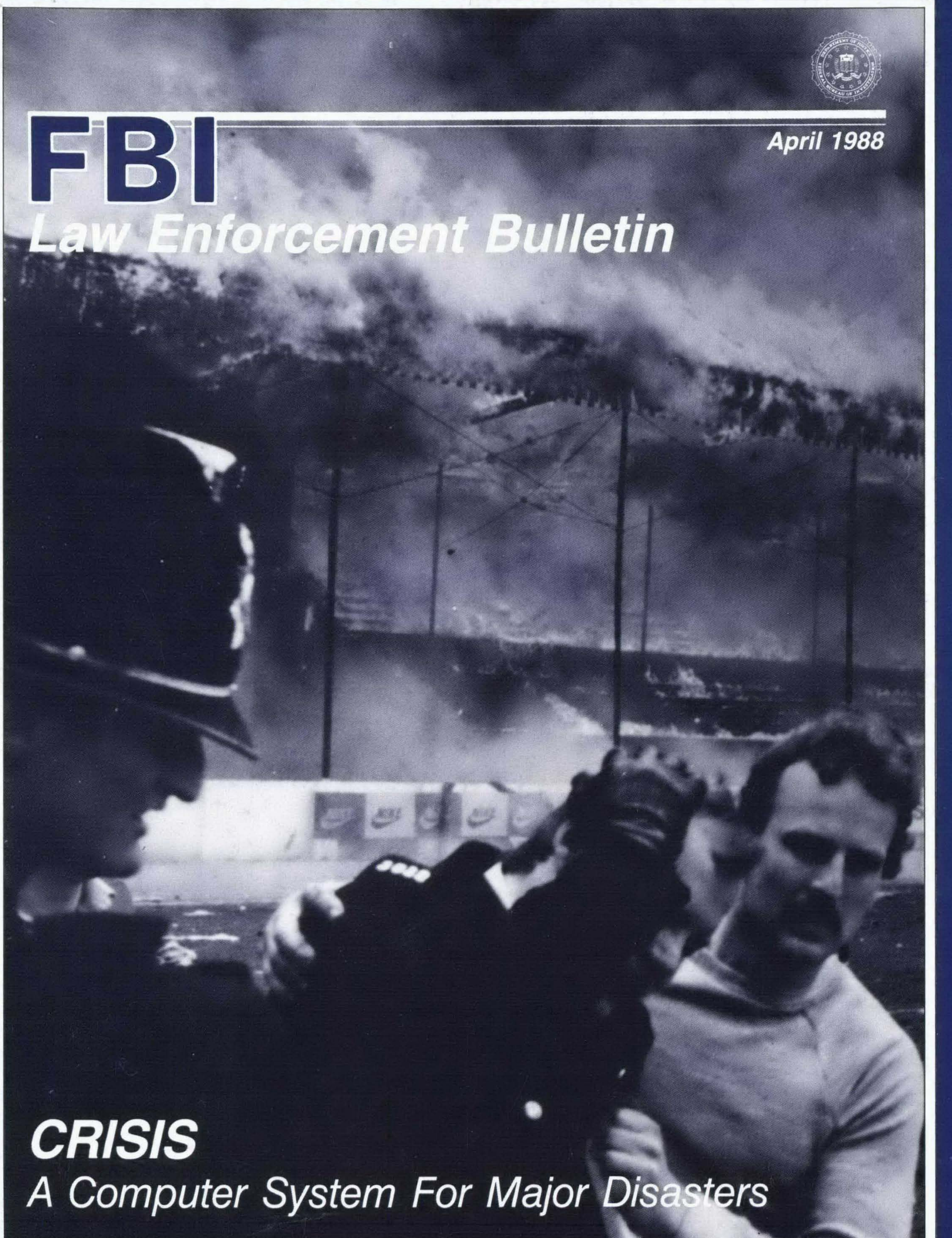


FBI Law Enforcement Bulletin

April 1988

CRISIS

A Computer System For Major Disasters

Contents

April 1988, Volume 57, Number 4

FBI

Law Enforcement Bulletin

United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535

William S. Sessions, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Congressional and Public Affairs,
Milt Ahlerich, *Assistant Director*

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—John E. Ott
Production Manager/Reprints—David C. Maynard

The Cover:

The May 11, 1985, fire disaster at England's Bradford City football ground prompted the creation of the CRISIS computer system. (See article p. 8).

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-Class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.

ISSN 0014-5688 USPS 383-310

Director's Message

May 1988, is the 27th anniversary of President John F. Kennedy's approval of the law designating May 15 as Peace Officers Memorial Day. The words at Gettysburg of another eloquent, and assassinated, President are appropriate to honor "those who gave their lives that this nation might live."

President Kennedy's predecessor, Dwight D. Eisenhower, had established May 1 as Law Day 3 years before. While the theme of the 1988 Law Day is "legal literacy," one of the purposes of Law Day is to recognize the "support. . . [of] those. . . persons charged with law enforcement." In the decade 1977 to 1986, the FBI's Uniform Crime Reporting system has recorded 875 law enforcement officers feloniously killed. While law enforcement has reduced the 1979 high of 106 officers killed to a new low of 66 officers killed in 1986, this is still an unacceptable number, both in terms of the human tragedy involved and in sheer economics.

It is the duty, and the even greater moral obligation, of every law enforcement chief executive to see that the officers in his or her command have the very best training and equipment available to protect themselves in potentially deadly situations. Two of my predecessors, William H. Webster and Clarence M. Kelley, recognized and advocated the use of ballistic vests and training in night use of firearms. "The decline in officers killed is partially a result of technology, the development of Kevlar, the ballistic fiber used in soft body armor," according to FBI Director Webster, writing in this journal. Ten years before, Director Kelley pointed out that nighttime "and dimly lit situations predominate the encounters that prove fatal to law enforcement personnel." For this reason, the FBI then placed greater emphasis on training for these potentially dangerous nighttime encounters.

The loss of 875 officers in a decade is, and should be, sobering to every citizen. This represents more peace officers than all but the largest communities in this country have on their rolls—it is just under the size of the largest police department in Virginia, for example.

The man who led the FBI's efforts to successfully end the gangster era's bloody reign of terrror, J. Edgar Hoover, noted in one of the first Law Day messages, "The effectiveness of law is measured by the fairness, determination, and courage with which it is enforced. . . .Our society demands of the peace officer spotless integrity, uncommon bravery, and constant devotion to duty. It is fitting that Americans pause during the year to acknowledge a debt of gratitude to those who have been faithful to their trust."

It is also fitting that the law enforcement community, represented by 15 law enforcement organizations ranging from the International Association of Chiefs of Police and the National Sheriffs' Association to the Fraternal Order of Police and the National Organization of Black Law Enforcement Executives, has organized the National Law Enforcement Officers Memorial Fund to build a memorial to the thousands of officers who have given their lives to protect their fellow citizens since our Nation began.

I wholeheartedly support this memorial. As I said at the recent dedication of the FBI's Hall of Honor for fallen Special Agents, ". . .they could have chosen professions that paid far more, demanded much less, and presented few dangers. Instead they *chose* to carry the badge . . . and accepted the responsibility to do their duty." The same words of tribute apply to every peace officer in this land of ours built on the rule of law.

William S Sessions

William S. Sessions
Director

Law Enforcement Administration
Yesterday—Today—Tomorrow

". . . the present-day top law enforcement administrator is thinking ahead, moving with the times, and is sensitive to the changing role of the law enforcement agency in the community."

By
JAMES H. EARLE, Ph.D
Special Agent
Federal Bureau of Investigation
Denver, CO

Over the past 2 centuries, the United States has changed from a rural, economically concentric society to a Nation characterized by diverse social, economic, and political units. Some of the institutions upon which society must depend for order and continuity have not been able to keep pace with the changes. The law enforcement system, in particular, is struggling to keep abreast of the present, while trying to determine what the needs of the future will be and how they can best be met.

Law enforcement personnel agree that tomorrow's law enforcement administrator (LEA) will be operating in a highly charged, complex environment. Factors such as rising crime rates, increased population, social unrest, more sophisticated crimes, and accelerated administrative costs will challenge the LEA to reexamine traditional police methodologies and management techniques. The administrator will be held accountable for much greater efficiency, productivity, and effectiveness.

The law enforcement administrator will have to discard the role of "top cop" and become a true chief executive officer (CEO), with responsibilities paralleling those of top corporate management officials. To those responsibilities, however, will be added a task not shared by business executives—the burden of maintaining order in the community.

In the past, and even today, law enforcement administrators have tended to play "administrative catch up." They have reacted to problems rather than anticipating them. This is a luxury they will no longer be able to afford. The 21st-century administrator will have to be a forecaster and long-range planner in order to run a professional department. No longer will he or she be able to function in a response mode. It will be critical to be ahead of events if the department is to function effectively.

To make this shift in focus, the LEA will have to change attitudes toward the requirements for being a top management official. In the past, the conventional wisdom has decreed that experience as a police officer was the major criterion for assignment to top law enforcement positions. This no longer holds true. A top administrator will, of course, build on the foundation

Special Agent Earle

of solid law enforcement experience, but education and specialized training in modern managerial skills and techniques must be added to this experiential base.

The President's Commission on Law Enforcement and Administration of Justice Report of 1967 cited critical areas of competence managers should possess. These were management by objectives, planning, programming and budgeting systems, operation research, and information systems. This knowledge was considered the minimal acceptable level of management expertise for anyone assuming a key position in law enforcement.

Are present-day law enforcement administrators responding to this challenge to grow from a responder to a predictor and planner? To investigate this question, the writer conducted a study in 1979 in which top law enforcement administrators in communities of over 250,000, with 300 or more sworn officers, were surveyed and asked to rank their current managerial problems and to predict what the major managerial problems would be during the next decade.

In the 1979 study, 120 administrators were sent questionnaires; 85 were completed, a very good rate of return of 71 percent. The demographic distribution of the respondents is presented in figure 1.

Each participant was asked to respond to a 57-item, 6-section questionnaire. A five-point rating scale, ranging from "very important" to "not at all important," was used. Results were summarized in rank order tables using the percentage of highest response to determine the rank order. Participants were asked specifically to rate the importance of 11 managerial factors in terms of (1) their importance in the LEA's current responsibilities, (2) their probable importance to an LEA in the next decade, and (3) what knowledge and skills they believed the LEA of the future should possess.

In the 1979 study, the top five current management/administrative problems faced by respondents were:

1) Determining policy and program priorities (62.4%),
2) Administering the budget (56.5%),
3) Maintaining effective community relations (52.9%),
4) Developing effective working relations with elected or appointed public officials (e.g., police commissions, city managers, and city councils) (50.5%),
5) Establishing and administering personnel systems and procedures, including recruitment selection, training, and discipline of key employees (47.1%).

The respondents predicted the major future problems would be:

1) Administering the budget (69.4%),
2) Maintaining effective community relations (68.2%),
3) Determining policy and program priorities (62.4%),
4) Developing effective working relationships with elected or appointed officials (50.6%) and negotiating with employee unions and other employee groups (50.6%),

"The problems law enforcement administrators are meeting today are the ones they predicted they would be facing less than a decade ago."

5) Establishing and administering personnel systems and procedures, including recruitment selection, training, and discipline of key employees (44.7%).

The 1979 responses suggested that LEA's did not perceive their current management problems to be temporal in nature, but were fundamental problems which would loom even larger in the future. The top-ranked problems remained the same, although their position in the rank order changed slightly and there was a tie for fourth place. Although policy and program priorities dropped from first place in the current 1979 rank to third place in the future rank, it maintained the same percentile rating of 62.4 percent.

The attention of the LEA's was focused on relationships, with maintaining effective community relations a major concern. This was a plus for the administrators and their predictive abilities, inasmuch as current professional observers of the field of law enforcement consider the law enforcement agency's relationship with the community to be the single most important element of law enforcement administration in the future. Participants concluded that the problems they faced today would not change with time, but that their focus might be different.

The purpose of the 1987 study, therefore, was to determine how accurate the LEA's predictions were and what changes in importance, if any, occurred as a result of the passage of time.

In the followup study, those 85 departments which responded in the 1979 survey were again surveyed. The response to this questionnaire was 70, an 82-percent rate of return.

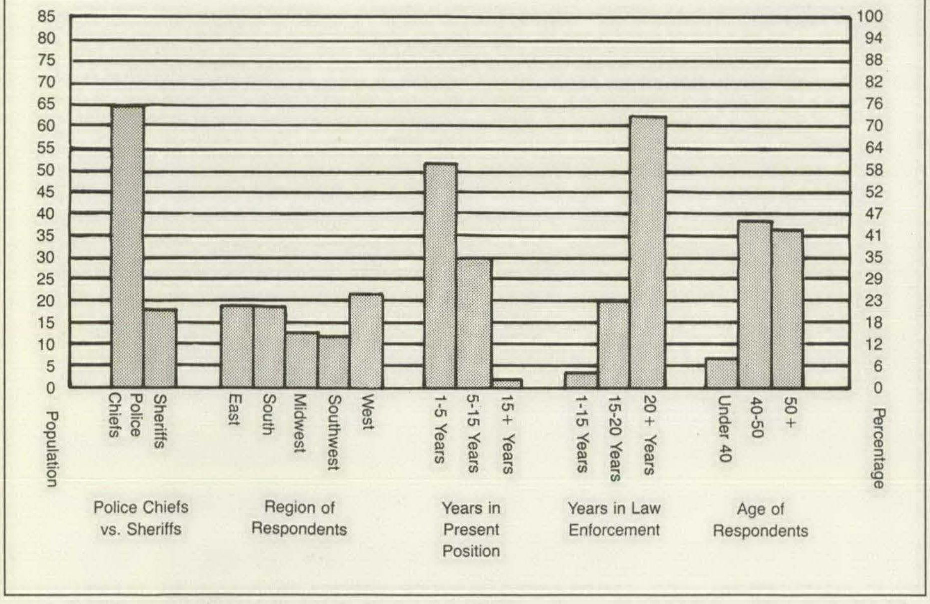
For the second study, the participants were sent questionnaires with the same factors and rating options that were in the first survey. In the second study, however, the sections on knowledge and skills were omitted. It was believed that if the results of the second study paralleled those of the first study, the data obtained from the original responses as to knowledge and skills would be valid for the second study. If, however, the results were markedly different, a separate, followup study of the knowledge and skills required would be conducted using the new base information. Essentially, however, the purpose of the second study was to determine how accurate the LEA's predictions were and what changes in importance, if any, occurred as a result of the passage of time.

