DNA-TR-83-32

Proceedings of the
Sixth Annual Symposium
on the

Role of Behavioral Science in Physical Security

3-4 June 1981
Springfield, Virginia

Sponsored by:
Defense Nuclear Agency
Nuclear Security Division
Washington, D.C. 20305

dna

Approved for public release;
distribution unlimited.

DISPOSITION

Destroy this report when no longer needed. Do not return it to the originator.

DISCLAIMER

The findings in this report are not to be construed as an official Department of Defense position unless so specified by other official documentation.

WARNING

Information and data contained in this document are based on the papers available at the time of preparation. No attempt has been made to edit papers. The views expressed in them are those of their authors and should not be construed as representing the Defense Nuclear Agency. Correctness is the sole reponsibility of the authors.

TRADE NAMES

The use of trade names in this report does not constitute an official endorsement or approval of the use of such commercial hardware or software. The report may not be cited for purposes of advertisement.

COMPONENT PART NOTICE

THIS PAPER IS A COMPONENT PART OF THE FOLLOWING COMPILATION REPORT:

(TITLE): Proceedings of the Symposium on the Role of Behavioral Science on Physical Security (6th Annual) Held at Springfield, Virginia, 3-4 June 1981.

(SOURCE): Defense Nuclear Agency, Washington, DC.

TO ORDER THE COMPLETE COMPILATION REPORT USE AD-A141 426.

THE COMPONENT PART IS PROVIDED HERE TO ALLOW USERS ACCESS TO INDIVIDUALLY AUTHORED SECTIONS OF PROCEEDINGS, ANNALS, SYMPOSIA, ETC. HOWEVER, THE COMPONENT SHOULD BE CONSIDERED WITHIN THE CONTEXT OF THE OVERALL COMPILATION REPORT AND NOT AS A STAND-ALONE TECHNICAL REPORT.

THE FOLLOWING COMPONENT PART NUMBERS COMPRISE THE COMPILATION REPORT:

AD#:	TITLE:
P003 369	Personnel Fatigue in Closed Circuit Television Assessments.
P003 370	The INS Enclosed Space Detector Program.
P003 371	Physical Security Man-Machine Interface: An Operational View of Security Functions.
P003 372	Biotechnology Predictors of Physical Security Personnel Performance.
P003 373	Privacy and the Loss of Privacy and Their Possible Relationship to Military Security Guard Performance: An Analysis of the Issue.
P003 374	Generic Adversary Characteristics and the Potential Threat to Licensed Nuclear Activities from Insiders.
P003 375	Staffing and Shift Hours: Performance Considerations.
P003 376	Problems in Guard Force Training.
P003 377	DoD Guard Tactics Simulation: A "Free-Play" Role-Playing Methodology for Security Training.
P003 378	Unconventional Threat Assessment.
P003 379	Behavioral Science: Events Outside the Skin.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER DNA-TR-83-32	2. GOVT ACCESSION NO. ADA141 426	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* PROCEEDINGS OF THE 6TH ANNUAL SYMPOSIUM ON THE ROLE OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY		5. TYPE OF REPORT & PERIOD COVERED Technical Report
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR*(s)* Compiled by Major Barbara G. Curtis, USA		8. CONTRACT OR GRANT NUMBER*(s)*
9. PERFORMING ORGANIZATION NAME AND ADDRESS Defense Nuclear Agency Nuclear Security Division Washington, DC 20305		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS		12. REPORT DATE 16 November 1983
		13. NUMBER OF PAGES 212
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)* Director Defense Nuclear Agency Washington, DC 20305		15. SECURITY CLASS. *(of this report)* UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A since UNCLASSIFIED
16. DISTRIBUTION STATEMENT *(of this Report)* Approved for public release; distribution unlimited.		
17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)* Physical Security Human Performance Threat Assessment Training		
20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)* These proceedings represent papers presented at the 6th Annual Symposium on the Role of Behavioral Science in Physical Security which was held in Springfield, Virginia on 3 and 4 June 1981.		

TABLE OF CONTENTS

PERSONNEL FATIGUE
IN
CLOSED CIRCUIT TELEVISION ASSESSMENTS

Joseph A. Barry

June 1981

Prepared For

DEFENSE NUCLEAR AGENCY
Sixth Annual Meeting
on
The Role of Behavioral Science in Physical Security

by

THE LOSS PREVENTION INSTITUTE, INC.
286 Congress Street
Boston, Massachusetts 02110

ABSTRACT

PERSONNEL FATIGUE IN CCTV ASSESSMENTS

This paper was prepared in response to a concern expressed by security professionals on a personnel fatigue factor in CCTV assessment assignments. A number of different engineering, procedural, physical and psychological variables have to be considered regarding the use of CCTV security systems by government, industry, equipment manufacturers, financial institutions, law enforcement agencies, penal facilities, and retail management.

The Sixth Annual Meeting of the Role of Behavioral Science in Physical Security Conference, sponsored by the Defense Nuclear Agency created the opportunity to document existing practices, hear the operator's concerns, review procedural problems, discuss industry rationale for constraints on CCTV operations, explore CCTV hardware manufacturing guidance and original equipment manufacturing (OEM) or vendor required engineering modifications, and stimulated input from security professionals on this subject.

This paper addresses issues that require answers in today's world of high technology, insight into human resource requirements for CCTV monitoring, engineering and environmental factors, procedural and training standards, all as they pertain to personnel fatigue on individuals assigned to monitor CCTV systems.

CCTV equipment manufacturers offer little or no guidance on how to best utilize their equipment in accordance with established security procedures. Contract guard companies function under client imposed restraints that may hinder proper use of CCTV equipment. Some banks and retail firms have prohibited individuals from experiencing more than an hour of uninterrupted CCTV monitoring while some manufacturing firms insist on an eight hour period of monitoring by an individual. Law enforcement facilities generally assign CCTV monitoring contingent upon staff availability. In short, the equipment is used in as many different ways as it has users. The only constant is the human element.

Initial data indicates that human monitors of CCTV are subject to boredom, eye strain, headaches, and a desire to be reassigned. As a result, the user often fails to obtain the level of security that led to the investment in the equipment. Attempts to reduce fatigue have been made through sequential switching, audio and video distractions, cockpit design, sensor activated systems and other engineering advances. However, these steps are being taken in the absence of solid behavioral studies of the behavioral factors involved.

This paper points out that CCTV monitor fatigue should be evaluated in terms of current standards and procedures established for the use of the hardware and by accepted behavioral research methodology. Hardware engineering and procedures have been developed and examined without much consideration or integration of the human factor. Further deliberation is necessary to create appropriate ways of dealing with fatigue and its effect on the effectiveness of CCTV.

TABLE OF CONTENTS

I. INTRODUCTION

A. BACKGROUND AND RATIONALE FOR THE PAPER

The impact of personnel fatigue in closed circuit television (CCTV) assessment has not enjoyed a high measure of concern or research effort over the last twenty years. Over seventy-five studies have researched stress or vigilance in such areas: airplane cockpit, intrusion detection system consoles, sonar systems, and air traffic control and equipment design. Only six recorded studies could be found that addressed fatigue as a factor in CCTV assessment. While indicating fatigue as a factor these studies did not address the operational concerns informally voiced by security professionals over conflicting guidance between assessment standards, personnel training, and duration of assessment requirements. Government, industry, equipment manufacturers, financial institutions, criminal justice facilities and retail operations all appear to operate CCTV security systems under a number of different engineering, physical, procedural and psychological variables.

The opportunity to review recorded studies, document existing practices, hear the operator's concerns, review procedural problems, discuss industry rationale for constraints on CCTV operations, explore CCTV hardware manufacturing guidance and Original Equipment Manufacturing (OEM) or vendor required engineering modifications, and input from security professionals was fostered by the Sixth Annual Meeting of the Role of Behavioral Science in Physical Security Conferences, sponsored by the Defense Nuclear Agency in June 1981.

B. GENERAL HYPOTHESIS AND SPECIFIC ISSUES TO BE REVIEWED

This paper is designed not as a behavioral study but a research paper which has as its general hypothesis that personnel fatigue in CCTV assessment is a real problem, one that has been under-researched, and one that hardware engineering has unsuccessfully attempted to resolve. Variable operational standards have only served to accentuate the inconsistencies between hardware, men and procedures. For the purpose of this paper, assessment is defined as the process of detecting, evaluating, and reacting to incidents or signals displayed on a CCTV monitoring screen. Surveillance is included in this definition. Fatigue is defined as that momentary or progressive decrement to performance reflected either by decreased response to a screen incident or increased probability of missing the incident altogether. Such behavioral changes may be accompanied by physiological changes that are indicators of reduction in the individual's level of arousal (O'Hanlon and Beatty, 1977). Survey data will disclose a wide variety of ideas by users on how to operate similar equipment. Engineering variables will range from sensors, audio/visual alerts, and programmed switchers to the number and size of the monitors. The assessment of environmental variables considers shape, design, lighting, noise level and temperature. Assessment duration time, other task requirements, watchloads, qualifications and training, and rotation of jobs are the major procedural variables to be addressed. Physical health considerations include evidence of eye strain, headaches and in some cases reports of cramps, numbness, and pain. Reports of emotional stress, fatigue, job anxiety and social pressure are also covered in psychological health considerations. All the above are presented without clinical analysis or validation. They represent raw indications of a weakness in one aspect of the physical security system.

C. AN OVERVIEW OF DATA COLLECTION TECHNIQUES

The concept that environment, equipment engineering, procedures, policies and other events may influence an individual is by no means new. Information on these concepts has been gathered for hundreds of years. The importance of vigilance to various tasks such as air traffic control, nuclear plant operation, safeguarding resources, and motor vehicle operation has prompted a variety of reseach directed at determining the variables that enhance or degrade vigilance. Many of the studies conducted in controlled laboratory settings have application to nuclear weapon site security guard performance. Many characteristics indicate security guards are prime victims of reduced vigilance (Mackie and Miller January 1980). All of these studies touch on fatigue but only a few deal with the issue of CCTV assessment and fatigue. These few studies view fatigue as a by-product of other causes, and therefore, add only a small data base to this paper.

In order to obtain additional operational data, other sources were developed. Sales and engineering representatives from three major manufacturers of CCTV were interviewed to obtain data about anti-fatigue efforts or applicable study results. Ten major high technology manufacturing firms provided input from corporate and facilitiy security management personnel. Interview data from over a hundred CCTV operators was compiled. Six manufacturers authorized representatives and vendors were solicited for comments, fifty physical security surveys on penal facilities, financial institutions, retail operations and precious metal operations were reviewed. Interviews with numerous members of the American Society for Industrial Security added additional data. Lastly, the personal experiences of the author and four close associates were collected to complete this data base.

II. DISCUSSION OF VARIABLES

A. GENERAL

There have been many surveys and studies done on TV monitoring, mostly by networks and advertising agencies. These inquiries have focused on determining what type of program the audience is watching during what specific period of time. They involve voluntary concentration and a level of behavioral arousal influence by what is happening on a screen. Few studies have looked at CCTV as a single system. The best of these studies has been a three-part series by A. H. Tickner all dealing specifically with CCTV. However, the issue of fatigue as a part of vigilance is only addressed for short viewing periods (30 to 120 minutes) and does not address security guards in an operational setting. Peripheral studies included brief considerations of the major theories concerning vigilance performance and then address the influence on vigilance of such variables as background event rate, signal probability, signal complexity, signal-to-noise ratio, signal duration, sensory mode, environmental stressors, overall monitoring load, social influences, personality traits, use of drugs, sleep disruption, variation in psycho-physiological arousal, watch scheduling, state of health, motivation, and performance fedback. Fatigue is treated as a decrement factor decreasing vigilance in these studies. Both the studies and the testimony of the guards we surveyed indicate that a lack of vigilance is the most common mistake made in the performance of the security job. (Hall, Hannah, Weaher and Benner 1979b). Vigilance literature does suggest both important variables and theoretical constraints that have potentially significant implications for guard force performance. Research to date has been related to the guard force with respect to four general characteristics of the vigilance task and its setting:

1. Stimulus conditions that may affect vigilance.
2. Characteristics of work environment that may affect vigilance.
3. Characteristics and health status of individuals that may affect vigilance.
4. Operational procedures that may affect vigilance.

CCTV studies to date contribute to evaluating monitoring load, display design, and watch scheduling, rather than fatigue as a decrement to assessment. Few researchers have attempted to model monitoring tasks after the real world monitoring requirement.

B. ENGINEERING VARIABLES

In general, studies on vigiliance are available but not studies addressing the impact of engineering on assessment fatigue. Manufacturers of CCTV systems do not acknowledge the existence of any fatigue studies for user guidance. Vendors or OEM representatives do, however, acknowledge attempting to engineer into the systems ways to reduce error and boredom. Personal experience by consultants in the safeguard field indicate user preference to such sensor driven or automated systems versus multi-screen sterile viewing. Engineering efforts and studies were found to include sensor activated CCTV systems, sequential switching units, audio or visual alerts and panel design. The reasons for the engineering efforts in the above areas were numerous but none specifically addressed the fatigue problem.

Sensors...

There are a number of CCTV security systems on the market that employ intrusion detection sensors of various types to actuate or draw attention to a specific field of coverage. Assessment is more easily made by the operator who waits until the picture is actuated by a sensor instead of constantly viewing a screen for an event. In this area no studies could be found that attempted to determine any difference in fatigue or vigilance. Practical application in industry has resulted in evidence that a rapidly moving event such as an individual or vehicle crossing the zone of coverage could be missed due to switch-on delays. Most application of sensor driven CCTV systems merely transfer the picture from a smaller monitoring screen to the main monitoring screen to alert the viewer that an event has taken place. Security guards have expressed greater confidence in the event detection with sensor driven CCTV systems. Engineering can cause a pan, tilt and zoom unit to view in on the specific area covered by a single sensor being activated. Vendors and OEM responses to data collection for this paper indicated their preference for a sensor actuated monitoring system over the constant view type. Vigilance studies support the idea that the stimulus of the event coming up on a blank screen or the interruption of one event by an overriding event replacing it on center screen captures an individual's attention because it is now sudden or unexpected (V. Machworth 1969). The reinforcement theory dealing with operator conditioning indicates that vigilance performance will be improved, and the degree of decrement reduced, by the use of the signal injection technique. Use of sensor activated cameras should achieve the same result. The problem is that the concept should be studied to determine the degree of effectiveness.

Sequential Switches...

These devices are designed to allow CCTV monitors to watch the zone of coverage for more than one camera on only one monitor for a pre-set period of time. A guard would watch twelve camera-views on one monitor-view and see each camera field for half a second to two or more seconds. This equipment eliminates the need for one monitor per camera and a monitoring task involving twelve different screens. These switching units can be manual, automatic time sequence with a manual override and automatic with a sensor activated override. Tickner's studies showed that the greater the number of screens monitored the lower the observer's reliability. (Tickner, A. H., Poulton, E. C., Copeman, A. R., and Simmonds, D. C. V., 1972). Over 100 users of security CCTV systems were surveyed for this paper. All users who had six or more cameras used switches (82). None of these users expressed fatigue as a reason for the procurement of switching equipment. Eighty users thought it should reduce fatigue while the remaining two (six cameras and eight cameras, respectively) stating that they didn't know.

Audio or Visual Alerts...

Studies have been conducted indicating the value of audio and/or visual signals in security system monitoring. A general finding is that audio signals are more effective to the human monitor than visual (Hall, et al 1979b). When systematic visual scanning is required, an audio signal produces a higher degree of vigilance and guard acceptance than a redundant visual signal (Colquhoun 1975). NRC design guidance for Central Alarm Station (CAS) and Secondary Alarm Station (SAS) facilities (Wait, H. J. 1981) specifies indicator lights, indicator flash rate, degree of brightness, visual axis, and size and color considerations. Their guidance on audio alerts states only that they be used sparingly and for urgent warnings. While some of their other design criteria indicates fatigue as a consideration it is not reflected in either audio or visual signal comments. This document indicates the signal value increases with size brightness, loudness or motion of a signal. Additionally, it states that an effective warning device will attract the attention of a busy or bored person. Of our 100 CCTV system user population only three employed audio/visual alerts. These three (a federal nuclear facility, a federal prison and a state penal facility) were equipped with sensor driven pre-programmed sequential switching devices. Operators interviewed expressed more confidence in the automated systems and indicated that they were more prone to be alert than with the previous system which had banks of single monitors. Six of eight guards had experienced monitoring with and without the switching device and audio alert devices. They stated that the old system "turned them off" mentally after about an hour and their observation was without event recognition.

Panel Design...

Panel design has been studied for years, not for CCTV assessment but for alarm system assessment. In this case again fatigue is not specifically addressed as a prime factor but as a possible reason for vigilance decrement. Peripheral studies have been done on airplane cockpit design establishing both lateral and vertical instrument placement constraints. Tickner's research indicates that clutter and observation distance from screens are factors that impact on performance degradation. His maximum desirable number of screens to be viewed when there is frequent movement is nine.

The NRC CAS and SAS design and procedures manual calls for video recorders, tilt, pan and zoom camera features with automatic sequential switching. Display consideration that affect operator performance are stated as:

1. Size--more time is required to scan an extremely large display.
2. Shape--the frame around a CRT display should conform to the general configuration of the screen.

The combined efforts of the Air Force and Sandia Laboratories indicate that the most effective way to array CCTV screens is on a lateral line. It's hard to understand, then, why the FIDS program is designing a cluster of two up and two down for its panel.

Actual design as reported by user survey and on site consulting ranges from isolated cockpit style design in some retail and financial institution systems to CCTV panels mounted overhead or behind the observer who has access control tasks that require vision away from the field of CCTV screens. As many as forty screens per operator and mixed fields of view with multiple views of the same fields displayed out of view sequence were the worst cases found. Interviews with guards and user comments indicated that poor design was more likely to result in an observer "turn-off" (self-imposed reliability reduction) than fatigue or stress. If the design is inconsistent with the tasks required, the observers reject the design and intentionally ignore the CCTV in favor of other required tasks. The recent installation of forty cameras watched through forty screens by one man at Oak Ridge illustrates poor engineering resulting in watch overload.

Vendors and OEM representatives report the necessity to employ audio buzzers, instant playback, tilt, pan and zoom cameras, and programmable sequential switchers as necessary sub-elements of CCTV systems. Fatigue and distraction are credited by them as reasons for these special engineering components being incorporated into a system. Their experience, not studies or manufacturer guidance, indicates the need for this type of engineering at the time of local application.

C. ENVIRONMENTAL VARIABLES

Temperature: Poulton (1977) emphasized that the most physically comfortable environment is not necessarily the optimum environment for vigilance tasks such as CCTV monitoring. A modest amount of temperature initiated stress enhances effective monitoring. Mild heat helps but moderate heat induces fatigue. World War II studies have shown that sonarmen housed in warm cabins, free of noise and distraction frequently fell asleep on the job. Cold and wind also, have a degradation effect on monitoring. Data on the latter is extremely limited due to the nature of the studies done to date. Fatigue-decreased proficiency studies have been criticized because they were laboratory tasks performed over short periods of time. Long term exposure to heat and cold has not been sufficiently studied. Over seventy-five percent of the users surveyed for this paper indicated heat as a fatigue problem. Less than fifty percent (47%) indicated that cold was a degradation factor. None of those giving a positive reply to temperature problems know of any existing standards or guidance in this area.

Noise level: Background event rate or noise is considered an important characteristic that affects performance on tasks such as CCTV monitoring (Hall et al 1979b). The higher the background noise introduced into the experiments, the lower the accuracy and frequency of response. Where all background noise was removed, sleeping on duty became a problem. Arousal theory studies confirm the need for some level of background noise. Commercial users surveyed indicated a higher amount of background noise than government users. Commercial users also indicated that the presence of an extremely noisy background setting caused the monitor to reduce his level of monitoring effectiveness rather than developing stress or headaches.

Lighting: Peripheral studies and discussions with Air Force Personnel and Base Installation Security Systems (BISS) contract personnel surfaced information that illumination, if too bright, glare producing, or too dim produces a degradation in monitoring vigilance. The studies reviewed in preparation for this paper offered no information in addition to the points mentioned above. The NRC CAS - SAS Work Station design and procedures manual mentions illumination as one of the ways to combat fatigue. Comments from the user survey provided a wide range of information. Monitoring sites surveyed ranged from only the light provided by the screens themselves to daylight conditions 24 hours per day. Those activities such as retail and banking facilities that use CCTV for surveillance operate in minimum light without degradation. In a large part the effectiveness of their operation may be due to the fact that they rotate their monitor personnel between every 30 and 45 minutes. Some facilities such as several manufacturing plants, three penal institutions and one GSA guarded facility report sleeping as a problem when a lone monitor is on duty and supervision is infrequent or when tasks are minimal. Full daylight conditions were reported as a problem in those cases where lighting and console design resulted in glare to the operator's eyes.

D. PROCEDURES AND POLICIES

Probably the area that has the greatest impact on fatigue, stress and vigilance is procedures and policies. This represents the most complex issue of this paper. Staffing policy, assessment workloads, task rotation policies, training standards and personnel selection procedures all may impact more directly on the individual than the previously discussed variables. Behavioral studies, both CCTV-specific and general vigilance yield results that form a framework for procedures and policies. Actual data from this study survey indicates little of the resultant information has been implemented in developing contemporary guidance to both the government and the private sector. The variance in existing procedures and policies create opportunities for operator degradation.

Staffing studies indicate that the number of operators or monitors is based on such factors as system design, number of screens, manual or automatic support equipment, and other duty post requirements. The Underwriters Laboratories (UL) standard 611 - Central-Station Burglar Alarm Units and Systems recommends a minimum of one operator if the number of alarm subscribers is less than 100. For a UL planning figure, that standard translates to one operator per 100 alarm points. CCTV screens are considered by UL to be a monitoring or alarm point.

Studies and survey data do not support this aspect of their staffing guide. The survey conducted for this paper indicates staffing patterns range from one person per three cameras (with and without an alarm panel) to the recently installed Oak Ridge CCTV system employing one operator to monitor forty cameras through forty screens. Study findings show that as monitor task overload increases, stress and fatigue increase while vigilance is continued at a set level. However, continued long term stress and fatigue causes an involuntary reduction in vigilance. Workload studies to date address, almost completely, short task assignment and not eight hours of constant monitoring such as practiced by the U. S. Air Force and many segments of commercial security. The NRC CAS-SAS manual cites studies which show that the length of time an operator can perform his duties efficiently ranges between two to eight hours. Efficiency normally decreases about two hours after work begins. Another reduction is experienced at the middle of the second half of the day with an increase in efficiency being experienced an hour before end of shift. Most studies in this area have used task lengths of 60 minutes or less. None could be found addressing 8 hours or more. The studies of this short a duration are not helpful for determining optimum watch duration.

Input from the user survey indicates a wide difference in duration data. The Army and the Navy use a four hour duration as a standard. The Air Force uses eight hours. The 15 penal institutions in the survey group settled for a four hour duration using an average of eight cameras and alert signals from either duress or alarm sensors. The duration policy of several Fortune Five Hundred companies ranges from none, which translates to eight straight hours, to four hours using guard rotation. Medical facilities (25 hospitals) have an average of three hour posts per shift, seven days a week. Major manufacturing firms such as Raytheon and Texas Instruments go to an eight hour monitoring shift with post relief on a contact basis. Small businesses, hotel security, warehousing, trucking, jails, and TV and radio stations are not staffed to rotate tasks so their duration is normally eight hours with as many as six authorized breaks by contact per shift. Six major guard companies were contacted for position and policy information on watch duration. All but one indicated concern over duration as a factor in efficiency and to a lesser extent fatigue. Five of these firms settled on four hours as a reasonable duration for CCTV monitoring. Their opinion was based on a combination of guard feedback and "gut feelings". All six indicated that their thoughts on the matter were irrelevant as they had to comply with the policy of the customer and unless the contract had sufficient manning to rotate personnel they enjoyed no flexibility. The remaining users established their own duration based on perceived need, workload, and staffing levels.

It was interesting to note that high intensity surveillance for events such as shoplifting and bank monitoring required rotation every 20 to 40 minutes where staffing would permit. Rotation studies have shown that frequent shift rotation does not allow individuals to establish a new sleep wakefulness cycle thus increasing fatigue and stress while reducing vigilance (Cantrell, G. K. et al 1968). An instance where rotation did not resolve degradation problems was cited in an Air Traffic Controller Health Study (Rose, R. M., Jenkins, C. D., and Hurst, M. W. 1978). In this case the controllers were simply shifting to another sector each hour in an attempt to relieve the boredom. The study report and recommendations resulted in a reduced duration of performance and other than monitoring task rotation.

The question of monitoring load emphasizes two different aspects of the problem of maintaining vigilance. The first is the problem of maintaining alertness during periods of no change on the monitoring screen. The second problem is maintaining vigilance in an overload or high stimulus load condition. In this latter case some movement will go undetected as has been supported by some Department of Defense surety tests. The monitoring load studies done by Tickner and Poulton showed a vigilance degradation when the number of screens were raised from 16 to 24 over a short (30-120 minute) duration. Feedback from the commercial security arena indicates that CCTV monitoring is most often coupled with an access control task. In prisons, jails, manufacturing plants, hospitals, high tech facilities and precious metal activities, access control constitutes over 75% of the workload during the day shift. Monitoring during these conditions is done on a random basis. Many firms have gone to using video tape recorders to overcome the missed real time events resulting from the overload. Central stations, both proprietary and contract, report combined radio communication, alarm monitoring and CCTV tasks. Interviews with operators for both type at functions reveal that as work density (openings, closings, and severe weather problems) increases, vigilance on CCTV monitoring goes down in favor of the other competing type tasks. The optimization of monitoring load has not focused on the behavioral science needs of the operator in the overall system design.

Management practices which enhance vigilance while reducing stress and fatigue are not readily apparent in the material reviewed for this paper. Mention was made in two studies that supervisor feedback in response to detection and false alarm reporting had a positive influence on guard morale and alertness. In addition, the assignment of busy tasks such as time recording, radio checks, and data recording tasks increases vigilance. Evidence that government agencies conduct performance testing on operator alertness was noted. Nuclear surety and planned penetration tests have confirmed or denied acceptable monitoring performance. Of the 90 plus commercial users responding, not one has made any attempt to introduce foreign material or personnel into a static scene. Not one tried to determine if such a challenge or performance act would be detected by their monitoring personnel.

Training: The discussion of training will be limited to what information or study results go beyond normal training requirements necessary to prepare a monitor operator to handle the basic equipment. Simulation training should be provided in which the field of view is altered in graduated steps with the interjection of foreign objects. The altered view would then be compared with the original. Such comparison training should enhance the monitoring person's perception and general observational techniques. Training should also be provided based on optimum field of views, depth of field, optimum distance and contrast, etc. Such training criteria would first have to be developed after a comprehensive research effort. Training to shift supervisors in developing sensitivity to man-machine interface problems, performance factors for CCTV monitoring posts, and their key role in alertness motivation, would also be an aspect of this research.

Pesonnel Selection: The studies reviewed for this paper offer little in the way of personnel selection guidance. Limited findings indicate that there appears to be no measurable difference between men and women in terms of performance capability. Age considerations are not adequately addressed except by Tickner who indicates that below 30 year olds adjusted to inceased monitoring loads better than the 45 and over group. These short term studies add little to the solution of today's operational problems. The survey input offers little as to the ratio of preference of male to female operators, but does indicate that 18% of the users employ handicapped personnel. These respondents report a "feeling" that the handicapped operate at a more sustained rate of vigilance than the non-handicapped. Individual traits that may reduce stress or fatigue in a monitoring situation were not identified.

E. PHYSICAL HEALTH CONSIDERATIONS

In general the studies available for review in the area of assessment do not deal with CCTV monitoring. The Air Traffic Controller Health Study is an excellent document dealing with the nature and extent of health changes. It addresses stress and fatigue induced health related changes such as headaches and stomach and lower back pains. The study by Mackie and Miller (1980) explores the influences of drug use and sleep loss on vigilance. Older studies indicate viral and bacterial infections have an adverse affect on vigilance. Most of my information on physical health came from survey data, guard interviews and consultant feedback.

Eye strain was mentioned by a third of the guard activities as being a problem in the monitoring task. While no attempt was made to validate their input with verification checks of medical records and absentee data, the information offered indicated a possible link between eye strain and monitoring load, duration, console design and/or illumination. Reporting activities used such wording as glare, color contrast, screen distance, screen size and blurring to describe the problems.

Headaches were reported in survey data. Instances of headaches were normally attributed by the respondents as due to poor ventilation, excessive watch load, excessive background event rates, and excessive environmental heat. Reports contained such descriptive words as high activity rate, stale air, uncomfortably warm, and too noisy. There was no evidence of long term or chronic headaches. One can only assume that job change occurred before some of their problems could be measured or observed.

Cramps, body pains and numbness were reported by less than 2% of the users surveyed. What was reported was lower back pain and numbness in feet and hands. Those reporting the lower back pains indicated that the problem could have been stress-related. Reassignment out of monitoring tasks reportedly reduced or eliminated the symptoms. Instances of numbness were related to duration of monitoring. Where video tape recorders and unrestricted movement in and adjacent to the control room was permitted, the numbing sensations would disappear. Sleep loss and sleep disruption were credited with lower body pain development. This pain was associated with watch load, duration and frequent shift changes. People reporting lower back pains indicated a reduction of symptoms when supervisors expressed support and emphasis of CCTV monitoring tasks or peers were present or visited the operators frequently during the shift. While the introduction of peer visits appears to reduce stress it also degradates vigilance by distraction from the monitoring task.

F. PSYCHOLOGICAL HEALTH CONSIDERATIONS

Two of the major complaints about monitoring tasks from both study results and the user surveys were that the job was boring and lonely. Few of the studies were found to have examined the stability of individual differences in vigilance over extended periods of monitoring. Social or peer pressures have been found to decrease vigilance by pushing a guard into a direction of response conservatism. This factor has been observed in both commercial and government settings. Evidence of stress, fatigue, and job anxiety were reported and considered.

Stress: One of the original arousal or stress-related studies was done by Duffy (1934). His inverted "U" hypothesis stated that there is a certain optimal level of arousal for every type of response or learning. Under-arousal causes inattention and a slow response. Over-arousal causes distraction and irrelevant responses. The degree of stress faced in this type of monitoring task is determined by a number of variables. Since stress is normally a product of arousal, the stimuli can be considered counterproductive. Such stimuli as poor engineering, and environment, watch overload and excessive duration and excessive background events will cause stress. We acknowledge the causes of stress but their impact on watch load and duration in CCTV monitoring have not been adequately examined. Operational settings have not been examined to determine stress producing perimeters.

Fatigue has been treated as a product of stress or result of sleep loss. I could not find evidence of studies that address fatigue itself as a factor in CCTV assessment. Input from the survey reported incidents of fatigue due to boredom, sleep loss, and dim lighting. No attempt was made to correlate this data.

Job anxiety information, while not addressed directly in the studies reviewed, was gathered from the survey. Approximately 40 people interviewed acknowledged requesting job change away from monitoring tasks. The reasons stated for the job change requests were boredom, loneliness, lower back pain, sleep loss and an uncomfortable working environment. All of these individuals were in positions where rotation was not pracciced and watch duration exceeded four hours. Where supervisors and policy allowed rotation of tasks, stress was considered present but not to the point of individuals requesting a change in assignment.

III. FINDINGS

A. GENERAL

The applicability of the short term laboratory vigilance research results are questioned due to the type and frequency of stimuli used. Relatively few such research efforts have attempted to model such tasks and projects after real-world CCTV and security system monitoring requirements. Loss of vigilance in similar tasks found in allied disciplines within industry conclude that loss of vigilance is a common phenomenon in complex real-world operations.

No valid effort could be located which determined the level of alertness for an eight hour watch under real operational settings. The shorter settings and guard testimony indicate the need for additional study in an operational setting.

Two of the most important research voids appear in the need to develop data on optimum monitoring duration and workload.

B. ENGINEERING FINDINGS

1. Beyond a certain performance level, the number of CCTV screens added to a workload reduce the vigilance and increase fatigue, error rates, and stress.
2. The size and distance from the monitoring screens affect vigilance.
3. From an engineering and design point of view the definition of surveillance vs. assessment tasks is not clear.
4. An optimum workload factor does not seem to be a planning factor in the CCTV system design.
5. Hardware manufacturers provide no guidance to the user, installer, or sales representative to promote improved vigilance.
6. No studies could be found that describe the degree of difference between sensor driven assessment systems and surveillance systems in terms of vigilance or fatigue measurement.
7. Field problem solving or user tailored engineering is done by OEM or vendor personnel without the benefit of behavioral study research results.

C. ENVIRONMENTAL VARIABLES

1. The effect of relatively long term exposure to environmental stresses has not been tested.
2. Existing studies hypothesize that the impact of environmental stress will be more adverse in real world situations than the short term laboratory results reflect.
3. Noisy environments cause operators to reduce their vigilance efforts to avoid stress and fatigue.
4. Too little light promotes sleep and inattention to CCTV monitors.

5. The three major aspects of the work environment which impact adversely on monitoring are overall monitoring load, presence of environmental stresses, and the absence of presence of peers and supervisors.

D. PROCEDURES AND POLICIES

1. Performance under moderate work loads will be superior to light or heavy monitoring workloads.
2. Virtually no stress/fatigue study performed has addressed a duration requirement of eight or more hours.
3. There is a wide variety of policies governing duration and workload for CCTV monitoring most of which are not based on the results of previous behavioral studies.
4. Very little engineering, design, staffing or workload and duration studies are in the hands of the private sector.
5. Keep-busy type tasks and good supervision enhance vigilance.
6. Planned exercises or spot-checks to determine what operators will and will not detect are not being conducted by supervisory personnel.
7. Studies that present optimum staffing, workload and tour duration are non-existent.
8. Personnel selection against job requirements and performance expectations has not been adequately studied.

E. MEDICAL PROBLEMS

1. Viral and bacterial infections have an adverse effect on individuals required to perform tasks of vigilance.
2. Evidence indicates that the effects of light, screen size and viewing distance and duration of tour, reduce vigilance and promote eye strain.
3. Evidence suggests that headaches are being produced by stress, temperature, noise, poor ventilation, and excessive watch load. Additionally, it appears that rotation of tasks reduces this problem.
4. The single most common body pain experienced in CCTV monitoring is lower back pain believed to develop as a symptom of stress.

F. PSYCHOLOGICAL PROBLEMS

1. There have been few if any attempts to systematically study the impact of social variables on vigilance or CCTV monitoring.
2. The highest reported cause of stress, fatigue, and vigilance reduction is monitoring length and workloads.
3. Evidence indicates that vigilance degrading symptoms disappear after job reassignment out of monitoring tasks.

IV. IMPLICATIONS

A. It is difficult to reduce the volume of raw survey data, study results and finding to conclusive fundamental implications for future considerations or actions. Some findings carry limited implications that will have to be reconciled with existing engineering and design constraints. Other findings in the areas of staffing, procedures, practices, and environment have implication of more broad based application.

My goals in this paper were: (1) to review existing studies for useful data on fatigue as a factor in CCTV assessment; (2) survey the field for information to validate or add to existing study data; (3) to determine the need for further study which might resolve some of the unanswered questions surfaced by users of CCTV equipment.

B. SPECIFIC QUESTIONS POSED IN THIS PAPER

1. Is there an optimum CCTV monitoring tour duration?
2. Is there an optimum workload for CCTV monitors in a real life operational setting?
3. Is there a need for research that takes the issue into the operational world both civil and military?
4. From an engineering and design point of view, is there a need to a clearer definition of assessment and surveillance?
5. Are there differences in fatigue and stress levels between sensor driven CCTV systems and surveillance systems?
6. Are study hypotheses correct in predicting more adverse impact on vigilance due to environmental stresses in the real world than experienced in laboratory research correct?
7. Should the private sector share in the results of government research in the area of CCTV assessment studies?
8. How widespread is the monitor "turn off" or vigilance reduction problem in cases where stress levels are on the increase?

V. RECOMMENDATIONS

A. The review of existing studies and survey data indicate a need for further study on engineering and environmental issues to be conducted in operational situations. Even more important is the lack of research in the area of watch duration and watch workload. Fatigue, stress, and vigilance must be measured in both commercial and military environments to fully evaluate how to optimize security systems.

B. SPECIFIC RECOMMENDATIONS INCLUDE:

1. Re-examine the engineering requirements for CCTV monitoring based on behavioral science recommendations for system design.
2. Redefine surveillance and assessment in terms of engineering and environmental functions.
3. Research the optimum workload factors for CCTV monitoring.
4. Provide the public sector with vigilance study update material.
5. Research the degree of difference between sensor driven CCTV assessment and surveillance systems.
6. Study the affect of long term exposure to environmental stress in CCTV monitoring situations.
7. Determine if environmental stress will have a greater impact on monitoring in a real world situation than in laboratory studies.
8. Examine the "turn-off" or reduced vigilance effect of excessive environmental stress stimuli.
9. Establish a program to determine the effectiveness of spot checks or supervisor programs to test CCTV detection efforts.
10. Continue to study task reduction as a stress reduction technique.
11. Further explore the impact of social variables on vigilance and CCTV monitoring.

REFERENCES

Contrell, G. K., Hartman, B. O., Sanford, S. F., Steinkerchner, R. E., Trimble, R. W., Alertness, Fatigue and Morale of Air Force Sentries, USAF School of Aerospace Medicine, 1968.

Colquhoun, W. P., Evaluation of auditory, visual, and dual mode displays for prolonged sonar monitoring in repeared sessions. Human Factors, 1975, 17, 425-437.

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

Fitts, P. M., Posner, M. I., Human Performance, Belmont CA, Brook/Cole, 1967.

Hall, R., Hannah, W., Weaver, R. & Brenner, P., Security Personnel Performance Measurement System, Vol I Final Report MRC R-513, Santa Barbara, CA, Mission Research Corp., 1979.

Mackie, R. R., Miller, J. C., Vigilance Research and Nuclear Security: critical review and potential applications to security guard performance. Human Factors Research Inc., Goleta CA. 1980.

Machworth, J. F., Vigilance and Habituation, Hermondsworth, Middlesex, (England), Pequin Books, 1969.

O'Hanlon, J. F. & Beally, J., Concurrent of electroencephalographic and performance changes during a simulated radar watch and some implications for the arousal theory of vigilance; Vigilance: Theory Operational Performance and Physiological Correlates, New York: Plenum Press, 1977.

Rose, R. M., Jenkins, C. D., Hurst, M. W., Air Traffic Controller Health Change Study, Boston University School of Medicine, Office of Aviation Medicine, FAA, 1978.

Thackray, R. I., Bailey, J. P., Touchstone, R. M., Physiological, Subjective, and Performance Correlates of Reported Boredom and Monitoring While Performing a Simulated Radar Control Task (AM-76-8), FAA, Oklahoma City: Civil Aeromedical Inst., 1975.

Tickner, A. H., Poulton, E. C., Copeman, A. K., Simmonds, D. C. U., Monitoring 16 Television Screens Showing Little Movement, Ergonomics, 1971, 15, 275-291.

Tickner, A. H., Poulton, E. C., Monitoring 16 Television Screens Showing a Great Deal of Movement, Ergonomics, 1972, 16(4), 381-401.

Wait, H. J., Manning, M. W., CAS-SAS Operational Work Station Design and Procedures, NUREG/CR 1467, Mason & Hanger-Silas Mason Co., Inc.

