LAW ENFORCEMENT INTELLIGENCE OPERATIONS

CONCEPTS ISSUES TERMS

BY

DAVID L CARTER

SCHOOL OF CRIMINAL JUSTICE

LAW ENFORCEMENT INTELLIGENCE OPERATIONS

An Overview of Concepts, Issues and Terms

Researched and Written By:

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University
East Lansing, MI 48824-1118

(517) 355-2197

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES (continued)

LIST OF FIGURES (concluded)

PREFACE

Intuitively, most people have a sense of what is meant by *law enforcement intelligence*. It typically is viewed as information gathered surreptitiously to identify and prosecute serious criminal offenders. While there is some truth to this, the intelligence function is far broader than this. Intelligence not only fulfills the role of investigative support, it is also an important management tool for decision making, resource allocation, deployment, and a spate of other administrative responsibilities. As such, law enforcement intelligence is *not* just vast amounts of collected information. It is information which has been comprehensively and logically analyzed. This analysis gives raw information its meaning and role in the larger puzzle of police responsibility.

Past criticisms of law enforcement intelligence have focused on the facts that it was too intrusive and that vast files may violate constitutional rights of citizens. Indeed, problems related to these concerns have occurred in the past. However, the law enforcement intelligence function is maturing with greater emphasis on effective *analysis* rather than just developing vast amounts of information. I have taken this a step further by presenting a *value-based philosophy* of law enforcement intelligence operations. The material in this monograph reflects this ideology.

The information contained herein is intended to be a primer. The chapters are of an eclectic nature to identify issues which are relevant to the intelligence function. The monograph is an evolutionary document in that it is updated and expanded on a continual basis to both address a wider range of issues and incorporate more contemporary developments. It is not meant to be the "last word" on law enforcement intelligence; however, for many it serves as the important "first words".

The subjects have been presented in outline form to more effectively facilitate training. At the end of each chapter are learning objectives as well as study questions addressing critical issues in the chapter. Various figures have been used throughout the monograph to help illustrate important points and provide direction on a wide range of issues. In addition, there is a glossary of terms and a comprehensive bibliography to assist the student of intelligence.

Many people shared information and provided input for this document. I would like to particularly thank: **Bill Beard**, U.S. Customs Service-Washington; **Bill Tafoya**, FBI Academy-Quantico, VA; **Joe Harpold**, FBI Academy-Quantico, VA; **Judy Bertini**, Drug Enforcement Administration-Washington; **Hobie Henson**, formerly with the Illinois State Police and currently with the Federal Law Enforcement Training Center-Glynco, GA; **Tim Edgerton**, U.S. Immigration and Naturalization Service-Toronto, Ontario; **Merle Manzi**, Florida Department of Law Enforcement-Tallahassee; **Ken Sanz**, Florida Department of Law

Enforcement-Tampa; **Allen Sapp**, Central Missouri State University-Warrensburg, MO; **Darrel Stephens**, Police Executive Research Forum-Washington; **Kai Martensen**, formerly with the Baltimore County, Maryland Police Department-Towson, MD; **Mike Robinson**, Michigan State Police-East Lansing, MI; **Allen Spyke**, Ingham County, Michigan Sheriff's Department-Mason, MI; and the members of the **International Association of Law Enforcement Intelligence Analysts** who provided feedback on earlier versions of this monograph. And to **Dennis Banas**, Michigan State University, who was with me "at the beginning" of this odyssey and whose warped sense of humor has given me needed relief and a realistic perspective of what's important—and what's not.

Special appreciation and thanks is extended to **David Westrate**, Assistant Administrator of Operations, Drug Enforcement Administration, whose ideas sparked this work and whose assistance truly got this project "off the ground". I am also indebted to my colleague **Robert Trojanowicz**, Director of the School of Criminal Justice, Michigan State University, for the time, flexibility, and support he has given me throughout this project. Finally, I thank my wife and children—**Karen**, **Hilary**, **Jeremy**, and **Lauren**—who have tolerated my work and travel throughout this and many other projects. I always know you are with me.

David L Carter
East Lansing, Michigan

CHAPTER 1
DEFINITIONS AND CLASSIFICATIONS OF INTELLIGENCE

"Intelligence is man's ability to manipulate the world with the help of thought."
Erich Fromm (The Sane Society, 1955).

1. THE MEANING OF LAW ENFORCEMENT INTELLIGENCE

The intelligence concept has meant many different things to people. It conjures up images of clandestine, high technology, risk-taking for the purposes of gathering sensitive information about crimes and criminals. To be sure, this is part of intelligence. However, this image is a one dimensional view of selected intelligence *methods*.

In general terms, law enforcement intelligence (LAWINT) has three basic goals.

- Development of ***evidence*** for prosecution of criminal cases.
- Identification and seizure of ***illegal commodities*** (contraband and fruits of unlawful transactions).
- Development of information to direct the ***allocation and deployment of law enforcement resources.***

These needs, with specific reference to drug enforcement, were articulated in the *National Drug Control Strategy*, which stated:

> "The war against drugs cannot be fought—much less won—without good intelligence. No military commander goes into battle without the best available information about both his adversary and about the field of battle itself. If we are to target our efforts effectively where traffickers are most vulnerable, we must know the enemy far better than we do now. ... That means we must collect critical information ... in imaginative and efficient ways; analyze data from all sources; produce intelligence tailored to the varying needs of decisionmakers from the national

to tactical levels; and see that the intelligence is disseminated to users in a timely fashion" (1989:87).

As a result, LAWINT must become more **directed**, more **structured**, and more **regionalized.**

A. *Defined*:

> Law enforcement intelligence is the end product (output) of an analytic process which collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgements and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends.

B. Traditional perspectives of law enforcement intelligence are changing dramatically

1. Those involved in intelligence work ...

   a. Must become more open to change

   b. Must re-focus their roles

   c. Must become more "holistic' in their approach to intelligence

2. Similarly, those who have questioned the need and methods of LAWINT in the past ...

   a. Must recognize the true role of contemporary LAWINT

   b. Must recognize the need for LAWINT activities

   c. Must recognize that change is occurring in the LAWINT function

2. ROLES AND NATURE OF LAW ENFORCEMENT INTELLIGENCE

A. As evidenced through the definition and subsequent classifications presented, the roles of law enforcement intelligence can be summarized as follows (*See* Figure I-1):

1. **Obtaining and integrating information** into a cohesive and logical case file or description of crime trends

2. **Identifying crimes and crime trends** through information assessment, report review, data comparisons, and crime analysis

3. **Identifying criminals** through the use of deduction, information assessment, and application of the scientific method

4. **Developing cases** for prosecution in court

5. **Providing support to investigators** involved in long term and complex case investigations

6. **Projecting crime trends** for purposes of planning and law enforcement resource allocation

B. *Intelligence* has often been confused with *information*—this confusion even exists within the law enforcement community

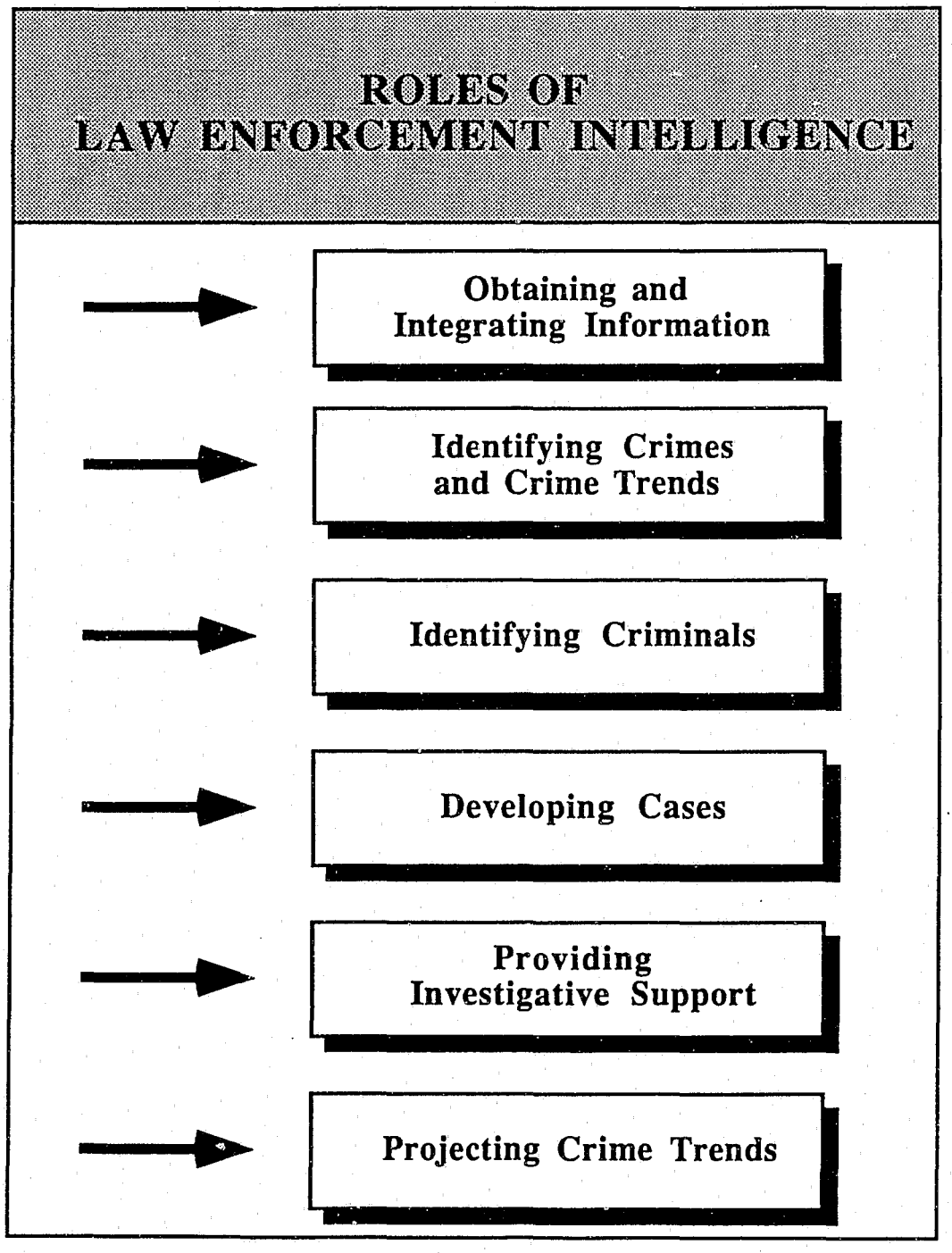
1. A common misconception is that if an agency has a system—computerized or manual—which stores information about crimes and suspects that this is intelligence

CASE EXAMPLE:

The White House Conference for a Drug Free America recommended that "the federal government should designate a unified, national law enforcement drug intelligence system" (White House Conference, 1988:59) as a tool in developing criminal cases against drug traffickers. The essence of the discussions on this system (observed by the author) was that law enforcement needed data files which had nation-wide input which could accessed to assist in developing criminal cases. All discussions were focused on the acquisition and implementation of a nationwide computerized "intelligence" system, yet there was no discussion on *how* the information would be used or *analyzed*. The fallacy was that the system would be a nationwide data base that would have limited utility as an intelligence resource for state and local law enforcement.

Figure I-1

ROLES OF LAW ENFORCEMENT INTELLIGENCE



2. There are clear distinctions between "information" and "intelligence"

   a. Intelligence takes "raw' information—facts, evidence, events, etc.—and integrates it all together through the application of logic

      1) Thus, with "information" one has pieces of data

      2) With "intelligence" one has *knowledge*

   b. Another distinction is...

      1) Information is *passive*—it is simply data which has been accepted and stored

      2) Intelligence is *proactive*—it can...

         a) Forecast

         b) Correlate

         c) Offer supposition

         d) Direct an investigation/inquiry

3. CLASSIFICATIONS OF LAW ENFORCEMENT INTELLIGENCE

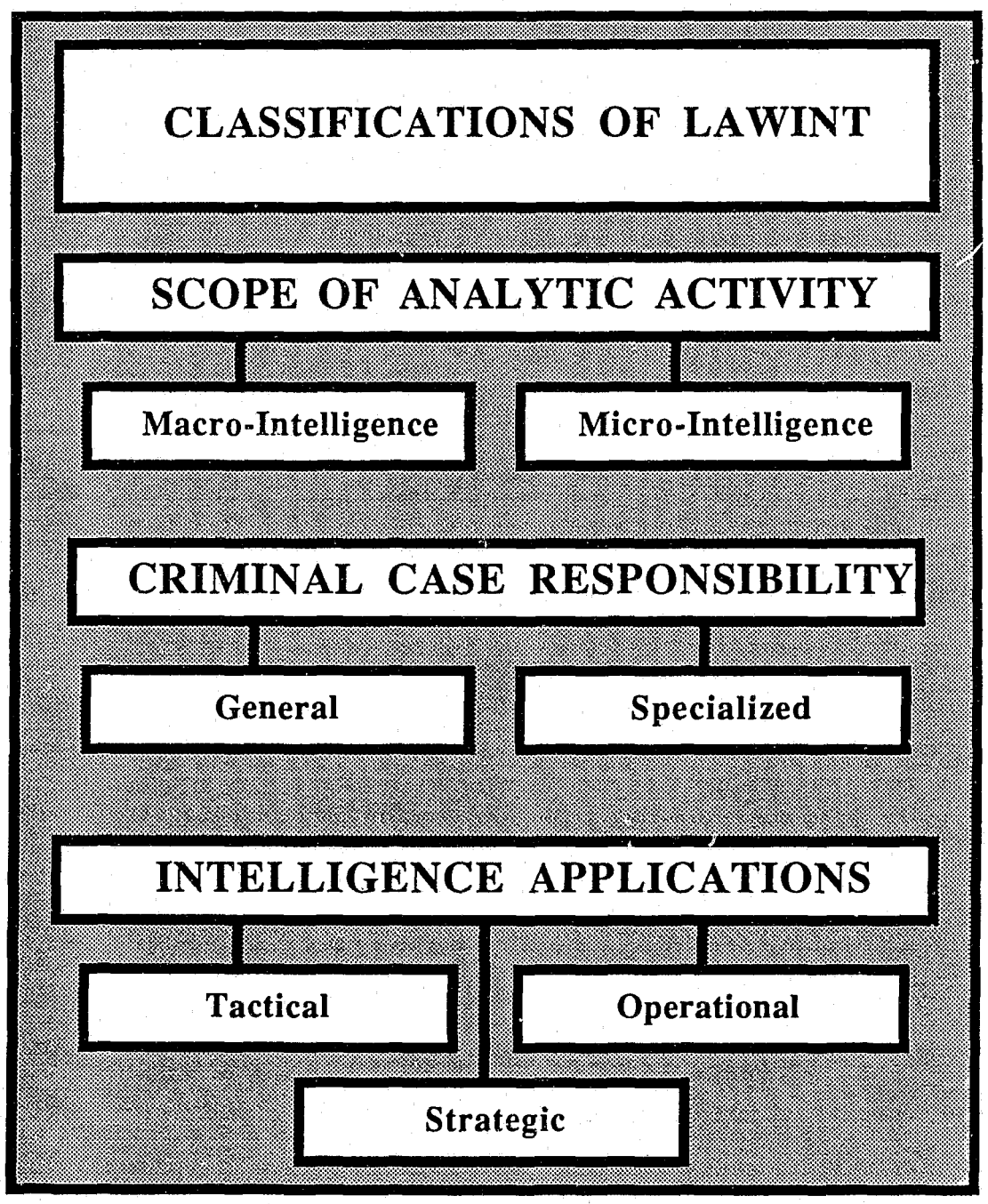
The law enforcement intelligence function varies significantly depending on an agency's jurisdiction and the types of cases for which intelligence resources are allocated/directed. The following represents alternate means to classify intelligence. The classifications are not mutually exclusive, rather they are designed to give perspective based on the use of an agency's intelligence unit (*See* Figure I-2).

A. *Scope* of Analytic Activities

1. **Macro-intelligence** - An overall view of general demographic, social, and crime trends which indicate environments and types of crimes which are emerging or projected to emerge

Figure I-2

CLASSIFICATIONS OF LAW ENFORCEMENT INTELLIGENCE



2. **Micro-intelligence** - Intelligence activities focusing on current problems and crimes for either case development or resource allocation

   NOTE: Macro is a planning and forecasting activity for general administrative use while Micro is a functional, current, applied activity, generally applied at the line level

B. *Criminal Case* Responsibility

1. **General intelligence** - Intelligence unit will collect information on crimes in general in support of an agency's investigative responsibility -- typically associated with a municipal, county, or state law enforcement agency with general law enforcement responsibilities

2. **Specialized intelligence** - Intelligence unit (or section within a unit) focuses on an exclusive issue whether it is a crime (e.g., narcotics, terrorism, etc.) or entity (e.g., organized crime, right wing extremist groups, abortion protests, etc.)

C. Intelligence *Applications*

1. **Tactical intelligence** - Evaluated information on which *immediate* enforcement action can be based; intelligence activity focused specifically on developing an active case

2. **Operational intelligence** - Intelligence information is evaluated and systematically organized on an active or potential target. This process is developmental in nature wherein there is sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information in order to develop a case for arrest or indictment

3. **Strategic intelligence** - Statistical crime patterns and crime trends are collected, analyzed, and evaluated for management use in decision-making, resource development, and policy planning

4. NATIONAL SECURITY/POLICY INTELLIGENCE (NASINT)

There has always been confusion about the similarities and differences between LAWINT and National Security/Policy Intelligence (NASINT). The confusion has been compounded since 1986 when President Reagan declared that drugs were a national security threat. The thrust of this executive action was that NASINT organizations—such as the CIA—were given the responsibility to collect intelligence on drugs. While this information could be useful for interdiction, "source country eradication strategies", and strategic intelligence projections, it could generally not be used as evidence in criminal proceedings. Further complications arise for agencies which have both LAWINT *and* NASINT responsibilities. As a result of this and other factors it becomes useful to have a conceptual understanding of National Security Intelligence.

A. *Defined*:

> National security intelligence is the collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States' sovereign principles.

B. Classifications of National Security Intelligence Agencies

1. The **Intelligence Community** is a phrase that customarily refers to those agencies which gather National Security intelligence information—they can be classified as being an **exclusive** or **non-exclusive** policy intelligence agency

   a. **Exclusive** - Intelligence gathering agencies whose responsibility and resources are focused solely on information which may be used in national policy decisions.

   EXAMPLES:

   - Central Intelligence Agency (CIA)
   - Defense Intelligence Agency (DIA)
   - National Security Administration (NSA)

b. **Non-Exclusive** - Intelligence gathering agencies whose responsibilities and resources address both issues of national security and enforcement of criminal laws.

EXAMPLES:

- Drug Enforcement Administration (DEA)
- Federal Bureau of Investigation (FBI)
- U.S. Customs Service (USCS)

2. Those agencies in the non-exclusive category can face unique problems with respect to the *type* of information they collect and *how* it is used in a LAWINT capacity.

C. Roles of National Security/Policy Intelligence

The current roles of national security intelligence are actually set forth in the Presidential Executive Order 12333, *United States Intelligence Activities* (1981) in its charge to the agencies of the intelligence community as noted below:

1. The agencies within the U.S. Intelligence Community shall, in accordance with applicable United States law and with the other provisions of this Order, conduct intelligence activities necessary for the conduct of foreign relations and the *protection of the national security* of the United States, including:

   a. Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;

   b. Production and dissemination of intelligence;

   c. Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotic activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

   d. Special activities;

e. Administrative and support activities within the United States and abroad necessary for the performance of authorized activities; and

f. Such other intelligence activities as the President may direct from time to time.

2. These roles may be fulfilled by:

a. **Collection.** "The acquisition of specified information ... through the use of both special human and technological means, ... in relation to our national security."

b. **Counterintelligence.** "... the countering of similar intelligence activities by other groups, governments, or individuals through the identification, neutralization, and manipulation of other states or groups intelligence services."

c. **Analysis and estimates.** "The processing, analysis, production, and dissemination of all available information from collection and counterintelligence and presentation to policy-makers of a finished product that has more clarity than may be inherent in the data itself."

d. **Covert action.** "Influencing events and behavior in other states or groups without revealing one's involvement."

5. DISTINCTIONS BETWEEN LAW ENFORCEMENT AND POLICY INTELLIGENCE

A. The essential differences are ...

1. Law enforcement intelligence must be *crime-driven*

2. National security intelligence is "driven" by *Presidential policy* which defines threats to the national security of the United States

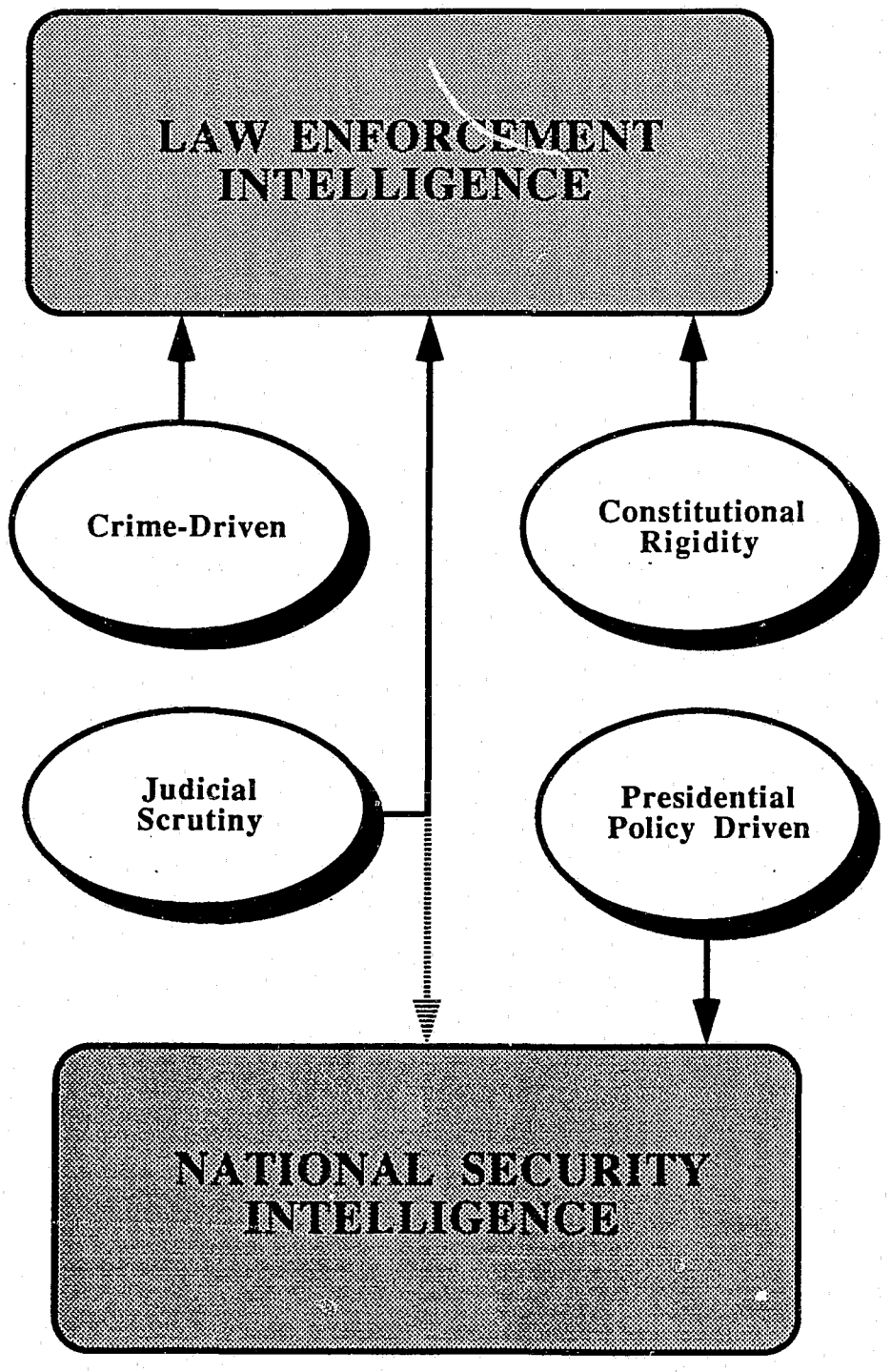
3. Law enforcement intelligence information must pass *judicial scrutiny* for admissibility as evidence in criminal trials

4. National security intelligence is used for decision making by the executive branch of the federal government and does not have to meet the same *constitutional rigidity* of criminal trial evidence

B. This is not to infer no constitutional safeguards apply to policy intelligence matters, however, they are overall far less restrictive. As illustrated in Figure I-3, each element of constitutes and equal and substantial difference between LAWINT and NASINT.

Figure I-3

ILLUSTRATION OF THE DIFFERENCES BETWEEN LAW ENFORCEMENT AND NATIONAL SECURITY INTELLIGENCE



1. DEFINITION AND CLASSIFICATIONS OF INTELLIGENCE

Instructional Support and Criteria

GOAL:

> To articulate the meaning of *law enforcement* intelligence (LAWINT) and describe the different types of LAWINT methodologies.

OBJECTIVES:

1. Students will be able to define law enforcement intelligence.
2. Students will be able to distinguish LAWINT form national security or policy intelligence.
3. Students will have a working knowledge of the different applications and methodologies which can be used in LAWINT.

STUDY QUESTIONS:

a. Discuss the various roles of law enforcement intelligence and their meaning with respect to the development of a new intelligence unit.

b. Law enforcement intelligence can be classified based upon its *scope*, its *application*, or its *criminal case responsibility*. If you were managing an intelligence unit, which classification would you find **most functional** in the fulfillment of that responsibility? Why?

c. In your own words, describe the *relationship* between law enforcement intelligence and national security intelligence.

d. What can be learned from the application of national security intelligence principles to law enforcement?

e. Describe any misconceptions you may have had about the role and function of law enforcement intelligence. How do you feel those misconceptions were developed?

NOTES

CHAPTER 2
HISTORY OF LAW ENFORCEMENT INTELLIGENCE

"History shows that bad police methods breed disrespect for law, shake the confidence of law-abiding citizens in the administration of justice, and weaken the national morale."
Former Los Angeles Police Chief William Parker, 1957 (Marx, 1988).

1. THE HISTORY AND DEVELOPMENT OF LAW ENFORCEMENT INTELLIGENCE

While there is no definitive history of law enforcement intelligence (LAWINT) , there are a number of trends and critical incidents which can be identified as having contributed to the develop, use, and control of intelligence actions by police agencies. LAWINT evolved out of two largely independently developing activities:

- Forensic Science in Law Enforcement
- National Security Intelligence

The following represents a synopsis of these elements.

A. As a methodological activity, law enforcement intelligence has roots in the *application of the scientific method* to criminal investigation (e.g., logical records systems, disseminating wanted notices, fingerprinting, photographing criminals, various forensic sciences.)

1. Each of these added a new tool for investigation and the identification of criminals

2. Most of these developments occurred independently rather than through an organized, systemic process

3. As expertise, technology, and LAWINT evolved as a body of knowledge, forensic and technological applications became increasingly important for:

   a. Collection

   b. Analysis

   c. Dissemination

B. Early military intelligence influences

1. The military employed intelligence gathering activities as a means to learn more about the enemy

2. Early attempts included

   a. War of 1812 soldiers were "planted" to gain information about enemy plans and troop movements

   b. Use of scouts in the late 1800s

   c. 1880s the Army and Navy formed intelligence units

   d. 1890s Military intelligence mounted camera's to kites to experiment with developing reconnaissance photographs

   e. In 1919 the "Black Chamber" was formed as a cryptology unit

      1. Initially to break enemy codes

      2. Grew into code making

      3. Intercepted mail and telegraph wires to read messages and codes

      4. In 1929, then Secretary of State Stinson disbanded the Black Chamber because "Gentlemen did not read other gentlemens' mail."

      5. The Black Chamber was reorganized and implemented prior to World War II

f. Important aspect of early intelligence; mostly information *gathering*—little emphasis on analysis until after cryptology influence

g. These practices—among other factors—led to the National Security influence in intelligence

C. The national security influence on the intelligence concept

1. **During World War I ...**

a. Generally recognized as the first *modern* application of intelligence methodologies in a *systemic* method

b. **EXAMPLES:** Overt and covert data gathering, developing strategies based on this data, creating integrated manual information systems

c. Developing information on persons and events through a *dossier system* which was also used after the war concerning persons deemed to be a threat to national security—Included:

1) Establishing cross-indexed and key word filing systems

2) Evaluating information for validity and reliability

3) Making projections based on the analyzed information and rating the probability of accuracy of that information

d. Significant emphasis on cryptanalysis (code breaking)

e. It should be noted that these were very rudimentary and uncoordinated applications—they served as a foundation of ideas

2. **After World War I...**

a. As a result of concern for growing world tensions and distrust, the *information* and *dossier system* used in the war were applied to:

1) Countries, persons, and events perceived to be threats to United States security

2) Potential (and sometimes perceived) criminals

b. These intelligence activities were little more than a clearinghouse—perhaps more accurately, a storehouse

1) The information was collected and stored

2) Little effective analysis and dissemination

c. During this time, public and governmental concern about crime increased due to:

1) Prohibition and increased bootlegging

2) Growth in organized crime

3) Evolution of the "high profile" criminals and their subsequent lore (e.g., Bonnie and Clyde; Barker Gang; Al Capone; Machine Gun Kelley, etc.)

4) Some increases in crime attributed to large numbers of persons discharged from the service and placed out of work in war support industries

d. This crime concern prompted...

1) Development of the Uniform Crime Reporting System (initiated by the International Association of Chiefs of Police and later assumed by the FBI)

2) A rudimentary application of the dossier and file systems used in the military to keep track of the criminals

e. *These developments represent the "roots" of data collection and analytic activity used in law enforcement intelligence*

1) A few formally designated intelligence units existed in these formative years (e.g., FBI Intelligence Section, New York Police Department's Radical Squad)

2) Law enforcement intelligence was largely a rudimentary information clearinghouse system with minimal analysis being performed

f. In 1939, President Roosevelt created the Interdepartmental Intelligence Committee (IIC)

1) The Committee's purpose was to coordinate information between:

a) Federal Bureau of Investigation

b) Military Intelligence

c) Office of Naval Investigation

2) This move was actually the first step toward creation of the modern intelligence establishment in the United States

3. **During World War II ...**

a. Intelligence activities produced greater sophistication in the:,

1) Collection strategies;

2) Enhanced comparison and analysis of information

3) More thoughtful and thorough dissemination of intelligence information

b. Greater reliance on the *scientific methods* and the forensic sciences; particularly integrating forensics into the intelligence system

c. Notably through naval research, applications of *operations research* for strategic intelligence projections (e.g., modeling theory, game theory, decision matrices, probability models, etc.)

d. Information gathering methods, covert data collection, and the dossier systems became more sophisticated

e. More sophistication in cryptanalysis and cryptography (code making)

f. Increased emphasis on methodologies of intercepting messages (cable and radio)

g. In 1941, President Roosevelt extended the concept of the IIC by creating a new position called the Coordinator of Information (COI)

1) The COI was responsible for coordinating all national security intelligence information with the intent of creating a "big picture" of national security issues and threats, notably as related to the War

2) The COI extended just this "coordination" function by adding a *research and analysis* branch—a move which proved to be important for expansion of intelligence activities

h. The rapidly increased activity of the COI resulted in further expansion of the formal intelligence structure

1) The COI was reorganized into the Office of Strategic Services (OSS) in 1942 under the authority of the Joint Chiefs of Staff (JCS)

2) Beyond being the formal intelligence office of the U.S. government, the OSS:

a) Served as a training ground for an entire generation of intelligence personnel

b) Engendered the "intelligence spirit" leading to the "discipline of intelligence"

c) Established the tradition of housing *analysis* and *operations* within the same agency

4. **After World War II...**

a. At the National Security level of intelligence...

1) There was a recognition of the need to build stronger intelligence capabilities for the security of the U.S. in light of rapidly evolving worldwide changes in:

a) Communications

b) Transportation

c) Economic relationships between countries

d) Changing political dynamics/shifting powers, worldwide

2) In 1949 the Central Intelligence Agency Act was passed creating the CIA as the next growth element of the old OSS

a) The Director of Central Intelligence (head of the CIA) became the chief intelligence advisor to the President

b) The DCI had all the previous roles of the COI and OSS but was given more authority and greater access to higher levels of decision making in government

3) From these organizational changes grew what has become known as the **Intelligence Community** which currently includes:

- Air Force Intelligence
- Army Intelligence
- Bureau of Alcohol, Tobacco and Firearms
- Central Intelligence Agency
- Customs Service
- Defense Intelligence Agency
- Department of Energy
- Department of State
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Immigration and Naturalization Service
- Internal Revenue Service
- Marine Corps Intelligence
- National Security Agency
- Navy Intelligence
- Offices for Collection of Specialized National Foreign Intelligence
- Secret Service

b. These changes in organization and emphasis had a subtle, yet definite impact on the emerging idea of law enforcement intelligence

c. During this same period of time, there was greater public and government recognition of organized crime beyond bootlegging—particularly...

   1) Gambling

   2) Prostitution,

   3) Narcotics trafficking

   4) Participation in legitimate business using illegitimate means (e.g., bribery, extortion, etc.)

d. The complexity of organized crime networks required the use of more sophisticated evidence gathering mechanisms and more complex analytic methods

e. National security intelligence techniques and practices were adopted by law enforcement to develop organized crime cases because:

   1) Of the complexity of organized crime cases

   2) Traditional police investigative methods were not fruitful—particularly with regard to the closed organized crime networks

   3) The integration of crime with legitimate business

   4) The military model was already established and shown to be effective (notably the dossier system)

   5) Many former military intelligence officers and analysts had entered the police ranks, bringing with them the military intelligence system they knew

5. Adoption of the national security model ...

    a. **Was good** because it provided a tested structure and process—the wheel did not have to be reinvented

    b. **Was bad** because it was based on a process of non-controlled information gathering with little regard to the constitutional rights afforded to U.S. citizens

    c. **Was limited** because it was not developed to collect the quantity and quality of evidence needed to sustain the burden of proof in a criminal case

D. Law enforcement intelligence development and influences ...

1. Creation of the *Law Enforcement Intelligence Unit* in 1956 consisting of several police intelligence specialist throughout the U.S. to establish a network and and share information—did not work well do to poor organization, poor communication, lack of sophistication in the intelligence process, and poor agency cooperation

2. Domestic influences on law enforcement intelligence

    a. A significant point of history affecting law enforcement intelligence was *McCarthyism*—aggressive searches for so-called Communist sympathizers who allegedly were attempting to undermine and overthrow the U.S. government

        1) Fear of Communism was pervasive during the 1950s

        2) The idea of the government giving security was appealing against this fearful and largely unknown ideological enemy

        3) The public supported the idea of identifying the "Communist threat" in this country

        4) In light of this apparent public mandate, law enforcement agencies began to collect dossiers on suspected Communists and Communist sympathizers,

a) Intent was to ...