As evidenced by the 1979 study, law enforcement administrators did not foresee any changes in the types of problems they were facing over the next decade. The result of the second study confirm this assessment.

In the current study, regardless of a factor's final rank order placement, every management factor listed was ascribed a degree of importance by at least 92 percent of the respondents. While the comparison presented in this article is limited to the five factors which garnered the highest number of "very important" rantings (no. 5), it should be noted that a large percentage of responses centered on the "important" and "moderately important" ratings (nos. 3 and 4). For example, factor I (which ranked 11th overall) in the 1979 rank order of responses (fig. 2) had a

Figure 1

Summary of Demographic Data



combined strength of 74 percent in ratings 3 and 4, although only 18% gave it a 5 rating. Therefore, it is important to remember that even if a factor did not make the top five in importance, it usually had a relatively high percentile average in the 3 and 4 ratings.

The five top rated factors in 1987 were practically the same as those rated in 1979. (See fig. 3.) There was a slight shift in position for policy/program priorities and official relations and personnel systems, but it was so slight as to be insignificant. The only change from the predicted future problems of 1979 was the negotiating with employee unions which was not ranked as high in the current survey. However, establishing and administering personnel systems was listed in all rankings, and it is conceivable that some of the concern for union negotiations was included in that category. Additionally, a comparison of the rank order of factors in 1979 with those of the 1987 study shows a shift of only 1 or 2 positions in the lower half of the rank order. The problems law enforcement administrators are meeting today are the ones they predicted they would be facing less than a decade ago. They also predict that they will continue to be facing these same problems in the future, although perhaps in a different societal climate.

Figure 2

1979 Management Problems
Percentile Distribution of Responses

Factor	1	2	3	4	5
A. Administering the budget	2%	2%	5%	23%	69%
B. Developing effective working relationships with elected or appointed officials (e.g., police commissions, city managers, city councils)	1%	—	9%	36%	54%
C. Determining organization structure	1%	6%	29%	39%	25%
D. Determining policy and program priorities	—	—	15%	29%	56%
E. Establishing and administering operating systems and procedures	—	3%	15%	37%	35%
F. Establishing and administering personnel systems and procedures, including recruitment selection, training, and discipline of key employees	—	7%	7%	42%	49%
G. Directing and administering program operations under emergency conditions—in politically sensitive situations	—	1%	17%	43%	39%
H. Developing cooperative relationships with other law enforcement agencies at Federal, State, and local levels	—	6%	19%	47%	28%
I. Negotiating with employee unions and other employee groups	1%	7%	35%	39%	18%
J. Maintaining effective relations with representatives of the media	—	5%	28%	39%	28%
K. Maintaining effective community relations	—	3%	4%	27%	66%

Code: 1—Not at all important
2—Not important
3—Moderately important
4—Important
5—Very important

In addition to the problems presented in the questionnaire, the respondents were asked for comments and/or to list additional problems not covered in the survey.

One administrator rated EVERY factor at the 5 level—very important—and returned the survey with an item-by-item analysis describing the reasons behind the rating. This respondent remarked, "The force views the foregoing administrative/managerial concerns as key building blocks for our future development as an efficient and effective police force, and thus, the future importance attached them is expected to remain unchanged."

In another instance where the respondent had listed "administering the budget" at the 3 level—moderately important—his comment was, "It should be noted that the makeup of the department budget and control over it are political administrative endeavors controlled by special sections of the city government, not the police department. From the managerial aspect of running the operations of a police department, this is not desirable, but nevertheless, it is the historical practice." It should be

"... current LEA's believe the role of tomorrow's chief law enforcement administrator will be complex and challenging."

noted that this officer elevated his responses to the factors of official relationships, organization structure, policy priorities, and administering operating systems and procedures to top ratings, an assessment consistent with his problems with the budget as noted in his comment. Certainly, in such a situation, it would be necessary to apply the highest level management skills to the resolution of difficulties between other departments and the police department.

Other respondents commented on how the special situations would influence which factors would be most important, e.g., a force whose major police activities center on drug traffic would have different priorities from one whose problems center on offenses such as burglary, assault, gang violence, etc.

There was a clear consensus, however, that the factors presented in the study were true problems, representative of all types and levels of law enforcement administration. There was no evidence presented that the LEA's did not recognize that their roles require top-level management education and experience.

Figure 3

1987 Management Problems
Percentile Distribution of Responses

Factor	1	2	3	4	5
A. Administering the budget	1+%	1+%	1+%	18%	77%
B. Developing effective working relationships with elected or appointed officials (e.g., police commissions, city managers, city councils)	1%	—	5%	40%	54%
C. Determining organization structure	4%	3%	28%	42%	23%
D. Determining policy and program priorities	—	—	11%	41%	48%
E. Establishing and administering operating systems and procedures	1+%	1+%	25%	40%	32%
F. Establishing and administering personnel systems and procedures, including recruitment selection, training, and discipline of key employees	—	—	9%	42%	49%
G. Directing and administering program operations under emergency conditions—in politically sensitive situations	—	3%	18%	43%	36%
H. Developing cooperative relationships with other law enforcement agencies at Federal, State, and local levels	—	5%	21%	46%	28%
I. Negotiating with employee unions and other employee groups	1+%	1+%	30%	38%	29%
J. Maintaining effective relations with representatives of the media	—	1%	24%	38%	37%
K. Maintaining effective community relations	—	1%	8%	25%	66%

Code: 1—Not at all important
2—Not important
3—Moderately important
4—Important
5—Very important

One interesting result of the 1979 study was the very sophisticated assessment of the LEA's as to the knowledge and skills that would be required of them at that time and in the future. Inasmuch as that knowledge and those skills were directly related to the 1979 response—answers which have been confirmed in the present study—they are valid as accompaniments the current results.

Respondents placed a great deal of emphasis on acquiring knowledge in the relationships that govern society. They believed they needed to understand the political climate in which they worked, have knowledge of legal responsibility, understand causes of major urban problems, and have knowledge of theories of human behavior and knowledge of values underlying the behavior of people in urban situations and of their institutions. They recognized the need to know the principles of financial management, principles of governmental planning, policy analysis, and personnel administration, including labor negotiations.

At the skill level, they placed great emphasis on acquiring skills in assessing community needs, handling interpersonal relations, problem solving and planning, delegation of authority, and understanding minority, disadvantaged, and culturally distinctive groups. While they recognized the need for technical skills, such as systems design, written communications, job analysis, and operations analysis, it appeared from the low ratings given these technical items (and from the comments) that they believed the day-to-day handling of such matters would be a staff function. They were aware, however, of the need to understand the fundamental principles of these technical functions. They concluded, however, that a top law enforcement administrator should be much more concerned with the larger issues of community effectiveness and human relations, plus the efficient management of the department.

It is the belief of the writer that these perceptions, set forth 8 years ago and confirmed in 1987, show clearly that the present-day top law enforcement administrator is thinking ahead, moving with the times, and is sensitive to the changing role of the law enforcement agency in the community.

In the original study, one of the respondents observed, "Executives must be developed whose minds are able to think in terms of the future, able to synthesize great amounts of data, make decisions of complex matters, have broad, even national, perspectives, and be able to see the organization as a whole as it exists within society."

The information obtained in both studies has shown that current LEA's believe the role of tomorrow's chief law enforcement administrator will be complex and challenging. They stressed that new demands will be placed on these administrators from the communities which they serve and the environment in which they work. The chief LEA will become a manager of a varied and demanding organization, one which will call upon all the knowledge and skills that he or she can muster.

FBI

Book Review

Kelley: The Story of an FBI Director by Clarence M. Kelley and James Kirkpatrick Davis Andrews, McMeel & Parker, publisher, 4900 Main Street, Kansas City, MO 64112 $17.95, 315 pages.

A career FBI executive who modernized the Kansas City, MO, Police Department as chief, and then led the FBI at its most tumultuous time, tells his story of police and law enforcement professionalism.

As the foreword by former Attorney General Elliot L. Richardson notes, one of the most important facets of Kelley's leadership of the Kansas City Police Department and of the Federal Bureau of Investigation was the man's character. In the 1960's, police departments around the Nation were wracked with corruption, not the grafts from vice enforcement of earlier years, but outright lawlessness in the form of burglary rings.

Strong, incorruptible leadership was required at the top, for only by example could police leadership set the tone for any department. Kelley had this character, installed in him in childhood and reinforced by two decades of service as an FBI Agent. It served him well in Kansas City. But, as important were two other characteristics: Kelley's willingness to innovate and his style of participatory management. He brought all three character traits to the FBI as successor to J. Edgar Hoover as Director and reshaped the FBI in important ways.

Kelley's record as Chief of Police in Kansas City in the 1960's was evidence of the new trends in law enforcement professionalism that have become standard two decades later. Innovative use of technology, including computers and helicopters, enlightened treatment of minorities, including minority recruitment into the department, and more advanced training of onboard personnel. Cooperation with the Police Foundation in the landmark Kansas City Preventive Patrol experiment again presaged the future of police professionalism.

Kelley again brought his integrity, commitment to participatory management, and willingness to innovate to his leadership of the FBI and was able to restore the morale of this agency, shaken as it was by the disclosures of abuses of power that characterized the last years of J. Edgar Hoover's tenure. His book provides an historical perspective on the FBI and the last years of the Nixon administration. Probably his most important contribution to FBI organization was the establishment of innovative investigative priorities for an organization that had depended on fines, savings, and recoveries statistics for many years to justify its existence to the Congress and to the American people.

Kelley started the FBI on the road to recovering its reputation as the finest investigative organization in the world. Students of law enforcement history will be grateful for Kelley's frank, but self-effacing account of his years in law enforcement.

SA Thomas J. Deakin, J.D.

CRISIS
A Computer System For Major Disasters

". . . CRISIS suggests matches and lists evidence . . . it is up to a team of experts to review the case and to agree or disagree with the suggestions."

By
MARK RAND
Chief Superintendent
Kirklees Division
West Yorkshire Police
Castlegate, Huddersfield, England

On May 11, 1985, a fire swept through the crowded main stand at Bradford's Valley Parade football ground, killing 56 people and seriously injuring many more. The event was seen worldwide on television, and in an instant, West Yorkshire Police found themselves inundated with telephone inquiries from anxious relatives.

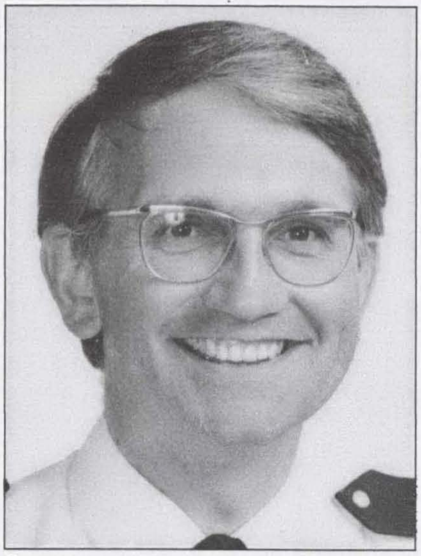
Hardly had the flames died when there was an outcry for answers to the cause of such a bizarre disaster. Foul play was the early suspicion, and a murder inquiry was soon launched. Then there was the gruesome, and at first sight, impossible task of identifying the victims.

After a meticulous and massive investigation, the cause was determined to be nonmalicious. This finding was aided by the use of MICA (Major Incident Computer Application). This system has since evolved into HOLMES (Home Office Large Major Enquiry System) which is nowadays the mainstay of murder inquiries. That left two key areas of police activity for which no computer program had been designed—the work of the Casualty Bureau and the identification of victims.

Casualty Bureau

Police assigned to the Casualty Bureau assemble lists with the names of injured, missing, and deceased individuals, as well as those who are unharmed. They also handle the vast number of telephone inquiries which any major disaster generates. The Bradford fire, unlike an air disaster, was an open incident in that there was no passenger list or its equivalent. A telephone number circulated worldwide on news bulletins resulted in numerous calls being placed to the Casualty Bureau. The lines were quickly jammed with callers. The standard documentation for the Casualty Bureau then in use required callers making a missing person report to answer at least 23 questions over the telephone. These questions sought descriptive details of the missing person and his or her clothing.

Such questioning, however, has four unwanted results. First, data acquired in this manner tend to be inaccurate. (The reader would be hard pressed at this moment to describe accurately his or her immediate next of kin, including clothing). Second, callers who are asked to provide such descriptive details begin to fear the worst.



Superintendent Rand

Third, the more details which are sought the longer the conversation, the greater the delay for other callers trying to reach the bureau. Finally, the stress to Casualty Bureau operators increases with the complexity of their task.

Casualty Bureau personnel also have to collate the information of those who were actually involved in the disaster. Documentation teams are sent to the hospitals (five in the case of the Bradford fire) to complete standardized forms of similar complexity. The completed documentation is sent to the Casualty Bureau, hopefully to be matched with missing person reports.

Identification

An early decision was made at Bradford to allocate one police officer to each dead body. That officer was instructed to visit the temporary mortuary to which the body had been removed, examine the body and its associated property, and then accompany it to the autopsy, taking copious notes throughout. With this procedure, it was believed that the officer would have the best possible description of the body in question, although in many cases that description was limited to gender, a crude estimate of height, and at times, a brief list of property.

