems that are not educationally based. Those with faster neurological processing speeds do better in their academic efforts, and generally those with physiological parameters in the normal range perform and achieve more at the Academy than those who fall outside of these normal ranges.

However, before we adopt these tests a study is needed to determine how security guard profiles relate to their performance. Perhaps the best security guards do not have all of their physiological and psychological parameters in the normal range. For example, a more anxious than average security guard might be the best to have on the job since he may always be alert to danger. We could speculate for days on what are the ideal parameters for the security guards, however since the technology exists to measure those who are on the job and thus empirically make the decision, as we have been able to infer from midshipman performance results, it would seem that the appropriate next step is to do some research and try to determine the necessary factors for "good" security guards.

REFERENCES

[1] Kent, E. W., BYTE, January 1978, p. 11.
[2] Beatty, J., Dept. of Psychology, UCLA, Los Angeles, Calif. 90024.
[3] Raher, R. *et al.*, Diseases of the Nervous System, June 1972, p. 403.
[4] Giannitrapani, D. *et al.*, Electroencephalography and Clinical Neurophysiology, 1974, 36: 377-396.
[5] Montor, K., U.S. Patent No. 3,877,466.
[6] Hughes, J., *et al.*, Northwestern Univ. Medical Center, Chicago, Ill.
[7] Brenner, D. *et al.*, Science 190.480 (1975).
[8] Luscher, Max, The Luscher Color Test (Basel, Switzerland: Test Verlag 1947).

PSYCHOLOGICAL DETERRENCE IN ROBBERIES OF BANKS AND ITS APPLICATION TO OTHER INSTITUTIONS

Willard D. Tiffany and James M. Ketchel

SRI International, Menlo Park, California 94025

INTRODUCTION

A variety of objectives have been cited by agencies concerned with combating robberies and burglaries. In general, these objectives can be subsumed within seven basic aims: to deter the criminal; failing this, to thwart him or physically block him in his criminal intent; and failing these, to identify, apprehend, convict and confine him, and recover the loot.

Whatever the primary mission or interest of the various agencies concerned with crime, virtually all of them seem to agree that it is most desirable to deter a would-be criminal before the crime is committed.

Early in our work on the security of financial institutions, we became intrigued when one bank branch in a busy downtown area was robbed 15 times during the 5-year period 1963-1967 while another branch just two blocks away on the same street was only robbed twice in the same period of time.

Similiarly, in another metropolitan area, a bank office had not been hit in the 2 years of its existence, while in the same period, branches in a surrounding four-block area had been hit a number of times. Moreover, one of the branches that had been robbed was located diagonally across the street from the office that was not hit.

In the 5-year period noted above, a large banking house having 939 branches experienced from one to three robberies per year in 25 of those branches (2.7%); 362 branches (38.6%) were hit at least once in the 5 years; but 552 (58.8%) were not hit at all. This led us to ask, "What characteristics do infrequently hit banks have that make them unattractive targets?"

When questioned by police, captured robbers usually could not explain why they had selected a particular office except to say that others they had first visited were "wrong," and this one was "right." In our study of reasons for this selectivity, we have elected to group the variables that lead to rejection under the heading of "psychological deterrence." This term includes intuitive factors, those subconsciously sensed by the potential criminal, as well as factors that are consciously perceived as being threatening, difficult, unfavorable, or "not right."

Since deterrence was not a major aspect of previous research, only a brief examination of psychological deterrence was possible. We were able to examine 14 different bank offices and gather data regarding their appearance, architecture, layout, location, size, and some environmental characteristics, as well as their histories of holdups. We also interviewed the police robbery details of five large California cities and obtained data from a former assistant warden of a Federal penitentiary who had interviewed 150 bank robbers being held in five Federal prisons. Then we compared the interview data with the recorded 5-year holdup experience and with other data on physical characteristics of the 14 bank offices.

From our preliminary research we concluded that a number of identifiable factors, or variables, do indeed appear to act as psychological deterrents. However, the importance of some individual factors seems to be strongly influenced by the presence of others. For example, good interior lighting and high exterior-to-interior visibility may be overshadowed as deterrents by the existence of several excellent escape routes. Or, the type of counter design may be insignificant if there are some male tellers behind the counters, particularly if they are known to be off-duty

policemen. There are clearly a large number of variables that both individually and collectively warrant analysis.

At this point, it would be useful to review briefly what the police think of deterrence; what a knowledgeable scientific investigator thinks; what the robbers say they think; and what we learned from the bank data and our own preliminary observations.

WHAT THE EXPERTS THINK ABOUT PSYCHOLOGICAL DETERRENCE

POLICE

At the time of our research, the Los Angeles Police Department (LAPD) Robbery Detail expressed the following beliefs:

- The sharp increase in bank holdups during the 1950's and the 1960's was the direct result of increasing use of the low silhouette counter line and the warm, "homey" atmosphere that banks were beginning to adopt.
- Bank holdups are encouraged by the imposition of inadequate sentences for convicted robbers and the predilection of judges to release captured bank robbers on inadequate bail, pending trial. In some cases, the criminal had been captured and released on bail for several previous robberies while still awaiting trial for the first offense in the string.
- Bankers virtually invite holdups by publicizing their policy of cooperating with the robber.
- The extensive freeway system, coupled with the nearly universal mobility of the population, has not only encouraged robbery; it has also diffused the geographic incidence of robbery, moving it away from the generally distressed areas, where it has been centered.

The San Francisco Police Department (SFPD) Robbery Detail agreed with the LAPD Robbery Detail and added the following:

- Officer-tellers are an effective deterrent (LAPD did not permit its officers to "moonlight" in this way because of the uncertain status of their injury-disability rights under such an arrangement).
- Uniformed guards inside the bank are effective deterrents.
- The news media dramatize holdup incidents, thereby encouraging additional attempts. One well-publicized holdup tends to produce a series of subsequent holdups.
- Banks that are close to tenderloin and ghetto areas are hit most often.
- High visibility within banking offices and between the outside and the inside is a strong deterrent to holdups.

The Oakland, San Jose, Sacramento, and Redwood City Police Departments generally concurred with the LAPD and the SFPD.

SCIENTIFIC INVESTIGATOR

Dr. George M. Camp, former assistant warden at the Marion Illinois Federal Penitentiary, interviewed 150 bank robbers who were held in five Federal prisons. The interviews were conducted for his doctoral dissertation in sociology (Yale University, 1967). His principal conclusions were:

- Robbers know and are encouraged by the fact that large amounts of cash are often kept at tellers' positions, despite bank management instructions to limit the amount of cash, and that the tellers are instructed to offer no resistance.

- Robbers greatly fear early apprehension, either during the actual holdup, or before they can flee and successfully disappear with the loot. Thus, they are primarily concerned with completing the robbery speedily. Camp concludes that factors affecting ease of acquisition of the money and speed of escape are the principal areas where deterrence can be improved.
- "Typical" robbers prefer a small bank with few employees and poor visibility from the outside.
- The robbers' firm belief that they can get away before the police arrive tends to reduce the effectiveness of alarms as deterrents.
- Low counters invite robbery; metal grilles are more "forbidding."
- Frequent, unscheduled police checks and visits by patrol cars are a strong deterrence to robbery.
- The presence of guards is not a great deterrent (although Dr. Camp found that only 10 percent of the sample banks that were robbed had guards).
- Very few bank robbers are irrational. Of the 150 interviewees, more than 130 said that they would have thrown down their guns if the police had demanded it.
- Publicity of robberies and the amounts taken is an inducement to rob banks.
- Prison inmates are an excellent source of information; more of the 2,000 to 3,000 robbers who are now incarcerated should be interviewed.

WHAT THE ROBBERS SAY THEY THINK

Some of Dr. Camp's observations given above were direct reflections of what the interviewed robbers told him. In addition, the interviewees provided the following information:

- Robbers are divided in their views regarding one or two entrances to a bank branch; the principal concerns are control versus flexibility of escape route. However, they view too many entrances as difficult to watch and as likely avenues from which they can be surprised. (This factor is probably less important to gangs of 4 or 5 persons who rob a bank.)
- Only 5 percent of Camp's interviewees picked a bank because it had no camera.
- Only 10 percent picked a bank because they knew it had no silent alarm system.