(1) Have information in case of insurgency or overthrow attempt; and

(2) Have information on which to base some form of punishment to the Communists

b) Importantly, the data was collected as *contingency information* not in support of any known or reasonably suspect crime(s)

5) One can reasonably argue that the police acted in good faith in light of:

a) The fear of the time

b) The apparent public mandate

6) However, the actions were found to be inconsistent with the mandate of constitutional criminal procedure

7) Actually, at this point in time, the police suffered virtually no ill side effects from this practice

8) Unfortunately, the practice being institutionalized in law enforcement was establishing a trend which would later prove damaging to ...

a) law enforcement generally, and

b) law enforcement intelligence specifically

3. In the 1960s and 1970s a number of social and governmental events affecting law enforcement intelligence transgressed these decades

a. "President Kennedy's assassination in 1963 occasioned a critical review of the intelligence capabilities of the Secret Service, the FBI, and the CIA as well as many state and local criminal justice agencies. The Warren Commission Report criticized the FBI in particular, and called for expansion of **preventive intelligence** capabilities" (SEARCH, 1985:19) (Emphasis added)

b. Some accusations also arose about the inadequacy of law enforcement intelligence in the wake of the assassinations of Martin Luther King, Jr. and Robert Kennedy

c. Law enforcement intelligence also became a controversial issue in association with

   1) The riots and civil disorders of the 1960s

   2) The Vietnam War protesters,

   3) Civil Rights Movement

d. Regarding the Civil Rights Movement and the Vietnam War protesters, intelligence units were criticized for *over aggressiveness* by unlawfully intruding on the rights of citizens by

   1) Collecting information about citizens who were expressly exercising their constitutional rights in the form of lawful, peaceful protest

   2) Collecting information on people for their mere participation in domestic political activity

   3) Maintaining dossiers on citizens without having any reasonable or articulated grounds for belief that the person(s) may have committed a crime

      a) This was a direct result of the Communist dossier days

      b) Law enforcement agencies were challenged to explain and justify their actions this time

e. Conversely, regarding the riots and civil disorders, the police were criticized for having **insufficient** intelligence information

   1) This may seem a paradox, however, the difference is in the type of intelligence information that was being collected

   2) In the case of protesters, the problem was unwarranted dossiers on citizens

3) In the case of riots, the problem was that the police did not have sufficient information on ...

   a) The community dynamics:

   b) Problems within the communities

   c) The "pulse" of the community regarding the potential for riots

   d) In essence, law enforcement had not developed an adequate strategic intelligence capability

4) It is not necessarily suggested that had the police had "proper" information, the riots could have been prevented

5) It is suggested that the police could have been better prepared thus both the human and economic costs could have been reduced

f. The 1960s and early 1970s also saw the "Love Generation" which with "Hippies" and "Yippies" was somewhat unsettling to the police

   1) This was unsettling to the police because of the different lifestyles of this movement:

      a) Communal living

      b) Advocation of "free love"

      c) *Open* drug use (notably marijuana and hallucinogens to facilitate "rapping" and "getting in touch")

      d) Different "looks" (notably the clothing style, long hair, painted cars/vans)

e) Type of music ("acid" or "psychedelic" rock such as Jimi Hendrix and The Iron Butterfly)

NOTE: The "establishment" could understand the folk music of the time because of its clear messages of "peace". Acid rock music simply could not be "translated" because of its "feedback" sounds and cryptic lyrics.

f) The desire to "do your own thing" regardless of the rules (either law or custom) of society (e.g., "dropping out" of society)

2) Many of these behaviors were either lawful or only minor crimes which was frustrating to law enforcement, unaccustomed to the radical changes in lifestyle

3) The fact of their unique difference along with underlying assumptions of impropriety led the police to keep a close eye on such persons

4) Intelligence units kept dossiers on people in these groups, not because they were suspects of specific crimes, but because their "difference" was inferred to be symbolic of potential criminality

g. Police intelligence units were criticized strongly by both the Congress and the media

h. Court challenges also found that many police departments were holding unlawful intelligence dossiers and ordered

1) The so-called "Red Files" expunged and destroyed, or

2) In some cases where the police could articulate a reason to maintain the files, the subjects had to be given access to see what types of information the police had collected on them (notably in cases bordering on domestic political activity)

i. In light of these facts—and the residual impact of Watergate which illustrated scandal in government and hinted at improper use of domestic intelligence—the Congress, courts, and public became very critical of police intelligence operations

j. The old intelligence philosophy (dossier building) was giving way to new intelligence techniques

k. Fortunately, many of the new techniques were being explored at this time

4. **Recent History**

a. The legal mandates and operational developments were forging new directions in police intelligence

b. These were supported by such government reports as

1) **The President's Commission on Law Enforcement and the Administration of Justice**

"There needs to be a greater exchange of (intelligence) information among federal, state, and local agencies" (1967:20)

2) **The National Advisory Commission on Civil Disorders**

"Police departments must develop means to obtain adequate intelligence for planning purposes, as well as on-the-scene information for use in police operations during a disorder" (1968:78).

3) **National Commission on the Causes and Prevention of Violence**

"... the process of crime control in most cities lacks any central collection and analysis of criminal justice information. ... It has no mechanism for planning, initiating or evaluating system-wide programs or for setting priorities" (1968:154).

4) **National Advisory Commission on Criminal Justice Standards and Goals**

"Every police agency and every state immediately should establish and maintain the capability to gather and evaluate information and to disseminate intelligence in a manner which protects every individual's right to privacy while it curtails organized crime and public disorder" (1973:250).

c. Based on all of the above reasons, the law enforcement intelligence function has evolved (and started to loose much of its unfavorable image—including an unfavorable image in some law enforcement circles)

d. In this evolution both the intelligence community and police management ...

1) Grasped the *concepts* of an Integrated Criminal Apprehension Program (ICAP) *before* this strategy was formally proposed

2) That is, they began relying on research results to explore new applications of intelligence.

3) The research indicated

a) Previously undiscovered and emerging crime trends

b) New law enforcement intelligence strategies

e. International issues converged with law enforcement issues making LAWINT both more complex and more controversial

1) Both law enforcement and national security interests were involved in cases such as:

a) Terroristic acts...

- Against U.S. citizens
- Against U.S. officials
- On U.S. soil and reservations
- Against U.S. owned or based international carriers

b) International money laundering

c) International transportation of stolen property

d) Flight of international criminals

e) Smuggling of prohibited goods *into* the United States (such as contraband or counterfeit merchandise)

f) Smuggling of restricted trade goods *out of* the United States (such as computer hardware and software)

g) International transactions involving stolen trade secrets

h) International drug and narcotics trafficking

2) The latter crimes—drug trafficking—are notably complicated since President Reagan declared drugs to be a National Security Threat

a) As a result of this, increased international activity by the U.S. government has increased efforts to interdict and eradicate drugs

b) This involves using national security intelligence collection techniques and closer working relationships between the national security and law enforcement intelligence communities

c) The complexities proper *access to* information and *use of* the information without violating provisions of either national security restrictions and constitutional criminal procedure

3) Law enforcement has also increasingly adopted the military C^3 conceptual applications of intelligence: *Command, control, communications*

4) To further integrate the roles of law enforcement and national security organizations, a provision was included in Executive Order 12333, *United States Intelligence Activities* (1981)—*See* Figure II-1.

Figure II-1

EXECUTIVE ORDER 12333—UNITED STATES INTELLIGENCE ACTIVITIES (EXCERPT)

2.6 *Assistance to Law Enforcement Authorities*: Agencies within the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or intentional terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency; and

(d) Render any other assistance and cooperation to law enforcement agencies not precluded by applicable law.

f. *Previously undiscovered and emerging crime trends* —Included:

1) Multi-national crime cartels

2) Continuing criminal enterprises

3) Terrorism

4) Narco-terrorism

5) Merger of crime profiteering in legitimate business in complex corporate and accounting structures (including embezzlement, "insider" trading, etc.—crimes outside of "traditional" organized crime areas)

6) Serial crimes

7) Right wing extremists

8) Sophisticated money laundering

9) Bias or hate crime

g. *New intelligence strategies* —Included:

1) Applications of computer models

2) Enhanced use of automated information systems and artificial intelligence

3) Criminal (and target) profiling

4) Violent Criminal Apprehension Program (VI-CAP—discussed in detail in Chapter 10)

5) High technology eavesdropping

6) Planned and scientific approach to case development

7) Implementation of strategic intelligence

5. The most recent trends are now in the areas of:

   a. New generation computer capabilities

   b. Technological developments

   c. Better preparation (both education and training) for intelligence analysts

   d. An overall revitalization of the intelligence concept and its application

E. The cumulation and interactive effects of all these factors shaped law enforcement intelligence into its role today

F. The next important elements are:

   1. Incorporating the value-based philosophy

   2. Better preparing intelligence analysts for their job

   3. Capitalizing on evolving technologies

   4. Providing more efficient and effective use of intelligence information—both...

      a. In the field for investigations, and

      b. In management decision making

2. HISTORY OF INTELLIGENCE

Instructional Support and Criteria

GOAL:

To provide an overview of historical events leading to LAWINT as it is used in American law enforcement today.

OBJECTIVES:

1. Students will have an understanding of how LAWINT evolved from policy intelligence applications.
2. Students will be able to articulate reasons that LAWINT experienced criticisms and lawsuits as a result of past practices.
3. Students will be able to discuss the reasons why contemporary LAWINT must have a broadened perspective as a result of historical events.

STUDY QUESTIONS:

a. Describe what is meant by the "dossier system" of intelligence.

b. What **positive** influences did military/national security intelligence activities have on law enforcement intelligence?

c. What **negative** influences did military/national security intelligence activities have on law enforcement intelligence?

d. Law enforcement intelligence came under sharp criticism for its work. What were the issues focused on in the criticism which led to curtailment and change of LAWINT activities?

e. Describe the events which had the greatest effect on changing law enforcement intelligence.

NOTES

CHAPTER 3

A CONTEMPORARY PHILOSOPHY OF INTELLIGENCE

"Any intrusion into a person's private conversations or correspondence should be covered by a warrant, and no information gathered as a result of such intrusions should ever be used to harass or intimidate individuals, or to blackmail or publicly humiliate them."
Madison, WI Police Chief David Couper (1983).

1. THE ROLE OF A "PHILOSOPHY" OF INTELLIGENCE?

A philosophy serves as the *foundation* for the organization's perspective of its mission and the performance of intelligence activities. It sets the tone for defining actions which are organizationally acceptable and legally permissible. It is, in essence, the stated "conscience" of the organization.

Law enforcement intelligence (LAWINT) has always had a philosophy, however, it was not overtly stated. Rather, it evolved as custom becoming imbedded in the tradition of LAWINT. The past philosophy can be understood through a review of intelligence practices (as discussed in Chapter 2, entitled *History*). Particularly noteworthy are the problems experienced by LAWINT resulting in lawsuits against a number of law enforcement organizations which had intelligence practices that violated rights of citizens.

2. TWO PHILOSOPHIES OF LAWINT

A. **Tradition-Based** - The historical context of LAWINT wherein *information was amassed* on persons who were either suspected of directly of being involved in criminal acts or persons whose characteristics, beliefs, or associations indicated the potential for criminal involvement or that they may have knowledge about persons involved in crimes.

1. The approach of amassing the information for *contingent usage* evolved based on the integrated tradition of law enforcement and national security intelligence.

2. Inherent in the *tradition-based* approach was the problem of information **collection** and **storage.**

   a. Information was *amassed* as it become available

   b. It was disseminated rather freely for a wide range of purposes

   c. The information was rarely purged

   d. The information was often collected surreptitiously and frequently unlawfully

B. **Value-Based** - LAWINT activities which are clearly designed in support of legitimate organizational goals and performed in a manner which is consistent with law and ethical standards.

IMPORTANT NOTE: Emphasis is *not* on the *quantitative* amassing of information but on the *analysis* of collected information to yield a substantive contribution to the accomplishment of goals

1. Ideally, the law enforcement organization, or at least the intelligence function, will have formally articulated **values** which serve as *guiding principles* for the LAWINT function

2. Characteristics of *value-based* LAWINT include

   a. Use of ***legitimate means*** to accomplish legitimate goals

   b. LAWINT has specifically oriented responsibilities which are ***consistent with the mission and goals*** of the law enforcement agency

   c. ***Analytic outputs*** are emphasized over the development of large information files

   d. Information has ***wide application*** to both case development and resource allocation

e. Deviance from established LAWINT principles are ***not tolerated*** regardless of the intent of the deviation

3. THE CHANGE IN LAW ENFORCEMENT INTELLIGENCE PHILOSOPHY

Value-based LAWINT represents a *maturation* in law enforcement strategies. Tradition-based LAWINT was *adolescent*—awkward, rough, lumbering—attempting to be an all-encompassing resource which could be accessed in attempt to gain lead information to further criminal investigations.

Value-based LAWINT is more sophisticated in that it relies on more selective information and attempts to make better use of that information by establishing causal links. Tradition-based was also problematic in that the intrusive data collection methods frequently violated citizens' constitutional rights. While value-based intelligence also relies on some intrusive collection methods, they are more carefully controlled and performed in accordance with constitutional standards.

A. Characteristics of tradition-based intelligence leading to change:

1. Lawsuits for violating rights and privacy of citizens became commonplace.

2. It was not totally effective in that links between crimes, evidence, and suspects frequently not made.

3. It was a cumbersome process; it did not efficiently use or direct law enforcement agency resources.

4. There was a lack of effective training, structure, and organizationally integrated role for LAWINT.

B. The value-based approach evolved as a result of several factors:

1. There have been increases in technology facilitating strategic and tactical analysis.

2. The frequency of multi-jurisdictional crimes has increased.

3. There have been significant increases in drug trafficking—both in frequency and quantity.

4. Increased complexity of crimes (e.g., crime cartels) and criminal investigations (e.g., money laundering) has emerged.

5. There has become a demand for a comprehensive approach to integrate multi-jurisdictional crimes.

6. A need exists to maximize resource efficiency in complex, long-term criminal investigations.

7. Law enforcement administrators began taking a more aggressive stance department-wide by...

   a. Articulating formal values

   b. Emphasizing adherence to constitutional rights (emphasizing *means* is as important as *ends*)

   c. Holding officers to ethical and professional standards

C. Comparison of law enforcement intelligence philosophies

In light of the factors described above, Figure III-1 illustrates the difference between tradition-based and value-based intelligence.

4. VALUES IN LAW ENFORCEMENT

Chapter 15 of this monograph (entitled *Maintaining Control*) provides a detailed integrated discussion of ethics and values as they related to the total LAWINT function. As a point of reference, Figure III-2 presents the organizational values of the Houston, Texas Police Department.

A. These are designed to be *beliefs* and *principles* by which the police department fulfills its responsibilities

1. The values represent the department's commitment—its "social contract"—to the community

   a. The "social contract" essentially means that:

      1) The police derive their authority from the community

Figure III-1

COMPARISON OF "TRADITION-BASED"AND"VALUE-BASED" LAW ENFORCEMENT INTELLIGENCE

Tradition-Based	Value-Based
• Data-Driven	• Analysis-Driven
• Exploratory	• Contemplative
• Emphasizes Amassing Data	• Emphasizes Analysis
• Infers Crimes From Suspected Persons	• Infers Criminal Suspects From Crimes
• An Aggregate Approach To Information Collection (Dragnet)	• Targeting/Specificity On Information Regarding Reasonable Suspicion Of Crimes
• Explores All General Inferences About Potential Criminality	• Selectively Explores Crime Leads
• Explores Collected Information To See If There Are Questions To Answer	• Answers Questions By Collecting And Analyzing Information
• Develops Intelligence Files For Contingency Needs	• Develops Intelligence Files In Support of Active Crimes and Investigations
Statistics Produced For Descriptive Purposes	• Statistics Produces For Decision Making

Figure III-2

HOUSTON, TEXAS POLICE DEPARTMENT PHILOSOPHY AND VALUES

The mission of the Houston Police Department is to enhance the quality of life in the City of Houston by working cooperatively with the public and within the framework of the United States Constitution to enforce the laws, preserve the peace, reduce fear, and provide for a safe environment. The articulated values of the Houston Police Department in support of this mission are:

- Policing the community involves major responsibility and authority. The police cannot carry out their responsibilities alone; thus they must be willing to involve the community in all aspects of policing which directly impacts the quality of community life.
- The Police Department believes it has a responsibility to react to criminal behavior in a way that emphasizes prevention and emphasizes rigorous law enforcement.
- The Police Department adheres to the fundamental principle that it must deliver its services in a manner that preserves and advances democratic values.
- The Police Department is committed to delivering police services in a manner which will best reinforce the strengths of the city's neighborhoods.
- The Department is committed to allowing public input in the development of its policies which directly impact neighborhood life.
- The Department will collaboratively work with neighborhoods to understand the true nature of the neighborhood's crime problems and develop meaningful cooperative strategies which will best deal with those problems.
- The Department is committed to managing its resources in the most effective manner possible.
- The Department will actively seek the input and involvement of all employees in matters which impact job performance and manage the organization in a manner which will enhance employee job satisfaction and effectiveness.
- The Department is committed to maintaining the highest levels of integrity and professionalism in all its operations.
- The Department believes that the police function operates most effectively when the organization and its operations are marked by stability, continuity, and consistency.

2) In accepting that authority, the police agree to perform their function in a manner consistent to community social and moral standards as well as within the standards of law

3) The community, in exchange, agrees to support the police (fiscal support, legal support, emotional support)

4) While the police have the authority to restrict behavior and exercise *reasonably* intrusive practices *with just cause*, they remain accountable to the public

5) Police behavior should reflect both the *letter* of the law and the *spirit* of the law (i.e., a recognition of applied police discretion)

c. Theoretically, the concept of social contract postulates that...

"... each individual surrender[s] only enough liberty to the state to make the society viable. Laws therefore should merely be the necessary conditions of the social contract, and punishments should exist only to defend the total sacrificed liberties against the usurption of those liberties by other individuals" (Reid, 1982:87).

b. An inherent recognition of the social contract is that:

1) Authority and responsibility rest with the community, *and*

2) The police are *accountable* to the community

2. Values are applied to all functions of the agency

3. In the past few years an increasing number of police departments of various sizes and in different locales have articulated for value statements (e.g., Alexandria VA; Houston, TX; Madison, WI; McAllen, TX; Newport News, VA, among others)

B. Selected portions of the values have particular application to LAWINT

1. Adherence to the Constitution and democratic values are particularly important in light of historical abuses of LAWINT in the collection, storage, and dissemination of LAWINT information

2. The commitment to rigorous law enforcement implies the use of a wide variety policing resources—including tactical LAWINT—to deal with crime

3. The value of pursuing crime prevention can have important implications for strategic intelligence (STRATINT) as a means of analyzing crime trends and focusing preventive activities

4. Understanding the nature of crime problems in neighborhoods also has implications for STRATINT

5. The pledge that police employees will perform their tasks with integrity and professionalism is a capstone affecting both tactical and strategic LAWINT

5. VALUES SPECIFIC TO THE LAWINT FUNCTION

While a law enforcement organization may articulate formal broad values applicable to the agency as a whole, there are some principles which are particularly idiosyncratic to LAWINT operations. These values should be promulgated by the administration with adherence to these principles communicated as a clear expectation for all intelligence personnel. *See* Figure III-3.

A. These values are offered in addition to those established for the total organization.

B. The values should be supported by appropriate policy and procedures for sanctioning behavior should improprieties occur.

Figure III-3

SAMPLE VALUES FOR LAW ENFORCEMENT INTELLIGENCE OPERATIONS

Because of the sensitive nature of law enforcement intelligence activities, the Police Department establishes the following values as guiding principles for the Intelligence Unit.

- Intelligence information shall not be collected on any individual simply because that person supports an unpopular cause.
- Intelligence information shall not be collected on any individual simply because of that person's race, ethnicity, or religious affiliation.
- Intelligence information shall not be collected on any individual simply because of that person's political affiliation or political ideologies or beliefs.
- Intelligence information shall not be collected on any individual simply because of that person's personal habit, predilections, sexual preference, or lifestyle.
- Intelligence information shall only be collected using means, technologies, and methods which are legally acceptable and safeguard the constitutional rights of all persons.
- Intelligence unit personnel shall not employ or direct persons to collect information through unlawful means nor shall any unlawfully collected information be used by the intelligence unit.
- Intelligence unit personnel shall not employ nor utilize any person as an "agent provocateur" in a law enforcement intelligence operation nor shall means be used to unwittingly induce a person's participation in an unlawful act.
- Confidential information within the Intelligence Unit's records systems shall not be disseminated to persons outside of the defined distribution network without explicit authorization from a designated supervisor or manager.
- Confidential information within the Intelligence Unit's records systems shall not be used for political and/or economic purposes.

3. PHILOSOPHY OF INTELLIGENCE

Instructional Support and Criteria

GOAL:

> To instill a philosophical foundation for the performance of law enforcement intelligence which balances productive application of LAWINT with legal and ethical standards.

OBJECTIVES:

1. Students will be aware of a philosophical change in the use of law enforcement intelligence.
2. Students will have direction for development of fundamental values in the collection, analysis, and dissemination of LAWINT information.

STUDY QUESTIONS:

a. In your own words explain the need for values in law enforcement intelligence.

b. What is the pragmatic relationship of the "social contract" to LAWINT?

c. What do *you* see as the primary difference between "tradition-based" intelligence and "value-based" intelligence?

d. Review the sample values proposed in Figure III-3. Which of the values, if any, do you feel would hamper effective intelligence activities. Explain your reasoning. If you think all of the values are appropriate, justify your position.

NOTES

CHAPTER 4

THE ORGANIZATION AND ADMINISTRATION OF AN INTELLIGENCE UNIT

"Knowledge of the spirit world is to be obtained by divination; information in natural science may be sought by inductive reasoning; the laws of the universe can be verified by mathematical calculation; but the dispositions of the enemy are ascertainable through spies and spies alone."
Chinese Philosopher and Warrior
Sun Tzu, Circa 510 B.C.

1. ESTABLISHING AN ORGANIZATIONAL FRAMEWORK

Just as any other function in a law enforcement agency, organizational attention must be given to the administrative structure of the intelligence unit (INTELUNIT). Administrators and managers must examine:

- The *need* for the unit,
- *How it functions* on a daily basis,
- Issues of *resource* acquisition, deployment, and management, and
- The *future agency needs* for the intelligence function.

This section generally examines a wide range of administrative issues associated with intelligence operations. Concerns are addressed which affect the central administration of the agency, the unit's specific chain of command, and the personnel within the unit. It is assumed that the reader has a fundamental knowledge of administrative principles. Based on this assumption, the substance of this section focuses on specific issues of intelligence management.

A. The need and role of the intelligence unit (INTELUNIT)

1. The unit's presence or planned creation indicates a perceived need for intelligence

   a. This need must be assessed to determine the validity of the need

   b. It may be that such an assessment will indicate that

1) Need is not warranted

2) Need is not warranted under the present structure

3) The INTELUNIT's responsibilities are too broad

4) The INTELUNIT's responsibilities are too narrow

5) The INTELUNIT's direction is insufficiently defined

6) The INTELUNIT's role has not been clearly articulated

c. If any of these problems or questions exist, they need to be resolved before any other management concern is addressed

2. On the issue of the need for an INTELUNIT, Dintino and Martens noted:

> "If properly operationalized and staffed, the intelligence component serves as an in-house consultant or advisor to management. It defines the scope and dimensions of the problem, recommends alternatives and options, and most importantly, provides an internal mechanism for critical reflection and discourse. It draws upon the specialized knowledge of in-house specialists (criminologists, sociologists, economists, political scientists, and attorneys) who engage in critical analysis, void of institutional pressures, constraints, and ideologies" (1983:18).

3. There has been reluctance by some law enforcement agencies to fully develop an intelligence unit—including both tactical and strategic activities—for several reasons (*See* Figure IV-1; Dintino & Martens 1983:19-21):

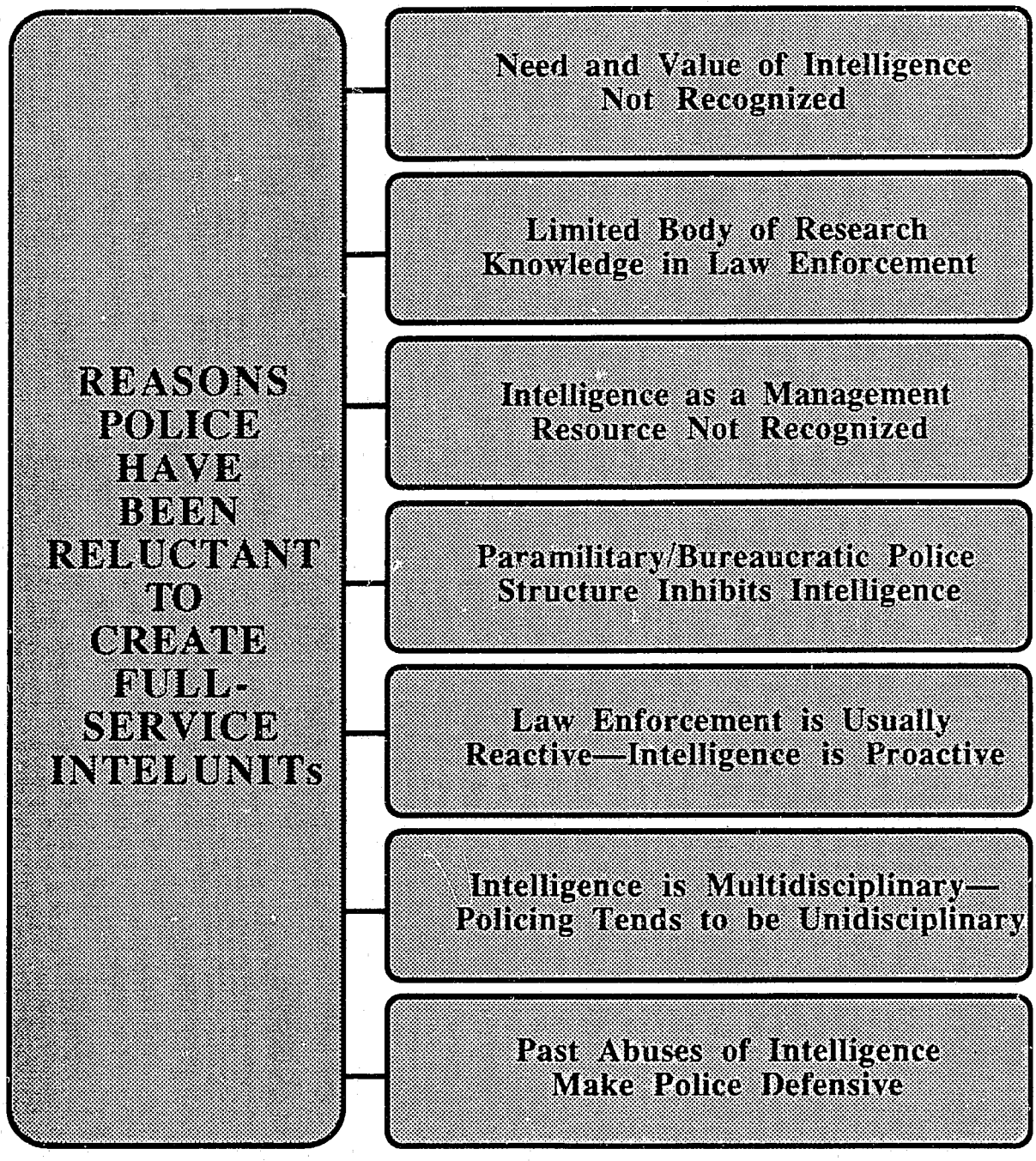
a. The need and value of an INTELUNIT is not recognized

b. Law enforcement administration has a relatively limited body of knowledge related to research and applications of the scientific management to the resolution of law enforcement management problems

c. The lack of understanding of the role and capabilities of intelligence as a *management resource*

Figure IV-1

REASONS LAW ENFORCEMENT AGENCIES ARE RELUCTANT TO ESTABLISH INTELLIGENCE UNITS



d. The paramilitary structure and bureaucratic nature of most law enforcement organizations is inconsistent with the operational and research activities of a full intelligence unit

e. Most law enforcement agencies are *reactionary*—responding to crises—rather than being proactive—anticipating crises

f. Intelligence activities are inherently multidisciplinary, whereas police management traditionally tends to be inwardly focused and more unidisciplinary

g. The misuse and abuse of intelligence in the past has made law enforcement take a defensive posture on the issue

B. Administrative commitment

1. If agency administrators determine an INTELUNIT is justified, they must give that unit:

   a. Philosophical and administrative support

   b. Sufficient organizational authority

   c. Sufficient direction or a "charge"

   d. Sufficient resources to perform the defined duties

   e. Sufficient time to demonstrate its ability to perform as intended

2. It is not suggested that the INTELUNIT should necessarily take precedence over any other unit with respect to organizational commitment—it should be noted, however, by the nature of the intelligence function...

   a. A new unit will take a notable amount of time to functionally evolve;

   b. An established INTELUNIT, if not effectively organized and administered, needs time for self-assessment and revised operations

3. Importantly, administrators must understand the concept of law enforcement intelligence (LAWINT)

a. There sometimes exists a misdirected perception of what the LAWINT function is or what it can perform

b. A tendency exists to narrowly perceive:

1) The types of crimes subject to tactical intelligence

2) The information available for decision making through strategic intelligence

4. With organizational commitment, the INTELUNIT needs to be *chartered*—the charter will define the INTELUNIT's

a. Mission

b. Goals

c. Authority

d. Responsibility

5. **Mission**

a. *Defined*:

> The mission is the *role* which the unit fulfills in support of the overall mission of the agency—it specifies in general language *what* the unit is intended to accomplish.

b. It establishes the *direction and responsibility* for the INTELUNIT for which all other administrative actions and activities are designed to fulfill

NOTE: See Figure IV-2 for sample mission statement from one law enforcement agency

Figure IV-2

SAMPLE MISSION STATEMENT

The mission of the Intelligence Unit of the Hypothetical Police Department is to collect, evaluate, analyze, and disseminate intelligence data regarding criminal activity in this city/county and any criminal activity in other jurisdictions that may adversely affect this city/county. The Intelligence Unit will furnish the Chief of Police with the necessary information so that Operations Units charged with the arrest responsibility can take the necessary enforcement action.

6. **Goal**

a. *Defined*:

> A goal is the end to which all activity in the unit is directed.

1) It is broad based, yet *functionally* oriented

2) Importantly, the goal must *mission-related*—that is, accomplishment of goals support the mission of both:

a) The agency

b) The INTELUNIT

b. The goals will give the unit direction in support of the mission

c. Since the mission of an INTELUNIT will typically be comprehensive and incorporate diverse functions, multiple goals will typically be stipulated;

d. In that the environment of the community will change over time as will crime patterns and problems, goal statements should be reviewed on an annual basis and changed or revised to reflect current issues and trends

NOTE: Figure IV-3 illustrates the LAWINT *goals* of one agency

7. **Authority**

a. *Defined*:

> The right to act or command others to act toward the attainment of organizational goals (Robbins, 1977).

Figure IV-3

SAMPLE GOAL STATEMENTS

1. The Intelligence Unit shall supply the Chief of Police with accurate and current strategic intelligence data so that the Chief will be kept informed of changing criminal activity in the jurisdiction.

2. The Intelligence Unit shall provide a descriptive analysis of organized crime systems operating within the jurisdiction to provide operational units with the necessary data to identify organized crime groups and individuals working as criminal enterprises.

3. The Intelligence Unit will concentrate its expertise on the following crimes:

a. **Outlaw motorcycle gangs** - organizational structure, participants, and types of crimes.

b. **Racial/Anti-Semitic activity** - monitor, record, and give investigative assistance to operational units regarding these types of criminal activity.

c. **Labor/strike activity** - monitor and gather strategic intelligence to be supplied to the Operations Bureau with regard to this activity.

d. **Subversive/Extremist groups** - to closely monitor and disseminate information regarding extremist groups such as the *Ku Klux Klan*, *Nazi Party*, etc., whose actions typically involve criminal activity.

e. **Major Narcotics Traffickers** - provide tactical intelligence and information analysis to the Operations Bureau on persons identified as being involved in narcotics trafficking enterprises.

4. The Police Intelligence Unit recognizes the delicate balance between the individual rights of citizens and the legitimate needs of law enforcement. In light of this recognition, the unit will perform all of its intelligence activities in a manner that is consistent with and upholds those rights.

b. ***Organizational Authority***

1) What type of authority does the administration view the INTELUNIT to have:

   a) Line authority as contributing directly to organizational goals, or

   b) Staff authority which advises and supports the line

2) Whereas the INTELUNIT as a staff function is the most common model, some agencies may perceive the need to place it as a line function

3) If the INTELUNIT is organized as a line function, the administrator must consider this:

   a) Would maintain better control of its cases

   b) Would enhance security of information and cases

   c) Would ease coordination problems by not having to rely on other units

   d) Would have enhanced flexibility

   e) Would minimize liability for improper records management

   f) Would have to assign sworn personnel

   g) Would be actively involved in undercover work and information collection

   h) Would require more resources in order to perform its function

   i) Would tend to engender conflict between the INTELUNIT and investigators or undercover units

   j) Would tend to become more elitist, perhaps being more isolated from other units within the department

4) The line/staff decision is one that must be made within the context of each department based on:

   a) The agency's jurisdiction

   b) The agency's size and resources

   c) Any unique or particularly pervasive crime problems requiring intelligence operations

   d) Any unique or pervasive problems concerning major case confidentiality or security

   e) The responsibilities of other units within the department which would typically work with the INTELUNIT

   f) The formal role of the INTELUNIT with regard to other law enforcement agencies

c. ***Operational authority***

1) Decisions must be made concerning:

   a) The degree and type of activities the INTELUNIT may perform without seeking administrative authorization

   b) Financial flexibility of unit to fulfill its objectives

   c) Types of inter-departmental records the INTELUNIT has access to without special authorization

   d) Degree of direction or precedence the INTELUNIT can exercise over other departmental units

   e) The extent to which the INTELUNIT can maintain "case security" and withhold information from other department units or administrative personnel

2) The nature and limitations of operational authority should be stipulated in written policies and procedures

8. **Responsibility**

a. *Defined*:

> Responsibility reflects how the authority of a unit or individual is used and determining if goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority

b. The unit and its members must be held accountable for its charge and administrative mechanisms must be set in place to assess the degree to which the unit is meeting its responsibilities

9. Collectively, the mission, goals, authority, and responsibility all reflect the *organizational charter* of the INTELUNIT

2. ORGANIZATIONAL FUNCTIONS

There are extensive organizational principles which apply to every element of law enforcement administration. The issues discussed below are not intended to be comprehensive. Rather, specific elements of organizational functions have been identified and discussed in light of their special application to an INTELUNIT.