Recovery of bodies from the scene had been meticulously documented. In no case was visual identification remotely possible, and for some, all dental evidence had been destroyed by the fire. The officers charged with this grim task then returned to the Casualty Bureau to embark on the process of comparison, elimination, and trial and error so that the most likely set of relatives could be confronted with remnants of clothing and metal objects which had survived the fire. Meanwhile, other officers had to skillfully and sensitively question relatives of those most likely to be among the dead to gather a more accurate description than the one obtained over the telephone. Figure 1 shows the methods used and their relative degrees of usefulness given the unique circumstances applying to Bradford. After 72 hours, all the dead had been identified, a remarkable result given the formidable task.

Computer Assistance at Bradford

As has already been mentioned, computer technology had been used to assist with the criminal side of the inquiry. While the Casualty Bureau was still frantic with activity, a program based on MICA was devised by the West Yorkshire Police Computer Unit in an effort to assist with identification. In theory at least, the task of matching detailed descriptions of missing people with detailed descriptions of dead bodies should be capable of computerization. Despite its hasty conception and execution, the program enabled a multitude of facts and figures to be assembled. In at least two cases, the computer was actually able to help officers identify a particular body. The only documents needed for the opening of the coroner's inquest were the computer printouts detailing in a common format the case for identification of each body.

The Development of CRISIS

The application of the computer to the aftermath of the Bradford fire produced sufficiently encouraging results to take into consideration the idea of a computer program written purposely for disasters. A small team was assembled to look at the options. This team was motivated by the Bradford experience

"[CRISIS] has the capability whereby the parameters for comparison can be varied to suit the circumstances of the disaster."

Fire breaks out at Bradford City football ground.

and a determination that something positive should, if possible, come out of the tragedy. The likelihood of West Yorkshire Police having to deal with another peacetime disaster in the future was remote, and therefore, a program specification must have wider relevance, especially since it was determined that no comparable program existed anywhere. However significant the Bradford experience, there was a danger that it would distort any computer solution toward that unique scenario. Therefore, the development team consulted with officers who had more experience in the field of disasters. In particular, advice was obtained from the Royal Air Force, British Airways, and Kenyons, London undertakers who have tended disaster victims since the 1920's.

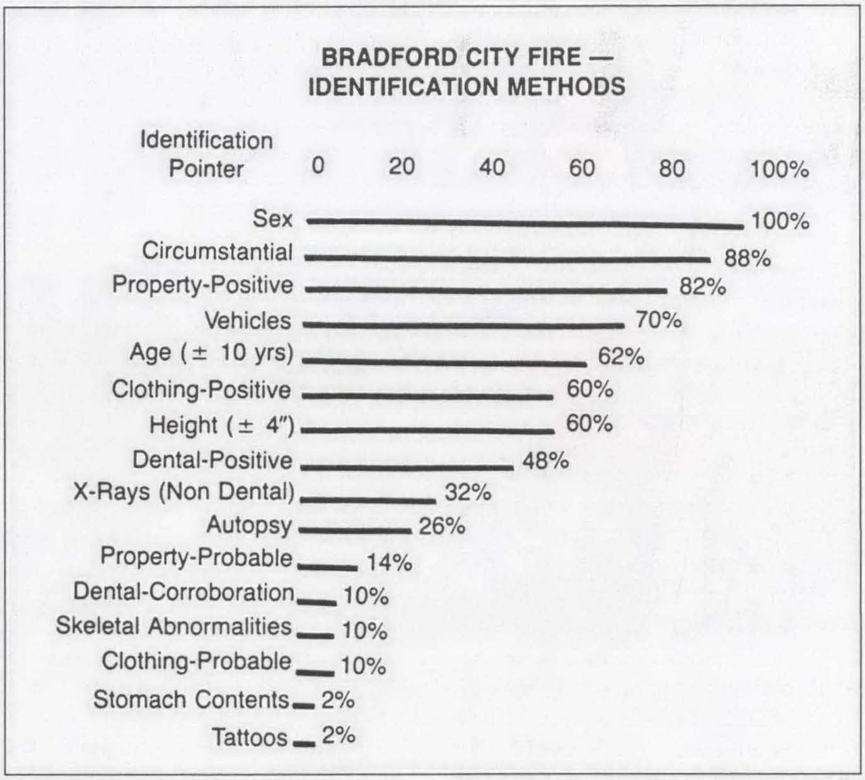
The procedures of London Airport's Emergency Procedures Information Centre (EPIC) were also noted, since it is probably one of the most frequently tested and tried systems. Significantly, this system does not concern itself with personal descriptions for the very reason identified earlier. The EPIC documentation system seemed to be a sound basis for general use and on which to base the Casualty Bureau's aspect of CRISIS.

From the beginning, one thing was perfectly clear. Any program developed had to be sufficiently user-friendly to enable untrained staff to use it. Experience has shown this to be the case with CRISIS. Every field had behind it a "HELP" screen, whereby the operator needs only to press the key to get simple instructions to resolve any uncertainty.

West Yorkshire Police's Casualty Bureau is now fully computerized with CRISIS. Any caller reporting a missing person is asked to give only basic details such as name, address, date of birth or age, and the reason why the caller thinks that the missing person may be involved in an accident. As soon as the name is entered into CRISIS, an automatic search takes place and a list appears on the visual display unit of all those having that or a similar sounding surname who are already reported missing or listed as casualties. Callers are given a number to call in the event that the missing person should return, thereby enabling CRISIS to be quickly updated.

As a computer application, the Casualty Bureau is relatively simple; identification is a more complex problem. The CRISIS development team initially had to find adequate and widely acceptable documents. INTERPOL provided the answer, because in 1968, it produced Disaster Victim Identification (DVI) forms. For air disasters, in particular, it is vital that police forces everywhere use the same forms when obtaining full descriptions of missing persons and dead bodies. INTERPOL has since produced a comprehensive manual on identification. This system had been used successfully as a paper-only method in many international disasters, notably jumbo jet crashes at Mount Erebus, Antartica (1979), Mount Fuji, Japan (1985), and Shannon, Ireland (1985). INTERPOL is presently reviewing its DVI forms in the light of these and other experiences. Nonetheless, it was clear that CRISIS had to be capable of using the INTERPOL forms as its input documents.

Essentially, CRISIS absorbs detailed descriptions of missing persons and dead bodies and then compares them. The vague nature of the ante mortem information, in particular, makes it essential that CRISIS does not eliminate the apparently impossible on



BRADFORD CITY FIRE — IDENTIFICATION METHODS

a particular characteristic. It has the capability whereby the parameters for comparison can be varied to suit the circumstances of the disaster. Thus, for a fire, height and weight may not be too relevant, and a wide variation can be pre-set.

Dental chartings are compared by CRISIS using the Federation Dentaire Internationale (FDI) system of dental charting. This is the INTERPOL standard and the one which is becoming the most widely used of the six or more main dental charting systems. When ante and post mortem data are entered, CRISIS will suggest the more likely matches in descending order of probability. For physical features, such as height, weight, eye color, etc., the system lists these characteristics as "hit" or "miss" within the set parameters for the disaster. On dental matchings, it shows a mathematical match on an arbitrary points scale. It will also print out graphics of the chart for expert scrutiny.

One thing must be clear—CRISIS suggests matches and lists evidence. Thereafter, it is up to a team of experts to review the case and to agree or disagree with the suggestions. The computer can only be as good as the information entered into it. Even ante mortem dental charts have been found to be less than totally accurate. CRISIS goes some way to compensate for this by not eliminating the apparently impossible. Thus, a tooth shown on an ante mortem chart as extracted but which is very definitely present on the dead body is not rejected in the matching process. The system also accepts the fact that ocassionally, dentists have been known to make mistakes. Even so, there comes a point where the computer cannot replace human guile, intuition, and experience.

Besides the matching processes described, there is an English search facility whereby the entire data base can be searched for RED garments or individual BANK CARDS in an effort to do rapid matches on individual bodies when compared to the missing and unidentified persons.

Another large element of CRISIS is its administration package. Such mundane, though important, matters as records of employee hours worked, costs, and statistics can be entered for documentation.

Overall, CRISIS is a powerful computer system (between 0.5 and 8.0 megabytes of memory and 1 to 408 terminals connectivity) capable of bringing order to the chaos of disaster and speeding up the necessary processes of the Casualty Bureau and identification. It was tested using data from the Bradford fire and from the Manchester air disaster (August 1985) in which 54 people died when a Boeing 737 airliner caught fire on take-off.

Zeebrugge

On the evening of March 6, 1987, the Townsend Thoresen roll-on/roll-off car/passenger ferry, "Herald of Free Enterprise," left Zeebrugge in Belgium for its home port of Dover. It is now known that the ship's bow doors were open as it gathered speed. Not far past the outer harbor wall at Zeebrugge the ship capsized. It was carrying some 550 passengers and crew and its vehicle decks were laden. By far, the majority of those aboard were British, and

"CRISIS has proved to be a powerful tool for use in major disasters."

of those, the majority were from the southeast of England, Kent in particular. The disaster was clearly in Belgian waters, but the main focus was in Kent. Kent police very quickly set up a manual Casualty Bureau at their Maidstone headquarters and dispatched a number of officers to Zeebrugge.

In very much the same way as at Bradford, this was an open incident. There was no passenger list and it remains to this day impossible to say precisely how many people were on board the vessel. West Yorkshire offered CRISIS to Kent police for what seemed initially to be a straightforward, if tragic, application. In any event, West Yorkshire officers were in Kent and Zeebrugge for the next 64 days, so long was the recovery operation.

Two important decisions were made early. First, it was accepted that CRISIS would not be used in its Casualty Bureau role because of the time factor. Second, it was clear that CRISIS was under a test and would run in parallel with Kent's manual identification system. In fact, CRISIS came to be relied on more and more as the days progressed, but it would have been foolhardy in the extreme to rely from the outset on the then untried system. A key factor in the decision to use CRISIS at all came from Belgium where the Gendarmerie, charged with the identification task, were using the INTERPOL system—the very system on which CRISIS is based.

There has been much ill-informed and insensitive criticism of the efforts which were made to produce an accurate list of casualties and survivors. Heroic efforts were made by several agencies in Belgium to produce accurate lists but language differences, coupled with the urgency of the rescue need, conspired toward duplication and confusion. The resulting data had to be regarded with caution, and despite the earlier decision not to use CRISIS in the Casualty Bureau role, its facilities were in fact used to assist.

It was in its identification role that CRISIS was put to a rigorous test. As they were recovered from the ship, bodies were taken to Zeebrugge Naval Base where every detail of the physical description, property, and clothing was recorded by Gendarmerie officers onto INTERPOL forms. Bodies were also photographed and fingerprinted. The forms were completed in Flemish and faxed to Maidstone from Zeebrugge. As a precaution, copies were also sent on the overnight ferry to Dover. A similar process took place in reverse; the night ferry from Dover brought completed ante mortem forms for the Gendarmerie.

Thus was set up a parallel identification operation in England and Belgium with a mutual and total sharing of information. Interpreters translated the forms into English. After the recovery of 53 bodies, it became clear that the risk to the divers was such that no more bodies could be recovered safely until the ship was brought upright. That process took several weeks, during which there was time to take stock of identification procedures. While the bodies initially recovered were suitable for visual identification, it seemed obvious that as time passed, the other bodies would be less readily identifiable. As soon as the first 53 bodies had been identified, the CRISIS forms were themselves translated into Flemish. Thereafter, all of the 135 bodies later recovered were documented in English by the Gendarmerie onto CRISIS forms. All the documents were faxed to England for assimilation into the manual system and into CRISIS. For operational reasons, the Identification Bureau was moved to the Dover police station.

It was possible during the course of the incident to modify and improve the computer programs. A property index was written to handle the large amount of identifiable property recovered from the seas around the Herald of Free Enterprise; passports in particular were entered in this index. More importantly, dental charts were put into CRISIS at Dover by a small team of odontologists who encoded ante mortem dental charts obtained from British dentists and the post mortem chartings faxed across from Zeebrugge. All of the recovered bodies have been identified.

Conclusion

CRISIS has proved to be a powerful tool for use in major disasters. It is capable of being used by a staff who, though familiar with computers in a general way, are not necessarily conversant with CRISIS. After minimal training by West Yorkshire officers, the system was used most proficiently by Kent policemen who, before the disaster, had no knowledge whatsoever of CRISIS. The system is simple, yet effective, and a number of police forces in the United Kingdom and elsewhere are installing it. Further details on CRISIS can be obtained from:

ISIS Computer Service
Elton House
12 Gloucester Road
Bishopston
Bristol
Avon, BS7 8AE
Telephone: (0272) 428191
Telex: 449071
Fax: 425752

A Terrorist Psychosocial Profile
Past And Present

By
THOMAS STRENTZ, Ph.D
Special Agent
Behavioral Science Instruction and Research Unit
FBI Academy
Quantico, VA

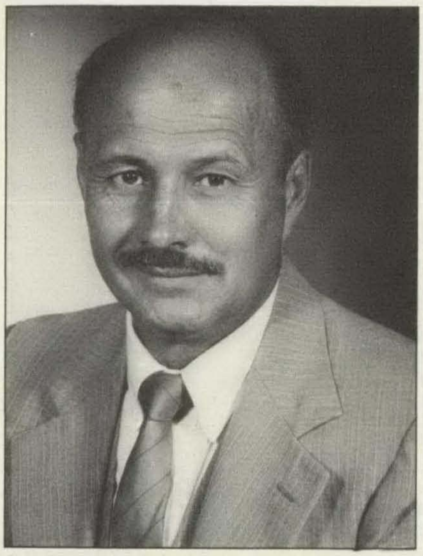
As we grow older, so I am told, we tend to think and talk more of the simplicity of the good old days and begin to realize that according to the country western ballad, life does get more complicated when you pass the age of 16.

This article presents one aspect of law enforcement which was less complicated, or at least more clearly structured, several years ago. I will present my interpretation of how terrorist groups were constituted then and will cite the structure of the Symbionese Liberation Army (SLA) as a domestic example. I will use the Japanese Red Army (JRA) as an international model and discuss their hijacking of Japan Air Lines (JAL) 472 as an example of their success and terrorist sophistication of days gone by. After laying this foundation, I will cite some of the changes in the terrorist group structure.