THE INS ENCLOSED SPACE DETECTOR (ESD) PROGRAM

Harry D. Frankel

US Immigration and Naturalization

ABSTRACT

ENCLOSED SPACE DETECTOR PROGRAM

Since 1974 the Immigration and Naturalization Service (INS) of the Department of Justice have been investigating the feasibility of automatically and reliably detecting the presence of people concealed in the enclosed spaces of vehicles and rooms.

The investigation is based on using a transducer such as a geophone to pick up heartbeat signals generated by a human as they are coupled into the floors, and walls enlosing spaces.

A laboratory model ESD-1, of a detector for use against small-mass vehicles (less than 6000 lbs) was fabricated and tested in 1978 and found to be quite effective: 95% reliable. However, it was found that greater capability was needed in noise suppression if the technique were to be successful in the larger masses of tractor-trailers, railroad cars, and rooms of buildings.

The current 12-month study seeks to fabricate a laboratory model ESD-2, of a detector demonstrating large-mass capability and to analyze novel techniques for performing in noisy large-mass enclosures.

The research work of this program may be applicable to problems of unique identification of people and analysis of human stress.

THE INS ENCLOSED SPACE DETECTOR (ESD) PROGRAM

THE PROBLEM

Since 1976, the Immigration and Naturalization Service (INS) of the Department of Justice has been sponsoring research in the automatic detection of people concealed in vehicles and buildings. The research is directed at relieving Inspectors and Border Patrol Agents of the difficult tasks of inspecting vehicles -enclosed spaces- against illegal entries of people at land, sea, and air ports-of-entry, and along the borders and at traffic checkpoints. Millions of passenger and freight vehicles are inspected yearly and many more would be inspected if a fast, reliable search technique were available. The problems in inspecting commercial vehicles are especially difficult, particularly when loaded vehicles such as tractor-trailers or railroad cars are involved. And the safety of inspecting personnel is frequently jeopardized when inspections require entry into such large vehicles.

INS is required by law to monitor all incoming traffic coming into the US and frequently INS, in the course of investigating cases of people-smuggling are required to check-out buildings.

GOALS

The research of so-called enclosed space detection seeks to establish the feasibility of providing an Inspector the means by which the presence of a person or persons concealed in a vehicle or room of a ship or building could be reliably determined without requiring entry of the Inspector. The capability being sought is based on the principle of detecting heartbeat signals coupled from a human body to the surfaces of enclosed spaces. The research thus far confirms that it is possible to incorporate the required technology into a highly portable (fit into an inspector's pocket), highly reliable (better than 95% certainty of detection), low false alarm rate (less than 5%), relatively cheap system (estimated at $400 in 1976 dollars).

From the outset, INS has focused on:

1. Proving the feasibility of detecting and identifying heartbeat signals imbedded in panels, walls, and ceilings of enclosed spaces amid noise due to wing and manmade sources.

2. Demonstrating how the detection and identification of very small surface fluctuations (10^{-7} centimeters) caused by a heartbeat, would be performed rapidly, reliably and automatically by appropriate electronic and analytic techniques.

As the research has progressed, numerous technical difficulties have been encountered. The major one to be resolved is reliable detection in spaces enclosed by massive surfaces such as in rooms of buildings.

CURRENT PROGRAM

In the current 12-month program, a laboratory model, ESD-2, is being designed and fabricated to demonstrate the feasibility of the ESD concept for relatively large structures. In addition, the feasibility of new concepts for handling the large mass-enclosures more reliably are being analyzed and potential countermeasures to the ESD are being evaluated. One of the concepts will seek to determine the number and location of people within an enclosed space.

The ESD-2 will consist of:

1. A single geophone

2. A low-pass filter and amplifier

3. An A/D converter

4. A microcomputer with 64K bytes of RAM/ROM memory and software

5. Noise removal and alarm circuitry

The geophone in contact with the surface of an enclosed space, will detect the very small compressional waves or vibrations in the surface.

The low-pass filter will separate out the higher frequency (above 10Hz) components of these waves which are mainly noise, and the amplifier will increase the power of the remaining lower frequency signals.

The A/D converter will digitize the remaining signals and store them in the RAM portion of the microcomputer.

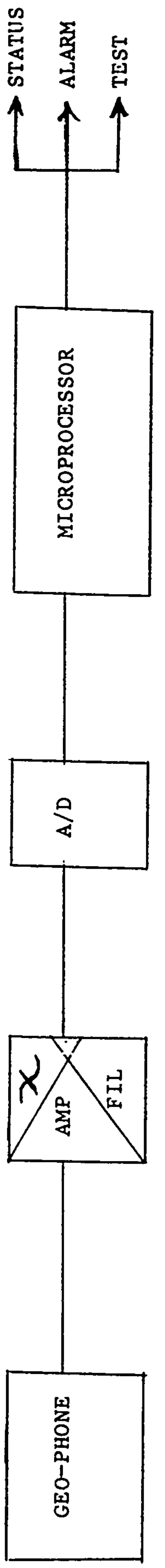
The ROM portion of the microcomputer will contain the software for analyzing signals stored in the RAM to determine whether they contain heartbeat signals. The power and spectral content of small samples (approximately three seconds each) of the RAM - stored signals will be analyzed and, depending upon the total power and spectral componenets in each sample, a decision will be made as to whether a person (or persons) are present or absent in an enclosed space. An average of 15 seconds (approximately four samples) of time is expected to be needed to decide with better than 95% accuracy. The decision time depends upon the noise content, including wind effects, of the environment.

The low frequency effects due to wind which may be coupled to the surface of an enclosed space are minimized by a software routine.

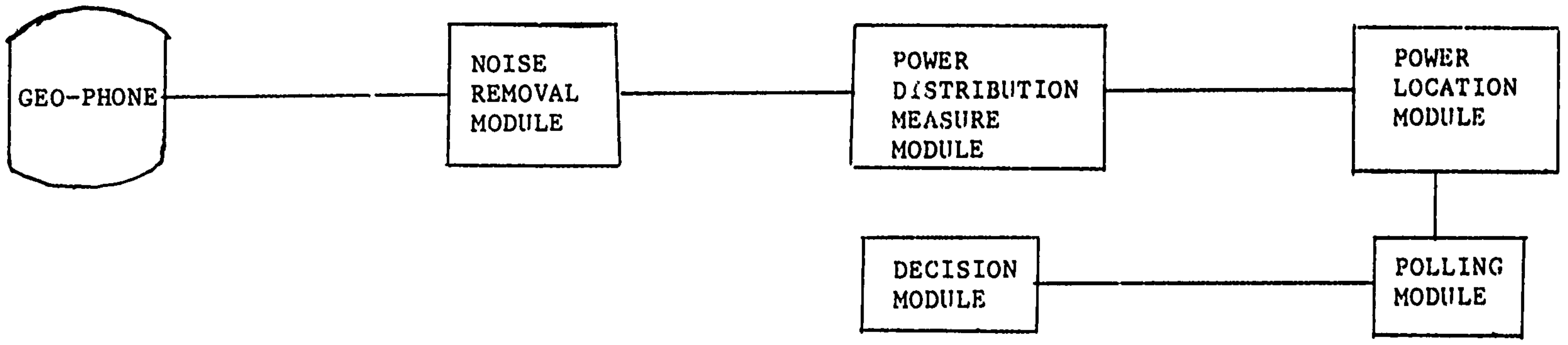
The alarm circuitry signals the results of the decision.

The design dream for a portable system is to package all the electronics in a small container which would fit in the breast pocket of a jacket with the geophone connected to it by a wire long enough to facilitate resting it on a horizontal surface of the enclosed space. For a room with no horizontal surfaces available the geophone might be attached to a wall with suction or adhering material.

Multi-channel systems (i.e., systems with multiple geophones) have been investigated and appear feasible, a capability which is expected to enhance both portable and stationary system applications to massive enclosures. The enhancement is expected to improve performance on massive enclosures by enabling great reductions in noise, lowering average decision time, and providing greater accuracy even in high noise environments.



MAJOR COMPONENTS ESD HARDWARE



ESD SOFTWARE MAJOR MODULES

PHYSICAL SECURITY MAN-MACHINE INTERFACE

AN OPERATIONAL VIEW OF SECURITY FUNCTIONS

Prepared at the
Invitation of
the
Defense Nuclear Agency

By
R. Kozuma, H. Darmetko, F. Marcks,
R. Ravenelle, L. Segal

1 June 1981

Analytical Systems Engineering Corporation

PREFACE

The authors undertook the writing of this paper on short notice and with collective concern for adequate treatment of a complex subject. The particular subject matter of operator interactions with security system elements at his work station was undertaken because of individual awareness of inadequacies in current security systems. The authors realize that human engineering practices have generally been applied in current security systems only as necessary to correct obvious design incompatibilities with a minimum of a priori efforts to establish congruity between human capabilities and limitations and equipment configurations.

Collectively, the authors have experience in security system operations, equipment design and development, security system project management, and human factors application to security operator work station design. Four of the authors are currently working with security systems in various roles and all maintain a current interest in security system evolutionary progress.

At the present time, R. Kozuma, F. Marcks, R. Ravenelle and L. Segal are employed by the Analytical Systems Engineering Corporation. H. Darmetko is employed by Support Systems Associates, Inc.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

1. INTRODUCTION

1.1 BACKGROUND

Physical security has been a necessary social function throughout human history. However, significant reliance upon non-human security aids is a very recent development. Prior efforts to heighten security simply involved an increase in the number of posted guards. An intense concern for physical security on a broad basis among the uniformed services arose less than ten years ago. Once this concern materialized, budgetary resources for development and production of security hardware were provided in abundance along with demands for immediate action to enhance security. This situation is attributed to three factors. First, concern for security of lethal military weapons which would seriously threaten society should they fall into belligerent hands unconstrained by accepted political or moral conventions. Second, recognition of the terrorist threat, and the continued exercise of violence and the increasing sophistication of various terrorist movements. Third, recognition of the scarcity, expense and ineffectiveness of human guards in surveillance and detection roles.

A great deal of initiative by many individuals and companies has produced a plethora of physical security devices for the commerical market place. The uniformed services had taken a similar approach, individually embarking upon development, production and deployment projects to enhance security. Readily applicable technologies have been quickly employed to produce equipment for surveillance and intrusion detection, alarm signal transmission and simple display of intrusion alarms. The equipments currently in use represent a first generation of devices which were developed and produced in an almost entrepreneurial fashion. As one might reasonably expect, the equipment designer's concept of intrusion detection methods, the threat to be countered, and the means to alert the guard force have prevailed. A truly cooperative effort among equipment designers, research scientists, operators and human engineering specialists is yet to take place in an organized fashion. There are, additionally, some political and organizational issues yet to be resolved to facilitate a union among the development and using communities, but these are beyond the purview of this paper.

1.2 PURPOSE

The objective of this paper is to show the need for a deeper, more timely involvement of behavioral scientists, and human factors and human engineering specialists in the field of physical security. The authors attempt to convince the sponsoring institution, the Defense Nuclear Agency, and applied research groups to bring their skills to bear on the specific and general recommendations presented in this paper. The three general needs that should be considered are to:

1. Apply the large body of human engineering knowledge extent to solve existing problems being encountered in security operations where man-machine deficiencies are evident.
2. Include behavioral scientist participation in all stages of advanced security system development and continue analyses and guidance into the operational phase.
3. Develop a large scale test/training facility for DoD wide use, free from operational encumberances of critical resources protection needs, to perform concept development and testing, procedures evaluation and equipment tests and evaluation.

1.3 SCOPE

This paper presents a description of the functional states of a physical security system and depicts representative operator tasks, information needs, display media and controls, and communications media involved in current security systems operations. Operational scenarios involving system functions and operator tasks are described to illustrate the problems arising from rapid successions of multi-step processes. Factors which complicate situational control are presented and "what if" questions are posed which indicate further complications to stimulate the reader to envision operator saturation and the rapid development of a chaotic situation. Specific considerations are developed and recommendations for further study are presented based upon some of these specific considerations. In Appendix A, a bibliography is provided. It shows the general references used by the authors as general background information.

2. SECURITY SYSTEM FUNCTIONAL STATES

A physical security system to safeguard critical assets is a composite system with the following elements:

1. Physical Barriers
2. Intrusion Detection and Assessment Equipment
3. Entry Control
4. Lighting
5. Operational Personnel
6. Response Forces
7. Communications
8. Armament
9. Vehicles
10. Physical Hardening
11. Alternate Power Systems
12. Operational Doctrine and Procedures

These elements are deployed to counter postulated threats. The security system exists in various states depending upon the absence or presence of a threat and the physical progress of a tactical engagement of an actual threat.

This section defines and discusses the functional states of a security system and the operator actions required by current security system and equipment configurations during each functional state. These discussions are centered about the active elements (the man and the electronic detection devices) intended to detect and assess surreptitious penetration of the secured boundaries. In Table 2-1 a taxonomy of security tasks is presented in a matrix of Security System Functions and Operator Tasks with related information requirements, displays and controls, and communications media.

2.1 SECURITY SYSTEM FUNCTIONS

The primary functions of a physical security system are: 1) Surveillance, 2) Detection, 3) Assessment, 4) Decision, 5) Response, and (6) Engagement. All other functions are ancillary and should not interfere with the primary functions. Typical system configuration elements include the protected area perimeter, entry control entrapment areas, storage structures, alert area structures, and alarm

TABLE 2-1

SECURITY SYSTEM TAXONOMY

	SECURITY SYSTEM FUNCTIONAL			
MAN-MACHINE INTERFACE	**SURVEILLANCE**	**DETECTION**	**ASSESSMENT**	**DECISION**
OPERATOR TASKS	1 Observe General Situation & Equipment Status 2 Housekeeping/Ancillary tasks a. Perform equipment tests b. Perform communication checks c Coordinate security force movement. d Process administrative communications. e Exercise overall Security Command & Control. f Monitor all movements in the area g Supervises free zones h. Coordinate disaster control procedures. i Record administrative actions. (1) Log incidents, alarms, and actions taken (2) Opening/closing of secure structures (3) Sensor performance checks (4) Maintenance performed.	1. Acknowledge Sensor Alarm Message (SAM) & CCTV. 2. Acknowledge Equipment Fault Alarm	1 Examine Display Data 2. Determine Location 3. Assess visually or remotely (CCTV) Assess auditorally 4 Assessment by voice communication with posted guards 5 Discriminate Nuisance vs Intrusion Alarm 6 Determine Numbers Direction Armament Equipment 7 Discern degree hostility/intent	1 Decides A Nuisance B Intrusion – hostile C Intrusion – non-hostile. D System Fault 2 Notify Note Local operator's failure to ackn and perform decision function result in alarm at CSC
INFORMATION REQUIREMENTS	1. Area activity. 2 Weather activity 3 Operational advisory	Distinction between sensor alarm message and equipment fault message	1 Target Characteristics (motion & location). a Visual b Audible 2 Area activity status	1 Based on previous informatio 2 Response force status
DISPLAY & CONTROLS	1 Audio alerts. 2 Visual indicators. 3 Automated historical record	1 Geographic map presentation a. Color coded light indicators. b. Pulse coded light indicators 2 Tabular Displays a. Alphanumeric b Light indicator c Positional 3. CCTV monitor displays 4 Controls a. Acknowledge b CCTV c Communications	1 Geographic map presentation 2 CCTV monitor displays 3. Controls a CCTV b Communications	None required
COMMUNICATIONS	1 Landline 2 Radio 3 Voice Warning system (PA) 4 Intercom 5 Data Links			

TABLE 2-1

SECURITY SYSTEM TAXONOMY

SECURITY SYSTEM FUNCTIONAL STATES

DETECTION	ASSESSMENT	DECISION	RESPONSE	ENGAGEMENT
owledge Sensor Alarm Message) & CCTV owledge Equipment Fault Alarm	1. Examine Display Data 2. Determine Location 3. Assess visually or remotely (CCTV). Assess auditorally 4 Assessment by voice communication with posted guards. 5. Discriminate Nuisance vs. Intrusion Alarm 6 Determine Numbers Direction Armament Equipment 7 Discern degree hostility/intent.	1 Decides A Nuisance B Intrusion — hostile C Intrusion — non-hostile. D System Fault. 2. Notify Note Local operator's failure to acknowledge and perform decision function will result in alarm at CSC	1 Resets display 2 Dispatches ART 3 Challenge intruders 4 Dispatch Reserve Forces 5 Advise Central Security 6 Advise all area security posts 7 Turn on area lighting (if at night) 8 Place problem sensor channel in access 9 Advise maintenance Note Determine reason for failure to acknowledge	1. Directs ART to intrusion location. 2 Provides information on numbers, direction, armament and equipment 3 Monitor the situation and site activities 4. Provide information and communication coordination.
on between sensor alarm and equipment fault message	1. Target Characteristics (motion & location). a. Visual b Audible 2 Area activity status.	1 Based on previous information inputs 2. Response force status	Confirmation of transmissions	1 Situational status 2 Central security advisory
aphic map presentation. lor coded light indicators. lse coded light indicators r Displays hanumeric ht indicator sitional V monitor displays ols knowledge CTV mmunications	1 Geographic map presentation 2 CCTV monitor displays 3 Controls a CCTV b. Communicators	None required	1 Geographic map presentation 2 CCTV monitor displays 3 Controls a Reset b CCTV c Communications d Lighting switches e Sensor access switches	None presently provided

system components. The ancillary functions include but are not limited to the testing of alarm system equipments, post and patrol communication status checks, back-up power system status checks and testing, lighting status, security force personnel location/status, opening and closing protected structures and interior circulation control. Execution of such tasks are necessary to assure the day-to-day functioning of the security system. When the system changes state from surveillance to detection, essential operational functions dramatically change and ancillary activities cease where they would interfere with the sequences of alarm assessment, decision, response and engagement.

2.1.1 Surveillance

Surveillance is the functional state of the security system wherein the intrusion detection sensors and related equipment are ready to detect sensor stimuli should any occur. The security system operator periodically observes the functional status of his equipment. In support of the general security mission during a quiescent state of operation for security of nuclear resources, 360 degree perimeter surveillance of potential ground avenues of hostile approach to the area is provided by patrols both external and internal to the area, by tower observation and by sensor operation. The alarm panel security operator depends on a number of other sources for general surveillance, including other cleared personnel working within or near the restricted area in capacities other than security as well as the entry control point security personnel. Ancillary functions during the surveillance state includes entry control of vehicles and personnel generally associated with and cleared for work within the restricted area, visitor pre-entry coordination, visitor entry clearnance and visitor escort. Surveillance procedures generally follow stringent rules requiring any aberration to be investigated by the defending security force.

As the result of installation of sophisticated electronic detection and assessment capability being annunciated at one focal point, which in turn serves as the command and control element, a number of ancillary or housekeeping tasks have been allocated to such work centers. Some of these tasks should be associated with such a work center, but other tasks have been placed there arbitrarily. All such tasks add to operator work load and detract from the primary mission of the alarm control center. The following tasks are representative of restricted area operator's ancillary responsibilities.

a. Monitor entry control point ingress/egress

b. Check communications equipments status

c. Coordinate security force actions, relief and meal breaks

d. Handle phone calls to and from the area

e. Observe free zone construction areas

f. Monitor all movement in area

g. Log incidents and actions

h. Control opening and closing procedures for all storage structures

i. Coordinate and conduct periodic checks of structures and sensor equipment tests

j. Coordinate fire/accidents actions

k Receive severe weather reports

l. Participate in Broken Arrow, Bent Spear, Dull Sword exercises

m. Monitor convoy operations

The above list as well as many other housekeeping tasks require near constant activity for alarm panel operators in the surveillance mode.

2.1.2 Detection

Detection of intruders is the basic function for sensors placed along the secured area boundaries and for those mounted on and within buildings in the protected area. Sensor activiation signals are transmitted to the security operator to alert him to the change in the state of the system. In some instances, detection of intruders is provided by human sentries at boundary or inner zone observation posts or by personnel assigned other dutuies within or near the area.

Intrusion detection sensors, while markedly superior to human detectors (in all weather, long attention span aspects) currently provide simple binary data - alarm or no alarm. At the moment of detection, no data regarding intruder characteristics is provided. When a detection takes place supplementary equipment indicates the distinction between sensor alarm messages and equipment fault detections. The sensor does not discriminate between stimulation by a nuisance alarm source or an intruder.

For a single alarm detection, this a momentary state. The operator moves quickly into the assessment state to determine cause(s) of the alarm.

2.1.3 Assessment

Assessment of an intrusion alarm is presently a human function. Current intrusion detection sensor subsystems do not discriminate, identify or interpret intruder stimuli. The security operator can employ various receptive modalities to discriminate between intrusion alarms and equipment fault alarms, to identify and classify intruders or causes of non-intruder nuisance alarms. Currently, human vision is the primary mode used to make assessments. If direct or remote viewing (by CCTV means) is not possible by the security operator, a posted sentry observing an alarm cause must verbally communicate sufficient data for interpretation.

Regardless of the source of the alarm message, alarm assessment must be performed as rapidly as is possible consistent with the probability of correct assessment. Near real time assessment of the alarmed sector is necessary so that the cause of the alarm can be accurately determined with respect to location, numbers, equipment/arms, mood of an intruder, or non-intruder causes.

2.1.4 Decision

Security operator action decisions are the crucial human acts to gain and maintain control of a security situation. The equipments throughout the system must facilitate functions leading to this primary operator function. While current equipment assists in operator information processing, decision making is principally a human function. Problem recognition and problem diagnosis had been completed during the assessment state. The third phase in decision making, action selection, is affected by a number of factors. These factors are:

a. Nuisance alarm rates

b. Size, shape and location of blind zones

c. The boundary barrier system

d. Perimeter lighting uniformity

e. Cleared distance from protected resources

f. Security operations/exercises in progress

g. Electronic sensor system malfunction or failure

h. The amount of data immediately available from sensor alarm messages and assessment sources

i. Communication system efficiencies

j. Operator training and proficiency

The ability of the operators to provide accurate decisions swiftly for prompt notification of response forces is aided or degraded by the quality and the dimensions of these factors.

2.1.5 Response

The response function is the implementation phase of the security operator's initial decision. In this functional state of the security system, one of three basic actions take place: 1) a nuisance alarm is reset and the system reverts to the surveillance state; 2) a malfunctioning part of the system is turned-off until repaired, then corrected, checked-out and placed on-line in a normal operating mode; 3) an actual intrusion is countered with dispatch of an alarm response team (ART). A number of rapidly sequenced actions take place after immediate dispatch of the ART to alert other security posts and supervisory personnel and to deploy reinforcement personnel.

In response to an actual intrusion, a 15 man response force (RF) will typically be dispatched at installations that routinely support nuclear weapons or systems. One of the elements of the response force is a designated two-man alarm response team (ART). ARTs are the immediate investigative and response element for alarms received within their assigned area from any source including intrusion detection systems. The number of ARTs required for immediate response in a particular restricted area will depend on the size and topography of the area. ARTs are dispersed within the area to quickly apply effective fire power at any location on the area perimeter within their area of cognizance, hopefully, before an intruder(s) successfully penetrate the innermost fence. The Alert Fire Teams (AFTs), part of the overall RF, and their vehicles are housed, at some installations, in a hardened facility within the restricted area on standby alert (except when protecting a nuclear weapon ground convoy). A backup force (BF), in addition to the RF, of at least 17 personnel is required to respond when the response force is utilized. The BF is generally composed of security personnel posted to lower priority resources or to law enforcement duties and may include off-duty members. An Augmentation Force (AF) of other military personnel or units is also required but generally requires a period of time of up to four hours to assemble and respond.

2.1.6 Engagement

This phase is the end game of an intrusion scenario wherein all of the facilities, protective resources, preparatory work and training is ultimately tested. In this functional state, the tactical situation command and control comes under the purview of the on-scene commander. Under these volatile conditions, predetermined rules of engagement blend with on-the-spot situational decisions.

The local area security operator must maintain vigilance over the sectors remaining in the surveillance state. He must simultaneously coordinate communications; assist in coordinating RF, BF and AF movements; and in present day systems, must also concurrently log all activities.

The central security controller also constantly records the force deployments and conditions of security forces, other security resources, and overall security status. The controller initiates up-channel reports and sends down-channel alerting orders, controls the movement and response of BF and AF security forces and advises security supervisors of the security situation and other information needed in their decision making role. The complexity, speed of actions, and the maelstrom of communications activities creates an tense situation.

2.2 MAN-MACHINE INTERFACE

2.2.1 Security Operator Tasks

In the surveillance state, the operator will be in an observation mode. Numerous tasks may be accomplished in support of the general security mission and housekeeping/ancillary chores.

In the detection state, the operator will receive a sensor or equipment fault alarm and will reflexively discriminate between the two and immediately acknowledge.

In the assessment state, the operator examines the display and data determines the location of the alarm. He may continue assessment by visually looking out the window, utilizing a CCTV system or by communicating with personnel located in the area. The operator must now determine if the alarm is a nuisance or an intrusion alarm. If it is an intrusion alarm the operator now attempts to determine numbers of people, direction, armament and equipment and also attempts to discern the degree of hostility or intent.

During the response state, the operator decides if the alarm is in fact a nuisance or valid alarm, or if the alarm is a system (sensor) problem.

In the response state, the operator resets the alarm if he decides that it is a nuisance alarm. If the alarm is valid the operator notifies the Alarm Response Team (ART), turns on area lighting (during hours of darkness), challenges intruders via a public address system (an optional action), dispatches the Armed Fire Team, advises the Central Security Control (CSC) and all restricted area posts and patrols in the restricted area via a public address system. If the problem is a persistent system fault, the operator obtains permission to place the malfunctioning sensor into the access mode. The operator will then advise the CSC to contact the maintenance organization to respond and repair the affected equipment. Failure to acknowledge a sensor alarm message will result in an alarm at the CSC.

Upon receipt of an actual alarm, the CSC operator also must respond by notifying the base command post for up-channel notification, notify backup forces of contingency actions to be taken, notify "friendly forces", and notify all appropriate security and base officials not notified by base command posts. If the local operator fails to acknowledge an alarm, the CSC will receive a unique audible and visual alarm which causes the central operator to initiate a check of the local operator to ascertain the situation.

In the engagement state, the operator informs response teams, to the extent known, of penetrator location, numbers, directions, armament and other supporting equipment. Further, the operator monitors the entire site situation with its unfolding activities and provides information and communication coordination to various security force units/work centers.

When the CSC has to assume security operation functions for the local operator (loss of the local alarm panel operation), the CSC operator does so generally without means for visual assessment. The CSC operator has to rely on information relayed by voice communication from sentries in the affected local area.

The ancillary operator tasks are varied and depend on individual service doctrine and requirements. A representative list is shown in Table 2-1 under surveillance/operator tasks. These tasks are primarily performed while the system is in the surveillance state.

2.2.2 Operator Information Requirements

In the surveillance state, the operator's information requirements primarily include area activity, weather advisories and operational advisories as they may influence security force operations.

In the detection state, the operator's information (needs) involve a distinction between sensor alarm messages and equipment fault messages to allow him to acknowledge immediately. By training, he recognizes, discriminates, and decides to acknowledge, reflexively.

There is an extensive need for information in the assessment state. A great deal of interaction takes place between the operator and the displays and controls to analyze alarm causes. Equipment fault data needs to be examined to isolate malfunctions. Nuisance alarms caused by weather conditions are particularly time consuming and vexing requiring several iterations of data search and examination cycles. Actual intrusions require a search for data concerning target location, movement, specific characteristics and interpretation of their intent and hostility. Other current and immediately prior general area activity information need to be integrated with display data in this part of the decision making process.

In the decision state, the operator requirement for information is provided by previous data inputs and the operator's knowledge of response force location(s) and status.

In the response state, the operator requirement for information involves receiving confirmation of receipt of transmitted messages to various security forces.

In the engagement state, the operator needs real-time situational status from response teams and advisory status from the CSC on back-up forces and other imminent threats.

2.2.3 Displays and Controls

In the surveillance state, equipment operational status is displayed to the operator. Visual indications of equipment automatic self-test, non-critical failures, automatic event recording print-outs are provided. Control over lighting, audio alarm volume, and communication equipment are manipulated to adjust for varying environmental conditions and conduct of ancillary tasks.

An operator's display and controls for the detection state are currently provided in a number of approaches. The primary display may take the form of a static geographic map display presentation utilizing color coded and pulse coded light indicators at sensor locations or a CRT display with selectable area portrayals. Tabular displays use either alphanumeric, light indicators, or positional approaches for operator detection states. Along with one of the alarm panel displays, CCTV monitor displays are frequently employed with controls to acknowledge alarms, to control the TV system and to operate the security force communications network.

In the assessment state, the display and control interface with the operator requires not only a geographic map presentation, but also CCTV monitor displays and controls for the CCTV and communications newtork.

During the decision state, controls and displays are not required for the operator to make decisions. In the case of pre-programmed equipment decisions automatic decisions would be displayed to the operator.

The response state again may require the display and controls interface with the human operator. This would be with the the geographic map presentation, CCTV monitor display and the controls that allow for reset, CCTV operation, communication, turn-on of area lighting, or placement of sensor channels into the access mode.

In the engagement state, the operator does not presently have displays or controls to efficently monitor the tactical situation. The operator is obliged to depend upon radio reports from on-scene forces.

2.2.4 Communications

In all of the security system functional states, the operator communicates either by landline, radio, voice warning system, (Public Address), intercom with security forces on through data links with the sensor system. The communications capability can appropriately be utilized by the operator in various security system functional states.

2.3 ACTION FLOW EXAMPLES

The operator's security system tasks will transition from one state to another depending upon the situation. Three single thread examples are provided to illustrate the interrelationships between Sections 2.1 and 2.2.

2.3.1 Example 1 - Sensor Alarm

The operator is in a surveillance state until a Sensor Alarm Message (SAM) is detected by the equipment (detection state). The operator acknowledges the SAM and now searches for the location of the sensor and seeks to identify the source of the activation (assessment state).

2.3.1.1 Nuisance Alarm

If the assessment reveals that the SAM was generated by an animal or authorized personnel working in the area, the operator decides that the SAM is a nuisance alarm (decision state) and resets the security system (response state).

2.3.1.2 Intrusion Alarm

If the assessment reveals that an intruder caused the SAM, the operator decides that the SAM is an intrusion alarm (decision state) and dispatches ART's to the location (response state). The operator returns to assessment of the alarm (assessment state) to attempt to determine numbers, direction, armament and equipment. If this information can be determined, the operator provides (decision state) this information to the ART (response state).

2.3.2 Example 2 - Sensor Line Integrity Alarm

The operator is in a surveillance state until a Sensor Line Integrity Alarm (SLIA) is detected by the equipment (detection state). The operator acknowledges the SLIA and now examines the location of the SLIA and searches for the source of the activation (assessment state). If the operator cannot assess the SLIA from his location (decision state), an ART is dispatched to the location (response state) to determine the source of the activation (assessment state).

2.3.2.1 Nuisance Alarm

If the ART determines that maintenance is working on the lines (decision state), the operator is notified (respons‹› state). The operator decides that the SLIA is a nuisance alarm (decision state) and resets the security system (response state).

2.3.2.2 Intrusion Alarm

If the ART determines that a covert intruder caused the SLIA (decision state), the operator is notified (response state). The operator requests the status of the situation (assessment state) from the ART. The ART may communicate that the situation is under control. Since the equipment has been damaged, the operator decides (decision state) to notify maintenance for equipment repair (response state).

2.3.3 Example 3 - Equipment Status Alarm

The operator is in a surveillance state until an equipment status alarm (ESA) is detected by the equipment (detection state). The operator acknowledges the ESA (response state) then and examines the effects on the system (assessment state).

Fail safe indicators show failure of the entire system, back-up power supply, or parts of the intrusion detection system (assessment state).

The ESA may indicate to the operator that the entire system or a portion of the system has malfunctioned. The operator decides (decision state) to notify the security forces and maintenance forces of the malfunction (response state).

3. PHYSICAL SECURITY SCENARIOS

In Section 2.3, some simplistic, single trace action sequences were presented. A more likely, representative case of a security system operator scenario is described in this section. (It is presented in cryptic phrases to facilitate presentation and reader visualization of activity sequences.)

3.1 ALARM PANEL CONSOLE, MULTIPLE ALARMS

1. Operator senses audible alarm while in the surveillance state. A sensor alarm message (SAM) is visually indicated on the display. Current displays in use are Navy Bridge Annunciator, Digital Multiplex System, Multiple Sensor Annunciator (MSA), P-1 Annunciator and Small Permanent Communications and Display Segment (SPCDS).

2. Operator acknowledges (Detection State) by pressing a control which silences the audible alarm and causes the visual indicator to go from a blinking to a steady light. The operator must rapidly determine whether the alarm is in a visual or a CCTV camera coverage zone. This detection state is enhanced when the CCTV equipment is interfaced with the display console and the CCTV control indicator will go to a steady state.

3. CCTV monitor coverage is automatic for first sensor alarm messages only if in a CCTV zone (Assessment State). If the local operator is in a ground based building without benefit of CCTV, landline or radio communication is necessary with manned perimeter assessment posts to ascertain a positive assessment. These actions may require several manual actions. Operator bodily movement is required if visual operator assessment is required in a non-CCTV zone and if alarm display is in a tower (recheck display for operator orientation).

4. An audible alarm will indicate a second SAM. Second SAM is visually .indicated on the display. The CCTV control indicator will also provide a visual indication if the first SAM has not completed the assessment state. The operator must manually acknowledge the sensor display and manually call up the second SAM video display. An "ON" (white light) will slow flash on the switch which indicates the need for viewing the alarm on the CCTV monitor (if the alarm was generated in a CCTV coverage zone).

5. An audible alarm indicates a third SAM. Third SAM is visually indicated on the display. Operator acknowledges to silence the audio tone. An "ON" (white light) will slow flash on the switch of the CCTV control panel which indicates the need for viewing the third SAM alarm on the CCTV monitor (if the alarm was generated in a CCTV coverage zone).

6. Decision points arrive for the operator. Should he:

   a. Complete the assessment of first SAM and ignore 2nd and 3rd SAMs for the moment?

   b. After finishing with the first SAM, determine if the second SAM zone is visual or CCTV and if the SAM is in a CCTV zone press the switch to call up for viewing on the CCTV monitor? (The first SAM automatically goes to fast flashing "ON" which means that you have viewed it already and it is still available to be called back.)

   c. Repeat the same action with the 3rd SAM? (The 2nd SAM automaticaly goes into fast flash.)

   d. Assess CCTV coverage SAMs first and then accomplish visual assessments?

   e. Establish a time allocation for assessment of each SAM?

      Note: Since SAM alarms are not generally presented on the alarm display in the order that they were received, the operator cannot determine which SAM was displayed 2nd and which SAM was displayed 3rd in order to estimate the extent of penetration progress.

      When in a ground based alarm panel mode without CCTV, operator communication with manned assessment posts in the multiple alarm mode can be extremely confusing and can further delay decision points.

7. If any of the SAMs are valid intrusions, then the operator actions in the (Response and Engagement States) alert, as listed below, will conflict with the additional assessment tasks when in the multiple alarm mode.

   a. Notify the area alarm response team

   b. Notify the area response forces

   c. Notify the area security posts

   d. Notify central security control

e. Monitor penetrator(s) progress

f. Inform defending forces of continuing penetrator status

g. Advise and update central security control

h. Advise approaching reserve forces nearing the affected area

i. If at night, incrementally turn on area interior lighting to illuminate penetrator(s) who may have advanced beyond the perimeter illumination

j. Notify munitions personnel or other responsible agencies to secure assets if in the open

l. Observe perimeter for supporting or backup elements of penetrating forces and advise central security control

3.2 WHAT IF?

This section is intended to indicate other complicating factors, which, when superimposed upon the preceding scenario, could cause very serious situations to develop with presently deployed security systems.

1. What if the perimeter sensor system in the clear zone is in a state of malfunction requiring access mode, and intrusions occur that will severely limit CCTV assessment time?

2. What if primary power is lost and intrusions occur during the backup generator start phase?

3. What if a camera or a monitor fails during a critical assessment state?

4. What if the alarm panel fails to function properly, yet it indicates that conditions are normal?

5. What if the redundant display is slaved from the local alarm display and the local ceases to function?

6. What if the intruders can jam the security forces radio channel?

7. What if intruders can induce nuisance alarms causing operators to hastily acknowledge and reset repeated nuisance alarms or place sensors in the access mode?

8. What if key microprocessor capability malfunctions cause catastrophic system failure?

9. What if primary to backup power switching time delays ‹r electrical transients cause microprocessor aberrations?

10. What if static electricity discharges between operator and alarm console equipments cause system changes?

11. What if severe weather (lightning, high winds) occurs causing tower evacuation or extensive sensor blanking?

12. What if the operator has to assess not one alarm but two, three, and perhaps even four, simultaneously? The following sub-questions show some additional issues to be resolved.

    a. In what order do you call-up each alarm for assessment?

    b. What are your chances of not assessing an alarm?

    c. If an alarm is a hostile penetration, how will factors such as mean viewing time and probability of correct assessment influence the engagement outcome?

    d. At what point does the operator become frustrated?

4. GENERAL PROBLEMS AND FACTORS

The foregoing sections presented definitions, descriptions and characterizations of current security operations and the responsibilities of security operators. These representative situations which the operators may face pose problems and highlight work station factors that need to be resolved since they detract from operator effectiveness and may result in behavioral aberrations.

4.1 PRESENT DAY PROBLEMS RELATED TO THE HUMAN OPERATOR DURING MULTIPLE ALARM SITUATIONS

It appears that physical security system functions will degrade at alarm panel work stations as the number of actual intrusion or nuisance alarms increase. At some undetermined point, depending upon individual operator capabilities, functions might be omitted, delayed or prolonged. The primary problem, as it relates to the the man/machine interface issue, is the possiblity for an actual penetration to occur with detection of the penetrators but with no assessment or, at best, a delayed assessment compromising effectiveness of the response force. The possible saturation of the operator creates conditions whereby the electronic equipment can detect and announce information, but the human operator, for a variety of reasons is unable to keep pace with the equipment capabilities.

In addition to the limitation of operator speed to accomplish tasks relative to the equipment's capability, there is a related but equally problematic issue. When multiple alarms form a queue awaiting operator actions, several problems can surface. The operator may:

a. Freeze or give up

b. Consciously slow down to try to recover his composure

c. Become frustrated and indecisive in choosing which alarms from the queue to process. (Most alarm panels do not provide references for time of receipt of each alarm.)

d. Speed up and mechanically process all alarms as rapidly as possible without regard to his lack of effectiveness in interpreting and assessing alarm causes

Most alarm panel consoles appear to be in reasonably efficient design configurations and do not exhibit serious limitations for singular sensor alarm message inputs. However, the security system taxonomy depicted in Table 2-1, becomes a multiple layered, complex structure when many alarms are annunciated within a short period of time. The human operator is faced with simultaneous tasks covering most of the security system functional states. Once the operator is placed in this position of overlapping states and tasks with a number of sensor alarm messages to handle, errors in perception and judgement may be expected.

4.2 ALARM PANEL WORK STATION FACTORS

The following issues suggest areas for human factor studies in support of the design work for alarm panel consoles. These are:

1. Can each work station function with only one operator?
2. Is additional automation necessary to reduce the manual interface actions between the equipment and the human operator? If so, to what degree and for which functions?
3. When alarm panel consoles are designed for expandable modular capability, has the increased workload capacity been human-engineered to allow the operator to function effectively?
4. Does the highly variable size of the security force at each installation impact the alarm panel operator's communication workload? If so, in what way and to what degree?
5. In what way does the geographic size and shape variability of the restricted areas affect operator performance?
6. In what way and to what degree has fragmented equipment design and implementation by many separate organizations affected operator performance?