A. Planning

1. *Defined*:

> Planning is the anticipation of future situations, estimating organizational demands and resources needed to attend to those situations, and initiating strategies to respond to those situations.

a. Planning is an ongoing responsibility, typically of the unit administrator or supervisor

b. Personnel within the unit should also be attentive to planning issues in order to address issues they identify during the course of their work

2. Within the INTELUNIT, planning issues can be classified based on:

   a. Unit organization and development

   b. Unit administration

   c. On-going operations

3. Within this tripartite model, the person(s) responsible for INTELUNIT planning should answer the following questions:

   a. **Unit Organization and Development**

      1) How extensive will resource allocation to the INTELUNIT be in comparison to other organizational units?

      2) Do the crime patterns in the jurisdiction warrant an INTELUNIT?

      3) If so, are the unit's anticipated size, structure, goals, and responsibilities consistent with the crime demands?

      4) What is the relationship of the INTELUNIT to other units in the department?

      5) Will there be changes needed in the authority and responsibility of the unit?

      6) How comprehensive will the unit be? Macro? Micro? Specific? General?

      7) What growth patterns, if any, are expected in the unit and what expertise will be needed to respond to growth?

      8) What are the anticipated equipment needs for the unit depending on changes in size, crimes pursued, and "products" of the unit?

   b. **Unit Administration**

      1) What criteria and procedures will be used to target crimes to be addressed by the unit?

2) What type of strategic intelligence reports are expected and on what schedule?

3) What will be the relationship and extent of resource allocation...

   a) For investigating crimes which occur outside the jurisdiction but have an impact on the jurisdiction

   b) For contributing INTELUNIT resources to extra-jurisdictional multiple agency investigations

4) On what criteria are INTELUNIT goals changed or revised?

c. **On-going Operations**

1) What types of intelligence information will the unit produce? Strategic? Tactical?

2) What will be the unit's performance measures and why?

   EXAMPLES:

   a) Number and types of strategic reports generated

   b) Number of cases resolved for court disposition

   c) Complexity and/or diversity of cases involved in

   d) Perceived usefulness of INTELUNIT by investigators and administrators

   e) Obviously difficult to assess—performance measures are dependent on goals, needs, and unique characteristics of the unit and agency

3) How can on-going, forward-looking goal preparation be best accomplished

4) Based on changing intelligence needs, are any unique staffing patterns emerging (e.g., accountants for tactical intelligence; researchers or statisticians for strategic intelligence, etc.)?

5) Are new training programs needed or anticipated based upon new crime trends (e.g., bias crime, computer-related crime, new drugs or trafficking patterns, etc.)?

6) Do alterations in crime trends indicate the need for formal links with specialized agencies or different jurisdictions?

7) How could the INTELUNIT better serve other units within the agency?

B. Organizing

1. *Defined*:

> The rational coordination of the activities of a number of people for the achievement of some common explicit purpose or goal through division of labor and function and through a hierarchy of authority and responsibility (Swanson, Territo, and Taylor, 1988:50).

2. Organizing the INTELUNIT depends on a number of factors discussed previously:

   a. It is goal directed and must coordinate resources and functions to support integrated goal attainment

   b. It relies on authority to exert organizational needs and is accountable for the success of the organizing efforts via responsibility

3. Certain organizational principles are worthy of note ;with respect to the organization and administration of the INTELUNIT

   a. **Coordination** - *Defined*:

> The processes of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

1) An INTELUNIT will necessarily have overlapping responsibilities within the organization, such as:

   a) Tactical intelligence

      • Criminal investigation division
      • Vice and narcotics unit

   b) Strategic intelligence

      • Planning and research
      • Administrative resources sections

2) The unit will also have to rely on support from other units such as records, computer operations, and investigations

3) Administrators and supervisors must ensure...

   a) A cooperative environment exists

   b) Procedures are articulated which stipulate the processes of information, assistance, and resource exchange

   c) Subordinates work cooperatively with other units

   d) When problems arise, they are worked out with other units rather than being "forced"

3) Extra-jurisdictional coordination

   a) As noted earlier, the nature of the intelligence function is particularly susceptible to interaction with other law enforcement agencies—sometimes on a regular basis

   b) Procedures for intelligence and information release or exchange with other agencies (with and without Mutual Aid Pacts) must be coordinated with those agencies as well as applicable internal units

b. **Division of labor** - *Defined*:

> Tasks within the organization are divided among personnel based on expertise required to perform the tasks, demand for the tasks to be performed, or, due to the inherent nature of the tasks, there is a need for close supervision and/or security; specialization of duties is part of the division of labor.

1) Within the INTELUNIT administrators must examine the crime demands and unit goals to determine the extent of division of labor

2) High narcotics trafficking or the pervasive presence of organized crime are examples wherein special personnel assignments (or subunits) within the INTELUNIT may focus only on these crimes

3) The need to conduct financial crime investigations associated with money laundering is an example where the division of labor may be based on expertise

4) In some cases, the division of labor may be on a temporary, or task force, basis to investigate a particular crime

EXAMPLE: A serial murder case in a jurisdiction may require a division of labor, either internal to the unit or a multi-unit task force within the agency, to concentrate on the crimes until the cases can be closed.

c. **Unity of Command** - *Defined*:

> The principle of organization referred to as "one man, one boss". Each person within the organization should be operationally and functionally responsible to *only one* supervisor.

1) In intelligence, this can become a problem when an analyst is working exclusively, or nearly exclusively, on a major case

2) In such cases, the analyst will be working closely with operations investigators

3) Unity of command becomes a problem when an investigations supervisor gives direction to the analyst

4) Who is the analyst responsible to? The investigations supervisor or the INTELUNIT supervisor?

5) The problem can be worked out rather easily, including options such as temporary operational assignment to the investigations supervisor during the course of the case

6) The important aspect is that the problem is addressed as a matter of policy and procedure

4. Functional and operational organizational issues

a. **Hierarchical organizational placement**

1) Where is the INTELUNIT to be placed in the command structure...

- Directly responsible to the chief?
- Responsible to an operations bureau commander?
- Responsible to criminal investigations division commander?

2) The hierarchical placement of the INTELUNIT influences both the formal and informal authority of the unit—the higher in the hierarchy, the more inferred authority of the unit

3) Hierarchical placement of the unit is indicative of the unit's "influence, power, and access"

b. **Physical placement of the unit**

1) When an INTELUNIT is created it must be physically placed somewhere whether it is in headquarters, a substation, or alternate location

2) The physical placement of the INTELUNIT must focus on three basic criteria:

   a) *Convenience* - The INTELUNIT needs to be placed so personnel have access to needed resources such as records, lock-ups where suspects may be interviewed, and computer facilities (depending on the nature of computer resources the agency has)

   b) *Sufficiency* - As with any organizational unit, the INTELUNIT needs sufficient space to perform its function; this includes...

      - Individual analyst areas
      - Meeting/conference room
      - Space for microcomputers and/or computer terminals
      - Secretarial/support area
      - Sufficient room to store the many records and items collected as part of the intelligence process.

      NOTE: It should be remembered, that many INTELUNIT records must be segregated from other departmental records, thus facility planning must account for this

   c) *Security* - Because of the sensitive nature of the intelligence function, the physical placement of the unit must be one which maximizes the security of records, activities, personnel, and persons visiting the unit as part of the intelligence function

c. Organizational communications

1) It is essential that administrators communicate to agency personnel...

   a) The role of the unit

   b) The capabilities of the unit

   c) How the INTELUNIT can be used as a resource

d) How to input information into the unit

2) The authority and responsibility of the INTELUNIT must be clear to all personnel

C. Direction

1. Direction involves the tasks of:

   a. Making decisions

   b. Guiding the organization or unit toward its goals

   c. Ensuring consistency in performance

   d. Providing leadership to the organization as a whole and to individuals

   e. Ensuring compliance with authority and responsibility mandates

   f. Ensuring comprehensive task performance

   g. Establishing mechanisms and procedures to deal with personnel who do not perform adequately, lawfully, or within the bounds of organizational authority

2. While many activities are involved in direction, a critical aspect of this responsibility is *the articulation of policy, procedures, and rules*—collectively known as **directives**

3. *Definitions...*

   a. **Policy**

> The principles and values which guide the performance of a duty. A policy is *not* a statement of what must be done in a particular situation. Rather, it is a statement of *guiding principles* which should be followed in activities which are directed toward the attainment of goals. (Carter, Embert, and Payne, 1987:11).

b. **Procedures**

> A method of performing an operation or a manner of proceeding on a course of action. It differs from policy in that it directs action in a particular situation to perform a specific task within the guidelines of policy. Both policies and procedures are goal oriented. However, policy establishes limits to action while procedure *directs responses* within those limits.

c. **Rules**

> A specific requirement or prohibition which is stated to prevent deviations from policy or procedure. A violation of a rule typically results in an internal investigation and may result in disciplinary action.

NOTE: See Figure IV-4 for a sample LAWINT policy, procedures, and rule.

4. The INTELUNIT has needs for specific directives to address the intelligence function in order for the unit to achieve its goals within the authority that has been vested in the unit

5. Collectively the directives will authorize and give guidance to every aspect of INTELUNIT organization and administration discussed herein

6. A manifest of topics for directives in support of the INTELUNIT and intelligence related functions may be found in Figure IV-5

7. Two sources providing additional information on directives (as well as other intelligence administration matters) are:

   a. "Standard 9.11--Intelligence Operations". *National Advisory Commission on Criminal Justice Standards and Goals: Report on Police*. Washington: U.S. Government Printing Office, 1973.

Figure IV-4

SAMPLE PORTIONS OF A DIRECTIVE ON *INFORMATION SECURITY* TO ILLUSTRATE POLICY, PROCEDURES, AND RULE

POLICY:

The Intelligence Unit collects a wide variety of sensitive information on persons suspected of criminal activity. Because release of sensitive information could jeopardize the safety of undercover investigators, jeopardize the integrity of the investigation, and cause harm or embarrassment to the individual targeted in the investigation if the allegations are untrue, it is the policy of this department to not release classified intelligence information to persons outside of the Intelligence Unit unless such release is consistent with the procedures set out in this directive or the release is pursuant to a lawful court order.

PROCEDURE:

•
•
•

3. RELEASE OF INTELLIGENCE INFORMATION TO LAW ENFORCEMENT AGENCIES AND THE "THIRD AGENCY RULE"

   a. The Intelligence Unit may release classified case information to another law enforcement agency if

      1) The agency certifies the information is needed in support of a criminal investigation.

      2) The information release would not violate privacy or civil rights of the person(s) who are the subject of the information.

      3) The person to whom the information is released is a member of the Intelligence Unit or has an equivalent intelligence or investigative responsibility of a government law enforcement agency.

   b. Information released to the agency may include copies of surveillance reports, copies of incident and arrest reports, information obtained through searches of criminal history records and other information systems, copies of open documents, news reports, and other open materials which have relevancy to the investigation.

(Figure IV-4 concluded...)

1) Requesting agency representatives may view association matrices, commodity flows, link analysis, and narrative hypothesis reports developed by our intelligence analysts but may not be given copies of these materials without the written permission of the Intelligence Unit supervisor on-duty.

2) Copies of photographs, videotapes, and audio tapes produced as part of the intelligence collection process may be provided with the approval of the Intelligence Unit supervisor on-duty.

3) Copies of departmental mug shots are not part of this exclusion and may be freely released.

4) No reimbursement for copies of materials released will be required unless, after consultation with the supervisor, the intelligence analyst feels that the information is of such bulk that reimbursement for reproduction should be made.

c. The receiving agency must sign an agreement of confidentiality concerning the information.

d. The agency must certify that it will abide by the **Third Agency Rule** and not release the information to any other law enforcement organization and refer that organization to this agency.

RULE:

No person shall release classified intelligence information except in accordance with the procedures stipulated in this directive.

Figure IV-5

MANIFEST OF SUBJECT AREAS FOR DEVELOPMENT OF INTELLIGENCE UNIT DIRECTIVES

- INTELUNIT Organization, Role and Responsibilities
- INTELUNIT Staff Position Requirements, Selection and Training (Particularly important when analysts are not sworn personnel)
- Intelligence Unit Records Management
  —Quality Control Procedures for Data and Information
  —Reviewing, Archiving and Purging Records
- Access and Documentation of Use of Information From...
  —The International Criminal Police Organization (INTERPOL)
  —The El Paso Intelligence Center (EPIC)
  —Investigation or Intelligence Records of Other Jurisdictions
- INTELUNIT Reporting Procedures and Dissemination
- Undercover Operations in Support of the Intelligence Function
- Undercover Reporting Procedure
- Investigative and Undercover Expense Fund Accountability
- File Maintenance of Tips and Incidental Field Interviews
- Classification and Security System for the Agency and/or INTELUNIT
- Rules for Violations of the Security System
- Surveillance Operations
- Consumption of Alcoholic Beverages During Undercover Operations or Surveillance
- Narcotic Simulation During Undercover Narcotic Investigations
- Access to Equipment and Resources in Support of Intelligence Activities

b. "Chapter 51--Intelligence". Commission on Accreditation of Law Enforcement Agencies (CALEA). *Standards for Law Enforcement.* Fairfax, VA: CALEA, 1984.

NOTE: See Appendices for copies of these standards.

D. Organizational Control and Accountability System

1. Many of the administrative issues discussed above intimate the clear need to establish control and accountability systems for:

   a. Resource usage

   b. Investigative funds

   c. Records access and maintenance

   d. Production of intelligence reports/products

2. This administrative function would embody such activities as:

   a. Auditing activities of intelligence unit for propriety

   b. Inspection of unit activities for adherence to policy and procedures

   c. Establishing means and authority of INTELUNIT internal investigations

   d. Identifying needs and establishing processes, as appropriate, for security clearances

   e. Information release procedures

   f. Special budgeting issues

      1) Equipment

      2) Travel

      3) Special investigative funds

E. Evaluation

1. Evaluation of INTELUNIT activities must occur at two levels:

   a. The unit overall

   b. Evaluation of individuals within the unit

2. Evaluations are important to ensure:

   a. Performance has been goal directed

   b. Activities of the unit have been fruitful

   c. Each element and individual in the INTELUNIT is contributing to the unit's mission

   d. The unit's resources are not being wasted

3. Evaluation can also identify problem areas and insufficiencies which can be built into the planning process for remedial action

4. A number of factors are interrelated with INTELUNIT evaluation—these will be discussed in detail in Chapter 15 entitled **Maintaining Control**

3. STAFFING

One of the most critical responsibilities of management in any organizational environment is staffing. Personnel represent the organization's largest investment, its greatest source of productivity, and its greatest source of problems.

The INTELUNIT provides some unique staffing issues in that the unit will typically have an admixture of sworn and civilian personnel frequently performing the same or similar tasks. The role and "organizational life" of these two groups are quite different and can lead to problems such as inconsistency in performance and conflict. This is complicated by the fact that civilian analysts are doing important crime-related work and frequently need to give direction to investigators in the field on avenues to pursue in a case. Many staffing problems can be resolved before they occur if

- The "right person" is selected for the position,

- That person is properly and effectively trained to perform his/her responsibilities, and

- Personnel problems—such as conflict in role or authority—are identified and addressed before they become a problem.

A. Staffing an organizational unit includes:

1. Personnel selection

2. Personnel training

3. Personnel placement/assignment

B. Collateral staffing functions may also include:

1. Personnel motivation

2. Job enrichment

3. Personnel problem solving

4. Promotional preparation

C. Staffing occurs at the:

1. *Functional level* - those positions in the unit where the direct goal-oriented work of the unit is being performed (e.g., intelligence analysts or technicians)

2. *Support level* - those positions in the unit which provide support and assistance to the functional level (e.g., clerks or secretaries)

3. *Hierarchical level* - those positions in the unit which represent the chain of command (e.g., supervisors or managers)

D. Should INTELUNIT staffers be sworn or civilian?

1. This answer will depend on:

a. The size of the INTELUNIT,

b. Its breadth of responsibility,

c. The autonomy assigned to the unit to perform its various functions—particularly the collection of information, and

d. Factors of personnel management, including:

1) Civil service rules
2) Union contracts
3) Historical personnel management practices of the department

2. The position of intelligence *analyst* would probably best be served over the long term by a civilian because:

a. The characteristics and background desired in an analyst may be somewhat different than those found in sworn personnel

b. While "street" experience as a law enforcement officer may help the analyst understand the investigative process, this experience could also be a deficit

1) It can narrow the perspective of the analyst

2) The analyst needs to view crime problems from the "big picture"

3) The street experience tends to make the person's view more provincial

c. The analyst builds his/her expertise and knowledge on a cumulative basis throughout his/her work life

1) Much of this expertise is substantive knowledge and information (e.g., persons, crime patterns, locations, etc.) learned on working intelligence cases and interacting with persons in the INTELUNIT

2) A sworn officer is likely to either transfer out or be promoted out of the INTELUNIT thereby reducing the unit's overall efficiency

d. The function of an analyst does not require law enforcement authority, thus placing a sworn person in an analyst's position

may be viewed as "wasting" the officer's/agent's training and authority

3. If the unit is organized as a line function or given line responsibilities (such as undercover work), then sworn personnel would be needed to fulfill those applicable roles

4. Staffing *supervisory* positions in the INTELUNIT can become an issue

   a. Sworn personnel do not like to be supervised by civilians, thus a source of conflict exists

   b. Without the chance of being promoted, a civilian intelligence analyst might experience burnout or at least have his/her job satisfaction and morale suffer due to limited opportunity for upward mobility

   c. Sworn supervisory personnel, who will typically "rotate" through a unit, will not have the knowledge and expertise of a civilian analyst who has evolved with the unit

   d. In dealing with other units of the department and other agencies, sworn personnel may not receive as much resistance as a civilian supervisor

5. The impact of these problems/issues will vary greatly depending on the organization's environment and the legacy of civilian employment within a given agency

6. There are clearly mixed models of civilian and sworn personnel in law enforcement agencies throughout the country—an agency can only examine the issues closely as applicable to that department and make decisions in light of that examination

7. The recommended model is:

   a. Civilian analysts with a civilian chain of command

   b. Liaison officer who is sworn

   c. Intelligence units with line responsibilities need sworn personnel in those positions with a sworn supervisor

E. Selection of intelligence analysts

1. **Intelligence Analyst** - *Defined*:

> A person who takes the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a crime and places them into a logical and related framework for the purpose of developing a criminal case, explaining a criminal phenomenon, or describing crime and crime trends.

a. In tactical intelligence, the framework will consist of:

1) Identifying the principals in the crime and their relationships

2) Tracking commodities and instrumentalities involved in the crime

3) Establishing the framework of a wide variety of evidence for case presentation in court

b. In strategic intelligence the framework is to describe trends and make projections

c. The analysts duties will vary depending on the jurisdiction of employment and whether the analyst is sworn or a civilian—beyond the analytic function, duties may include:

1) Conducting interviews

2) Participating in surveillance

3) Working with undercover officers/agents to develop a case strategy

4) Field research for records and other materials for which the analyst has a better understanding of needs than the investigator

d. The analyst should be capable of effectively performing the basic duties as outlined in Figure IV-6

Figure IV-6

MAJOR TASKS TO BE PERFORMED BY A LAW ENFORCEMENT INTELLIGENCE ANALYST†

INTELLIGENCE ANALYST RESPONSIBILITIES ELEMENT A

Read and Determine Disposition of Information Received

Determine Whether Material is of Sufficient Value to be Indexed and Filed	If of Value, the Information Must be Assigned an Accession Code & Indexed	Determine *if* Material Should be Circulated to Other Analysts—If So, *To Whom*

INTELLIGENCE ANALYST RESPONSIBILITIES ELEMENT B

Providing Tactical Support to Investigators Working a Case

Any New Material From Current Cases Should Automatically be Checked for Names, Addresses, etc. With Results Reported to Investigators and/or the Case Supervisor	Analyst Keeps List of Known Current Cases in his/her Field of Responsibility and Reviews All Incoming Material to Determine if New Material Should be Brought to the Attention of the Case Supervisor

(Figure IV-6 *Continued...*)

INTELLIGENCE ANALYST RESPONSIBILITIES ELEMENT C

Respond to Requests for Assistance Regarding Known or Alleged Criminals

Request File Search by File Clerks and Records as Appropriate	Have Files Checked Regarding and *Associate* or Other Criminal Activity That Surfaces

INTELLIGENCE ANALYST RESPONSIBILITIES ELEMENT D

Develop Expertise in Areas of Responsibility

Develop and Maintain Lists of Major Criminals in the Analyst's Area of Responsibility	Develop Location (Geographic Based) Foci of Crime for Which the Analyst is Responsible	Develop Understanding of Crime Patterns With Current Strategic Intelligence Data	Be Alert for Developing Patterns of Criminal Activity Occurring in New Areas	Continue to Develop Personal Expertise and Skills as Notably Related to Work Assignment

INTELLIGENCE ANALYST RESPONSIBILITIES ELEMENT E

Perform Strategic Analysis As Related to Current Cases and Field of Responsibility

Connect Current Case (or Cases) to Other Potential Cases or Patterns of Crime	Connect Criminal Activity in One's Field of Responsibility to Other Criminal Activity	Maintain a Correlational Inventory Between Crimes, MO's, and Criminals	Develop Self Generated Topics for Strategic Intelligence Reports

INTELLIGENCE ANALYST RESPONSIBILITIES
ELEMENT F

Develop Requirements for Information to Fill Gaps. Priority Suggested by Major Criminals and/or Location for Such Activity or by Major Cases Currently Being Investigated ...			
... As Needed With Respect to Current Cases In Which the Analyst is Advised	... As Developed as Part of the Analyst's Self-Generated Study of Crime Problems	... As Needed With Respect to Developing Strategic Study of Areas of Crime	... As Needed to Complete files and Forms for Current Intelligence Data

†Adapted with modification from Harris, (1976).

2. The duties and responsibilities of an intelligence analyst must be articulated by the administration in light of the unit's mission, goals, and organization

   a. These should be embodied in a job description

   b. The job description articulates the responsibilities of a person employed in a given position stipulating:

      1) Duties to perform

      2) Qualifications to fulfill those duties

      3) Criteria for performance evaluation

   c. Each position in the hierarchy as well as each *different* position assignment should have a job description

      NOTE: Ideally, the job description is a product of a "job task analysis" which assesses each position requirement in minute detail. A sample Intelligence Analyst job description is illustrated in Figure IV-7. Figure IV-8 illustrates the tasks for which an analyst is typically responsible

3. Qualifications for an intelligence analyst

   a. **Articulated qualifications** - those which are required as minimum by law, charter, or regulation—will be easily identified following a review of applicable statutes.

   b. **Performance qualifications** - those minimal requirements which can be clearly articulated and measured (e.g., college degree, no felony arrests, etc.) and can be *demonstrated to be job related* (a Bona Fide Employment Qualification-BFOQ)

      NOTE: Ideally, the job task analysis is the basis for identifying these qualifications

   c. **Preferred qualifications** - those additional qualifications desired for job candidates (e.g., intelligence experience, knowledge of computerized statistical packages, etc.)

Figure IV-7

SAMPLE JOB DESCRIPTION FOR A LAW ENFORCEMENT INTELLIGENCE ANALYST

JOB TITLE: Intelligence Officer I

CLASSIFICATION: Job Code: 132 Object Code: 1 Grade: 11

JOB SUMMARY:

This is an analyst position assigned to the Law Enforcement Intelligence Unit. The employee will serve as a beginning intelligence analyst primarily assigned to general casework and may be assigned to major projects or task forces assisting an Intelligence Officer II, Intelligence Officer III, or Intelligence Supervisor. Primary responsibilities are:

- Providing technical analytical skills to general intelligence projects (case work) to support the mission and goals of the Intelligence Unit.
- Providing technical analytical skills to major intelligence projects to support the mission and goals of the Intelligence Unit.
- Providing technical assistance to intelligence specialists within the Unit as directed.

JOB CONTROLS:

Works under the direct supervision and broad guidelines of the Supervisory Intelligence Officer of the General Intelligence Section. The employee expected to adhere to organizational directives and exercise initiative in planning and executing assigned responsibilities within these guidelines. Accomplishments are reviewed by the supervisor in terms of contributions to project assignments.

MAJOR DUTIES:

1. The employee is responsible for, but not limited to, the following activities:
   - Collation and in-depth analysis of data and information relating to the crimes on projects assigned.
   - Providing technical assistance to Intelligence Specialists.
   - Providing technical advice to Investigators on the same case assignment.
   - Evaluating information to be employed as part of the total project analysis effort.
2. Assists a Senior Intelligence Officer on specific projects and serves as a principal source of technical skills for the effort.
3. Disseminates intelligence, including oral reports to the supervisory level.
4. Suggests new projects to the Intelligence Supervisor.

Figure IV-8

RECOMMENDED PRE-SERVICE TRAINING SUBJECTS FOR INTELLIGENCE ANALYSTS

GENERAL INTELLIGENCE TRAINING SUBJECTS:

- An Overview of the Law Enforcement Intelligence Concept (Including definitions and classifications)
- Past Problems and Issues Facing the Intelligence Analyst
- Intelligence Agencies at Various Levels of Government and Their Responsibilities
- Techniques in the Analytic Process
  - —Link Analysis ("Wire Diagrams")
  - —Commodity Flow Charts
  - —Association Matrices
- Law and Legal Issues
  - —Criminal Law
  - —Criminal Procedure
  - —Civil Rights
  - —Freedom of Information Act
  - —Privacy Act
  - —Special Use Laws (e.g., RICO/continuing criminal enterprises, forfeiture laws, electronic eavesdropping)
- Information Collection Techniques and Technologies
- Intelligence Support Activities/Associations (e.g., Profiling, National Center for the Analysis of Violent Crime, EPIC, INTERPOL, etc.)
- Computer Information Systems
- Intelligence Resources (e.g., public records, types and means of access)
- Preparation of Criminal Cases
- Methods of Interviewing and Interrogating
- An Overview of Specific Crimes and Their Relationship to Intelligence
  - —Organized Crime
  - —Narcotics Trafficking and Cartel Organization
  - —Serial Crimes
  - —Bias Crime
  - —White Collar Crime
- Intelligence Records Management
- The Need for Information Security and Classification
- Policies and Procedures of the Intelligence Unit
- Field Exposure With Various Operations Units (e.g., investigations, vice, narcotics)
- Geography
- Practice Sessions/Sample Problems

SUPPLEMENTAL SUBJECTS FOR PERSONS ASSIGNED TO STRATEGIC INTELLIGENCE:

- Research Methods (Statistics; Qualitative, Quantitative; & Operations Research)
- Technical Report Writing
- Crime Analysis Methods
- Problem Oriented Policing Model
- Computer Statistical Systems

1) When two applicants have virtually similar *articulated qualifications* and *performance qualifications*, the preferred qualifications can be relied on to select an applicant

2) Preferred qualifications must also be job related

d. **Desired characteristics** - factors manifest in an individual's personality, experience, education, values, interests, and other factors which are determined through the interview process, personality exams, background investigation, or other source

1) These are not typically listed in job announcements or even job descriptions

2) They are characteristics which tend to indicate that a person would be a competent, productive employee and would "fit well" into the organizational environment

4. **What characteristics are desired in a good analyst?**

a. ***General factors*** [modified from Frost (1984)]

1) Impeccable standards of honesty and integrity

2) A thorough understanding of the concepts of ...

a) Intelligence

b) Civil liberties

c) Criminal law enforcement

3) The capacity to think in a logical and rational manner

4) Capacity of approaching situations from broad and divergent perspectives

5) The ability to comprehend complex masses of data and communicating its contents to others

b. ***Background Factors***

1) Broad range of interests

2) Developed research ability (library, qualitative, quantitative)

3) Helpful previous experience (law enforcement, military, security, etc.)

c. ***Mental traits***

1) Intellectual curiosity

2) Rapid assimilation of information

3) Keen recall of information

4) Tenacity

5) Willingness and capacity to make judgements

d. ***Communication skills***

1) Developed writing ability

2) Skill in oral briefing

3) Interviewing and interrogating skills

4) Eliciting information from officers

e. ***"Liberal arts" skills***

1) Good writing ability

2) Fluency in a second language desirable

3) Good knowledge of geography

f. ***Work style***

1) Initiative and self-direction

2) Effective personal interaction

3) Disciplined intellectual courage

F. **Training** for intelligence analysts

1. Overall, training—both pre-service and in-service—for intelligence analysts has been limited, particularly in comparison to other aspects of law enforcement

2. The training which has occurred has typically been characterized by a twofold approach:

   a. Technique-oriented classroom training almost exclusively focusing on the intelligence cycle—analytic activities—with a specific focus on develop various matrix analytic techniques; usually very good training on this aspect, but limited in scope

   b. On the job training through a largely unstructured approach of observation and practice, sometimes under the tutelage of an experienced analyst

3. Agencies conducting their own training programs typically supplement the above two approaches with agency policies and procedures related to intelligence and investigations

4. It is argued that this approach to training is insufficient and fails to address the array of subjects needed for comprehensive training for analysts

5. A suggested training program for intelligence analysts is presented in the following model:

   a. **Component 1: Classroom Training** - a comprehensive presentation of subjects designed to:

      1) Familiarize the student with the meaning and role of law enforcement intelligence (LAWINT)

      2) Identify issues and resources associated with LAWINT

      3) Training individuals on specific techniques, procedures, and law needed to effectively fulfill the LAWINT function

      4) Providing supervised experience with practice cases

NOTE: Figure IV-9 proposes a list of training subjects for the pre-service LAWINT training program

b. **Component 2: Field Training** - working in the intelligence unit to apply the techniques presented in the classroom training

1) The new analyst should be assigned to be under the supervision of an experienced analyst who helps train, observe, and evaluate the new employee

2) This should be a formal field training role designed to sharpen the skills of the new employee while under the direction of a skilled employee

c. **Component 3: Reinforcement Training** - following a defined time period in field training (probably about six months) the analyst returns to classroom training for forty hours to have techniques refined, critical subjects reinforced, and questions answered

6. While this "pure" model may not be the most appropriate for all agencies, its intent is to give direction for a more structured and comprehensive approach to intelligence analyst training

7. Analysts should also receive periodic in-service training programs for updates on:

a. The law

b. New or emerging crime trends

c. Recently developed resources for the analyst

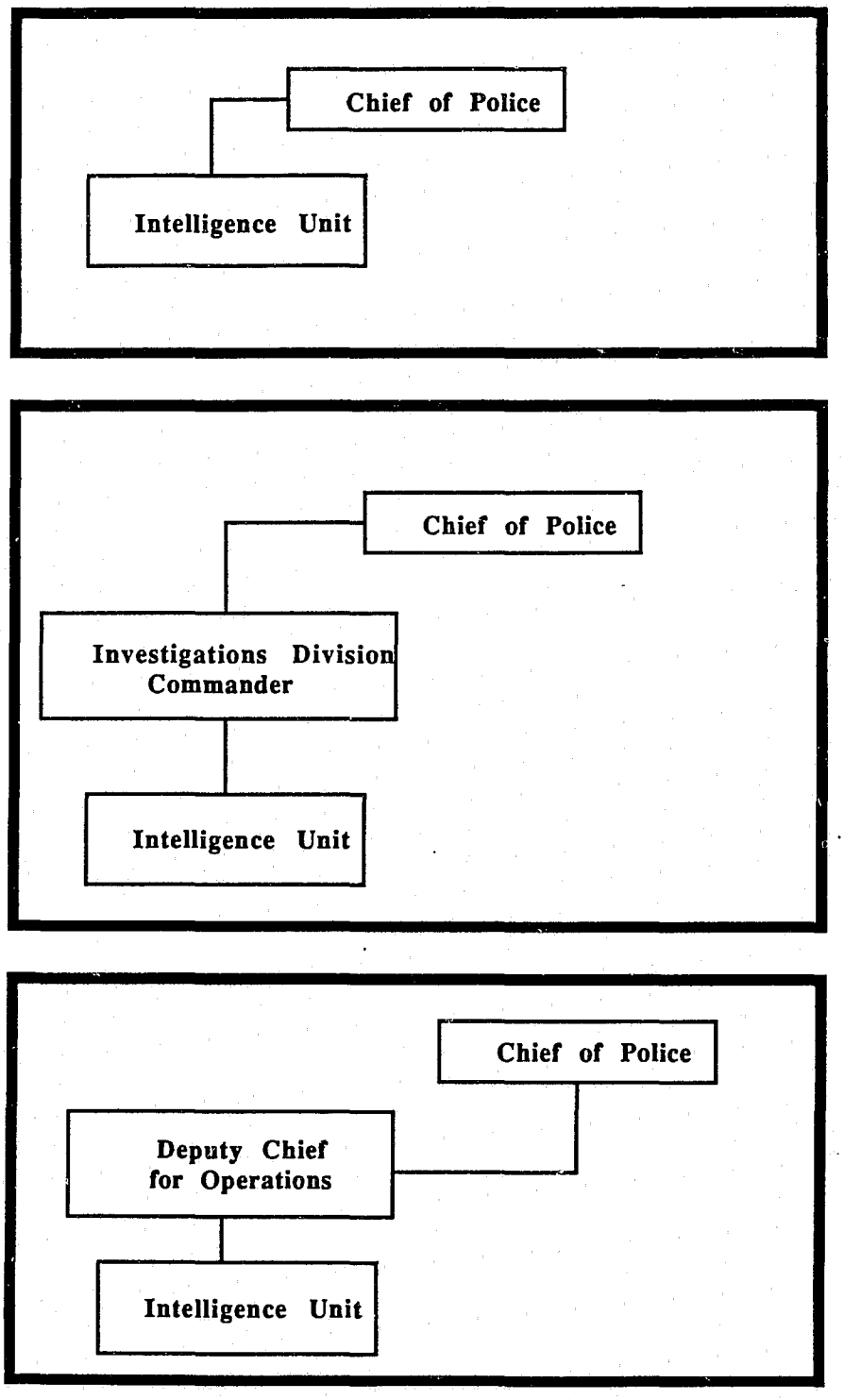
d. New organizational directives affecting the intelligence function

e. Other relevant subject unique to the jurisdiction or LAWINT analysis which has evolved since the last training period

G. The value of the INTELUNIT will be directly related to the effectiveness of staffing efforts

Figure IV-9

OPTIONS FOR ORGANIZATIONAL PLACEMENT OF THE INTELLIGENCE UNIT



4. CONCLUDING OBSERVATIONS

Too often when discussing LAWINT we focus on the technical aspects of analysis and fail to adequately deal with issues of organization and administration. Regardless of the technical expertise of the unit, the productivity of the intelligence process can be increased if care is taken to address the administrative issues discussed in this chapter.

4. ORGANIZATION AND ADMINISTRATION OF THE INTELLIGENCE FUNCTION

Instructional Support and Criteria

GOAL:

> To identify issues and realistic alternatives for organizing, staffing, and managing the intelligence function in a law enforcement agency.