During our earlier research, we received several unsolicited letters from incarcerated bank robbers. They offered the following comments:

- In midtown Manhattan, New York City, crowd density was deemed desirable because of the mass confusion, protective coloring, the unlikelihood of an exchange of gunfire, and the difficulty of pursuit. This, coupled with the existence of many large corporations and some of the country's largest banks on virtually every corner, greatly encourage the act of a holdup.
- The slow traffic flow during the noon rush was considered useful. The correspondent said he had researched the matter and found the noontime average traffic speed to be 9 miles per hour (mph), as opposed to 13 mph at the turn of the century.
- Cameras are not a deterrent even though it was known that the camera would record the event.
- Bank-picking is like "comparison-shopping": especially attractive and big banks that have a "gold fish bowl" decor; low counters; and modern, bright, clean appearance.
- City banks are attractive to single holdup men, whereas suburban banks are preferred by armed gangs who flee in automobiles.

- Desirable getaway routes include subways, underground garages, tunnels, stations, streets, highways, and alleys.
- One robber preferred the city's largest bank on the city's "most prestigious" street.
- Newspaper accounts of bank robberies glorify the act and precipitate the very thing that the police are trying to discourage.

WHAT THE SRI TEAM DISCOVERED

As mentioned earlier, SRI obtained holdup and related data from a large banking house in California. We also made limited examinations of six branches in the Los Angeles area and eight branches in the San Francisco Bay region.

The branch locations and their 5-year holdup experiences are shown in tables 1 and 2.

TABLE 1

5-YEAR HOLDUP EXPERIENCE FOR 6 LOS ANGELES BANK OFFICES

Branch Location and Numbers of Entrances ( )	1963-1967 Holdup Experience					
	63	64	65	66	67	Total
Hollywood & Western (2)	—	—	—	—	2	2
Washington & Western (1)	1	4	6	—	2	13
7th & Spring St (3)	—	1	—	1	—	2
7th & Broadway (2)	1	5	4	1	4	15
Central-Jefferson (2)	—	—	1	1	1	3
Broadway-Washington (1)	—	—	—	1	1	2

TABLE 2

5-YEAR HOLDUP EXPERIENCE FOR 8 SAN FRANCISCO BAY AREA BANK OFFICES

Branch Location and Numbers of Entrances ( )	1963-1967 Holdup Experience					
	63	64	65	66	67	Total
San Francisco Airport (2)	—	—	—	—	—	0
Market & New Montgomery (2)	—	—	—	1	—	1
Morgan Hill (3)	—	—	—	—	—	0
Menlo Park (1)	—	—	—	1	—	1
Palo Alto (2)	—	1	—	—	—	1
Sunnyvale (2)	—	—	—	—	—	0
Sacramento Sixth & K (1)	—	—	—	—	—	0
San Jose (2)	—	—	—	—	—	0

An examination of the physical layout and internal and external characteristics of the small sample of branches mentioned above (N=14) led the research team members to some preliminary conclusions regarding factors that might encourage or discourage potential robbers.

Our findings indicate that frequently hit branches (one or more times per year) also tend to differ from others in the following ways:

- They are usually older and dingier in appearance and tend to be cluttered with old furniture, filing cabinets, office machinery, and stacks of records and reports. The woodwork, floor, and walls are not in as good condition as in branches that were not hit as often. Note that this contradicts the statement made by one of our incarcerated correspondent robbers.
- The frequent victim branches tend to have less floor space for customers with a resultant crowding, especially on Friday afternoons (usually pay days for numerous businesses that often surrounded such branches). In addition, these branches often have large pillars which impair visibility between teller positions and the "platform" (space for manager and operations officer).
- Interior lighting is comparatively low. In some of the more frequent victim branches, most of the interior lighting is obtained by reflection off the outside sidewalk, through partially closed venetian blinds, and off the ceiling.
- The victim branches tend to have poor visibility from outside. Although several have large windows on one or sometimes on two sides, these are all either shuttered by venetian blinds, obscured by drawn curtains; or, the reflection on the glass windows, coupled with low interior lighting, tends to reduce the visibility of the interior from the outside. Less frequent victim branches tend to have good visibility between outside and inside.
- An overriding factor appears to be the robber's desire for a variety of external avenues of escape. When such avenues exist, offering several routes through alleyways or through complexes of residential and other buildings, even a modern, well-lighted interior layout apparently becomes a suitably enticing target.
- We suspect, but have insufficient data to prove that the more frequent victim branches are likely to be located either on a broad boulevard with relatively low business-hour traffic, or at busy downtown intersections with high density foot traffic and contested, slow-moving vehicular traffic.
- Contrary to the observations of both the police and the incarcerated robber-correspondents, our findings suggest that low counterlines are deterrents and that the older high counter and wickets encourage robbers. It appears that a high degree of intervisibility between teller positions is either consciously or unconsciously viewed as a threat by would-be robbers.

This hypothesis is supported by two bodies of evidence:

- Of the 14 branches that were examined in detail during the earlier research, two had been hit significantly more times than the others (see table 1). In contrast to the others, these two had 42-inch counters along with 5- and 6-foot windows and glass partitions between teller positions.
- The holdup data depicted in table 3 also provides strong evidence that old fashioned, high wicket teller positions are more attractive targets to robbers than the modern, low silhouette counters. From the data, it can be seen that the ratio of preference is approximately two to one. Note that we do not have information regarding the types of locations in which the two major classes of counter lines were used. The influence of other variables could have had a substantial bearing on the results.

TABLE 3. *Bank holdups by type of counter (1967).*

Type*	Branches by Type of Counter		Holdups by Type of Counter		Ratio of Holdups to Type of Counter
	Number	%	Number	%	
1	554	59.0	102	43.6	1 to 5.4
2	104	11.1	17	7.3	1 to 6.1
3	281	29.9	115	49.1	1 to 2.4
	939		234		

* 1 - Flexible Counterline--Glass Top

2 - New Counter--with Window Openings

3 - Old Type--High and with Wickets

TABLE 4. *Bank holdups vs. number of entrances (1967).*

Number of Entrances	Branches by Number of Entrances (Approximate)		Holdups by Number of Entrances		Ratio of Holdups To Number of Entrances
	Number	%	Number	%	
1	141	15	108	46.2	1 to 1.3
2	704	75	118	50.4	1 to 5.9
3	66	7	7	3.0	1 to 9.4
4	28	3	1	0.4	1 to 28
	939	100	234	100.0	

° Holdup data obtained from the major banking house in 1967 indicates an interesting correlation between numbers of entrances to a branch and the numbers of times it had been held up. These data are contained in table 4.

Here it can be seen that the overwhelming preference of robbers is for branches having one or two doors. The results seem to support Dr. Camp's findings that numbers of entrances are matters of considerable concern and that robbers view too many entrances as difficult to watch and as likely avenues from which they can be surprised while committing the robbery.

° Despite Camp's finding that only 5 percent of the incarcerated bank robbers whom he interviewed picked a bank because it had no camera, it is our opinion that today the camera is probably a deterrent. At the time of Dr. Camp's work, cameras were not in widespread use. In the years following enactment of the Bank Protective Act of 1969, TV or still cameras became necessary; robbers increasingly took evasive measurements by wearing ski masks, shooting at or smashing the cameras, spraying the lenses with paint, and averting their faces to prevent their being identified by these devices.

- Finally, based on discussions with the SFPD, we believe that some percentage of robbers are motivated on the spur of the moment and that these are less likely to be deterred by subtle measures, such as numbers of doors, counter height, or level of illumination, than a more rational "professional" robber.

The limitations of our preliminary analysis of psychological deterrence are obvious: our sample was small and not systematically chosen to isolate cause and effect relationships. Even so, we were able to gather enough information to formulate tentative hypotheses about some of the factors that appear to affect deterrence significantly.

More comprehensive, carefully structured research would enable us to gain a better understanding of the factors that affect psychological deterrence and their interrelationships.