7. Can human factor oriented solutions be provided to guide integration of all equipments required for operator tasks in the various security states?

8. Assuming worse case multiple alarm situations, what human factor assistance can be provided to reduce or eliminate operator confusion or omissions when alarms are in a queue?

In Appendix B an additional list of questions are provided which may be useful in studying human factors aspects, or in designing equipment.

5. RECOMMENDATIONS

This section presents recommendations for exploratory development studies in the behavioral sciences area for inclusion in the DNA FY 1983 nuclear weapons security program. Most of the recommendations stem directly from the considerations of Sections 2, 3 and 4 above. Apart from the specific 6.2 studies recommended below, the general recommendations of this paper are:

1. At the present stage of security system evolution the large body of human engineering knowledge extent (including military specifications, standards and design handbooks) should be brought to bear on the existing problems being experienced in security operations where equipment and man-machine design deficiencies are evident.

2. Behavioral Scientists need to participate in all stages of planning, designing, testing and implementing of DoD advanced security system development before the fact, and not after the fact as in (1) above.

3. DoD should develop a large scale test/training facility, using dummy critical resources, where operational concepts, procedures, tactics, equipments and human interactions can be defined, tested and evaluated.

5.1 WORKLOAD ANALYSIS OF SECURITY OPERATOR STATIONS

Use time-line analysis or other appropriate human engineering methodology to analyze the security operator's tasks, decision processes and work station layouts. Particular emphasis is required in the areas of controls and displays, communications work load and information requirements. Identify critical issues which relate to probable mission success or failure during multiple alarm situations.

5.2 MULTIPLE ALARM ASSESSMENT DISPLAYS FOR LARGE AREAS

Large nuclear storage sites have five to ten miles of perimeter requiring remote surveillance. The large number of cameras, sensor sectors and associated hardware has a cumulative effect on the security operators' workload since the potential number of intrusions, the nuisance alarm rate (NAR) and the equipment considerations vary directly with the perimeter length. Schemes for managing the large number of displays associated with large sites need to be investigated before the serious design of an advanced development security system commences. In this study, video monitoring, recall and switching actions need to be investigated across the security functions of surveillance, detection, assessment, decision and response to determine the optimum number of displays required along with a switching scheme best suited to the operator's capability to perform his mission.

5.3 ANALYSIS OF SECURITY OPERATOR ANCILLARY FUNCTIONS

Conduct in-depth studies of the security operator's ancillary tasks. Table 2-1 in this paper, may be a useful starting point. Identify interference with primary or other secondary functions. Identify opportunities for functional automation; and recommend procedural changes, work aids and additional equipment to relieve operator burdens during critical situations (automatic logging of alarms is a suggested example).

5.4 SECURITY OPERATOR DECISION FUNCTION TREE

Determine whether or not a decision function tree presented to the operator would minimize lost time and errors during sequential and multiple alarm situations. This decison tree could provide a data base for a subsequent step toward a computer generated CRT "decision-steps" display.

5.5 KEYBOARD APPLICATION STUDIES FOR NON-TYPIST OPERATORS

Determine keyboard word/coding arrangements that would aid non-typing operators in speeding up succinct operational communications.

5.6 ANALYZE SECURITY OPERATOR WORK STATIONS IN TERMS OF ONE VERSUS TWO PERSON OPERATION

The security operator becomes task saturated in cases of multiple alarms, equipment malfunction, or other emergency situations. This study should define and optimize the options among added equipment and automation and additional personnel.

5.7 AUDITORY PRESENTATION OF INFORMATION IN SECURITY OPERATIONS

Examine and define the opportunities to use audio signals to augment the visual presentation of information at the security operator's work station so as to enhance security operator effectiveness across the spectrum of security system functional states.

5.8 IMPROVE SECURITY OPERATOR VIGILANCE

Apply the known body of knowledge in the area of vigilance to the problem of the security operator's work station to determine ways to improve operator efficiency. It is postulated that a continous eight-hour shift may not be appropriate to the task in many security operations environments.

APPENDIX A

GENERAL REFERENCES

Abbey, D.S., "Control - Display - Subject Interaction and Performance in a Complex Perceptual Motor Task," Ergonomics Vol. 7, 1964, pp 151-164.

AFSC Design Handbook (DH) 1-3 Human Factors Engineering, Third Edition, Revision 1, 25 June 1980.

Childs, J.M., "Time and Error Measures of Human Performance: A Note on Bradley's Optimal - Pessimal Paradox," in Human Factors, Vol. 22, Feb. 1980, pp 113-119.

Connolly, D.W. et al, "Tactical Decision Making: II. The effects of threatening weapon performance and uncertainty of information displayed to the decision maker on threat evaluation and action selection," Report ESD-TR-61-45 and AFCRL 1100, Operational Applications Laboratory, Bedford, Mass., December 1961. (AD 288-878.)

Corrick, G.E., Haseltine, E.C., and Durst R.T., Proceedings of the Human Factors Society, 24th Annual October 1980 Meeting.

Craig A., "Effect of Prior Knowledge of Signal Probabilities on Vigilance Performance at a Two-Signal Task," in Human Factors, Vol. 22, No. 3, April 1980, pp 361-373.

Equipment Guide for the DOD Base and Installation Security System, Dynatend Incorporated, Burlington, MA.

Finley, D.L. et al, "An Analysis and Evaluation Methodology for Command and Control: Final technical report," Contract N00014-74-C-0324, Naval Analysis Program, Office of Naval Research, Arlington, Va., 1975 (in press).

Fowler, F.D., "Air Traffic Control Problems: A Pilots View," in Human Factors, Vol. 22 No. 6, December 1980, pp 645-655.

Geiselman, R.E. and Amet M.G., "Summarizing Military Information: An Application of Schema Theory," in Human Factors, Vol. 22, No. 6, December 1980, pp 693-707.

Gibson, R.S. and Nicol, E.H., "The Modifiability of Decisions Made in a Changing Environment," Report ESD-TDR-64-657. Decision Science Laboratory, Hanscom Field, Bedford, Mass., 1964. (AD 610-122.)

Howell, W.C. et al, "An Evaluation of Two Variables Contributing to the Difficulty of a Sequential Decision Task," Report AMRL-TDR-63-58, Aerospace Medical Research Laboratories, Wright-Patterson AFB, Ohio, June 1963. (AD 411-187.)

Kidd, J.S., Kidd and Hooper, J.J., "Division of Responsibility Between Two Controllers and Load Balancing Flexibility in a Radar Approach Control Team," Lab of Aviation Psychology, April 1959.

Kinkade, R.G. et al, "A Study of Tactical Decision Making Behavior," Report ESD-TR-66-61. Decision Sciences Laboratory, Hanscom Field, Bedford, Mass., Novemeber 1965. (AD 478-769.)

Kinney, G.C., Lawson R.N, and Maher, J.E., "Results of Human Factors Tests of Small Permanent Communications and Display Segment (SPCDS 11)," Mitre: Bedford, MA, August 1976.

Kreifedldt, J.G., "Cockpit Displayed Traffic Information and Distributed Management in Air Traffic Control," in Human Factors, Vol. 22, No. 6, December 1980, pp 671-693.

Kurabayashi, T., "Judgement Attitude of Operator Derived from Decision Rule," in Human Factors, Vol. 22, No. 1, Feb. 1980, pp. 37-43.

Marras, W.S. and Kroemer, K.H.E., "A Method to Evaluate Human Factors/Ergonomics Design Variables of Discrete Signals," in Human Factors, Vol. 22, No. 4, August 1980, pp 389-401.

Morgan, C.T. et al, Human Engineering Guide to Equipment Design, New York: McGraw-Hill, 1963.

Meister, D., Behavioral Foundations of System Development, Wiley and Sons: New York, 1976.

Rieck, A.M., Ogden, G.D., and Anderson, N.S., "An Investigation of Varying Amounts of Component - Task Practice on Dual - Task Performance," in Human Factors, Vol. 22, No. 3, April 1980, pp 373-385.

Schum, D.A., "A Further Evaluation of Computer-Assisted Processing of Complex Evidence Sets in a Simulated Military Threat-Diagnosis Task," Aerospace Medical Research Laboratories, Wright-Patterson AFB, Ohio, 1967.

Sidorsky, R.C. and Houseman, J.F., "Research on Generalized Skills Related to Tactical Decision Making," Report NAVTRADEVCEN 1329-2, U.S. Naval Training Device Center, Port Washington, N.Y., December 1966. (AD 813-382.)

Siegel, A.I. and Bronn F.R., "An Experimental Study at Control Console Design," in Ergonomics, Vol. 1, Nov. 1957 - Aug. 1958, pp 251-257.

Smith, S.L., and Maher, J.E., "Master Surveillance Control Facility Operators Job," Mitre: Bedford, MA, 15 September 1977.

Tactical Air Command, "Small Permanent Communications and Display Segment (SPCDS 11) IOT & E," May 1977, Tactical Air Command, USAF Tactical Air Warfare Center, Eglin AFB, Florida.

Uhlaner, J.E., and Druker A.J., "Military Research on Performance Criteria: A Change in Emphasis," in Human Factors, Vol. 22, No. 3, April 1980, pp 131-141.

Walt, H.J. and Manning M.W., "CAS-SAS Operational Work Station Design and Procedures," Mason and Hanger - Silas Mason Co., Inc.: Lexington, Kentucky, November 1980.

APPENDIX B

Below is a list of questions relating to security system design which may be useful to the human engineering community.

1. Is the local area alarm panel merely a readout (passive) display with no operator decision controls with the guard located in a assessment or fighting position?

2. Is the local area alarm panel a command and control system with operator decision controls for guard force notification and tactical deployment? (In this mode the position is not considered a primary fighting location.)

3. How large an area can one operator and annunciator cover?

4. How do you define and engineer redundency of displays?

5. What combination of alarm displays and TV assessment monitors saturate the operator?

6. Should annunciator operators be expected to visually assess as well as assess via CCTV? Is there a trade-off among orientation, loss of time, or disfunctioning of operator performance with the total equipment package?

7. What is the maximum channel capacity required of the annunciator?

8. What is the minimum channel capacity required?

9. What are the advantages/disadvantages of a hardcopy printer?

10. How do you protect against an internal threat to the annunciator system (covert by-pass)?

11. How do you provide a cross-check on the human operator to assure that proper follow-through is being accomplished?

12. How much work space and file space is required for the operator?

13. How long can an operator work until relieved?

14. Do annunciator functions require more than one operator at certain times?

15. What ancillary guard duty tasks assist or complicate the successful operation of the alarm annunciator?

16. What additional electronic equipments must interface with the operat r while he is performing annunciator duties?

17. What special skills are required for annunciator operators?

18. Can control panels be merged into one panel?

19. Can all visual alarms be centralized?

20. What are the tolerance thresholds for confusion and disorientation for operators on two, three, and four simultaneous alarms?

21. Where is the radio mike located relative to the operator position?

22. What is the maximum decision time for operator actions for each sensor alarm message? What is the maximum acceptable decision time for each multiple sensor alarm message?

BIOTECHNOLOGY PREDICTORS OF PHYSICAL SECURITY PERSONNEL PERFORMANCE

G.S. Lewis, Ph.D.

Command and Support Systems
Navy Personnel Research and Development Center
San Diego, California 92152

BIOTECHNOLOGY PREDICTORS OF PHYSICAL SECURITY PERSONNEL PERFORMANCE*

G. W. Lewis, Ph.D.
Command and Support Systems
Navy Personnel Research and Development Center
San Diego, California 92152

ABSTRACT

The military services depend heavily on paper-and-pencil testing to evaluate personnel. Such testing is able to predict school and training performance fairly well, but not on-job performance. On-job performance places heavy demands on right hemisphere brain processing (spatial, integrative, simultaneous) in addition to left hemisphere processing (verbal, analytical) which paper-and-pencil testing primarily measures. This Center has been investigating the feasibility of directly assessing brain functions using event related brain potential (ERP) recordings to improve the prediction of on-job performance. Promising results have been found in relating ERP data to the performance of pilocs, radar intercept officers, antisubmarine warfare trainees and basic recruit trainees. Under Defense Nuclear Agency funding, this Center recently undertook (FY81) a research project to determine the feasibility of using biotechnology measures (e.g., ERP) to improve the prediction of physical security personnel performance reliability. Predicting the tolerance to stress/duress is of particular interest. Project plans and progress are reviewed in this presentation.

BACKGROUND

The security of nuclear weapons is a primary concern of the Navy ship and shore community. Handling and storage of such weapons requires the highest quality and reliability in personnel. Security forces must be able to cope with a variety of threats from terrorist attack, disaffected crew members, or radical groups. One of the most crucial aspects of physical security is the security guard. Each guard must remain alert and prepared to detect, identify and respond to a variety of potential threats. There is a definite requirement

*The views expressed in this paper are those of the author and not necessarily the Department of the Navy or Defense Nuclear Agency.

to be able to assess the performance efficiency and reliability of the security guard force. One extremely important aspect of personnel reliability is the tolerance to stress by the guard. A capability for predicting security guard performance effectiveness under duress or stressful conditions could greatly increase the reliability of nuclear security operations.

Current physical security personnel assessment procedures are not very effective in predicting on-job performance. An experimental procedure which has shown promise in predicting on-job performance better than techniques currently being used is the direct recording of brain wave activity (e.g., event related brain potentials, ERP).

The brain, having two hemispheres, has been shown to have at least two different modes of cognitive processing. A verbal, analytic, sequential, logical mode of information processing has been associated with left-hemisphere activity in most right-handed individuals. Likewise, spatial, simultaneous and integrative processing has been attributed to right-hemisphere activity. These two modes of cognitive processing were initially discovered by anatomical studies using war wound, lesion, and "split-brain" subjects. More recently, these processes have been confirmed by modern computer technology and measures of brain electrical activity such as electroencephalographic (EEG) and event related brain potential (ERP) records. EEG and ERP records show brain activity as minute signals recorded from the scalp. The EEG shows on-going activity while the ERP shows activity after the brain has been stimulated (e.g., light flashes or clicks to the ears). Typically, for people performing verbal tasks, there is decreased EEG/ERP amplitude over the left hemisphere. For spatial tasks, there is generally a decrease over the right hemisphere. Such decrease in EEG/ERP activity is considered an index of increased information processing within that hemisphere. Some individuals may predominantly use a verbal-analytic information processing style for learning, problem solving, and decision making; whereas others predominantly use a spatial-integrative cognitive style for such tasks (Bogen, 1969; Galin & Ornstein, 1972; Dimond & Beaumont, 1974; Callaway, 1975; Galin & Ellis, 1975; Knights & Bakker, 1976; Ornstein, 1977; Kinsbourne, 1978).

One of the reasons we feel traditional paper-and-pencil aptitude tests predict academic performance fairly well, but not on-job performance, is that they tap the verbal, analytic processing performed by the left hemisphere. On-job performance requires much of the spatial, simultaneous processing performed by the right hemisphere. There have been many attempts to assess right hemisphere functioning by traditional testing procedures, but with little success. Procedures like the ERP may not only tap right hemisphere processing to a greater degree, but predict on-job performance more accurately than the traditional paper-and-pencil tests. Assessing individual differences with an emphasis on "process" rather than "content" variables, as suggested by the concept of brain activity, may prove more successful in predicting human performance.

An approach to increasing the prediction of personnel reliability which deserves careful study is the use of brain wave activity, such as the ERP. Recent research has shown ERP measures to be able to better predict on-job performance than paper-and-pencil tests (Lewis, 1980b; Lewis & Rimland, 1980; Lewis, 1981).

Jerison (1977) has suggested that vigilance (sustained and selective attention) may be assessed by the concept of brain asymmetry. He also suggested that selective attention and sustained attention may be very different behaviors, and that left hemisphere may be most involved with selective attention and the right hemisphere with sustained attention. Brain recording techniques similar to those described in a number of NPRDC reports (cited later) may be able to test Jerison's hypothesis and lead to better assessment of vigilance in physical security personnel.

OBJECTIVE

Major advances have occurred during the last several years in the areas of brain wave analysis (e.g., ERP) and psychophysiology (the study of behavior using physiological procedures). NPRDC initiated the Applied Psychobiology Project in FY75 as the first major effort to apply the findings of this research to the Navy's problems in the areas of personnel and training. The initial funding for this project was supported by NPRDC Independent Research (6.1) and Independent Exploratory Development (6.2) funds. In the NPRDC laboratory, ERP measures have been shown to be useful in predicting the success of Navy remedial trainees (Lewis, Rimland and Callaway, 1976); describing relationships between visual ERP measures and Navy paper-and-pencil aptitude test scores (e.g., AFQT) (Lewis, Rimland and Callaway, 1977); recording visual ERPs for the first time in a very "noisy" (electrical and acoustical) aviation environment, being able to differentiate pilots from radar intercept officers and relating brain ERP asymmetry relationships to aviator performance (Lewis, 1979a, 1979b; Lewis and Rimland, 1979); showing visual ERPs as potentially useful in predicting performance of sonar operators (Lewis, Rimland, Callaway, 1978; Lewis and Rimland, 1980); and that ERP measures may have relevance and application to physical security personnel (Lewis, 1980a). More recently, the ERP brain wave measures have been shown to have possible relationships to methods of processing cognitive information (Lewis, Federico, Froning and Calder, 1981; Federico, Lewis, Froning and Calder, 1981) and describe relationships between sensory interaction and reading using conventional electrode contact procedures (Lewis and Froning, 1981).

Physical security personnel assessment, training, and performance predictions may be greatly enhanced by brain activity recordings. It may be feasible to establish consistent relationships between brain wave patterns and stable, dependable performance. Brain recordings may provide extremely important information in the area of personnel reliability, that is, assessing and predicting the performance of personnel under duress conditions (e.g., the family taken hostage by terrorists). It may be possible to determine a pattern of responses to a set of stimuli that can provide a basis for identifying personnel who are tolerant to stress conditions. Perhaps changes in the dependability of physical security personnel could be detected through periodic measurement of brain waves for comparison against earlier baseline records. This technique may be able to detect unusual stress problems, disgruntled crew members, or collusion by "insiders".

Techniques must be developed for rapid, unobtrusive measurement of brain wave patterns. New techniques are now experimentally available using noncontact sensors for measurement of magnetic activity from brain (magnetoencephalography, MEG), muscle (magnetomyography, MMG) and other body functions.

To date, our brain recordings have been obtained by using a traditional contact electrode procedure. A noncontact procedure (e.g., MEG) procedure would greatly speed data collection. Descriptions of this technology have been presented in several papers along with discussion of similarities (and differences) between the conventional contact recordings and the MEG/MMG noncontact recordings (Brenner, Williamson, & Kaufman, 1975; Cohen, 1968, 1972; Cohen & Givler, 1972; Reite, Zimmerman, Edrich, & Zimmerman, 1976; Sarwinski, 1977; Wikswo & Barach, 1980). We feel that with further development, the noncontact approach may prove very useful in assessing physical security personnel behavioral characteristics related to performance reliability and effectiveness.

The current research effort provides for initial testing of ERP stability and reliability in predicting performance under baseline and stress conditions. Comparisons will be made between contact and noncontact techniques (ERP and MEG). Upon successful laboratory demonstration of feasibility, the MEG candidate predictors will then be developed for field trials and later possible implementation in order to improve prediction of security guard performance reliability and effectiveness.

APPROACH

An extensive laboratory of advanced hardware and software has been developed for recording and analyzing a large number of electrical signals (brain, heart, and muscle activity) from military personnel. A large library of predictor and performance follow-up data has been established. The laboratory capability will be expanded to assess subjects under a variety of baseline and duress conditions using non-contact procedures.

Each subject (approximate N = 40) will be given :he NPRDC-developed ERP assessment battery a total of three times over a four-hour period of time. Recording sites will conform to international standards (Jasper, 1958). Stability and reliability of the ERP measures will initially be determined over a relatively short time period (4 hours) and subsequently over a longer time period (days and weeks).

The ERP battery assesses sensory and cognitive function and includes the following tests: (a) eyes-open and eyes-closed electroencephalography (EEG) to assess two different arousal states; (b) visual ERP using a 5 foot-Lamberts full-field, black-and-white, red, green or blue checker board stimulus subtending a 9 degree visual angle and presented aperiodically about every 2 seconds; (c) auditory ERP using aperiodic click stimuli, 70 db(A), presented randomly between the left and right ears separately and both ears simultaneously; (d) bimodal ERP which includes the simultaneous presentation of stimuli discussed in (b) and (c) above; and (e) information-processing tasks (derived from Turner, 1965) to assess verbal (e.g., word abilities), spatial skills (e.g., solid figure turning) and combined verbal-spatial skills (e. ., cube counting).

PLANS AND PROGRESS

Table 1. BIOTECHNOLOGY PROJECT MILESTONES

FY	Milestone Description
81	Initiate laboratory experiments as inputs to physical security behavioral attributes profile. Assess stability and reliability of biotechnology contact procedures under baseline conditions appropriate to physical security personnel.
82	Develop experimental tasks which emulate duress. Assess those procedures developed in FY81 under baseline and duress conditions. Integrate magnetic analysis equipment (non-contact) into laboratory.
83	Compare contact and non-contact procedures under baseline and duress conditions.
84	Develop field trial capability for non-contact procedures. Initiate field trials.
85	Complete field trials assessing feasibility of using non-contact procedures for predicting personnel reliability and performance effectiveness.

Table 1 outlines the project milestones for the Biotechnology Project through FY85. This work unit was a new start in FY81.

A comprehensive literature review has been made to determine the most effective tasks and procedures to emulate stress/duress situations. Recent research has suggested relationships between brain hemisphere activation, stress, anxiety and emotion (Ley and Bryden, 1979; Sackeim, Gur, and Saucy, 1978; Tucker, Roth, Arneson and Buckingham, 1977; and Tucker, Antes, Stenslie and Barnhardt, 1978). A thorough review has been made of the Department of Navy Science and Technology Objectives (STOs) regarding potential relationships to the utilization and/or management of personnel associated with nuclear weapons (about 20 STOs were relevant).

Related work at NPRDC has been directed toward testing visual and auditory sensory interaction of Navy recruits undergoing basic training at the Naval Training Center, San Diego. Findings are presented in two reports:

1. Lewis, G. W. and Froning, J. N. Sensory interaction, brain activity, and reading ability in young adults. (Open literature publication).

2. Lewis, G. W., Federico, P-A., Froning, J. N. and Calder, M. Event related brain potentials and cognitive processing: Implications for Navy Training. (NPRDC Technical Report).

The behavioral literature, cited in the first report suggests a high relationship between sensory interaction (or the lack of it) and attention/distraction. One of the areas of interest to us in this DNA work unit is sustained and selective attention (e.g., vigilance) of the security guard force. Assessing sensory interaction/attention factors may be of considerable value in increasing on-job performance and training effectiveness of security personnel. These factors may also be key elements in stress tolerance of the guard force.

This research project has been reviewed and approved by the NPRDC Committee for the Protection of Human Subjects. Additionally, the legal implications (Privacy Act) of the use of human subjects in this project have been investigated by the Naval Reserves Legal Unit [VTU (LAW) 0614] stationed at the Naval Surface Weapons Center, White Oak (NSWC/WO). The results of interaction with the JAG unit indicates that there are no adverse legal implications for this research.

Software for the event related brain potential (ERP) battery data acquisition and analysis system has been converted from the black and white videographic to a new color videographic system. This conversion was required prior to testing subjects in fulfillment of FY81 milestones. Testing of subjects with the new software started during the second quarter. A comprehensive battery of ERP data has been acquired from about 10 subjects. Data analysis are underway.

An important requirement which must be met in this research is that our measures must be sensitive to individual differences among security personnel. At the same time, the measures must be stable and reliable over a specific period of time, for example one month or year. Being able to assess performance under baseline conditions and then to predict performance reliably when the guard is under duress, or under the influence of drugs or alcohol, necessitates meeting both of the above requirements.

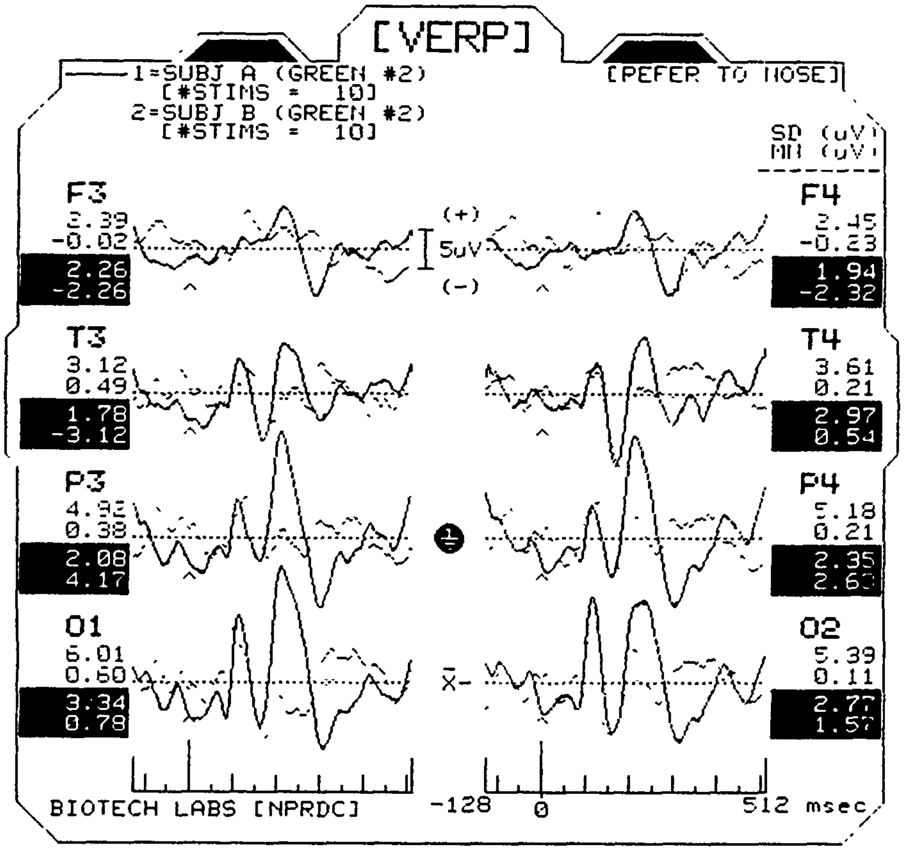


Figure 1. Visual (green stimuli) ERP waveforms for two subjects.

Figure 1 displays the new hardcopy format for ERP data from two subjects as a result of green visual checkerboard pattern stimulation. A more detailed description of our data analyses and displays may be found in Lewis and Froning, (1981) and Naitoh and Lewis (1981). This figure shows the eight channels of visual ERP data for subject "A" overlayed on subject "B". Calibration, polarity, and time base information were displayed along with the pre-stimulus waveforms. Post-stimulus waveform amplitude (SDμV) and mean (MNμV) values were computed and displayed for each group's electrode site. The waveforms in the left column were derived from the left hemisphere (LH). The waveforms from top to bottom were from the front to the back of the head at frontal (secondary association area), temporal (auditory reception area), parietal (primary association area), and occipital (visual reception area) sites (F3, T3, P3, 01). Right hemisphere (RH) ERP data were represented in the right column similar to LH (F4, T4, P4, 02). The top two values for each site represent the SD and MN values for subject "A" group, while the bottom two values represent those for subject "B". Few similarities are apparent for the two subjects' ERP records. Any similarities between the two subjects' records are probably due to the effects of the stimulus.

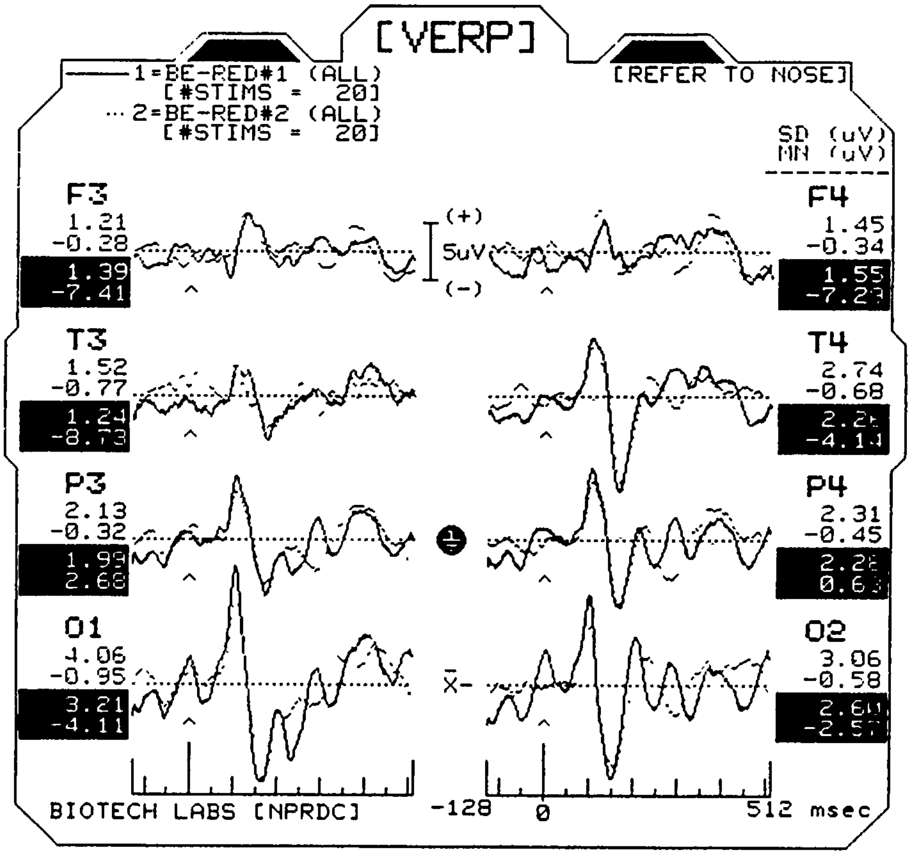


Figure 2. Visual (red stimuli) ERP waveforms recorded about two hours apart for a single subject.

Figure 2 shows a single subject's ERP waveforms produced by red checkerboard stimuli using the same display format as in Figure 1. The data were obtained about two hours apart. A great amount of intra-subject reliability may be seen. Figure 2 and similar data from other subjects suggest that we may be on the right track in meeting our second requirement for this research (intra-subject waveform stability). Color stimulation produces high intra-subject reliable waveform records, yet preliminary data analyses suggest that they also show maximal inter-subject variability. Data analyses are continuing.

Quantitative assessment of these records will require a "template" or pattern recognition and analysis procedure. Currently, cross-correlation and auto-correlation data analytic techniques are being examined. One of the most dramatic ways to assess the similarities and differences in ERP waveforms has been recently developed in our laboratory. Data are analyzed and displayed over the color video monitor. Either black and white hardcopy or color 35mm slides may be made of the displayed data. Our color videographic system is able to display up to 256 colors simultaneously. We can take advantage of this capability by overlaying two separate displays of data at one time in separate colors. Where the waveforms do not overlap, the original color is seen (e.g., yellow and green or red and blue). Where the waveforms overlap, however, the new combined color may be seen, such as purple. Such color-coding makes it very easy to see those ERP waveform areas which are stimulus-dependent (similarities) and those areas which are unique between subjects (differences). Similarities within a subject may also be observed when different stimuli are presented (e.g., visual, auditory).

REFERENCES

Bogen, J. E. The other side of the brain I, II, III. Bulletin of the Los Angeles Neurological Society, 1969, 34, 73-105, 135-162, 191-220.

Brenner, D., Williamson, S. F., & Kaufman, L. Visually evoked magnetic fields of the human brain. Science, 1975, 190, 480-482.

Callaway, E. Brain electrical potentials and individual psychological differences. New York: Grune and Stratton, 1975.

Cohen, D. Magnetoencephalography: Evidence of magnetic fields produced by alpha-rhythm currents. Science, 1968, 161, 784-786.

Cohen, D. Magnetoencephalography: Detection of the brain's electrical activity with a superconducting magnetometer. Science, 1972, 175, 664-666.

Cohen, D. & Givler, E. Magnetomyography: Magnetic fields around the human body produced by skeletal muscles. Applied Physics Letters, 1972, 21, 114-116.

Dimond, S. J. & Beaumont, J. G. (Eds.). Hemisphere function in the human brain. New York: John Wiley, 1974.

Federico, P-A., Lewis, G. W., Froning, J. N., and Calder, M. Validation of brain event related potentials as indicators of human cognitive processing. (NPRDC Technical Report DIN 304-80-10). San Diego: Navy Personnel Research and Development Center. In press, March 1981.

Galin, D. & Ellis, R. R. Asymmetry in evoked potentials as an index of lateralized cognitive processes: Relation to EEG alpha asymmetry. Neuropsychologia, 1975, 13, 45-50.

Galin, D. & Ornstein, R. Lateral specialization of cognitive mode: An EEG study. Psychophysiology, 1972, 9, 412-418.

Jasper, H. The ten-twenty electrode system of the International Federation. Electroencephalography and Clinical Neurophysiology, 1958, 10, 371-375.

Jerrison, H. J. Vigilance: Biology, psychology, theory and practice. In Mackie, R. R. (Ed.), Vigilance: Theory, operational performance, and physiological correlates. New York: Plenum Press, 1977, 27-40.

Kinsbourne, M. (Ed.). Asymmetrical function of the brain. New York: Cambridge University Press, 1978.

Knights, R. M. & Bakker, D. J. The neuropsychology of learning disorders: Theoretical approaches. Baltimore: University Park Press, 1976.

Lewis, G. W. Field applications of evoked potentials. Presented to U.S. Air Force School of Aerospace Medicine (AFSC), Brooks AFB, Texas, 9 May 1979a.

Lewis, G. W. Visual event related potentials of pilots and navigators. In Lehmann, D., & Callaway, E. Human evoked potentials: Applications and problems. New York, NY: Plenum Press, 1979b. (Proceedings of the NATO Conference on Human Evoked Potentials held at Konstanz, West Germany, 26-29 August 1978. Sponsored by the NATO Special Program Panel on Human Factors).

Lewis, G. W. Job performance and brain asymmetry: Relevance for physical security personnel. Presented at the Fifth Annual Meeting on the Role of Behavioral Science in Physical Security, held 11-12 June at the National Bureau of Standards, Gaithersburg, Maryland, 1980a.

Lewis, G. W. Event related brain potentials and job performance. Invited speaker and Open Forum participant, 24th Annual Human Factors Society Meeting, held 13-17 October at Los Angeles, California, 1980b.

Lewis, G. W. Biotechnology predictors of attrition. In preparation, 1981.

Lewis, G. W., & Rimland, B. Hemispheric asymmetry as related to pilot and radar intercept officer performance (NPRDC Tech. Rept. 79-13). San Diego, CA: Navy Personnel Research and Development Center, March 1979. (AD-A068 087)

Lewis, G. W., & Rimland, B. Psychobiological measures as predictors of sonar operator performance (NPRDC Tech. Rept. 80-26). San Diego, CA: Navy Personnel Research and Development Center, May 1980. (AD-A085 030).

Lewis, G. W. and Froning, J. N. Sensory interaction, brain activity, and reading ability in young adults. (Submitted for open literature publication) April 1981.

Lewis, G. W., Rimland, B., & Callaway, E. Psychobiological predictors of success in a Navy remedial reading program (NPRDC Tech. Rept. 77-13). San Diego, CA: Navy Personnel Research and Development Center, December 1976. (AD-A037 339).

Lewis, G. W., Rimland, B., & Callaway, E. Psychobiological correlates of aptitude among Navy recruits (NPRDC Tech. Note 77-7). San Diego, CA: Navy Personnel Research and Development Center, February 1977.

Lewis, G. W., Rimland, B., & Callaway, E. Visual event related potentials: Toward predicting performance. In Callaway, E., Tueting, P., & Koslow, S. H. Event related brain potentials in man. New York, NY: Academic Press, 1978. (Proceedings of Event Related Brain Potentials in Man Conference, held at Airlie House, Virginia, 26-29 April 1977. Sponsored by the Clinical Research Branch, National Institute of Mental Health, Rockville, Maryland.

Lewis, G. W., Federico, P-A., Froning, J. N., and Calder, M. *Event related brain potentials and cognitive processing: Implications for Navy training*. (NPRDC Technical Report DIN 302-80-5). San Diego: Navy Personnel Research and Development Center. In press, January 1981.

Ley, R. G. and Bryden, M. P. Hemisphere differences in processing emotions and faces. *Brain and Language*, 1979, *7*, 127-138.

Naitoh, P. and Lewis, G. W. Statistical analysis of extracted features. In Yamaguchi, N. and Fujisawa, K. *Recent advances in EEG and EMG data processing*. Proceedings of the International Conference on EEG and EMG Data Processing, Kanazawa, Japan, 10-12 September 1981. Amsterdam: Elsevier Press.

Ornstein, R. E. *The psychology of consciousness* (2nd Edition). New York: Harcourt Brace Jovanovich, Inc., 1977.

Reite, M., Zimmerman, J. E., Edrich, J., & Zimmerman, J. The human magnetoencephalogram: Some EEG and related correlations. *Electroencephalography and Clinical Neurophysiology*, 1976, *40*, 59-66.

Sackeim, H. A., Gur, R. C. and Saucy, M. C. Emotions are expressed more intensely on the left side of the face. *Science*, 1978, *202*, 434-436.

Sarwinski, R. E. Superconducting instruments. *Cryogenics*, December 1977, 671-679.

Tucker, D. M., Roth, R. S., Arneson, B. A., and Buckingham, V. Right hemisphere activation during stress. *Neuropsychologia*, 1977, *15*, 697-700.

Tucker, D. M., Antes, J. R., Stenslie, C. E., and Barnhardt, T. M. Anxiety and lateral cerebral function. *Journal of Abnormal Psychology*, 1978, *87*, 380-383.

Turner, D. R. *Practice for the Armed Forces Tests, the ARCO Self-Tutor for High Test Scores*. New York: ARCO, 1965.

Wikswo, J. P., Jr. & Barach, J. A. Magnetic field of a nerve impulse: First measurements. *Science*, 1980, *208*, 53-55.

PRIVACY AND THE LOSS OF PRIVACY AND THEIR POSSIBLE RELATIONSHIP TO MILITARY SECURITY GUARD PERFORMANCE: AN ANALYSIS OF ISSUES

Stephen T. Margulis

National Bureau of Standards
Washington, D.C. 20234

PRIVACY AND THE LOSS OF PRIVACY AND THEIR POSSIBLE RELATIONSHIP TO MILITARY SECURITY GUARD PERFORMANCE: AN ANALYSIS OF ISSUES

Stephen T. Margulis*

National Bureau of Standards
Washington, DC 20234

1. INTRODUCTION

The Defense Nuclear Agency (DNA) mission includes the responsibility to manage and conduct exploratory research directed toward the improvement of the physical security of nuclear weapon storage facilities. Much of this research is directed toward hardware. However DNA recognizes that the effectiveness of a security system depends on the military personnel assigned to operate the system and to respond to attempts to penetrate into the protected area. Therefore, DNA has encouraged the behavioral science community to suggest research programs with the potential for generating solutions to "people problems."

On occasion, DNA has suggested topics to the behavioral science community for evaluation of their potential for solving "people problems." For example, in 1979, DNA requested the Law Enforcement Standards Laboratory (LESL) of the National Bureau of Standards (NBS) to include within the scope of its examination of human vigilance an independent review of the topic of privacy as it relates to guard force performance. This was a consequence of the possibility that privacy could influence vigilant behavior. Specifically, LESL was asked to conduct a limited review of the topic of privacy in sufficient detail to establish what is known in general about the influence on job performance of the psychological and environmental factors associated with privacy and its loss, and to establish a framework for future research.