OBJECTIVES:

1. Students will be able to develop the mission and goals of a LAWINT unit.
2. Students will have a perspective to define organizational authority and responsibility for the management of the LAWINT function.
3. Students will have the foundation for organizing a LAWINT unit within an agency.
4. Students will be able to define personnel management issues for the LAWINT unit.

STUDY QUESTIONS:

a. What is the purpose for defining a mission and goal specifically for the intelligence unit?

b. In your opinion, would an intelligence unit be better staffed by civilian or sworn analysts? Justify your position.

c. Your are assigned to explore the creation of an intelligence unit in a municipal police department of 300 sworn officers. What are the initial management tasks you would address? Justify your response.

d. Discuss some of the problems of **coordination** the manager of an intelligence unit would face and have to resolve.

NOTES

CHAPTER 5

THE INTELLIGENCE CYCLE: THE HEART OF ANALYTIC ACTIVITIES

"Intelligence isn't just information—it's a way of thinking; it's a logical thought process which permits you to take all kinds of diverse information and put it into a coherent, integrated form that produces evidentiary information. Sounds easy, doesn't it?"
Statement of DEA Intelligence Chief to Author.

1. THE CONCEPT OF ANALYSIS

As noted in previous chapters, the fundamental ingredient in Law Enforcement Intelligence is the *analysis* of information. Hence the job description, as noted in Chapter 4, seeks to define the skills for an intelligence *analyst.*

There is no easy method or computer system which will permit information to be input and quickly generate an analytic report. There are systems and processes which can be used to expedite the process and make it easier, yet the actual analysis of information is one which requires a "human touch".

It must be recognized that intelligence analysis is a cumulative process—it requires **skills, experience,** and **knowledge** which the analyst develops over a period of time working on cases. Thus, it is impossible for a person to go through any given course or read any given document and become an analyst. The courses and books supply the individual with the *tools*—the *skills* to be an effective analyst evolve with the reasoned application of those tools.

A. The Intelligence Cycle ...

1. *Defined*:

> The intelligence cycle is an organized process by which information is *gathered*, *assessed*, and *distributed* in order to fulfill the goals of the

intelligence function—it is a method of performing analytic activities and placing the analysis in a useable form.

2. The cycle has six integral steps or process which facilitate the assessment and application of intelligence information—these are:

   - Collection
   - Evaluation
   - Collation
   - Analysis
   - Reporting
   - Dissemination

   NOTE: (*See* Figure V-1.)

3. The Intelligence Cycle is viewed as the *heart* of the intelligence function because it provides a framework to perform all activities related to LAWINT

   a. There are different configurations of the intelligence cycle discussed in various documents

   b. The description in this chapter is meant to provide a "holistic" perspective on law enforcement intelligence analysis

2. ELEMENTS OF THE INTELLIGENCE CYCLE

The following section presents the essential elements of the intelligence cycle with commentary on various special issues, concerns, and resources.

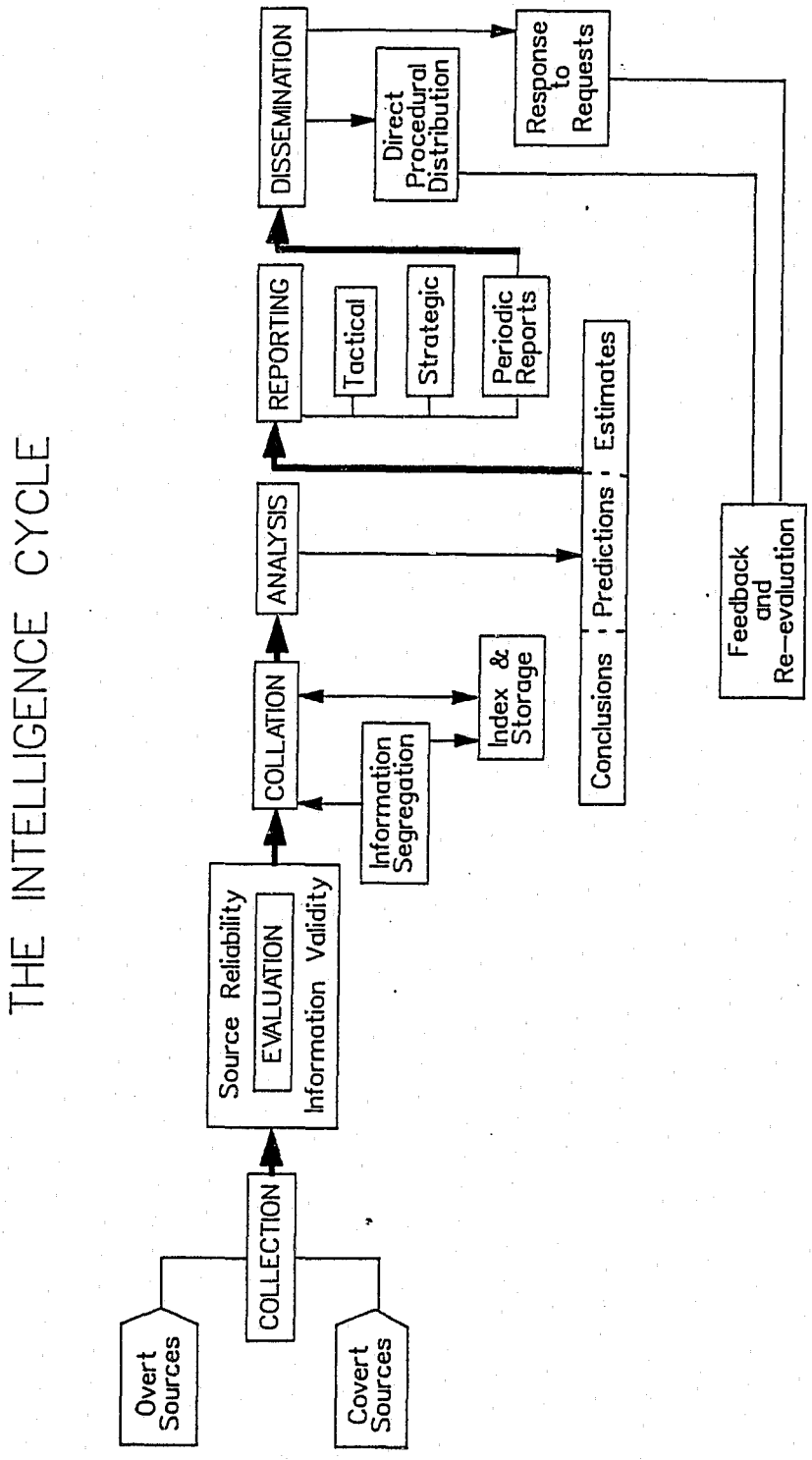
A. **COLLECTION** of Information

1. *Defined*:

The identification, location, and recording of unanalyzed information, typically from an original source and using both human and technological means, for input into the intelligence cycle to determine its usefulness in meeting a defined tactical or strategic intelligence goal.

Figure V-1

ILLUSTRATION OF THE INTELLIGENCE CYCLE



2. Collection is accomplished in five ways ...

   a. *Routinized Input* - The intelligence unit has arranged for certain types of information to be regularly submitted for review

   b. *Selected Access* - The intelligence unit has access to information sources which can be used as needs demand

   c. *Special Access* - The intelligence unit utilizes a means to especially collect information on a targeted person, group, organization or issue

   d. *Casework Availability* - The intelligence unit has access to information simply as a product of a specific case which is being worked. Sometimes the information may be a product of the analyst's initiative or it may be the product of simple circumstances

   e. *Unsolicited Input* - The intelligence unit receives information which is initiated by a source other than the unit itself or it is information which is serendipitiously discovered outside the established information collection chain.

3. The unit must recognize the diversity of these sources and

   a. Established procedures to utilize the sources most *efficiently* and *effectively*

      1) Efficient—*Defined*:

      > Doing the *job right*. It is concerned with the judicious use of resources and effort to accomplish the intended tasks without expending undue time, money, or effort.

      2) Effective—*Defined*:

      > Doing the *right job*. It is performing the tasks and expending the effort to accomplish the specifically defined goal of the task(s) at hand.

b. Account for the type of information received from each source for further detail or verification

c. Establish procedures for thoroughly reviewing each information source for needed information or information of potential value

d. Analysts and other unit personnel should be trained in the means to utilize each information source

e. Account for the value of each source for evaluation purposes

4. The specific types of information the unit will collect and the sources which will be used depend on several criteria:

   a. **What is the intelligence case responsibility?** (e.g., general intelligence or specific case intelligence)

   b. **What is the authority or jurisdiction of the intelligence unit's parent agency?**

      1) Access to information will vary somewhat with the agency

      2) Access to certain computer systems

      3) Access to classified information

      4) Existence of the "Third Agency Rule" (i.e., An agreement wherein a source agency releases information under the condition that the receiving agency *does not* release the information to any other agency—that is, a "third agency")

   c. **What is the nature of the crime being investigated?**

      1) Certain information may be restricted unless related to a specific crime

      2) **EXAMPLES:**

         a) Use of NADDIS to narcotics trafficking (See Chapter 11)

         b) Access INTERPOL only if quality control criteria are met (See Chapter 10)

c) Access to information which may be restricted by privacy act (See Chapter 14)

d) Information that has both criminal case and national security implications

d. **What are the applications for which the information is being gathered?** (e.g., tactical, operational, strategic)

e. **What are the resources of the agency?**

1) A realistic consideration is how much the agency can spend and how much staff time can be allocated to the intelligence function

2) **EXAMPLE:** If an agency could not afford high technology surveillance equipment it would have to find alternate sources to gain information

5. Information collection may be *overt* or *covert*

a. **Overt Methods** - The analyst or investigator directly accesses information with the expressed or implied purpose of obtaining the information for use in a criminal investigation. Sources include:

1) *Internal Sources* - those sources an analyst has access to within the law enforcement system (e.g., criminal histories, police reports, suspect interviews, INTERPOL, etc)

2) *External Sources* - those sources an analyst accesses outside of the law enforcement system (e.g., tax rolls, phone records, newspapers, etc.)

NOTE: One must be aware of the restrictions, if any, that apply to each type of information; for example:

- Privacy act
- Limitations of court orders used in information access
- Interviews given with the guarantee of confidentiality

- Limitations on with whom the information may be shared (e.g., classified information)

- Third Agency Rule

b. **Covert Methods** - Direct collection of information from an individual, organization, or intelligence target through some form of active or passive observation wherein the subject is unaware that the information is being collected for an intelligence investigation. Techniques include:

1) *Active observation* - covert technique interacts with the target; the target's actions are frequently a reaction to the stimulus or opportunity provided by the investigating body

EXAMPLES:

a) Undercover investigator

b) Surreptitious inquiry to target (e.g., fake questionnaire or invitation)

c) Storefront or sting operation

d) Informants

2) *Passive observation* - covert technique is non-reactive in that there is no interaction with the target by investigator/intelligence officer

EXAMPLES:

a) Physical surveillance

(1) Moving

(2) Fixed

b) Electronic surveillance

(1) Phone/wire tap

(2) Radio intercept

(3) Electronic eavesdropping

(4) Remote sensing

NOTE: Collection of information will be discussed in greater detail in Chapter 6.

6. There is an extremely wide range of information sources available to the investigator and analyst

   a. Types of information sources sought will depend on:

      1) *Nature* of the investigation

      2) *Accessibility* to information in light of the agency's:

         a) Jurisdiction/authority

         b) Supporting evidence (in cases where a court order is needed)

      3) *Unique statutory alternatives* (e.g., continuing criminal enterprise, forfeiture statutes, habitual criminal act, etc.)

   b. Frequently information collection will require a blend of overt and covert activities

      1) The divisions between the activities are made to understand the differing mandates

      2) The information will eventually have to be integrated together

7. One very important information source of information is **records.** *Reasons*:

   a. They are usually comprehensive

   b. They are reliable and verifiable

   c. They clearly identify persons, actions, events, and/or transactions

d. They frequently provide direction for new avenues of investigation

8. Records may be categorized as:

a. ***Criminal justice system records***

EXAMPLES (not comprehensive):

1) Criminal histories
2) Police reports (arrest, crimes, accidents, etc.)
3) Field interrogation cards
4) Court records
5) Probation and parole reports
6) Corrections classification reports
7) Intelligence systems (e.g., EPIC, INTERPOL, PATHFINDER, etc.)

b. ***Non-criminal justice government records***

EXAMPLES (not comprehensive):

1) Business licenses
2) Deeds
3) Tax rolls
4) Drivers' licenses
5) Vehicle licenses
6) Corporate charters

c. ***Private records***

EXAMPLES (not comprehensive):

1) Phone records
2) Medical records
3) School records
4) Bank records
5) Credit bureau
6) Business transaction records

9. Access to the records by the intelligence analyst or investigator may be:

a. **Access by Permission** - The custodian of the records, whether governmental or private, knowingly gives permission to review the records.

b. **Access by Status as a Public Record** - As a matter of custom, statute, or court decision the record is open to for review by any member of the public including law enforcement officials.

1) Some agencies may charge a fee for:

a) Reproducing the record

b) Searching for the record

2) Some records may have to be accessed through a "Freedom of Information Act" request—the record may be *sanitized*; which means certainly critical information, based upon the interpretation of the records' custodian, may not be released or may be excluded from the document.

c. **Access by Legal Process** - Investigators request the court to order access to records, public or private, when either the records are not public or permission cannot be obtained.

1) *Subpoena duces tecum* - a court order mandating the records' custodian to bring forth the records described in the subpoena

2) Enforcement order of the court to force a records' custodian compliance with an open records statute or FOIA request (See Chapter 14)

10. Remember, this discussion on "collection" represents only the first step in the Intelligence Cycle

a. Obviously a very important step

b. Without collection, the process ends

B. **EVALUATION** of the collected information

1. *Defined*:

> All information collected for the intelligence cycle is reviewed for its *quality* with an assessment of the validity and reliability of the information.

a. **Reliability** - Is the *source* of the information consistent and dependable?

b. **Validity** - Does the information *actually represent* what we believe it represents?

2. Assignment of reliability and validity factors to information helps provide insight to the value of the information in hand

a. *See* Figure V-2 for the scales on "Data Validity" and Figure V-3 for the scales of "Source Reliability" to illustrate how information may be evaluated

1) The rating systems permit the information to be rated on an *ordinal scale*

2) They permit the assessment of value to information—although the value is not absolute

3) The scales help to evaluate future information and the quality of the information collectively through review of the evaluative measures

b. Thus, when evaluating information, one must focus on:

1) The *source* of the information

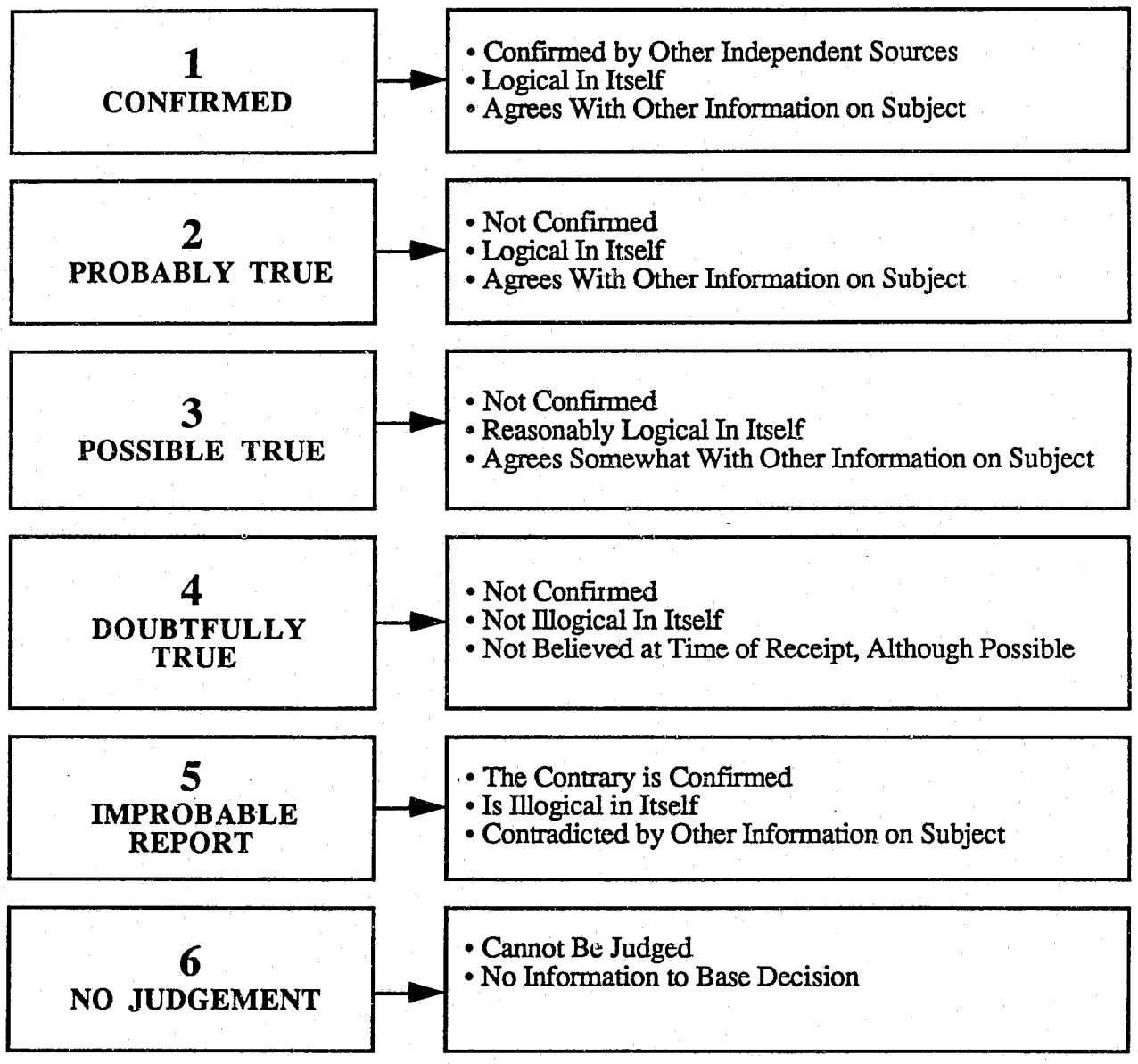
2) The mechanism on *how* the information was received (e.g., directly received, hearsay, etc.)

3) If the information was received in a manner consistent with *constitutional and statutory law*

4) Amount of *corroborative* information

Figure V-2

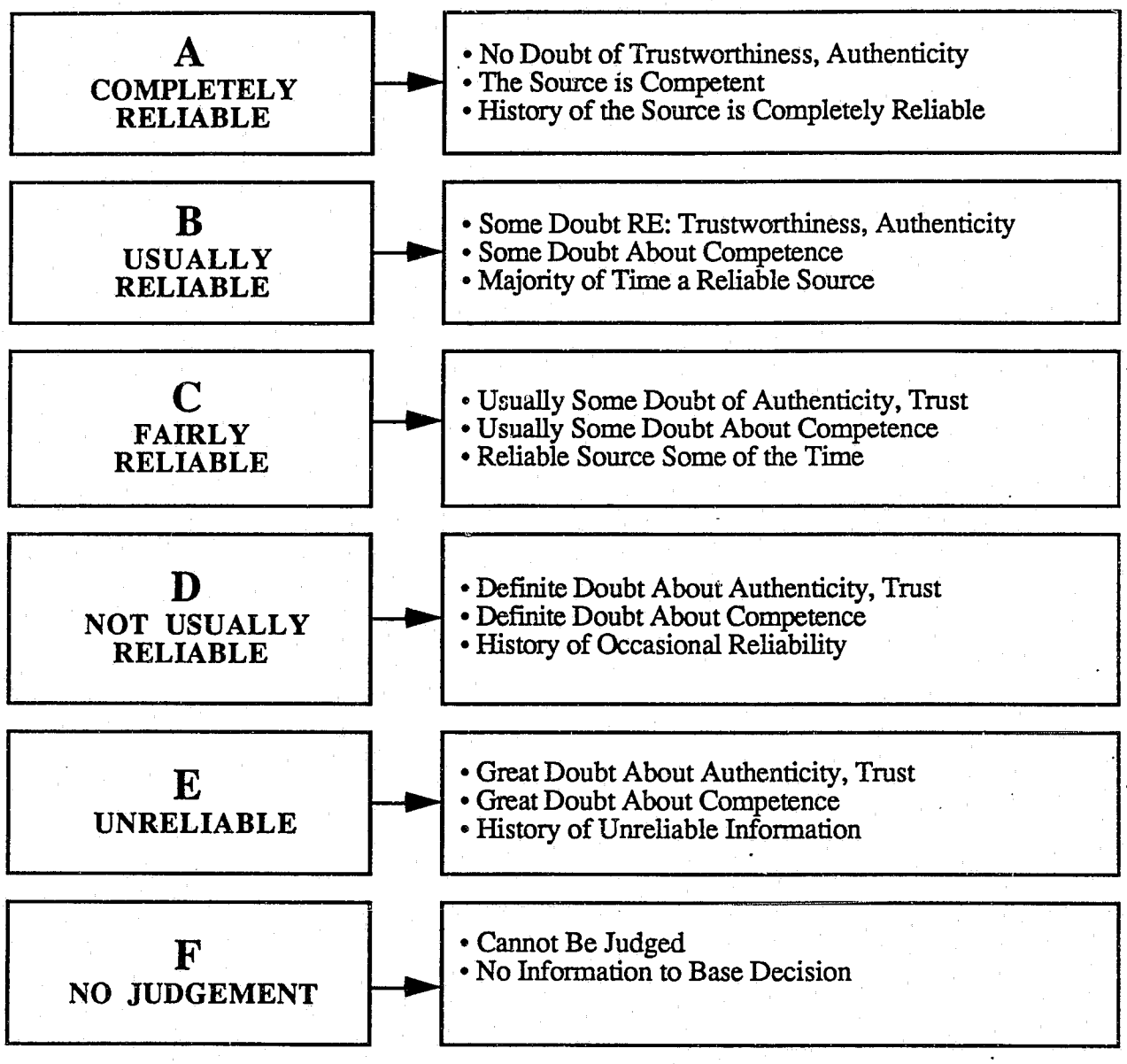
SCALE OF VALIDITY†



†Adapted from the U.S. Customs Service *Intelligence Training Manual*

Figure V-3

SCALE OF RELIABILITY†



†Adapted from the U.S. Customs Service *Intelligence Training Manual*

5) Amount of *contradictory* evidence

6) How *current* the information is

7) The *relevancy* and *materiality* of the information to the case at issue

3. Once we know the value or quality of the information we can begin the pre-analytical process of collation

C. **COLLATION** of the information

1. Whereas ...

a. Evaluation examines *individual* pieces or sources of information as it enters the intelligence cycle,

b. Collation brings all the collected and evaluated information together to examine it in the *aggregate*

2. *Defined*:

> A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system which permits easy and rapid access and retrieval.

3. The purpose of collation is to examine all of the information together and...

a. **First Step**: *Remove* information which is:

1) Irrelevant

2) Incorrect

3) Useless to the investigation

b. **Second Step**: *Create* an orderly arrangement of the collected materials to make comparisons of facts and events easier (indexing)

c. Placing the information in a form for:

1) Systematic storage, and

2) Rapid retrieval

4. A key task of collation is indexing information—this is essential for efficient and effective analysis

5. Indexing may be manual or automated (computerized) based on the:

a. Amount of information involved in the case

b. Complexity of the case

c. Resources of the agency

6. Indexing requires that the analyst:

a. Identify critical information, such as:

1) Names of ...

- Suspects
- Victims
- Witnesses
- Associates

2) Addresses relevant to persons and the crime(s) at issue

3) Descriptions of vehicles

4) Descriptions of property

b. Identify critical labels and words for the information which are:

1) Logical

2) Descriptive

3) Substantively relevant

c. Place the labels and words into cross-referenced retrieval system for research, comparison and analysis

d. The system must be of a nature that anyone with authority to access the information can do so without unnecessary complexity

1) "Individualized" systems are inefficient and ineffective

2) Such systems "lock in" the information to the exclusive effective use of the individual creating the system

7. Indexing systems may be:

a. *Alphabetical* - words and labels are simply placed in the storage and retrieval system in alphabetical order (manual or automated)

1) One must know the "rules" for alphabetizing within the system (e.g., last name, dropping the article, dealing with adjectives, dealing with numbers, etc.)

2) Has limitations when dealing with long, descriptive labels

3) Cross-referencing may become laborious

4) Works best with clearly defined categories such as names, vehicles, locations, etc.

b. *Hierarchical* - words and labels are arranged in a hierarchy beginning with the most general topic and going to more specific topics (manual or automated)

1) Each step in the hierarchy is assigned an access number for ease of reference and access

2) Process requires deductive reasoning

3) An access problem is that not everyone thinks alike therefore the hierarchical orders may not be as efficient to access

4) Works best on "common criteria" or discrete variables such as seriousness of crimes, values of property, sizes of drug shipments

c. *Key Word In Context (KWIC)* - This is an automated system which indexes selected key words which represent the evidence or information being stored

1) Can have multiple descriptors for an evidentiary item or lead

2) KWIC develops alphabetical lists of all principal words in a book or document (i.e., concordances) with reference to the passages where they occur (Levine, 1979)

3) KWIC systems can sort and correlate large amounts of information on a wide array of specified variables

4) Very effective system and efficient use of staff time

5) Typically requires at least a micro-computer system with a hard drive

6) "Sort" programs for micro-computers, mini-computers, and mainframes can also work, but are less effective and efficient

8. Index systems in the collation process may be:

a. Designed to serve the entire intelligence unit

b. Be specific systems for an individual case which is complex or involves a long term investigation with many variables

NOTE: Variables can include persons, addresses, vehicles, or any factor used in the case development process.

9. Most intelligence units will have:

a. A combination of indexing systems

b. Permanent intelligence files used as a monitor and reference source

EXAMPLES:

1) Field interview (FI) cards may be kept on file to monitor certain persons

2) Information is used by analyst for reference

3) Importantly, this is not the same as a dossier

4) An FI form is typically filed by a patrol officer or investigator

   a) On a "suspicious" person

   b) Person flagged by the computer

5) An FI form will typically contain only:

   a) Physical descriptive information

   b) Vehicle information

   c) Clothing description

   d) Information on companions, if any, during the field interview

   e) Comments about the circumstances of the stop and other relevant information

   NOTE: *See* the example Field Interview Form from the Kansas City (MO) Police Department (Figure V-4) and the Missouri Uniform Intelligence Report (Figure V-5).

10. Collation—like collection and evaluation—is not a one-time process

    a. It is an on-going process that is done *each time* information comes into the intelligence cycle

    b. As information is increasingly collated into the intelligence system, the ability of the analyst to make accurate projections, hypotheses, and conclusions increases

Figure V-4

FIELD INTERVIEW FORM
KANSAS CITY, MISSOURI POLICE DEPARTMENT

FIELD INTERVIEW FORM
Kansas City Missouri Police Department

APPROVED BY: | ENTRY IN COMPUTER ( ) YES ( ) NO | DATE: | TIME: | BEAT: | LOCATION: | INSIDE | CASE REPORT NO.

NAME: (LAST) (FIRST) (MIDDLE) (JR./SR.) | RACE: ( ) WHITE ( ) INDIAN ( ) OTHER ( ) NEGRO ( ) ORIENTAL | SEX: ( ) MALE ( ) FEMALE | BIRTH DATE:

10-32 J9 | HEIGHT: | WEIGHT: | HAIR: ( ) 1. BLONDE ( ) 2. RED ( ) 3. BROWN ( ) 4. BLACK ( ) 5. GREY ( ) 6. NO HAIR | EYES: ( )1. BROWN ( ) 2. GREY ( )3. BLUE ( )4. HAZEL ( ) 5. GREEN ( )6. MAROON | ALIAS OR MONIKER

SOCIAL SECURITY NO. | DRIVER'S LICENSE NO.: | DRIVER'S LICENSE STATE: | COMPANIONS: ( ) YES ( ) NO

STREET NO.: | APT. NO.: | CITY: | STATE: | ZIP: | NO. IN GROUP:

LICENSE NO.: | LICENSE STATE: | LICENSE YEAR: | VEHICLE YEAR: | VEHICLE MAKE: | VEH. MODEL | VEH. STYLE | VEH. COLOR: (TOP) / (BOTTOM)

COMPLEXION: ( ) 1. FAIR ( ) 2. MEDIUM ( ) 3. DARK ( ) 4. LT. BROWN ( ) 5. DK. BROWN ( ) 6. RUDDY ( ) 7. FRECKLED | TATOOS: ( ) 1. ARM ( ) 2. HAND ( ) 3. FINGERS ( ) 4. CHEST ( ) 5. NECK ( ) 6. LEG

SCARS: ( ) 1. CHEEK ( ) 2. LIP ( ) 3. EAR ( ) 4. FOREHEAD ( ) 5. CHIN ( ) 6. NOSE ( ) 7. ARM / HAND

AMPUTATIONS/DEFORMITIES: ( ) 1. ARM ( ) 2. HAND ( ) 3. FINGER ( ) 4. FOOT ( ) 5. LEG ( ) 6. EAR

GENERAL APPEARANCE: ( ) 1. LONG HAIR ( ) 2. MUSTACHE ( ) 3. BEARD ( ) 4. SIDEBURNS ( ) 5. WELL DRESSED ( ) 6. NEAT ( ) 7. UNIFORMED ( ) 8. DIRTY ( ) 9. SLOPPY ( ) 10. GLASSES

SCHOOL (JUV.) – EMPLOYER (ADULT) | ADDRESS | TELEPHONE | CITY | STATE

J-1 MURDER J-3 ROBBERY J-5 BURGLARY J-7 AUTO THEFT J-9 A. CRIMINAL ASSOC.
J-2 RAPE J-4 ASSAULT J-6 LARCENY J-8 NARCOTICS B. SUSPICIOUS ACT

COMMENTS:

CLOTHING DESCRIPTION

* CIRCLE THE PROPER SQUARE	WHITE	BLACK	GREY	BROWN	BLUE	RED	YELLOW	GREEN	PINK	ORANGE	PURPLE
HAT	00	01	02	03	04	05	06	07	08	09	0+
CAP	10	11	12	13	14	15	16	17	18	19	1+
COAT	20	21	22	23	24	25	26	27	28	29	2+
JACKET	30	31	32	33	34	35	36	37	38	39	3+
SHIRT	40	41	42	43	44	45	46	47	48	49	4+
TROUSERS	50	51	52	53	54	55	56	57	58	59	5+
SWEATERS	60	61	62	63	64	65	66	67	68	69	6+
SHORTS	70	71	72	73	74	75	76	77	78	79	7+
BLOUSE	80	81	82	83	84	85	86	87	88	89	8+
SKIRT	90	91	92	93	94	95	96	97	98	99	9+
DRESS	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	++

* CIRCLE THE SQUARE WHERE THE APPAREL AND THE COLOR OF THE ITEM INTERSECT.

COMPANIONS

NAME: (LAST) (FIRST) (MIDDLE) (JR./SR.) | RACE: ( )NEGRO ( )WHITE ( )OTHER | SEX: ( ) MALE ( ) FEMALE | BIRTH DATE: | SOCIAL SECRUITY NO.:
ADDRESS: | DRIVER'S LICENSE NO.:

NAME (LAST) (FIRST) (MIDDLE) (JR./SR.) | RACE: ( ) NEGRO ( ) WHITE ( ) OTHER | SEX: ( ) MALE (.) FEMALE | BIRTH DATE: | SOCIAL SECURITY NO.:
ADDRESS: | DRIVER'S LICENSE NO.

NAME (LAST) (FIRST) (MIDDLE) (JR./SR.) | RACE: ( ) NEGRO ( ) WHITE ( ) OTHER | SEX: ( ) MALE (.) FEMALE | BIRTHDATE: | SOCIAL SECURITY NO.:
ADDRESS | DRIVER'S LICENSE NO.:

( ) ON VIEW | OFFICER'S SIGNATURE: | OFFICER'S SERIAL NO.: | BEAT:

FORM 408 P.D. (REV. 2-73)

Figure V-5

MISSOURI UNIFORM INTELLIGENCE REPORT

Send Original and One Copy To:
MISSOURI ASSOCIATION OF DRUG ENFORCEMENT
Box #62, Jefferson City, Missouri 65101

UNIFORM INTELLIGENCE REPORT

(Please Type or Print)

NAME (LAST) (FIRST) (MIDDLE) 1.	RACE 2.	SEX 3.	FILE (LEAVE BLANK) 4.
ALIAS 5.	SOCIAL SECURITY # 6.	ADDRESS 7.	
HEIGHT 8. / WEIGHT 9.	EYES 10.	HAIR 11.	DATE OF BIRTH 12. / PLACE OF BIRTH 13.
MARKS OR SCARS 14.	M.O. SPECIALTY 15.	16. PHOTO	
FATHER 17.	MOTHER		
WIFE OR GIRL FRIEND 18.			
CHILDREN 19.			
RELATIVES 20.			
PLACES FREQUENTED & HABITS 21.			
ASSOCIATES 22.			

MADE NO. 23.	BNDD NO. 24.	CODE	RS NO. 26.
MSHP NO. 27.	FBI NO. 28.	OTHER NO. 29.	CHECK ONE BELOW: OWN / MANAGE / WORK
BUSINESS - OCCUPATION - LOCATION 30.			

CLASSIFICATION

31. ☐ RESTRICTED ☐ COMPLETELY RELIABLE ☐ RELIABLE - HEARSAY
☐ NOT RESTRICTED ☐ RELIABLE SURVEILLANCE ☐ NOT EVALUATED

DATE SUBMITTED AGENCY OR DEPT. 32. INFORMATION

MADE FORM - 1

(continued on reverse - remove carbon)

D. **ANALYSIS** of the information

1. *Defined*:

> Analysis is that activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information (*See* Harris, 1976).