A good understanding of psychological deterrence is by no means limited in application to the areas of bank design, location, and practices. Later work in the area of protection of Armed Forces arms rooms and munitions storage facilities for the Department of Defense suggest that most of the principles discovered in the bank research are also applicable to weapons and munitions storage. Any general principles that may be developed in more comprehensive research will probably be applicable to a wide range of potential criminal targets. For example, many military post exchanges, clubs, and other money-handling facilities are robbed repeatedly. It seems likely that some useful guidelines could be developed to help these victims. The same applies to many small civilian businesses. And, of course, a general knowledge of psychological deterrence, if properly developed, could probably be extended to the protection of nuclear facilities and other critical installations.

One of the difficulties to be faced is that of making a distinction between guidelines applicable to casual or impulse intruders from those that apply to dedicated persons or gangs. Our initial efforts were focused, in a very preliminary way, entirely on the former. However, we feel that the initial findings are sufficiently promising to warrant a more comprehensive follow-up.

RECOMMENDED FOLLOW-UP RESEARCH

A follow-up research program might include:

- Rigorous, analytical research of environmental factors of a selected number of frequent victim branches compared to infrequently attached branches, for the discernment of major deterrence factors.
- Detailed, carefully structured interviews with statistically acceptable numbers of incarcerated bank robbers, to determine psychological and experience factors contributing to deterrence.
- Interviews with police, FBI personnel, and authorities associated with various research and academic organizations concerned with criminal behavior and psychology, for their observations and views.
- A plan for data collection; a methodology for predicting the relative effectiveness of possible deterrence measures and their costs, and for defining, analyzing, and measuring experimental and test results.

WORKSHOP SUMMARIES AND SYNTHESIS

KRAMER: The first workshop summary will be "Human Sensory Capabilities/Limitations." The summary and synthesis will be given by three of the four co-chair individuals in the following sequence: Commander Tom Niedbala, Naval Council of Personnel Boards; Dr. Robert Hall, Mission Research Corporation; and Dr. Charles Wallach, Private Consultant.

The second workshop, "Human Engineering of the Workplace," will be summarized by Dr. Dan Jones, Army Research Institute.

The third workshop, "Human Motivation, Attitudes, Error/Reliability," will be summarized by Dr. Earl Alluisi of Old Dominion University.

The fourth workshop, "Personnel Selection, Placement, and Training," will be summarized by Dr. Bill McClelland of the Human Resources Research Organization.

HUMAN SENSORY CAPABILITIES/LIMITATIONS WORKSHOP

NIEDBALA: Overall, physical security is essentially the protection of the integrity of various identified aspects of an organization's capability to operate its business or carry out its mission. Where nuclear materials are involved, the most important specific objective is to prevent unauthorized access to those materials.

People are involved in physical security to protect identified material or equipment against threats of disruption, theft, or damage of that material or equipment by other people—the adversaries. People are also involved as part of systems to detect threat imminence or for intrusion detection surveillance, be the threat terrorist, casual passer-by, burglary operation, deliberate sabotage, or vandalism.

Various electronic sensor aids may be employed as extensions of the senses to assist in detecting intrusion attempts or threat imminence, wherever the installation needs to be tailored to the environmental conditions of the site.

People are also involved in intercepting and controlling the adversaries to prevent access to the material or equipment threatened. We need to try to make our people as effective as possible in whatever mode they are involved—be it intrusion detection or encounter with the adversaries. Thus, we need to shape our people's behavior toward the highest level of desired performance.

One method which can be employed is the Pygmalion concept. In Greek mythology, Pygmalion was a sculptor who lavished so much love and attention sculpting his statue of a woman that his statue came to life.

In 1967, Rosenthal, in "Pygmalion in the Classroom," reported on a project in which an entire population of one of the elementary grades was tested at the beginning of the school year. The names of the students who tested exactly average were given to teachers as being exceptional students. By the end of the year, those students, in fact, had accomplished outstanding work. Essentially, this demonstrated the importance of teacher attitude upon student performance in the classroom.

Livingston, in the 1971 Harvard Business Review, reported on the Pygmalion concept in management and how the attitude of management and supervisors toward the employee can profoundly influence productivity and performance when the employee perceives that management regards him as a highly-valued performer. This creates greater self-esteem which in turn helps him to live up to management's expectations that he will be an outstanding performer. It is important,

CONTINUED

1 OF 2

however, that the employee perceive that the supervisor or manager is speaking the truth; otherwise, there will be a credibility gap.

In 1959, Edward T. Hall, a cultural anthropologist, in his book, "The Silent Language," proposed ten primary message systems by which we communicate with each other without words. We can easily transmit messages, indicating a low regard for another—and this is readily perceived—without any specific spoken words. The result may be reduced performance, where, with a little care and concern for other people, we could raise their self-esteem and, as a result, their valued performance.

At this point, it is worthwhile to comment on a generalized problem in physical security—how security is often perceived by management. It is often perceived, as far as cost and contribution to the productivity of the firm or organization, as pure overhead.

Therefore, to reduce this cost, minimum salaries are paid, turnover is rapid, and, from the standpoint of career development, both satisfaction and performance may be nil. Management must be convinced that physical security involves risk management and the minimization of certain risks, maximizing the readiness of the organization, or the ability to carry on its business.

If that business is $500 million per year, what is the value in minimizing the risk of the occurrence of a chaotic event which could totally disrupt or destroy the business? Surely, security people viewed in this light, indeed, become important.

The company insures against fire and comprehensive personal liability which could destroy the business. Security is the provision of insurance to safeguard the continued operation of the business or the operational readiness of the organization.

As to the adversary, we need to influence his behavior so that his decisions, based upon what he perceives of the situation, will be more advantageous to the protectors. Further work is definitely needed in this area.

Finally, one last word on rewards and recognition for rewarding good performance. Rewards should be immediate, and they need not be complicated. A simple smile, attentive listening to a worker's special problems, and a nod of approval cost little or nothing, but often suffice.

HALL: I am going to try to bring up some of the things that people suggested during the course of the workshop. I think we had good participation, and want to touch on a few things that may be important.

There were people really concerned about the problem of how do you sustain sensory performance and what can we do about it? Is there some training process in which we can engage? There was real interest in this approach.

There was a question about the things that affect sensory performance. For example many people, who are not like the laboratory type of person which I am or at least they don't come from that background, are quick to point out the effects of weather and the effects of transportation—the car one is riding in—maybe we should use golf carts, and this sort of thing.

There were a number of interesting ideas that tended to indicate how the security situation is tailored and affects the individual's sensory performance.

We talked about how you measure the sensory capacity of the guard. Typically, we use static acuity charts. We all know that dynamic visual acuity is a very important factor. However, it is possible to have people with good static acuity but with poor dynamic visual acuity.

What is done about the auditory capacity? What type of checks are performed periodically on people to ensure that they have reasonably good sensory capacities? For the guards, we talked about a training package that explains something about how their sensory capacities operate, what they are and what the guard might do to improve his or her capability is this area. The workshop revealed that we do not have "measures of effectiveness" in terms of being able to predict and sustain sensory performance.

If we want to improve the situation, what can we do? Do we increase patrols; do we buy more sensors? A gentleman from Canada asked: How does one measure how good the performance is now; what do we know about it? Would the level of security we have now indicate what level of security we should have?

It is very easy to justify your budget if you have a detailed plan. But how can you go to management and ask for more guards and more sensory equipment to improve security; how do you quantify that? How do you validate that statement?

There were a number of workshop comments about simulation and exercises—using techniques which would provide feedback and adapting some of the man-machine relations that have been learned from radar and other systems.

A number of people frequently talked about the problem of matching man to the sensor. We do not transmit an adequate signal to the observer to do the signature analysis. The desire to overload the observer is often the rationale that is used.

In many instances, we throw away valuable information which someone could use. For example if we have a sensor that goes off in a safe, it might be very beneficial to transmit any acoustic information so that the monitor could determine whether the safe is being drilled or that the noise is from some other extraneous sound (such as construction down the street).

Another idea was brought up and that is: What is the cognitive map of the guard in terms of the terrain and his surroundings? Has he ever been on the other side of the fence and looked at it from the standpoint of an adversary? Has he seen how he might approach his own position? Does he really know where every bush, tree, and rock is?

For example, in conditions where it is dark or there is something that might impair sensory capabilities, if the guard can hear a sound on a gravel walkway, he can immediately do a signature analysis that tells him when somebody is walking across a gravel walkway 20 feet away.

I guess this means that we can do better. We can do a lot better than we are doing right now. And I think some of the other speakers will bring this out.