The pool of potential college-educated, multilingual, middle class, and sophisticated international terrorists has been depleted by civil war and revolution. The universities and other centers of learning from which recruits were drawn have been replaced by refugee camps and criminal street gangs. Within the United States, the recruiting by the left was affected by the end of the draft and U.S. withdrawal from Vietnam. Today, the issues are problems in Central America and prison reform. These issues have less appeal and have resulted in a narrower base of support. However, the right-wing radicals have gained some ground in the Midwest and Northwest. Examples of terrorist operations reveal something about how terrorist personalities and their politics affect their group structure and the mechanics of each operation. Additionally, some thought will be given to the radicals on the right, like the Aryan Nations and the Ku Klux Klan. For the sake of clarity, the terms "left" and "right" refer to groups of opposite political ideals. Left-wing groups oppose the legitimate government and seek change; they deny the authority of the government. Those on the right want to maintain the status quo and oppose those who seek change; they deny the legitimacy of the opposition.[1] Finally, I will provide you with some thoughts on the myth of contemporary suicidal terrorist dedication as evidenced by several recent events.

One Week In London

The changes in the demographics of the left, particularly with Middle Eastern groups, came to our attention in the late 1970's and were dramatically manifest to the world in the spring of 1980 during the Iranian Embassy siege. This 6-day hostage situation in the Iranian Embassy, near Hyde Park in London, was caused by terrorists who were dissidents from Khuzistan, a province they call Arabistan, in southwest Iran. The Khuzistans had expected to gain some degree of autonomy after the overthrow of the Shah. Instead, the persecution increased. Iraq used their hatred of the central government in Tehran and frustrations over their lack of progress toward autonomy to recruit them for an operation against an enemy upon whom they would soon declare war. These terrorists were ill-trained and misled into believing they would succeed



Special Agent Strentz

in freeing friends from Iranian jails and would return to their homes as heroes. These frustrated few citizens from Khuzistan have been characterized as immature, rural, ill-trained, and uneducated young men who had no idea of the complexity and gravity of the operation they had initiated. Simply because they were well-armed, they quickly took control of the embassy. However, an alarm was automatically sounded, and these terrorists were quickly trapped within the embassy without any help from their alleged allies in Iraq and Iran.

After 6 days of negotiations by Scotland Yard, the stress of the siege took its toll, and the terrorists killed one hostage, the youthful press attache, Abbas Lavasani. He had been arguing with the terrorists throughout the siege, and these arguments had become violent. Other hostages had tried to calm Lavasani, but he was adamant in his support for the Ayatollah. Some of the hostages believed he was intent on martyrdom. His overtly antagonistic relationship with the terrorists that led to his murder has given rise to the term "London Syndrome." Today, this term is used to express similar hostage-toward-hostage taker antagonism which results in death or injury to the hostage. The terrorists killed Lavasani around noon on the sixth day and placed his body outside the embassy several hours later. Soon after that, the British Special Air Service commandos assaulted the embassy and rescued the remaining hostages. During this assault, five of the six terrorists died.[2] The survivor, Ali Nejad, hid amongst the hostages during the assault. He remains in a British jail cell from which he regularly provides the free-world counterterrorist forces with a wealth of information.[3]

Subsequent to this incident, our allies in the Middle East and a Special Agent assigned to the Washington Field Office of the FBI, who has interviewed more Middle East terrorists than any other FBI Agent, verified the decrease in terrorist group sophistication. These sources agree that terrorist groups have changed rather dramatically. This new image is also echoed by another FBI Special Agent who lectures at the FBI Academy on the theory and politics of terrorism. Today, terrorist groups, particularly those in the Middle East (but not the Armenian groups, the Jewish Defense League, or the Puerto Rican groups in the United States) are using the young and the naive as their expendable front-line operators. The older group members are more educated and possibly more dedicated. But, they probably recognize that today's counterterrorist strategies and forces, like the German GSG-9, British and Australian SAS, French GIGN, and the Hostage Rescue Team of the FBI, are too sophisticated for them to combat successfully. To challenge these counterterrorist forces in a hostage situation guarantees failure and may mean death, a price they are clearly not willing to pay.[4] We learned in Munich that hostage negotiations and SWAT skills are a necessity. The terrorists learned how unprepared we were then for such a confrontation. For several years, they continued to exploit our weakness. However, times have changed and we have learned from the mistakes at Munich.

Today Versus Yesterday

Terrorism is different today than it was yesterday, and it will, like every dynamic organization, change again by tomorrow. Terrorists learn new tactics

"We [in law enforcement] must be prepared always; the terrorist need to be lucky only once."

and adapt and adjust to countermeasures developed by governments or airlines, or they die and are replaced by more dynamic individuals. One change is that today, terrorist organizations spend less money and time training than in the past. When they do train, it is for a specific operation; therefore, they find it difficult to deal with the unexpected.

A few years ago, several authorities published their research findings on the psychological profile of the terrorist groups the civilized world encountered in the 1970's. One book is that of Frederick Hacker entitled *Crusaders, Criminals, Crazies: Terror and Terrorism in our Time*.[5] Charles A. Russell and Bowman H. Miller wrote an article with a similar message, which appeared in *Terrorism: An International Journal*, and was entitled "Profile of a Terrorist." [6] The last article is one I wrote entitled "A Terrorist Organizational Profile: A Psychological Role Model." This was printed as chapter six in a book entitled *Behavioral and Quantitative Perspectives on Terrorism*.[7] Although each of us was working independently with different data bases, our findings showed a high level of concurrence.

It is because of this level of agreement that I will discuss my article as a historical document which presents what terrorist groups were. To present the profile of left-wing terrorist groups using this 1970 prototype as a guide to current structure and activities would be like teaching someone to start a modern car by discussing the elements of setting the spark, throttle, and choke before turning the crank.

Yesterday on the Left

In the late 1960's and into the 1970's, the majority of American and international terrorist groups were composed of males and females who were flexible, college-educated, well-trained, urban, multilingual, well-traveled, and reasonably sophisticated middle-class young people. (See table 1.) They were disciplined, well-trained, and sophisticated enough to deal with last-minute alterations in plans; they could adjust to change and still complete the mission.

The Japanese Red Army in the 1970's was composed of people like Shigenobu Fusako, Haruo Wako, and Osamu Maruoka who were tactically trained by the then proficient Popular Front for the Liberation of Palestine (PFLP) and were middle-class college students from professional families. Similarly, the German Baader-Meinhoff gang, the media name for this group that called themselves the Red Army Faction, was staffed by college students from good families who were also well trained. Ulrike Meinhoff had earned a master's degree, Horst Mahler was an attorney, and Gudrun Ensslin was the daughter of a Lutheran minister.[8] The Palestinians could claim college types, such as Leila Khaled who, like some of her American counterparts, is now a suburban housewife with a family.[9]

In the United States, the membership of the Weather Underground and the SLA drew heavily from college students who harkened from upper middle-class families.[10] Their operations were well-planned and their training thorough. Further, the demands of these organizations were well-written treatises of alleged injustices; each member knew the political justification for their activities, discussed world politics with arresting officers, and frequently argued their cause in courts of law. Thus, as discussed in the referenced articles and displayed in the chart, the group profile that emerged reflected organizations which were a blend of the highly motivated and well-

Table 1
Demographic Profile of the 1960's and 1970's Leftist Groups

Leader	Opportunist or Criminal Element	Follower
Male or female	Male	Male or Female
No specific race or religion	No specific race or religion	No specific race or religion
College education or attendance	Limited education	College education or attendance
25-40	20-30	20-25
Middle class	Lower class	Middle class
Urban/sophisticated	Urban or rural with good street sense	Urban/sophisticated
Multilingual	Literate in native language	Multilingual
High verbal skills	High verbal skills	Good verbal skills
Well-trained perfectionist	Learned criminal skills	Well-trained
Dedicated	Selfish	Dedicated
Strong personality	Strong personality	Weak personality
Politically active prior to terrorist/criminal activity	Years of criminal activity/recruited from prison/ politics are peripheral	Politically active prior to terrorist/criminal activity

". . . to prevent terrorism, law enforcement must remain vigilant against a persistent but unsophisticated, untrained, and minimally dedicated enemy."

educated members with the involvement of a criminal element.

The leader was a theoretician with a strong personality. Certainly, Ulrike Meinhoff fit this mold. The leader was generally assisted by a more volatile, less moral, more operationally oriented, and frequently a former felon, like Andras Baader. In the United States, this person was at times a former convict, like Donald David DeFreeze in the SLA or Greg Daniel Adornetto in the San Francisco-based Emiliano Zapata Unit. The last element in this old prototype was, like the leader, a college student or graduate but was not quite as strong a personality as the leader. The Harrises in the SLA come to mind as examples. Similar types of zealots are seen in other groups around the world.[11]

There is a lot to be said in favor of this older prototype. Among other things, it enabled law enforcement to view these groups as a collection of individuals who did not always share the same motives, roles, or ideals.

The Japanese Red Army

But that was then and this is now. In those days, when a JRA operation was not initiated because of a security precaution, an unexpected obstacle, or an inability to arrive at a specific location on time, the groups were more likely to reorganize and strike again. The most successful terrorist hijacking of a commercial aircraft was conducted by the JRA in 1977 and is an example of this sophistication. This operation was successful because the JRA demands, $6 million and the release of jailed friends in Japan, were met, and all involved made good their escape. Ten years later, with the exception of the recent arrest of Osamu Maruoko, they are still free, and the money remains missing.

There is some evidence to indicate that in addition to a July 1973, hijacking of a JAL aircraft, the JRA made two other attempts, one in Rome and the other in Cairo, before the 1977 success. At these airports, alert security prevented terrorists from boarding the aircraft. Unfortunately, the JRA plan came together on Tuesday morning, September 28, 1977, when five of them cleared security in Bombay, India, with automatic pistols, hand grenades, and plastic explosives. They boarded the Bangkok-bound flight, and shortly after takeoff, diverted the DC 8 to Dacca, Bangladesh. Enroute, selected passengers were reseated, and specific belongings collected. At strategic times during the week on the torrid tarmac in Dacca, the terrorists returned most of these items and released some hostages. The **terrorists** made announcements to the passengers by using the public address system and speaking Japanese, English, and Arabic. The hijackers were courteous and extremely polite; they were careful not to antagonize their hostages. Passengers and crew were so effectively manipulated psychologically by them that upon release each hostage, at the request of the JRA, completed a critique of their experience and dutifully turned it in as they left the aircraft. The critiques included a review of the strengths versus the weaknesses of the operation, as well as recommendations to the subjects for their next hijacking. In each of their many hostage-taking incidents, the middle-class, college-educated men and women of the JRA were similarly successful. Additionally, their operations reflected a high level of discipline, training, organization, and flexibility.

Today on the Left

Unfortunately, the American media and some elements of the military have fixated on this 1970's prototype. They cite the infamous Illich Ramirez-Sanchez, also known as "Carlos," as the jackal who is said to epitomize modern international terrorism. Ramirez-Sanchez, the assaulter of unprotected targets in the 1970's, has probably been dead for several years.

Unfortunately, we in law enforcement tend to think of our adversaries as well-trained, intelligent, disciplined, and dedicated individuals. It is difficult for us to accept the fact that lone and deranged gunmen probably kill more prominent world figures than do people who are engaged in complex terrorist conspiracies.[12] Yet, to quote the Irish Republican Army, when their attempt to kill Prime Minister Margaret Thatcher failed, "Today, we were unlucky. But remember, we have only to be lucky once. You will have to be lucky always.[13]

Today, it seems that this luck, plus the great number of potential targets provided by a free society, the availability of weapons and explosives, and excessive publicity by the media, give the impression that terrorists are supermen who can and do strike at will, where and when they wish. In fact, a quick review of recent events seems to indicate the opposite.

Life in a free society has its price. Just as we are free to travel and tour for pleasure, the terrorist has the ability to ply his trade at his whim, when luck is with him.

A Profile of the Left in the Middle East

Recent Middle Eastern terrorist incidents, particularly the taking of hostages, have occurred only when an already-lax security system was circumvented.[14] Today, some of the Middle Eastern terrorists who attack Western interests are more likely to be poorly educated, a member of a very large family, unskilled and unemployable, illiterate, rural, undisciplined, and an ill-trained **male** refugee. They are young, age 17 to 23, and have grown up as members of street gangs. They know little of politics; they hate Americans and others who have made a success of this life. Yet, **few** are willing to engage in suicidal missions away from their homelands to learn what comes next. We represent what many of them would like to achieve and are a nation to which they would willingly move, if only they had the opportunity.

This new profile is displayed in table two and represents some significant differences. Among the changes are the absence of the specific criminal type and the much lower educational level of the followers. Further, their recruitment from refugee camps and street gangs rather than the university campus, with all that entails, is the most significant change.

Recent Events in the Middle East

As evidence of this, one need only look at those who assaulted TWA 847 in June 1985, the bungling of those on the Achille Lauro, or the individuals on Pan Am 73 who left most of their gear on the tarmac and had difficulty finding the cockpit. Additionally, a walk through the airports at Rome and Vienna will quickly reveal how much damage a trained team of dedicated individuals could have done.