2. This is the step where the analyst takes the information in the intelligence system and attempts to:

   a. Make hypotheses

   b. Establish case links

   c. Draw conclusions

   d. Identify other relevant avenues to search for information

3. There are *five elements* in the analysis process:

   a. **Data Integration and Description**

      1) Indexed information is accessed and organized in order to:

         a) Facilitate understanding

         b) Emphasize investigation requirements

         c) Identify new leads

      2) An important technique for data integration is the use of **link diagrams** (also called link analysis, link networks, wire diagrams or analysis matrices)

      3) Link diagrams permit:

         a) A *systematic approach* to data comparisons, and

         b) A *visual assessment* of the relationship between information elements

4) Link diagrams and association matrices, illustrated in Appendix 1, show the relationship between multiple variables of evidence collected during the course of an investigation—such as:

   a) Relations (business or social) between persons

   b) Linking people to organizations

   c) People to vehicles

   d) Phone numbers called between persons

   e) Flow of illicit commodities

   f) Relation of people to known behaviors

5) The matrices and diagrams should be viewed as important tools for correlating intelligence information

   a) The analyst must remember that the techniques are only tools—there is a tendency to become focused on the *process* rather than the *outcome*

   b) As such, focusing on "models" or "rules" for developing association matrices and diagrams should not overshadow the *intent* of the process

b. Logical Reasoning

1. The use of inductive logic to develop inferences about:

   a. Criminal operations

   b. Key individuals involved

   c. Methods of operation

   d. The extent of the criminal activity or influence

2. The analyst must use his/her reasoning abilities to infer a cohesive meaning from specific items of information collected

c. **Hypothesis(es) Development**

1. Development of a tentative explanation or theory

2. Focuses further information collection activities to either confirm or deny the hypothesis(es)

3. Analyst may develop multiple hypotheses (or scenarios) for an investigation to:

   a. Focus investigation in different areas

   b. Explain different elements in a complex case

d. **Hypothesis Testing**

1. The application of further collected data to either:

   a. Confirm or reject a hypothesis, or

   b. Select among alternate hypotheses

2. This process should require robust levels of information and evidence to:

   a. Support case development in court (in the case of tactical intelligence), or

   b. Be sufficiently sound to make management decisions for resource allocation and planning (in the case of strategic intelligence)

e. **Conclusion, Prediction, or Estimate**

1. *Conclusion* - a definitive statement about a suspect, action, or state of nature

2. *Prediction* - Projection of future criminal actions or changes in the nature of crime trends based on analysis of intelligence information

3. *Estimate* - Strategic projections on the economic, human, and/or quantitative criminal impact of the crime or issue subject to analysis.

4. The analysis process is a complex exercise requiring a significant amount of creativity and application of technique

   a. While it has been presented in a prescriptive manner, do not be misled

   b. It is a process that can be frustrating and difficult to apply when "some of the pieces are missing" in the evidentiary trail

   c. When this occurs, the analyst must go back to the beginning of the intelligence cycle and collect further information to be processed

   d. Such information would be "targeted" to fill the information voids

E. **REPORTING** the results of the analysis

1. *Defined*:

The process of taking the analyzed information and placing it in the proper form for the most effective consumption of that information as dependent on the type of intelligence.

2. The types of reports most frequently used are:

   a. *Oral Tactical Response* - characteristics:

      1. A verbal report

      2. Non-specific format

      3. Directly responds to a specific inquiry from investigators or other entity with access to the intelligence unit

b. *Written Tactical Response* - characteristics:

1. Brevity

2. A focus on a specific enforcement problem

3. Typically prepared in response to a request for an assessment or estimate about a particular person, criminal entity, or crime problem

c. *Comprehensive Case Report* - characteristics:

1. Detailed tactical report

2. Sets forth evidence and hypotheses in case

3. Used in complex, long term, cases (e.g., continuing criminal enterprises, serial crimes, etc.)

4. Nature of report may be:

a) Status report

b) Summarize information to see where to go next

c) Prepared to assist in gaining arrest and/or search warrants

d) Used as an aid in case preparation for court

d. *Strategic Reports* - characteristics:

1. Detailed report

2. Addresses future criminal activity and crime problems

3. Poses hypotheses

4. Detailed discussion of analytic procedure to provide perspective for validity and reliability

5. Identifies points where more information is needed

e. *Periodic Reports* - characteristics:

1. Produced on defined schedule (e.g., weekly, monthly)

2. Addresses wide range of crimes and intelligence concerns (including all classifications of intelligence)

3. Focus is on newly developed information or changes in previously reported trends

F. **DISSEMINATION** of intelligence

1. *Defined*:

> This is the process of effectively distributing analyzed intelligence information in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

2. Dissemination will depend on:

a. *The nature of the information*

EXAMPLES:

1) Degree of conclusiveness, validity and reliability

2) Whether the information is classified

3) Tactical intelligence

4) Strategic intelligence

b. *Nature of the crime(s) involved*

c. *Relevant internal needs* (e.g., investigators, administrators, planners)

d. *Relevant external needs*

EXAMPLES:

1) Case in multiple jurisdictions

2) Suspect(s) reside in other jurisdictions

3) Intelligence information indicates possible crime to be committed in another jurisdiction

4) Another jurisdiction is working on a case and wants to compare notes to see if possibly the same perpetrator(s)

3. Dissemination must be controlled by procedure to ensure:

a. Critical information is not released in a manner that might jeopardize the investigation

b. That analysts can account for information shared with other jurisdictions for later reciprocity

c. Certain types of information—particularly some hypothetical or low reliability information—may not be released

d. Insure standards of constitutional rights and privacy remain intact

4. *Official* information release may be in the forms of:

a. Formal verbal information release

b. Written report summary

c. Copies of periodic reports

d. Copies of case documents and intelligence files

5. The recommended procedure is that intelligence information only be released on authority of the intelligence unit chief or section supervisor

6. Without appropriate internal and external intelligence dissemination, the value of the process is limited

3. EXAMPLES OF CONCLUSIONS, PREDICTIONS, AND ESTIMATES FROM THE ANALYSIS STEP OF THE INTELLIGENCE CYCLE ...

A. **Conclusion** - a definitive statement about a suspect, action, or state of nature

EXAMPLES:

1. "Frank White sells sensitive microcomputer chips to communist bloc countries using legitimate front companies."

2. "The Carta Rojo drug cartel is responsible for the deaths of undercover DEA agents."

3. "The distribution of drugs by high school students coupled with easy accessibility to guns made available by drug suppliers has caused the increase in assaults and deaths of high school students in Detroit."

B. **Prediction** - Projection of future criminal actions or changes in the nature of crime trends based on analysis of intelligence information

EXAMPLES:

1. "A possible change in the shipment of microcomputer chips will be routing through the Port of Houston mixed with overseas oil drilling equipment supplies instead of through the presently used Ports of New York and Los Angeles."

2. "Attempted assassinations of suspected DEA agents in Mexico by the Carta Rojo organization in an attempt to undermine U.S. drug enforcement efforts will widen to include representatives of other U.S. government agencies in Mexico as well as possible attacks on the U.S. Embassy and Consular offices."

3. "The possession of guns by high school students is becoming a status symbol in the Detroit schools thereby increasing both the number of students involved in drug sales and the number of students possessing guns in school."

C. **Estimate** - Strategic projections on the economic, human, and/or quantitative criminal impact of the crime or issue subject to analysis.

EXAMPLES:

1. "Frank White's illegal gross income of microcomputer chips to Communist bloc countries is estimated to be $8.5 to $10 million during the next 12 months."

2. "In light of the projected broadened tactic of the Carta Rojo organization to attack U.S. government officials in Mexico, it is estimated that 235 persons on assignment in Mexico are at risk of attack."

3. "At the current rate of assaults by firearms in the Detroit schools, it is estimated that 12 persons will die and 28 will be injured on school premises as a result of shootings."

4. SUMMARY OBSERVATIONS ON THE INTELLIGENCE CYCLE

A. The intelligence cycle is **tautological**—circular, systemic, on-going through each step from collection through dissemination; this is ...

1. Information is *constantly being **input*** into the cycle

2. Information is *constantly being **processed*** by analysts

3. Information is *constantly being **output*** in various forms of reports and disseminated as necessary

NOTE: Illustrated in Figure V-6

B. The intelligence cycle does not have a defined point of initiation or termination—it should be viewed as *continuous* rather than finite

C. The tactical and strategic conclusions of the intelligence cycle need to be evaluated in light of new information brought into the cycle

1. Essentially, conclusions need to be reviewed
2. Hypotheses need to be reviewed

D. The intelligence cycle *as a procedure* needs to be regularly assessed to make sure it is working:

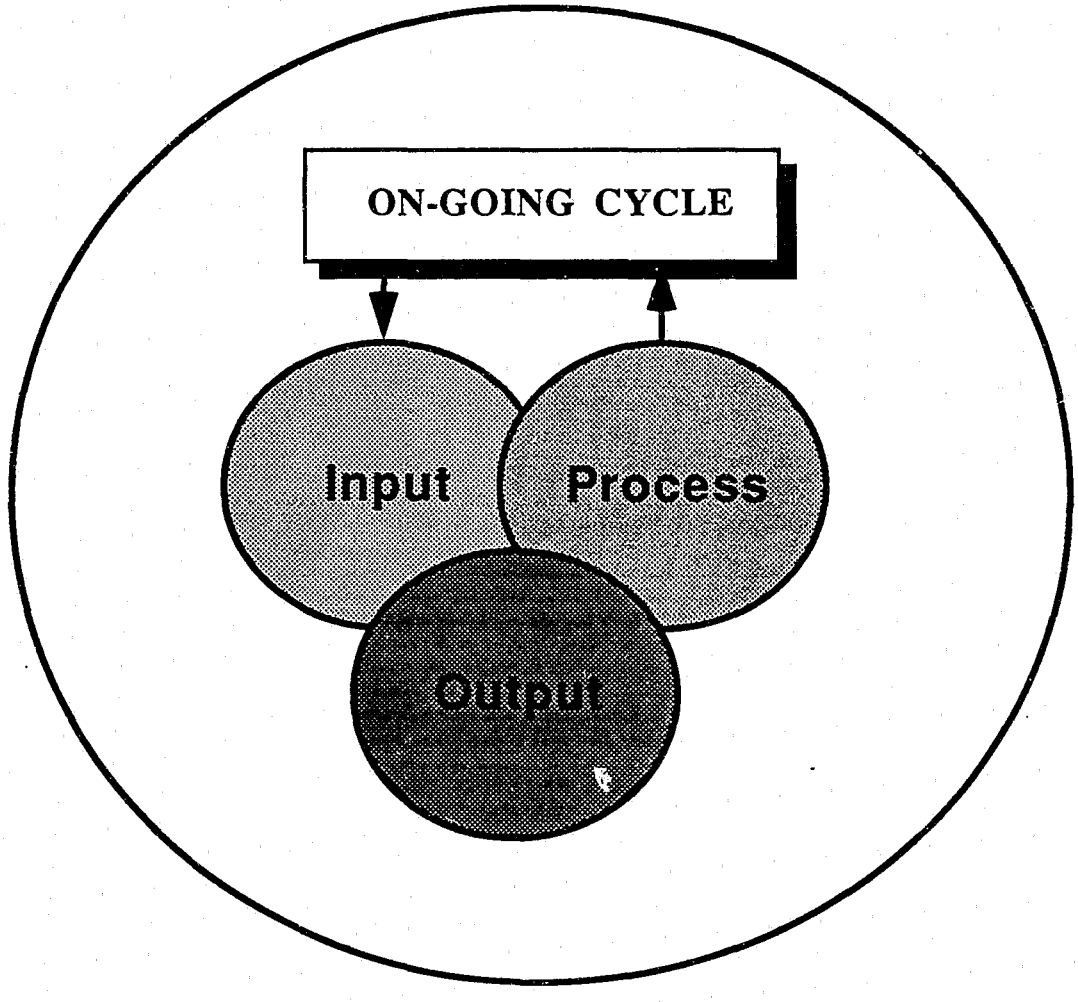
1. Efficiently,

2. Effectively, and

3. Lawfully

Figure V-6

TAUTOLOGY OF THE INTELLIGENCE CYCLE



5. THE INTELLIGENCE CYCLE

Instructional Support and Criteria

GOAL:

To define a framework/methodology which may be used to collect, process, and disseminate intelligence information in a thorough, efficient, and effective manner.

OBJECTIVES:

1. Students will be able to articulate the different processes required to effectively perform the LAWINT function.

2. Students will be able to differentiate between distinct responsibilities in intelligence analysis and define resources to assist in the fulfillment of those responsibilities.

STUDY QUESTIONS:

a. In your own words, describe the **purpose** of the Intelligence Cycle.

b. Why are records considered a valuable source for intelligence analysis? How can records be lawfully obtained?

c. Explain the difference between **validity** and **reliability** in evaluating information.

d. How do **evaluation** and **collation** differ in the intelligence cycle?

e. In your own words, describe the intent and processes associated with the **analysis** of intelligence information.

f. Why is it necessary to have a wide variety of intelligence report formats?

NOTES

CHAPTER 6

COLLECTION OF INFORMATION FOR INTELLIGENCE ANALYSIS

"You have to be innovative when it comes to collecting good intelligence. It's not always pleasant, but sometimes the least pleasant efforts produce the best results. Personally, I find going through the garbage of an intelligence target is usually very rewarding."
Comment of an intelligence officer in a southern state to the author.

1. INTELLIGENCE COLLECTION PROTOCOL

In discussing information collection in the intelligence cycle, some general observations were made concerning techniques and processes in the collection function. Because of the critical, and frequently controversial, nature of collection, this chapter will provide more detail on the *manner* in which information can be collected. Given the perspectives provided in this chapter, the following chapter will address some of the critical issues involved in collection.

A. The protocol of intelligence collection is important to under stand because of concerns for:

1. Civil liberties

2. Alternate means to collect different types of information for different purposes

3. Alternate types of expertise and resources are needed to collect information based upon the protocol employed

B. Protocol of Intelligence Collection—*Defined*:

> Information collection *procedures* employed to obtain verbal and written information, actions of people, and physical evidence required for strategic and tactical intelligence analysis.

1. As a result of the varying degrees of information availability and the evolution of intelligence gathering technology, the protocol options are quite extensive.

2. Predominantly, these protocols are used for tactical intelligence, although residual information may also be used for strategic intelligence.

C. To understand these options, the protocol can be divided into two interactive components.

1. **Component 1—Operations Methodology**

a. This, essentially, refers to the *degree of confidentiality* associated with the information collection.

b. Different levels of confidentiality are required...

1) To solicit information which is difficult to obtain,

2) To protect the identity of the officers/agents, and

3) In some cases, protect the agency sponsoring the collection.

2. **Component 2—Operations Media**

a. Specifically, this is the *means by which the information is collected.*

b. Different media are required depending on the:

1) Configuration or type of information being sought, and

2) The source of information being sought.

c. Some of the methods described are most applicable to law enforcement intelligence (LAWINT) while others are predominantly employed in national security intelligence (NASINT)

D. The collection protocols described in this chapter include NASINT options to illustrate the wide array of techniques available.

E. The selection of a protocol in a LAWINT collection operation will depend on a wide range of legal and administrative factors.

F. A comprehensive delineation of collection protocols is presented to give the reader a perspective on the approaches:

1. Most applicable to LAWINT,

2. Those most applicable to NASINT, and

3. Those protocols frequently shared by both intelligence operations.

G. This comprehensive approach also illustrates the technologies available and their intrusive nature which, if employed in LAWINT, must be carefully controlled to meet constitutional and statutory requirements.

H. As illustrated in Figure VI-1...

1. *Component 1—Operations Methodology* includes:

- Overt Activities
- Discrete Activities
- Covert Activities
- Clandestine Activities.

2. *Component 2—Operations Media* includes:

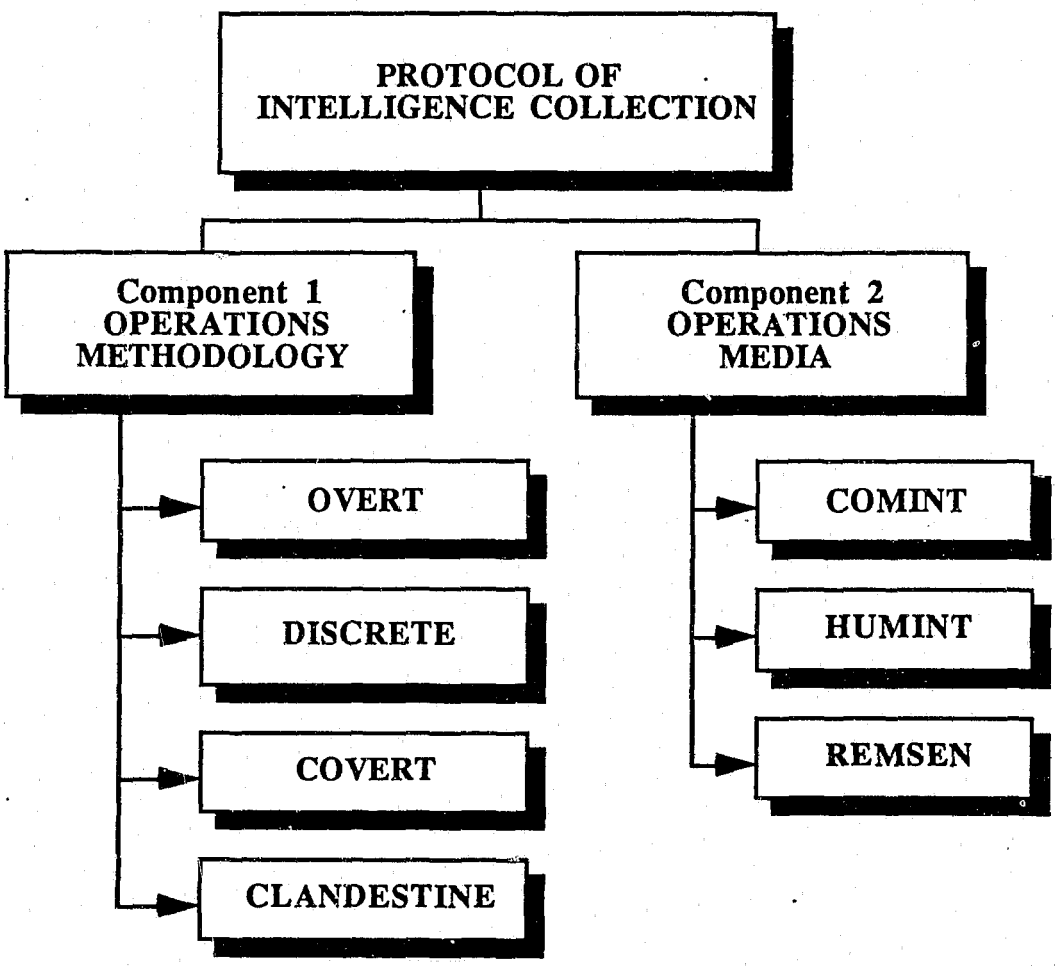
- Communications intelligence (COMINT)
- Human intelligence (HUMINT), and
- Remote sensing (REMSEN).

2. COMPONENT 1—OPERATIONS METHODOLOGY

A. **Overt Activities** - A collection activity which is conducted openly and may be acknowledged by and attributed to its agency/sponsor and participants.

Figure VI-1

INTELLIGENCE COLLECTION PROTOCOL



EXAMPLES: Interviewing criminal suspects or witnesses and accessing public records are examples of overt LAWINT collection.

B. **Discrete Activities** - A collection activity which must be conducted cautiously to avoid undue curiosity and public interest, to minimize interference with the collection activity, and to minimize the suspicions of the intelligence target. Discrete activities may be acknowledged by and attributed to its agency/sponsor.

EXAMPLES: Surveillance of an intelligence target's associates, photographing an intelligence target, or interviewing neighbors and acquaintances of an intelligence target.

C. **Covert Activities** - A covert activity is planned and executed to conceal the collection of information and/or the identity of any officer or agent participating in the activity.

EXAMPLES: Undercover operations, electronic eavesdropping, and "closed" surveillance of an intelligence target would fall within this category.

NOTE: In NASINT, a covert activity is designed to collect information or influence events of an intelligence target in a manner wherein the activity's sponsor(s) may maintain "plausible deniability" of participation or sponsorship.

D. **Clandestine Activities** - An activity which is usually extensive and goal-oriented, planned and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation.

EXAMPLES: "Storefront" operations, "stings", and certain concentrated undercover investigations (such as ABSCAM) can be classified as clandestine LAWINT collection.

NOTE: In NASINT, clandestine activities are designed to gather information and/or influence events without detection that the operation ever occurred.

3. COMPONENT 2—OPERATIONS MEDIA

A. Human Intelligence (HUMINT)

1. *Defined*:

> Intelligence gathering methods which require human interaction or observation of the target or targeted environment.

2. The intelligence is collected through the use of...

   • One's direct senses,

   • Optical enhancement of the senses, and/or

   • Audio enhancement of the senses. (*See* Figure VI-2)

3. ***Types of HUMINT***:

   a. *Direct Interaction* - The LAWINT analyst or investigator interacts in an official capacity with the intelligence target or principals of the case usually through an interview or interrogation.

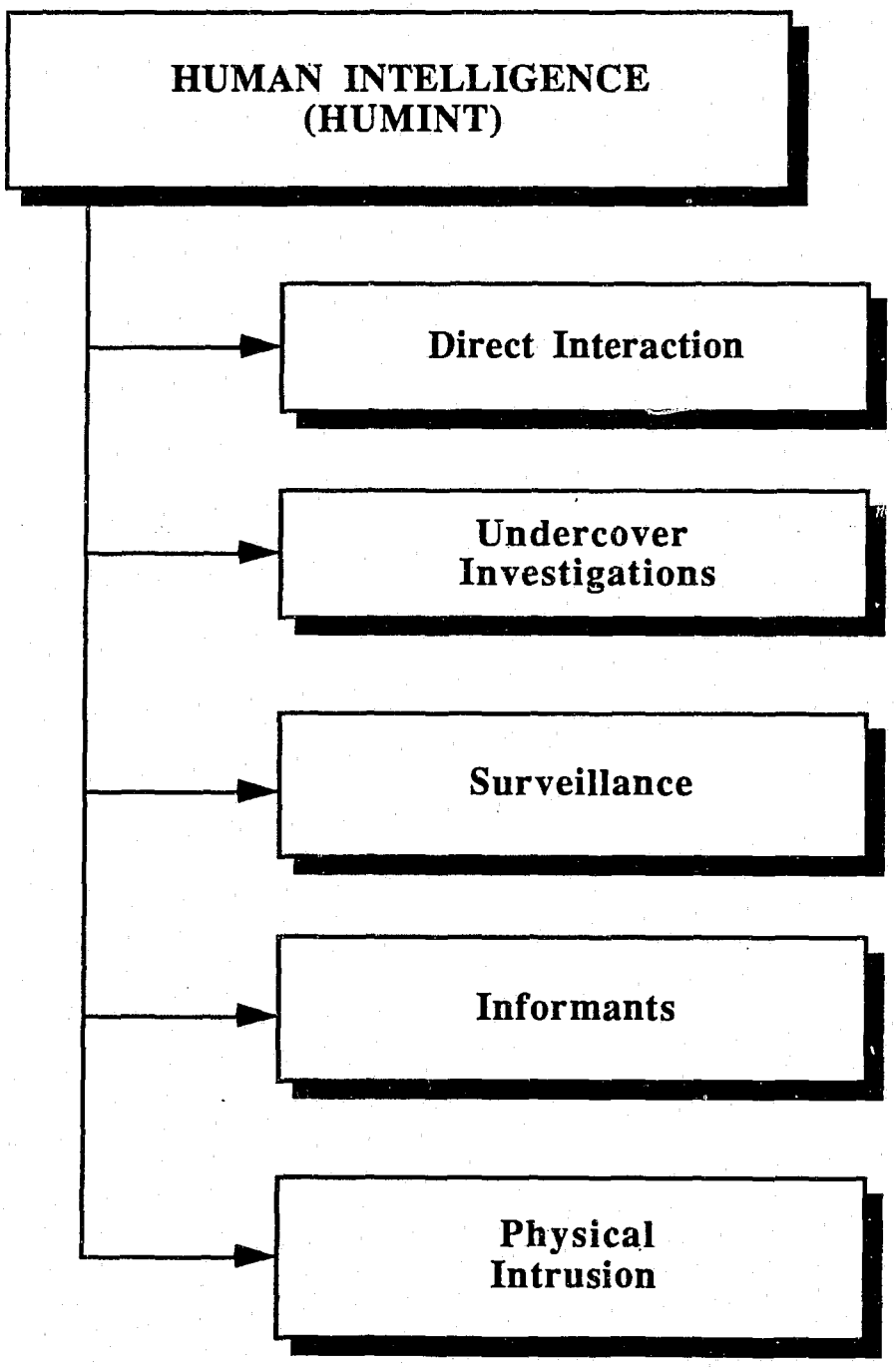
   b. *Undercover Investigation* - Active infiltration (or attempting to infiltrate) a group believed to be involved in criminal activity and/or the interaction with a LAWINT target with the intent to gather incriminating information or "lead" information which is used for the furtherance of a criminal investigation.

   c. *Surveillance* - The observation of activities, behaviors, and associations of a LAWINT target (individual or group) with the intent to gather incriminating information or "lead" information which is used for the furtherance of a criminal investigation.

   d. *Informants* - The solicitation of information from persons not affiliated with the LAWINT agency for purposes of gathering incriminating information on the intelligence target or information which will further the investigation.

Figure VI-2

HUMAN INTELLIGENCE



1) The individual may be either a "citizen" informant or "criminal" informant.

   a) A "citizen informant" is a person whose motives are based on their personal interest in maintaining order and minimizing crime in their community

      (1) On face value the citizen is reliable

      (2) There are no "payoffs" or other reciprocation expected beyond keeping the citizen informed

   b) The "criminal informant" is a person who gives the police information for ulterior, personal reasons

      (1) Motives may include:

      - Money
      - Revenge
      - Removing "competition"
      - Fear

      (2) Care must be taken to:

      - Ensure the criminal informant's reliability
      - Protect the informant's identity
      - Maintaining control records of the informant's information, payments, use of information, etc.

      NOTE: Figure VI-3 presents a model policy dealing with Confidential Informants

2) The information sought may be that learned by the informant during past interaction with the LAWINT target or that of planned future interaction with the target.

e. *Intrusion* - Information is gathered by intelligence officers/agents through the physical intrusion into a residence, building, or vehicle.

   1) In LAWINT the intrusion is typically part of a lawful search.

Figure VI-3

SAMPLE POLICY FOR USE OF CONFIDENTIAL INFORMANTS

I. PURPOSE

The purpose of this policy is to provide regulations for the control and use of confidential informants (CI).

II. POLICY

In may instances a successful investigation cannot be conducted without the use of CIs. While the use of CIs is an effective tool in investigations, it can be undermined by the misconduct of either the CI or the officer utilizing the informant. Therefore, it shall be the policy of this law enforcement agency to take necessary precautions by developing sound informant control procedures.

III. DEFINITIONS

A. Confidential Informant File: Files maintained in order to document all information that pertains to confidential informants.

B. Unreliable Informant File: files containing information pertaining to individuals determined generally unfit to perform as informants.

IV. PROCEDURES

A. Establishment of an Informant File System

1. The commanding officer in charge of the criminal investigations function shall be responsible for developing and maintaining master informant files and an indexing system.

2. A file shall be maintained on each CI used by officers. Each file shall be coded with an assigned informant control number and shall contain the following information:

a. Informant's name

b. Name of officer initiating use of the informant.

c. Informant's photograph, fingerprints, and criminal history record.

d. Briefs of information provided by the CI and its subsequent reliability. If an informant is determined to be unreliable, the informant's file shall be placed in the unreliable informant file.

e. Signed informant agreement.

f. Update on active or inactive status of the informant.

3. The confidential and unreliable informant files shall include an indexing system. An informant history summary, coded with the informant control number, shall be prepared to correspond to each informant file and include the following information:

a. Special skills or avocations;

b. Date of birth;

c. Aliases, monikers

d. Height, weight, hair color, eye color, race, sex, scars, tattoos or other distinguishing features;

e. Current home address and telephone number;

f. Residential addresses over the past five years;

g. Current employer, position, address and telephone number;

h. Marital status and number of children;

i. Vehicles owned and their registration numbers; and

j. Places frequented

4. Informant files shall be maintained in a secured area within the criminal investigations or intelligence section.

5. The two informant files shall be utilized in order to:

a. Provide a source of background information about the informant;

b. Provide complete history of the information received from the informant;

c. Enable review and evaluation by the appropriate supervisor of information given by the informant; and

d. Minimize incidents that could be used to question the integrity of investigators or the reliability of the CI.

6. Access to the informant files shall be restricted to the chief law enforcement executive, the commander of criminal investigations, or their designees.

7. Sworn personnel may only review an individual's informant file upon the approval of the commander of criminal investigations. The requesting officer shall submit a written request explaining the need for the review. A copy of this request, with the officer's name, shall be maintained in the CI's file.

B. Use of Informants

1. Before using an individual as a CI, an officer must receive initial approval from a supervisor authorized to make this approval.

2. The officer shall compile sufficient information through a background investigation in order to determine the reliability and credibility of the individual.

3. After the officer receives initial approval to use an individual as a CI, an informant file shall be opened.

4. All persons determined to be unsuitable for use as a CI shall be referenced in the Unreliable Informant File.

5. An officer wishing to utilize an unreliable informant shall receive prior approval from the chief executive officer or his/her designee.

C. General Guidelines for Handling CIs

1. All CIs are required to sign and abide by the provisions of the department informant agreement [sample agreement attached.] The officer utilizing the CI shall discuss each of the provisions of the agreement with the CI, with particular emphasis on the following:

a. Informants are not law enforcement officers. They have no arrest powers, are not permitted to conduct

searches and seizures, and may not carry a weapon.

b. Informants will be arrested if found engaging in any illegal activity. They will receive no special legal considerations.

c. Informants are not to take, and the department will not condone, any actions that may be considered entrapment. Entrapment occurs where the informant encourages, persuades or otherwise motivates a person to engage in criminal activity.

2. No member of this agency shall knowingly maintain a social relationship with CIs while off-duty, or otherwise become personally involved with CIs. Members of this agency shall not solicit, accept gratuities, or engage in any private business transaction or sexual activity with a CI.

3. Whenever possible, an officer shall always be accompanied by another officer when meeting a CI.

4. Juveniles shall only be utilized as CIs in accordance with departmental regulations and state laws pertaining to juveniles.

BY ORDER OF

CHIEF OF POLICE

This model confidential informants policy was developed under the auspices of the Advisory Board to the IACP/BJA National Law Enforcement Policy Center.

This policy is intended to serve as a guide to the police executive who is interested in formulating a written procedure to govern the use of confidential informants. The police executive is advised to refer to all federal, state, and municipal statutes, ordinances, regulations, and judicial and administrative decisions to ensure that the policy he/she seeks to implement meets the unique needs of the jurisdiction. See, ***The Police Chief****, January (1990), pp. 56—57.*

(Figure VI-3, ***continued next page...*** **)**

(Figure VI-3, *concluded...*)

INFORMANT AGREEMENT

*During my association with the (**name of jurisdiction**) Police Department as an Informant, I, the undersigned, do hereby agree to be bound by the following conditions and procedures while so associated:*

1. *I agree that I have no police power under the State of (**name**) or any local government subdivision and have no authority to carry a weapon while performing my activity as an informant.*

2. *I acknowledge that I am associated with the (**name**) Police Department as an Informant on a case or time basis as an independent contractor and that any payment I receive from the (**name**) Police Department will not be subject to Federal or State income tax withholding or Social Security. All reporting of income is the responsibility of the Informant.*

3. *I further acknowledge that as an informant and independent contractor, I am not entitled to Workman's Compensation or Unemployment Compensation from the State of (**name**) and I shall not hold (**name**) County liable for any injuries or damage incurred by reason of my association with the (**name**) Police Department.*

4. *I further agree not to divulge to any person, except the investigator with whom I am associated, my status as an informant for the (**name**) Police Department unless required to do so in court, and shall not represent myself to others as an employee or representative of the (**name**) Police Department.*

5. *I further agree not to use the (**name**) Police Department or any of its officers as credit references or employment references unless prior approval is obtained from the Investigator with whom I am associated.*

6. *I further agree that my association with the (**name**) Police Department does not afford me any special privileges.*

7. *I further agree that after making a purchase of anything of evidentiary value, I will contact the Investigator with whom I am associated as soon as possible for delivery of such evidence to him/her.*

8. *I further agree to maintain a strict accounting of all funds provided by me by the (**name**) Police Department as part of my activity as an Informant. I understand that misuse of government funds could be grounds for criminal prosecution against me.*

9. *Finally, I agree that violation of any of the above enumerated provisions will be grounds for immediate termination and probable criminal charges.*

*Dated this (**numerical**) day of (**month**), 19 (**year**).*

INFORMANT AND INVESTIGATOR SIGNATURES

2) In NASINT, evidence exists of intrusion into offices, residences, and vehicles to inspect or record documents and inspect premises or equipment for intelligence purposes.

NOTE: The specific degree of lawfulness of such activities is difficult to stipulate based on the varied locales, circumstances, and authorizations for such intrusions.

3) In LAWINT, any intrusions must be based on a lawful court order, one of the *bona fide* exceptions to the Fourth Amendment search warrant requirement, or, in limited cases, circumstances of exigency.

B. Communications Intelligence (COMINT)

1. *Defined*:

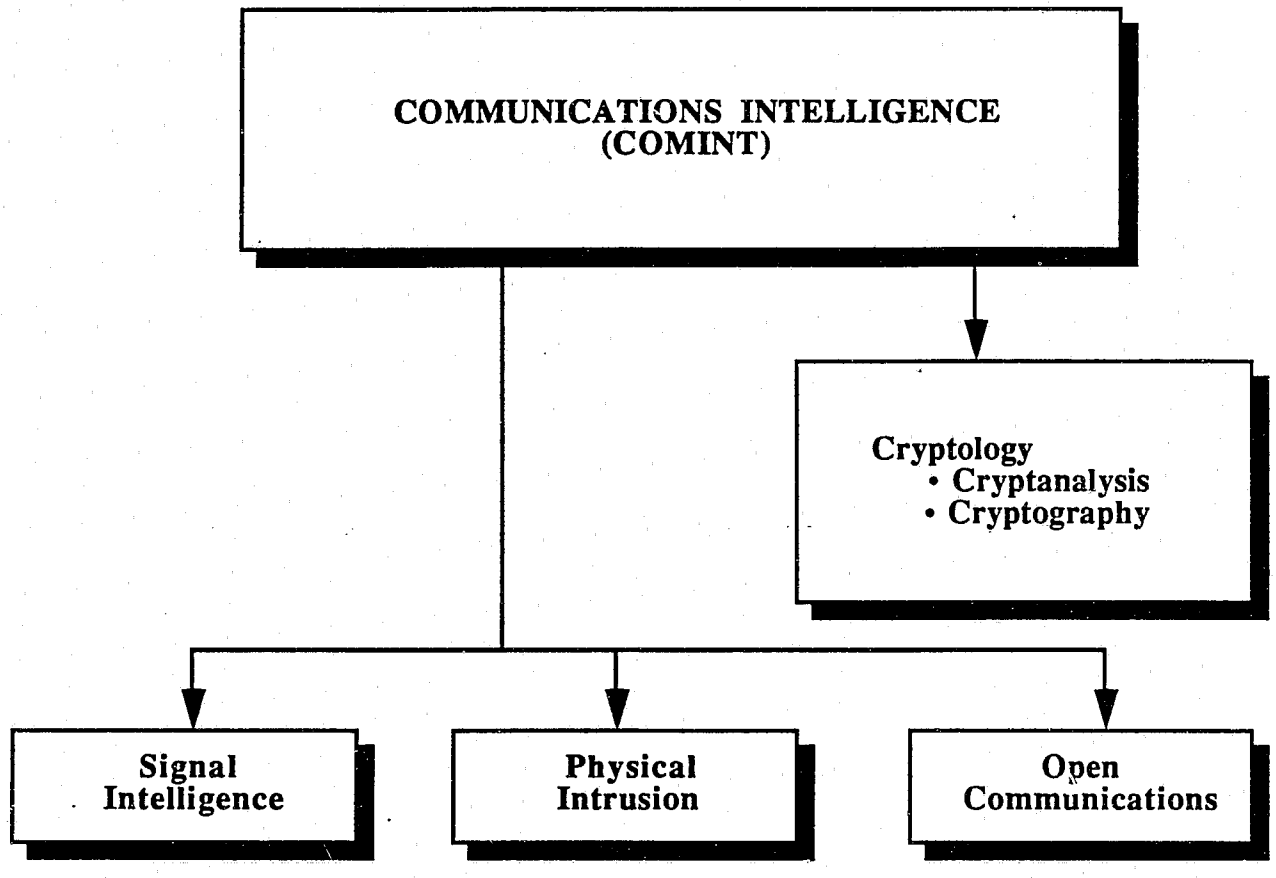
> This is the capture of information—either encrypted or in "plaintext"—exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between inter-communicating parties or groups, and/or analysis of the substantive meaning of the communication. (See Figure VI-4)

2. ***Types of COMINT:***

a. *Signal Intelligence (SIGINT)* - The interception of various radio frequency signals, microwave signals, satellite audio communications, nonimagery infrared and coherent light signals, and transmissions from surreptitiously placed audio micro-transmitters in support of the COMINT activity.