The purpose of this paper is to briefly summarize National Bureau of Standards ~~NBS~~'s review for ~~DNA~~ Defense Nuclear Agency of the topic of privacy and the loss of privacy as they relate to military security guard performance. First, the paper addresses the use of the term "privacy" because privacy has many meanings. Next, it describes the context within which privacy should be viewed. That context is the contrast between the civilian and military sectors in the status of personal privacy. Then, after describing the situation faced by the military security guard, the remainder of the paper focuses on selected environmental, organizational, and psychological variables that could contribute to privacy and the loss of privacy from the perspective of military security guard performance.

*Center for Building Technology, National Engineering Laboratory.

1.1 Privacy: Its meanings

The concept of privacy appears as a part of everyday speech, as a scientific concept in behavioral theories of privacy, and as a legal and philosophical concept. A 1977 review of the meanings of privacy in these various domains demonstrated that in each domain there was a variety of meanings and that there were similarities in the distinctions among meanings [1].[1]

A careful study of these meanings of privacy suggests a core definition of privacy: Privacy, as a whole or in part, represents the control of transactions between one or more persons and others, the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability [1, p. 10]. This core states the essential means and ends of privacy and it is an adequate umbrella for many of the meanings of privacy.

The core definition should not be regarded as the true meaning of privacy but as an abstract skeleton. It follows that the variability in the meanings of privacy is the result of different interpretations of the concepts and linkages among concepts in the core definition [1].

To illustrate this point there have been broad and narrow interpretations of the concept of transactions [1]. For example, a broad interpretation tends to equate transactions with all forms of social interaction. By contrast, a narrow interpretation tends to equate transactions with communicative acts. These are a subset of social interaction [9]. This paper emphasizes the narrow interpretation but uses the broad one when appropriate.

There is also some consensus on meanings. For example, the emphasis of many psychologists on autonomy and self-development as the essential ends of privacy is consistent with the position of those social and political philosophers who argue that self-respect, human dignity, and autonomy are the fundamental reasons for protecting privacy [2-8].

1.2 The Right of Privacy in U.S. Civilian and Military Life[2]

The importance of privacy in civilian life can be illustrated in several ways. In national surveys in the 1970's on the perceived quality of life, adult Americans regarded privacy as one aspect of quality of life [14]. The importance of privacy also has been reflected in the interest in privacy by all three branches of the Federal Government during the past 15 years.

[1] Numbers in brackets refer to references listed in section 8 of this report.

[2] This section draws heavily on references [10-13].

This interest has its roots in the American political philosophy that argues that to encourage individual action, thought, and decisionmaking, governmental interference with individual freedom must be limited. In this view, respecting individual privacy is a necessary condition for individual freedom. Therefore, personal privacy must be protected except in those instances in which the government has a reasonable and legitimate right to limit privacy. One such exception is the right of the military to limit the individual freedom, hence privacy, of its personnel.

Americans recognize and accept the principle that in order to develop an effective military unit with efficient, uniform operations, service personnel have to accept limitations on certain civilian "rights." In the area of personal privacy, service personnel will find that private items can be exposed to public view during "shakedown" inspections; limits are placed on where they can go, what they can do, and with whom they can associate even when off duty; and the public expression of private beliefs is more limited than in the civilian sector. These examples of limits on privacy cover both social communication and social interaction. The issue is not the legitimacy or justifiability of these limitations. Rather. the issue is their possible impact on the performance, career intent, and morale of our citizen-soldiers if the loss of privacy is too great, too unexpected, or too intolerable.

1.3 The Military Security Guard

Recent DNA-sponsored projects by Abbott Associates and Mission Research Corporation point to the less than optimal work situations faced by many military nuclear security guards [15-17]. Specifically, there is conflict between the military security mission and the military security guard's reality. The mission is predicated on a crisis: the detection, assessment, and response to an intruder. However, "an enemy never appears, war games never occur, and every 'crisis' is a simulated one" [16, p. 6]. This results in a lack of urgency or of purpose. In response, the mission of protecting nuclear weapons is transformed by superiors into "passing inspections, meeting operational readiness standards, and reducing behavioral infractions" [16, p. 6]. Tasks become routine and mentally unchallenging. Guards come to believe that their status in the military is low; that their mission may be important but their jobs aren't; that there is little opportunity to reach desired goals such as promotions or transfers; and that their superiors stress punishment for failure rather than rewards for success [15-18]. These conditions can lead to low motivation [19], job dissatisfaction, increased variability in job performance, and increased attrition [16,20].

Given this state of affairs, the question DNA and LESL posed to the author was to examine the contribution of privacy and the loss of privacy to the creation of the aforementioned problems and ultimately to their remediation.

The rest of this paper briefly describes privacy-related personal, organizational, and environmental factors that could affect the job performance, career intent, or morale of full-time military nuclear security guards.

2. THE PHYSICAL ENVIRONMENT

Privacy involves behavioral strategies for controlling the flow of information to others and/or controlling encounters with others so that these activities do not occur at the wrong time, wrong place, or under the wrong conditions. Like all social behavior, privacy behaviors are tied intimately to the physical settings in which they occur. For this reason, many behavioral theories of privacy directly address the role of the setting, that is, of the physical environment. These theories discuss settings that drive people to seek privacy elsewhere; that reduce desired privacy into painful isolation from others; and that are suitable for some forms of privacy but not others [21,22]. In short, the physical setting can create or destroy opportunities for privacy.

Three predictions will illustrate possible ways in which privacy-related aspects of the physical environment could affect the performance of military nuclear security guards. First, the location of observation posts on nuclear weapons storage sites and the locations of sites themselves both can be isolating--isolating guards from others on site or from amenities off site. Several psychologists suggest that physical isolation, a form of privacy in which control over transactions is lost, can affect morale and performance [23-25]. Second, it is hypothesized that the location of a guard's observation post will determine how well the guard can monitor intruders and, conversely, how well intruders can monitor the guard [22]. There is a third, corollary prediction. Because of the boredom of watchstanding, it is predicted that some guards will "tune out" while on duty if they believe no external threat against their site is likely and if they believe that their location will permit them to monitor the approach of a duty officer before being seen by that duty officer. These two predictions have obvious implications for the role of vigilance in guard force performance.

There are many privacy-related aspects of the physical environment that could impact on the service person. For example, work station location may affect job performance, housing and amenities available to guards' families may affect career decisicns, and lack of privacy in the barracks may affect morale. Unfortunately, in the absence of substantial research on the effects of the physical environment on privacy, these hypotheses remain speculations.

3. ORGANIZATIONAL FACTORS

All organizations, including the armed services, must coordinate both information and the activities of its employees so that organizational goals are achieved. The organizational means to this end is called the organizational control system. Control systems specify the behaviors that are appropriate and the consequences, such as rewards and punishments, of an employee's behavior. Extrinsic control systems emphasize rewards and punishments under the organization's control [26]. The military, in many instances, employs an extrinsic control system.

Under conditions of low employee motivation and employee dissatisfaction--conditions that appear to characterize nuclear guards--, extrinsic control systems are likely to produce dysfunctional privacy-related consequences. Based on a recent, trenchant analysis of control systems, the following consequences are predicted. Guards will behave in ways that satisfy the measures used to evaluate them even if these behaviors do not satisfy the real needs of the organization. It also is predicted that guards will attempt to control how they are evaluated [26, pp. 1254-1259]. These attempts will include, when feasible, the creation of invalid data. These attempts at information control will be more likely when an evaluation relies on subjective data, or when it is unlikely or difficult for the organization to check on the accuracy of the evaluations [26]. In this context, a guard who is acting vigilantly because the guard believes he or she is being monitored by a superior illustrates the creation of hard-to-verify invalid data by the guard.

4. DEINDIVIDUATION

There is another organizationally-linked, privacy-related notion with potentially dysfunctional implications for the military. It is the psychological concept of deindividuation [27]. Deindividuation has been described as a loss of uniqueness which can result in attempts at reaffirmation. It also has been described as a loss of identifiability, which can result in antisocial acts based on a lack of concern about sanctions or about how others will evaluate the acts. Acts associated with deindividuation are known to include defacing and destroying property, theft, and aggression against others.

Among the conditions that create deindividuation are membership in a large group, group governance by formal rules, dominant leadership, and members having similar equipment and tools [28]. All of these organizational conditions are found in the military. However, these are the necessary conditions for deindividuation. Personal, social, and environmental factors, such as the presence or absence of like-minded peers, establish the sufficient conditions [28,29].

Thus, according to theories of deindividuation, if the military strips service personnel of their identity and uniqueness, then the military can expect, under the appropriate conditions, acts of reaffirmation, which could include destructive or other undesirable acts of retaliation.

5. SURVEILLANCE

As the last few topics have suggested, under certain conditions, people will break rules. Rule breaking is probably universal. As a consequence, it should come as no surprise that all social systems will invade the privacy of its members by monitoring them in order to catch and punish rule breakers, thereby protecting the rules. Just as important, monitoring is used to make sure that certain conditions, such as remaining productive on the job, are being met. However, monitoring and surveillance can be highly stressful for their targets in addition to being a powerful incentive for obeying rules and working productively. Thus, monitoring and surveillance have implications for job satisfaction, morale, and performance.

In this regard, one potentially useful application of the concepts of surveillance and monitoring to guard performance is the extensive literature on work place supervision [30]. An unusual analysis, with supporting experimentation, which is applicable to supervisor-worker relations, will be used to illustrate this literature [31]. This analysis concluded that breaking rules becomes likely when workers find that when they obey the rules, their supervisor profits at their expense. Thus, if nuclear security guards feel that their commanding officers get the rewards for guards passing an inspection but all the guards get are punishments for their failures, then this analysis suggests that the conditions for rule breaking are present. To prevent rule breaking, the analysis offers the supervisor at least two options: to keep the workers under constant surveillance or to make sure that the distribution of rewards to workers and to the supervisor is equitable. Surveillance reduces rule breaking so long as it is maintained. When it is not maintained, retaliation, in the form of rule breaking, becomes very likely. By contrast, when rewards are equitably distributed, there is less likelihood of rule breaking and also less need for surveillance.

There is another application of the concept of surveillance to military job performance. This one focuses on the related concept of socialization. Socialization, at its core, employs monitoring in order to teach individuals what is expected of them and in order to inculcate values consistent with these expectations. The process of socialization takes place at all stages of our lives, psychologists now argue. Making a civilian into a soldier is an example of socialization. It follows that a recruit who accepts the military way as his/her own during training should not require extensive subsequent monitoring. By contrast, if a recruit does not learn to think like a service person but only to act like one in order to avoid disciplinary action, then this recruit might require extensive monitoring. In this case, the use of monitoring and surveillance, backed by the application of contingent rewards and punishments, is the military's principal basis for ensuring conformity with its rules. (This approach was discussed in section 3.) The problem, then, is how to socialize recruits so that their private beliefs are consistent with and further the military mission.

6. PERSONNEL POLICIES

The military has a number of personnel policies with loss-of-privacy implications. One illustration will suffice. In contrast to the civilian sector, in the military, communications between physicians, including psychiatrists, and their patients are not priveleged. In fact, the medical officer must report visits to the patient's commanding officer. A related practice is that visits by service personnel with a grievance to an Inspector General can be reported to the visitor's commanding officer. Notwithstanding the arguments favoring such regulations, these violations of privacy can worsen a situation for an individual who has already demonstrated a need for help, and could make these channels less attractive to those seeking help [13].

There is an important topic that will not be discussed but which must be acknowledged. It is individual differences in the need for privacy, in preferences for different forms of privacy, and in attitudes toward invasions of privacy. For example, there seem to be telling differences between military nuclear security guards and volunteers for behavioral science research on privacy in occupation, education, ethnicity, and related characteristics. These differences raise questions about the applicability of this research to military guards.

7. PRIVACY AND THE LOSS OF PRIVACY: THE FUNDAMENTAL ISSUE

In closing, the issues raised in this paper about the effects of privacy and the loss of privacy on job performance have been addressed at two levels. At one level are the fundamental, underlying issues, and at the other, are more "symptomatic" issues. The emphasis has been on symptomatic issues because these appear to be more open to remediation. However, if symptoms are treated superficially, the fundamental issues and the associated potential threats to a viable security system could remain.

One fundamental issue is that American civilians desire and expect to be treated as unique, autonomous, worthy individuals. If these desires and expectations carry over to the military setting, then many of the potential problems that have been identified could have their origin in whether these desires and expectations are acknowledged, fostered, or met in military life.

The tie to privacy and to the loss of privacy is based on an argument raised by many psychologists and social and political philosophers. To become a unique, autonomous, worthy individual requires, as one antecedent, opportunities for privacy [2-8]. An important analysis has cogently argued that through feedback from our successes and failures at regulating communication and interaction with others, we generate an understanding and evaluation of ourselves. In turn, this understanding is the basis for our sense of uniqueness and autonomy and this evaluation is the basis for our sense of worth [2].

Thus, any proposed solutions to actual privacy-based problems ultimately must address this fundamental issue.

8. REFERENCES

[1] Margulis, S. T. Conceptions of privacy: Current status and next steps. Journal of Social Issues, 1977, 33(3), 5-21.

[2] Altman, I. Privacy: A conceptual analysis. In D. H. Carson (ed.), Man-environment interactions: Evaluations and applications (Part II, Vol. 6: S. T. Margulis, Vol. Ed.). Stroudsburg, PA: Dowden, Hutchinson & Ross, 1975.

[3] Westin, A. Privacy and Freedom. NY: Atheneum, 1967.

[4] Proshansky, H. M., Ittelson, W. H., and Rivlin, L. G., Freedom of choice and behavior in a physical setting. In H. M. Proshansky, W. H. Ittelson, and L. G. Rivlin (Eds.), Environmental psychology: Man and his physical setting. NY: Holt, Rinehart and Winston, 1970.

[5] Margulis, S. T., Privacy as information management: A social psychological and environmental framework. (NBSIR 79-1973). Washington, DC: National Bureau of Standards, 1979.

[6] Benn, S. I., Privacy, freedom, and respect for persons. In J. R. Pennock and J. W. Chapman (Eds.), Privacy. NY: Atherton Press, 1971.

[7] Freund, P. A. Privacy: One concept or many? In J. R. Pennock and J. W. Chapman (Eds.), Privacy. NY: Atherton Press, 1971.

[8] Simmel, A. Privacy is not an isolated freedom. In J. R. Pennock and J. W. Chapman (eds.), Privacy. NY: Atherton Press, 1971.

[9] Shaw, M. E., and Costanzo, P. R. Theories of social psychology. NY: McGraw-Hill, 1970.

[10] Kurland, P. B. The private I--Some reflections on privacy and the constitution. The University of Chicago Record, 1976 (July), 10(4), 107-124.

[11] Margulis, S. T. Introduction. Journal of Social Issues, 1977, 33(3), 1-4.

[12] Pennock, J. R., and Chapman, J. W. (Eds.). Privacy. NY: Atherton Press, 1971.

[13] Sherman, E. F. The rights of servicemen. In N. Dorsen (Ed.), The rights of Americans: What they are--What they should be. NY: Pantheon, 1970, 1971.

[14] Andrews, F. M., and Withey, S. B., Developing measures of perceived life quality: Results from several national surveys. Social Indicators Research, 1974, 1, 1-26.

[15] Abbott, P. S. Candidate assessment phase I: Perceptions and job environments of physical security personnel. (Final draft report: Abbott 22500FR). Alexandria, VA: Abbott Associates, February 1979.

[16] Orth, R. H. Candidate assessment nuclear security--Domestic site job analysis. (DNA 5045F). Washington, DC: Defense Nuclear Agency, August 1979.

[17] Hall, R., Caldwell, J., Solomonson, D., Weaver, R., and Hanna, W. Security performance measurement system--phase I: Literature search and data collection design--Volume II. Santa Barbara, CA: Mission Research Corporation, January 1979.

[18] Hall, R., Security performance measurement methodology. In G. Lapinsky, A. Ramey-Smith, and S. T. Margulis (Eds.), The role of behavioral science in physical security: Proceedings of the fourth annual symposium, July 25-26, 1979. NBSIR 81-2207(R). Washington, DC: National Bureau of Standards, February 1981.

[19] Shaw, M. E. Group dynamics: The psychology of small group behavior. NY: McGraw-Hill, 1971.

[20] Locke, E. A. The nature and causes of job satisfaction. In M. D. Dunnette (Ed.), Handbook of Industrial and Organizational Psychology. NY: Rand-McNally, 1976.

[21] Laufer, R. S., Proshansky, H. M., and Wolfe, M. Some analytic dimensions of privacy. In R. Kuller (Ed.), Architectural Psychology: Proceedings of the Lund Conference. Stroudsburg, PA: Dowden, Hutchinson & Ross, 1974.

[22] Archea, J., The place of architectural factors in behavioral theories of privacy. Journal of Social Issues, 1977, 33(3), 116-137.

[23] Brownfield, C. A. Isolation: Clinical and experimental approaches. NY: Random House, 1965.

[24] Altman, E., An ecological approach to the functioning of social groups. In J. E. Rasmussen (Ed.), Individual and group behavior in isolation and confinement. NY: Aldine, 1971.

[25] Haythorn, W., Project Argus--1967: Five year review and preview. (Report No. 31). Bethesda, MD: Naval Medical Research Institute, August 1967.

[26] Lawler, E. E., III. Control systems in organizations. In M. D. Dunnette (Ed.), Handbook of Industrial and Organizational Psychology. NY: Rand-McNally, 1976.

[27] Dipboye, R. L., Alternative approaches to deindividuation. Psychological Bulletin, 1977, 84(6), 1057-1075.

[28] Ziller, R. C., Individuation and socialization. Human Relations, 1964, 17, 341-360.

[29] Zimbardo, P. G., The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. _Nebraska Symposium on Motivation_, 1969, 17, 237-307.

[30] Weiner, E. L. Vigilance and inspection. In J. S. Warm (Ed.), _Sustained attention in human performance_. NY: Wiley, in press.

[31] LaTour, S., & Thibaut, J., Surveillance and the pattern of interdependence in the lawmaker-individual relationship. Paper presented at the 82nd annual convention of the American Psychological Association, New Orleans, August 1974.

[32] Westin, A., _Computers, personnel administration, and citizens rights_. (NBS Special Publication 500-50). Washington, DC: National Bureau of Standards, 1979.

GENERIC ADVERSARY CHARACTERISTICS AND THE POTENTIAL THREAT TO LICENSED NUCLEAR ACTIVITIES FROM INSIDERS

Sarah Mullen

Division of Safeguards
U. S. Nuclear Regulatory Commission

GENERIC ADVERSARY CHARACTERISTICS AND THE POTENTIAL THREAT TO LICENSED NUCLEAR ACTIVITIES FROM INSIDERS

Sarah Mullen
Division of Safeguards
U.S. Nuclear Regulatory Commission

NRC has been charged by Congress with the responsibility for provision and maintenance of safeguards against theft and sabotage of licensed nuclear materials and facilities. In the discharge of this mandate, the Commission directed the Division of Safeguards to undertake two studies: one aimed at a systematic determination of the characteristics of potential adversaries to nuclear programs and the second aimed at a more detailed examination of the potential insider adversary.

The first study, entitled Generic Adversary Characteristics (GAC), was intended as an initial NRC effort at threat definition. It entails an analysis of characteristics associated with subnational conventional crimes and terrorist actions that could be analogous to potential nuclear events. Notce I said "analogous"--since adversary actions directed against nuclear facilities have been so few, we relied on an analog methodology under the assumption that a study of serious non-nuclear crimes can provide insights into the characteristics of potential nuclear adversaries.

p102

The data sources for the study consisted of over 650 articles, studies, books, NRC reports and memoranda, as well as interviews with Federal experts, criminologists, psychiatrists and social scientists.

The study addressed six generic adversary groups: terrorists, organized/sophisticated criminals, extremist protestors, disoriented persons, disgruntled employees, and miscellaneous criminals. They constituted the perceived range of possible threats of concern to us at the time. Data were drawn from incidents wherein laws were broken or in which criminal intent was obvious. We integrated the results of the data analysis into an adversary characteristic matrix like the one you received. Each column of the matrix represents a composite profile of one of the six generic adversary types based on observed actions and behavior.

Please recognize that these composites do not represent the upper or lower limits of adversary characteristics. Rather, they are the characteristics commonly found in the criminal acts we reviewed. As such, they can be considered representative of the characteristics that might be exhibited by such groups should they target nuclear activities in the near future.

I don't have the time today to discuss the matrix in detail, but I would like to mention briefly some of the study's conclusions. First, one of the least likely methods of attack is an overt armed assault. Even highly dedicated terrorists usually choose to approach their targets without resorting to arms, preferring to display firepower only once inside and in control of a facility. Second, physical danger appears to have some deterrent effect on all adversaries except the psychotic. Most adversaries proved to be risk avoiders. Third, organized and professional criminals often recruit insiders to provide them with some form of assistance, and disoriented persons, disgruntled employees, and white-collar criminals usually operate as insiders.

Finally, pegging defense capabilities to some predetermined number of postulated adversaries might be an inappropriate tack for security planners since behavioral characteristics such as motivation and dedication appear to influence adversary success at least as much as group size.

The Insider Study addresses the two types of insider crime that are the primary concern of nuclear safeguards--theft and sabotage--and focuses on the insider adversary, one whose authorized access to a facility or activity may be exploited by him or others in the commission of a crime.

The three objectives of the study are shown here. Data used in fulfilling these objectives were derived primarily from case histories of insider crime, but also from expert opinion and from non-NRC studies. Today, I will concentrate on objectives one, two and the prevention portion of three.

As with the GAC, we relied on an analog approach. Our criterion for determining which of the cases we gathered were the best analogs was the degree to which the safeguards systems in place at the time of the crime approximate the safeguards required of nuclear licensees.

From the cases that met our criteria, we extracted data on a variety of characteristics of the insider adversary and grouped them into the four categories shown on this vu-graph: position-related (e.g., screening and length of service); behavioral (such as motivation); resource (e.g., group size and equipment); and operational (such as tactics).

The major sources of data for the study fall into the two categories shown--U.S. Government agencies and private industry. Examples in the first category include the FBI, Department of Energy, and Bureau of Engraving and Printing. The second category includes money handlers, such as banks and casinos; material handlers, such as drug firms and chemical manufacurers; and money or material transporters, sucn as explosives carriers and armored transport companies.

In presenting the results of our characteristics analysis, I will be addressing the typical insider thief, the typical insider saboteur and a comparison between the lone thief and the theft conspiracy. First, the thief. The typical insider thief acted alone in 70% of the theft cases, whereas 10% involved two insiders and 20% three or more insiders. Typically, and not surprisingly, the insider thief was motivated by greed, indebtedness or financial inducement. These money-related motivations accounted for 74% of all the motivations identified. The next most frequently occurring motivations were drug use/abuse (6%) and personal loyalty (5%). The largest percentage of insider thefts (38%) occurred during the 6-10 year period of employment, 27% in the 3-5 year time period, and 19% during the first two years of employment. Approximately 80% of the insider thieves planned their crimes well or moderately well. By the way, all of these figures are based on 112 cases of insider theft involving 237 insiders.

Next we looked at the role of the insider, defining role as either overt or covert. By "overt" we mean that the insider was able to perpetrate the crime in the presence of others without arousing suspicion. "Covert" means that the insider was unable to carry out the crime in the presence of others without arousing suspicion. Approximately two-thirds of the insider thieves relied on covert activity to commit their crimes. Lastly, in 87% of the cases, equipment necessary to commit the crime was available at the site of the theft. Although not shown on the vu-graph, we also gathered data on the insiders' level of pre-employment screening. Over 40% of the insider thieves had received poor screening or none at all, with only 11% receiving high-level screening and just a handful undergoing psychological evaluation.

Before looking at the typical insider saboteur, I would like to emphasize that our sabotage analysis is based on a small data base, and thus our findings represent a limited characterization. First, 85% of the analogous sabotage cases were committed by a single insider. Although no one motivation dominated the insider saboteur, the combined motivations of psychological problems, disgruntlement and revenge accounted for 54% of the identified motivations. Approximately two-thirds of insider saboteurs committed their crimes in the first two years of employment, and they tended to plan less well for their crimes than did the thieves. In fact, about one-third of their actions could be characterized as spur of the moment acts executed against targets of opportunity. The insider saboteur, like the thief, relied on covert action 88% of the time and most frequently used equipment that was readily available at the site of the crime. As with the thief, psychologcal evaluations were rarely administered and over a third had received poor screening or none at all.

The next three vu-graphs depict a comparison between the single thief and thieves who operate in conspiracy.

For nearly every case in the data base, we identified the one or more generic weaknesses in the security system that rendered it vulnerable to the insider adversary. The five vulnerabilities shown here are the ones that most frequently accounted for the success of the crimes we analyzed and were most often cited by government and industry experts. Let me say a few words about the fourth entry. Personnel security deficiencies include inadequate pre-employment screening, insufficient behavioral observation, and poor management/employee relations. These three deficiencies contributed to the success of about 15% of the theft cases and about 70% of the sabotage cases.

Inadequate screening was judged a vulnerability when it was discovered after the fact that the insider had a criminal record that made him a poor risk or that he had a history of emotional instability that cast doubt on his ability to function reliably. Insufficient behavioral observation was applied when the malevolent insider suffered from a psychological or personal problem (including drug abuse) that should have warned an alert co-worker or supervisor to potential difficulty. Poor management/employee relations refers to situations in which management failed to provide a mechanism for airing and resolving employee grievances or proper recognition and incentives for its employees.

In assessing prevention method effectiveness, we looked at a number of different techniques now in use in industry and government and derived some implications about the prevention strategies shown. For today's symposium, I will discuss only the first three methods listed.

As for screening, our data suggest that it is an effective theft control strategy, and most of the experts we interviewed strongly advocated its use. Its effectivesness arises from several factors. First, it's generally accepted that a potential adversary may be deterred from even applying for a job at a facility that employs screening. Second, it conveys to prospective employees, as well as to those who are eventually hired, that the organization is concerned with insuring a high degree of integrity among its workforce. And third, good screening correlates with reduced conspiracy formation. Of a l the insider thieves in our data base who underwent "good" screening (i.e., screening based on a full-field background investigation or its equivalent), about 60% acted alone with 40% acting in conspiracy with other insiders. This table also suggests that screening must be "good" to make a difference because for any level of screening less than "good," the results are nearly the same: more conspiracy formation. (The total number of insiders represented by this table is 169.)

With respect to government clearances, we found the following. A clearance cannot be expected to provide full assurance of future trustworthiness because any number of factors can impair employee stability and reliability after hire. It can, however, reduce the likelihood of infiltration by criminal or terrorist elements and lessen the chances that a facility will hire persons who misrepresent their identities or backgrounds or persons with histories of relevant criminality or emotional instability.

Behavioral observation appears to pick up where screening leaves off by providing a post-employment means of recognizing and dealing with instability or aberrant behavior in employees. By so doing, behavioral observation can increase employee reliability after hire, but for such a program to be effective, three elements are necessary. First, employees' baseline stable behavior should be identified at the time of hire. Second, supervisory personnel must be properly trained to recognize aberrant behavior. And third, criteria for determining unreliability must be unambiguous and applied equitably.

Less data was available to us on the subject of psychological evaluations because many of the industries we contacted do not employ this technique due to privacy act considerations. However, the technique is widely used in police departments and the intelligence community. Generally, we concluded that psychological assessments can be an effective adjunct to screening and behavioral observation if they are evaluated by professionals, but that great care must be taken to prevent their misuse and mitigate their intimidating impact on personnel. Psychological evaluations may be especially important in preventing sabotage, which was often motivated by psychological problems.

Since the Insider Study was completed last summer, the Commission has taken action with respect to the pre-employment screening issue. In November, NRC issued a final rule requiring individuals who have access to or control over strategic quantities of special nuclear material to be cleared for such access through an NRC-administered personnel security program. Affected individuals will undergo government background investigations concomitant with their level of access at the expense of the licensee.

More recently, the NRC Staff is preparing for Commission review a rule that will govern access to non-weapons-grade nuclear material at power reactors. This program would be administered by reactor licensees themselves, not by NRC. As currently envisioned, and I emphasize that this rule is still in the draft stage, the program will consist of three components. First, a background investigation, perhaps with FBI criminal record checks initiated by the licensees. Second, psychological assessment, consisting of two written personality tests, one geared toward "abnormal" behavior patterns and one toward the "normal" adult population, and a clinical interview for individuals whose test results are questionable or indicate abnormal personality traits. And third, a post-employment behavioral observation program to detect psychological changes that may be manifested as behavioral changes in job performance, competence or judgment capabilities. As for the psychological tests, the NRC has determined the MMPI and the 16PF to be acceptable instruments for use in this program. Should a licensee wish to use other inventories, he would have to establish that they meet a number of standards, including high test-retest reliability and statistically validated scores. Both the tests and the interview should be based on the criteria shown here, which are measures of behavioral unreliability that have been shown to be relevant to the nuclear work setting.

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES / ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
ORGANIZATIONAL CHARACTERISTICS						
1. Organization	Well organized, hierarchical, bureaucratic, specialization common, compartmentalization practiced	Efficient, hierarchical, bureaucratic (TOC)* No specific organization (WCC & CC)**	"Range" of organizational structure from no formal organization to well organized groups (i e , collectives, small cells, etc)	Little or no formal organization except for the psychotic cult Anti s ials may belong to some organized criminal entity	Little or no formal organization with the exception of organized strike violence	Little or no formal organization
2. Recruitment	Universities, prisons, vocational training centers, refugee camps and ethnic population centers	Self-corrupted Blackmail Criminal Birthright (TOC)	High schools, universities, prisons.	Psychotics and neurotics exhibit no propensity to recruit others - they operate alone. Anti-socials often recruit others for riminal acts	Normally operate alone and do not recruit others Recruitment may occur within ;*or groups during organized strike violence	Often act alone If others are recruited, they normally are associated with street criminal "clan
3. Financing	Criminal activities robbery, kidnapping/extortion Donations by foreign countries, intelligence agencies, other terrorist groups, private citizens	Criminal activities gambling, drug sales, loan sharking (TOC) Legitimate business investments (TOC) No sustained financing other than personal resources (WCC/CC)	Criminal activities robbery, fraud Legitimate jobs, parental assistance, donations	Use of personal funds as necessary Normally, no financing required Drug addicted commit crimes to finance habit	Use of personal funds as necessary No significant degree of financing required	Criminal activities as appropriate No significant degree of financing required
4. International Connections	"Very High training, political support and financing from many Third World and Communist states Extensive contacts between groups	"High" - Worldwide (TOC) "Very low" None determined (WCC & CC)	"High" for Western European groups "Low" for domestic groups	"Very low" none determined	Very low" none determined	"Very low none determined

A Examples include Baader Meinhof Gang Red Army Faction, PLO, Red Brigades, IRA, SLA, FALN, Anti Castro Cubans, etc

B Examples include (a) traditional "family" oriented groups (e g Mafia in Chicago), (b) ethnic "family" oriented groups (c) matrix oriented groups, (d) one time operating groups (e g , Brinks and Purolator robberies), (e) computer crimes, (f) other sophisticated crimes/capers

C Politically motivated, issue oriented acts of violence or criminality normally of symbolic nature Differentiated from terrorist acts in that violence is generally low level Terror is not an objective

D Psychotics, neurotics and personality disorders to include drug/alcohol influenced, etc

E This group also includes former employees

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime

SCALE:

Very Low – Low – Moderate – High – Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES / ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
OPERATIONAL CHARACTERISTICS						
5. Planning	"High" Normally involves target intellinence natherinq, casino, and careful preparation	"Very High" - Detailed preparation to include casing and rehearsal	"Unknown" - Planning detail not known for most domestic groups Western European extremists exhibited careful planning	"Range" of planning Acts often spontaneous and involve no planning, other times detailed preparation	"Low" little evidence of extensive or long term planning	Very Low" little or no planninq
6. Timing	Function of political, symbolic and operational objectives and requirements	Timed to minimize risk of discovery - m st "operationally" expedient moment	Function of political, symbolic and operational objectives and requirements	"Contagion" timing effect for psychotics No other discernible timing pattern - individual unique	Most acts timed to minimize risk of discovery most "operationally expedient moment	Often spontaneous and unpredictable Maximize "operational chances of success
7. Tactics	Bombinn most common Also, assassination, armed attacks, kidnappinn, skyjackinn	Deception, diversion and crimes such as theft, fraud extortion, hijacking, corruption, bombing	Bombing most common Violent demonstrations, property destruction, sabotane	Bombing, arson, skyjacking, hostage taking, multiple homicide, sabotage, fraud	Bombing, sabotage, theft, intrusion, property destruction, vandalism	Burglary, theft, assault, drug sales, forgery, bombing
8. Collusion (Insider)	Very Low"	"High" - Insider assistance frequently sounht (TOC) "Very High" - most often are insiders (WCC & CC)	"Very Low"	"Moderate" - Individuals may in fact be insiders	"Very High" most often are insiders	Low" however, inside information is frequently sought as opposed to using individual inside

A Examples include Baader Meinhof Gang, Red Army Faction, PLO Red Brigades, IRA, SLA, FALN, Anti Castro Cubans, etc

B Examples include (a) traditional "family" oriented groups (e g , Mafia in Chicago), (b) ethnic "family" oriented groups (c) matrix oriented groups (d) one time operating groups (e g , Brinks and Purolator robberies), (e) computer crimes, (f) other sophisticated crimes/capers

C Politically motivated, issue oriented acts of violence or criminality - normally of symbolic nature Differentiated from terrorist acts in that violence is generally low level Terror is not an objective

D Psychotics neurotics and personality disorders to include drug/alcohol influenced, etc

E This group also includes former employees

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime

SCALE:

Very Low – Low – Moderate – High – Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
BEHAVIORAL CHARACTERISTICS						
9. Motivation	Political and Ideological Hatred of Society (nihilists)	Financial gain and increased personal power	Politically-centered and 'ssue-oriented Often result of frustration, discontent, anger, etc	Wide 'range " Is a function of the individual s mental disorder	Range" of employment related problems (e g , being fired, passed over for promotion, etc)	Financial gain Desire for drugs and alcohol
10. Dedication/ Discipline	"Very High"/"Moderate"	"Moderate"/"High" (TOC) "Low"/"Moderate" (WCC & CC)	"Moderate"/"Moderate"	"Very High"/"Very High" (psychotic) "High"/"Low (neurotic) "Low"/"Low" (anti-social)	"Low"/"Low	"Low"/"Low
11. Willingness To Kill	Very High"	"Moderate" (TOC) "Very Low" (WCC & CC)	"Low"	Very High" (psychotic) 'Moderate" (neurotic) "High (anti social)	Low	Moderate
12. Willingness To Give Up Life	"High" - not generally suicidal but willing to give up lives for cause if required	"Low" (TOC) "Very Low" (WCC & CC)	"Very Low"	"High" (psychotic) "High" (neurotic) "V--y Low" (anti-social)	"Very Low	"Low

A Examples include Baader Meinhof Gang, Red Army Faction, PLO Red Brigades, IRA, SLA, FALN, Anti-Castro Cubans, etc

B Examples include (a) traditional "family" oriented groups (e g , Mafia in Chicago); (b) ethnic "family" oriented groups (c) matrix oriented groups, (d) one time operating groups (e g , Brinks and Purolator robberies), (e) computer crimes, (f) other sophisticated crimes/capers

C Politically motivated, issue oriented acts of violence or criminality normally of symbolic nature Differentiated from terrorist acts in that violence is generally low level Terror is not an objective

D Psychotics, neurotics and personality disorders to include drug/alcohol influenced, etc

E This group also includes former employees

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime

SCALE:

Very Low – Low – Moderate – High – Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1

ADVERSARY CHARACTERISTICS MATRIX

GROUPS BY GENERIC CATEGORIES / ADVERSARY CHARACTERISTICS	A Terrorist Groups	B Organized/ Sophisticated Criminal Groups	C Extremist Protest Groups	D Disoriented Persons	E Disgruntled Employees	F Miscellaneous Criminals
RESOURCE CHARACTERISTICS						
13. Training/Skills	"High" levels of training in weapons use, tactics, explosives manufacture, forgery, codes, security, etc	"High" levels of training from Criminal experience (TOC) "High levels of college and technical training (WCC & CC)	Domestically, a range of informal group training and use of criminal experience	Wide "range " Is a function of adversary's background, training and experience	Wide "range " Is a function of individual's background, training and experience	"Low" levels of formal training "Street wise" criminal experience
14. Personnel Technical Sophistication	Typically "Moderate" Explosive device technical knowledge "High"	"Very High" with high levels of ingenuity and improvisation	"Moderate"	Wide "range " Is a function of individual's background, training and experience	Wide "range " Is a function of individual's background, training and experience	"Low" Use of simple and unsophisticated techniques
15. Group Size	Typically 1-6	Typically 1-6	1-4 covert crimes Up to 35,000 mass/violent demonstrations (Western Europe)	Psychotics and Neurotics typically operate alnne Anti social operatas alone or part of criminal group (size indeterminate)	Typically 1-2 6 or more in strike related crime	Typically operate alone Occasionally in groups of 2-5
16. Weapons	Handguns, rifles, shotouns, automatic weapons, explosives, grenades, anti-tank weapons, surface-to-air-missiles, chemicals and poisons	Handnuns, rifles, shotouns, automatic weapons and explosives (TOC) None documented (WCC X CC)	Handnuns, rifles, shotouns, explosives and incendiaries	Handguns and other small arms, explosivas anc incendiaries, objects of convenience	Handguns and other small arms, explosives anc incendiaries, objects of convenience	Handguns and other small arms
17. Equipment	Simple tools for barrier penetration False documentation Communication equipment	Sophisticated security systen bypass and physical barrier breaching equipment Other sophisticated improvised equipment	Protective helmets, gas masks, wire and bolt cutters, basic communications enuipment, etc for mass/violent demonstrations Simple breakinc and enterinn equipment and false ID for covert acts.	"Range" of equipment Is a function of individual's background, training and experience	"Range" of Equipment Is a function of individual's background, training, and experience Use of items of convenience in work area	Simple breaking and entering equipment Low level explosives for penetration
18. Transportation	Private and leased vehicles, stolen vehicles, commercial aircraft, railway, small boats, motorcycles, on-foot	Private or leased vehicles, stolen vehicles, public transportation, privately owned aircraft	Privately owned vehicles, oublic transportation, motorcycles, on-foot, hitchhikinn	Privately owned vehicles, public transportation, aircraft, on-foot	Privately owned vehicles, public transportation, on foot	Privately owned and stolen vehicles, public transportation, on font

A Examples include Baader Meinhof Gang Red Army Faction, PLO Red Brigades, IRA, SLA, FALN Anti Castro Cubans, etc

B Examples include (a) traditional "family" oriented groups (e g Mafia in Chicago), (b) ethnic "family" oriented groups (c) matrix oriented groups, (d) one time operating groups (e g , Brinks and Purolator robberies); (e) computer crimes, (f) other sophisticated crimes/capers

C Politically motivated, issue oriented acts of violence or criminality normally of symbolic nature Differentiated from terrorist acts in that violence is generally low level Terror is not an objective

D Psychotics neurotics and personality disorders to include drug/alcohol influenced, etc

E This group also includes former employees

F The crimes committed by elements of this generic adversary group generally fall into categories of violent personal crime, public order crime and commonplace crime

SCALE:

Very Low — Low — Moderate — High — Very High

* TOC - Traditional Organized Crime

** WCC & CC - Single White Collar Crime and Computer Crime

Figure 1

STAFFING AND SHIFT HOURS: PERFORMANCE CONSIDERATIONS

Harold E. Price
Marjorie B. Bauman

BioTechnology, Inc.