Those who hijacked TWA 847 had intended to hijack an ElAl flight leaving for Israel. In spite of the wide publicity ElAl gives to its security precautions, these terrorists did not know of these procedures. One gets the impression that they may never have been in an airport. Further, their tumultuous behavior in Athens would have alerted security forces in most Western airports. However, a post-incident review in Athens revealed that the staff was lax and did not know how to use their screening equipment. Once on board the aircraft, the hijackers unnecessarily abused their hostages, robbed them, were impulsive in their actions, were ill-trained, and displayed ignorance of routine aircraft operational procedures.[15]

Those on the Achille Lauro were discovered cleaning their weapons and had no knowledge of the language or country whose passports they carried. Once discovered, they ran amok and were undisciplined until Muhammed Abu Abbas arrived to take control and arrange their safe passage.[16]

The Palestinians who attempted to hijack Pan Am 073 lacked the sophistication to penetrate Pakistani passenger screening, and once on the aircraft, gave the impression that this was their first time in such an environment. They were illiterate and had limited mechanical aptitude. This ignorance caused a fatal turn of events when they could not comprehend the need for service of the auxiliary power unit and panicked when, after several hours of unattended operation, it failed. They had been warned of this possibility, yet did not understand the need. When the lights went dim and then went out, they began shooting. The one terrorist who had explosives attached to himself and was supposed to detonate them in a suicidal act did not. With his so-called suicidal peers, he tried to hide among the hostages and now languishes in a Pakistani prison. In the final analysis, many of these terrorists panic and seek to save themselves.[17]

Finally, the Rome and Vienna airport settings provided the terrorists with hundreds of potential targets. Tragically, 20 died; however, of the 7 so-called suicidal terrorists, only 1 stood his ground and died. The other six were killed or captured while attempting an escape.[18] As in London, those in custody are talking to whomever will listen.[19]

It is my impression that in each of these incidents, the commanders sent out what they thought was a suicidal team. Yet, under the stress of their self-induced brush with death, the veneer of training, discipline, and dedication vanished. Several of these terrorists have been in jail for a few years, and no attempts have been made to free them. Is this because they failed to die as they were supposed to and have thus been deserted by their leaders? Or is it that the organization lacks the resources and expertise to free them? In either case, one begins to see a clearer picture of today's terrorist and his not-so-vast support structure. They are individuals and organizations who succeed only when the system fails. While I am sure there are a number of well-trained, educated terrorists out there somewhere, this prototype, at the operational level, has not been seen during the 1977-1986 lull in JRA activities and remains unique to them. In recent years, the JRA has avoided hostage-taking or suicidal airport episodes in favor of stand-off rocket attacks. I suspect there are more car and truck bombs available for service than there are drivers to deliver the deadly cargo.

So today, the Middle East terrorists are mostly males who are unable to operate against Western security sys-

". . . terrorists are a concern because of their potential rather than their performance."

tems. While one should never consciously underestimate the enemy, neither should one make them into supermen. The refugee terrorists from the Middle East succeed only against unprotected targets outside their homeland when their plan goes exactly as it was intended. Today, we are seeing excellent examples of the Irish Republican Army statement. To succeed, they must be lucky; to prevent terrorism, law enforcement must remain vigilant against a persistent but unsophisticated, untrained, and minimally dedicated enemy.

Most Middle Eastern terrorist types represent left-wing orientations. They want change and are prepared to kill, but not die, to achieve this goal. On the right, we see a similar lack of dedication and equally low education at the operations level. Unlike the left, which has changed since the turbulent 1960's and 1970's, the demographics of the right-wing terrorist have changed little over the years.

Thunder on the Right: Or Is It a Firecracker?

I recall as a child hearing of the activity of the Ku Klux Klan, and I remember an article in *Life* magazine which discussed the background of those arrested. I recall that many of them listed their occupation as a part-time service station attendant.

In Europe, as well as in North America, the neo-Nazis, and in the United States, the Klan and more current groups such as the Covenant, the Sword and the Arm of the Lord (CSA) and the Aryan Naiton, continue to attract the people who are easily manipulated to their rank and file. The role of the female in these groups is historically that of a servant to the male. Again, we see evidence of the insecure male who, in this example, does not consider a female as an equal. While there is some movement of the female to positions of responsibility in radical right-wing groups, their role still lags far behind those of females in left-wing radical organizations. These groups generally surface in times of economic and social change. They provide quick-fix solutions to complex problems for the easily manipulated. Their self-proclaimed messiah, who is usually very intelligent and well spoken, has the answer to their problems. His answer focuses the attention of his followers away from the issue and onto a minority group whom he identifies as the real troublemakers, an ancient tactic called scapegoating.

Table 2
Demographic Profile of Middle East Leftist Groups in the 1980's

Leader	Follower
Male	Male
No specific race or religion	No specific race or religion
College education or attendance	Poorly educated/illiterate
30-45	17-25
Middle class	Lower class from a large family of 9-15 children
Urban/sophisticated	Refugee/not comfortable outside of Middle East
Multilingual	Poor verbal skills
High verbal skills	Unskilled worker
Well-trained perfectionist	Training poor to none
Dedicated	Limited dedication
Strong personality	Criminally active in street gang
Politically active prior to terrorist/criminal activity	Politically naive
Opportunist or Criminal Element	
Now an infrequent member as a specific entity	

The general philosophy of these organizations lends itself to the mind of a man who has failed and is seeking an excuse, a scapegoat. Their alleged evidence would convince a person of normal intelligence that the philosophy of the radical right is weak and caters to those looking to excuse social or economic failure. Their message has its listeners among the weak and intellectually lazy. Thus, the listeners are told of and believe in great conspiracies and the efforts of minority groups to dilute their race and rob them of their heritage. Today, their favorite text is the *Turner Diaries*, a well-written fictional account of their victory over the tyrannical, race-destroying system.[20]

A Profile of the Right

A general profile of the membership of radical right-wing groups reflects people who have a limited education, are members of the racial and religious majority, and have experienced a social or economic failure. Their age ranges from teenagers to senior citizens. Maturity does not seem to cure those of the radical right. Just as Adolph Hitler appealed to young and old with his message which included hate and scapegoating, today the right in the United States does the same. An example of their rigid thought process can be seen in the Sheriff's Posse Comitatus' interpretation of the U.S. Constitution and their perception that only the local sheriff is a legitimate law enforcement officer. The leadership of the right, like the left, is generally well-educated, articulate, and dedicated. However, unlike the left, these leaders generally represent the racial and ethnic orientation of the majority population.

Table 3
Demographic Profile of the Right Wing

Leader	**Follower**
Male	Male
White Protestant	White Protestant
College education or attendance	Limited formal education
35-50 plus	20-50 plus
Middle class	Lower and lower middle class
Urban/sophisticated	Urban or rural/unsophisticated
Literate in English	Literate in English
High verbal skills	Poor verbal skills
Well-trained perfectionist	Poor work skills
Strong controlled paranoid type personality	Weak personality/shared paranoid personality type
Politically active and articulate	Politically naive
Opportunist or Criminal Element	
Generally his skills are incorporated within the leader	

The violent activity of the right has been in the form of attacks on police officers, the robbery of banks and armored cars, and similar criminal acts. They have not attempted aircraft hijackings or other offenses which would put them in a situation requiring negotiations. The profile of these groups, presented in table 3, has changed little over the years. Additionally, while the left-wing radical community occupies itself with excessive planning, the radicals on the right seem to collect weapons and explosives.

We have, over the years, seen incidents involving cooperation between left-wing groups, such as the Lod airport massacre in May 1972, the Vienna OPEC oil ministers siege in December 1975, and the hijacking of Lufthansa 181 in October 1977. However, right-wing cooperation is more a reflection of their rhetoric than a political reality. Radical right-wing groups tend to lack the trust necessary for such operations. Perhaps it is the basic paranoia of these groups which prevents any extensive cooperation. Certainly, they talk of helping each other. On some of their video tapes, they speak of a great uprising of right-wing groups against the government. They claim that an attack on one group will be considered an attack on all of them and that they will unite against the Federal Government. In my judgment, their basic lack of trust and their paranoia will preclude such an alliance. However, in their fantasies, such alliances are real and just an incident away from an absolute.

One could speculate on the fantasy lives of radicals at both ends of the political spectrum. The radical left enjoys the planning operations. Those on the radical right express their fantasies of power and control through their collection of great caches of weapons. They tend to plan less and shoot more.

Terror Today

To put modern terrorism in perspective, one should recall the metaphor of Brian Jenkins—terrorism is theatre. It's not what they do so much as it is the perception they create. Their bombings in the United States represent less than 3 percent of such incidents. We have had one kidnaping and a decreasing number of bank and armored car robberies. Most terrorist groups have low personal intelligence among their operators and equally poor intelligence about their targets. It is not the percentage of violence they represent which concerns us, but rather the random nature of their assaults. Mao said that terrorists should kill one to influence a thousand. So, terrorists are a concern because of their potential rather than their performance. They are a force to be reckoned with, but must be viewed within the perspective of reality. When they succeed, time and again, it is not because they are so good or well-trained or disciplined, but rather because one of us did not do our job as we should have.[21] It is more than a matter of luck that is helping us win the war against terrorism. We **must** be prepared always; they need be lucky only once.

Footnotes

[1] Personal interview with Special Agent Joseph Conley, Behavioral Science Unit, FBI Academy, Quantico, VA, June 9, 1987.

[2] *Sunday Times, Siege!* The Hamlyn Publishing Group Ltd., Astronaut House, Feltham, Middlesex, England, 1980.

[3] *Time*, April 7, 1987, p. 26.

[4] Personal interview, Special Agent Gary Noesner, Washington Field Office, Federal Bureau of Investigation, Washington, DC, June 4, 1987.

[5] Frederick J. Hacker, *Crusaders, Criminals, Crazies: Terror and Terrorism in our Time* (New York: Norton, 1976).

[6] Charles A. Russell, and Bowman H. Miller, "Profile of a Terrorist," *Terrorism*, vol. 1, No. 1, Spring 1977, pp. 17-34.

[7] Thomas Strentz, "A Terrorist Organizational Profile: A Psychological Role Model," ch. 6 in *Behavioral and Quantitative Perspectives on Terrorism*, Y. Alexander and J. M. Gleason eds. (New York: Pergamon Press, 1981), pp. 86-104.

[8] Lillian Becker, *Hitler's Children* (Philadelphia: J. B. Lippincott Co., 1977).

[9] Conrad V. Hassel, "Terror—the Crime of the Privileged," *Terrorism*, vol. 1, No. 1, Spring 1977, pp. 1-16.

[10] Los Angeles Police Department, July 19, 1974, The Symbionese Liberation Army in Los Angeles, Los Angeles, CA.

[11] Eric Hoffer, *The True Believer* (New York: Harper and Row, 1952).

[12] Conrad V. Hassel, "The Political Assassin," *Journal of Police Science and Administration*, vol. 2, No. 4, pp. 399-403.

[13] *The Washington Post*, October 12, 1984, P. A1.

[14] Time, June 24, 1985, p. 20.

[15] *U.S.A. Today*, "17 Days: A Diary," July 1, 1985, p. 1.

[16] *Time*, October 21, 1985, pp. 22-23.

[17] *The Wall Street Journal*, June 15, 1987, p. 12.

[18] *Washington Times*, May 19, 1987.

[19] *The New York Times*, February 6, 1987, p. A6.

[20] Andrew Macdonald, *The Turner Diaries* (Washington, DC: National Alliance, 1978).

[21] "The Agony of Pan Am Flight 73," *Newsweek*, September 15, 1986, pp. 18-23; "Hijacking Survivors: There Was No Rescue," *The Washington Post*, September 8, 1986, p. 1A.

Product Tampering

"Since 1982, 12 people have died from poisioning of over-the-counter drugs and food products."

By
DAVID LANCE
Security Manager, Heinz U.S.A.
and
Chairman, Security Committee
National Food Processors Association
Washington, DC

"Tampering is an insidious and terrible crime. It is a form of terrorism not unlike planting a bomb in some public place to gain media attention, notoriety, or some sick sense of control over human life." Dr. Frank E. Young, Commissioner, Food and Drug Administration

In 1986, the Federal Food and Drug Administration (FDA) was involved in nearly 1,700 cases of actual tampering or hoaxes. The FBI investigated over 300 of these incidents for criminal conduct. Suspected tamperings or tampering complaints increased 13-fold. In all such incidents, certain principles apply:

—Rarely is a threat to tamper actually carried out. Experience has shown that those intent on adding poison to a product do so without warning. "Callers don't kill and killers don't call," the saying goes.

—Tampering is a copycat crime. Sensationalized news accounts about a tampering threat nearly always lead to more threats.

—Nearly two-thirds of the threats are directed at retail stores. Those who make threats also contact food and drug manufacturers, news organizations, and law enforcement agencies.

—Products threatened are usually well-known national brands.

—There is no such thing as a "tamper-proof" package. One who is intent on carrying out the act will find a way to do so.

Tampering offenses include the *rare act* in which a product is actually contaminated. Yet, there are additional crimes associated with this offense. For example, in fake tampering cases, an individual adds a harmful agent to a product to make it appear that someone in his or her household has been the victim of a random tampering. Or, the offender makes false allegations of tampering, alerting the industry, the media, a law enforcement agency, or others to a tampering that has not occurred.

Threats to tamper and/or threats to allege tampering also occur. These cases are often accompanied by an effort to extort money or valuables. Sometimes, a person seeks to have a store or manufacturer take some action (for example, remove a particular product from the shelves). Others threaten that a product has been poisoned. Usually, however, the threat is to falsely inform the news media that a product has been contaminated.

Mr. Lance

Federal regulatory agencies respond to each and every consumer complaint about a food or drug, and they investigate each tampering threat.

Product Seeding

In addition to tampering cases, food and drug manufacturers deal with many false reports by consumers alleging that they were harmed by foreign objects or substances in their products. Last year, in a wave of complaints fueled by extensive media coverage, there were more than 600 reports of glass in baby foods packed by a major baby food producer.

The Food and Drug Administration inspected the company's plants and found them to be state-of-the-art in terms of quality assurance procedures. The agency also inspected more than 50,000 jars of the company's products and found no evidence of a problem in their manufacture. Many of the complaints were false claims by consumers seeking some monetary reward or other gain by claiming that glass in the products had caused them some injury.

The Consumer Claims Division of the National Food Processors Association (NFPA) investigates some 5,000 claims cases every year for NFPA member companies. In the course of investigating the baby food complaints, the industry developed a case against one individual with a prior criminal record who had deliberately fed shards of glass to his retarded child. In another incident, a disturbed woman sought damages after ingesting glass from a broken mirror, claiming that it came from a jar of baby food.