WALLACH: I have attempted to analyze a relatively small sample (22) of the questionnaires returned by our workshop participants. I find it interesting that roughly 50 percent of the questions raised could best be satisfied by a tutorial approach to the workshop. The other 50 percent consisted mostly of specific problems that required a real workshop approach and open discussion.

We specifically asked for new directions in further research and development. Thirty (30) percent of the responses related to training requirements; 23 percent related to requirements for some sort of criteria to be developed.

Both the desired training programs and the desired criteria development seemed to involve three primary factors: vigilance, sensory capabilities, and motivation. There was heavy emphasis on the function of the individual guard.

Eighteen (18) percent of the responses involved requests for evaluation tasks that could entail actual R&D. In many cases, people didn't realize that these tasks had already been performed and the information was available.

For over 10 percent of the responses, interest was shown in the development of profiles—profiles of adversaries, profiles of the ideal guard recruit, and profiles of other particular functions involved in security which could be combined with criteria.

As a suggestion to the good people who organized this symposium, it might be of interest in the future to allow the participants to choose between a tutorial or a participating type of workshop. The choice will probably depend upon whether they have their own particular problems to discuss or just seeking an overview of the general subject being discussed in a workshop.

HUMAN ENGINEERING OF THE WORKPLACE WORKSHOP

JONES: I am fond of saying that human engineering cuts across all areas; in other words, man is an integral part of all our systems. I think the results of our Human Engineering Workshop will clearly show this.

We defined Human Engineering as the application of what we know about human performance and behavior to the design, training, and use of equipment and we discussed this in some detail.

We asked the participants: In what areas do you need more information and where would you like to see more research done? The following describes what we concluded:

First, we would like to apply the principles, methods and data of human engineering to see if we can influence the effects of duress, stress, boredom, and yet increase alertness.

Second, we would like to know how we can effectively use equipment that we have, since in many cases—cost being one thing—it is almost impossible to design new equipment to exactly fit user requirements. We simply have to accept the provided equipment, redesign, and reuse it to fit our own personal requirements. What can human engineering do for this?

Next, we want to do such things as task analysis, looking at workplace layout, duty cycles and SOPS. We'd be looking at the display/control layouts we currently have available and the display/control interactions.

The following questions came up: how many displays can one man handle, and under what conditions can he handle them? In what locations should those displays be? What types of controls should be used and how should we use them?

Next we wanted to look at human engineering as related to training and placement. We would like to design equipment for optimal use from both the operational and training standpoints. We would like to design equipment layout for the quality of the people that we get. We know that in many cases we do not get the world's greatest individuals to be security guards.

Recognizing these limitations, how is it possible to use and design the equipment so that an individual with an IQ of less than 190 can use the equipment best, it must be designed for his operation and not for operation by someone else.

A subject of great interest, I thought, was what do you do about security response devices and procedures? Not the design of the workplace where the guy works but designing the equipment that he may use to respond to a threat or an attack. We heard about the approaches banks use to solve this problem and, obviously, in our security layouts and our secured areas, we would like to know what we can do to make our response devices more effective.

We discussed the problem of internal identification. We have heard that in almost any attack or, in many cases at least, for actions involving sabotage, that there is an inside man involved.

What can we do for internal identification and control? What sort of human engineering procedures can be developed to make internal identification of individuals possible? What sort of internal procedures can be developed? How can we design these procedures from a human factors point of view to make them more effective?

Finally we discussed man/machine interactions and man/computer interactions. Based upon some of the information we heard yesterday, I think I'd have to add animal interaction. How can we human engineer the man, the machine, the biosensor, and the computer so that they all fit together as one integral system?

These are the areas we discussed and the research areas that we thought were important, essentially in this order, in our analysis of what were the key and important ideas from a human factors point of view.

HUMAN MOTIVATION, ATTITUDES, ERROR/RELIABILITY WORKSHOP

ALLUISI: I am sorry for Bill McClelland who speaks next, because I feel that everything I have to say has already been said. And I know if I repeat it, then there isn't going to be much left for Bill.

I represent the workshop group on Human Motivation, Attitudes, Error and Reliability. In our group were Pat Manion (Ms.), Bob Mackie, and Loren Bush. We were the group that used the matrix.

In one of our groups, Pat and I asked people to respond, listing the areas of research and interest in order of priority by referring back to the matrix. In other words, we purposely structured the responses. We asked the participants to list the areas of management actions, such as assignments of tasks, watch duration, watch schedules, and so on—a, b, c, d, e and f on the bottom. Or, if appropriate, to list needed areas of research on the characteristics of the job (the numbers on the left)—Task Characteristics, Performance Requirements, Importance of Performance, and so forth. Or if the research should be on characteristics of the human in the system, to list the things along the top, using Roman numerals I, II, and III.

Our colleagues—the other pair—didn't use this system but rather left it more unstructured. Let us see then to what extent we received common responses with either a structured or unstructured system. We have analyzed the whole thing as though it were one big pot.

The analysis indicates that using both frequency of mention and a weighted frequency of mention—those that are first, second, and third and getting a sum of ranks and being statistically, if not accurate, at least sophisticated—we came out with five general areas that seemed to be listed and based upon order of priority into three groups. Let me present and discuss those now.

The two listed at the top, research on systems tests and exercises, and performance feedback (ways of providing information to the humans in the system and to the managers as to the system's condition, capabilities, possible degradations, and weakness), were the two that we interpreted to be most important by the people who attended our workshops. Included therein were the methods of evaluating the reliability of the security system that included the manned part and the capability to say when the system is alert and what it can do now. These were listed in our first category, and they differed by a sum of ranks of one, which we held to be not substantially statistically significant.

The next category had one general area, namely, research on the assignment of tasks. This means, in the broad sense, that both the allocation of tasks between man and machine in the system and the allocation of tasks to the man, such as the use of secondary tasks as an alerting technique, and the question of when the alerting technique passes no longer alerts but begins to degrade performance. This is the whole area of being able to specify with greater accuracy and validity precisely what should be done in specific systems.

The third category also contained two areas, research on performance requirements (what is expected of the human in the system), and the system operation in the face of the environment and the threat.

The final category includes research on management attention, career patterns, and how to provide each.

I think what we have said can be summarized in two briefer, more general statements.

First we need to state our worth in compelling terms. Perhaps cost-effectiveness criteria is necessary, so that we can submit to management convincing words of proof that the job we are doing is important and that we are performing a very important function in a cost-effective way. Although this is a big task, it is only one part of what we are saying. The other part is saying that we want to develop a profession and a professionalism. What distinguishes a professional from a non-professional in this world? It is an internalized standard.

The professional is the person who knows what should be done and does not need a supervisor to tell him what should be done. We want to see professionalism developed, but we want it developed

throughout the system. We want to see the guard as a professional and we're asking for research to help us develop this capability.

There were some specific comments that we thought were particularly illustrative. Unfortunately we were not able to record all the comments and we have reworded nearly all of those we recorded. It should be noted that the following comments, that were presented, do fit herein.

- Research to show how we can recognize the importance of the job and demonstrate the importance through increased salaries.
- Determination of individual value and reward—this means finding appropriate rewards and that what is rewarding to one person may not be rewarding to another, so that you will know how to reward different people.
- Optimum operator loading—this has to do with our distribution of tasks or secondary loading. How much work should they have for best job performance when the job is monitoring?
- Analysis of different kinds of security functions and requirements—a really crucial first step. A good system analysis of types of security functions is needed to determine the real functions and requirements.
- Follow-up with descriptive analysis of current systems, including demographic and selection-type information—like what kind of person applies for the job of a guard? Why does he want to be a guard and what does he expect of the job?
- Proposal and the design of alternative ways of meeting the requirements in an analytical way. It may be that we have a system that has grown top heavy. We are doing things this way because this is the way we've always done it. This may not be the optimum. It may turn out that the humans we use should be used in entirely different ways, but we won't know until we take the first step; then the second step of seeing how we do it now; followed by the third step of designing some alternatives.
- Increased involvement of behavioral scientist researchers with firsthand observations of security system operations. What this means is don't sit back at your university or in your office at a desk and do your analysis on a piece of paper from a document you read. Go out there and walk the beat; go around and check the locks, and find out what the job is really like. Then maybe you will be qualified to state what your research can help with. I think this is important; we have to know firsthand what is going on, or we will tend to misinterpret by not being able to translate the words into real concrete images.
- Development of training and skill in maintenance training techniques, possibly through the use of simulation, including such things as games that teach tactics or that keep alive the tactics you have taught. The military is doing this; they are turning to it. Somebody thought it was a good idea for our security force to look at these concepts and practices.
- Identification of the inside adversary. This leads to a very intriguing thought. Can we learn how to specify the deterrent value of different aspects of the security system? What is the deterrent value of having a uniformed guard at a door? What is the deterrent value of having that uniformed guard inspect on a random basis a certain number of documents or packages that go in and out? This is an empirical question and we could determine the answer.
- We need to determine gender differences in vigilance, whether or not women and men can be equally vigilant at monitoring and whether or not there might be a difference according to the time of the month.