STAFFING AND SHIFT HOURS: PERFORMANCE CONSIDERATIONS

Harold E. Price
Marjorie B. Bauman
BioTechnology, Inc.

Abstract. An important consideration in site surveillance is whether trade-offs in staffing configurations could be used to compensate for less than desired numbers of personnel at nuclear sites. This is a report of a literature search to deterr the state of knowledge about the effects on per 'mance with staff manning and shift duration as variables. While this literature search was done for nuclear power plant control room operators, the findings may have broader applicability to guard force staffing and shift policies. The alternatives examined were working longer shifts, reducing the number of qualified personnel required on any shift, and using individuals with less training and experience. The results were inconclusive, but the least desirable alternative is using less qualified personnel. Long shift hours probably result in some performance decrement, as compared to 8-hour shifts, but the extent of the decrement is uncertain. A reduction in manning is the favored alternative, but this holds only for normal operations.

Introduction

A number of nuclear power plants are experiencing manpower shortages in the areas of control room personnel and security guard staffing. The Nuclear Regulatory Commission (NRC) is particularly concerned with the staffing problems of control room operators of near term operating license power plants. Many of these plants are unable to meet the staffing requirements necessary for licensing until more licensed personnel are available. If these plants are to operate, they must employ alternative staffing configurations.

To evaluate the adequacy of several staffing options, the NRC recently tasked BioTechnology, Inc., to perform a review of the existing research literature (Price et al. 1980). The Defense Nuclear Agency (DNA) expressed interest in this topic and the current paper has been modified to address the special concerns of the DNA and the security personnel.

The problems of less than desirable numbers of qualified workers, as well as the inherent difficulties involved with shift work, are also applicable to the nuclear security guard forces. Some of the common problems associated with shift work will be discussed first, and then some of the major findings of the NRC-sponsored literature review will be summarized. Where applicable we will point out the relevance of the findings to the nuclear security guard personnel. Three alternatives regarding optimal staffing configurations under conditions of reduced manpower were considered:

1. Changing from an 8-hour rotating shift to a 12-hour rotating shift
2. Reducing the number of qualified personnel required on any shift
3. Utilizing individuals with less experience and training.

The present paper highlights a review of the available scientific literature regarding the alterations in performance that might be expected under each of these three staffing alternatives. The studies selected for inclusion in this paper emphasize those components of performance that are most similar to the job requirements of control room operators, the original target population for the review, with comments noted to point out the relevance of the findings to the nuclear security guard force. Specific components of performance addressed in this review included measures of vigilance, watch-keeping, monitoring displays, reaction time, cognitive processing, problem solving, decisionmaking, and performance under stressful conditions. Both laboratory and field studies were examined. Applied studies from observations of workers in related occupations were also included, focusing on data from investigations of air traffic controllers, radar display monitors, prolonged driving, nurses, and plant operators.

General Review of Shift Work

Figure 1 depicts some of the adjustment problems facing workers changing shifts or assigned to evening or night shifts that conflict with conventional habits, as well as individual psychological and physiological responses. The psychological and sociological costs of shift work are often described as feelings of isolation, and those who try to maintain normal off duty activities with their family and friends are frequently plagued with loss of sleep. On their days or weekends off, most night workers stay awake during the day and go to bed at night. The importance of leisure time habits overrides the concern for letting their bodies fully adjust to working at night. Therefore, each week these workers pay physiological costs associated with continual rephasal of their disrupted circadian rhythms. These problems are exacerbated for rotating shift workers. In addition, both night and rotating shift workers tend to be less efficient on the job because they are working at the time when their bodies want to be sleeping.

One measure of job performance problems linked with shift work is increased accidents or injuries on the job. Tasto et al. (1978) reviewed the health and safety files of 1,200 nurses and

1,200 food processors. Figure 2 presents the relative accident rates of day, evening, night, and rotating shift workers for nurses across a 6-month period. For both groups, rotating shift workers had the highest accident rate--approximately 20% above fixed shift workers.

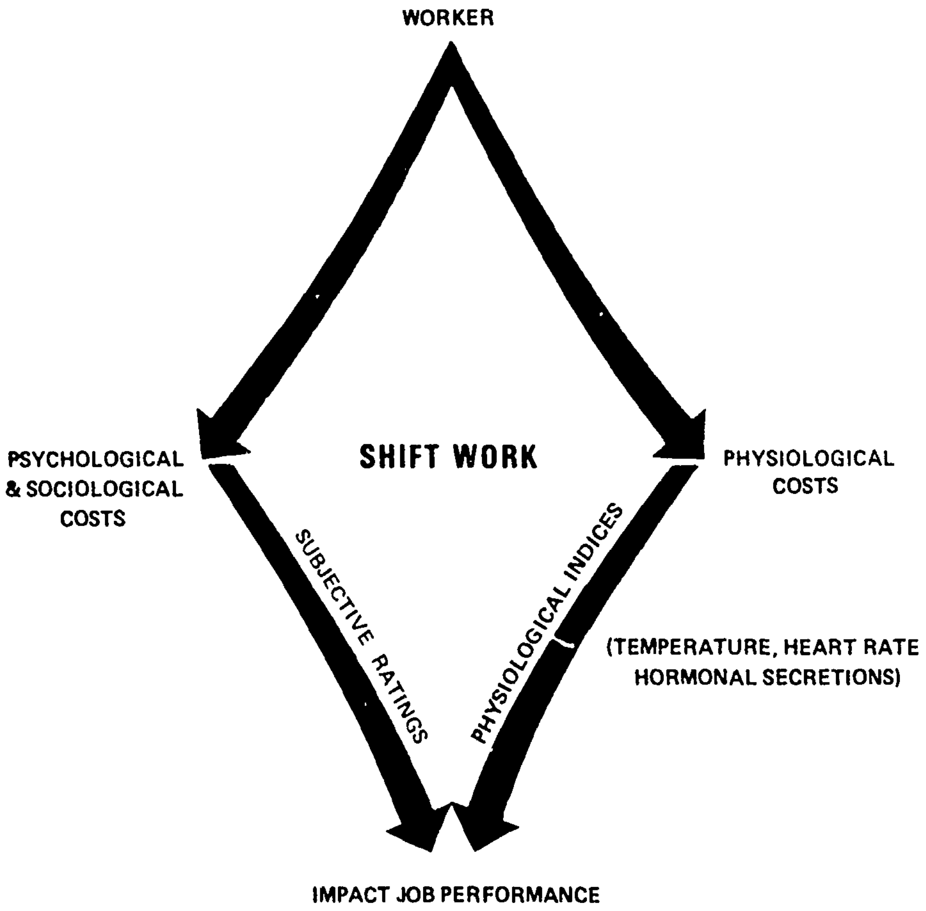


Figure 1. Adjustment problems associated with shift work.

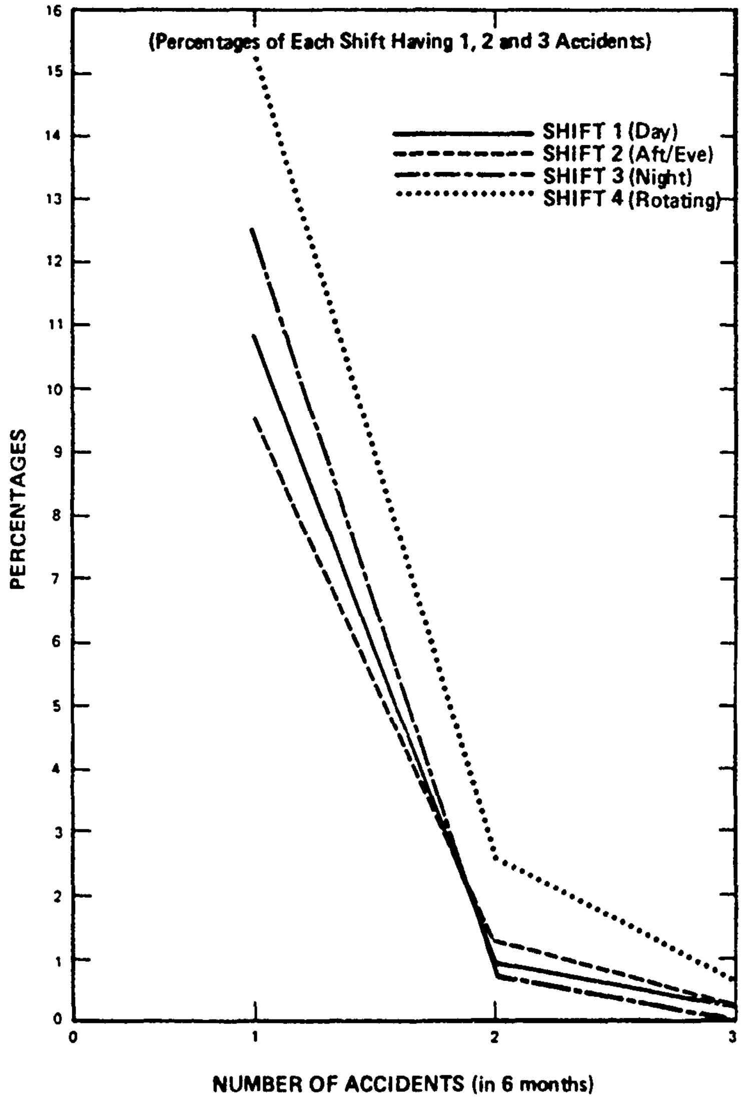


Figure 2. Accidents – nurses. (From Tasto et al., 1978)

Another type of job performance problem associated with shift work is decreased job efficiency and actual performance decrements. Colquhoun et al. (1968) investigated performance measures and physiological variables in British navy subjects on a standard 8-hour night shift. Simple addition tasks were tested. Figure 3 presents the results of this 12-day study in terms of number of sums attempted, percent of error, and body temperature. The graphs show a consistent fall in body temperature and number of sums attempted throughout the 4 daily work periods across the 12 days. It is important to note that the patterns of decline for body temperature and number of sums attempted are remarkably similar, suggesting that the circadian rhythm disruption that occurs during night work is associated with a distinct decline in speed of performance.

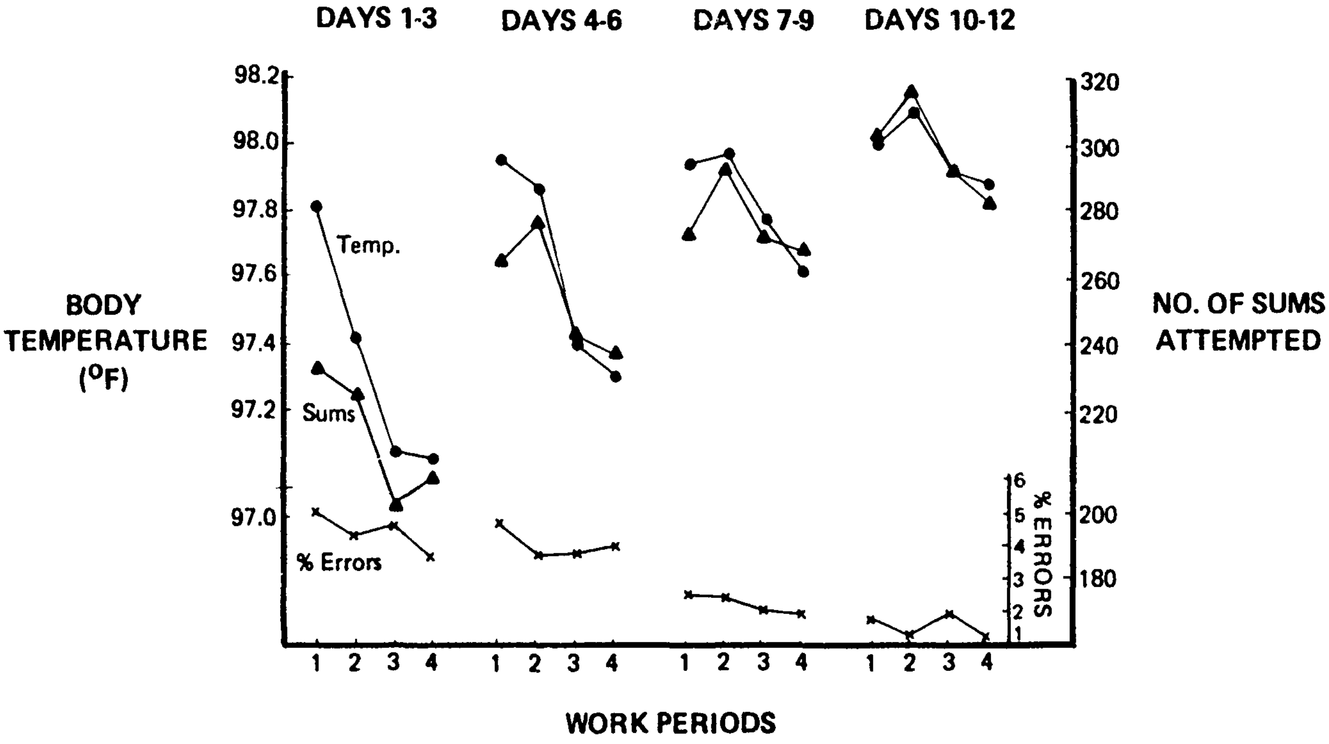
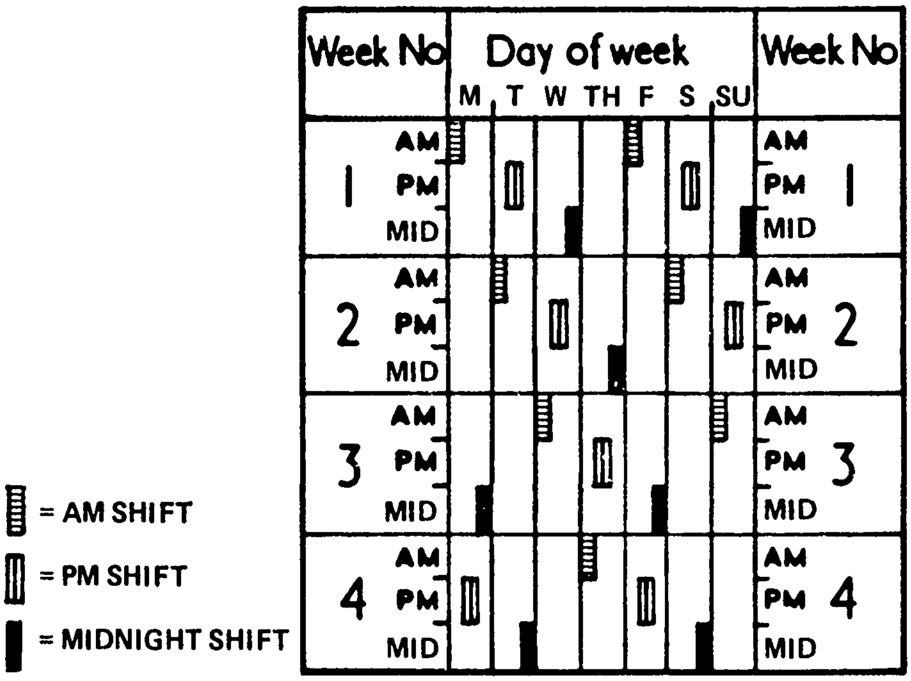


Figure 3. Night shift: Mean scores in the calculation test, and mean temperature, averaged over successive 3-day periods of the trial for each work period of the shift.
(From Colquhoun et al., 1968)

Several innovative work schedules have been developed in an attempt to give workers more opportunity to adjust or rephase to varying work hours. For rotating shift workers who appear to have the most serious problems rephasing to continually changing shifts, Poulton (1979) devised a simple 8-hour rotating shift system. The system allows workers 24 hours off between shifts instead of the usual 16 hours that separate periods of work occurring at the same time of day. Figure 4 shows this scheme set up on a 4-week basis with weeks manned consecutively by 4 separate teams. However, this system allows only 24-hour weekend breaks between one shift and the next. To better accommodate the night shift portions of rotating shifts, Poulton (1979) designed a mixed shift system, presented as Figure 5, that allows a 40-hour break every 8 days, placed between 2 night shifts. The complete scheme is repeated every 8 weeks.



Week No		M	T	W	TH	F	S	SU		Week No
1	AM	▤				▤			AM	1
	PM		▯				▯		PM	
	MID			▮				▮	MID	
2	AM		▤				▤		AM	2
	PM			▯				▯	PM	
	MID				▮				MID	
3	AM			▤				▤	AM	3
	PM				▯				PM	
	MID	▮				▮			MID	
4	AM				▤				AM	4
	PM	▯				▯			PM	
	MID		▮				▮		MID	

▤ = AM SHIFT

▯ = PM SHIFT

▮ = MIDNIGHT SHIFT

Figure 4. A simple 8-hour rotating shift system. (From Poulton, 1979)

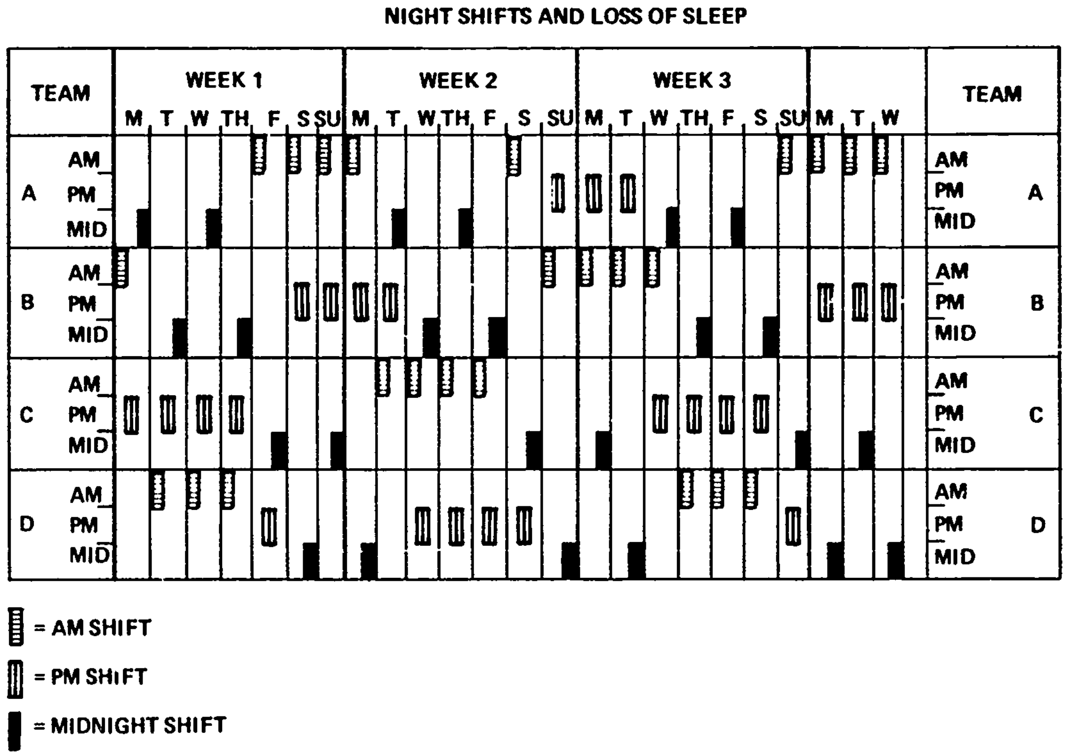

NIGHT SHIFTS AND LOSS OF SLEEP
TEAM
WEEK 1
WEEK 2
WEEK 3
M T W TH F S SU M T W TH F S SU M T W TH F S SU M T W
A
B
C
D
AM
PM
MID
= AM SHIFT
= PM SHIFT
= MIDNIGHT SHIFT

Figure 5. A mixed shift system that repeats every 8 weeks. (From Poulton, 1979)

The introduction of the 4-day work week is another attempt to accommodate shift workers by allowing them more consecutive leisure time. The 4-day work week has also become an attractive, cost-effective alternative for many employers because it enables them to close down operations for three days each week and thus cut their ever-increasing energy expenses.

After this brief overview of general shift work problems, we will now move on to discuss the specific staffing alternatives examined in the NRC-sponsored project.

Alternative 1: Changing from an 8-Hour to a 12-Hour Rotating Shift

A large number of studies have been reviewed that relate to the possible effects of changing from an 8-hour rotating shift to a 12-hour rotating shift on performance of workers engaged in different types of monitoring tasks. For the purposes of this review, the effects of this staffing alternative have been examined from two perspectives. First, this option requires longer working hours in each working day, but a shorter workweek (4 days per week rather than 5). Second, because of the weekly rotations, this alternative incurs larger circadian rhythm disruptions than the 8-hour rotating shift. The effects of each of these variables are treated separately.

Longer Working Hours

Most of the studies of prolonged performance in the laboratory have found decrements in performance on at least one measure of performance, but not necessarily all. For example, Ellingstad and Heimstra (1970) exposed 15 male students to a primary tracking task and a variety of subsidiary tasks for three blocks of 5 hours separated by 15-minute breaks. The tracking task involved following a target on a screen by means of a steering wheel, and the speed of the target was altered every 20 minutes. Subsidiary performance tasks included a vigilance test requiring the subject to respond to the deflection of a needle on a small meter, two reaction time tasks, mental multiplication, and "digit span" that required the subject to repeat as rapidly and accurately as possible a set of five, six, or seven digits.

Figure 6 shows the results for the primary tracking task, in terms of mean time off target and mean number of times off target, for each of the three target speeds. Both performance measures showed a gradual decrement throughout the 15 hours, but the decrement was more pronounced and began earlier for the number of times off target measure. Performance tended to show improvement after each of the 15-minute breaks.

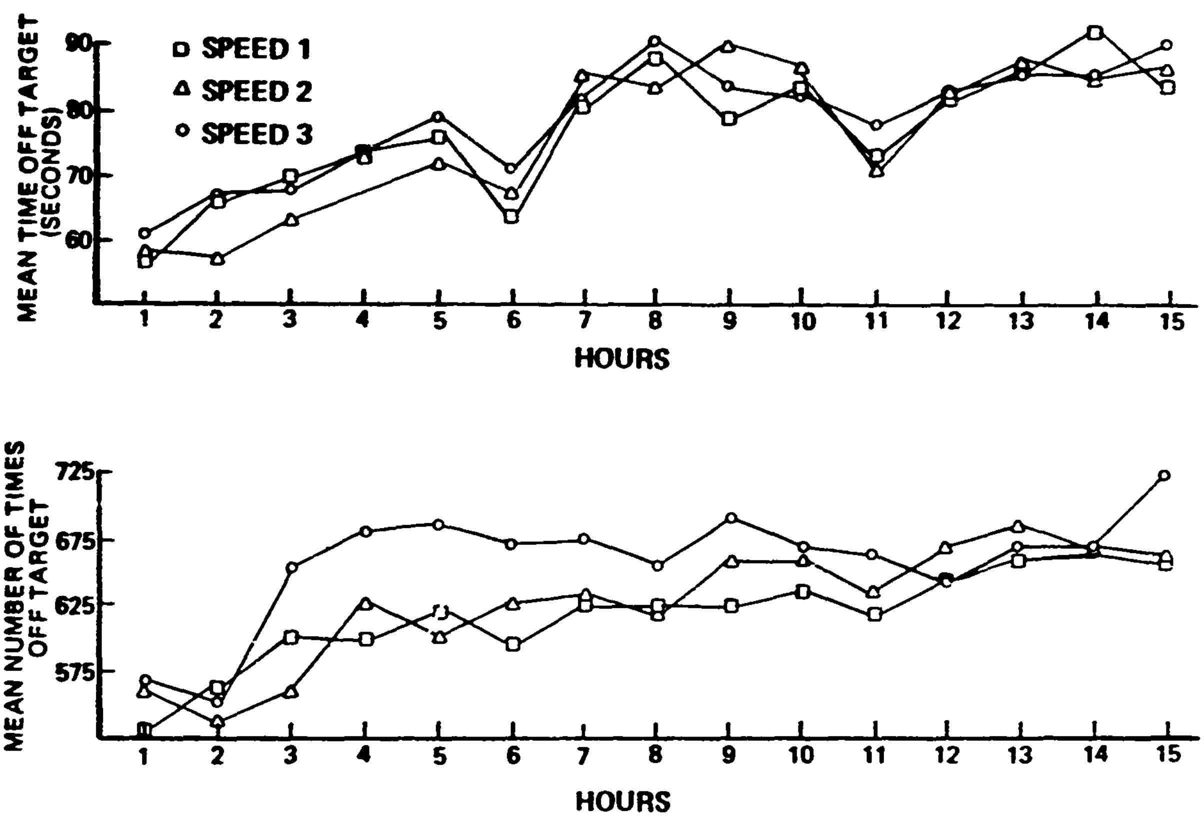


Figure 6. Mean amount of time off target and mean number of times off target each hour of the 15-hour session. (From Ellingstad & Heimstra, 1970)

Perhaps more pertinent to the present review are the investigations involving workers in related occupations whose performance is measured across a lengthy workday. Some researchers attempt to measure actual job performance, or accident rates, and others measure performance on subsidiary tasks derived by the experimenter.

Air Traffic Controllers. Grandjean et al. (1971) investigated performance changes on subsidiary tasks during a 10-hour workday in 68 Swiss air traffic controllers. The measurements were critical fusion frequency, which measures the frequency of light flashes at which the subject perceives a steady beam, and generally is used as an index of the rate of information processing by the visual system; speed of grid tapping; and a self-rating of fatigue. Figure 7 presents the results: the abscissa represents the hours since starting work, regardless of shift position; the ordinate represents flicker fusion frequency (Hz), and number of contacts for the two tapping tests.

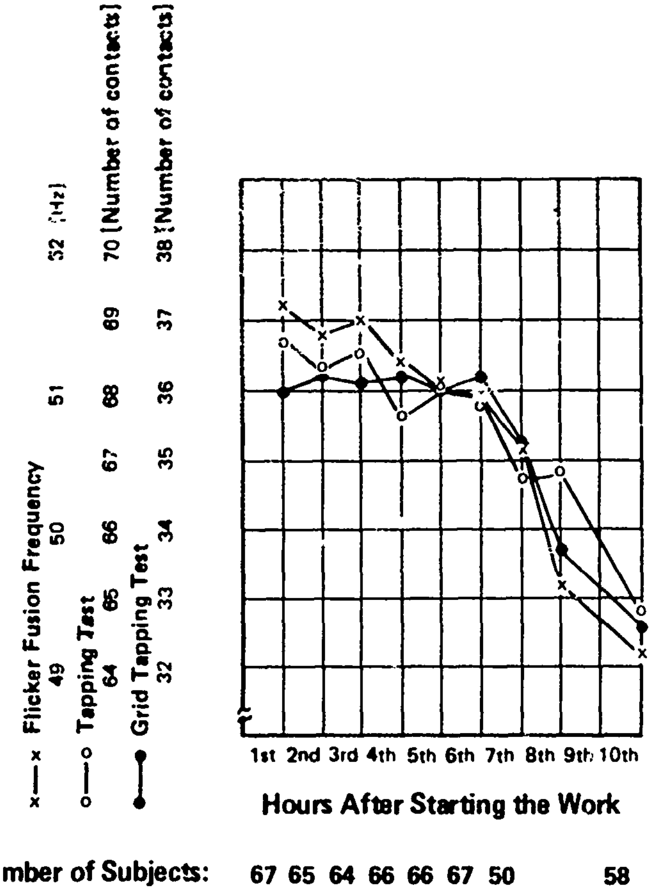


Figure 7. Mean values of critical fusion frequency, of a tapping and of a grid tapping test in relation to hours after starting work. (From Grandjean et al., 1971)

Performance on these subsidiary tasks declined gradually until about the 7th hour after starting work; thereafter, the decline was precipitous. The overall performance decrements from the 1st to the 10th hour of work on these measures of nervous system function averaged between 5 and 12%. Figure 8 shows responses to a self-rating of fatigue for these same air traffic controllers. The questionnaire included five paired adjectives: strong-weak, relaxed-tense, refreshed-tired, vigorous-exhausted, and awake-sleepy. Each subject was asked to rate his own feelings of fatigue, each hour after starting work, on a 7-point scale for each of the paired adjectives. For example, if the subject felt "strong" rather than "weak," he might mark "6" for that pair of adjectives. The graph represents changes in the mean scores for each of the five pairs of adjectives across the workday. It demonstrates that subjective feelings of fatigue, as measured by this questionnaire technique, tend to follow rather closely the changes in performance, as measured by critical fusion frequency and tapping speed.

Industrial Employees. Haider (1963, cited by Grandjean, 1968) investigated changes in performance on a subsidiary task in 21 female industrial employees working a 9-hour day. Small light bulbs were fixed on the heads of the subjects, and light signals were presented at irregular intervals during the workday. The number of missed signals and reaction times were recorded. Figure 9 presents the results from this investigation.

The number of omitted signals increased during the first 5 hours of work, decreased after lunch, then increased again for the remainder of the working day. Reaction time increased throughout the working day, but appeared to level off somewhat from the 7th through the 9th hour of work.

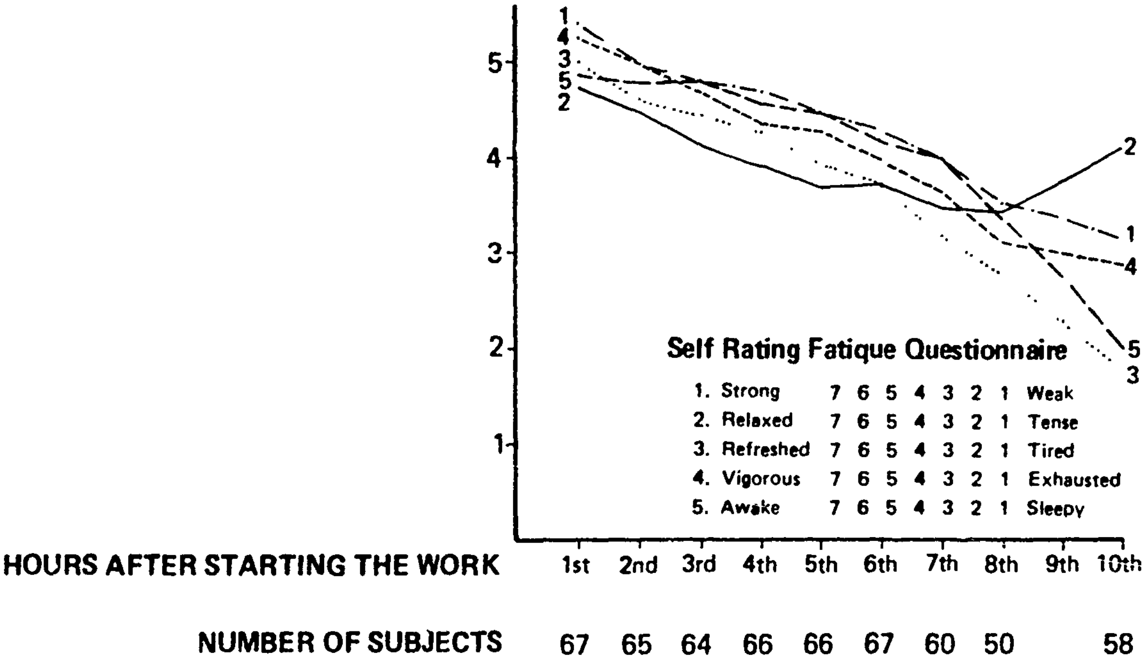


Figure 8. Mean values of each of the five paired adjective items of the self rating test in relation to the hours after starting work. (From Grandjean et al., 1971)

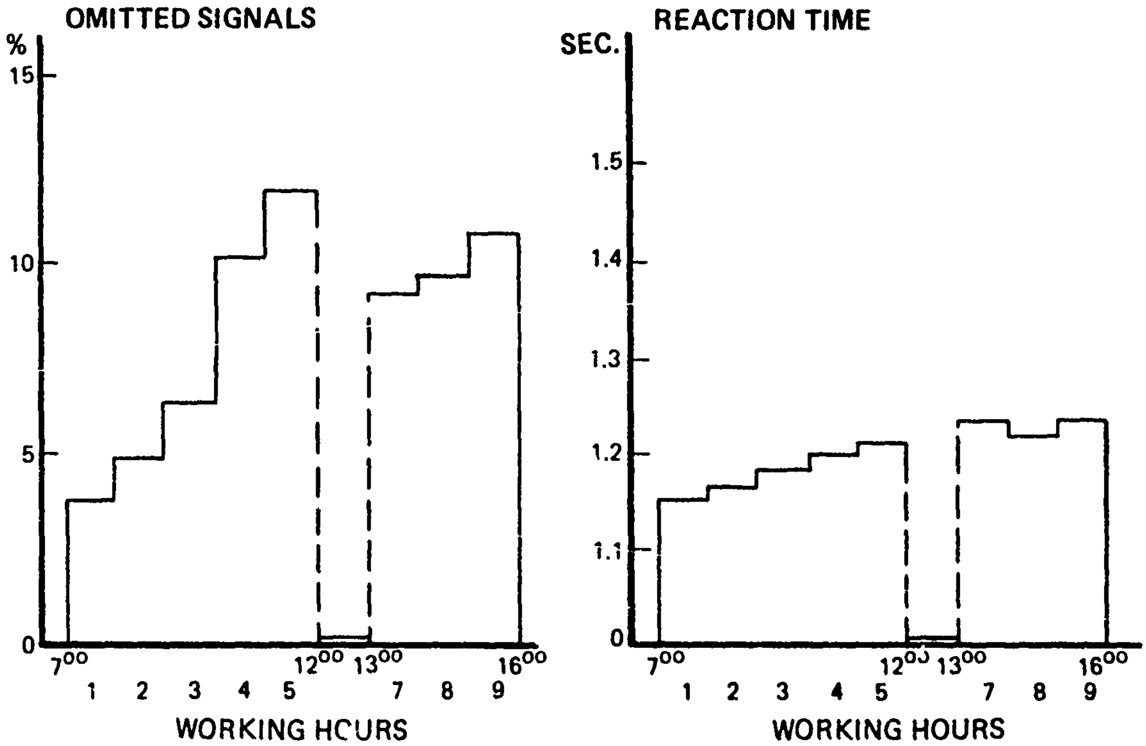


Figure 9. Vigilance of 21 female workers occupied with time paced and monotonous work (10 light signals per 40 min.). According to Haider (1963). (From Grandjean, 1968)

Prolonged Driving. A number of studies have been conducted on prolonged driving behavior, again using actual measures of driving as well as performance on subsidiary tasks.

A series of studies performed in the Netherlands is representative of this type of research and demonstrated consistent performance decrements during prolonged night driving (Riemersma et al., 1976). Twelve students were pretested on a driving battery at 8 p.m. that included measures of lane driving and variability in speed, as well as performance on two subsidiary tasks (reporting kilometers driven in multiples of 20 km, and reaction time to change in the color of a light on the dashboard). The pretest was followed by 12 hours of night driving, during which the same measures were recorded, and finally, by a repeat of the pretest. On another day, the subjects were pretested at 8 p.m., allowed to sleep, and then given the battery post-test in the morning.

The results of the driving test found changes in behavioral measures of actual driving measured by lane drifting and speed variability. Throughout the prolonged driving, lane drifting tended to increase and speed tended to become increasingly more variable. Performance on both of these variables tended to improve slightly after the break for fuel.

Figures 10 and 11 show changes in performance on the subsidiary task. In the figures, the pretest results are presented at the left for the condition in which the subjects slept between the pre- and post-tests (C_b), and for the driving condition (E_b). The results from the driving runs are presented in two pairs of five runs each, separated by a fuel stop. The post-test results (E_a and C_a) appear at the right of the figures. Percentage of incorrect reports on the kilometer reading task

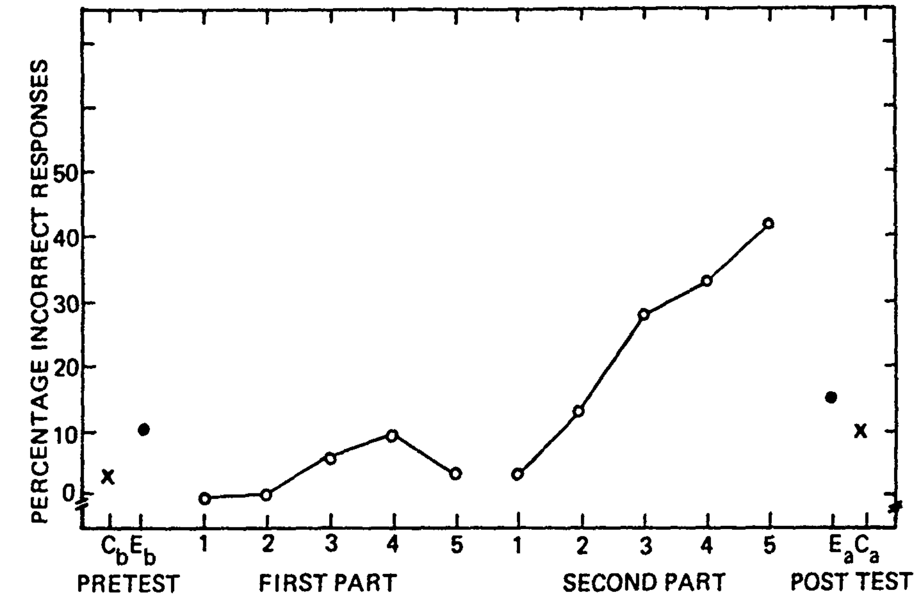


Figure 10. Percentage incorrect reports in the kilometrage task as a function of driving time. (From Riemersma et al., 1976)

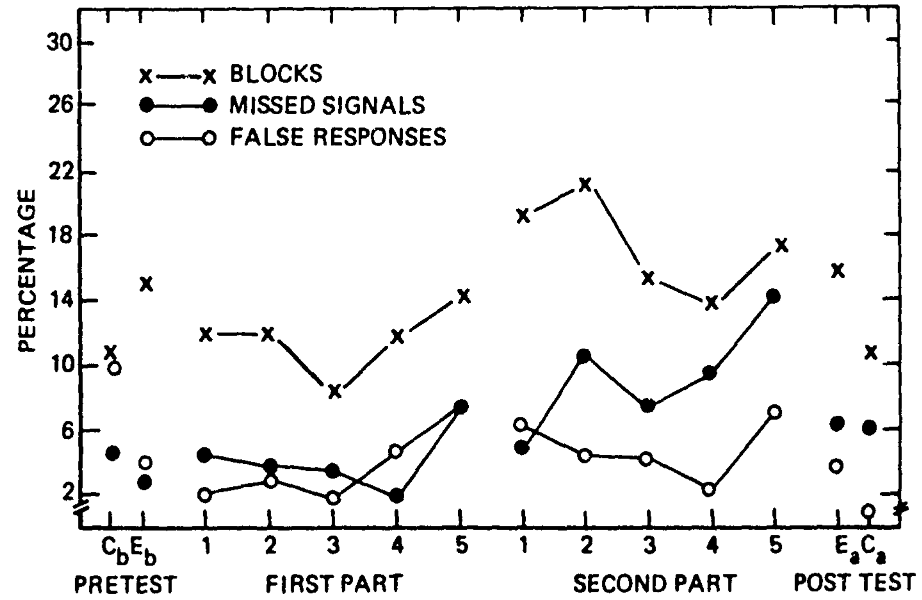


Figure 11. Percentage blocks, missed signals and false responses in reaction-time task as a function of driving time. (From Riemersma et al., 1976)

increased rather dramatically from 0 to 40% during the second half of the 12-hour night driving test (Figure 10). Performance on the vigilance task which required reaction to a change in light color on the dashboard also showed increasing decrements throughout the period of driving. Although the number of false reports tended to remain about the same, tne number of missed signals tended to increase. The number of "mental blocks" (defined as a reaction time to the light change that exceeded twice the median reaction time) increased for the second part of the 12-hour period, but appeared to have improved somewhat during the last few hours of the second driving segment (Figure 11). These authors concluded that when the effects of long periods of driving, accumulating lack of sleep, monotony, and diurnal rhythms in performance converge, several performance measures show marked and progressive impairment.