Who Tampers?

Dr. Park Elliott Dietz, a professor of law and psychiatry at the University of Virginia who has studied the acts and motives of tamperers, commented, "What we know about tampering offenders suggests that the vast majority of adult offenders are ordinary criminals and con artists who commit offenses for a profit, revenge, thrills, and other motives that lead such people to commit other crimes. Despite the occasional terrorist or mentally ill tamperer, the evidence to date suggests that most tampering springs from greed, anger, and hatred among immature and antisocial people, just as is true of other crimes. Product tamperers are part of our criminal population and will not turn their attention elsewhere until they learn that the only goal they can reach through tampering is a crowded jail cell."

Penalties for Tampering

Since 1982, 12 people have died from poisoning of over-the-counter drugs and food products. Cyanide, a poison available from laboratory supply houses and other sources, was used in each of these deaths. To date, one person has been charged in a tampering case which resulted in two deaths in the State of Washington, but there is a growing list of tamperers and hoaxers who have gone to jail.

Many of those serving time were convicted under tough laws enacted by Congress after the Chicago Tylenol murders of 1982. The Federal law carries fines of up to $250,000 and prison terms ranging from 5 years to life for tampering or falsely reporting tampering.

"Local authorities have jurisdiction over tampering cases because of the inherent threat to community health and safety."

The stiffest penalty to date was given Edward Arlen Marks, who tampered with Contac and other SmithKline Beckman products in an effort to profit from a decline in the company's stock. A Florida judge ordered Marks to serve 27 years under the Federal antitampering statute after a trial resulting from an extensive investigation conducted by the FBI and the FDA.

While the tough, new law is undoubtedly a deterrent to would-be tamperers, it hasn't stopped them.

The Victims of Tampering

FDA Commissioner Young has said that tampering holds us all hostage—consumers, regulatory officials, the news media, and those in law enforcement agencies.

News media representatives are victims of tampering hoaxes, since many of these criminals perform their acts for no reason other than to see coverage of their crimes on television or read about it in newspapers. Law enforcement agencies devote valuable investigative time and resources to tampering hoaxes at the expense of other duties. And, society in general pays a price in terms of lost faith in consumer products and higher retail prices.

The industry has spent millions of dollars to make its packaging tamper-resistant or tamper-evident. Added millions have gone into withdrawing products that have been threatened by calls or letters. Even though virtually every threat is a hoax, the industry must react as if the threats are real until it knows for certain that they are not. SmithKline Beckman's removal of its products after the threats by Mr. Marks cost the company more than $40 million. And a company's sales losses may continue long after it has been determined there was never a real risk to the public.

Investigative Allies

Local authorities have jurisdiction over tampering cases because of the inherent threat to community health and safety. They may become involved in an investigation as a result of receiving the threat, learning about it from the media, or being asked for assistance by a retailer or manufacturer.

In carrying out its investigation, the local law enforcement agency has a number of allies. The Food and Drug Administration investigates all complaints of tampering with foods, drugs, and cosmetics. The U.S. Department of Agriculture oversees meat, poultry, and egg products. The Federal Bureau of Investigation, the FDA, and the USDA share investigative responsibilities under the antitampering act. The three agencies regularly exchange information and coordinate investigative activity. The FDA and the manufacturer should be among the first to be contacted during a tampering investigation.

The manufacturer of the product also can be a strong ally in tampering investigations. Manufacturers can provide valuable information, ranging from facts about codes used on the product to information about how the product was processed and packaged that may have a direct bearing on whether a tampering threat should be taken seriously.

All manufacturers employ a series of screening processes to detect objects which may have found their way into the product prior to the final closure. This information may also assist the law enforcement investigation.

Using the manufacturer's codes and other records, local investigators can determine when and where the product was manufactured and to which part of the country it was distributed. It is not uncommon for a hoax caller to claim that a product with a particular code has been contaminated in a certain city when the product was never even shipped to that area.

In jurisdictions where it is legal, manufacturers and store operators often record incoming telephone calls. They may have valuable tape recordings of threats and other suspicious communications that can be used in a criminal investigation.

The National Food Processors Association maintains a "repeater" list of "people" who have filed numerous complaints about food products with the association's member companies. Law enforcement agencies can consult with NFPA regarding the list and its contents.

Working with Retailers

Since most tampering threats are hoaxes, it is important that the investigation at the local food or retail outlet be handled in a way that doesn't call attention to the threat.

The Food Marketing Institute (FMI), a national association whose members operate supermarkets, trains store employees in the proper ways to deal with tampering threats. FMI teaches supermarket operators that the first responsibility is protection of the public. Customers must not have access to threatened products. If a threatener has identified a particular product as "contaminated," the first step is to take that product from store shelves.

The FMI recommends that store employees handle the product in a manner consistent with standard rules for collection and preservation of evidence, because these events may result in criminal prosecutions. The successful outcome of these cases may be determined by fingerprint analysis of the packaging and laboratory testing of the product, provided that the evidence is handled properly and the claim of custody is maintained.

A product that has been removed from shelves should be replaced as quickly as possible with the same product, bearing a different code, from the store's stock room or warehouse. Removal of products from store shelves should be limited only to the affected product and codes, instead of simply sweeping the shelves clean of entire categories of products.

Products should be removed quietly and calmly so as not to panic customers. It may be explained to shoppers that the store is taking inventory or simply a routine restocking of shelves is taking place. If the customer wants a package of the product being removed, FMI suggests that a store employee personally provide the customer with the same item from the stock room.

Closing the store is a last resort, a drastic action that nearly always is a mistake. Not only does such action cause lost revenue for the store, but it also is upsetting to shoppers and is sure to draw media attention.

Samples of the threatened product should undergo complete laboratory analysis as quickly as possible. In addition to the laboratories operated by the FDA, USDA, and FBI, many food and drug manufacturing companies have sizeable laboratories. Manufacturers also employ independent testing facilities and laboratories operated by organizations like the National Food Processors Association.

Minimizing Imitators

How a tampering investigation is conducted can directly affect the outcome of a given case and help determine if the community will be victimized by "copycat" criminals. To help assure their own freedom of action, investigators should avoid media attention until the facts are known.

When the media become aware of a tampering threat, the natural reaction is to send reporters (and camera crews) to cover the incident. This can cause the incident to mushroom, ultimately generating new threats and spreading the event beyond the initial crime scene to additional locations.

Premature release of information to the media can cause undue alarm and failure to apprehend the perpetrator. It may also hinder efforts to locate contaminated items.

Many law enforcement agencies handle their initial response to a tampering call as they might handle a bomb threat. Instead of normal radio transmissions, they might use codes or other means of communications. Instead of sending uniformed police to the crime scene, they might rely upon plainclothes investigators.

While there is a need to protect the public from the risks of actual tampering episodes, premature or sensational press coverage of the thousands of hoax threats only serves to cause panic and encourage more fake tamperings by the criminals in our society.

Summary

Product tampering poses serious threats to society's well-being. However, Federal agencies, law enforcement, manufacturers, and retailers are actively involved in protecting the public from the dangers associated with these threats. By working together to reduce the number of tampering claims, disprove claimants, and apprehend the offenders, these organizations are counteracting the tactics of the product tamperer.

FBI

The Electronic Communications Privacy Act:

Addressing Today's Technology

(Conclusion)

By
ROBERT A. FIATAL, J.D.
Special Agent
Legal Counsel Division
FBI Academy
Quantico, VA

Law enforcement officers of other than Federal jurisdiction who are interested in any legal issue discussed in this article should consult their legal adviser. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

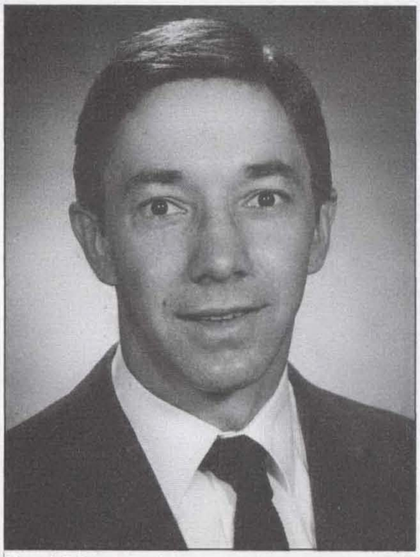
Part one of this article identified the problem areas which caused Congress to pass the Electronic Communications Privacy Act[42] (the ECPA). Part two discussed the portion of the ECPA which requires law enforcement officers to obtain wiretap-type court orders to nonconsensually intercept electronic communications, to include messages sent to digital display pagers, messages sent from one computer terminal to another, and written messages, photographs, drawings, or documents electronically transmitted from one point to another.

Part three will now examine two remaining provisions of the ECPA of common significance to Federal, State, and local law enforcement officers. First, it will consider the required procedures to use pen registers and trap and trace devices. Second, it will address the required procedures to obtain stored electronic communications and transactional records of communications services.

Pen Registers and Trap and Trace Devices

The pen register device, which records the telephone numbers dialed from the phone targeted by the device, is a particularly useful investigative technique. It is of particular value in narcotics distribution investigations, providing the investigator a pattern of calls between suspected sources of supply, dealers, buyers, and money launderers. A trap and trace device, which determines the phone number from which a call is made, is invaluable in kidnapping and extortion investigations to determine the origin of ransom or extortionate calls. As discussed in part two of this article, the ECPA specifically states that law enforcement officers are not required to obtain wiretap-type orders to use these devices.[43]

Further, the Supreme Court has determined that the user of a telephone has no reasonable expectation of privacy in the numbers dialed from that phone.[44] The user could reasonably expect the telephone company to routinely use a pen register device for numerous legitimate purposes. Similarly, when one dials a number on the telephone, he voluntarily provides the telephone company the number of the phone he is dialing and assumes the risk that the telephone company might



Special Agent Fiatal

trace that call and provide the police with the number and location of the phone from which the call originated.[45] Therefore, law enforcement officers do not need to obtain a search warrant to use a pen register or trap and trace device, as those devices do not intrude into a reasonable expectation of privacy.

Nonetheless, phone companies, which provide necessary technical assistance to law enforcement when using pen registers and trap and trace devices, commonly insist in nonemergency situations upon some type of court authorization before providing their assistance. In order to set forth a standardized procedure for law enforcement officers to obtain court authorization for the use of pen registers and trap and trace devices and to provide limited judicial monitoring of the use of these devices by law enforcement, Congress, in the ECPA, set forth specific procedures that police officers must follow to obtain authorization for using these investigative techniques.

Although law enforcement officers are not required to obtain a traditional wiretap order or a search warrant to use pen registers or trap and trace devices, they must follow this proscribed procedure.[46] Federal officers have had to comply with this procedure since the ECPA's effective date of January 20, 1987. State and local law enforcement officers do not have to follow this procedure until 2 years after the effective date the act was passed, or by October 2, 1988, unless, of course, their respective State law is now more restrictive than the ECPA or their State adopts the ECPA's procedure prior to October 2, 1988.[47] For example, if State law requires a State law enforcement officer to obtain a search warrant to use a pen register device, officers in that State must continue to follow the State-mandated procedure.

Under the provisions of the ECPA, an attorney of the government, to include assistant U.S. attorneys and State and local prosecuting attorneys, or a State law enforcement officer must make written application, under oath, to a court of general criminal jurisdiction for proper authorization to use either a pen register or a trap and trace device.[48] Magistrates of U.S. district courts also have the power to approve these applications in Federal investigations.[49]

In the application, the attorney or State investigator is only required to identify himself and the law enforcement agency conducting the investigation and certify to the reviewing judicial official that the information likely to be obtained from the pen register or trap and trace device is relevant to an ongoing criminal investigation of that particular agency. The applicant does not have to set forth facts meeting any evidentiary standard. The applicant is only required to affirm the relevancy of the anticipated information to the criminal investigation.

Likewise, the reviewing judicial official makes no independent review of the relevancy of the information anticipated to be gained from the pen register or trap and trace device, but only ascertains that the submitted application is complete. Therefore, the applicant is not required to supplement the application with any factual affidavit. Upon receipt of the appropriate application, the court is to approve an order

"Law enforcement . . . has the responsibility to have both a working knowledge of the technical aspects of [communication facilities] and the legal requirements necessary to access the communications on the facilities and related records and information."

authorizing the identified law enforcement agency to use the requested pen register or trap and trace device.

The order, which should be prepared by the applicant and presented to the judicial official with the application, must include certain information: 1) The identities, if known, of the subscriber to the telephone to which the pen register or trap and trace device is to be attached and the person who is the subject of the criminal investigation; 2) the number, and if known, location of the phone to which the pen register or trap and trace is to be attached; and 3) the type of criminal activity being investigated.

The order will direct the appropriate telephone company to furnish the technical assistance necessary to accomplish the pen register or trap and trace. It will also direct the phone company not to disclose the existence of the pen register or trap and trace device to any person, to include the subscriber to the phone to which either type device is attached. The ECPA also requires the order be sealed from public access, so the subscriber of the targeted phone or the criminal under investigation cannot determine the existence of the device by perusing court records. The order is effective for 60 days, although the law enforcement agency may seek 60-day extensions of the order by repeating the same authorization procedure.[50]

The ECPA additionally requires the agency which uses the device to compensate the telephone company which has been directed to provide the necessary technical assistance for the reasonable value of that assistance. This includes costs reasonably incurred by the phone company for maintaining lines necessary for a pen register or trapping incoming phone calls.

Finally, Congress recognized that law enforcement officers principally use the trap and trace device in fast-moving criminal investigations, such as those involving kidnappings and extortions. In these types of investigations, the investigating officers seldom have sufficient time to obtain appropriate judicial approval for the use of a trap and trace device. Therefore, law enforcement officers may use trap and trace devices, as well as pen registers, and seek the necessary assistance from the appropriate telephone company after obtaining the consent of the user of the telephone to which the device is to be attached without obtaining judicial approval.[51]

Stored Communications and Transactional Records

As previously noted, the ECPA alters the law in three distinct aspects of the communications area. It not only requires the police officer: 1) To obtain a wiretap-type order to intercept electronic communications during the course of their transmission; and 2) to obtain prior judicial approval to use pen registers or trap and trace devices in the absence of consent; but 3) it also requires the officer to follow specific procedures when obtaining certain information from institutions which provide communication services to the public, such as telephone and computerized message companies.