° More research in the area of subjective correlates—that is, how people feel and how feeling affects performance. This brings to mind an announcement I heard on the radio. I haven't seen the publication, but I'm told one exists.

In November or December of 1977 an announcement was made that a consulting firm in California had completed an analysis of civil aircraft accidents in which the fault had been laid to the pilot error. I ask Bob Mackie if it was his outfit or if he knew who made the study. Bob did not lay any claim to the work nor did he claim to know who did.

In a substantial proportion, 60 to 80 percent, of those cases, they were able to identify a serious life stress that the pilot was living with at the time of the accident. What happens to the performance of the guard when he is worried about some other life stress, not related to the job?

Someone asked me what do we mean by life stress. I said: I'll give you the answer a pilot gave to me, because I asked him the same question. The pilot said: "When the mortgage, the wife, and the stew are all overdue at the same time, that is 'life stress'."

PERSONNEL SELECTION, PLACEMENT, TRAINING WORKSHOP

McCLELLAND: While our order of presentation and our order on the program was last, we nonetheless probably have one thing to contribute which none of the other workshops have. Since you like psychological profiles of one sort or another, I would like to present to you a profile of the leaders of our workshop.

The organizer/worker/leader/catalyst of our particular workshop is a left-handed, Boston Irishman. Two of the people are Irish, three are left-handed, and three are from Boston. So there you have a good profile.

I want to do two things. First, I want to tell you what the major topics the attendees of our two sessions appear to be most interested in, incensed, or depressed about; and, secondly, a list of recommendations for research areas. Not all of the topics stem from the outline/agenda we followed.

The topic which appeared to be of the greatest single interest to the groups, and for which there seemed to be the greatest agreement (this was also true in other sessions that I attended), dealt with the reaction of people under various circumstances. Job analysis turned out to be the kind of thing we should know much more about—in terms of the personnel involved in the security force operation.

A topic, in the training area believe it or not, which seemed to get considerable attention is the need for standards and levels of performance coupled with the need for orienting training in security operations to the performance of certain kinds of jobs and duties.

I didn't hear anybody speak with warmth and affection in terms of the number of hours you should spend on small arms training and the number of hours you should spend on arrest procedures. Rather, it was what is a person supposed to be able to do in a guard activity, and that the training should be to teach him/her to perform at a given level of proficiency adequate for the system.

The topic of perceptions was mentioned but considerably underplayed. These include security personnel self-perception and their perception by top management and fellow workers. Relatively little, if anything, was said about how they are perceived by the general public.

Another topic on which there was considerable discussion is the kinds of restraints which exist in getting information; these are governmental constraints of one sort or another. Since there is variation in constraints at Federal, local, and State levels and also across state levels it is difficult to obtain information on the performance of certain kinds of personnel operations in security applications. Nobody had any good suggestions on this topic.

Related to the last topic is the variation that exists from jurisdiction to jurisdiction in matters of certification, the establishment of the "standards," or the hours that should be met in order to qualify persons for either Federal or private security forces.

The recommendations for research tend as well to be more general than specific. The need for research on techniques, procedures, methods, and devices for testing the efficiency and effectiveness of system output was identified in all workshop sessions. This is a very high-ranking research requirement.

A second research area is training and how it is conducted. Concern was expressed for improving the techniques, methods, and procedures by which guard training is accomplished.

A third research area is perhaps best characterized by the people who went from workshop to workshop saying: I'm worried about the problem of vigilance; I'm worried about the problem of boredom; I'm worried about the whole topic of a tedious kind of situation in so many guard contexts. Research certainly could be conducted to develop better techniques for enhancing vigilance and to reduce tedium in guard activities.

A fourth research topic was suggested, and this is a thorny one, in which clearly there would be interest and clearly not many of us have any good ideas of how to go about it or we would have already done it, had to do with whether it is possible to develop ways and procedures in selection to pick individuals based upon some of those less-tangible kinds of characteristics, like dependability, reliability and character traits.

Another research area is techniques to maintain guard performance. This area is not unrelated to the first topic, because we are talking about testing the system. If we both develop standards and orient the training so that persons could perform effectively, we could determine if guards could do the things they have supposedly been trained to do.

One research area that I have an excellent chance of butchering is a complex statement which involves the trade-off, blend, or optimum balance between reward—in this instance, a mostly tangible reward, pay, benefits, and so forth—and the kinds of characteristics that are required for successful guard performance.

This is an issue in which there was obviously tremendous variation in the experiences of those at this conference. The experience has been almost exclusively with guards who are paid $6,000 to $8,000 a year; in one case in a private force, the guards were being paid $20,000 a year. The point being that higher pay has been possible and has turned out to be economically feasible in some contexts.

An issue which has already been touched upon and one that, I think, should be underscored, is that it would be desirable to do research on the general issue of job ladders, or career development. We are not talking about just a single job, as far as security force operations are concerned; we are talking about a family of jobs.

Very frequently, you think you have just supervisors and guards. The situation is much more complex, and research should be conducted to determine whether this is really the case.

If it is only possible, because of the nature of the system, for the guard to go from being a guard to a job in some other area within the organization, then obviously we do not have a situation where there is much of a possibility for development of career ladders. But this may or may not be true, and certainly it will vary from organization to organization.

Another issue which seemed to get a lot of attention had to do with the role of women in high risk security jobs. Three examples were response force work, SWAT operations, and the recovery of stolen weapons.

I think this is an area in which research in some context is being conducted. It is an area that clearly some felt should be given greater emphasis.

One area, which I think most of you who aren't in the supervisory business, would feel a little unhappy about, or at least uncertain about, but which many people in our group did feel important, had to do with the training of supervisors. What is the best kind of training content and the best source of training experiences for people who are supervisors of guard force personnel? Again, this is related to the issues of career ladders and whether or not we have defined the jobs in any kind of meaningful and performance-oriented sense, based on analysis of what is required in the system itself.

Finally, there was considerable interest in a general topic which I will try to summarize in this fashion. I am speaking more about information passing, education, attitudes and perspectives than I am about the physical performance of tasks when I talk about security system education.

Certainly both operators and managers need to know how to make judgments when they are in a situation in which they have to choose between what the system actually needs and how each particular need is going to be satisfied by a change in procedure, a new concept, or new equipment. In a sense, this is a kind of physical security consumerism, from the perspective of people who operate the security system. This summarizes what happened in the Workshop on Personnel Selection, Placement, and Training.

PANEL DISCUSSION ON NEW RESEARCH THRUSTS

KRAMER: I'd now like to briefly introduce the members of the panel:

Colonel Herbert M. Dixon is from the Office of the Under Secretary of Defense for Research and Engineering and is also Chairman of DOD's Physical Security Equipment Action Group;

Dr. Harold Van Cott is Chief of the Consumer Sciences Division of the National Bureau of Standards;

Colonel Charles R. Linton, U.S. Air Force, is Director of Nuclear Surety, Defense Nuclear Agency;

Marvin C. Beasley is Program Manager for Behavioral Science in Physical Security at the Defense Nuclear Agency;

And myself, Joel J. Kramer, Group Leader, Human Factors, National Bureau of Standards.

Now that we have each heard the results of the workshops in terms of problems and researchable areas, we'll start with Colonel Herb Dixon and then move down the table for panel reactions and comments on what we have heard in terms of the synthesis and ideas with respect to where we should be going in the future.