Circadian Rhythms in Performance and Night Shift Work

Laboratory studies have frequently demonstrated performance changes across the circadian cycle on a variety of tasks relevant to both control room and security guard operations. Deviations from mean performance usually average around 10%. However, Klein et al. (1977) point out that estimates of performance decrements found in laboratory studies frequently underestimate the decrements that are found in actual working situations.

On a rotating shift, the worker is exposed to circadian rhythm disruptions in which the onset of the work period is advanced or delayed by the length of the shift. Several laboratory investigations have been conducted that demonstrate the physiological and behavioral effects of this kind of circadian rhythm disruption. It is clear from these studies that individuals vary in their ability to rephase after a circadian rhythm disruption, and that during the rephasal period, some physiological parameters tend to adapt faster than others. Furthermore, it is generally true that the larger the phase shift, the longer it takes to adapt to it.

Higgins et al. (1975), at the Civil Aeromedical Institute, studied the effects of a 12-hour phase shift on physiology and performance of 15 male subjects aged 20 to 28. Circadian changes of a number of physiological variables (heart rate, body temperature, urine metabolites) were obtained for 5 baseline days before the circadian rhythm disruption. On the day of the shift, the subjects went to sleep at their normal time (2100), slept only 3 hours, and on day 6 began the new work/rest cycle in which they slept during the day (1030 to 1800) and worked at night. The subjects followed this schedule for 10 days.

Figure 12 shows the mean number of days required for rephasal for several physiological variables. Heart rate adapted to the new schedule the fastest, and other measures took as long as a week before their circadian cycle adapted to the new schedule. Higgins et al. (1975) point out that several subjects showed little or no adaptation to the new schedule, and continued to show physiological peaks at the same time of day as before the circadian rhythm disruption.

Measures of performance were obtained by the Multiple Task Performance Battery (MTPB), which covers monitoring light rates, signal presentation, arithmetic computations, and target identification skills. The MTPB was given 5 times throughout each 12-hour "day." Figure 13 shows the results from this measure. Of interest in the present context is the large decline in performance during the later hours of the 12-hour working "day" during the first 3 days after the circadian rhythm disruption.

Composite performance scores did not reach baseline levels during the 9 days of this experiment; the pattern of changes across the "day" began to resemble the baseline pattern by days 7 to 9.

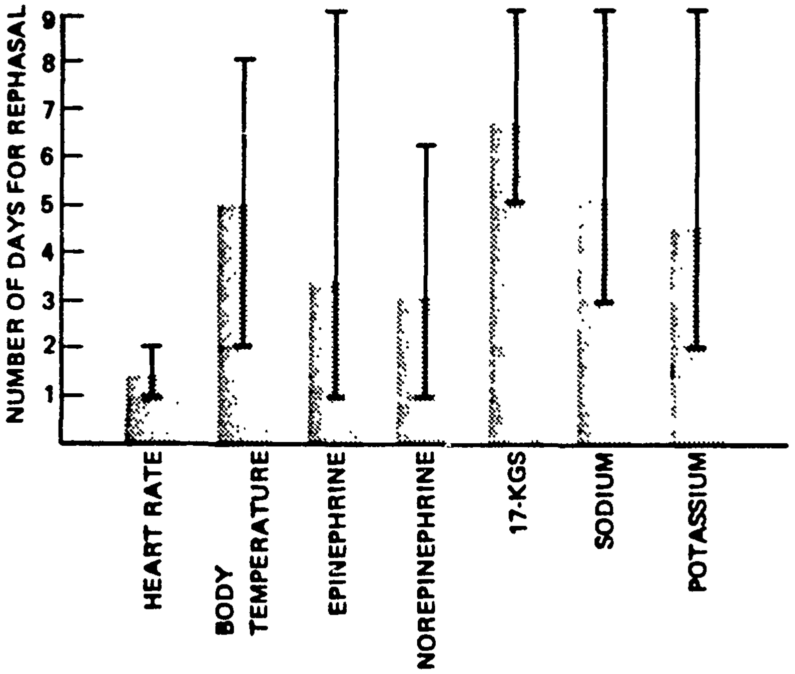


Figure 12. Average number of days to rephasal for human subjects undergoing a 12-hour phase shift. (Vertical lines represent range.) (From Higgins et al., 1975)

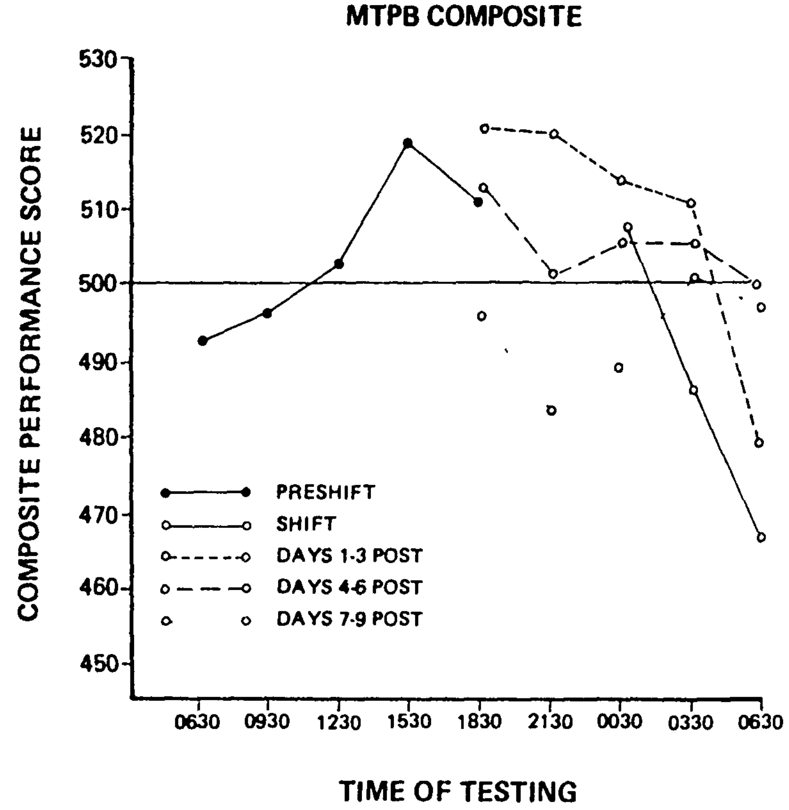


Figure 13. Multiple Task Performance Battery mean composite performance scores as a function of time of testing (n=15). (From Higgins et al., 1975)

Discussion

From the studies reviewed that are relevant to the first alternative, that of changing from an 8-hour rotating shift to a 12-hour rotating shift, it is possible to identify trends in the literature, and to speculate that longer working hours, combined with shift rotation, are likely to result in measurable performance decrements on some tasks that are relevant to the job requirements of the security guard forces. A number of scientists suggest that an individual has a limited capacity for attention, and the stressors (such as circadian rhythm disruption, monotony, fatigue, sleep loss, and unpredictable noise) tax the individual's "performance reserves" (e.g., Cohen, in press). As these stressors increase, performance on a central task may not show any decrement and subjects may be able to compensate by increased motivation, but performance on subsidiary tasks may be affected. Furthermore, performance on "automatic" behavior, such as driving skills, may not be as affected by the increase in stress, compared to performance on tasks that require some decisionmaking.

A conservative interpretation of the studies reviewed in this alternative would suggest that a change from an 8-hour rotating shift to a 12-hour rotating shift is not a particularly desirable option, and is likely to result in certain types of performance decrements and a decrease in "performance reserves." Performance on the night shift is likely to be especially affected by the combined effects of longer working hours and larger circadian rhythm disruptions. Whether these changes in performance have operational significance in the security office environment is unknown.

To counteract these effects, it may be feasible to incorporate longer breaks into the shift. Although some studies demonstrated a decrease in performance after the lunch break, most appear to suggest that prolonged performance can be maintained if breaks are provided. The findings indicate that a crew working 12 hours a day may show fewer performance decrements if duty periods are limited to 4 hours with intermittent breaks that are as long as possible. Longer breaks may also tend to counteract the tendency towards increaed sleepiness that is usually associated with night work, longer working hours, and shift rotations.

Alternative 2: Reducing the Number of Staff on Any Shift

While the literature relevant to this alternative is sparse, it appears to suggest that reductions in manning have neutral and in some cases positive effects on crew performance, depending on the circumstances and workload. Wicker (1968) defined the phenomenon of undermanning as existing in behavioral settings in which there are high manpower needs relative to supply.

In a laboratory setting, Wicker et al. (1976) investigated the effects of undermanning by studying the performance of groups of four male college students (total n = 180) who were asked to perform either two jobs on a slot car race (overmanned condition), four jobs (adequately manned), or six jobs (undermanned). Figure 14 shows that the subjects in the undermanned condition reported greater feelings of task involvement and more positive attitudes toward the task. Surprisingly, there were very little differences in performance measures among the groups in the three manning conditions, as measured by running times or number of penalties.

A study of park rangers in Yosemite (Kirmeyer, 1978) supports Wicker's prediction by finding that on days in which the rangers experienced overload stress (more contact with visitors and more feelings of being pressured and busy), they also had more feelings of being challenged, involved, and needed. However, no measurements of performance were taken.

Poulton (1979) describes the effects of work overload and work underload. He defines work overload as resulting from the irregular flow of work with characteristic peak periods of workload, having several things to do at once, and/or occasional panics. Poulton states that long-term effects of work overload can result in higher incidence of coronary heart attacks or mental illness. In defining work underload conditions, Poulton says that they may occur in the same jobs as work overload, during the periods when there is little or nothing to do. Air traffic controllers, control room operators, and security guards all experience work underload conditions. Poulton describes these jobs as "waiting for nothing to happen." The job incumbent becomes bored and inefficient, is likely to have brief lapses of attention, and during night work is more prone to falling asleep on the job.

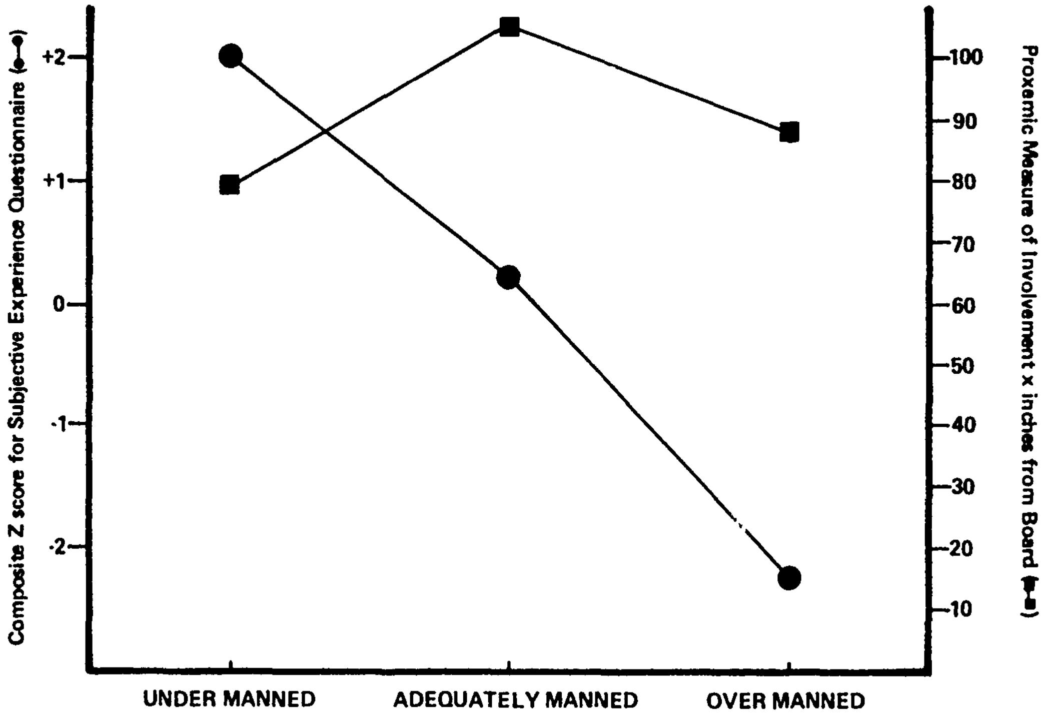


Figure 14. Subjective experience of job as a function of manning level. (From Wicker et al., 1976)

These types of problems associated with work underload seem especially applicable to the nuclear security guards, who tend to perceive their jobs as boring, burdened with high false alarm rates, lacking feedback regarding their performance, and having no career potential, as measured by a survey of security guards conducted by Hall (1981).

Discussion

No clear-cut answers can be obtained from a review of the literature regarding the effects of reduced manning on performance. With careful planning, the participation of subject matter experts, and good task analysis data, it appears to present a positive, viable alternative to the change from an 8-hour to a 12-hour rotating shift.

The question of assessing the effects of reduced manning for security guard personnel is intimately related to workload in that setting, during both normal operating conditions and under emergency conditions. It is likely that reduced manning may be a viable staffing alternative during normal operations, when workloads are comparatively low. This approach may tend to improve worker attitudes toward their jobs, and will probably have no effect on performance. However, the question of whether the increases in workload during emergency conditions exceeds the capacity of a reduced staff size is an important one, and cannot be answered in the present review. In the absence of task analyses and workload estimates during normal and emergency conditions, it is difficult to evaluate the impact of a reduction in the number of personnel. The objective is to maximize the fit between the amount of work found in these settings and the size of the work force.

Alternative 3: Reduced Qualifications of Personnel

The literature that we were able to accumulate on this topic can be broken down into the relationships between training and performance, and between experience and performance.

The effects of training on performance have a great deal to do with the relevance of the components of the training program to the task. In general, some training programs, particularly those that include a great deal of theoretical framework, include a substantial amount of material that makes the worker overqualified for some of the task requirements of the job. In contrast, exclusively job oriented training programs include little or no conceptual course content and may produce workers who are underqualified for some job requirements.

The critical importance of both conceptually oriented and job oriented training was underlined by an analysis of pilot error under high workload situations. Ricketson et al. (1973), in a report of pilot-error accidents in the Army, found that pilot experience and training were frequently cited as causal factors resulting in aircraft accidents. The errors tended to occur mostly during landing and involved faulty decisionmaking concerning the selection of the most appropriate procedures given the type of landing situation. The authors suggested that these errors may stem from information processing problems; that is, the pilots made the wrong procedure selections because they improperly assessed the flight situation. There did not appear to be a high correlation between the pilots' experience and the incidence of decisionmaking errors; two to three times as many accidents were assigned to the procedural decisionmaking variables than to the limited experience factors. It must be assumed that the information processing skills which produced these accidents are not gained through on-the-job performance.

The situation faced by security guards in nuclear facilities is analogous to the Army pilots' situation reported by Ricketson et al. (1973) in terms of the criticality of procedural decisionmaking. Hall (1981) noted that security guards at nuclear facilities experience the same sort of procedural decisionmaking problems in emergency situations, and he called for additional on-the-job training utilizing realistic exercises or simulations of different types of possible intrusions to improve the operational readiness of the security guards.

Studies of the relationship between length of experience and job performance in air traffic controllers suggest that specific experience at a particular airport is more important for maximal performance than overall air traffic control experience at a variety of airports. Rhoades and Samuel (1979) conducted a survey of the effects of the recently declining experience levels of Air Force air traffic controllers on job performance as measured by Hazardous Air Traffic Reports (HATRs) filed from January 1975 to April 1978. The authors found that controllers with 2 years or less local experience at a given airport made up 64.73% of the total air traffic controller population, but accounted for 78.43% of the HATRs. The HATRs were subdivided into "cause" and "non-cause" mishaps, depending upon whether human error by the air traffic controller was responsible. When "cause" and "non-cause" controller groups were compared, a significantly higher number of controllers having less than 24 months local experience was found in the cause factor group.

Figure 15 depicts the skewed distribution of HATRs across local experience levels. The data suggest that local experience, rather than total or facility experience, is the key to the critical differences in the performance ratings. These findings may have implications for the security office environment, which is also plagued by high turnover rates. Experience working on the specific surveillance equipment for which one is assigned, as opposed to total experience, appears to be the critical variable most likely to impact on-the-job performance.

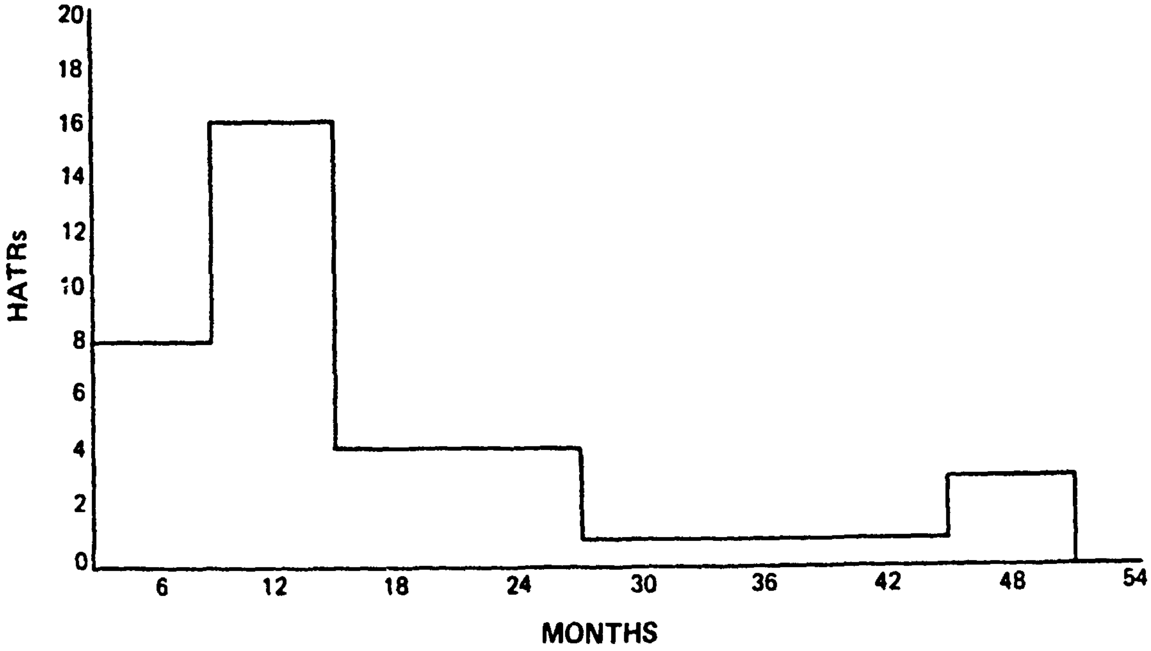


Figure 15. HATRs by local experience, categorical variables: Crew chief, VFR weather, light traffic, no trainee, no equipment failure (38 cases). (From Rhoades & Samuel, 1979)

The role experience plays in job performance during stressful conditions has been rarely investigated. Ricketson's data on pilot error (Ricketson et al., 1973) might suggest that experience per se is not a critical factor in performance under the high demand conditions of landing an aircraft. However, more relevant data on the effects of highly stressful emergency conditions on performm̀ance of experienced and inexperienced personnel have been obtained by Berkun and coworkers.

Berkun et al. (1962) examined the relationship of experience levels and performance of Army soldiers reacting to experimentally induced highly stressful situations. Three types of high stress performance conditions were assessed: (1) an artillery situation in which simulated artillery shell explosions were set off; (2) a chemical, biological, and radiological (CBR) situation in which simulated exposure to radioactive contamination took place, as indicated by an exposure to meter reading; and (3) a simulated forest fire emergency using artificial smoke to produce the emergency effects. Inexperienced recruits and experienced combat-ready soldiers were evaluated in the three types of hazardous conditions. Subjects under all conditions were given instructions to repair their field radios in order to regain communications with the command post. A Composite Performance Score (CPS) was obtained for each individual by consolidating the individual scores on five related performance measures: speed of beginning work on the radio, speed of reading a diagram and connecting wires, speed of reading instructions and completing cross-over task, and reaction time to a secondary light monitoring task.

Additional experienced and inexperienced subjects were tested during similar field operations, but they were simply told that the radio required repair in order for them to request water and rations for the future. No simulated emergencies, in the form of artillery explosions, fire, or radiation hazards, occurred during the control experiments.

In one of Berkun's reports (1964), he presents a graph depicting the crossover performance effects of the inexperienced and experienced soldiers working the radio repair tasks under unstressed conditions and the most adversive artillery situation. Figure 16 presents this performance graph. Berkun concludes that the effects of experience on job performance are a function of the operating environment in which the individuals are working. Under monotonous, routine working conditions, experience may be an impairment; however, under highly stressed conditions, experience may provide the wherewithal to sustain higher performance levels.

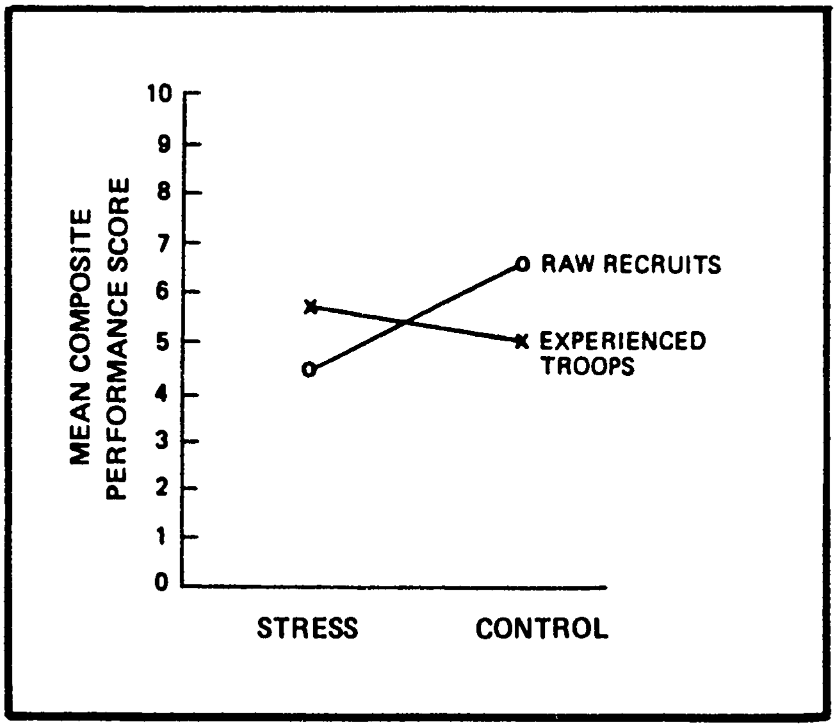


Figure 16. Mean performance scores in the "Artillery" situation. (From Berkun, 1964)

Discussion

The impact of reducing the qualifications of security guards on their performance in nuclear facilities is uncertain. The research regarding the effects of training on job performance demonstrates the need for job relevant training based on the definition of job requirements determined from job/task analysis data. The importance of the job/task analysis data cannot be overemphasized. Performance requirements on-the-job should be the foundation for identifying training requirements. Most of the research regarding the effects of experience on performance indicates that experienced personnel perform better than inexpereinced personnel when (1) their experience is obtained at the specific work site, and (2) abnormal emergency conditions are present. Applying these findings to the nuclear security guard population, there appears to be a need to improve the job relevance of current training programs. In addition, the research literature suggests that guards with local experience at specific facilities will perform better under emergency conditions. For this reason, management at nuclear facilities may be wise to address the high personnel turnover and advancement problems to encourage guards to stay with their organizations.

Conclusions and Recommendations

The present paper has summarized the findings of a literature review that examined a large number of studies relevant to the potential effects of three different staffing configurations. These findings may be applied to the nuclear security guard population, where there appears to be shortages of qualified personnel and a need to consider staffing options. The nuclear facility environment requires around-the-clock manning and the security guard's job consists of long periods of work underloading involving primarily monitoring tasks, with infrequent emergency conditions demanding maximum performance and the critical need for rapid procedural decisionmaking skills. The negative effects of rotating shift work, night work, and work underload may be exacerbated when applied to these types of work demands.

For these reasons, the third option--reduced qualifications--appears to be the least desirable. While studies on this option were sparse, they tend to indicate the importance of training in on-the-job performance. They also indicate the importance of experience to personnel who are required to perform under emergency conditions.

Given that nuclear security guard positions are generally perceived as passive, boring, and often dead-end jobs, option two--reduced manning--may prove most appropriate without strong concern for overloading the guards. However, the issue of required performance under emergency conditions remains germane. The workload of security guards appears to vary dramatically depending upon whether abnormal conditions are present. Because the fundamental role of the nuclear security guard force is to be ready to deal with surprise intrusion, some of the studies on reduced manning on tasks requiring more consistent and less critical workloads may not be analogous. In the absence of task analysis and workload data this option can only be tentatively recommended.

A change from 8-hour rotating shifts to 12-hour rotating shifts is likely to produce problems of sleep loss, fatigue, and increased circadian rhythm disruption. It may also produce marginally higher illness, occupational injury, and absenteeism rates. While the effects of these changes in performance are difficult to evaluate in terms of their operational consequences, some studies suggest that the 5 to 10% decrements found in laboratory studies of sustained performance may translate into larger decrements in the field. Despite these changes, it appears that an emergency situation is capable of increasing arousal levels and performance in fatigued subjects. It is possible that the stress of emergency conditions at a nuclear facility may counteract the influence of longer working hours and increased circadian rhythm disruptions. However, more fatigue may also produce higher error rates that can lead to potentially dangerous situations. The effects of longer working hours may be partly overrided by changes such as an increase in the length and frequency of work breaks, and an alteration in the rotation schedule.

Performance on the night shift is likely to be poorer than on days, regardless of whether the individuals are working 8-hour or 12-hour shifts. However, this performance might be improved by an alteration of the weekly rotation schedule such as Poulton (1979) suggested. This recommendation is based on results from laboratory and field investigations, demonstrating the problems arising from circadian rhythm disruptions and the need for a week or more of adaptation time after a major phase shift.

If reduced manning is not considered a viable option for security guard personnel, certainly changes in shift schedules and shift breaks to accommodate the special needs of rotating and night shift workers are called for to ensure a satisfactory level of readiness and security for the nuclear facilities.

References

Berkun, M.M. Performance decrement under psychological stress. Human Factors, 1964, 6, 21-30.

Berkun, M.M., Bialek, H.M., Kern, R.P., & Yagi, K. Experimental studies of psychological stress in man. Psychological Monographs, 1962, Whole No. 534, 76(15), 39 pp.

Cohen, S. Environmental load and the allocation of attention. To appear in A. Baum & S. Valins (Eds.), Advances in environmental research. Norwood, NJ: Lawrence Erlbaum Assoc., in press.

Colquhoun, W.P., Blake, M.J.F., & Edwards, R.S. Experimental studies of shift-work I: A comparison of 'rotating' and 'stabilized' 4-hour shift systems. Ergonomics, 1968, 11(5), 437-453.

Ellingstad, V.S., & Heimstra, N.W. Performance changes during the sustained operation of a complex psychomotor task. Ergonomics, 1970, 13(6), 693-705.

Grandjean, E. Fatigue: Its physiological and psychological significance. Ergonomics, 1968, 11(5), 427-436.

Grandjean, E.P., Wotzka, G., Schaad, R., & Gilgen, A. Fatigue and stress in air traffic controllers. Ergonomics, 1971, 14(1), 159-165.

Hall, R. Security performance measurement methodology. Proceedings of the Fourth Annual Symposium on the Role of Behavioral Science in Physical Security (NBSR 81-2207(R)). National Bureau of Standards, Washington, D.C., 1979.

Higgins, E.A., Chiles, W.D., McKenzie, J.M., Iampietro, P.F., Winget, C.M., Funkhouser, G.E., Burr, M.J., Vaughan, J.A., & Jennings, A.E. The effects of a 12-hour shift in the wake-sleep cycle on physiological and biochemical responses and on multiple task performance (FAA-AM-75-10). Prepared for U.S. Department of Transportation, Federal Aviation Administration, October 1975.

Kirmeyer, S.L. Effects of work overload and understaffing on rangers in Yosemite National Park. Unpublished Dissertation, Claremont Graduate School, 1978.

Klein, K.E., Herrmann, R., Kuklinski, P., & Wegmann, H.-M. Circadian performance rhythms: Experimental studies in air operations. In R.R. Mackie (Ed.), Vigilance. New York: Plenum Press, 1977.

Poulton, E.C. The environment at work. Springfield, IL: Charles C. Thomas, 1979.

Price, H.E., Wallace, P.M., Bauman, M.B., & Smith, M.G. Review of staffing requirements for near term operating license facilities (NUREG/CR-1764). Prepared for the Nuclear Regulator; Commission by BioTechnology, Inc., October 1980.

Rhoades, J.R., & Samuel, C.E. The effect of air traffic control experience levels on quality of service (AFIT-LSSR 26-79B). WPAFB, OH: Air Force Institute of Technology, School of Systems and Logistics, Graduate Education Division, September 1979 (Master's Thesis).

Ricketson, D.S., Johnson, S.A., Branham, L.B., & Dean, R.K. Incidence, cost and factor analysis of pilot-error accidents in U.S. Army aviation. Paper presented at the AGARD Aerospace Medical Panel Specialists meeting held at Soesterberg, Netherlands, 7 September 1973.

Riemersma, J.B.J., Sanders, A.F., Wildervanck, C., & Gaillard, A.W. Performance decrement during prolonged night driving. In Proceedings of the NATO Symposium on Vigilance II: Relationships among theory, physiological correlates and operational performance, held in St. Vincent, Italy, 3-6 August 1976.

Tasto, D.L., Colligan, M.J., Skjei, E.W., & Polly, S.J. Health consequences of shift work (NIOSH-78-154). Prepared for the National Institute for Occupational Safety and Health by SRI International, March 1978.

Wicker, A.W. Undermanning, performances, and students' subjective experience in behavior settings of large and small high schools. Journal of Personality and Social Psychology, 1968, 10(3), 255-261.

Wicker, A.W., Kirmeyer, S.L., Hanson, L., & Alexander, D. Effects of manning levels of subjective experience, performance, and verbal interaction in groups. Organizational Behavior and Human Performance, 1976, 17, 251-274.

PROBLEMS IN GUARD FORCE TRAINING

Dr. Robert Pulliam

BioTechnology, Inc.

Problems in Guard Force Training

Dr. Robert Pulliam
BioTechnology, Inc.

Abstract. Basic problems in guard force effectiveness could be solved by training, but only within a basically revised guard force doctrine. Present approaches are weakened by circumstances which include the tactical vulnerability of a fixed procedure approach. Modern control systems could enable development of procedures that enforce activity and attention, and that vary the guard routine unpredictably. Simulation of incidents could ensure the perception of a credible daily threat. Reaction forces could be trained for a flexible response, and made effective by engagement simulation exercises.

This paper is not directly about training. In fact, the thesis is that training will not solve the most important guard force problems which it tries to address. These problems can be solved only by changes in the security system, and will require basic changes in doctrine. A key issue is proceduralization; it must be recognized that highly procedural routines can be psychologically counterproductive, and are tactically vulnerable to defeat.

Training can contribute to substantially more effective nuclear security, but only as part of a basic security system redesign. Otherwise, it can in fact create a dangerous confidence. Training can develop a force that looks good, knows the right answers, and follows procedures reliably, but is essentially unsafe. It can give commanders a false sense of security. We should look instead to "systems" answers, in which better methods, system design, and training interact to provide security which is genuine and dependable.

Human Reliability

First of all, training cannot make people reliable or vigilant.[1] Most managers understand this, and yet a large portion of guard force training is meant to teach guards to be vigilant, or thorough, or careful. We know that this will not work from practical experience, and from our knowledge of the psychological causes of surveillance error.[2] We also know it from the history of safety research.[3] For the most part, we have not been able to teach workers to be safe. But several of the techniques that do work for industrial safety will also increase the reliability of a security guard. These techniques include personnel selection,

[1] Fechter correctly observes that vigilance as it applies here has a different meaning from that term as it is usually applied in the human engineering literature (Fechter, J. Status report on the NBS vigilance research project. In G. Lapinsky and A. Ramey-Smith (Eds.), *The role of behavioral science in physical security*. Proceedings of the Fourth Annual Symposium, July 25-26, 1979. Washington, D.C.: National Bureau of Standards and Defense Nuclear Agency, 1981.) Vigilance in the sense of signal detection while attending to an information display is in some respects responsive to training, but the maintenance of attention across time is not.

[2] Vigilance and its absence are a consequence of the interaction of situational factors such as lack of variation in the task environment and basic biological factors that are not modifiable by training, as training is normally conceived. See: Broadbent, D. A mechanical model for human attention and immediate memory. *Psychological Review*, 1957, *64*, 205-215; and Bergram, B., & Lehr, D. Vigilance performance as a function of task and environmental variables. HumRRO, Ft. Bliss Research Unit, Ft. Bliss, Texas, 1962.

[3] For example, a massive public education program to promote seat belt use has not importantly affected public behavior. See Knoblauch, S. (Ed.). *Attention and performance, Vol. IV*. New York: Academic Press, 1973.

Note also the effect of media safety campaigns: Haskins, J. Effects of safety communication campaigns: A review of the research evidence. *Journal of Safety Research*, 1969, *1*(2), 59-65.

proceduralized positive activity, interest enhancement, and the enforcement of perceptual survey behavior. We will discuss these in turn:[1]

Personnel Selection. Effective vigilance, and most other reliability variables, are a function of the work setting and of individual neurophysiological differences.[2,3] For these characteristics there is wide variance among individuals, but little variance within an individual over time. These characteristics cannot be modified by training, and are not strongly affected by motivation. The only way to secure a reliable force is to choose reliable people.

Vigilance is also affected by the work setting--the facilities and procedures. Having selected people for reliability, we should proceed on the assumption that they will, nevertheless, prove

[1] The reliability of a guard force and its supported system in detecting intrusion conforms in general to the four event/ response model of signal detection theory (Green, D., & Swet, J. *Signal detection theory and psychophysics*. New York: Wiley and Co., 1966). Across any time interval an intrusion may or may not be attempted; in either case the evidence is masked by informational noise. The four possibilities are: (1) No intrusion occurs and no alarm occurs--the "normal" condition. (2) An intrusion occurs, and is detected--the "hit" condition. (3) An intrusion occurs, and is not detected--the "false dismissal" condition. (4) Finally, no intrusion occurs, but an alarm occurs anyway--the "false report" condition. Our objective is to minimize the error cases (3) and (4). The conditions which affect this have been defined in the signal detection research literature. Detection of a target event is unlikely to occur, for instance, if the observer does not really believe an event will occur.

[2] Ware, J., et al. Auditory vigilance in repeated sessions. *Perceptions and Motor Skills*, 1961, *13*, 127-129.

[3] Poulton, E., et al. Effect of cold and rain upon the vigilance of lookouts. *Ergonomics*, 1965, *8*, 163-168.

unreliable. The conventional guard setting and procedure is one that breeds unreliability because of boredom,[1] inactivity, and lack of moment-to-moment reinforcement. We should design a work procedure which enforces reliability and compensates for human failure. Here are some things that will help:

Provide Positive Activity. The security system should keep guards active. Guards should be provided with a steady, but not distracting, sequence of tasks. This combats boredom and inattention, and prevents unauthorized departures from procedure. If possible, choose tasks which accomplish necessary work; they need not be part of the security mission if they are properly chosen. When suitable, necessary tasks do not exist, provide structured and controlled guard force activity. Begin with communications and reporting, which are natural tasks. The guard routine should enforce frequent scheduled and randomly occurring occasions for communicating with other guards, and there should be plenty of reporting checks, inspections, and incident reports. Guards should be encouraged (and required) to report every trivial event or abnormality which occurs within their observation. So that there will be a minimum of writing, most reporting should be by verbal comments and recorded through the communications system. If additional tasks are still needed, insert artificial, pro forma tasks.

Obviously the selected tasks should be heads-up actions that are quickly accomplished, and which enhance or do not interfere with attention to the surroundings. The goal is to keep each guard reasonably busy and alert. It is important to maintain a

[1] Hall reports that 81% of guards with 2 or 3 years experience found their work boring. (Hall, R. Security performance measurement methodology. In Lapinsky and Ramey-Smith, op. cit.)

psychological pace that does not permit inattention on the one hand, and does not overload short-term memory or attention on the other.

Enhance Interest. Clearly, we should do anything possible to make the job and the job setting interesting (but not distracting). A well-structured task sequence will help a great deal. In addition, the guard routine should be under the control of a procedure which deliberately varies in unexpected ways. Modern control systems make this easier to do. Guard posts should rotate unexpectedly; patrol routes should change; the required checks and inspections should change in their sequence and rhythm.

So that the schedule will be truly random and unpredictable, Monte Carlo effects should be introduced by the control system to provide psychological variety. This will also make it more difficult for a subverted guard to manipulate the security system. An even more compelling reason for varying the routine is to reduce its vulnerability to an external threat, as will be explained later.

Enforce Survey and Analysis Behavior. To the extent possible, tasks should be provided which force each guard to make an active survey of his surroundings, and an active analysis of what he observes. Guard checks and reports should avoid an "everything normal" content. If nothing else, they should require an observed time and a changing location authenticator code. For instance, a security system could provide and display a random 3-digit authenticator code which is unique for each time and location. Occasionally something to report should be deliberately introduced, and the guard who fails to note that abnormality should be reprimanded.

Credibility of a Threat

The problems of human reliability and vigilance are compounded by a second major problem:[1] No guard really believes there is a serious threat at any particular moment.[2] Training does not change that belief. Guards, in general, accept the proposition that a threat exists. They will believe that some sites may be penetrated, that spies and saboteurs exist, and even that some day someone might try to steal nuclear material from their own facility. But no guard really believes that anyone is going to threaten his post on his particular shift.

Training, especially continuation training, may heighten the awareness of a threat to some degree. But here again the problem is one of human variance. Some guards will never believe in a here-and-now threat, no matter how they are educated, threatened, or harangued. Others will respond by becoming overzealous.

The specific fix is to create a simulated threat, as is indeed often done. Every guard force should frequently experience threat gaming--a simulated penetration, a simulated security violation (from the inside), or a simulated intelligence probe. This can be backed by even more frequent plants of ordinary situational anomalies--something moved, something missing, or something not working normally. Here the requirement is that the anomaly be detected and reported.

[1] See Kohneman, D., & Tversky, A. On the psychology of prediction. *Psychological Review*, 1973, *80*, 237-251.

[2] Tversky, A., & Kohneman, D. Judgment under uncertainty: Heuristics and biases. *Science*, 1974, *185*, 1124-1131.

Problems of the Emergency Force

Special training requirements apply for the emergency reserve or reaction force. Conventionally, emergency force training has two principal components: procedures and small unit combat. The procedure component teaches how to deploy, communicate, respond to specific penetrations, establish a perimeter, control crowds and traffic, interact with civil authority, and so forth. The limited amount of combat training includes small arms firing, squad maneuvers, and perhaps running a combat course. This training leaves the guard force vulnerable to failure for several reasons:

(a) Any established procedure is defeatable.

(b) The combat training is unrealistic--it does not exercise all required behaviors, it does not reflect the real probable scenarios, and it cannot be validated.