Figure VI-4

COMMUNICATIONS INTELLIGENCE



b. *Physical Intrusion* - The interception of communications as a result of a physical intrusion into the communications medium such as opening mail; seizure of non-public written communications or documents; tapping telephone lines; interception of cable communications; or accessing computer-driven communications systems through direct or remote surreptitious access to the system.

c. *Open Communications (OPCOM)* - The collection of open or publicly available communications, broadcasts, audio or video recordings, propaganda, published statements, and other distributed written or recorded material for purposes of analyzing the information.

3. A support function for COMINT which is primarily found in NASINT, but is also found to a lesser extent in LAWINT, is **cryptology**:

a. *Defined*:

> Cryptology is the study of communications encryption methods which deal with the development of "codes" and the "scrambling" of communications in order to prevent the interception of the communications by an unauthorized or unintended party.

b. Two activities of cryptology are:

1) ***Cryptanalysis*** - The process of *deciphering* the encrypted communications of an intelligence target.

2) ***Cryptography*** - The *creation* of a communications code/encryption system for communication transmission with the intent of precluding the consumption and interpretation of one's own messages.

C. Remote Sensing (REMSEN)

1. *Defined*:

> The collection of information which is typically not communications but can be viewed or interpreted by intelligence personnel to learn more about the intelligence target and provide support for case preparation.

2. Remote Sensing methods include (*See* Figure VI-5):

   a. *Imagery* - The representation of an object or locale produced on any medium by optical or electronic means. The nature of the image will be dependent on the:

      1) Sensing Media - the technology and procedures used to capture and record the image

      2) Platform - the location or vehicle on which the sensing equipment is mounted

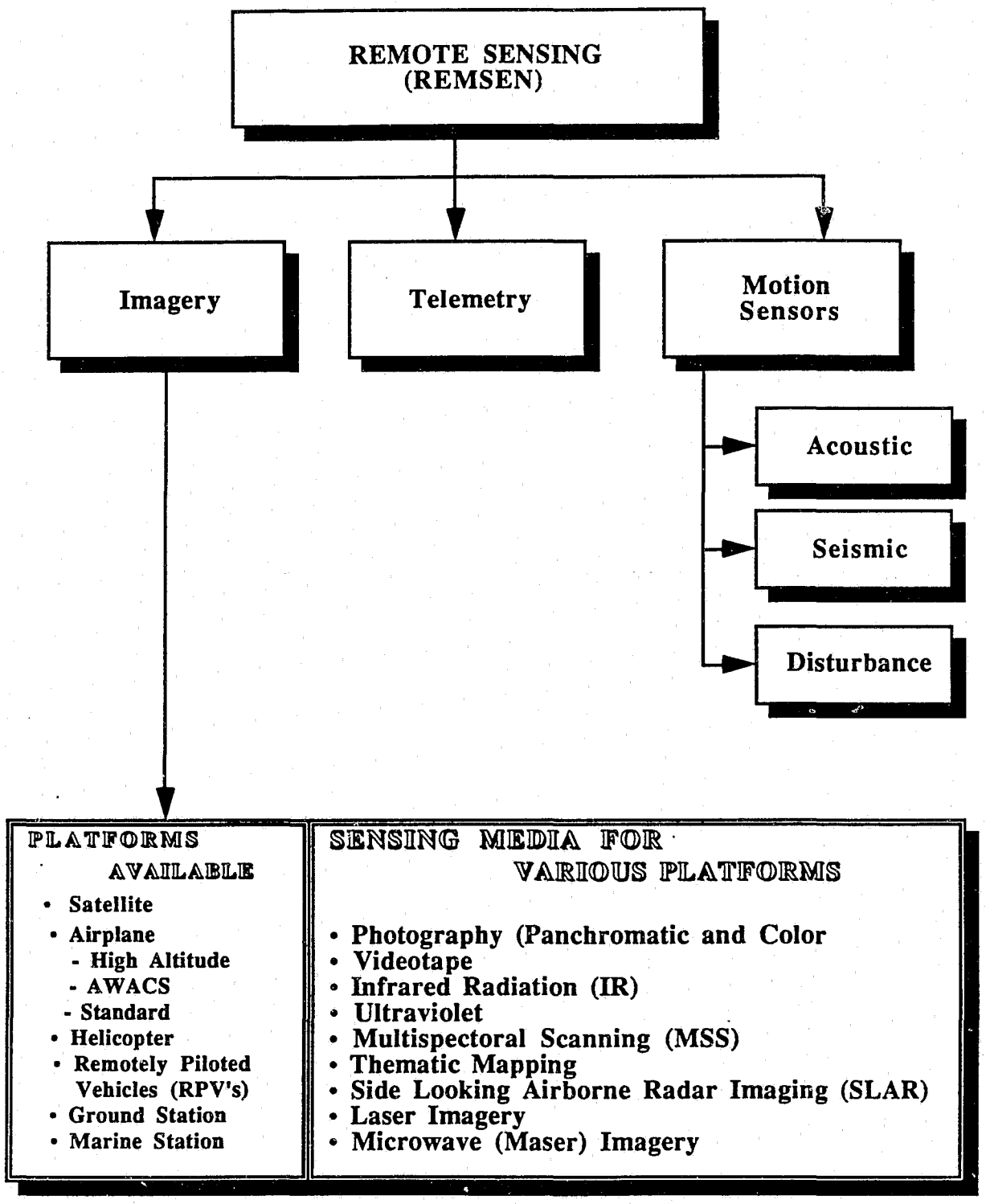
      NOTE: Importantly, many images, once captured and processed, will then require interpretation, and sometimes enhancement, by a trained professional before meaningful information can be gleaned from the image.

   b. *Telemetry* - The collection and processing of information derived from noncommunications electromagnetic radiations emitting from sources such as radio navigation systems (e.g., transponders); radar systems, and information/data signals emitted from monitoring equipment in a vehicle or device.

   c. *Motion Sensing* - Various methods exist to detect the presence, direction, and nature of moving people, vehicles, or objects. Motion sensors may be on either a fixed or mobile platform

Figure VI-5

REMOTE SENSING



1) Acoustic Sensors - Acoustic energy may be radiated in wave form through either air or water. Acoustic sensors, including both wave sensors and SONAR, can detect ships, boats, aircraft engines, motor vehicle engines, and other entities which create water or airwave disturbances. Some acoustic sensors are also attuned to certain noises/sounds and are activated upon detecting these acoustic disturbances.

   NOTE: Acoustic sensing does not include communications.

2) Seismic Sensors - Energy transmitted through reverberations in the earth ranging from foot steps, to vehicle movements, to the detonation of explosives.

3) Disturbance Sensors - Sensors designed to emit a notification signal if a "trip" or "switch" is disturbed as a result of the presence or passing of a person or object.

4. COLLECTION BARRIERS FOR LAWINT

A. It is evident that LAWINT may face barriers in the utilization of some collection protocols.

B. Administrative mechanisms should be in place to evaluate these barriers prior to the use of any particular protocol to ensure:

1. The protocol may be *properly used*, and

2. The protocol is within the *administrative capability* of the organization

C. The barriers include (See Figure VI-6):

1. **Legal Limitations** - LAWINT is subject to important constitutional and statutory provisions with respect to information collection. Certain methods of information gathering may only be used under limited conditions or not at all.

2. **Resources** - The agency may not have the equipment, personnel, or money to employ some collection methods.

3. **Access** - A LAWINT agency may not have access to certain technologies due to security restrictions or availability.

4. **Expertise** - An agency may not be able to employ certain protocols because personnel have not been trained in the use of the collection procedure or interpretation of the information collected.:

5. **Jurisdiction** - The authority of the agency and/or the geographic characteristics of the locale may preclude reasonable use of certain methods.

6. **Ramifications of the Collection** - An agency may decide against using a given protocol if it is perceived that public discovery of the protocol would adversely affect the agency's reputation or integrity. This may occur even if the protocol is lawful, but potentially offensive to the community.

7. **Ethics** - LAWINT personnel may determine that a particular protocol or situation may be inconsistent with ethical standards or values of the agency.

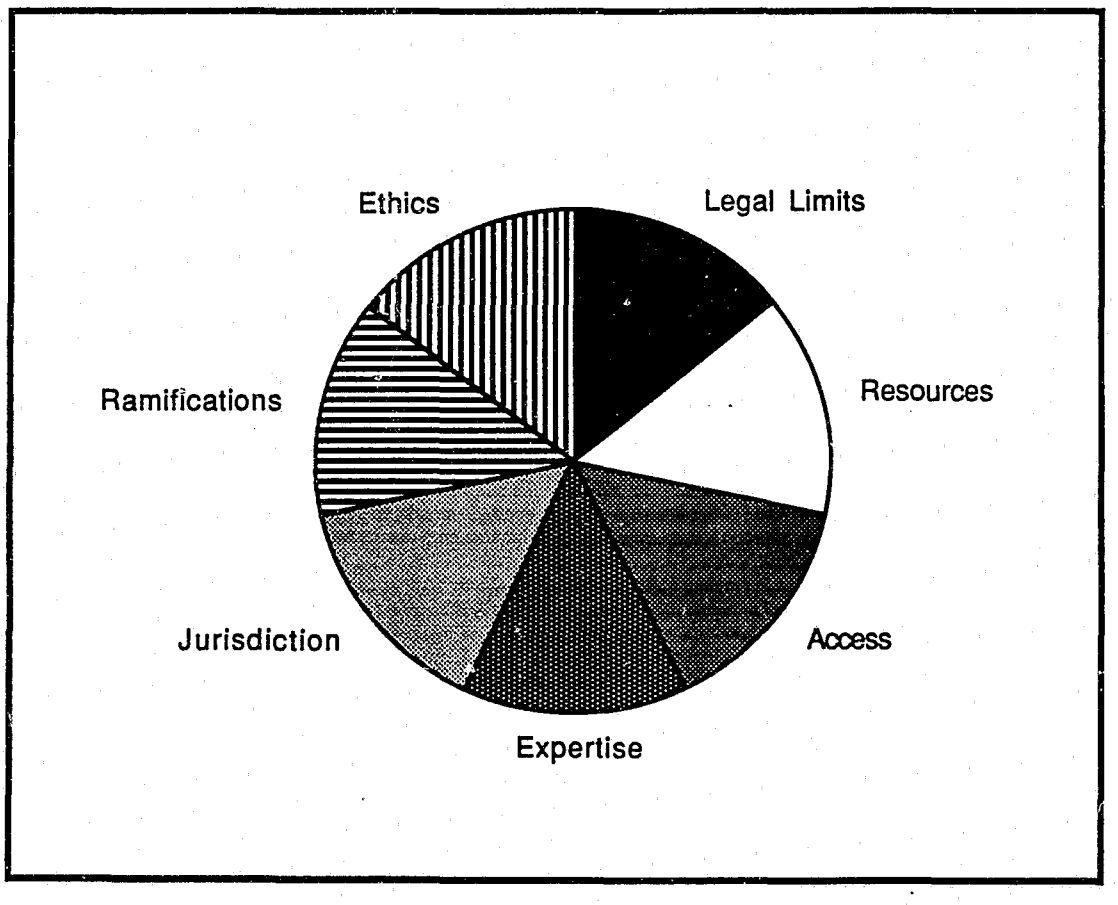
D. Recognition of these barriers, when properly addressed, have a positive effect on LAWINT by imposing controls on the intelligence function which will ...

1. Increase efficiency and effectiveness

2. Decrease accusations of improper police behavior

Figure VI-6

BARRIERS TO INTELLIGENCE COLLECTION



6. COLLECTION OF INFORMATION

Instructional Support and Criteria

GOAL:

To define the wide range of information useful for LAWINT and classify different methods and means to collect that information.

OBJECTIVES:

1. Students will be able to differentiate between information collection *protocol* and information collection *media.*

2. Students will have an overview understanding of techniques and technologies which may be employed for the collection of intelligence information.

STUDY QUESTIONS:

a. In discussing information collection, distinguish between *operations media* and *operations methodology.*

b. What different criteria must one consider in the use of the various types of *human intelligence*?

c. What types of communications intelligence would most typically applicable to a municipal police department?

d. What three barriers to intelligence collection would you consider to be the most important concerns of a police manager? Discuss your rationale for selecting those barriers.

NOTES

CHAPTER 7

THE INFORMATION COLLECTION RESPONSIBILITY: SPECIAL ISSUES AND UNDERCOVER OPERATIONS

"There has always been one untidy phase of police work, a distasteful but vitally important ingredient in the chemistry of manhunting...informers."
Melvin Pervis, FBI, 1936

1. A PERSPECTIVE ON INFORMATION COLLECTION

While basic categories of information collection were previously presented, a more detailed examination of the different methodologies and their ramifications is warranted given the importance of the collection function. The detail is needed in order to ensure:

- Expertise is developed in personnel utilizing the different methods
- Sufficient resources are available
- Policies and procedures are established to account for collection activities
- Assessment standards are in place to minimize dysfunctional ramifications arising from the collection process

2. DIFFERENT INFORMATION COLLECTION METHODS

A. **Direct** - Information is obtained through interviews, conversations, undercover interaction, or physical surveillance of the target

B. **Enhanced Direct** - Information is gathered through direct surveillance of the target from a distance through the use of technologies which enhance images or sounds

C. **Unobtrusive Collection** - Information gathered from records (public or private), newspapers, credit bureaus, and other sources

D. **Data Analysis** - Includes examination of aggregate data in individual information which can be distilled to present probabilistic or circumstantial information about the target

E. **Signal Interception** - The interception of radio, telephone, or cable messages of the target

F. **Image Recording** - The spectrum of methodologies range from traditional panchromatic photographs with standard photographic equipment to thermal infrared sensing from satellites

G. **Telemetry** - The remote measurement and observation of air or sea vessel movements based on propellant characteristics, noise/vibration, radar, or sonar detection methods

H. **Electronic Surveillance of Human Characteristics** - In collecting intelligence information a method of frequent importance is electronic surveillance—there are five types of human characteristics subject to electronic surveillance:

1. **Movements** - "where someone is"—Individuals can be tracked electronically via beepers as well as by monitoring computerized transactional accounts in real time

2. **Actions** - "what someone is doing or has done"—Electronic devices to monitor action include: monitoring of keystrokes on computer terminals (the so-called "Tempest System"), monitoring of telephone numbers called with pen registers, cable TV monitoring, monitoring of financial and commercial computerized accounts, and accessing computerized law enforcement or investigatory systems

3. **Communications** - "what someone is saying, writing, hearing, or receiving"—Two-way electronic communications can be intercepted whether the means be analog or digital communication via wired telephones, cordless phones, cellular phones, or digital electronic mail; two-way non-electronic communication can be intercepted via a variety microphone devices and other transmitters

4. **Actions and Communications** - "the details of what someone is doing or saying"—electronic visual surveillance, generally accompanied by audio surveillance, can monitor the actions and communications of individuals in both private and public places during either daylight or darkness

5. **Emotions** - "the psychological and physiological reactions to circumstances"—polygraph testing, voice stress analysis (which has some notable reliability problems), breath analyzers, and brain wave analyzers attempt to determine an individual's reactions to issues and/stimulants

3. THE USE OF UNDERCOVER OPERATIONS

An important strategy relied on heavily by law enforcement for information collection and case building is ***undercover operations***.

A. Covert, undercover, operations are an important element in gathering some forms of intelligence information in the development of cases.

1. In some agencies intelligence personnel may be directly involved in the undercover operation

2. In other agencies the intelligence unit will be indirectly involved through operational planning and specifying the nature and types of information which would be valuable in the overall development of a case.

3. In yet other agencies undercover operations will be totally segregated with the intelligence unit only being a recipient of applicable information.

B. Undercover operations are generally applied to:

1. Tactical intelligence

2. Operational intelligence

C. The different undercover approaches are dictated by...

1. Various laws affecting different agencies in different jurisdictions;

2. The nature of the law enforcement organization;

3. The size and sophistication of both the intelligence unit and the undercover entity;

4. The managerial philosophy of the agency's administrator; and

5. Organizational politics. (*which should never be underestimated*)

D. Perhaps the most desirable model is to have the intelligence unit serve in an advisory role in the planning and direction of an undercover operation.

1. Importantly, there must be open, timely, and comprehensive communications between the undercover operation and the intelligence unit on applicable cases.

2. Unfortunately, too many times these are seen as *competing* rather than *cooperative* actions, the result:

a. Overall reduced effectiveness

b. Wasted resources

4. THE JEOPARDY ASSOCIATED WITH UNDERCOVER OPERATIONS

Any covert or undercover activity has the potential for danger and abuse. Cognizance of these threats is necessary for not only undercover operatives and their managers but also for intelligence unit personnel and others who may have to deal with the information gathered and actions taken during undercover operations. In this regard, the following identifies broad based concerns and dangers of undercover operations (See Figure VII-1). (Distilled from the Report of the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, investigating FBI Undercover Operations, 641984.)

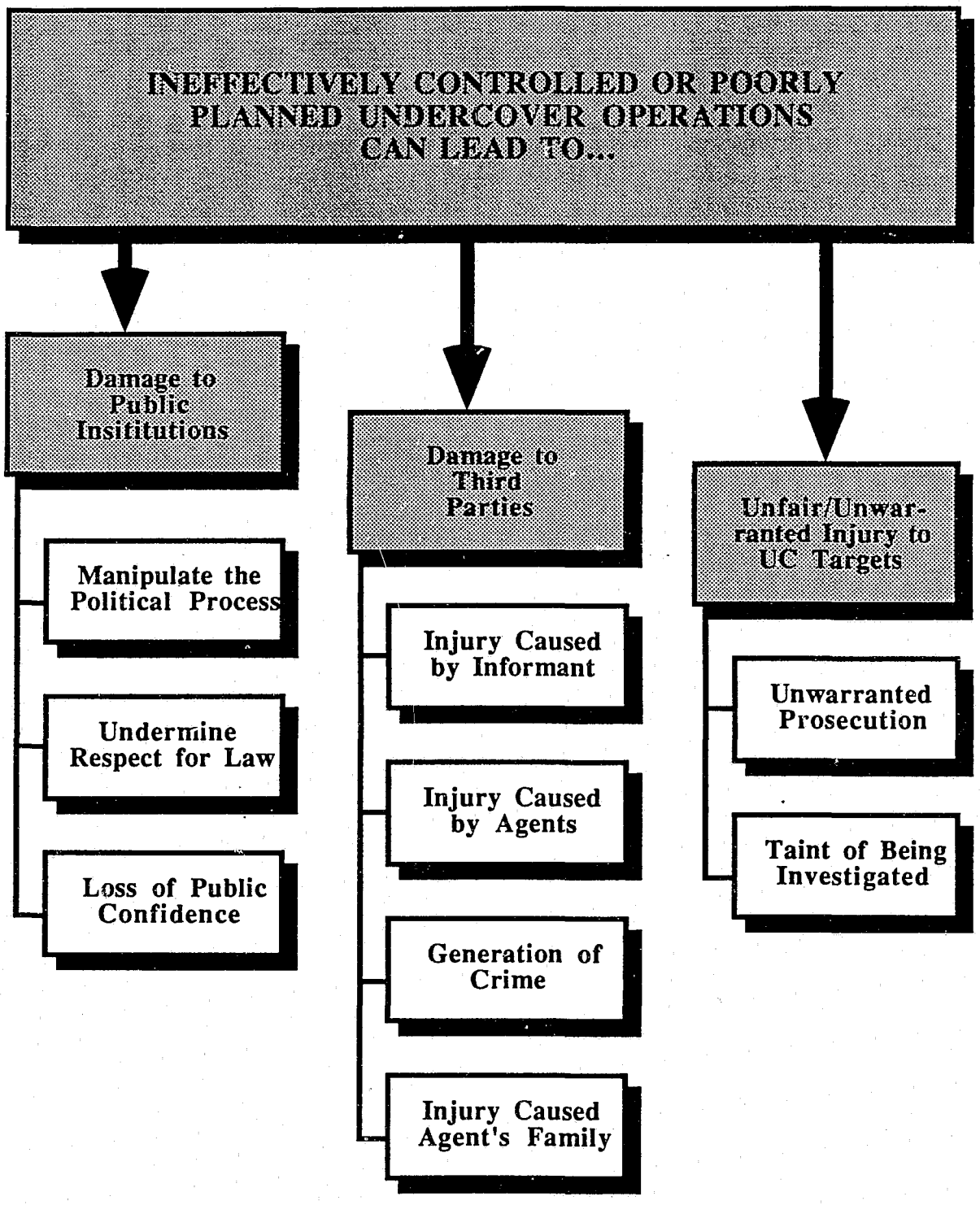
Importantly, all of the dangers and damages described below have occurred (and can be documented) during the course of various law enforcement undercover operations. An excellent source for discussion of issues on police undercover operations is Marx (1988), *Undercover: Police Surveillance in America.*

A. Damage to Public Institutions

1. *Manipulation of the political process*—undercover operations, particularly those involving public officials where wrong doing is not proven, carry the potential for manipulating the political process and tampering with history

Figure VII-1

JEOPARDY OF UNDERCOVER OPERATIONS



EXAMPLE: Unsustained allegations of bribery by members of Congress

2. *Loss of public confidence in government or an institution*— undercover operations focusing on public officials should be painstakingly controlled so as to collect necessary evidence yet avoiding any activity which exaggerates the extent or overly dramatizes any corrupt acts of officials

   EXAMPLE: Public perceptions of FBI competence and professionalism were undermined following the Watergate burglary and during the tenure of interim FBI Director L. Patrick Gray.

3. *Undermining respect for the law* —if undercover investigations do not maintain the sanctity and respect of law then the principles under which public institutions operate may be undermined encouraging others to disregard the law and those principles

   EXAMPLE: Publicized frustrations of police undercover officers planting evidence and committing perjury in order to "get a known criminal" when they had been unsuccessful by following lawful criminal procedure.

B. Damage to Third Parties

1. *Injury caused by informants*

   a. In efforts to maintain an informant's confidentiality and credibility as well as to keep the informant actively involved in the pursuance of a "higher level" criminal; agencies may give informants "tolerance" in behavior and, in fact, *support the informant's limited involvement in criminal acts*

   b. While this may need to be a legitimate trade-off in some circumstances, the agency needs to ensure that informants do not cause victimization or damage to other parties for the sake of a criminal investigation

EXAMPLE: A thief who is an informant continues to steal and pawn the stolen property with the knowledge of an officer. The officer uses this knowledge to obtain more information despite the continued criminal victimizations.

NOTE: There are both important legal and ethical questions in this practice.

2. *Injury caused by agents*

   a. In the furtherance of an undercover operation, agency personnel have caused losses of respect and trust to innocent persons and loss of income, even damage, to businesses only peripherally associated with the investigatory target

   b. In many of these cases the injury was caused by:

      1) Inadequate planning, evaluation, and monitoring of actions of undercover personnel

      2) Investigations were exploratory without a sufficiently sound evidentiary basis for direction or "target hardening"

         EXAMPLE: Agents may cause physical damage to a business, discourage customers, or involve the business owner in an investigation only because a crime target frequents the business, **not** because the business is suspect.

3. *Generation of crime*

   a. Evidence exists that some undercover operations actually increase or generate crime

   b. Undercover operations may contribute to crime by:

      1) Generating a market for the purchase or sale of illegal goods and services

      2) Generating the idea of crime

3) Providing a scarce skill or resource without which the crime could not be carried out

4) Providing a temptation to commit a crime to a person who would be unlikely to encounter the temptation had it not been for the undercover operation

5) Coercion, intimidation, or persuasion of a person to commit a crime who was not otherwise disposed to perform the criminal act

6) Generation of a covert opportunity structure for unlawful actions by undercover agents or informants

7) Retaliatory violence against an informer

EXAMPLE: Police operated pawn shops where undercover agents have "put the word on the street" that the pawn shop will "fence" stolen property

4. *Injury to agents, their families, and law enforcement agencies*

a. Physical threat of working undercover

b. Emotional/psychological stress of adopting a counter-cultural lifestyle

c. Effect of work hours, appearance, associates, etc. on personal behavior and family life

d. Danger of socialization into the criminal subculture targeted by the undercover operation

e. Participation in undercover operation opens possibility for corruption and misconduct

EXAMPLE: An undercover officer who works evenings and weekends, frequents bars, and may pretend to be single can have these factors negatively influence the officer's personal relationships causing a divorce or related familial problems.

C. Unfair or Unwarranted Injury to Targets of Undercover Investigations

1. *Unwarranted prosecution* (The *appearance* versus the reality of guilt)

   a. Sometimes initial information may indicate criminality even though a person may be innocent

   b. Undercover operations are to produce further information about the potential crime rather than create the environment and incentive for a criminal act

   c. To pursue prosecution on false beliefs and misstatements and to further prosecutorial efforts in this regard via undercover operations is a danger

   d. There is an enhanced potential for unjustified prosecutions as a result of the undercover investigation technique

      EXAMPLE: As a result of time, effort, money, reputation, and ego invested in a lengthy investigation, there is a tendency to not want to "go away empty handed"—thus, there may be prosecution on *some* charge to justify the investments.

2. *The taint of being investigated*

   a. Targeted individuals of an investigation may also suffer even if it is learned that initial impressions of impropriety are unfounded

   b. Being the subject of an investigation places suspicion in the minds of many persons associated with the target (including friends, family, and employers)

   c. While reasonable investigative leads should be followed-up, care must be taken in undercover operations to avoid any unwarranted taint of a person's reputation

   d. It must be remembered that there is a stigma (or taint) that attaches by merely being approached or identified as a possible investigation "target"

EXAMPLE: Notoriety of a person being investigated by the police is too often equated to guilt in the mind of the public, regardless of whether the suspect was excluded by police or found not guilty at trial (such as the McMartin child sexual abuse cases in Los Angeles.)

D. Safeguards Prior to Implementing Undercover Operations

1. Initiate investigations and employ undercover operations only when an agency *reasonably suspects* criminal activity of a given type or pattern is occurring or is likely to occur and an undercover operation is the most viable method to collect evidence and information concerning the criminal activity

2. The opportunity for illegal activity by the target(s) has been structured in the undercover operation so that there is reason for believing that persons drawn to the opportunity are predisposed to knowingly engage in the contemplated illegal activity

3. Undercover operations should be modeled as closely as possible to the conditions and environment of the real world so that the nature of the inducement offered by the undercover operation is not unjustifiable

4. In sum, avoid any behavior which may be construed to be entrapment

5. In evaluating the decision of whether to use undercover tactics, Marx (1988) offers arguments on both sides of the ethical debate

   a. These arguments can also aid in deciding the propriety of an undercover operation, hence, serving as an additional safeguard

   b. The arguments are presented as the overall "best case" situation

   c. *See* Figure VII-2 for the arguments

Figure VII-2

ARGUMENTS ASSOCIATED WITH USING UNDERCOVER OPERATIONS

For	*Against*
1. Citizens grant to government the right to use exception means.	1. Truth telling is moral, lying is immoral.
2. Undercover work is ethical when used for a good and important end.	2. The government should neither participate in, nor be a party to, crime nor break the law in order to enforce it.
3. Enforce the law equally.	3. The government should not make deals with criminals.
4. Convict the guilty.	4. The government should not offer unrealistic temptations or tempt the weak.
5. An investigation should be as nonintrusive and noncoercive as possible.	5. Do no harm to the innocent.
6. When citizens use questionable means, government agents are justified in using equivalent means.	6. Respect the sanctity of private places.
7. Undercover work is ethical when there are reasonable grounds for suspicion.	7. Respect the sanctity of intimate relations.
8. Special risks justify special prosecutions.	8. Respect the right to freedom of expression and action.
9. Undercover work is ethical when the decision to use it has been publicly announced.	9. It is wrong to discriminate in target selection.
10. Undercover work is ethical when done by persons of upright character in accountable organizations.	10. The government should not do by stealth what it is prohibited from doing openly.
11. Undercover work is ethical when it is undertaken with the intention of eventually being made public and judged in court.	

4. MANAGEMENT CONCERNS OF UNDERCOVER OPERATIONS

Previous discussions have addressed the management of undercover operations only peripherally. There are a wide range of issues which must be addressed for the undercover operation to be:

- Effective
- Safe
- Fundamentally Fair

The more critical issues are addressed below.

A. Selection of Undercover Personnel

1. Will the officer be physically and behaviorally able to assimilate information from the targeted undercover environment? — Can the officer adjust his/her personality?

2. Does the officer have the emotional and psychological attributes to perform in the facade necessary for undercover work?

3. Is the officer sufficiently responsible to work in the undercover environment with minimum supervision?

4. Does the officer have sufficient experience to assess and apply legal mandates?

5. Is the officer's integrity beyond question?

6. Does the officer have any history of disciplinary problems which may handicap his/her ability to function effectively in an undercover capacity?

7. Is the officer both *creative* and *accountable*?

B. Training for Undercover Work

1. What kinds of knowledge in *targeted substantive areas* are needed to be effective in undercover work?

EXAMPLES:
- Drugs
- Gang issues of "turf", "colors", etc.
- Techniques of burglars, auto thieves, etc.
- Street jargon for the targeted criminal areas

2. What kinds of unique *procedural knowledge* are needed for the targeted undercover operations?

EXAMPLES:
- Using informants
- Developing cases while avoiding entrapment
- Issues of narcotics simulation
- Report writing and documentation for undercover operations
- Use of special information collection equipment
- Accountability of confidential cash funds (e.g., informant money and "buy" money)

3. How much time will be afforded to "field train" a new undercover officer?

4. How will the undercover officers' "field break-in" period be evaluated?

C. Supervision of Undercover Officers

1. What kind of training is needed for supervisors to effectively supervise undercover officers?

2. On what basis will performance evaluations of undercover officers be made?

3. Given limited contact with officers, how can the supervisor best diagnose emerging problems associated with undercover officers?

4. How can officer accountability be ensured by the supervisor?

5. What kind of time schedules can be established for regular supervisor-officer conferences?

6. What types of counseling and leadership skills are uniquely needed for undercover supervisors?

7. How does the supervisor maintain accountability of overtime?

D. Employee Assistance

1. How long should the officer be permitted to remain in an undercover capacity?

2. What kind of balance needs to be made between an officer's personal sacrifices (e.g., family, friends, lifestyle, unique stress) associated with an undercover assignment and the benefits gained to the organization for an experienced and "established" undercover investigator?

3. How is the need for integrity maintained and reinforced?

4. What means can be taken to avoid the officer from being compromised?

   EXAMPLES:
   - Being "set up"
   - Officer's identity being discovered
   - Being socialized into the culture of the crime target
   - Avoiding *undue* danger
   - Ensuring officer back-up

E. Re-Integration into a Non-Undercover Assignment

1. Is retraining needed on "street" procedures?

2. What readjustment problems might the officer face?

3. Will the officer require any "re-socialization" counseling or assistance for the non-undercover assignment?

5. SPECIAL POLICY ISSUES

From an administrative perspective, there are a number of policy decisions which should be made with respect to the use of undercover operations as an intelligence collection method. Beyond those areas listed below, *See* Figure VII-3 for accreditation standards on police policy related to undercover operations. While the cited standards are from Chapter 43—*Organized Crime and Vice Control*, they have equal applicability to virtually all undercover operations.

Figure VII-3

SELECTED PROVISIONS OF LAW ENFORCEMENT ACCREDITATION STANDARDS RELATED TO UNDERCOVER OPERATIONS

The following standards are excerpts from the Commission on Accreditation of Law Enforcement Agencies' *Standards for Law Enforcement,* (1988), Chapter 43, Organized Crime and Vice Control, pp 43-3—43-4.

43.2.7 *The agency's budget provides for a confidential fund to support the operations of the vice and organized crime control functions.*

Commentary: The nature of the operations of these functions often requires frequent and sometimes large expenditures of money. This can include paying informants, purchasing contraband as evidence, and expenses for surveillance activities and equipment.

43.2.8 *A written directive establishes an accounting system for vice and organized crime control confidential funds, to include, at a minimum:*

- *authorization of one person as responsible for the system;*
- *submission of request for funds prior to payment;*
- *submission of receipt after payment to include: the amount and purpose of payment; officer's name; informant's name, if any; information or material purchased; subsequent law enforcement action, if any; date; case number.*
- *approval of chief executive for payments in excess of a specified amount; and*
- *quarterly audit and report of expenditures.*

Commentary: Although the amount of money in a larger agency's confidential fund can be much greater than the amount in a smaller agency's fund, the need for an accounting system is independent of agency size.

43.2.9 *A written directive establishes a system for the authorization, distribution, and use of surveillance and undercover equipment.*

Commentary: The intent of this standard is to establish a system of controls, policies, and procedures that will prevent unauthorized use and loss of often expensive and sophisticated surveillance equipment.

43.2.10 *A written directive establishes procedures for communication, coordination, and cooperation with other agency functions or components.*

Commentary: The control and suppression of vice and organized crime can be better accomplished with a concerted and coordinated effort by various components in the agency, especially the intelligence, patrol, and criminal investigation functions. The agency should establish procedures ensuring the exchange of information for both intelligence and operational activities.

43.2.11 *If an organized crime control, prosecution, and/or investigation unit operates in the agency's service area, a written directive establishes procedures for the agency's participation, communication, coordination, and cooperation with the unit.*

Commentary: Because organized crime can exist in several communities at one time, successful law enforcement efforts of one agency often displace the problem to another community rather than eliminate it. Organized crime control, prosecution, and/or investigation units are an effective means for coordinating the efforts of a number of local and state law enforcement agencies in the investigation and prosecution of persons involved in an organized criminal activity. The agency should establish procedures that enhance the exchange of information and personnel.