DIXON: As was indicated, my primary responsibility in the Department of Defense is to attempt to develop some hardware to make our security personnel better.

During the course of the workshop, one of the people mentioned that in the Air Force the whole thrust has been towards replacing man as the sensor or detector with equipment. I didn't really realize, I guess, until after the remark was made that that is exactly what our whole thrust seems to have been over the past year—to try to accomplish what we call the four "D's" of security by depending more and more upon equipment and less and less upon the human.

Briefly, the first of our four D's is to deter; we use barriers, and lighting, security personnel and guard dogs.

The second D is to detect. Here we are, as I indicated, going more and more to electronic equipment to perform the detection function.

The third D is denial of access to the protected asset. Here, once more, we are looking more and more at the use of gadgets to try to accomplish this objective and less and less on man.

Ultimately, we say that if we cannot deny access and if the asset is sensitive enough, then we will destroy it before we will lose it. We have, once more, non-human devices that will be used to effect this disable or destruction function.

After listening to some of the presentations here and participating in the workshops, I think I am more and more convinced that we need to reorient our thinking. But on the other side of the coin, we believe that we also need to understand fully what it is that we have learned about the human.

Although there are questions yet to be answered, people have told us a lot of things that we do know. I wonder how much of what we do know is being applied to the development of this

hardware just trying to make this man better. As indicated, I also wonder if we really know what we know—what we have observed and seen through experimentation.

I am reminded of a story that a Marine friend of mine told me. He was running a lab, and he had a young second lieutenant who had just graduated from college and come to work for him.

He said: I want you to conduct some behavioral experiments on a frog. So the Marine took a frog, placed it on the table and said: Jump frog. And the frog jumped two feet. So he got his notebook and wrote down: Frog with two legs can jump two feet. Then he took one leg and tied it to the side of the frog and said: Jump frog. And the frog jumped one foot. Then he tied the second leg to the frog's other side and said: Jump frog. And nothing happened. He said: Jump frog. And nothing happened. So he got his notebook and wrote down: A frog with both his legs tied to his sides is deaf.

The point is that many times we conduct experiments and we are not aware that we are passing up some existing information because we do not have enough understanding of the whole process to come forth with the answers.

I see here an opportunity for us to begin to look very carefully and seriously at a program in human behavior research. For the past several years we have played at it and have not had any large scale money dedicated to this particular project. But I think that now it is time for us to begin looking at the structuring of a program to see what we can do to make the man better in his performance of the security mission and also to apply some of these human behavior answers so that we, the developers, might apply them to some of the items that we are trying to develop.

Human behavior is a very exciting field. Again, I would like to emphasize that during the workshops I heard papers that gave to me the feeling that everyone is enthused about the potential that this subject and field offers.

Motivation isn't something new that we are trying to instill. Back in the early management and organizational theorist days these same basic ideas existed. How do you get the person all charged up so he will go out and excel every day and hour he is on the job?

These are the questions we are trying to answer. Perhaps we will never answer them, but to me it is encouraging that we have so many dedicated people who are pointed in that direction.

I see now that our responsibility is to come up with some structured, funded program that has meaningful experiments which can begin to answer some of the tough questions that you, as well as others who are not here with us this afternoon, have been posing.

To summarize, I would simply like to say that I have enjoyed the symposium very much and I, for one, will support our getting on with the serious business of focusing in on a structured human behavior research program to fill the gaps in the total effort that haven't already been covered; this is one of the things that Bob Linton and I were speaking about earlier.

A lot of people have looked into the problem of how you make the infantryman who is in the foxhole out in the snow stay awake all night long, observe, listen, and report back. This is very similar to the problem of the security guard as we have been discussing.

How do you keep the aviator from forgetting to put the wheels down on his airplane when he comes in for a landing? Experiments have been conducted on such questions, but how do we draw all this together? How do we find out what we really don't know, and how can we apply all the research that has been done to solving some of these problems?

I can't pass up this opportunity to publicly state that I believe we could do it with a good data base. If we had a data base program, I think that we would really be in good shape.

VAN COTT: Wednesday afternoon, halfway through the workshops, Brian Jenkins leaned over and said to me that the physical security field has been growing at a very, very rapid rate. People in private security forces have been increasing at the rate of approximately 13 percent per year. In the military, they have been increasing at a very rapid rate. And yet, when he looks at this rapid growth, concern and emphasis on the problems of physical security, he is really surprised with the primordial condition of the applied sciences as they relate to physical security.

This has been the second behavioral science symposium that I have attended. My observation of this meeting is that the papers have been very high in quality. The quality and degree of workshop participation has also been high and lively. There have been a large number of really good suggestions about research areas and the problems with which research needs to be mated to.

I think we might be able to say that a dialogue has been started at this meeting between people in the practicing arm of physical security and people in the behavioral sciences. This is a good omen if something is started based upon our deliberations.

Our workshop cochairpeople have done an outstanding job of summarizing the research themes that have been discussed in the various workshops; so I won't attempt to reiterate any of them. It does occur to me, however, that we are faced with a major problem in this field; it is similar to that in accident research. Accidents are rare events. So are the kinds of events that take place in physical security systems.

This poses an interesting methodological question as to how to develop techniques for assessing the effectiveness of any kind of alternative policies that we might introduce into the training or selection of guards or into any other component of the system. I think this is something that deserves a fair amount of attention.

When you are dealing with a rare-event situation, how do you decide to spend your money? How do you get the data that will permit you to make these assessments?

In terms of the research themes—job requirements of personnel, training requirements of personnel, the problem of duty cycles and their optimum lengths—kept re-emerging as I wandered from one workshop to another.

Methods of evaluating the effectiveness of various policies came up frequently. The integration of the guard force within the whole physical security system also came up frequently.

It occurred to me as I listened to these discussions that while we know a fair amount about human factors and although a lot of information has been developed within the context of other kinds of systems such as space and military weapons, we are only at the beginning in knowing how to reshape this knowledge to the problems of physical security. This would argue for not new and basic research but for the reorientation of some of the principles and knowledge that we already have to the problems that are peculiar to physical security systems.

I certainly endorse Colonel Dixon's comments. If we have this information from the field of human factors—and we, indeed do—we need an information system and a way of bringing it together, sorting it, and sifting out the good from the bad. Like any other field there is bad information in the information system of the human engineer, as well as good. How do we sort it and then make available the good material, indexed in such a way that practitioners in the field as well as other researchers can get their hands on the kinds of information that they do need to solve their particular problems?

In summary, I have been pleased at how active everyone has been in trying to optimize the process of applying behavioral science knowledge to the problems of physical security.

LINTON: My narrow role in the security area tends to deal almost exclusively with nuclear weapons. Two major programs that we have underway at the Defense Nuclear Agency now are: the Theater Nuclear Force Security and Survivability Program, and the exploratory development of nuclear security equipment.

The security and survivability program is particularly related, as the title says, to the Theater Nuclear Forces, particularly those we have in Europe. As most of you know, over the years, the Strategic Nuclear Forces, the so-called triad that is made up of the bombers, Minuteman missiles, and the Polaris/Poseidon submarines, have done great things to make them more secure and survivable.

We harden the silos for the ICBM. The submarines are under water most of the time and today they are virtually undetectable. A certain amount of the bombers can be kept on airborne alert, and with a certain amount of minimum warning time we can get them airborne.

Our problems tend to be for those systems, particularly in Europe and other parts of the world, for which we do not have that same degree of protection. So as we get started on this multi-million dollar program, my involvement is with the security aspect. How do you secure those systems which have to be out in the field in relatively exposed areas? This is a big question, and we don't know the answers to it.

The other area that DNA is embarking upon, starting in fiscal year 1979, is taking over all exploratory development of nuclear security equipment for the services and pioneering those ideas that will eventually lead to hardware and techniques that will be passed into the advanced development stage to the particular service that either has a peculiar service requirement or has been designated as the lead service for that particular type of equipment. So in both of these areas—the exploratory development and the protecting of our theater nuclear forces—we are really looking for ideas.

While our job may relate only to the nuclear world, we realize that many of the things that we do would have application to the private sector and to other government agencies. During the course of the coming months, I openly welcome you to contact me at my office or Don Richards or Marv Beasley with ideas and suggestions as to how we might best go about handling some of our problems.