(c) Training emphasizes individual rather than team behaviors, and classroom lecture rather than training in the field.

(d) The guard force does not really believe it will be employed, except in pro forma deployments (as was observed before).

Most of these defects are not within the resources of the average post commander to correct, but would require development at the DOD or Service Department level. Two actions are suggested: First, break up fixed procedural patterns, and second, provide more realistic combat training.

Break Procedural Patterns. Game theory[1] makes it clear that any fixed strategy is a losing strategy. Therefore, the first

[1] Von Neumann, J., & Rosenstern, O. *Theory of games and economic behavior*. Princeton, N.J.: Princeton University Press, 1947.

action suggested is to change guard force doctrine so that the guard force does not react in a highly procedural way. If a guard force responds (as it normally does now) in a stereotyped manner, the response is fully predictable by an adversary. It is reactive to the threat, and can be controlled or evaded by the threatening force. A safer procedure would be to train all but the senior leaders in a set of modular team behaviors, which can be combined to produce any needed response scenario, just as we train tank crews. Responsiveness to command becomes the central training objective, and the force can respond flexibly. The tactics which will actually be used in an emergency are kept confidential, and the plans are opened only when an emergency occurs. Training scenarios are varied and do not follow the exact sequence of the emergency plans.

No single post or facility commander has the time or resources to develop a non-procedural guard force methodology. Doing so is therefore an appropriate task for the Service Departments or for DNA.

Provide Realistic Training. The second action suggested to improve the emergency reaction force is to provide enabling materials for more realistic combat training. Recent Army developments in combat simulation point the way.

An initial condition is the availability of a valid task analytic base. Data are required which specify what expected threats are to be countered, and what action scenarios will result. These must then be analyzed to determine the critical team behaviors which are are required to succeed in the security mission.

An advanced training program will probably include elements of the small-unit training simulations of the SCOPES-REALTRAIN-MILES development sequence. SCOPES is a squad-level combat game, played by two opposing teams in real time, on the ground. Individual soldiers maneuver against each other, using their personal weapons or calling for supporting fire to win or lose an engagement. Weapons effects are simulated by blank small arms fire and artillery simulator charges. There is a scoring system that identifies individual casualties and takes them out of the game. REALTRAIN develops the SCOPES approach, introducing different weapons and combined arms engagements.[1] MILES will provide a better system for determining casualties, using a low-energy laser to identify hits.[2] These techniques make it feasible to practice a much more realistic simulation of combat, in which the outcome actually depends on the skills and actions of individual soldiers.

Simulations are desirable which fit the special conditions under which an emergency guard may be employed. They should include worst-case scenarios, interior deployments, and military operations on urban terrain (MOUT).[3] Ideally there should be a specially trained opposition force (OPFOR) which makes attempted

[1] Banks, J.H., Jr., et al. REALTRAIN validation for rifle squads: Mission accomplishment (ARI Research Report 1192). Army Research Institute for the Behavioral and Social Sciences, Arlington, Virginia, October 1977. See also research by USAF/TAC, not yet reported, which tested REALTRAIN concepts in defense of a missile installation. Contact is LTC Kane at HQ TAC, Langley AFB, Virginia.

[2] Xerox Corporation. Brochure entitled "MILES," 1969.

[3] Sullivan, B. MOUT training: A combat service support need. *Military Review*, LX:9, September 1980.

penetrations, or against which guard forces can be exercised at a central training center. OPFOR training can be used analytically to validate training methods, test doctrine or tactics, and analyze defensive scenarios.[1]

At least two indoor small arms fire simulators are under development.[2] Like other high fidelity training, they will require investment in development, capital costs, system operation, and trainee time. Which techniques are worth buying, and at what level of investment, is an open question. Therefore, it would be reasonable to compare the whole set of high technology options against the threat, using cost and training effectiveness analysis (CTEA)[3] methods. The product would be a recommended, balanced, long-range training development program.

Vulnerability

Finally, it is important to understand the basic vulnerability of a guard force. It must be understood that any established procedures can be defeated. Any security system can be penetrated if it can be analyzed and understood, and its responses can be predicted. This means that security against an active, intelligent adversary can be provided only if the system is itself active and, to a degree, unpredictable.

[1] Thompson, E. OPFOR today. *Military Intelligence*, 6:3, July-September, 1980.

[2] Two related contract developments have been announced in the news media. One is Army sponsored and administered by the Naval Training Device R&D Center at Orlando AFB, Florida. The other is USMC sponsored and designed for use on shipboard.

[3] TRADOC Pamphlet 71-10, Cost and training effectiveness analysis, 1977.

A guard force is by its nature defensive and an easy inte‸. gence target. The adversary has the initiative; he has secrecy; he has plenty of time to collect information and to plan; he has an unlimited range of options. So a great danger lies in relying on any fixed security system, no matter how good or sophisticated. Unfortunately, the direction of development has been toward a more rigid proceduralization of guard operations, plans, and training. That proceduralization creates a specific vulnerability. The single greatest improvement that training (or systems design) can provide is to develop guard procedures that cannot be predicted by an adversary, or by a subverted member of the security force.

Conclusion

Training alone will not solve the basic problems of security. These include assuring vigilance, providing the perception of an active threat, and assuring effective tactics against an adversary. There are fundamental psychological and tactical reasons why this is so.

Training could be highly effective, however, within a redesigned security system, if that system recognizes the basic vulnerability of the proceduralized approach. New systems should provide deliberately structured, random activity under automatic control. A properly paced, randomly controlled activity schedule can enforce alertness and an appropriate focus of attention. It will prevent an adversary from predicting the system, and make it difficult for a subverted guard to compromise the system. A redesigned system should provide each guard an assurance of something to observe, respond to, and report, including frequent simulated penetrations. For the reaction force, it should provide a flexible response scenario and realistic training based on engagement simulation.

DOD GUARD TACTICS SIMULATION
A "FREE-PLAY" ROLE-PLAYING METHODOLOGY
FOR SECURITY TRAINING

Donald R. Richards

Booz, Allen & Hamilton, Inc.

DOD GUARD TACTICS SIMULATION
A "FREE-PLAY" ROLE-PLAYING METHODOLOGY
FOR SECURITY TRAINING

Donald R. Richards

Booz, Allen & Hamilton, Inc.

INTRODUCTION

Motivation and training of security guards are extremely difficult tasks, especially after personnel have been on the job a few months. The inherent boredom and tedium of the job tends to dull the thinking and responses of the guard. Interviews with site security guards indicate that few guards view as credible an adversary attempt to remove or disable a nuclear weapon held at a storage site. The guards have not been exposed to incidents of this type during the time they have been at the site. They have never heard of such an incident occurring anywhere. They may also be aware of certain official threat analyses which question the likelihood of such threats to nuclear weapons.

When such attitudes are combined with the tedium and boredom experienced on security duty, concerns increase as to the guards' overall ability to deal with such a threat, should it occur. Security drills and training notwithstanding, bored guards, who believe that such events are highly improbable, are unlikely to think about how they would or should respond to various threats, or about site-specific vulnerabilities. Some guards may even contend that if adversaries attacked the site, they would easily succeed in their mission regardless of guard force response.

Every effective technique possible must be developed and utilized to improve guard attitudes toward their overall responsibilities and their chances of success in any encounter. Realistic and thorough initial training is important. Effective on-site training is vital in preparing for actual site defense. On-the-ground training has direct application to the mission but must be limited because of interference with actual security. It is not easy to present classroom training which is interesting and directly applicable to the mission. The DOD Guard Tactics Simulation (board game) fills some training and motivation gaps.

THE BOARD GAME

The board game is a free-play, role-playing methodology for security training. An adaptation of a concept originated by the Nuclear Regulatory Commission, the game will be utilized to stimulate guard thinking, initiative and innovation. Response force personnel on standby alert can play the game in the security control center building. Three personnel are needed. One plays the guard role, another the adversary, and the third acts as referee, applying minimal rules and guidelines to keep the play realistic and settle disputes. As in real life, adversary actions will produce guard force responses and vice versa. The free play scenario is played through until the adversaries win by escaping with a weapon or the guards win by neutralizing the adversaries before they can escape.

Materials utilized in the simulation are simple, durable and easy to use. Game boards are 30" by 30" and are separated by a divider so each player can see only his board (see Photo 1). Hinges, closures, and a handle are attached so the boards form a unit that can be closed, moved and stored easily. Colored felt cutouts and string are laid out on the boards identically and to exact scale to depict the specific site desired. All features of the site, including roads, buildings, fences, alarms, lighted areas and terrain can be easily and accurately represented. The board/site layout is covered with a plexiglas playing surface, overlaid (on the bottom side) with a hexagonal grid. A game board representing an example site can be seen in Photo 2.

Colored plastic 1/2" cubes represent individual guards and adversaries. A protrusion (interlocking device) on one side of the cube designates the direction the individual is facing. All individuals have a 180 degree field of vision. Photo 3 shows a tower guard (light piece) and an adversary who has come out of the woods approaching the fence at the base of the tower (darker piece).

One of the primary benefits of the board game is its applicability directly to the site where it is in use. For this reason, accuracy in the scale of the site map and in its layout are very important. Also vital to the effectiveness of this training tool are the allowable actions and freedom of play. Adversaries must be allowed to take any action possible in real life and the guards any action allowable under their real orders and procedures.

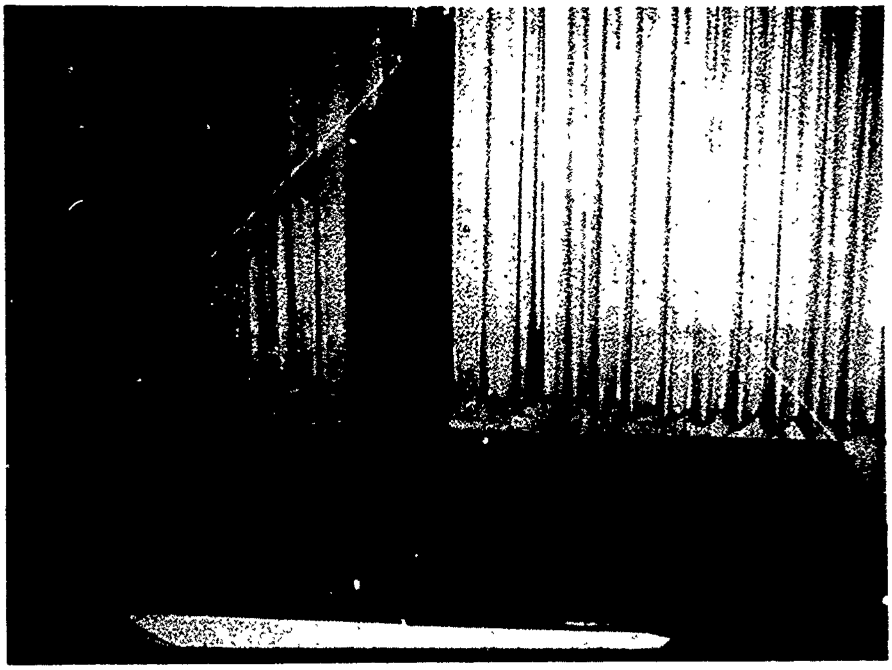


Photo 1

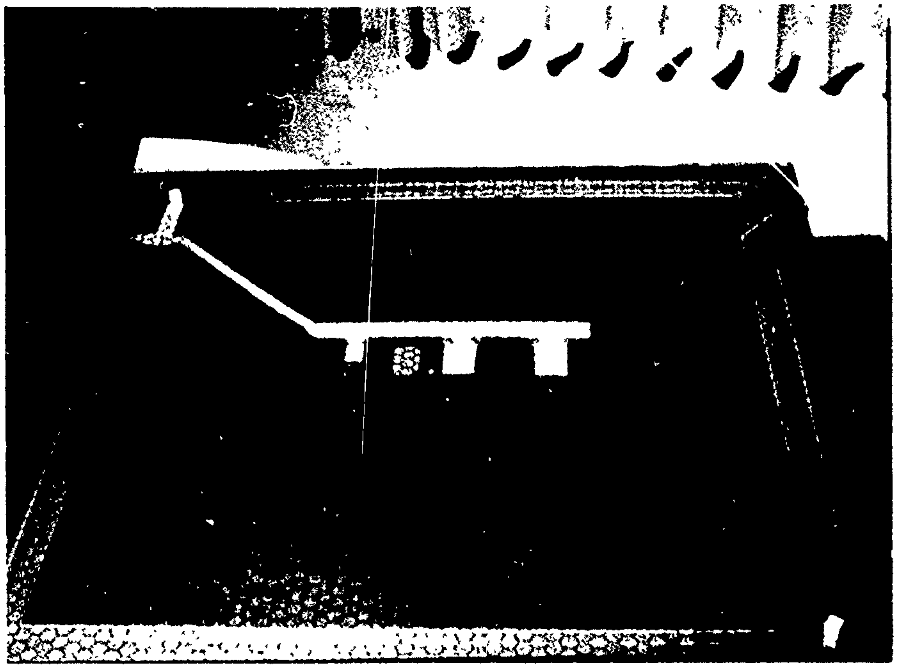


Photo 2

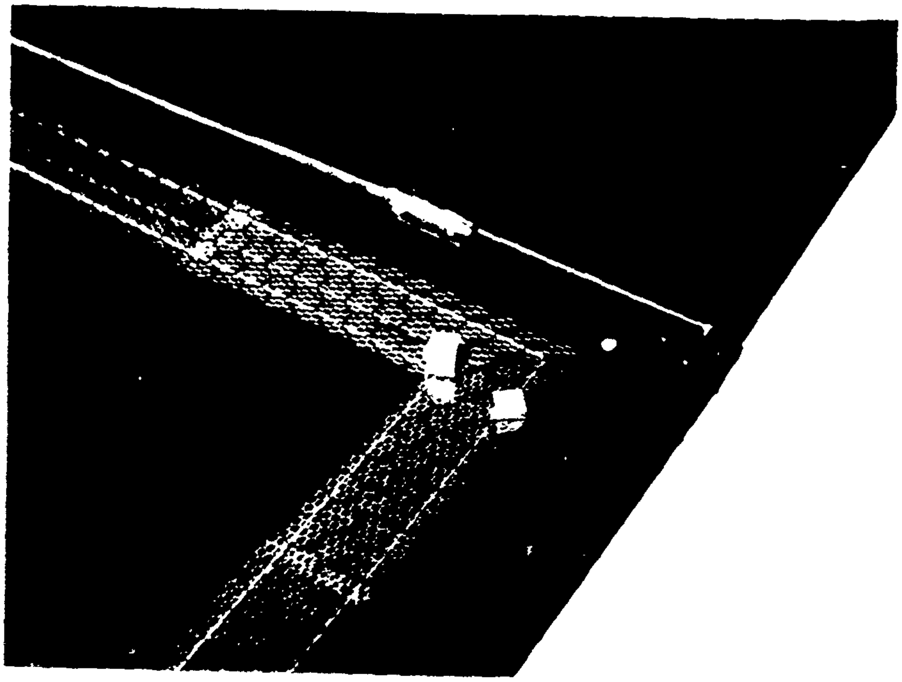


Photo 3

GAME PLAY

Once roles have been selected, the guard player leaves the room. The adversary player selects the month, day, time, weather conditions and strategy for his attack and discusses them with the referee. He then prepares his equipment lists, assigning specific weapons and equipment (explosives etc.) for each playing piece he will use. (He has six colors and up to 12 playing pieces.) The guard player returns and is informed of the month, day, time and weather by the referee. He then prepares his equipment lists (up to four colors and the actual number of guards on a shift) and places guard pieces on his board as they would actually be positioned under the conditions identified. The adversary player positions his pieces on his board as they would be, prior to the attack. The referee is given a copy of each equipment list.

After checking the equipment lists for realism, the referee checks the boards for player limits. He then places on the adversary board guard pieces for any guards who would be visible from off the site. If any adversary pieces were visible to guard pieces, the referee would put them on the guard board; however this is not likely, prior to the attack. The referee must take care to place pieces on the opponent's board exactly as the player has them on his board, so the pieces will "see" and not see the same portions of both boards and so the ranges will be the same. Guard pieces placed on the adversary board will all be of one color, as will adversary pieces on the guard board, unless there is some special situation which would realistically cause one individual to stand out from his colleagues.

The adversary player moves first and has 30 seconds to move and position his pieces. The 30 seconds represents 10 seconds of real time. At the end of the 30 seconds the referee stops further movement and, if necessary, checks to ensure that the distance moved is commensurate with the mode, i.e., crawl 15' but not 100'. When the referee is satisfied (he should work with all possible speed, in order to keep the game moving and keep stress on the players) he starts the 30 second clock for the guard player. The guard makes any moves he chooses, representing 10 seconds of real time. After making sure that the moves are realistic, the referee identifies any move that was visible to adversaries, and adjusts guard pieces on the adversary board accordingly.

If an adversary piece makes contact with an alarm system, in view of a guard, his position is confirmed and an adversary playing piece placed on the guard board. For the rest of the game, the position of this adversary is known to the guards and the referee will move the piece on the guard board each time the adversary player moves the corresponding piece on his board.

When the adversary player informs the referee (by signal or note) that one of his pieces has initiated a barrier penetration, that piece will be delayed an appropriate period of time, depending on the barrier and the penetration mode. When armed combat occurs, the referee will verify line of sight to the target and determine the range, utilizing the measuring ruler provided. Then, referring to the proper weapon/light condition combat table in his rule book and the correct range line for the hit/miss probability parameters, he throws the die to determine the hit or miss by the shooter. "Disabled" player pieces will be placed "face up" (protrusion VP) on the board to show that they can not move.

The free-play action-reaction format of the game causes the players to think about and learn what works and what does not work in attacking/defending the site. For example, a guard who has a playing piece shot from behind while firing around the side of an igloo, will remember in future games, and in real life, to get in the prone position to provide defensive fire. The guard will remember which attack tactics worked the best and be more alert to those scenarios. He can also be expected to be more aware of effective guard tactics and to apply them, should the occasion arise. The competitive spirit and playing both game roles should encourage innovative thinking and perhaps, raise the recognition of site-specific vulnerabilities. Because the site layout is easy to modify, the game will also be useful in evaluating the effects of possible changes in site layout as well as changes in guard procedures.

SUMMARY

This brief word description of the board game provides some understanding of the game materials and how they are used. Full understanding of the game and its unique interactions can only come from playing the game or seeing it demonstrated. The game is available at DNA, for demonstration. Game benefits are threefold. It motivates the players to think about their site and their job, both from the guard and adversary viewpoint. It causes the players to remember what actions were effective in protecting their lives, the site and the weapons. It is useful in evaluating site security and potential changes in the security program. Enhanced versions of the game will also be tested. These include use of a hand calculator to generate random numbers and determine hits and misses under the various combat conditions and the use of an earphone communications system to speed the game and increase realism in communications.

UNCONVENTIONAL THREAT ASSESSMENT

James L. Stinson

CACI, INC.-FEDERAL

UNCONVENTIONAL THREAT ASSESSMENT

INTRODUCTION

Over the past ten years the use of terrorism has increased throughout the world. The "problem" while growing in scope and intensity, has tactically diffused so widely that virtually all nations have been affected.

On the international scene the United States has been particularly hard hit, with Americans being on the top of the victims list for some time. Our U.S. Ambassadors have been held hostage and assassinated world wide. Our military facilities have been assaulted and our personnel murdered in the streets of foreign nations. Our civilians have been subjected to the most ruthless forms of terrorist assault. Most recently in the news has been the terrorist hostage situation in Iran and the general situation in the Middle East. These "situations" are not the exception but the rule. During the past decade, the United States and its interests have been targeted in over forty percent of all the international terrorist incidents.

Many nations have not waited for the figure to reach such an astounding level and have delegated special governmental responses teams to handle such situations. Several of these units brought the dramatic rescues at Entebbe and Mogadishu, both of which evidence the high governmental concern that international terrorism has engendered in recent years.

A Portrait of Complexity

The thrust of the first part of this presentation is to demonstrate that terrorism is amenable to systematic analysis. In doing so, it defeats the common wisdom assumption that terrorism is mystical and unmanageable by highlighting both the complexity of the problem and the types of patterns that emerge from a careful analysis of the phenomenon. The second part suggests that the best way to look at terrorism is to get away from the traditional focus on terrorist incidents, and begin analyzing the activities of the terrorist groups that perpetrate them. It then moves to a discussion of an organizational structure that can enhance investigations and make the most of the data that are collected during the investigative process. The presentation concludes with a discussion of how the investigative approaches and tools can be utilized in developing accurate and effective assessments of future terrorist threats.

This paper and the research conducted by the author presume and accept the fact that terrorism in a variety of forms is present within the United States and is growing, and that international terrorism is slowly but surely being delivered to our doorstep. It acknowledges that although much of the problem could best be handled at the national level, the organizations with charter have been curtailed in recent years resulting in an increased threat without adequate response. This leaves the response to the local and state authorities.

Terrorist targeting of U.S. interests is a fact in today's world. An extrapolation of present trends suggests that this process will not only continue, but could have extremely dire future consequences. Officials responsible for responding to terrorism express concern over future terrorist threats such as the Olympic games to be held in the United States in 1984, or the possible acquisition of nuclear materials and the fear that terrorists may obtain other mass destruction technologies such as biological and chemical warfare technologies.

The need for analytic support has developed from several areas, foremost of which has been the increase of terrorist activity both within the United States and against its citizens throughout the world. Recent CIA figures cite that the majority of victims of terrorist attacks worldwide

(40%) are U.S. The second fact demanding increased analytic support is the growing complexity of terrorist actions. Protection against terrorist attack has expanded into a billion dollar industry and although concerns are warranted, it also represents considerable overkill. The problem can be focused. Third in concern for development of support techniques has been the sensitivity of the investigative process. Accepting that the terrorist is a 'political criminal', the investigator walks a very sensitive line fraught with legal roadblocks. Successful investigations require the balancing of the individual rights of suspects against the need to protect key persons and facilities. This is not an easy task. Adding to the complexity is the long range and fragmented aspect of the investigation.

Very few cases have been successfully tried against terrorist group members. Most Weather Underground Organization members wanted in the early 1970's and currently "inverting" are receiving probation and shortened sentences. Five members of the Revolutionary Comittee in Los Angeles, California who plotted to assassinate a state senator and judge were never convicted of these offenses even though the FBI had infiltrated the group. Local authorities prosecuted them on illegal possession of explosives and other lesser offenses. Four of the 5 have served their sentences, and were released in November of 1979 to go back underground. More have since surfaced, taking the same path.

The international scene is even more complex. Mixing international intrigue with revolutionary violence, it has become fashionable to 'pick up the gun' for any of several hundred terrorist causes. The international scene is even more lacking in enforcement codes. In a study of Black September and the 135 actions they attempted, the group was found to be tactically successful 90.3 percent of the time. Even more alarming, while over 111 members were identified and 98 were apprehended at or near the scene of their terrorism crimes, 78 were released by the arresting governments. Releases were precipitated either by BSO reprisals or fear of such threats. Thirteen others were killed or apprehended in

West Germany at the Munich Olympics as^^ult and one even turned up in Fountain Valley, California, attempting to extort money from a businessman in a nearby city. Although the suspect machine gunned a small child and wounded many others in an Athens Airport attack, he too had been freed after other BSO comrades hijacked a plane effecting his release. In the terrorist world, repeat offenders are more commonplace than not. Being a terrorist is not necessarily a risky business, nor is it any kind of mystical entity as many have stated.

The complexity of the above problem is expressed through the terrorist organization and its objectives. This is best represented by its:

- o Cell structure,
- o Use of cut outs and dead drops,
- o Personal security measures,
- o Extensive use of false I.D., and
- o Increased use of multi-jurisdictional actions.

It creates an investigation that is quite 'hazy' and often beyond recognition until well established.

BACKGROUND

Although much has been written on what terrorism is, it still maintains a "mystical" aura and is often viewed as random activity ill suited to traditional forms of investigation and analysis techniques. This should not be the case. Research conducted by the author over the past five years holds that terrorism is simply purposive and directed activity carried out by clandestine political groups, amenable to systematic analysis.

Terrorism as a Unique Form of Crises

Research conducted on international terrorist incidents from 1946 to 1980 identified several unique characteristics of terrorism incidents as contrasted with "crisis" events of a conventional nature.

- o Terrorist crises are of very short duration.
- o The precrisis activities of authorities tends to be routine rather than at alert or prealert stages.
- o Relatively little warning, if any, is discerned prior to terrorist actions.
- o The threat in terrorist crises develops much faster than in other crises.

In addition, the distinctive character of terrorism was suggested by the experiences of U.S. and allied governments in responding to terrorist incidents:

- o Terrorists operate covertly but within civilian populations, making conventional investigative responses difficult and sensitive,
- o Terrorist organizations are fundamentally non-governmental bodies, not susceptible to most normal, political, economic, or investigative efforts,
- o Communications and response channels between governments and terrorists are unconventional (e.g., on the scene negotiators, victim or media), and
- o Responses to terrorism require interdepartmental multidisciplinary support, (e.g., intelligence, linguistics, logistics, psychology, and unconventional warfare forces) to deal with the problem.

Terrorism as Stylistic Behavior

Several developments in recent research efforts in this field have caused a substantial modification in the approach that terrorism research takes. Most of the research efforts to date have concentrated on incident oriented data collections and comparisons across incidents. The author's research findings indicate that this approach forces investigators into a reactive mode of operation. Research results suggest that governments will never be able to prevent or deter attacks if analytical expertise remains at the level of merely studying incidents after the fact. In fact, the only approach that allows for aggressive research aimed at early detection, interdiction, and prevention is that which focuses on the group. It is at this level that research begins to show the stylistic and patterned forms that the behavior takes. For example, patterns show up in the following categories:

- Target selection,
- Tactics, operational and strategic,
- Training methods,
- Weapons selection, acquisition and use,
- Joint operations,
- Name date use, and
- Incident contagion between and among groups.

These patterns are subject to systematic analysis. Research and collection efforts can be successfully directed toward the management and prevention of terrorist-induced crises, and a crisis management aid specifically designed to deal with terrorism can produce important benefits to the analytical team.

For example, one pattern emerging across incidents is the size of the operating teams different groups use. It appears that the size of the team will be dictated by the type of operation being undertaken and the "intelligence assessment" done by the group on its chosen target. For instance, the Italian Red Brigades uses a three person unit for most maimings, utilizing two team members as assailants and the third for escape and cover. The German RAF uses ⌄wo to four people for bombings and at least five for kidnappings. The typical Palestinian assassination team consists of five people -- an observer/spotter, one lay-off man who maintains communication with a headquarters unit, and a three man attack team to actually car¨y out the assassination. This pattern was used in the assassination of the Prime Minister of Jordan, Wasfi Tal, and the bombing of the Israeli Ambassador's residence in Rome.

There are also indications of learning processes at work in the development of team sizes. The Japanese Red Army's first major incident was a hijacking executed by a nine-man unit. All nine members were detained at the plane's final destination and have not been heard from or seen since. Thereafter, the JRA never used more than five people in any one incident.

Patterns apparently also carry across groups, particularly when groups have trained together. The Black September Organization invariably fielded teams with instructions to take no independent action. The team was to await instructions during incidents. In the barricade and hostage incident at Khartoum in which Black September killed two U.S. diplomats and the Belgian Attache, orders to execute the hostages emanated directly from PLO leader Yasir Arafat in Beirut. When a mixed team of Palestinians and Japanese hijacked an airliner out of Amsterdam and destroyed it at Benghazi, Libya, orders for the plane's destruction reportedly were received over the plane's radio, in German, from Switzerland. Later, when a mixed German and Palestinian team hijacked a French airbus to Entebbe in June of 1976, the team reportedly was in constant contact with PFLP leader Wadi Hadad, based in Mogadishu, Somalia. The four organizations involved -- BSO, PFLP, JRA, and RAF -- share many tactical similarities. Moreover, members of each trained in various Palestinian camps in Lebanon, Jordan, and South Yemen.

The sheer number of groups and individuals training together controverts what once was common wisdom among terrorism researchers. It was postulated long ago that the intense ideological committment required of terrorists inhibited exchanges among them. Terrorists were thought to be doctrinaire and unyielding in arguments on strategy and tactics. Communications and cooperation among groups was thus thought unlikely. Ideological divisions would run deeper than the perception of a common goal.

This belief was supported by a large number of examples. Groups frequently splintered over tactical considerations. Internecine conflict was frequent. This pattern has not held over time and the level of exchange among groups is increasing rather than decreasing. Cooperation is observed among groups with common ideologies and goals, as well as across ideological and tactical divisions. Groups exchange members, weapons, and explosives. Terrorists train together and share intelligence data, arrange secure staging locations and provide support for one another, and participate in joint operations. Although terrorist groups still factionalize, splinter, and follow separate tactical paths, cooperation, coordination of effort, and imitation now appear to be the rule. Determining how this exchange affects group actions, what changes in the terrorists' environment have occurred to promote the inter-group interaction, and examination of patterned relations across incidents are all questions that remain to be answered, but are within the scope of capabilities the analyst can provide on group assessments.

The present wave of terrorist violence began in 1968. Since then, the study of terrorism has undergone a number of important developments. Analysis has progressed from normative treatments and case studies to the use of quantitative methods. Such studies have shown that terrorist activity is amenable to systematic analysis and its patterns can be isolated and explored. Thus, the environment in which terrorists operate can be modeled.

Although the move to quantitative analysis has extended our understanding of terrorism, quantitative techniques must continue to be refined to increase our understanding and ability to respond to terrorism. Current quantitative research focuses almost entirely on incidents, using the individual incident as the unit of analysis. This section discusses the necessary shift in analytical focus from incidents to terrorist groups. The shift is made for two reasons. First, it is predicated on the assumption that incidents do not occur in a vacuum: terrorist activity is a function of group capabilities, objectives, motivations, and incentives. Other relationships within the terrorist environment -- the group's relations with national entities or other groups and its selection of tactics and operations -- are similarly constrained by the nature of the group. Second, the shift reflects the information requirements that present data collections are insufficient to meet. This section explores the shift to a group focus, discussing:

- The general use of databases,
- The rationale behind the shift to a group focus, and
- The mechanics of implementing the group focus.

THE GENERAL USE OF DATABASES

Databases are generally constructed to:

- Bring together diverse or fragmentary bits of information for storage in a central location,
- Determine which data are useful for a particular analysis, and which may be discarded as extraneous,
- Place data in a uniform format, and
- Prepare data for analysis.

The requirements for effective intelligence assessment go even farther, demanding:

- A framework for analysis,
- Preliminary analyses of the data, using statistics and other techniques, and
- Analytical techniques for interpreting their results.

A data collection cannot be put to unlimited use. Its contents are collected with some particular set of questions, hypotheses, and assumptions in mind. While each individual bit of information may be neutral, the entire collection is directed toward the investigator's purpose. When research needs change, data collections do not always remain useful. Old data are of limited utility when new questions are asked, for necessary information and variables are frequently missing. When confronted with such limitations, analysts can take one of two paths: they can "bend" the new question's requirements to be met by the old data and restructure the problem so it is more easily analyzed with the existing resources, or they can collect new data structured to meet new requirements. The former path is expedient. The latter is more difficult and time consuming, but provides the only true path to development and further understanding of the problem.

This suggests that before data can be collected for effective threat assessment, researchers must determine how the data will be used, what questions will be asked, and what hypotheses will be tested. Consideration should be given to the data requirements of the various methodologies to be used in the analyses.

In a study conducted by the author, the data holdings of a number of U.S. Government agencies, companies, and private individuals were surveyed. The data collections were found to be insufficient to meet current investigative and threat assessment needs. While large quantities of data have been collected and coded for an impressive array of variables, the data format remains inadequate to answer a number of important questions about terrorist groups and the terrorist environment. In general, the study noted that:

- Very little systematic information exists about the relationships among virtually all terrorist characteristics. As a result, much of the data needed for systematic forecasting, prediction, prevention, and incident management is missing.

- Existing data collections are of isolated incidents, and permit only abstract, global analyses of the available information. The only access to "group" data is through the aggregation of incidents known to have been perpetrated by a particular group. This allows a static analysis of past group action patterns, but is an insufficient base for judging group capabilities, goals, motivation, development, probable responses, and other factors important to crisis managers.

- The existing data collections also provide at best a weak base for studying group dynamics, target selection, contagion of tactics or weapons from group to group or within groups, cell structure, authority patterns, or training. This too, results in a critical information gap posing severe limitations on crisis managers responding to terrorist incidents.

SHIFTING THE UNIT OF ANALYSIS

The overall problem with existing threat assessment procedures is their approach. They view individual incidents as the core element of terrorism research, and believe that terrorist behavior can be understood by studying terrorist acts. Although individual incidents are coded extensively, the nature of the data limits the nature and scope of the questions they can realistically be expected to answer.

During the research study, it became evident that incidents are not the core element in terrorism research. Incidents very likely are a function of group objectives, capabilities, motivation, goals, and desires. The need to shift the focus of terrorism research from incidents to groups is based on a number of observations about the nature of terrorism, and the kinds of questions currently being asked by the terrorism research community:

- Incidents do not occur in a vacuum. They are planned, organized, and carried out by individuals acting alone or in groups. The nature of the incident, its target, the level of force used, the types of weapons used, the number of people involved, and the behavior of the perpetrators will be dependent on the nature of the group.

- Once a target is chosen, weapons choice and requisite force levels will probably be dependent on the nature of the target.

- Forecasting trends in terrorist activity presently rely on extrapolations from past trends. These become poor predictors, however, as changes occur in the environment in which terrorists act. Improving security systems, decreasing the vulnerability of targets, and increasing public awareness of how to avoid becoming a terrorist victim will have an impact on future activity. As terrorism becomes more sophisticated and "costly", predictions about terrorist behavior increasingly will fall into the realm of terrorist capabilities (Can they do it?) and motivation (Do they want to do it?)

Responding directly to the terrorist threat requires more than information about past incidents. Indeed, the response should not be directed at the incident but at its perpetrators. This requires redefining the unit of analysis and asking new kinds of questions. Analyses should focus on the terrorist group, including its size, capabilities, motivations, goals, targeting practices, relations with host and target countries, support networks, and in particular:

- The impact of capability and ideology on targeting practices,
- The impact of training on:
  - Capability
  - Incident outcome,
  - Target selection,
  - Time dedicated to planning and staging, and
  - Group reaction to adversity and success.
- The impact of factional divisions on later group activity and capability,
- The speed with which groups can acquire new capabilities,
- The impact of reorganization on cell autonomy, security patterns, authority structures, and intragroup communications and decision-making, and
- The interaction between the group and support elements, and its impact on:
  - Planning,
  - Movement, and
  - Staging.

Incident data and the findings of incident-focused research are not abandoned when the focus shifts to groups; rather, they are incorporated into the research. The group focus does, however, open new areas for research data collection by broadening the unit of investigation and analysis, and by asking new questions. This adds new variables, allowing for a greater variety of inputs and indicators, building a richer data collection, and making better information available to crises managers.

CONCLUSIONS

A pessimist could infer from the preceding case studies that governments were helpless against terrorist attack, and that the increasing sophistication of terrorist tactics and techniques had rendered all protective measures ineffective. Rather, a different set of conclusions can be drawn from the analyses:

- Military technology and sophistication in its deployment are no longer monopolized by governments or their agents;
- Terrorists have demonstrated remarkable ingenuity, skill, flexibility, innovation, and intelligence in planning and staging their attacks; and
- Increased force levels used by terrorists have effectively neutralized standard protection models, and require similar ingenuity and innovation in the construction of realistic protective approaches to deterring and preventing terrorist attacks.

It is clear that governments have fallen behind terrorists in developing and refining unconventional warfare techniques. The areas of intelligence, analysis, team design, training, and the deployment and recovery of highly effective quick strike commando units have been adopted and perfected by terrorists. While governments still maintain the edge in the control and deployment of resources in conventional warfare, terrorists have been able to breach standard low-level protective models.

Conventional responses to terrorism have been unsuccessful. The state of the art in facility and personnel protection relies on outdated concepts and techniques. Protective models have not kept pace with developments in terrorist targeting tactics. The response to terrorism requires a broad spectrum approach with the primary objective of prevention and deterrence. While the equilibrium state of governmental response lies in reaction -- waiting for the incident to occur to decide on an effective response -- governments must develop more proactive approaches to protection if they are to deal effectively with the terrorist threat. Protective models can be constructed at four general levels:

- Preventative deterrence,
- Ongoing incident management,
- Technical incident response, and
- Postincident analysis and investigation.

Most governments operate at the level of technical incident response and postincident analysis, failing to draw proper lessons from repeated terrorist confrontations. Simple analyses of terrorist behavior, as described earlier in this paper, indicate that terrorists are most vulnerable before and after their assaults, and are most resilient during an action as they maintain the element of surprise and exercise immediate control over the flow of events. Incorporating this idea into an indications and warning system that would monitor terrorist actions throughout the planning and execution phases of attacks can move government protection models out of the realm of reaction -- after the blow has been struck and lives lost or endangered -- into recognition of terrorists as threatening and dealing with them accordingly.

The broad spectrum approach of dealing with terrorists at all levels of their organizational development must further rely on the development and use of highly specialized counterforce elements capable of regaining government initiative and control once a terrorist action begins to unfold. Key response units dedicated to minimizing risk and damage to governments and the people and facilities they protect, backed with realistic assessments of terrorist capabilities and trajectories, may be able to restore the government's edge in the security field.

BEHAVIORAL SCIENCE: EVENTS OUTSIDE THE SKIN

Charles Wallach

Decisions and Designs, Incorporated

Introduction By

General C. James Douglas (USAF, Ret.)
Decisions and Designs, Incorporated

In this decade, behavioral scientists will be developing a much greater awareness of the psychological and metabolic effects of environmental factors on human task performance. It has long been recognized that people remain alert and work better within certain ranges of temperature, humidity, and illumination; it has become evident that there are also critical ranges of electromagnetic fields and atmospheric ion balance which have an impact, varying from subtle to dramatic, on human capacity to function in critical tasks. There is much to be learned about the mechanism of these effects. Since they vary widely from one individual to another with age, stress, health, and biological reaction time, we are also faced with the more immediate necessity of learning either how to provide all personnel with optimum working environments, or discovering the best means of discriminating between environmentally labile and stable individuals in making assignment selections for duty in critical or stressful environments. We have outlined recent accomplishments, near-term objectives, and potential applications of new ionic and aeroelectrostatic developments across a broad spectrum of military and civil requirements. We think that many of you will be able to identify with some of the problems and solutions discussed here.

BEHAVIORAL SCIENCE: EVENTS OUTSIDE THE SKIN

There are many anecdotes in written and oral history about the behavioral effects of weather -- people becoming dopey, morose or irritable before a storm, children becoming hyperactive and troublesome, while many older people suffer twinges of joint pain. This emphasis on unnatural, even irrational behavior before a storm has obscured the fact that all these manifestations are reversed as soon as the storm passes over; we take euphoria for granted!

Weather-related behavioral deviations have traditionally been related to atmospheric pressure changes, probably because these are easily observed on the crudest of barometers. But this ancient theory does not stand up to close examination. Greater pressure changes are experienced daily by people riding up and down the elevators of high-rise buildings, without any such effects. It has become clearly evident that the major, if not the only factor in weather-related behavioral and metabolic patterns is the balance and concentration of small, atmospheric ions which modify the electrical charges of the tissues in the respiratory canal.

The effects of such changes in the ambient ionic environment on the central nervous system, on mental nimbleness, job performance and human productivity, vary from slight to profound over the population spectrum. In one notable example of this phenomenon, after the passage of an unusually severe September storm in New England, it was found that the several hundred students taking a difficult college-entrance exam at an ivy-league institution achieved scores so high that their average has never been equalled before or since. Clearly, the invisible populations of ions in the air are of much greater importance to human and animal behavior than is generally realized.