> **AUTHOR'S NOTE:** For related discussion, *See* Chapter 13—Intelligence Records, for a discussion and sample Intelligence Mutual Aid Pact.

43.2.12 *A written directive states the agency's criteria that determine which organized crime and vice complaints are investigated.*

Commentary: Investigation into vice and organized crime offenses can involve tremendous expenditures of time, money, and effort. By establishing criteria with which to evaluate the accuracy and credibility of initial information and determine the scope and relative importance of the problem, the agency can determine which vice and organized crime offenses should be investigated. This can be accomplished by proposing specific questions, such as: (1) Is the original intelligence information valid? (2) What is the criminal nature of the problem? (3) How important is the problem? (4) What lead information exists? (5) What investigative techniques might be used? (6) Does the agency have sufficient resources? (7) What possible operational problems exist?

> **AUTHOR'S NOTE:** For related discussion, *See* Chapter 9—Targeting

43.2.13 *The agency has the capacity to conduct covert operations for the control of vice and/or organized crime violations.*

Commentary: Vice and organized crime offenses, by their nature, often require officers to learn of and develop evidence of crime by infiltrating an operation or associating with persons suspected of criminal activity. The agency should have the resources for decoy, undercover, and surveillance operations.

42.2.14 *the agency has a written plan for conducting vice and organized crime surveillance operations, to include, at a minimum, provisions for the following:*

- *analyzing crimes and victims;*
- *identifying and analyzing probable offenders and their habits, associates, vehicles, methods of operation, or any other pertinent information;*
- *familiarizing the officer with the neighborhood or target area;*
- *determining operational procedures for observation, arrests, and "tails";*
- *supplying officers with expense funds;*
- *establishing means of communication;*
- *selecting equipment or vehicles;*
- *providing relief; and*
- *determining legal ramifications.*

Commentary: The intent of the standard is to establish guidelines for surveillance operations.

43.2.15 *The agency has a written plan for conducting vice and organized crime undercover operations, to include, at a minimum, provisions for the following:*

- *identifying and analyzing suspects;*
- *making contacts with suspects;*

- *analyzing neighborhood or target area where officers will work;*
- *supplying officers with false identity and necessary credentials;*
- *maintaining confidentiality of officers' false identity;*
- *supplying officers with expense funds;*
- *establishing means for routine and emergency communication;*
- *determining legal ramifications;*
- *providing guidelines for arrest;*
- *providing back-up security for officers;*
- *providing for close supervision*

Commentary: None

43.2.16 *The agency has a written plan for conducting vice and organized crime decoy operations, to include, at a minimum, provisions for the following:*

- *analyzing victims, crimes, and crime locations;*
- *disguising officers to resemble victims;*
- *determining the number of back-up officers for security and protection;*
- *developing operational procedures, such as observation and arrest;*
- *determining legal ramifications;*
- *establishing communications;*
- *identifying participating personnel;*
- *notifying patrol commander responsible for target area; and*
- *providing close supervision.*

Commentary: None

Policy issues include:

A. Use and accountability of confidential funds (*See* Figure VII-3, Standards 43.2.7 and 43.2.8)

B. Narcotics simulation (*See* Figure VII-4)

C. Consumption of alcohol during undercover operations (*See* Figure VII-5)

C. "Sterile" contact points (e.g., locations, phone numbers) between the undercover officer and crime target

D. Procedures for protection of the undercover officer (*See* Figure VII-3, Standard 43.2.15)

E. Integration of undercover operations with visible/overt police activities (*See* Figure VII-3, Standard 43.2.16)

F. Undercover officers participation of investigative activities *outside* of the agency's jurisdiction (*See* Figure VII-3, Standard 43.2.11)

G. Sufficient funding to support all elements of undercover operations (See Figure VII-3, Standards 43.2.14—43.2.16)

H. Ensuring that information gained in undercover operations is input to the intelligence cycle (*See* Figure VII-3, Standard 43.2.12)

I. Coordination of activities to avoid duplication (*See* Figure VII-3, Standard 43.210)...

1. With other elements of the agency

2. With other jurisdictions

NOTE: It is important to recognize the *administrative* issues associated with undercover activities as well as the *operational* issues.

Figure VII-4

SAMPLE POLICY FOR UNDERCOVER OFFICER NARCOTICS SIMULATION†

TITLE: Narcotic Simulation

POLICY: It is the policy of the Intelligence Section that the simulation of narcotics will be done when absolutely necessary to maintain the integrity of the investigation and/or the safety of the detective.

PROCEDURE: I. Because simulation is dangerous, the detective should exercise extreme caution when attempting this procedure. The technique involves the following:

A. As the detective places the cigarette between his/her lips, he exhales slowly causing the fire end of the cigarette to burn lightly.

B. As the detective removes the cigarette from his/her lips, he/she deeply inhales, thus simulating inhaling the effects of the marijuana.

II. Prior to any detective participating in an undercover investigation in which simulation may be necessary, it will be mandatory that the detective receive proper training in simulation as directed by the Intelligence Section supervisor.

III. Simulation will be limited to marijuana that has not been treated with any other controlled dangerous substance.

IV. Prior supervisor approval will be obtained whenever possible.

V. In the event approval cannot be obtained due to exigent circumstances, the following will be adhered to:

A. Notification to the supervisor as soon as possible, but in all cases no later than 24 hours after the simulation occurred.

B. The incident will be documented by the detective and/or the cover detective when applicable.

VI. In all cases of such simulation, or inadvertent ingestion, the supervisor will order the detective to submit to a drug screening test within 72 hours.

VII. A positive drug screening test will result in the detective being ordered to submit to a medical and psychological evaluation.

VIII. The detective's supervisor will be responsible for documenting all actions taken in conjunction with this procedure.

†Policy from the Baltimore County, Maryland Police Department

Figure VII-5

SAMPLE POLICY FOR UNDERCOVER OFFICER CONSUMPTION OF ALCOHOLIC BEVERAGES†

TITLE: Consumption of Alcoholic Beverages

POLICY: This procedure is established to provide guidelines for Intelligence Section personnel when there is a need to consume alcoholic beverages while working in an on-duty status.

PROCEDURE:

I. Prior to entering any liquor establishment (whether in or out of [the jurisdiction]) there shall be an investigative purpose established. Approval must be obtained from the detective's immediate supervisor prior to entry.

A. In those situations when the detective's immediate supervisor cannot be contacted, then any other supervisor within the Intelligence Section will be contacted.

B. In the event that immediate supervisor approval cannot be obtained due to exigent circumstances, the procedure is:

1. Notification of the supervisor as soon as possible, but in all cases no late than 24 hours after consumption of liquor.

2. The incident will be documented by the detective and/or cover detective when applicable.

II. Personnel will not consume more than two (2) alcoholic drinks during a regular tour of duty. This limit does not apply to the number of drinks purchased. due care shall be used when consuming alcoholic beverages so that his/her ability to function as a law enforcement officer does not become impaired.

III. In any situation where a detective becomes ill, or is unable to perform his/her assignment, he/she shall immediately contact his/her supervisor. Driving a motor vehicle is not permitted. Arrangements must be made for transportation.

IV. All expenses incurred will be reported on an Expense Voucher. A confidential report will be submitted listing which liquor establishments were visited, the number of drinks purchased, and the number of drinks consumed. Money expended for such items as tips, video and pinball machines, etc. shall also be recorded in the report.

V. Any deviation of this procedure shall be at the discretion of the Intelligence Section's Commanding Officer. It shall be documented and submitted for his approval.

†Policy from the Baltimore County, Maryland Police Department

7. THE INFORMATION COLLECTION RESPONSIBILITY: SPECIAL ISSUES AND UNDERCOVER OPERATIONS

Instructional Support and Criteria

GOAL:

> To identify and discuss issues of law and ethics related to certain information collection methods and alternate approaches to deal with these issues.

OBJECTIVES:

1. Students will be able to discuss the potential complications arising from preliminary information collection activities as related to LAWINT.

2. Students will gain an understanding for the potential damage which can be done to third parties and government institutions when information collection techniques are abused or inadequately controlled.

STUDY QUESTIONS:

a. Describe what you feel are concerns about "intrusiveness" related to the five types of human characteristics subject to electronic surveillance.

b. Describe what you feel are some of the greatest problems associated with law enforcement undercover operations.

c. As a result of the nature of law enforcement intelligence operations, the "taint of being investigated" is of particular concern. What does this mean?

d. In your opinion, what steps could law enforcement take to minimize the threat of unwarranted damage resulting from undercover operations?

NOTES

CHAPTER 8

STRATEGIC INTELLIGENCE FOR LAW ENFORCEMENT: AN OVERVIEW

"The police chief can not know too much about the community and he dare not know too little."
Comment of a Police Chief (Marx, 1989)

1. PLACING STRATEGIC INTELLIGENCE IN PERSPECTIVE

The functions of strategic intelligence (STRATINT) are similar in many ways to crime analysis. Similar methodologies are used, similar information is addressed, and similar variables are used. If any difference can be defined it is in the *focus* of the activity. Crime analysis (CRIMAN) is typically far more broad-based than STRATINT. Nonetheless, the similarities are such that in a moderate-sized police department both crime analysis and strategic intelligence could be performed by the same unit. That unit may be part of intelligence, part of planning and research, or a separate CRIMAN unit charged with both activities.

While the differences are subtle they nonetheless exist and should be recognized. Much of the value of the STRATINT activity will depend on crime patterns within the jurisdiction and information demands of operational units and administrators.

This section will attempt to accomplish three things:

- Clarify the roles of STRATINT and CRIMAN,
- Examine the protocols associated with STRATINT, and
- Place STRATINT in perspective with tactical intelligence (TACTINT) and operational intelligence (OPINT).

2. DEFINING CRITICAL TERMS

Understanding critical concepts is the initial step in effectively comprehending any activity. The following definitions and concepts provide a perspective to understand STRATINT and CRIMAN.

A. Crime Analysis - *Defined*:

> The process of analyzing information collected on crime and police service delivery variables in order to give direction for police officer deployment, resource allocation, and policing strategies as a means to maximize crime prevention activities and the cost-effective operation of the police department.

1. *Examples of Output and Purposes of CRIMAN*:

a. Crime and call dispersion patterns over defined time periods

b. Trends (increases/decreases) and alterations (geography/time) in police service demands

c. Profiles of types of calls received (e.g., nature of call, times, locations, descriptive information, and dispositions of various calls)

d. Demographic profiles of criminals stratified by crime and *modus operandi* (MO)

e. MO comparisons of arrested suspects to other outstanding crimes

f. Summary profiles of crimes, services, traffic, officer initiated activity, and arrests stratified by patrol divisions and/or beats

g. Identification of anomalies in police service demands for targeting by remedial strategies

2. CASE EXAMPLE:

A patrol commander is integrating a community policing program into the patrol division. As a result, the commander needs to establish a new deployment plan. In order to do this effectively, the commander orders crime analysis reports to describe types of calls received stratified by:

- Day
- Time
- Location

- Nature of Call
- Calls Requiring Immediate Response

The data will give the commander information on which to base sound decisions for officer and resource allocation for the new community policing program.

B. **Strategic Intelligence** - *Defined*:

> An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making and resource allocation; and the focused examination of unique, pervasive, and/or complex crime problems.

1. ***EXAMPLES of Output and Purposes of STRATINT.***

   a. Descriptions of commodity movement and trafficking patterns

   b. Changes in the types of unlawful commodities

   c. Trends and projections of targeted crimes

   d. Descriptions and profiles of alternate manifestations of targeted crimes

   e. Profiles of criminals involved in targeted crime

   f. Alternatives for directions of long-term investigative efforts

   g. Evaluation of the effectiveness of intelligence and investigative activities

   h. Identification of special resource needs

   i. Descriptions of special crime problems most amenable to intelligence analysis

2. **CASE EXAMPLE:**

A multi-jurisdictional drug task force commander needs to maintain information on the *types* and *quantity* of drugs coming into the jurisdiction of the task force. As a result, strategic intelligence reports are regularly researched and prepared describing the factors and trend changes which have occurred in drug trafficking transactions as well as projections of anticipated changes in those trends.

C. Both STRATINT and CRIMAN are consistently concerned with *resource allocation* and *personnel deployment*

1. *Definitions...*

a. **Allocation**

> The long-term assignment of personnel by function, geography, and shift/duty tour along with the commitment of required supporting resources to deal with crime and police service demands in the most efficient and effective manner.

b. **Deployment**

> The short-term assignment of personnel to address specific crime problems or police service demands.

2. These definitions are somewhat different than one finds in the literature dealing with, for example, patrol administration

a. The basis for the long-term/short-term distinctions is to place the problems and analytic processes in perspective to best understand the problem and assist in developing remedies to the problems

b. *Both* STRATINT and CRIMAN are concerned with deployment and allocation

D. As a result of the intelligence function, a common term used in intelligence activities is **target**—this refers to any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis.

E. The term **commodity** is any item or substance which is inherently unlawful to possess (contraband) or materials which, if not contraband, are themselves being distributed, transacted or marketed in an unlawful manner.

EXAMPLES: Drugs/controlled substances; stolen property; unlawful export or import of items; etc.

3. THE MISSIONS OF STRATEGIC INTELLIGENCE AND CRIME ANALYSIS

A. The **strategic intelligence mission** is to control criminal behavior by...

1. Identifying and describing changes in the nature, pattern, growth, and distribution of defined intelligence human targets, organizational targets, and/or crime commodities, and

2. Identifying alternate strategies which may be used to control or inhibit complex, organized, or pervasive crime trends and apprehend persons involved in those criminal activities

B. The **crime analysis mission** is to control criminal behavior by...

1. Reducing the opportunity for offenses to occur by identifying crime targets and either:

   a. Removing the target, or

   b. Securing the target

2. Increasing the risk of apprehension for criminal offenders by improving detection and apprehension strategies

C. In both STRATINT and CRIMAN, it is essential that their missions be fulfilled within the following criteria:

1. Timely and contemporary

2. Comprehensive

3. Accurate and methodologically sound

4. Have utility for organizational actions

5. Understandable by the consumers of the information (easily understood and interpreted)

4. STRATEGIC INTELLIGENCE AND CRIME ANALYSIS: A LOOK AT THE SIMILARITIES AND DIFFERENCES

Understanding how STRATINT and CRIMAN are alike and dissimilar is important in order to understand the important role both play in the law enforcement organization. Significantly, it must be recognized that one is not more important than the other—they simply have differing responsibilities. This discussion is an attempt to place STRATINT and CRIMAN in perspective (*See* Figure VIII-1).

A. With respect to the nature of the targets addressed...

1. STRATINT provides *micro-analysis* of crime problems

   a. This means its analysis is directed toward a narrow spectrum of criminal activity

   b. It will concentrate on exclusively defined crime problems based on the specific nature of the crime, commodity, or criminal rather than all services provided by the law enforcement agency

   c. STRATINT tends to be predominantly supportive of the criminal investigation functions of the agency

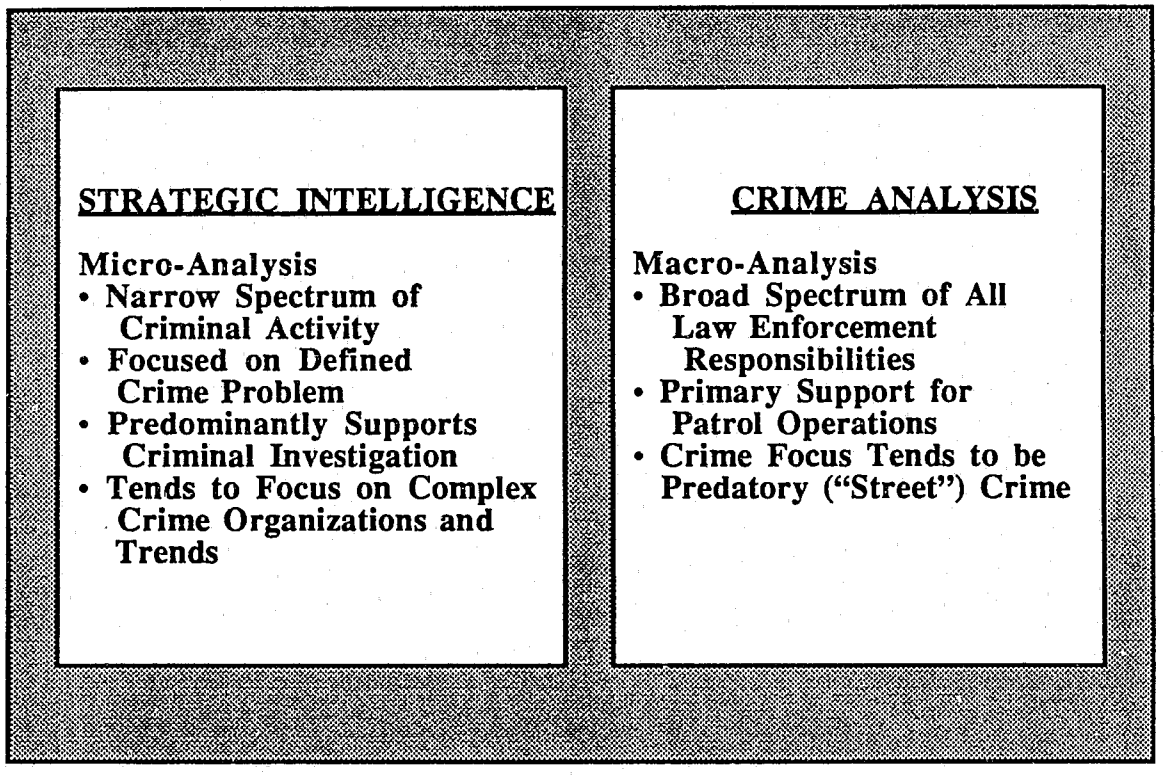
   d. STRATINT tends to focus on organized crime, crime cartels, white collar crime, complex criminal enterprises, and "non-traditional" crime

2. CRIMAN provides *macro-analysis* of crime problems

   a. It is broad-based focusing on all responsibilities of the law enforcement agency

Figure VIII-1

COMPARISON OF STRATEGIC INTELLIGENCE AND CRIME ANALYSIS



b. CRIMAN tends to provide primary support to the patrol function and secondary support to investigations

c. Typically CRIMAN will not focus on crime commodities but on behaviors and associated descriptive variables

d. On matters of criminal acts, CRIMAN tends to focus on general predatory crimes, burglaries, theft, and other "street crimes"

B. In many ways STRATINT is a microcosm of CRIMAN

1. STRATINT is more substantively limited than CRIMAN

2. STRATINT will frequently incorporate greater detail in intelligence reports

3. But STRATINT utilizes virtually the same the infrastructure (e.g., methodologies, variables, aggregate data sources, etc.) as does CRIMAN

C. STRATINT and CRIMAN activities should be cooperative and reciprocal, not competitive

5. METHODOLOGIES USED IN STRATEGIC INTELLIGENCE

As noted previously, both STRATINT and CRIMAN use similar methodologies to perform their functions. However, data sources and variables will obviously differ. Detailed discussion on how to perform the different methodologies is not appropriate at this point. Thus, a brief summary and description of methodologies which can be used in STRATINT will be presented.

A. In all cases, the first methodological issue is to determine what information is wanted in a STRATINT project

1. In cases of regularly submitted reports or summaries, this facet will be established

2. In special case reports—such as exploration of a new crime target or identification of emerging crime trends—the end result may not be as apparent

3. The desired information must be clearly articulated in order that the best method of developing that output may be employed

    a. Administrators may sometimes simply say "I want to know about..." with no further delineation

    b. Sometimes not enough is known about an issue to ask specific questions

    c. In such cases, the STRATINT analyst must investigate the issue, crimes, commodities, targets for a broad understanding and then develop desired identifiable output

4. Once it is determined what information is wanted in a STRATINT report, then the methodology is selected

B. In selecting the methodology the analyst must examine:

1. The variables which will yield the information desired, either...

    a. Individually

    b. Collectively (in the aggregate)

    c. Interactively

2. The ability to access the variables and measure them

3. The reliability of the variables

4. The validity of the variable information obtained

C. Regarding variables:

1. *Defined*:

A *variable* is any characteristic on which individuals, groups, items, or incidents differ.

2. Variables which may be examined in STRATINT and (CRIMAN) include, but are not limited to:

   a. Geography

   b. Time

   c. Types of crimes

   d. Demographic characteristics of persons

   e. Means of transporting persons and/or commodities

   f. Different types of crime commodities

   g. Law enforcement strategies

   h. Quantities of commodities and/or money

3. While these are common variables, the analyst must examine the nature of the intelligence target and the desired output in order to identify the specific (and sometime unique) variables which may be assessed to collect the desired information

D. With the desired output and the variables identified a methodology must be selected to accomplish the analytic task

1. The methodology is a set of scientifically-based procedures which are used to:

   a. Collect information from the variables;

   b. Control the information collection for validity and reliability;

   c. Analyze the information to describe the subject/target;

   d. Analyze the information to make inferences about the subject/target;

   e. Direct the interpretations of the analysis; and

   f. Report the information

2. Some methodologies are *quantitative* while others are *qualitative*

   a. The essential difference is that:

      1) *Quantitative* methods collect and analyze information which can be "counted" or placed on a scale of measurement which can be statistically analyzed

      2) *Qualitative* methods collect and analyze information which are described in narrative or rhetorical form and conclusions drawn based on the cumulative interpreted meaning of that information

   b. The nature of the methodology will be dependent on:

      1) The characteristics of the variables, and/or

      2) The method which is chosen to collect the information

3. Methodologies and analytic procedures which can be used in STRATINT include:

   a. Operations research (queuing theory, decision theory, modeling, simulation, gaming theory)

   b. Experimental and quasi-experimental design

   c. Descriptive and inferential statistical analysis (including probability-based projections)

   d. Case studies

   e. Qualitative descriptors based on interviews

   f. Expert analysis (such as the Delphi Technique)

   g. Econometric models

   h. Actuarial models

i. Spatial analysis (location/geography and associated patterns of crimes, persons, commodities)

1) Analysis of absolute locations

2) Analysis of relative locations

3) Analysis of spatial flow

4) Spatial theory

a) Macro-analysis

b) Micro-analysis

c) Mesoanalysis

j. Temporal analysis ("time"; e.g., monthly, weekly, daily, hourly, measures of incidents and changes of the targeted entity)

1) Pattern analysis

a) Time scale analysis

b) Graphical analysis

2) Numerical analysis

a) Direct time series

b) Regression of time series

4. While many methodologies are available, these are among the most useful for STRATINT

a. Many of the methodologies require specialized training in order to perform them properly

b. No methodology is "pure" or "conclusive" because they all require interpretation by the analyst

c. Thus, the best prepared analysts will produce the best output in STRATINT reports

6. STRATEGIC INTELLIGENCE AND THE INTELLIGENCE CYCLE

A. The intelligence cycle is, in itself, a methodology

1. It is designed within the parameters of general systems theory wherein it can continually receive input (collection) and subject the information to all stages of the assessment, analytic, and output processes

2. In case development, such as tactical and operational intelligence (TACTINT and OPINT), the end product of the cycle is based on the on-going accumulation of evaluated information which contributes to the eventual prosecution of a case. As such, constant, and many times changing, information is introduced into the cycle via various collection protocols throughout an investigation

B. STRATINT deals with a *cohort of information* designed via the methodology selected

1. There is typically not on-going input of information during the course of the production of a STRATINT product

2. While follow-up may occur, these are separate STRATINT analysis

C. The methodology of a STRATINT endeavor will follow, conceptually, virtually all the same steps found in the intelligence cycle for TACTINT, however...

1. The methodology will be more controlled

2. The data input more limited, and

3. The output—the strategic intelligence produced from the activity—will be limited to address a strictly defined purpose

D. The last two elements of the intelligence cycle—reporting and dissemination—are worthy of special note

1. The reports of the STRATINT will typically have two target options:

a. One set of reports for administrative decision making, and

b. One set for operational decision making

2. Conversely, TACTINT reports are directed toward the line/operations user and case preparation

   a. Administrative utilization of TACTINT reports are mainly limited to "keeping informed on a case" and, in occasional serious cases, resource allocation

   b. As such, different types of reports are prepared for STRATINT than for TACTINT

3. With respect to dissemination of intelligence information:

   a. TACTINT and OPINT reports are virtually always limited to law enforcement personnel—sometimes strictly limited on a "need to know" basis depending on the sensitivity of the case, target, or subject

   b. Conversely, many times STRATINT reports are openly available for anyone to review

      1) Some STRATINT assessments are specifically undertaken for public consumption, notably for the political decision makers

      2) Whereas some STRATINT will have restricted dissemination, at least for some period of time, far more frequently the information is readily available.

7. TYPES OF STRATEGIC INTELLIGENCE REPORTS

It was noted above that STRATINT reports are created for both administrative and operational purposes. This section will describe a typical model of various report types produced by STRATINT activities. (Similar reporting styles are also used in CRIMAN.)

Generally speaking, the STRATINT reports should have three component parts:

- **Descriptive** - The report describes the issues and processes which are subject to the analysis; the information and data are presented objectively for the user's consumption

- **Interpretative** - The STRATINT analyst takes the raw data and information and interprets it, based on analysis and experience, with respect to the meaning of the information and its impact on the crime issues involved

- **Available Alternatives** - In light of the interpretations, the resources available, jurisdiction of the agency, and capabilities/expertise of the agency, the analyst prescribes alternative actions and strategies for future action

(*See* Figure VIII-2)

A. *ADMINISTRATIVE DECISION MAKING REPORTS*

1. **Cost-Effectiveness Reports** - Includes STRATINT reports which show:

   a. Ratios of cost to activities or intelligence results;

   b. Analysis of various strategies with respect to their cost and "production"; and

   c. Linking available staffing, money, equipment, and facilities to planned TACTINT and OPINT activities

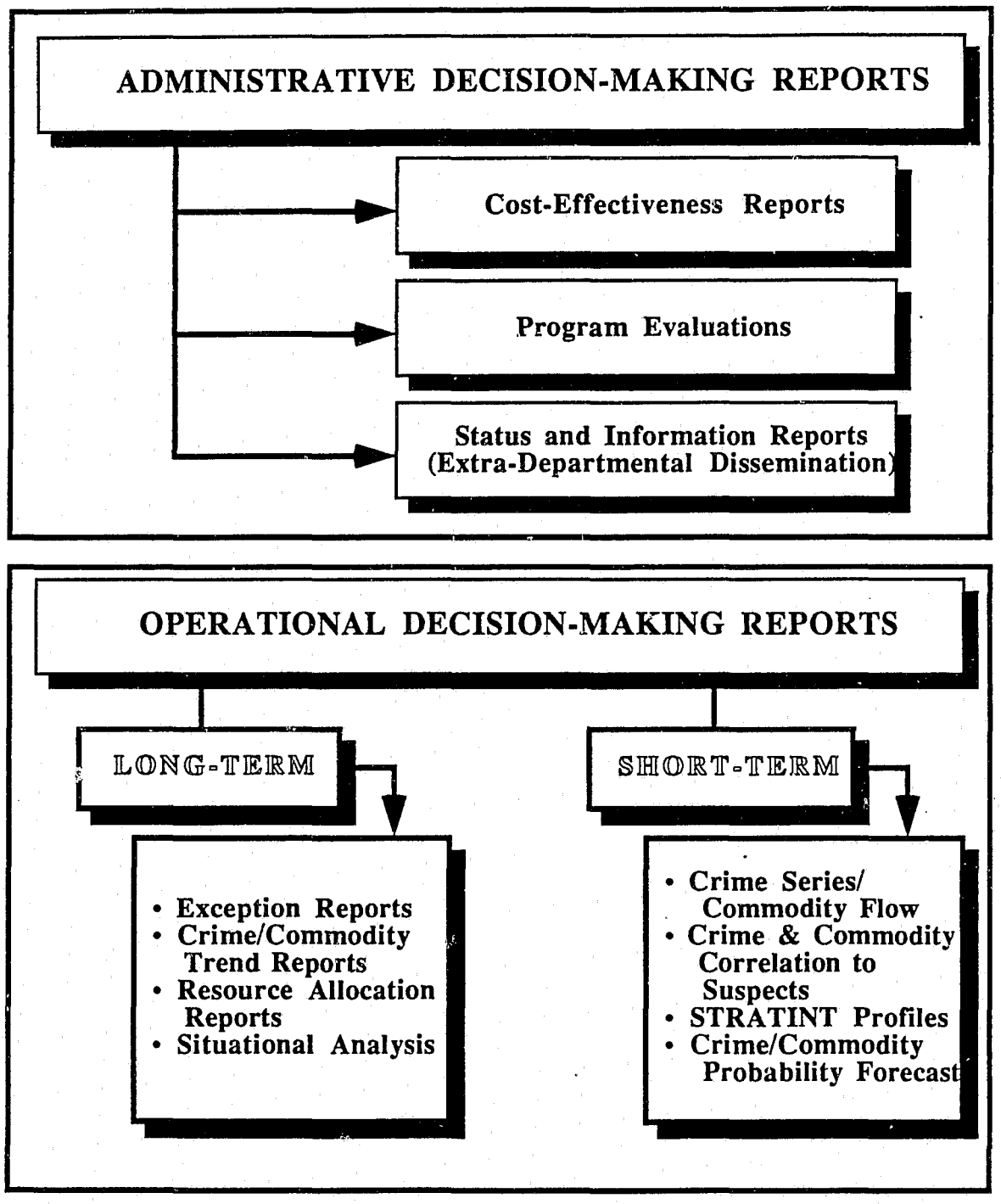
2. **Program Evaluations** - Reports which describe the analysis between TACTINT and associated investigatory activities (i.e., independent variables) on an intelligence target as correlated to outcomes of the planned intelligence activities (i.e., dependent variables)

   a. The nature of the correlations and comparisons is to determine if the strategies being used on an intelligence target are effective

   b. The report will describe the nature of the strengths and weaknesses of the program

Figure VIII-2

TYPES OF STRATEGIC INTELLIGENCE REPORTS



3. **Status and Information Reports for Extra-Departmental Dissemination** - These are reports primarily prepared to inform non-law enforcement government administrators and legislators about crime issues, trends, patterns, and commodities affecting the jurisdiction

   a. The reports can be on a specific crime issue or generally describing the various crimes and criminal enterprises under scrutiny by Law Enforcement Intelligence (LAWINT)

   b. The reports are designed to be informative about:

      1) The nature of the target crime problem(s) in the jurisdiction;

      2) Descriptive of the agency's activities associated with the target crime(s); and

      3) Provide information on what can be expected in the future on the crime(s)

B. *LAW ENFORCEMENT OPERATIONAL AND DECISION MAKING STRATINT REPORTS*

1. Long Term/Profile Reports

   a. *Exception Reports* - These are reports which indicate that an anomaly has occurred in the status of trends or patterns in intelligence targets (crimes or commodities). The report should document:

      1) The nature of the anomaly

      2) Potential impact

      3) Alternative law enforcement and intelligence responses to the anomaly

   b. *Crime/Commodity Trend Forecasts* - These are projections in changes of patterns or amounts of targeted crime(s) and/or commodities over a defined time period.

      NOTE: In order to establish a trend there must always be a baseline of "known" patterns and amounts against

which current and projected information can be compared

c. *Resource Allocation Reports* - This analysis looks at current and projected law enforcement activities and identifies anticipated resource allocation changes, typically staffing changes

1) Note that this is an operational report

2) As such, it is not concerned with the appropriation of resources to an operational unit, but how the resources will be allocated within the operational unit to address defined and targeted activities

d. *Situational Analysis* - This is a broad "big picture" description of a particular crime problem developed to give a "feel" of the magnitude and effects of the crime problem on the jurisdiction and the agency. Such reports are useful for:

1) Prioritizing LAWINT and investigative activities, and

2) As support documentation for...

a) Deciding on law enforcement strategies concerning a specific target, and

b) Resource allocation

2. Short-Term STRATINT Reports

a. *Crime Series/Commodity Flow Pattern Identification* - This report documents the crimes and/or commodity flows which have commonly defined characteristics in an attempt to link them together as being a product of the actions of a single criminal, cartel, or criminal enterprise—when patterns are established then the case investigation can be focused

b. *Crime and Commodity Correlations to Suspects* - Simply stated these reports attempt to make quantitative and/or qualitative correlations or comparisons of criminal incidents and/or unlawful commodities with persons who are suspected to be involved in the criminal acts

c. *STRATINT Profiles* - These analysis produce comprehensive reports on criminal suspects, criminal targets, and unlawful commodities in an attempt for operational units to identify potential involvement of other persons, etc. in the crime series or criminal enterprise

d. *Crime/Commodity Probability Forecasts* - These are short term operational projections of what crimes and/or commodity changes can be expected usually involving a single major case or narrowly grouped, commonly linked criminal cases—used as a means to plan tactical intelligence and investigative activities on the identified cases

8. CAVEATS REGARDING STRATEGIC INTELLIGENCE

Despite sophisticated methodologies and a structured reporting system, STRATINT clearly has limitations for which both administrative and operational personnel must be aware. In this regard, both the analyst and consumer of STRATINT should take heed of the following caveats (*See* Figure VIII-3):

A. The output of the STRATINT function is only as good as:

1. The raw data/information collected

2. The quality of the analysis

B. STRATINT is not conclusive

1. It is probabilistic

2. It is frequently subjective based on the experience of the analyst

C. STRATINT is descriptive, not prescriptive

1. It can tell what is and what may be

2. It can provide alternatives for action

3. It cannot tell what actions to take

D. STRATINT is *program* oriented, not *case* oriented

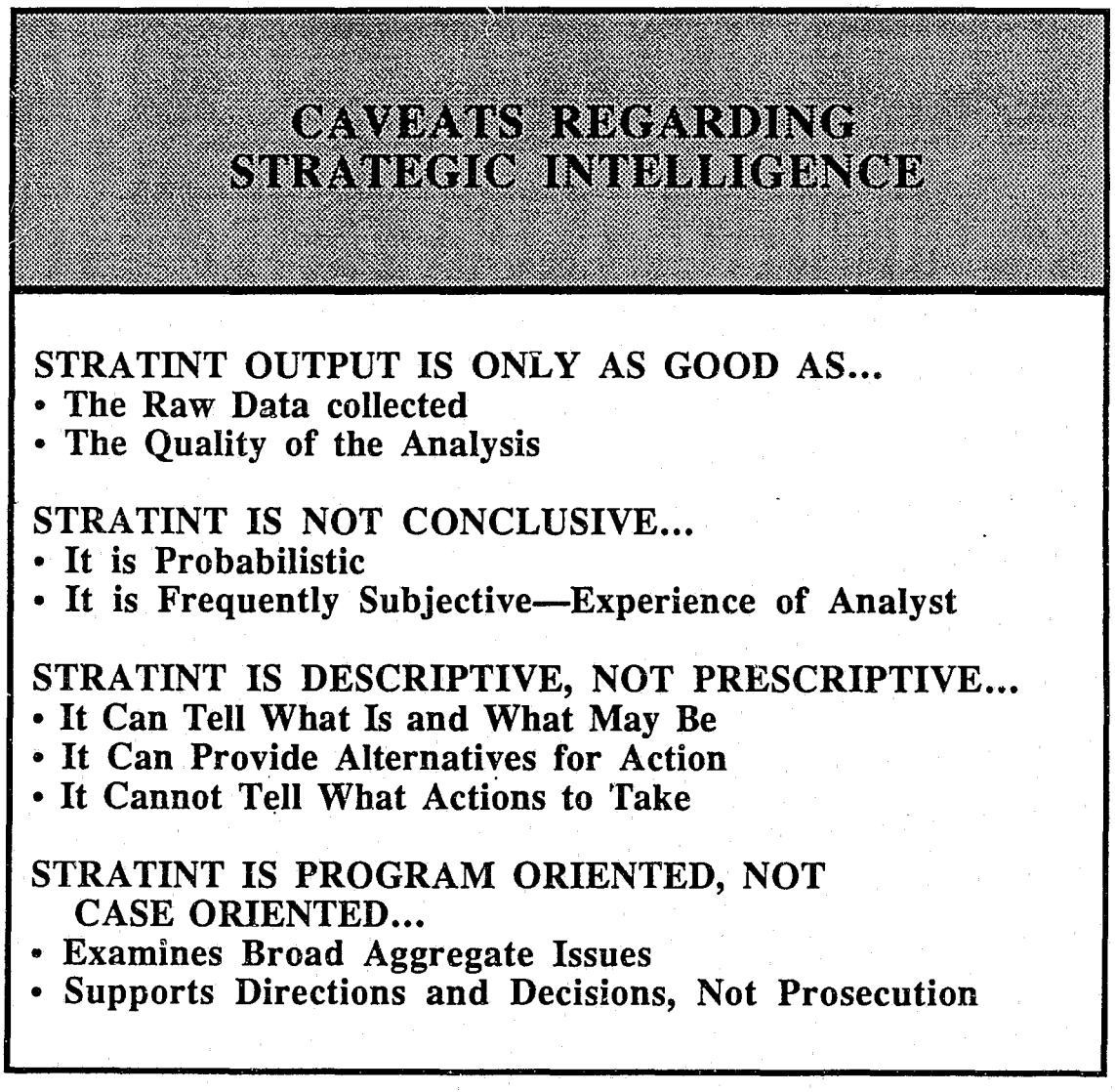
   1. It examines broad, aggregate issues

   2. It supports direction and decisions, not prosecution

E. STRATINT is an activity in support of organizational goals—the output of STRATINT is *not a goal in and of itself*

Figure VIII-3

CAVEATS REGARDING STRATEGIC INTELLIGENCE



8. STRATEGIC INTELLIGENCE

Instructional Support and Criteria

GOAL:

To define the meaning of strategic intelligence and present a framework for the application of strategic intelligence in a law enforcement agency.