The officer must follow this procedure to obtain both communications which have been stored by these service providers and transactional records of communication services which include billing information and nonpublic, or unlisted, subscriber information. That portion of the ECPA which sets forth this procedure is of immediate concern to all law enforcement officers, as it has applied to Federal, State, and local investigative activity since January 20, 1987. For this reason, all investigators should thoroughly acquaint themselves with this portion of the ECPA. The two types of records addressed by this portion of the ECPA are each discussed in turn below.

Billing Records and Nonpublic Listing Information

Billing records for telephone and similar communications services are frequently valuable sources of investigative information. These would include records maintained by a telephone company of toll, or long distance, calls made from a phone being used by the subject of a criminal investigation. These toll records not only indicate the numbers dialed in long distance calls but also the dates and times those calls were made. This information is frequently invaluable in ascertaining members of a wide-ranging criminal conspiracy and is often of evidentiary value. For example, long distance calls made from the phone of a narcotics distributor are frequently of assistance in identifying the distributor's sources and places of supply, customers, and money launderers.

Additionally, the criminal investigator will commonly find it necessary to determine from the telephone company the subscriber to, and location of, a certain phone number or the number and location of the phone of a certain subscriber. For example, the investigator may ascertain a certain phone number is relevant in an investigation, as it was recorded on a pen register attached to the phone of the subject of an investigation. In such circumstances, it would be significant to determine the location of and subscriber to that particular number. If this subscriber information is not readily accessible to the public because it is unlisted, the law enforcement officer must obtain it from the appropriate telephone company. The ECPA defines the procedures the police officer must follow to obtain these types of nonpublic information pertinent to the customer of a communication service, in the absence of the consent of that customer.[52]

These procedures permit the law enforcement officer to obtain this information from the communications service provider, most often a public telephone company, in several ways. In the absence of the subscriber's or customer's consent, the officer must present the appropriate telephone company with one of the following: 1) A fourth amendment search warrant predicated upon a determination of probable cause by a neutral and detached magistrate, 2) a subpoena, or 3) a court order directing the company to provide the requested information.

The subpoena may be a Federal or State grand jury subpoena or an administrative subpoena, if Federal or State law allows the use of an administrative subpoena under those circumstances. An administrative subpoena is generally one which has been issued by the head of a law enforcement agency for specific investigative purposes. For example, Congress has given the Attorney General the power to issue administrative subpoenas in investigations of Federal narcotics violations pursuant to the Controlled Substances Act.[53] The Attorney General has, in turn, delegated this administrative subpoena authority to certain officials of the Drug Enforcement Administration and the Federal Bureau of Investigation. Agents of these Federal law enforcement agencies can thereby use properly obtained administrative subpoenas to acquire toll records and unlisted subscriber information from telephone companies in narcotics investigations.

If a law enforcement officer resorts to obtaining a court order to access toll records or nonpublic subscriber-related information, he must, in the application for such an order, make a factual showing that the requested records or information are relevant to an actual, or legitimate, criminal investigation. This relevancy standard is obviously much less than the probable cause standard required for a fourth amendment search warrant, but nonetheless requires some affirmative, albeit minimal, recitation of facts in the application.

The law enforcement agency which acquires this type of information does not have to provide any type of notice to the subscriber or customer to which the information pertains, whether the information is obtained by search warrant, subpoena, or court order. The agency or department normally also does not have to reimburse the company which provides the requested information for any costs incurred in processing the information, such as copying and labor costs, unless a court determines the amount of information to be unusually voluminous or the request to be unduly burdensome.[54] In order to facilitate the acquisition of this transactional information from the involved telephone company, however, the agency should attempt to arrive at a figure for reimbursement which is mutually agreeable to the phone company when the request is in fact unusually burdensome.

Stored Communications

As previously discussed in part one of this article, police officers must now obtain appropriate judicial approval in the form of a wiretap-type order to intercept either a wire or electronic communication *during the course of its transmission.* Numerous communications service companies, however, provide more services to their customers than just facilities for the transmission of telephone calls and electronic communications. One such service allows the customer to electronically send the communication to the service provider, which will store the communication for later transmission to the intended recipient.

For example, numerous providers of electronic communications services allow their customers to send an electronic communication through their computer terminals and modems to an electronic mailbox maintained by the service provider. The service company will store the computerized message and transmit it only when the intended recipient, or addressee, accesses the mailbox through his own computer, by relaying the proper access code to the service provider. Similarly, a phone company may store a voice communication in computerized, digitized form for retrieval by the intended receiver. Those companies which provide this mailbox service also routinely copy

". . . police officers must now obtain appropriate judicial approval in the form of a wiretap-type order to intercept either a wire or electronic communication during the course of its transmission."

these computerized messages and electronically store them for a short period of time in case of electronic difficulties or failures in the mailbox system. If a failure occurred, they would still be in a position to provide the message to the addressee.

The ECPA provides certain procedures available to the law enforcement officer to acquire contents of communications when they are stored by the electronics communication service company for purposes of later transmission to an intended recipient, in the absence of consent of a party to the communication.[55] In this regard, if the customer to this service electronically places the communication, or message, on what is known as an electronic bulletin board which is electronically accessible by the public through their computer terminals, the customer impliedly consents to the message's acquisition by all, including law enforcement. In the absence of consent, whether implied or actual, however, the police officer must comply with the ECPA's procedures when acquiring these types of stored electronic messages.

Congress has determined that when communications intended for eventual transmission to another have been stored in an electronic mailbox, or copied and stored by the service provider for fail-safe considerations, for a period of 180 days or less, they are akin to the contents of traditional mail and therefore deserve similar privacy protection. The officer, in the absence of consent of one of the parties to the message, can only access this type of stored communication in the same way he would access the contents of mail. He must present a search warrant predicated upon probable cause and obtained from a judicial official to the communication service provider. He does not, however, have to notify the affected customer that he is about to or has obtained the stored communication.

If, however, the communication service provider has electronically stored the message for a period of more than 180 days, the officer has several alternative means of acquiring it. He may use a search warrant, in which case he does not have to notify the affected customer or subscriber. He may also present to the electronic communication company a subpoena, which can be either a grand jury or administrative subpoena, or a court order directing the company to provide the requested messages. To obtain this court order, the officer must set forth, in his application, sufficient facts to show or convince the reviewing court that the messages which are sought are relevant to the criminal investigation. Again, this relevancy standard is less than a probable cause standard and should be satisfied by a minimal recitation of facts in the application.

If, however, the law enforcement agency attempts to obtain this type of stored communication by the use of a subpoena or court order, it must first notify the affected customer that it is requesting the messages from the customer's electronic communication, or computerized message, company. This is required so that the affected customer has the opportunity to contest the request by attempting to quash the subpoena or vacate the court order in the appropriate judicial forum. If the customer does not contest the acquisition, the computerized message company must release the requested information.

Under the appropriate circumstances, however, the agency or department may delay this notification requirement for a period of 90 days, and in the interim, receive the requested messages.[56] The agency may delay notifying the customer if the notification might adversely affect the criminal investigation. For example, the agency may delay notification if it might endanger the physical safety of an individual or cause an individual to flee from prosecution, destroy or tamper with evidence, or intimidate potential witnesses. The agency may thereafter extend the notification requirement every 90 days if similar circumstances continue to exist.

The means by which the department or agency accomplishes this delay in notifying the affected customer depends on whether the department seeks the electronically stored messages by subpoena or court order. If the investigative agency seeks the messages by subpoena, the head of the agency's regional office, or his first assistant, or the chief prosecuting attorney, or his first assistant, is only required to execute a written certification, or affirmation, that notification might have an adverse result. For example, the Special Agent in Charge or Assistant Special Agent in Charge of an office of the Federal Bureau of Investigation or the chief or assistant chief of a police department may certify this delay. The requesting agency may attach this certification to the subpoena itself. If, however, the department or agency seeks to obtain these messages by court order, the court to which the application is made must make the determination that notification might lead to an adverse result. The requesting department would therefore have to make some assertions in its application for the order justifying this conclusion. Of course, once the period of delay, to include extensions, expires, the agency must present written notification of its acquisition of the stored electronic communications to the customer.

If the agency delays the notification, it may also obtain a court order commanding the electronic communication service provider to not notify any person, to include the affected customer, of the request for the electronically stored messages. The officer may obtain this order if the issuing court determines that the notification would again adversely affect the criminal investigation.[57]

Finally, with regard to stored communications, the ECPA defines the procedure law enforcement must observe to acquire records that have been electronically transmitted to a service providing company for purposes of storage or computer programming only.[58] For example, some electronic communications service companies offer a service to the public whereby their customers can transmit information through their own computer terminals and modems to the company. The company, in turn, maintains this electronically transmitted information in its computer bank for storage purposes only. It does not store the information for later transmission to another party, but only stores it for the sending customer without ever accessing it. It may, in some circumstances, electronically apply computer programs to the information, but otherwise simply leaves it in its computerized storage banks for later electronic retrieval by the sender.

In this manner, an individual involved in criminal activity might electronically transmit records of the criminal activity, such as narcotics distribution records, or records of fraudulent acquisitions to the service provider. The criminal is then in an extremely advantageous position. He can immediately access the recorded information through his computer terminal without physically possessing the records, which are electronically stored in the computer banks of the service company. If law enforcement officers were to search the criminal's residence or business, they would not likely, in such a situation, find any evidence of the criminal records. In such circumstances, the officers must obtain the incriminating records from the electronic communication storage company.

If the police officer obtains these types of records from the company which provides the electronic storage, he must follow the proscribed procedure of the ECPA. This procedure is exactly the same procedure law enforcement must follow when accessing electronic communications which have been stored for more than 180 days for the purpose of later transmission to another party, as previously discussed.

The officer may obtain these electronically transmitted records, which are being stored exclusively for storage purposes, by means of a search warrant. If the officer accesses this information by warrant, he does not have to provide the affected customer any prior notice of the acquisition. The officer may also obtain these records by use of a subpoena, grand jury or administrative, or a court order issued on a determination of relevancy, directing the computerized record storage company to provide the requested information.

If the officer relies upon a subpoena or court order, however, he must provide the affected customer prior notice of the acquisition, in order that the customer has the opportunity to contest the acquisition in a court of law. The officer can again delay this notice requirement for a period of 90 days, if it might adversely affect the criminal investigation, and during the delay, obtain the records. The appropriate law enforcement or prosecuting official must certify cause for the delay if the officer uses a subpoena to obtain this type of information. If, however, he obtains a court order, the authorizing judicial official must determine there is appropriate cause for delay.

If the law enforcement officer must provide the affected customer prior notice of the acquisition of the electronically stored information, he runs the risk that the customer, upon notification, might gain immediate access to the records through his computer terminal and either retrieve or erase them from the service company's electronic storage banks, before the company is able to copy them for the requesting officer. For this reason, the officer may, when requesting the records, also request the service provider to construct a backup copy of the records if, in his discretion, he believes that notification to the customer may result in tampering with evidence.[59]

In such circumstances, the service provider, without notifying the affected

"Under the provisions of the ECPA, an attorney of the government . . . or a State law enforcement officer must make written application, under oath, to a court of general criminal jurisdiction for proper authorization to use either a pen register or a trap and trace device."

customer, must produce this backup copy within 2 working days of the request and then advise the requesting officer that the reproduction has been completed. Once advised, the officer has 3 days to notify the customer unless, of course, the notification requirement has been properly delayed. If notified, the customer, in order to contest the acquisition, must seek the appropriate judicial remedy within 14 days. The records are therefore preserved if the customer attempts to electronically destroy them after notification. The service provider is also in a position to provide them to the requesting agency, whether the customer contests their acquisition or not.

CONCLUSION

Today's criminals are using sophisticated communications facilities in committing their illegal acts. Law enforcement therefore has the responsibility to have both a working knowledge of the technical aspects of these facilities and the legal requirements necessary to access the communications on the facilities and related records and information.

The ECPA provides common procedures for Federal, State, and local law enforcement officers to follow in discharging these duties. First, it requires a Federal officer to now obtain a wiretap-type order when nonconsensually intercepting an electronic communication. State and local officers with electronic surveillance abilities must do the same by October 2, 1988, unless, of course, their respective State law requires it sooner. Second, it requires Federal officers to also follow specific procedures in seeking authorization to use pen registers and trap and trace devices. Again, State and local officers must follow this procedure by October 1988, unless their State law is presently more restrictive or their State adopts the provisions of this portion of the ECPA before the October 1988, date. Finally, all officers, whether Federal, State, or local, must immediately observe the provisions of the ECPA when acquiring electronic communications stored by electronic communications service providers or information relating to the customers of communications services, such as toll records and unlisted subscriber information.

Because of these recent changes in the law and their resulting impact on law enforcement responsibilities, it is incumbent upon Federal, State, and local officers to acquaint themselves with these provisions of the ECPA. Moreover, law enforcement agencies should consider modifying any existing internal procedures or developing new ones as needed to achieve an ordered and effective compliance with ECPA requirements. They should also examine their liaison with communications service providers, such as telephone companies, to ensure that it is adequate to meet their fast-developing investigative needs pursuant to this statute.

Footnotes

[42] *Supra* note 1.

[43] *Supra* note 39.

[44] *Supra* note 19.

[45] *Supra* note 20.

[46] 18 U.S.C. 3121-3126. Federal agents may also obtain authority to use pen registers and trap and trace devices pursuant to the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801-1811, in foreign counterintelligence investigations.

[47] *Supra* note 25.

[48] 18 U.S.C. 3122.

[49] 18 U.S.C. 3126(2).