Since we can seldom depend on storms to produce optimum performance continuously over a six- or eight-hour shift in a critical task assignment, we try to instill discipline in task performance and reinforce this with training and drill, drill, drill, and more drill. It should be obvious that any reasonable intelligent human being, once taught to react to a certain stimulus in a logical manner, ought to be able to repeat this behavior pattern whenever that stimulus is received. In fact, it does happen occasionally that someone can repeat a learned or observed behavior pattern perfectly, even long after a single learning experience.

So why is it necessary to drill and redrill, to train and retrain, to preserve proficiency in the performance of a task? It must be because we cannot always rely on our central nervous system to process the stimulus properly, nor on our neuro-muscular coordination to function accurately on short notice. there are many factors that can influence your alertness, your sensory acuity, and your reaction time to an important stimulus; I'm sure you could name six or eight factors without drawing a breath.

One of the least known, and more insidious of the environmental factors that modulate behavior, metabolism, and task performance, is the electrical quality of the ambient air. It's least known because it's invisible, unsensible, and difficult to measure.

We have discussed the biological and behavioral effects of atmospheric ionization in each of the past four of these annual behavioral science seminars. This year we would like to focus more sharply on the behavioral applications of ion technology and give you a brief overview of the growing number of other applications in which we are becoming involved.

Let me briefly review what ions are all about for the benefit of anyone who is unfamiliar with the subject. In the very limited context of this discussion, we're talking about only the smallest and most active of electrically charged gaseous particles. Negative ions are, for the most part, normal oxygen molecules (O_2) which have acquired extra electrons in addition to their normal complement and become (O_2^-). This changes their energy state, but not their chemical composition; these should not be confused with ozone (O_3) which may also acquire a negative charge, but has a different chemical action. Negative ions always have a positive effect in our applications.

Positive ions, which often have a negative effect on human performance, are gaseous molecules of carbon dioxide (CO_2), water vapor, or other simple compounds which have had one or more of their normal complement of electrons knocked out of their outer ring.

On the average, in fresh air, in fair weather, there are roughly equal numbers of positive and negative ions which are continuously being created by natural subatomic events and continuously being neutralized. Under such average conditions, there are about a thousand of each per cubic centimeter of air, and in terms of biological and behavioral effects, they tend to cancel out.

It is only when there is a significant shift in this one-to-one ratio that we begin to see short-term behavioral effects. This relationship is conventionally expressed as "positive-to-negative ion ratio" (PNIR). This figure increases as negative ions are neutralized at an accelerated rate and/or when positive ions are added to the mix. Fractional PNIR indicates a preponderance of negative ions.

It becomes easy to relate to this picture if you are aware of the sticky, dead-feeling air that precedes a summer thunderstorm as the concentrations of positive ions are greatly increased by the electrical field of the storm cell. Conversely, immediately after a storm, negative ions predominate in the clear, invigorating air that characteristically follows the lightning and precipitation.

We're on firm ground, now, when we say that some critical human faculties are dulled by a prestorm or artifically created high PNIR and are quickly sharpened in a low PNIR environment. Recent research results both here and abroad have repeatedly confirmed this phenomenon beyond any question of doubt. For example, a surprisingly high correlation has been established between abnormally high PNIR conditions and vehicular accidents, clerical errors, diminished productivity, and degradation of vigilance or attention.

This is a new factor in environmental and architectural engineering, but in attempting to apply it as a useful tool in performance enhancement in critical task and training situations, we are faced with some practical considerations for which our present experimental data bas is not yet adequate to resolve satisfactorily.

- Which individuals are sensitive to PNIR variations? Some have an innate autonomic capability of stabilizing the affected biochemical systems adequately (except, perhaps, when under stress).

- Which types of critical task environments are characteristically subject to excessively high PNIR, and how may this condition be rectified most effectively?

We go to great lengths to control temperature, humidity, light, and even noise within their rather narrow margins of human comfort, to optimize performance and well-being; now we are aware of ionization as a new factor to be added to the list. Clearly, where poor ionic conditions are found, we should either use appropriate environmental controls or carefully select the individuals assigned there on the basis of their relative resistance to the undesirable effects.

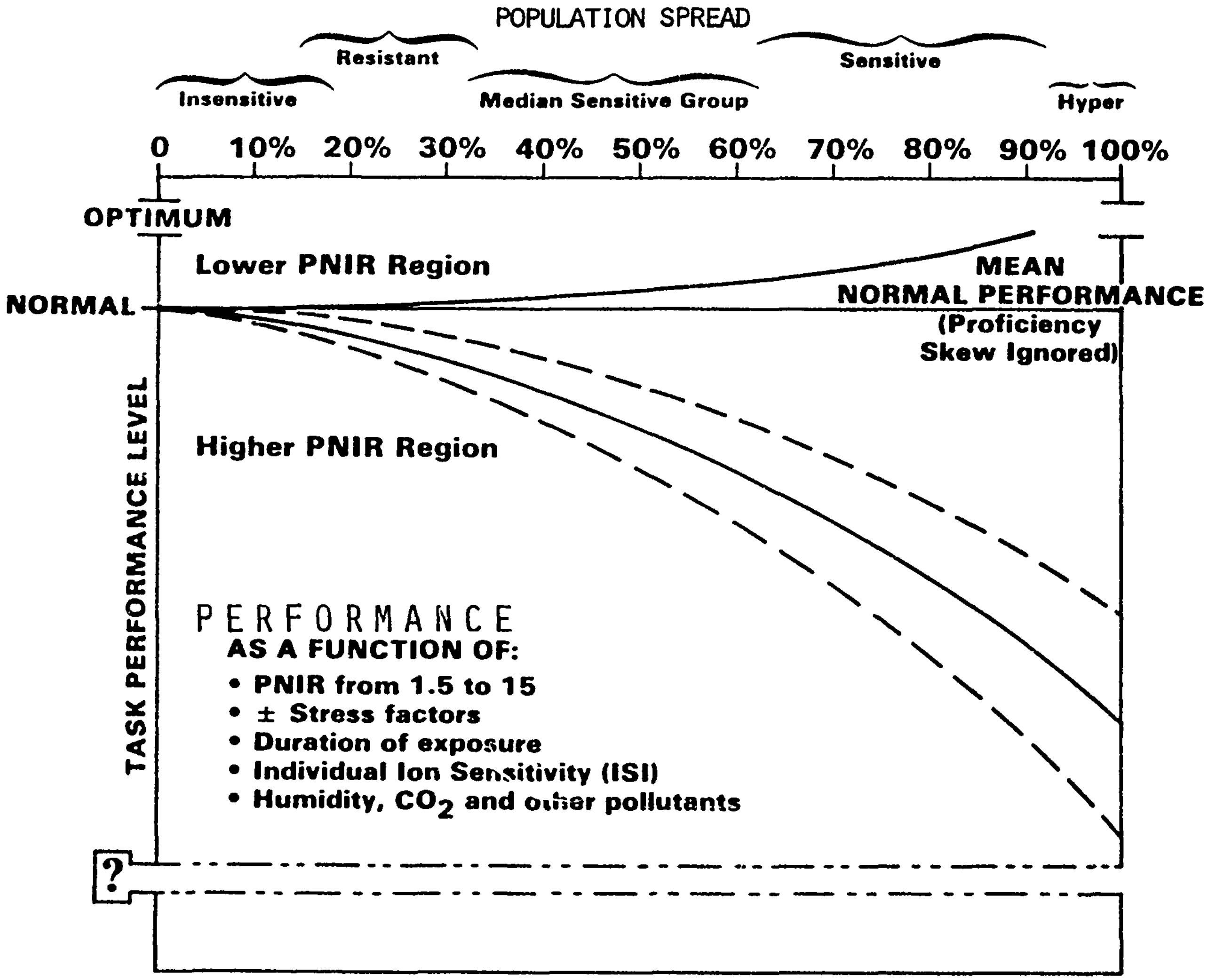
This is a practical and scientific frontier on which all of us have an opportunity to make substantial contributions in the near future. Many foreign and a few American researchers have contributed to our qualitative understandings of air ion phenomena; we now need to augment this substantial body of work by developing quantitative analysis and application-engineering standards for making practical use of it.

The first step is to validate and quantify the degradation in human performance which has been observed so often in everyday PNIR conditions found in many critical work environments. We are intrigued by the challenge of discovering the fundamental causes of ion effects in terms of metabolic chemistry and nervous system interactions, but these details are really not vital to our development of practical applications at this stage; in any case, that will probably require many years of costly and intensive research effort, some of which is already being pursued in medical facilities.

With respect to these immediate research objectives, we are comfortable with the knowledge that the quality of alertness is controlled by the Reticular Activating System (RAS) in the brainstem; we also know that the RAS is normally wired to maintain an optimum state of arousal, but this condition is overridden from time to time by chronobiological mechanisms, high PNIR, and any sort of stress from a toothache to an audit notice from the IRS. We shall focus on the ways, but not the means, in which ion balance affects the RAS and human behavior.

Reference is made to the performance decrement chart in Figure 1, entitled "The Reason for Concern." This graphically illustrates a number of points and highlights our present uncertainties which we hope to clarify in the near future. It makes the following points:

- Performance decrements can be anticipated among a certain meaningful percentage of personnel with increases in:
  - PNIR
  - stress factors
  - duration of exposure
  - humidity
  - dust and other pollutants.
- Performance can generally be skewed towards optimum as PNIR is reduced to very low values.
- In both cases, we have not yet acquired data on the basis of which the decrement or enhancement can be quantified in relation to the other variables.
- It is clear that some individuals are affected by ion ratios far more critically than others; the development of an Ion Sensitivity Index scale is needed to assist in rationalizing performance prediction characteristics.



Model of performance degradation (enhancement) by percentage with ambient air ion ratios varied above and below normal average 1.2:1

The Reason for Concern

Figure 1

Unfortunately, our observations of performance degradation thus far tend to suggest that the more creative and quick thinking types of individuals are prone to fall in the higher ranges of ion sensitivity (possibly because of interference with bilateral synchrony of cerebral lobe functions in the cognitive processing of information).

We need to learn what differences in easily observed or measured physiological reactions characterize the more sensitive individuals and to what extent any quantification of sensitivity level will vary with changes in other parameters of the task environment

Decreases in alertness (or arousal) are always accompanied by certain physiological and metabolic changes which we can monitor, and by subtle psychological shifts which we can measure. These data, however, vary widely with person, time, place, and circumstances; therefore, to develop meaningful information on ion effects as the PNIR is varied, we must start with an adequately large number of subjects to assure statistical significance. This is the first step in quantifying and validating performance effects as shown in Figure 2.

We prefer to use several different methods of evaluating performance, simultaneously during this first-phase investigation; this may enable us to identify the simplest and most effective method(s) and thereby facilitate and economize on future testing of this nature.

After establishing a firm foundation in demonstrating the existence of ion-related performance degradation among a subject population under carefully controlled conditions, the next step is to separate our subjects into sensitive, mid-range, and resistive groups on the basis of the amount by which their performance was affected.

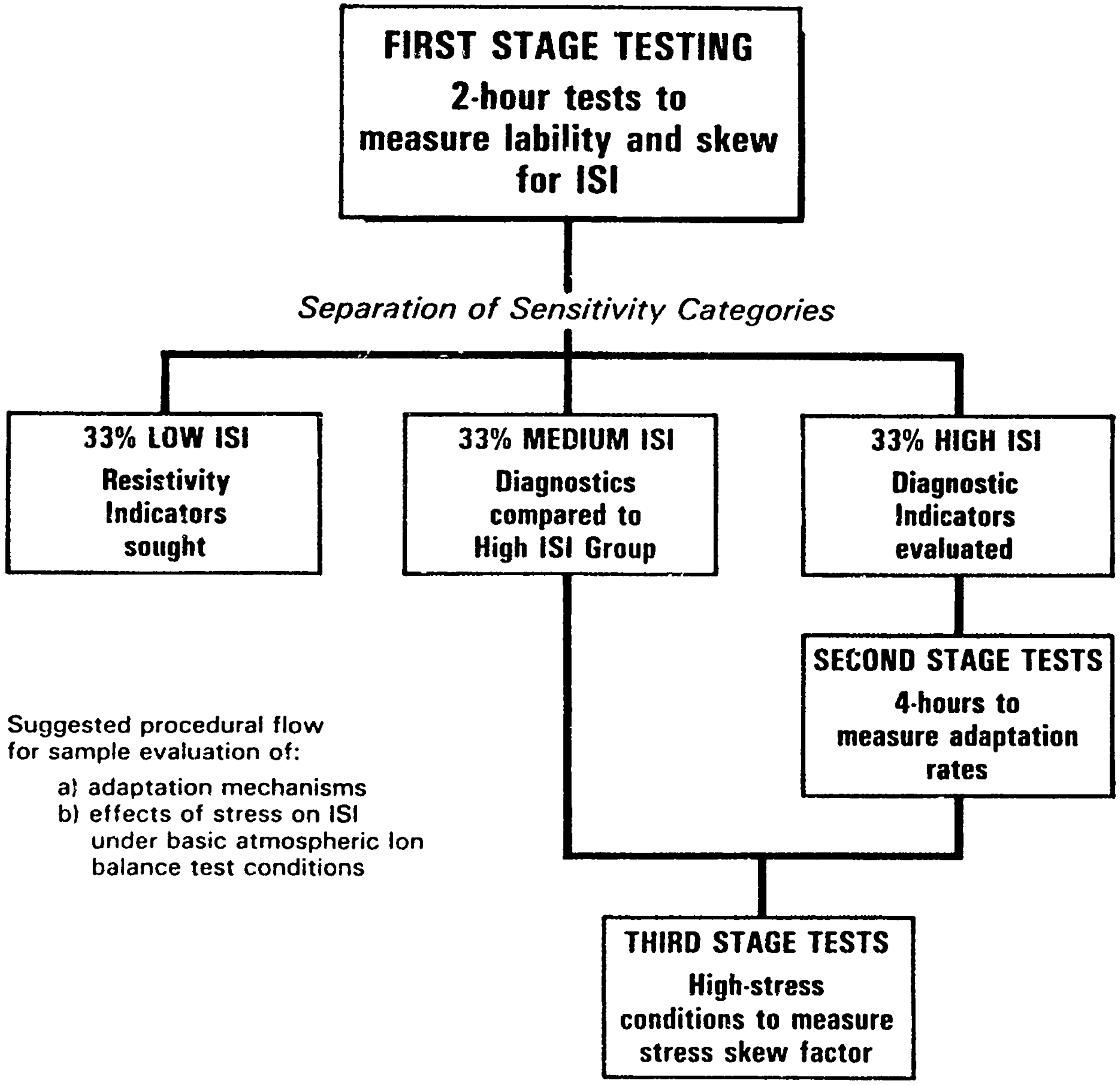
This detailed analysis of subject performance, when correlated with baseline physiological and psychological measurements of each subject, will enable us to make a first cut at the development of an individual sensitivity rating system, an Ion Sensitivity Index scale (ISI), which might ultimately be refined as a useful tool in personnel selection.

From past experience, however, we know in advance that any ion sensitivity scoring system must be used with caution within a framework of dynamic variation, since individual sensitivity will vary with many circumstances, chiefly age, comfort, arousal, and stress. Therefore, in order to develop some measure of objective awareness of the range of individual sensitivity variations, we must repeat our original protocol with stress as the controlled variable--possibly subdividing our sensitivity categories into age groupings if this should be feasible.

Thus far, we are assuming that our first-phase investigation will have clearly established a significant correlation between performance degradation and high PNIR. On the basis of published literature, I do not doubt that this will be shown if our testing procedures are properly designed. Having gotten that far, we have yet to demonstrate that significantly high PNIRs exist in the operational environments of concern. This will require a series of ion measurements in the actual environments, under uncontrolled conditions normal to such environments (heating/cooling, day/night, crowded/empty, etc.), with fairly sophisticated instrumentation, to establish environmental baselines, as opposed to behavioral baselines.

Given significant findings in this collateral line of investigation, we shall then be able to justify proceeding with the development of hardware with which to regulate and control the environmental ion factors within a suitable range in the same manner that we now control temperature and humidity.

ION SENSITIVITY INDEX (ISI)


FIRST STAGE TESTING
2-hour tests to measure lability and skew for ISI
Separation of Sensitivity Categories
33% LOW ISI
Resistivity Indicators sought
33% MEDIUM ISI
Diagnostics compared to High ISI Group
33% HIGH ISI
Diagnostic Indicators evaluated
SECOND STAGE TESTS
4-hours to measure adaptation rates
THIRD STAGE TESTS
High-stress conditions to measure stress skew factor

Suggested procedural flow
for sample evaluation of:

a) adaptation mechanisms
b) effects of stress on ISI
under basic atmospheric Ion
balance test conditions

Figure 2

With the rapid growth of the industrial and consumer market for air ion control hardware, it should not be difficult to modify production specifications to the military requirements. This would lead to a series of procurements which would necessitate the generation of installation engineering standards, equipment manuals and procedures, as each activity assimilated this new technology wherever appropriate.

This orderly pattern of research and development activity is classic in the military application of any new technology, and we would welcome the opportunity to initiate and implement it under the sponsorship of any operational or training activity where it will enhance performance objectives. We feel that it has important potential in many training activities because we are working on the enhancement of such human factors as attention focus, attention span, alertness, and arousal of mental faculties. Much of our training philosophy is based on the necessity for either forcing these factors through the application of stress in various forms, or repetition designed to overcome attention decrement due to various environmental and psychological factors.

However, we feel that the most immediate and needy applications of this new technology will be in ion-deficient environments in which critical tasks are performed, and where optimum alertness is essential to military duties.

To summarize the effects we are addressing in the Behavioral area which may be of cogent interest are:

- vigilance or alertness
- sensory acuity
- reaction time or arousal
- fatigue
- irritability and tension
- learning efficiency
- productivity.

The particular Environments of most immediate concern are:

- interior guard posts
- underground silos
- submarine compartments
- surveillance towers
- cockpits
- truck cabs
- armored vehicles
- communicatons centers
- training facilities.

There are also significantly promising applications in the field of Nuclear, Biological and Chemical (NBC) protection and countermeasures:

- Ionization technology has significantly important applications in the improvement of gas masks and in the incorporation of NBC protection into helmet configurations.

- These same methods can be applied to protecting the intake air supply of manned vehicles, shelters, and hardened installations or safe havens.

> An ionized chelation process has been demonstrated to be highly effective in quickly and easily decontaminating vehicles which have been exposed to NBC weapons, without paint damage and without the requirement for elaborate decontamination facilities.

A glance at Figure 3 will indicate the rapid development of ion technology and aeroelectrostatics in other areas.

Moving on to the Health sector, air ion technology has proven useful in the following areas of potential military and public interest:

- symptomatic relief of emphysema, asthma, aeroallergy;
- reduction of pain, motion- and altitude-sickness;
- acceleration of healing of wounds and burns.

In the Industrial sector, aeroelectrostatics can be used with dramatic effectiveness in;

- precipitating or neutralizing industrial pollutants which are hazardous to health;
- eliminating offensive odors;
- killing bacteria, virus, mold, and fungus spores which cause costly product contamination and waste; and
- eliminating static problems in computer environments, spinning mills, photo labs, and clean rooms.

Applications have been developed for these technologies in the Commercial sector, where inexpensive hardware is being used to:

- eliminate unpleasant odors;
- quickly dissipate tobacco and kitchen smoke and odors in public places; and
- Keep confined groups of people more alert and comfortable, from board rooms to auditoria.

When we consider what we have called the Environmental sector, however, we come around in a full circle to applications which impact on human behavior--not only in critical task performance, but also with respect to attitudes, moods, and well-being under off-duty conditions and in the performance of noncritical, routine duties. Among the working and living environments most commonly found to suffer from atmospheric ion disbalance and/or depletion are:

- office and operations quarters
- insulated houses and apartments
- subterranean and submarine spaces
- closed moving vehicles and tower cabs

Current Application Areas

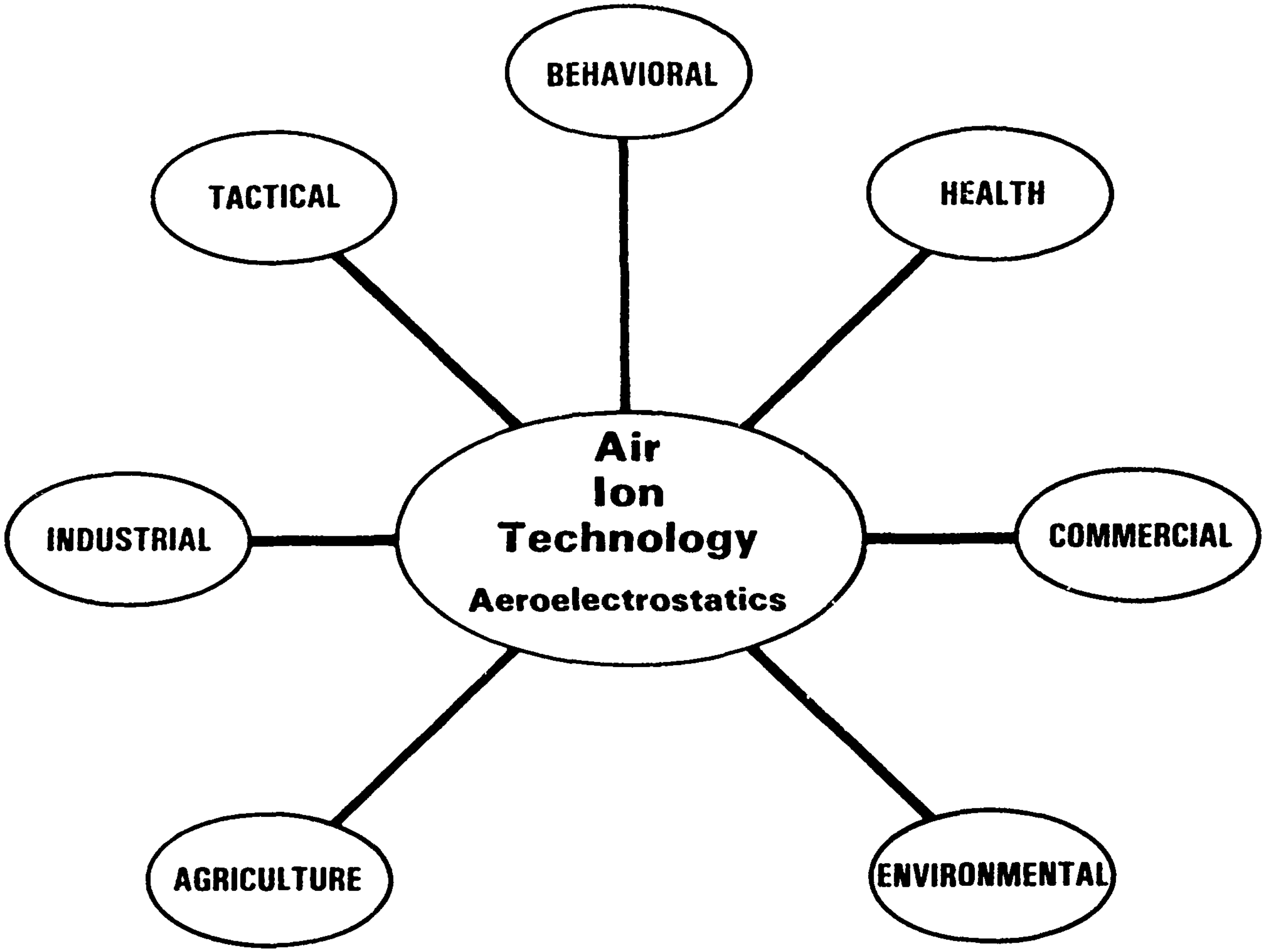


Figure 3

Figure 3

Each of these types of spaces is subject to particular sets of effects which degrade the ionic environment, as well as presenting other characteristic problems in heating, cooling, and humidity control.

Usually, there is no single, major factor which causes unnaturally elevated and sustained PNIR or air ion depletion; therefore it is of interest to note the many small factors which contribute incrementally, in varying degrees, to the reduction of negative ion concentrations, production of added positive ions, and/or the accelerated neutralization of both.

These degradation factors may be grouped into two classes: Architectural as a function of space design, and Artifactual as a function of space utilization. Most of these contributing factors will be found to coexist in all of the particular types of environments listed below:

° Architectural

- forced-air ventilation systems
- artificial illumination in windowless spaces
- synthetic floor surfaces or carpets
- low ceilings, which impede convection current formation
- electrically grounded shelters and conductive walls
- solar heating distribution systems
- external air/water friction on outer skin of structure
- high-efficiency insulation restricting air exchange.

° Artifactual

- auxiliary ventila ion fans and any moving metal parts
- fluorescent lamp fixtures using high voltage ballasts
- electrical machinery and communications equipment
- visual display terminals using cathode ray tubes
- metal and most types of plastic furniture
- tobacco smoke, open fires, and electrical heating elements
- wearing of synthetic clothing and insulating footwear
- overcrowding of closed spaces by occupants or animals.

The variety of behavioral and other problems engendered by inadequate atmospheric ion conditions in enclosed spaces have been little known and long ignored in this country for two basic reasons:

- lack of adequate research to provide coherent, objective, statistically significant, and quantifiable data on the nature and extent of biological effects; and

- not knowing what to do about such problems, absence of engineering standards, quantitative references, and nonavailability of proper instrumentation.

It is most interesting to note that most of the speakers who preceded me in this seminar have touched on points which are remarkably germane to my presentation. That is to say, they've touched on these point in the context of urging our research community to focus on these causes and effects of performance deficit. These are:

- mood and environmental affectors

- measurement of the mental and physical characteristics of Guard Force personnel and their performance under stress

- real-world performance degradation of people faced with cathode ray tubes. It is noted that this has become an issue of major concern with trade unions and occupational health groups in several countries because of the great number of Video Display Terminal (VDT) operators affected; the same problem exists for security guards monitoring close circuit TV.

Exciting new work with computerized brainwave analysis was mentioned; this holds promise of becoming an elegant tool for measuring both the degradation and enhancement of human task performance under varying ionic conditions.

Within the behavioral science discipline, we have just about picked clean the bones of gross performance and behavioral affectors which originate inside the human skin; we are now moving on to an exciting era of studying a whole new range of exogenic affectors in a hitherto ignored environmental factor which impacts significantly on human performance and behavior: The electrical quality of the air we breath.

ROSTER OF PARTICIPANTS

SIXTH ANNUAL SYMPOSIUM
"THE ROLE OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY"

3 - 4 JUNE 1981

HQ, DEFENSE NUCLEAR AGENCY
CONFERENCE ROOM A

NAME	ORGANIZATION/ADDRESS	TELEPHONE NUMBER
ABBOTT, Preston S.	Abbott Associates, Inc. 801 N. Pitt Street Alexandria, VA 22314	(703) 836-8080
BARRY, Joseph A.	Management Safeguards, Inc. 286 Congress Street Boston, MA 02110	(617) 482-2640
BAUMAN, Majorie B.	Biotechnology, Inc. 3027 Rosemary Lane Falls Church, VA 22042	(703) 573-3700
BEASLEY, Marvin C.	HQ, Defense Nuclear Agency ATTN: PSNS Washington, DC 20305	(202) 325-7395
BENNER, Patricia L.	Mission Research Corp. Capital Bldg II, Suite 201 5503 Cherokee Avenue Alexandria, VA 22312	(703) 750-3556
BICK, Frederic A.	Effects Technology, Inc. 5383 Hollister Avenue Santa Barbara, CA 93111	(805) 964-9831
BITLER, William D.	HQ, Defense Nuclear Agency ATTN: PSNS Washington, DC 20305	(202) 325-7091
BLACK, James R.	Tracor, Inc. Department of State Security Upgrade Contract 5201 Leesburg Pike, Suite 300 Falls Church, VA 22041	(703) 379-5410
BROWN, Terry L.	VITRO Engineering Corp. P. O. Box 296 1825 Terminal Drive, Suite 220 Richland, WA 99352	(509) 376-6517

BRUH, Daniel E.	TRW Inc., Washington Operations 7600 Colshire Drive McLean, VA 22102	(703) 734-6250
BUKOLT, Cezary R.	HQ, Naval Materiel Command ATTN: MAT 046 Washington, DC 20360	(202) 692-3216
BURKE, James E.	TRACOR, Inc. Department of State Security Upgrade Contract 5201 Leesburg Pike, Suite 300 Falls Church, VA 2041	(703) 379-5475
BUSH, Loren L.	US Nuclear Regulatory Commission Office of Inspection & Enforcement Mail Stop E/W - 359 Washington, DC 20555	(301) 492-8080
CHAMBERS, Owen S.	US Nuclear Regulatory Commission Mail Stop E/W - 359 Washington, DC 20555	(301) 492-8457
CHESTER, Stephen D.	Sandia National Laboratories P. O. Box 5800 Albuquerque, NM 87185	(505) 844-7026
CROSSLIN, Floyd	Dynalectron Corporation 6888 Elm Street McLean, VA 22101	(703) 893-2143
DAVIS, Elaine G.	Science Applications, Inc. 1710 Goodridge Drive McLean, VA 22102	(703) 827-4968
DAVIS, Michael F.	JAYCOR 205 South Whiting Street Alexandria, VA 22304	(703) 823-1300
DEMARCO, John M., Jr.	GSA/Federal Protection Service 18th & F Streets, NW, Room 2301 Washington, DC 20405	(202) 566-1063
DOULGAS, Clarence J., Jr.	Decisions & Designs, Inc. 8400 Westpark Drive, Suite 600 McLean, VA 22101	(703) 821-2828
DRAUSZEWSKI, Joseph C.	HQ, Defense Nuclear Agency ATTN: PSNS Washington, DC 20305	(202) 325-7365

ELIASON, Lawrence K.	National Bureau of Standards Law Enforcement Standards Labs US Department of Commerce Washington, DC 20234	(301) 921-3161
EVANS, John C.	The BDM Corporation 7915 Jones Branch Drive McLean, VA 22102	(703) 821-4256
FINELY, Brian H.	Sandia National Laboratories P. O. Box 5800 Albuquerque, NM 87185	(505) 844-6247
FRANKEL, Harry D.	US Imigration & Natralization 425 I Street, NW, Rm 6112 Washington, DC 20536	(202) 633-3343
FRANKS, Henry L.	Los Alamos National Laboratories P. O. Box 1663 OS-1, Mail Stop 688 Los Alamos, NM 87545	(505) 667-4673
GIESKE, Harry A.	Booz Allen & Hamilton, Inc. 4330 East Weat Highway Bethesda, MD 20014	(301) 951-2720
GILBERT, Gauvain	US Army Military Police School Fort McClellan, AL 36201	AV 865-3024
GOOCH, K. W.	Dynalectron Corporation 1313 Dolley Madison Boulevard McLean, VA 22101	(703) 356-0480
HABEN, John F.	Naval Surface Weapons Center White Oak Silver Spring, MD 20910	(202) 394-2890
HALL, Robert J.	Human Factors Research 5775 Dawson Street Goleta, CA 93117	(805) 964-8092
HAMMAKER, Charles A., Jr.	US Army Materiel Development & Readiness Command 5001 Eisenhower Avenue Alexandria, VA 22333	(202) 274-9033
HANNA, Bill	Mission Research Corporation P. O. Drawer 719 735 State Street Santa Barbara, CA 93102	(703) 750-3556

HARVEY, Stephen J.	CACI, Inc. - Federal 1815 N. Fort Myer Drive, 10th Floor Arlington, VA 22209	(703) 841-7800
HENRIKSEN, George G.	HQ, Naval Scty Group Command 3801 Nebraska Avenue, NW Washington, DC 20390	(202) 282-0235
HIRONAKA, Mas E.	Intelligence Materiel Development & Support Office Electronic Warfare Laboratory Fort George Meade, MD 20755	(301) 677-7616
HOLLADAY, Van D.	Carson & Associates, Inc. 7315 Wisconsin Avenue Bethesda, MD 20014	(301) 656-1024
JAMES, Joseph W.	US Nuclear Regulatory Commission Mail Stop EW - 359 Washington, DC 20555	(301) 492-7078
JOHNSON, Thomas E.	HQ, Defense Nuclear Agency ATTN: PSNS Washington, DC 20305	(202) 325-7365
KEANE, Bettye J.	Navy Civil Engineering Lab Physical Security Lab Port Hueneme, CA 93043	AV 360-5927
KOZUMA, Roger T.	Analytical Systems Engineering 5 Old Concord Road Burlington, MA 01803	(617) 272-7910
KREIS, Charles W.	Air Force Weapons Laboratory Kirtland AFB, NM 87117	(505) 844-9306
KUHLA, Cletus B.	Office of the Under Secretary of Defense for Research & Engineering ATTN: Chairman, PSEAG Washington, DC 20305	(202) 697-0638
LAWSON, Quinton Y.	GSA/Federal Protective Service 18th & F Streets, NW, Room 2039 Washington, DC 20405	(202) 566-1063
LEEDY, Herbert B.	US Army Military Personnel Center 200 Stoval Street Alexandria, VA 22332	(202) 325-0641
LEPAGE, Godfrey W.	HQ, USAF/RDSD Pentagon, Room 5C269 Washington, DC 20330	(202) 694-8440

LEVY, Girard W.	Battelle-Columbus Laboratories 505 King Avenue Columbus, OH 43201	(614) 424-7164
LEWIS, Gregory W.	Navy Personnel Research & Development Center San Diego, CA 92152	(619) 225-2081
LONG, Roger G.	Arthur D. Little, Inc. 25 Acorn Park Cambridge, MA 02140	(617) 864-5770
MACMURDY, Paul H.	US Nuclear Regulatory Commission Mail Stop 881-SS Washington, DC 20555	(301) 427-4191
MADDEN, Michael T.	Naval Surface Weapons Center White Oak Silver Spring, MD 20910	(202) 394-1692
MARCKS, Frederick	Analytical Systems Engineering 5 Old Concord Road Burlington, MA 01803	(617) 272-7910 Ext 198
MARGULIS, Stephen T.	National Bureau of Standards Room A355, Bldg 226 Washington, DC 20234	(301) 921-2102
MARKULIS, Kristina Z.	Nuclear Regulatory Commission 5650 Nicholson Lane Rockville, MD 20852	(301) 443-5976
MCWHIRTER, Michael R.	HQ, Defense Nuclear Agency ATTN: PSNS Washington, DC 20305	(202) 325-7361
MEDLER, Leon	US Army MERADCOM ATTN: DRDME-US Fort Belvoir, VA 22060	(703) 354-4455
MEYERS, Ira R.	GSA/Federal Protective Service 7th and D Streets, SW Washington, DC 20407	(202) 472-1632
MIDURA, Thomas J.	Harold Rosenbaum Associates, Inc. 40 Mall Road, Suite 207 Burlington, MA 01803	(617) 273-1964
MILLER, Rudy A.	GTE Products Corporation 100 Ferguson Drive P. O. Box 188 Mt. View, CA 94042	(415) 966-2415

MINICHINO, Camille	Lawrence Livermore National Labs ATTN: L-97 Livermore, CA 94550	(415) 422-1269
MOORE, Raymond T.	National Bureau of Standards Institute for Computer Sciences & Technology, Bldg 225, Room A219 Washington, DC 20234	(301) 921-3427
MORRISON, David C.	Naval Electronic Systems Command Washington, DC 20360	(202) 692-1762
MOTA, Manuel	HQ, Department of the Army ATTN: DAPE-HRE-PS Washington, DC 20310	(202) 756-1934
MOYER, Dale L.	HQ, Defense Nuclear Agency ATTN: PSNS Washington, DC 20305	(202) 325-7365
MULLEN, Sarah A.	US Nuclear Regulatory Commission Mail Stop 881-SS Washington, DC 20555	(301) 427-4191
MURPHY, Ralph H.	Magnavox, Government & Industrial Electronics Company 1700 North Moore Street, Suite 820 Arlington, VA 22209	(703) 522-9610
NORMAN, William	New Zeland Embassy	(202) 328-4821?
OWEN, James W.	US Army MERADCOM ATTN: DRDME-XIL Fort Belovir, VA 22060	(703) 664-2877
PELCZYNSKI, Casper J.	US Department of State Washington, DC 20520	(202) 557-3510
PETERS, Anthony J.	HQ Marine Corps Law Enfor (MP)	(202) 694-1930
PETERS, William G.	HQ, Defense Nuclear Agency ATTN: NASD Washington, DC 20305	(202) 325-7865
PRICE, Harold E.	BioTechnology, Inc. 3027 Rosemary Lane Falls Church, VA 22042	(703) 573-3700
PULLIAM, Robert	BioTechnology, Inc. 3027 Rosemary Lane Falls Church, VA 22042	(703) 573-3700

RAO, Magal H.	US Department of Energy Office of Safeguards & Security Mail Stop A2-1016 Washington, DC 20545	(301) 353-4120
RICHARDS, Donald R.	Booz Allen & Hamilton, Inc. 433 East West Highway Bethesda, MD 20014	(301) 951-2285
ROBINSON, Terry S.	HQ, USAF/IGS (Security Police) Pentagon, Room 5D287 Washington, DC 20330	(202) 566-0239
RODRIGUEZ, Joseph R.	General Services Administration 18th & F Streets, NW Washington, DC 20405	(202) 694-8641
ROTH, Thomas J.	Applied Science Associates, Inc. Box 158 Valencia, PA 16059	(412) 586-7771
ROZNER, Alexander G.	Naval Surface Warfare Center Bldg 24-6, Code R32 White Oak, MD 20910	(202) 394-2737
RUSSACK, Richard	Management Safeguards, Inc. 286 Congress Street Boston, MA 02110	(617) 482-2640
SCHMIDT, Raymond P.	HQ, Naval Security Group Command 3801 Nebraska Avenue, NW Washington, DC 20390	(202) 282-0873
SCHOFIELD, David	NUSAC, Inc. 7926 Jones Branch Drive McLean, VA 22102	(703) 893-6004
SCHWALM, Robert	Los Alamos National Laboratories P. O. Box 1663, MS 725 Los Alamos, NM 87545	(505) 667-5862
SHAFFER, Guy H. B.	HQ, Defense Nuclear Agency Deputy Director Washington, DC 20305	(202) 325-7065
SHAPIRO, Melvin	TRW, Inc. - Washington Operations 7600 Colshire Drive McLean, VA 22102	(703) 734-6218
SHORT, LaDonna	US Army MERADCOM ATTN: PO-PSE Fort Belvoir, VA 22060	(703) 664-5575

SPIES, Gordon N.	Nuclear Regulatory Commission Mail Stop 881SS Washington, DC 20555	(301) 427-4191
STINSON, James L.	CACI, Inc. - Federal 301 E. Colorado Blvd, Suite 400 Pasadena, CA 91101	(213) 796-5225
VAN COTT, Harold P.	BioTechnology, Inc. 3027 Rosemary Lane Falls Church, VA 22042	(703) 573-3700
WALLACH, Charles	Decisions & Designs, Inc. 8400 Westpark Drive, Suite 600 McLean, VA 22101	(301) 585-8881
WHEELER, James E.	HQ, Defense Nuclear Agency ATTN: Chief, PSNS Washington, DC 20305	(202) 325-7361
WITTER, William J.	HQ, Defense Nuclear Agency ATTN: PSNS Washington, DC 20305	(202) 325-7091
WOLFSON, Leonard	Nav Explosive Ordnance Disposal Technology Center Indian Head, MD 20640	(301) 743-4843