I couldn't help but notice how many times in the various workshops the idea of motivating the guard came up, because of the tedium problem. Ours is somewhat different perhaps from the private sector, to use Brian Jenkins' expression from the other day: the overweight, 58-year old, asthmatic guard who is thinking of going to Florida and playing golf.

We invariably have the 19-year old, high school dropout who is from a poor ghetto section of Birmingham, stationed on a northern tier SAC base—say at Grand Fork—when it is 40 below zero, and is out there alone. How do you keep him motivated?

Eventually, he becomes the private sector's problem because in many cases the man who spends 20 to 30 years as an MP or a cop in one of the services goes to work for the private sector when he retires. So, depending on how well or how poorly we do our job, I think greatly affects the quality of the person that you get.

One of the things that we are experimenting with—and we just concluded negotiations last week—is in making a terrorist movie. It is called: One Man's Terrorist is Another Man's Freedom Fighter. Again, we stole that title from Brian Jenkins. Brian actually helped us collaborate on the movie, giving us several good suggestions.

It is an animated film done in cartoon style. It takes about 30 minutes; we actually show how a hypothetical terrorist gang would plot the taking of a missile from a SAC base and what the reactions of the guard force and the eventual outcome might be.

Again, since we are dealing with the type of guard that I spoke of, we had to get somebody to do it that they can relate to. We were able to get Don Drysdale, who used to pitch for the Los Angeles Dodgers and now does many of the Monday night baseball broadcasts. He is going to narrate the film and do the lead-in, so that the guard can identify with somebody he knows.

The approach is something like this. Drysdale is going to be telling them: Baseball is a game of teamwork. While there are 25 guys on the team, there are only nine of them out on the field at the same time. And somebody has to sit in the bull pen and somebody has to be the utility man. But unless you are alert all the time, when it comes time for you to go into the ballgame, if you are not mentally and physically alert, you are not going to hack it.

This is the kind of lead-in that we are going to try. For those of you representing the various services here, as soon as we have the film finalized, probably in the next 3 months or so, we hope to make distribution to the Army, Navy, and Air Force for their use as they see fit for a motivational film.

I'm sorry I couldn't be with you the whole time, but on behalf of Admiral Monroe and General Cody, my bosses, I want to thank you all for your participation and to solicit your remarks in the months ahead to help us with the bog programs that we have.

BEASLEY: With respect to the need for a data bank; for the past 10 months, as some of you know, I have been involved with an in-depth study in collaboration with the military services, and with a lot of you in industry and government, dealing with the merits of and needs for a "central scientific and technological information analysis center," or "data bank" as some of you have referred to it for Physical Security Technologies. I am happy to report that we are just about ready to turn it loose for staff review and recommendations.

In wrapping up the panel at this time, I will not attempt to add to the information and the analysis that your panel moderators have made, except to say that we all owe them a debt of gratitude which I don't think we will be able to pay.

I am certainly not going to attempt, with my limited vocabulary, any comments on the welcoming speeches that were offered on behalf of the Bureau of Standards and the Director, Defense Nuclear Agency. Mr. Donaldson's and Admiral Monroe's welcomes set the tone, and you have responded magnificently. I know that I couldn't add anything to that most inspiring keynote speech of Dr. Brian Jenkins, or comment on his active participation in the two workshops that he was able to attend. I am, however, not reluctant to comment on some of the technical papers.

Dr. Bevan's paper on "Biosensors" left some of you cold with respect to "defender performance." I personally recognized some redeeming potentials for employing the phenomenon as a "people detector"—not like our shopping list of sensors which merely respond to any extraneous influence, which is necessarily related to people.

Dr. Weinstein's "rats" were only disturbing to me, in that he was better able to predict the response of his conditioned rats than I am able to predict the response for some of our trained guards.

Dr. Montor's "brain wave analysis" defies my mental processes. I am only thankful that Professor Montor has offered his help in defining how his findings can be related to security selection and training, an offer that DNA is most pleased to accept. So, we will be seeing more of Professor Montor in the future, and I know that you will all benefit from that assistance.

Dr. NiCastro's MAIT System has some definite benefits to offer in developing machine equations of threat scenarios, and we will be talking further with Lawrence Livermore Laboratory and Sandia Laboratory on this potential.

Professor Beres' startling suggestion of "rewards for terrorism" may be the reason that throughout this 3-day symposium LTC Glen Richards has stood by the exit escape route. I rather suspect that he may have been anticipating your requests for "payments in advance."

Dr. Andriole and Ms. Daly may have startled some of you by recognizing "that the total field of knowledge on adversaries" resides in the clipping services of the New York Times. While placing somewhat more credence on the other available source data, I do believe that the DARPA basic research program has merit in an applied sense and will be weighed against our security needs. We will be in contact with DARPA on this potential. I hope that we may get some additional suggestions along these lines from some of you in the audience.

Dr. Harris's "Link Analysis" had me lost at the third slide. But I would like to hear more about it. If 2500 police officers understand the methodology, the least I can do is learn what the intent of it is. And I will try to do that.

I am most indebted, however, to Mr. Tiffany's paper. He has solved my problems. If I may be permitted to quote his statistics, completely out of context, all we have to do, Colonel Linton, is to lower our high fences and cut in at least four more gates in the perimeter to reduce our nuclear weapons attack probability by 97.3 percent.

Ladies and gentlemen, the proof of your approval of our collective efforts is not in what you have said at this symposium. It is not in how you answered our questionnaires. The answer will be whether or not you would attend a fourth symposium on "The Role of Behavioral Science in Physical Security. Alas, that answer must wait until next year. So, until then, thanks for being here and for all your help and very generous contributions.

KRAMER: Before we invite some of the people from the audience to address any questions or reactions to the panel or workshop cochairpersons, I would like to briefly summarize what I think you heard at the workshops.

The best way of doing that is to think back to what Commander Niedbala said at the beginning of this session, describing physical security, the environment and its problems. And then think back to what Bill McClelland ended up with in terms of the description of all of those needed areas of research. We've seen a pretty nice mesh of things, in terms of a menu for the future and where we should be going. Many of these areas have been identified in the past. The last three days have reaffirmed these needs and importance as well.

I would like to thank the program committee, and I will mention those people again because they did help substantially in putting this program together.

Dr. John Fechter of NBS; Dr. Herb Leedy of the Department of the Army; Bill Immerman of NRC; Dr. Bob Mullen of NRC; Jack Hennessey from ERDA; my boss, Dr. Harold Van Cott, NBS; Marv Beasley, DNA; Lory Eliason of NBS's Law Enforcement Standards Laboratory; and John Nagay of the Office of Naval Research. They have all made a substantial contribution to this effort.

Let me just go through the list of the workshop cochairpersons. We had authoritative people in physical security, as well as in behavioral science: Bob Hall, Charles Wallach, Commander Niedbala, Gene Brown, Dan Jones, Tom Cook, Chuck Amazeen, George Byrne, Earl Alluisi, Bob Mackie, Loren Bush, Pat Manion, Bill McClelland, Preston Abbott, Gene Richard, and Colonel Barry. This is a very impressive group of 16 people who have made this symposium more comprehensive than those we have had in the past.

I would like to now turn to you who have attended and offer you the opportunity to ask questions of any of the workshop moderators and any of the people on the panel. We want to hear your reactions or comments.

[Question by Ralph Murphy, Consultant]

MURPHY: I must apologize for not having been here for the first two days of the session, but in the recap here today I noticed that there is one thing that seems to be missing in my estimation of the behavioral science symposium review of problems. That is, I didn't hear much in the way of discussion of good guys turning bad, and the motivation, psychology, and human factors of bad guys that make them bad.

It would seem to me that that is the nucleus of any security problem—to identify the enemy or the adversary in more precise terms rather than spending time identifying the tedium of training and requirements of the control people.

KRAMER: Let me attempt to answer that question by way of a little background history. In the first two symposia, we spent substantial time and effort, in both the papers and discussion, dealing with the area of adversary characteristics. To some extent the papers during previous sessions—I believe two or three of them—concentrated on the area of adversary characteristics.

The workshops that have been introduced this time—actually, the first time on a formal basis—were purposely aimed at the people side that we know most about and can possibly control the easiest. This is the good guys. They are there, and they are captive.