[50] 18 U.S.C. 3123.

[51] 18 U.S.C. 3121(b).

[52] 18 U.S.C. 2703(c)(1)(B). Special Agents of the Federal Bureau of Investigation can also obtain this information upon written request of the Director, or his designee, in foreign counterintelligence investigations. 18 U.S.C. 2709.

[53] 21 U.S.C. 874.

[54] 18 U.S.C. 2706(c).

[55] 18 U.S.C. 2703(a).

[56] 18 U.S.C. 2705(a).

[57] 18 U.S.C. 2705(b).

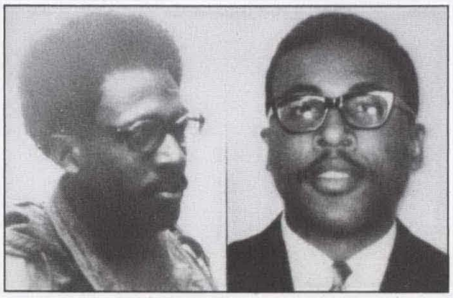
[58] 18 U.S.C. 2703(b).

[59] 18 U.S.C. 2704.

WANTED BY THE FBI

Any person having information which might assist in locating these fugitives is requested to notify immediately the Director of the Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC 20535, or the Special Agent in Charge of the nearest FBI field office, the telephone number of which appears on the first page of most local directories.

Because of the time factor in printing the FBI Law Enforcement Bulletin, *there is the possibility that these fugitives have already been apprehended. The nearest office of the FBI will have current information on the fugitives' status.*



Photographs taken 1970 and date unknown

Richard Bernard Thomas,

also known as "Ricky."

B; born 5-25-46, Philadelphia, PA; 6′1″; 170 lbs; med bld; blk hair; brn eyes; med comp; occ-telephone lineman; scars and marks: Vaccination scars on left arm, scars on right arm, right thumb, and left leg; remarks: May be wearing gold-rimmed glasses.

Wanted by FBI for INTERSTATE FLIGHT-MURDER

NCIC Classification:

2067151813DI66131812

Fingerprint Classification:

20 L 5 R OOO 13 Ref: 13

I 1 R OOO 1

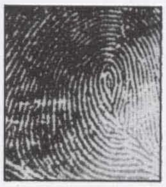
I.O. 4426

Social Security Number Used: 201-36-3251

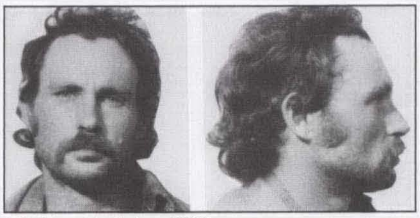
FBI No. 534 590 H11

Caution

Consider armed and extremely dangerous.



Right ring fingerprint



Photographs taken 1986

Paul David Crews,

also known as Paul D. Crews, Paul David Crews, Sr., "Butch."

W; born 8-2-52; Union County, SC; 5′5″; 150 lbs; med bld; brn hair; blue eyes; med comp; occ-laborer, migrant worker; remarks: Known to frequent libraries as Crews reads a great deal. He is described as a woodsman who can live off the land; scars and marks: Scar on chest, scar on abdomen; tattoos: "Casey" on right shoulder, "C" on left shoulder.

Wanted by the FBI for INTERSTATE FLIGHT-MURDER; ROBBERY

NCIC Classification:

22PI16CO161509131612

Fingerprint Classification:

22 L 25 W IOO 16

M 1 U IOO

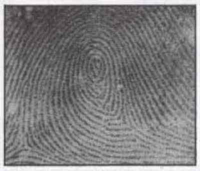
I.O. 5038

Social Security Number Used: 245-94-8548

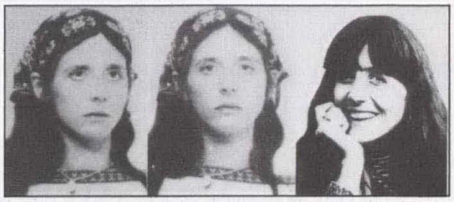
FBI No. 33 923 T3

Caution

Crews is being sought in connection with the brutal murder of a female victim wherein her throat had been slashed several times. Crews reportedly carries a sheathed hunting knife on his belt and should be considered armed and dangerous.



Right ring fingerprint



Photographs taken 1971 and 1983

Mary Kathleen Brooks,

also known as Mrs. Don Luis Church, Mary Kathleen Church, Marjorie Cummings, Mrs. Ron Firmi, Ann Haggerty, Mrs. Colin Marshall, Jane Roach, Mrs. David Henry Sidwell, Gloria Stewart, Mary Walker.

W; born 6-7-50 (true date of birth), 11-10-50; Baltimore, MD (true place of birth); Jarroo, Great Britain; 5′9″; 140-150 lbs; med bld; brn hair; brn eyes; lt comp; occ-clerk; remarks: Brooks may be accompanied by her three sons, ages 14, 10, and 8.

Wanted by FBI for INTERSTATE FLIGHT-POSSESSION AND DETONATION OF DESTRUCTIVE DEVICES

NCIC Classification:

POPOPOPOPO23PIPIPIPI

Fingerprint Classification:

23 O 28 W OOO

L 32 W III

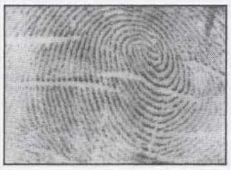
I.O. 4490

Social Security Number Used: 214-54-4597

FBI No. 956 352 H8

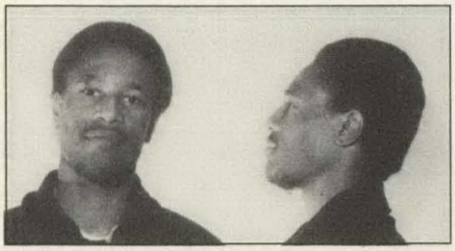
Caution

Brooks reportedly has carried a knife. Consider dangerous.



Right thumbprint

WANTED BY THE FBI



Photographs taken 1983

Bernardo Coles,

also known as Bernard Coles, Nardo Coles, Benjamin Harris.
B; born 6-15-59; Richmond, VA; 6′3″; 175 lbs; med bld; blk hair; brn eyes; light comp; occ-delivery service, gas station attendant, laborer; remarks: May have slight goatee and pierced left ear.
Wanted by the FBI for INTERSTATE FLIGHT-ARMED ROBBERY; ATTEMPTED MURDER

NCIC Classification:

1309111712 1209131813

Fingerprint Classification:

13 M 1 U IOO 12
M 1 U IOO

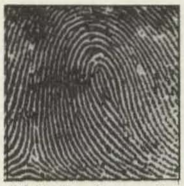
I.O. 5024

Social Security Number Used: 230-90-3132

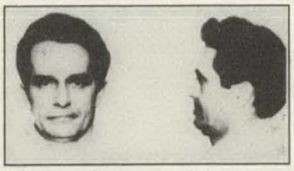
FBI No. 910 360 R6

Caution

Coles, a reported drug user, is being sought for a series of armed robberies and one attempted murder. In addition, he is wanted by local Pennsylvania authorities for armed robbery, attempted murder, and use of firearms in the commission of felonies. Coles has been known to carry a .357 magnum revolver in the past and has vowed not to be taken alive. Consider armed and extremely dangerous.



Right ring fingerprint



Photographs taken 1979

Donald Eugene Webb,

also known as A. D. Baker, Donald Eugene Perkins (True Name), Donald Eugene Pierce, Stanley J. Pierce, John S. Portas, Stanley John Portas, Bev Webb, Eugene Belvin Webb, Eugene Donald Webb, Stanley Webb, and others.
W; born 7-14-31, Oklahoma City, OK; 5′9″; 165 lbs; med bld; gray-brn hair; brn eyes; med comp; occ-butcher, car salesman, jewelry salesman, real estate salesman, restaurant manager, vending machine repairman; scars and marks: Allegedly has small scar on right cheek and right forearm; tattoos: Allegedly "DON" on web of right hand, "ANN" on chest; remarks: Webb, who is considered a career criminal and master of assumed identities, specializes in the burglary of jewelry stores. Reportedly allergic to penicillin, loves dogs, is a flashy dresser, and big tipper.
Wanted by FBI for INTERSTATE FLIGHT-MURDER; ATTEMPTED BURGLARY

NCIC Classification:

080406130804TT020906

Fingerprint Classification:

8 S 1 U III 8 Ref: TTU
S 1 T II TRR

I.O. 4873

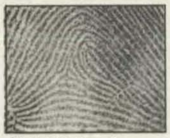
Social Security Number Used: 462-48-0452

FBI No. 4 513 086

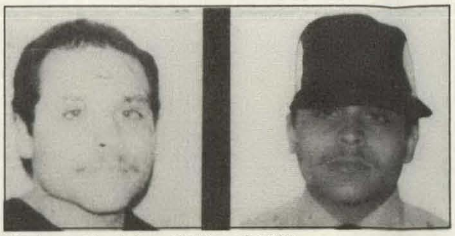
Caution

Webb is being sought in connection with the murder of a police chief who was shot twice at close range after being brutally beaten about the head and face with a blunt instrument. Consider Webb armed and extremely dangerous and an escape risk.

FBI TOP TEN FUGITIVE



Right index fingerprint



Photographs taken 1982 and 1983

Victor Manuel Gerena,

also known as Victor Ortiz, Victor M. Gerena Ortiz, Victor Manuel Gerena Ortiz.
W; born 6-24-58; New York, NY; 5′6″-5′7″; 160-169 lbs; med-stocky bld; brn hair; grn eyes; dark/med comp; occ-machinist, security guard; scars and marks: 1-inch scar on right shoulder blade, mole on right shoulder blade; remarks: Customarily wears light mustache, noticeably green eyes.
Wanted by the FBI for BANK ROBBERY, INTERSTATE FLIGHT-ARMED ROBBERY, THEFT FROM INTERSTATE SHIPMENT

NCIC Classification:

POTTTT1016DIAA032212

Fingerprint Classification:

10 O 5 Tt 16 Ref: 13
I 17 A 17

I.O. 4946

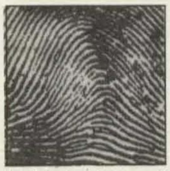
Social Security Number Used: 046-54-2581

FBI No. 134 852 CA2

Caution

Gerena is being sought in connection with the armed robbery of approximately $7 million from a security company. He took two security employees hostage at gunpoint, handcuffed, bound, and injected them with an unknown substance in order to further disable them. Gerena is believed to be in possession of a .38-caliber Smith and Wesson revolver and should be considered armed and dangerous.

FBI TOP TEN FUGITIVE

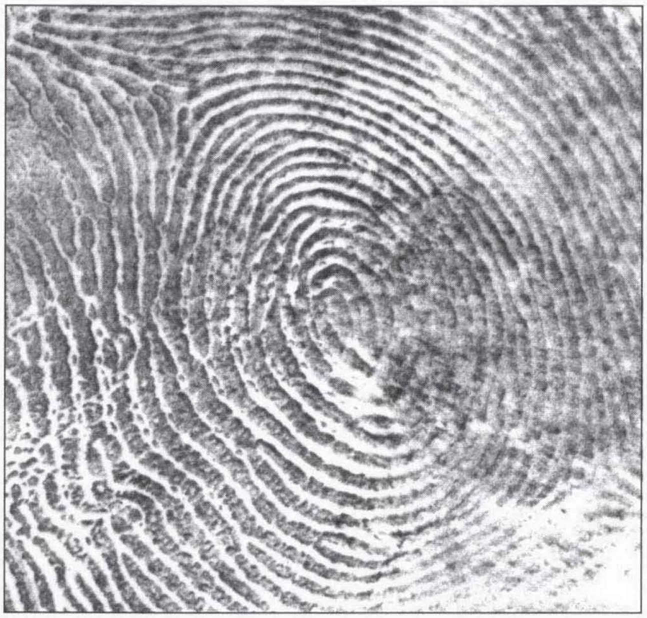


Left index fingerprint

☆ U.S. GOVERNMENT PRINTING OFFICE: 1988 — 202-051/80003

Unusual Pattern

This pattern is given the classification of an accidental whorl with an outer tracing. The accidental whorl is the only type of pattern which may possess more than two deltas. The pattern presented is less common in occurrence, inasmuch as the three deltas appear in absence of a combination of two different types of patterns exclusive of the plain arch.



Change of Address

Not an order form

FBI Law Enforcement Bulletin

Complete this form and return to:

Director
Federal Bureau of
Investigation
Washington, DC 20535

Name

Title

Address

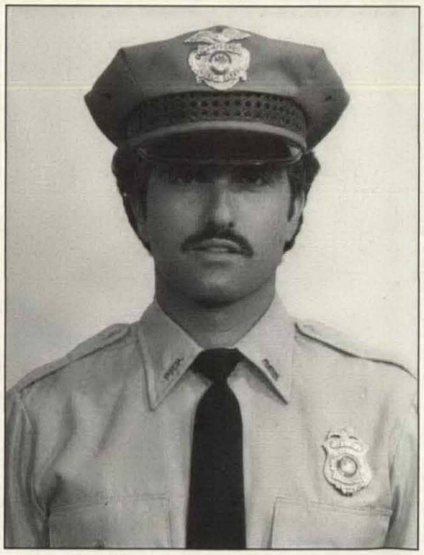
City State Zip

U.S. Department of Justice
Federal Bureau of Investigation

The Bulletin Notes

On September 27, 1987, Motorcycle Officer Michael Kizer and Patrol Officer Gregory Cavelli of the Alamogordo, NM, Department of Public Safety monitored a radio call dispatching an ambulance to a local business. At the scene, the officers found a 43-year-old male, who had been the victim of a robbery-assault, with his throat cut and rapidly losing blood. Both officers removed their undershirts, rolled them, and used them as compresses. Surgeons and emergency room personnel credited the officers with saving the victim's life. The Bulletin joins these officers' superiors in commending their lifesaving actions.

Officer Kizer



Officer Cavelli