While historically, we have concentrated on both, we decided that the emphasis should be switched for the third symposium.

BEASLEY: I might add a little explanation to this question. Mr. Murphy did not attend the second symposium on "adversary attributes" that was held last year. However, I hope he will benefit from the proceedings, when they are available from the Government Printing Office. But, Ralph, we did minimize that area this year because we spent most of our last symposium on the subject.

NAME AND COMPANY (OR BUSINESS) AFFILIATION OF ATTENDEES

Abbott, Preston—Abbott Associates, Inc.
Alexander, John C.—Computing Devices Company
Alluisi, Earl—Old Dominion University
Anderson, Etta—Human Science Research
Andriole, Stephen J.—DARPA
Ansell, Patrick—Canadian Solicitor General Dept.
Amazeen, Charles—Northrop Corp.
Bach, Marie L.—Navy Regional Data Automation Center
Barnard, Bob—MERADCOM
Barry, Joseph A.—DARCOM
Beasley, Marvin C.—Defense Nuclear Agency
Beres, Louis René—Purdue University
Bevan, Thomas E.—Science Applications, Inc.
Brown, Eugene E.—Office of the Chief Security Police, USAF
Buchanan, Rodney O.—Burns International
Bukolt, Cesary—Defense Nuclear Agency
Bush, Loren L.—Nuclear Regulatory Commission
Brucker, Steve E.—TRW Defense and Space Systems
Born, Jr.—Aerospace Corporation
Byrne, George—SRI International
Campbell Jr., Winton G.—USA Nuclear and Chemical Agency
Carpenter, Robert J.—NBS
Chambers, Owen S.—NRC
Chan, Warren W.—General Electric—TEMPO
Combs, Pamela G.—Student—Northern Virginia Community College
Cook, Thomas—Army Missile Research and Development Command
Cross, William R.—Duke Power Company
Daly, Judith A.—DARPA
DeWitt, Emery—Defense Nuclear Agency
Diamond, Q. K. LCDR—Defense Nuclear Agency
Dixon, Herbert, COL—USDRE (Chairman, PSEAG)
Donaldson, John L.—National Bureau of Standards
Douglas, C. J., Gen—Decisions & Designs, Inc.
Doyle, W. P.—Dept. of National Defense (Canada)
Egan, Terry—Defense Nuclear Agency
Eliason, Lawrence K.—National Bureau of Standards
Eliot, Warner—MITRE
Ellett, James—Defense Nuclear Agency
Ennis, Jerry D.—U.S. Nuclear Regulatory Commission
Ervin, Nancy E.—Student, Northern Virginia Community College
Evans, Henry C.—JAYCOR
Fassnacht, F. B.—Naval Surface Weapons Center
Fechter, John V.—National Bureau of Standards
Fineberg, Michael—BDM Corp.
Finley, Brian—Sandia Laboratories
Foster, Richard E.—Student, Northern Virginia Community College
Fraser, Ian H.—RCMP
Rugler, B. A.—E. R. Johnson Associates
Gately, E. Stack—NAECO Associates
Gharst, Douglas—Student, Northern Virginia Community College
Glass, Arnold, LCDR—CNO

Gloye, Eugene E.—Office of Naval Research
Harris, Douglas H.—Anacapa Sciences, Inc.
Hennessey, Jack—Department of Energy
Hall, Robert—Mission Research Corporation
Hill, Jack—PME—121 Navy
Hoagland, Gregg K.—Student, Northern Virginia Community College
Holt, Arthur W.—NBS
Hutnick, Joseph, LCDR—CNO
Immerman, William H.—Nuclear Regulatory Commission
James, Joe—NRC
Jenkin, T. C.—R.C.M. Police
Jenkins, Brian M.—The Rand Corporation
Jones, Daniel B.—Army Research Institute
Johnson, CDR—NAVMAT
Keeney, Harry W., National Crime Prevention Institute
Kish, Michael, CPT—Defense Nuclear Agency
Koenig, Alfred L.—NBS
Kramer, Joel J.—National Bureau of Standards
Landry, Donald E.—Department of Defense
Lavelle, J. D., GEN—DDI
Leedy, Herbert—Department of the Army
Leverance, R. A.—Naval Surface Weapons Center
Lindville, Larry—Met. Police Dept.
Luttrell, John L.—Naval Surface Weapons Center
Linton, Charles R., Col—Defense Nuclear Agency
Mackie, Robert—Human Factors Research, Inc.
Maimoni, Arturo—Lawrence Livermore Laboratory
Manion, Patricia—Xerox Corporation
Manning, Bernard—Department of Defense
McClelland, William—Human Resources Research Organization
McWilliams, Judy—Essex Corp.
Mendelsohn, Barry—Nuclear Regulatory Commission
Midura, Thomas J.—AVCO Systems Division
Monroe, Robert R., VADM—Director, Defense Nuclear Agency
Montgomery, John—U.S. Nuclear Regulatory Commission
Montor, Karol—U.S. Naval Academy
Moore, Goerge C.—Assoc. Prof. Northern Virginia Community College
Moore, R. T.—NBS
Morrison, David—Naval Electronics Command
Moss, Milton—Defense Nuclear Agency
Moul, Dale A.—NUSAC, Inc.
Murphy, Ralph H.—Consultant, Mardeck Ltd.
Nagay, John A.—Office of Naval Research
Nelson, Doeg M.—ANPP—Ariz. Public Service
NiCastro, James R.—Lawrence Livermore Laboratory
Niedbala, T. F., CDR—Naval Council of Personnel Boards
Nolan, Raymond V.—MERADCOM
Norman, William—New Zealand Government
Norwood, George E., LtCol—Defense Nuclear Agency
O'Brien, John N.—Brookhaven National Laboratory
Okyen, Louis, COL—Defense Nuclear Agency
Oliver, Hebren W.—JAYCOR
Oliver, Robert W.—Universal Systems, Inc.

Olson, Douglas—Naval Weapons Support Center
Orlando, Louis D.—Student—Northern Virginia Community College
Padand, Frank—NRC
Perkowski, Daniel, CPT—Defense Nuclear Agency
Phinney, Bruce, LTC—Defense Nuclear Agency
Ramirez, Raymond G.—U.S. Nuclear Regulatory Commission
Reddick, Pat, CDR—Defense Nuclear Agency
Richard, Gene—Nuclear Regulatory Commission
Richards, Donald R., LTC—Defense Nuclear Agency
Robertson, L. P.—Sandia Labs
Rocchio, Elena—JAYCOR
Rock, Richard M.—National Marina Assoc.
Russell, Mac D.—Dynatrend
Sanderlin, James C.—Mission Research Corp.
Schechter, Richard—Lawrence Livermore Lab.
Schofield, David G.—NUSAC, Inc.
Sergeant, William T.—U.S. Department of Energy
Shaw, Eric—C.A.C.I. Inc.
Short, LaDonna J.—Project Office, Physical Security Equipment, Army
Siedlarz, John—HQ, USAF/SPP
Sketon, Robert—NRC
Slotnick, Mr.—Aerospace Corp.
Sochard, Irving J.—Naval Surface Weapons Center
Solomonson, Daryl—Mission Research corp.
Stewart, R., CAPT—Defense Nuclear Agency
Strauchs, John J.—The Gordian Corporation
Sweeney, James—Air Force Weapons Lab
Stewart, Dick, GEN—DDI
Taber, Daniel E.—Student, Northern Virginia Community College
Tharpe, Samuel Q.—Philadelphia Electric Co.
Tiffany, Willard—SRD International
Timma, Ron—GSA
Valimaki, Ronald E.—Naval Surface Weapons Center
Van Cott, Harold P.—National Bureau of Standards
Wallach, Charles—Private consultant
Ward, Ralph—Ralph V. Ward, LTD
Weinstein, Sidney—NeuroCommunication Res Lab
Wells, Milton R.—Student, Northern Virginia Community College
Welsh, William—NAVSEASYS COM
Willenz, Erik—Department of State
Willoughby, John K.—Science Application, Colorado
Wimpey, Frank—Science Application, Virginia
Woodridge, E. L.—The MITRE Corporation
Worrell, G. P.—Naval Surface Weapons Center

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:1980-311-046/368

END