OBJECTIVES:

1. The student will be able to distinguish between *crime analysis* and *strategic intelligence* in terms of concept and application.

2. The student be able to define the uses of strategic intelligence for crime targeting, changes in crime trends, and administrative decision-making.

STUDY QUESTIONS:

a. Describe crime analysis and strategic intelligence in your own words showing the inherent similarities and differences between the two.

b. What is the relationship between strategic intelligence and the management functions of *resource allocation* and *personnel deployment*?

c. Distinguish between the mission and roles of *strategic* intelligence and *tactical* intelligence.

d. Strategic intelligence reports should have three components: They should be descriptive, interpretative, and describe available alternatives. Briefly explain what this means. Use an example in your discussion.

NOTES

CHAPTER 9

TARGETING: CRIMES MOST APPROPRIATE FOR INTELLIGENCE ANALYSIS

"If we are to target our efforts effectively where traffickers are most vulnerable, we must know the enemy far better than we do now"
National Drug Control Strategy (1989).

1. WHAT IS MEANT BY "TARGETING" CRIMES FOR LAWINT?

LAWINT is a labor-intensive, on-going activity which requires a long term investment before the fruits of the analysis are achieved. Moreover, tactical intelligence analysis is most useful in *complex crime patterns* and *criminal enterprises.* While some serious crimes (e.g., homicide or sexual assault) are clearly important, the nature of the offenses generally are susceptible to analytic techniques used in LAWINT. Similarly, strategic intelligence as a resource allocation and decision-making tool is most useful in high volume or high density crime incidents. As a result, LAWINT activities should be directed to those crimes wherein the intelligence effort can produce the most meaningful results.

2. TARGETING A CRIME FOR LAWINT

A. Offenses may be targeted based upon:

1. Crime Types

EXAMPLES: Narcotic trafficking, stolen car rings, labor racketeering, or gambling

2. Individual Cases

EXAMPLES: Serial murder, known drug trafficker, known stolen property "fencing" ring

B. *Defined*:

> The identification of crimes, crime trends, and crime patterns which have discernable characteristics that make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

C. Note that LAWINT is used to:

1. Increase **efficiency**

   a. Doing the *job right*

   b. Wise use and expenditure of resources

2. Increase **effectiveness**

   a. Doing the *right job*

   b. Using the techniques and procedures which permit you to accomplish the identified goals and objectives

D. While some crimes are inherently more susceptible to LAWINT activities than others, decisions for LAWINT crime targeting should be based on functional criteria

1. The criteria should be related to:

   a. Crimes particularly pervasive to the jurisdiction

   b. Crimes which can be effectively addressed through LAWINT based on available resources

2. The criteria are not absolute, rather they are on a *continuum* which can be weighted depending on their unique nature and influence

E. Decision criteria include (See Figure IX-1):

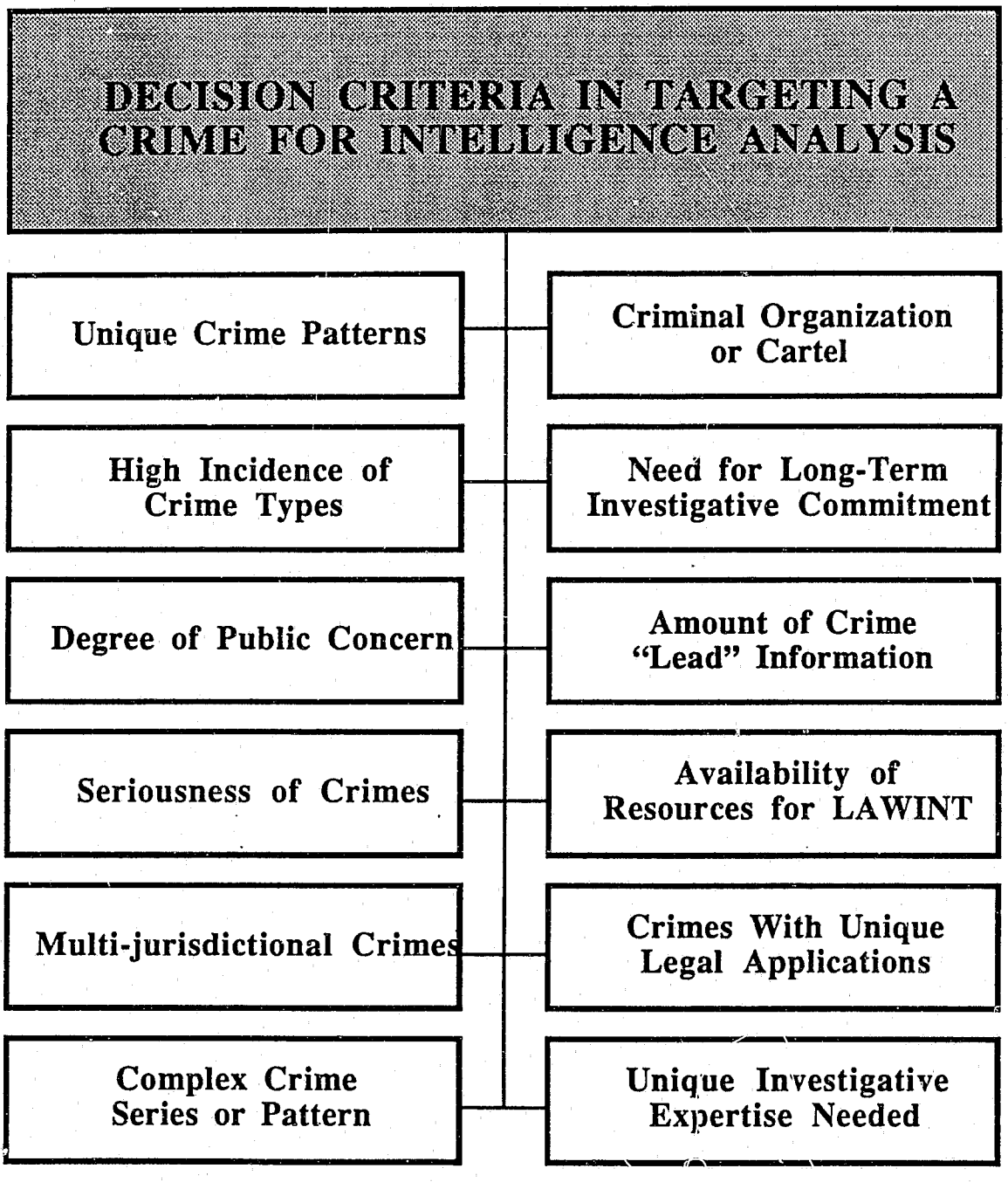
1. Unique crime patterns
2. High incidence of crime types
3. Degree of public concern about defined crimes
4. Seriousness of crime(s)
5. Multi-jurisdictional crime(s)
6. Complex organization of crime series/patterns
7. Involvement in crime by some form of criminal organizational or crime cartel
8. Need for long-term commitment to conduct a productive investigation
9. Amount of "crime lead" information available or reasonably available for development
10. Availability of sufficient resources to effectively perform LAWINT functions
11. Commission of crimes with unique legal applications (e.g., forfeiture, major conspiracy, continuing criminal enterprise/RICO, assets forfeiture, etc.)
12. Unique expertise needed for case development (e.g., financial investigations, computer associated investigations, comprehensive commodity flow analysis, etc.)

F. The *process* for crime targeting should includes several activities:

1. Identify presence of potential LAWINT crime target within the jurisdiction of the agency
2. Prioritize criminal incidents or series with respect to agency and/or public concern

Figure IX-1

DECISION CRITERIA FOR TARGETING



3. Assess resource requirements for LAWINT operations

4. Define goal or extent of LAWINT involvement in the crime target

5. Assign LAWINT analyst or team to target

6. Establish defined time periods for evaluation of LAWINT success toward resolution of the crime target

3. CRIME TYPES MOST SUSCEPTIBLE TO LAWINT

A. It was noted that the "crime type" should not be the exclusive criterion for making a LAWINT case assignment

1. In light of this, it should be noted that certain crime categories are more applicable to LAWINT than others

2. The crime types appear to change with *time* and *social trends...*

a. As such, one function of strategic intelligence (STRATINT) should be to identify and monitor these changes in crime trends

b. Thus, STRATINT can be an important tool in targeting activities

B. Characteristics of crimes which benefit most from LAWINT

1. The crime is of an *on-going nature* either as a continuing criminal enterprise or serial offenses

2. Typically, *multiple parties are involved* in the crime/crime series with similar motivations

3. There is a clearly defined *motivation* for the crimes which can be instrumental in applying analytic techniques

a. Most frequently, an *economic* motivation (e.g., drug trafficking, organized prostitution rings, etc.)

b. While less prevalent, some motivations are of a *political* or *ideological* nature (e.g., right wing extremists, terrorism, etc.)

NOTE: Some crimes may fall in both categories—such as labor racketeering

c. In serial crimes against persons (i.e., serial murder, serial rape) there is typically only one perpetrator with a unique *psychological* motivation

4. Crimes most appropriate for LAWINT will typically have a *strong goal orientation* such as money, power, or a political goal

5. Most such crimes are typically *multi-jurisdictional* making the investigation process more complicated

C. **EXAMPLES** of crime types most commonly appropriate for LAWINT

NOTE: These are only meant as examples—this is not a collectively exhaustive nor definitive list

1. Crime cartels/organizations and criminal enterprises involved in:

   a. Drug trafficking

   b. Prostitution

   c. Gambling

   d. Counterfeit properties (including textiles, watches, toys, etc.)

   e. Stolen vehicles

   f. "Fencing" operations

2. Financial crimes (including organized frauds, money laundering, securities-related offenses)

3. Serial crimes (murder, rape, robbery)

4. Terrorism

5. Civil disorders

6. Bias/hate crimes including White Supremacy groups

7. Gangs

8. Labor unrest and racketeering

9. Threats to public institutions and public officials

4. DECISION MAKING SYSTEM FOR LAWINT CRIME TARGETING

A decision-making system should be established which can be used to help determine if a LAWINT case file should be opened

A. The system should not be the sole determinant of whether a LAWINT case file will be opened, yet it can be a helpful decision-making tool

B. The system should incorporate a series of questions (variables) to be answered:

1. These are predominantly qualitative factors

2. The decision criteria/questions should be designed to focus on:

   a. *Jurisdiction* of the agency

   b. *Verification* of the target crime

   c. *Value/utility of LAWINT* in crime "solvability"

   d. *Effective* and *efficient* use of LAWINT resources

3. It is important to remember that...

   a. The decision-making system is for the *use of* LAWINT operations

   b. The decision process is *not* simply a decision of whether or not the department will investigate such crimes

4. Any decision-making system is dependent on the mission, goals, and charter of the LAWINT unit

5. The purpose of this approach is to focus known information to determine desirability and viability of LAWINT in a case

C. Different criteria will be applicable depending on:

1. The nature of the law enforcement agency

2. Departmental priorities

3. Resource allocations

4. Other LAWINT commitments

D. Each LAWINT unit should develop a decision-making system to meet its own needs.

E. A sample LAWINT crime target decision-making system is illustrated in Figures IX-2 and IX-3 relating to Bias/Hate Crimes (B/HC)

1. The sample system includes:

a. Criteria to focus and evaluate information

b. A flow chart of the decision-making process

2. Bias/Hate Crimes was chosen as an example due to the increasing frequency of B/HC incidents, the emergence and growth of numerous organized White Supremacy and B/HC groups, and the relative inattention given to B/HC by LAWINT and police organizations in general.

Figure IX-2

SAMPLE DECISION-MAKING SYSTEM FOR LAWINT CRIME TARGETING ON BIAS/HATE CRIMES (B/HC)

I. DEFINING A BIAS/HATE CRIME (B/HC)

1. *Definition*: Any criminal act directed toward any person as a result of that person's race, ethnicity, religious affiliation, or sexual preference.

   a. Motive is not necessarily a formal legal element of the crime(s) which was(were) committed.

   b. Motive is the fundamental determinant in the decision of whether the offense was a B/HC.

   c. That is, if the crime was directed toward the victim(s) *because* of racial, ethnic, religious, or lifestyle/sexual preference reason, then it is a B/HC.

2. Examples of B/HC's include:

   a. Burning of a cross or religious symbol

   b. Bomb threats

   c. Destruction of property

   d. Assault

   e. Disorderly conduct

   f. Interrupting or disturbing a religious meeting

   g. Deprivation of civil rights

   h. Disruption of a lawful public demonstration

   i. Harassment, threats, intimidation or retaliation

3. Do the elements of the incident give a preliminary indication that the incident was a B/HC?

   IF YES, DESCRIBE B/HC INDICATORS IN DETAIL.

II. VERIFYING THE CRIME AS A B/HC INCIDENT

1. Were the victim and suspect of different (particularly opposing) Racial, Ethnic, Religious, or Lifestyle (RERL) groups?

2. Did the B/HC incident occur solely because of RERL differences between the persons or was the incident a product of other reasons?

3. Did the B/HC incident coincide with celebrations which traditionally have pranks (e.g., Halloween, school rivalries)?

4. Was the victim the only (or one of a few) RERL group member in the neighborhood?

5. When multiple incidents occur at the same time ...:

   - Are all the victims members of the same RERL group?

   - Is the method of operation and/or ritual the same for each B/HC incident?

6. Has the victim been associated with any recent or past RERL activities such as protests or demonstrations (e.g., NAACP, Gay Awareness, protests against KKK, informational demonstrations concerning Nazi War Criminals)?

   - If such protests or demonstrations occurred, were they reported in the news media?

   - Were public documents concerning such events (e.g., parade permits, licenses, organizational charters) accessed by RERL opposition group members in search of leaders' names, addresses, and affiliations?

7. What was the manner and methods used in the B/HC?

   - Does it reflect a defined ritual?

   - Is the act similar to other documented incidents?

- Are there similarities in idiosyncrasies between the incidents? (Examples: symbols; words, abbreviations, or acronyms; spelling of words; colors of paints; ritualistic trappings).

8. Has the victim had past or repeated attacks of a similar nature?

9. Is there an ongoing neighborhood problem that may have contributed to the problem (e.g., masking an incident for a B/HC when it is really retribution for a disagreement)?

PROVIDE EVIDENCE IN SUPPORT OF THE ANSWERS TO THESE QUESTIONS INDICATING THAT THE INCIDENT WAS A B/HC.

III. JURISDICTION OF THE B/HC CRIMINAL INCIDENT

1. What was the specific criminal offense (or offenses)?

2. Does the law enforcement agency have jurisdiction to investigate the offense and take enforcement action?

IF NO, WAS A REFERRAL MADE TO AN AGENCY WITH JURISDICTION? DESCRIBE AGENCY AND REFERRAL.

3. Is there another agency which has superseding jurisdiction to investigate the offense?

IF YES, ...

- DESCRIBE THE AGENCY;
- COMMUNICATIONS WITH THAT AGENCY CONCERNING THE B/HC INCIDENTS;
- STATUS OF THIS B/HC INCIDENT; AND
- PLANNED FOLLOW-UP PROCEDURES BY THIS AGENCY

4. Did the offense transcend boundaries into other geographic jurisdictions?

IF YES, DESCRIBE...

- THE OTHER JURISDICTIONS
- NATURE OF CONTACT WITH OTHER JURISDICTIONS
- PLAN OF OTHER JURISDICTIONS CONCERNING THIS B/HC
- ROLE OF THIS AGENCY IN THE B/HC INCIDENT
- PROCEDURE AND SCHEDULE FOR CASE STATUS REVIEW

IV. EVIDENTIARY FOUNDATION

1. How much evidence currently exists in support of identification and/or prosecution of the perpetrator(s)?
2. What is the probability for developing useful intelligence information related to the crime?
3. What evidence exists to show motive toward a B/HC incident?
4. Is there evidence of another motive?

DESCRIBE...

- EVIDENCE COLLECTED
- DISPOSITION OF PHYSICAL AND FORENSIC EVIDENCE
- CLEARLY SHOW LINK BETWEEN EVIDENCE AND B/HC MOTIVE

V. CHANCE OF SYSTEMIC OR SERIES OCCURRENCE

1. Have there been previously reported B/HC incidents in the jurisdiction?

CITE INCIDENTS, CASE NUMBERS, CASE STATUS

2. Is there evidence of previously committed B/HC in the jurisdiction which were unreported?

DESCRIBE ...

- THE SUSPECTED INCIDENTS
- EVIDENCE
- HOW THE EVIDENCE CAME TO THE AGENCY'S ATTENTION
- ANY ACTION TAKEN ON THE INFORMATION

3. Does the reported B/HC appear to be a sporadic occurrence or part of a series in the present jurisdiction and/or in other jurisdictions within the region?

   DESCRIBE ...

   - OTHER INCIDENTS
   - SIMILARITIES BETWEEN INCIDENTS

   PROVIDE CASE NUMBERS

4. Is there evidence of a relationship to a defined organization based upon

   + The nature of the criminal incident

   + The criminal suspects

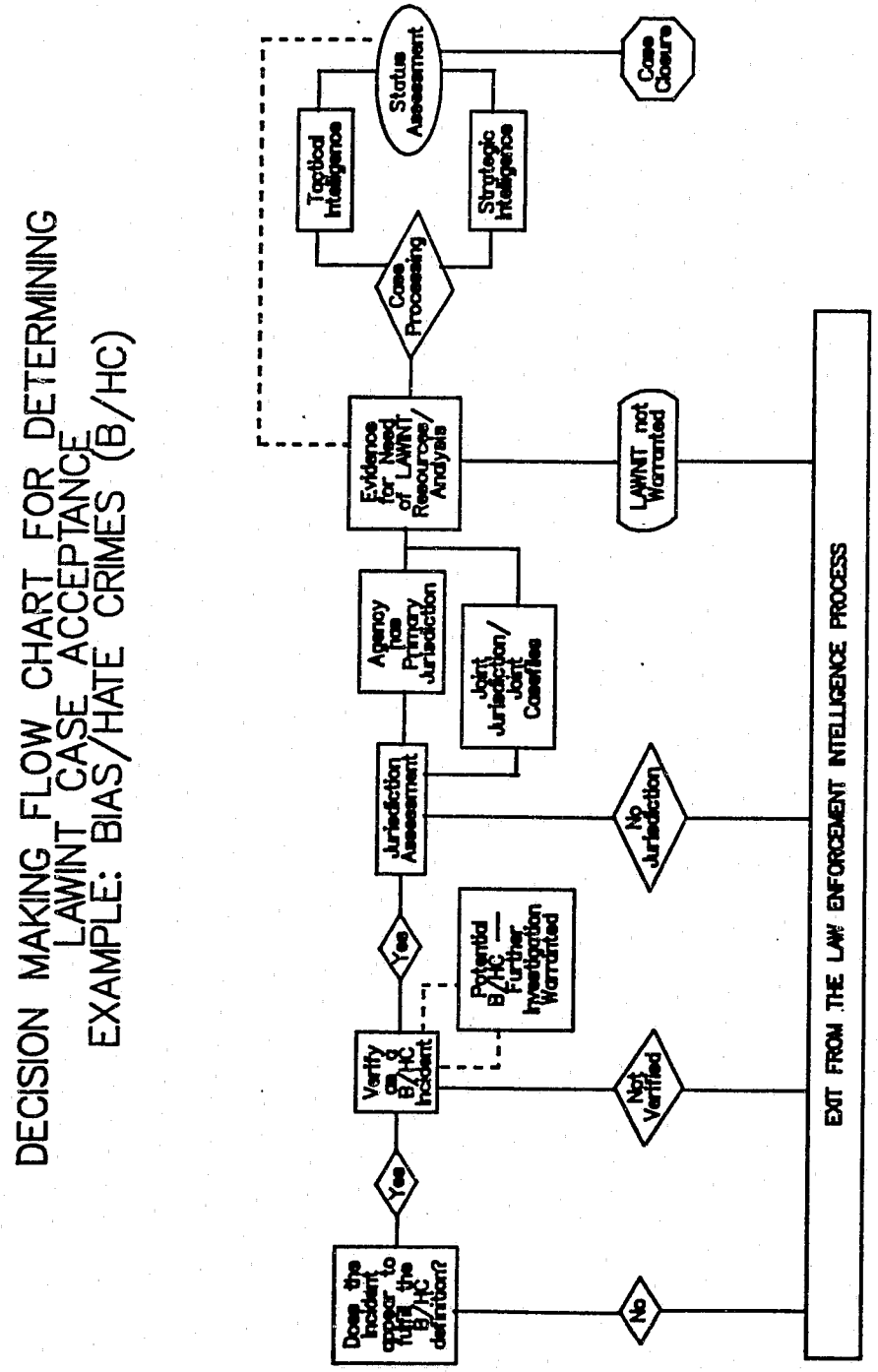
   DESCRIBE ...

   - THE SUSPECTED ORGANIZATIONS
   - THE RELATIONAL EVIDENCE

   PROVIDE A LINK ANALYSIS SHOWING CONFIRMED AND SUSPECTED RELATIONSHIPS

Figure IX-3

FLOW CHART ILLUSTRATING A SAMPLE DECISION-MAKING SYSTEM FOR LAWINT CRIME TARGETING ON BIAS/HATE CRIMES (B/HC)



9. TARGETING CRIMES FOR INTELLIGENCE ANALYSIS

Instructional Support and Criteria

GOAL:

> To present an overview of the "crime targeting" concept and illustration of a crime targeting model which can be used as a basis for developing target decision criteria for other jurisdictions.

OBJECTIVES:

1. Students will gain an understanding of the "targeting" concept as it applies to LAWINT.
2. Students will learn how to develop and apply a model for targeting crimes as a LAWINT case.

STUDY QUESTIONS:

a. What is meant by "targeting" in LAWINT? What is the *role* of targeting in LAWINT?

b. What types of criteria are used to target a crime for LAWINT? What is the rationale for using these criteria?

c. Why are some crimes more appropriate for LAWINT than others?

d. Select a crime (other than Bias/Hate Crimes) and develop a decision-making system to target that crime for LAWINT (in a manner similar to the model in Figure IX-2).

NOTES

CHAPTER 10

RESOURCES TO ASSIST IN SELECTED INTELLIGENCE ACTIVITIES

"Never forget: When your weapons are dull, your ardor dampened, your strength exhausted, and your treasure spent, other chieftains will spring up to take advantage of your extremity."
Sun Tzu Chinese Philosopher and Warrior, Circa 510 B.C.

1. UTILIZING EXTRA-DEPARTMENTAL RESOURCES IN SUPPORT OF THE LAWINT FUNCTION

Intelligence analysis is a process which cannot be effectively accomplished without interaction with other agencies. Other extra-departmental assistance is discussed elsewhere in this monograph with respect to Intelligence Mutual Aid Pacts (IMAPs), access to public records, and use of various information and statistical systems. Beyond these, however, there are some unique resources and techniques which can be of value to the intelligence analyst. These are:

- Criminal profiling
- VICAP - The FBI's Violent Criminal Apprehension Program
- INTERPOL - the International Criminal Police Organization
- EPIC - the El Paso Intelligence Center
- Intelligence Networks

The discussions in this chapter are meant to serve as a *guide* for these resources rather than serving as a prescriptive document.

There are a wide range of publications which address each of these resources in detail. The reader is referred to the bibliography for a list of those resources. In the case of the RISS projects discussed at the later part of the chapter, telephone numbers and addresses are provided for more information.

2. THE CONCEPT AND USES OF CRIMINAL PROFILING

A. Criminal Profiling—*Defined*:

> An investigative technique by which to identify and define the major personality and behavioral characteristics of the [criminal] offender based upon an analysis of the crime(s) he or she has committed (Douglas and Burgess, 1986:9)

B. *Purpose of Profiles*: To obtain a psychological and behavioral description (or image)—a personality composite—of the offender which may assist in:

1. Identifying the offender
2. Locating the offender
3. Developing a motive or reason for behavior to assist in prosecution

C. *When Profiles Can Be Used*: When the behavior of the offender as evidenced in the crime scene and not the offense, per se, provides sufficient clues to develop a profile

D. *Characteristics of the Profiling Process*:

1. The profile applies to crimes which are unique, distinct from similar crimes, and have defined evidence of the offender
2. The identification and interpretation of evidentiary items indicative of the personality type committing the crime
3. The description of salient psychological and behavioral characteristics of the offender
4. Psychodynamic portrayal of the offender based on "trait clusters" (determined from the crime scene evidence) which distinguishes the offender from the general population

E. *Most Common Profile Applications*:

1. Homicides and serial murders

2. Violent and/or serial rapes
3. Arsons
4. Hostage negotiation
5. Terroristic threats (verbal or written)

F. *Steps in the Profiling Process*:

1. Evaluation of the criminal act itself
2. Comprehensive evaluation of the specific characteristics of the crime scene(s)
3. Comprehensive analysis of the victim
4. Evaluation of preliminary police reports
5. In cases of death, evaluation of the medical examiner's autopsy protocol
6. Development of a profile with defined critical offender characteristics
7. Development of investigative suggestions predicated on the construction of the profile

G. Factors Frequently Included in a Psychological Profile:

1. Age
2. Sex
3. Race
4. Marital status/adjustment
5. Intelligence
6. Scholastic achievement/ adjustment

7. Lifestyle
8. Rearing environment
9. Social adjustment
10. Personality style/ characteristics
11. Demeanor
12. Appearance and grooming
13. Emotional adjustment
14. Evidence of mental discompensation
15. Pathological behavioral characteristics
16. Employment/occupational history and adjustment
17. Work habits
18. Residency in relation to crime scene
19. Socioeconomic status
20. Sexual adjustment
21. Type of sexual perversion or disturbance (if applicable)
22. Prior criminal arrest history
23. Motive

H. *Automated Crime Profiling*:

1. Process of using computer artificial intelligence to develop profiles of criminals
2. Artificial intelligence is a computer program which can make decisions

3. Benefits of computer artificial intelligence and profiling:

   a. Profiles may be more accurate because decisions are based on a very wide range of information in the data base

   b. Profile is developed much faster

   c. It is an efficient process

   d. Time factor may permit an agency to create more profiles for a wider range of crimes than if done manually

   e. Eliminate subjectivity and preconceptions which may exist if done by a person

   f. Increases consistency in profiling

   g. Can keep on-going records and statistics much easier and more accurately

I. *Applications of Profiling to Intelligence*:

1. Profiling provides another tool in the analytic stage of the intelligence cycle

2. When performing analysis and making hypotheses, to have a profile of the perpetrator(s) could be important for:

   a. Identifying certain types of evidence to pursue

   b. Making decisions about case factors

   c. Giving leads for investigating possible associates of the criminal

   d. Focusing in on unknown persons involved in some criminal enterprise

   e. Providing insight for undercover work

   f. Providing insight for conducting surveillances

   g. Giving leads to project future crime patterns of the suspect(s)

h. Understanding and identifying suspect(s) writings more readily through psycholinguistics

i. Contribute to the prevention of future crimes

3. VICAP—THE VIOLENT CRIMINAL APPREHENSION PROGRAM

A. *What is VICAP*?

> A nationwide data information center operated by the FBI's National Center for the Analysis of Violent Crime, designed to collect, collate, and analyze specific crimes of violence

B. *The Goal of VICAP*: Provide all law enforcement agencies reporting similar pattern violent crimes with the information necessary to initiate a coordinated multi-agency investigation which will lead to the expeditious identification and apprehension of the crimes' offender(s)

C. *Case Criteria for Acceptance into the VICAP System*:

1. Solved or unsolved homicides or attempts, especially ...

   a. Those that involve an abduction;

   b. Are apparently random, motiveless, or sexually oriented; or

   c. Are known or suspected to be part of a series

2. Missing persons where the circumstances indicate a strong possibility of foul play and the victim is still missing

3. Unidentified dead bodies where the manner of death is known or suspected to be a homicide

D. *Important Factor to Note*: VICAP's purpose is *not* to investigate cases, but *analyze* them for comparability to other crime patterns throughout the country and providing information on that comparability to the local and state law enforcement jurisdictions involved in the case

E. *Crime Factors Analyzed by VICAP For Case Comparability*:

1. Modus Operandi (MO)
2. Victimology
3. Physical evidence
4. Suspect description
5. Suspect behavior before, during, and after the crime—**NOTE THAT**:
   a. This behavior is known as the "ritual" and is different from the MO
   b. The behavioral characteristics are similar to those assessed in profiling

F. *How VICAP Works*:

1. Determine if case at issue fits VICAP criteria
2. If so, complete VICAP form
3. Submit form to the FBI's NCAVC
4. The data from the form is entered into the VICAP system (which is both an information and statistical data base)
5. All data remains confidential and consistent with the Privacy Act
6. An analysis is done on the case in comparison with the characteristics of other cases in the data base
7. When cases are linked ...
   a. The FBI notifies investigators of agencies where links are made
   b. FBI provides information on analysis (nature of similarities, etc.)
   c. Respective agencies responsible for further follow-up

G. *Application of VICAP to Intelligence Analysis*:

1. It can help to determine if a case is a random occurrence or part of a series

2. If possibly part of a serial, the system provides further investigatory and analytic leads

3. Help correlate missing persons, particularly important if person(s) is(are) associated with organized crime or crime cartel

4. With these new leads, more information can be used in hypotheses development and testing

4. THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION—INTERPOL

A. INTERPOL—*Defined*:

> INTERPOL is a world wide association of national police forces established for mutual assistance in the detection and deterrence of international crimes

B. Headquarters in Ste. Cloud, France (Headquarters is called the "General Secretariat")

C. *The purposes of INTERPOL are*:

1. Serve as an international clearinghouse of information on wanted persons, notably those whom there is reason to believe have traveled internationally

2. Serve as an international clearinghouse of information on stolen property believed to have been transported internationally

3. Serve as a resource, based on the intelligence analysis of each country's headquarters, to examine crime trends or criminal paths of an international nature

4. Serve as a liaison between U.S. law enforcement officials and their counterparts in other countries for purposes of conducting international criminal investigations

D. *Myths about INTERPOL:*

1. There are *no* INTERPOL investigators or agents

2. INTERPOL has no authority for arrest, search, seizure, or investigation—these police powers are vested in the officers of the host countries according to their laws

3. INTERPOL is not based on any international treaty nor part of any other international organization such as the United Nations or NATO

4. INTERPOL is not a government organization—it is a voluntary private organization funded and staffed by government employees

5. INTERPOL's focus is exclusively on **international crime** and does not involve itself in national security issues or political issues

E. *U.S. organization of INTERPOL*

1. Located in Washington and called the **U.S. National Central Bureau** (USNCB)

2. Operating authority is under the constitution and by-laws of the INTERPOL General Assembly

   a. General Assembly consists of one voting member from each member country

   b. Must also operate within the confines of U.S. law

3. Funding for the General Secretariat in France is from member country dues [U.S. pays roughly 5%]

4. Funding and staffing for the USNCB is from two sources:

   a. Part of an Executive Branch budget line item to pay for some staff and all office operations

   b. Salary of agency representatives paid by their respective agencies

5. USNCB Chief alternates between a Justice Department agency and Treasury Department agency—USNCB is a line item in the department of the NCB Chief

6. U.S. agencies participating in INTERPOL:

   - Bureau of Alcohol, Tobacco, and Firearms (BATF)
   - Criminal Division of the Justice Department
   - Customs Service (USCS)
   - Department of Agriculture—Inspector General (USDA—IG)
   - Drug Enforcement Administration (DEA)
   - Federal Bureau of Investigation (FBI)
   - Federal Law Enforcement Training Center (FLETC)
   - Immigration and Naturalization Service (INS)
   - Internal Revenue Service (IRS)
   - Office of the Comptroller
   - Postal Inspection
   - Secret Service

F. *Making an INTERPOL inquiry*:

1. INTERPOL-USNCB requests can be handled via mail, phone, NLETS, facsimile, photofax, telex, in person

2. Inquiries must:

   a. Be from a U.S. law enforcement agency at the municipal, county, state, or federal levels of government—no private organizations

   b. Be made directly to the USNCB

   c. All responses are subject to the **Third Agency Rule** (Information cannot be given to a third party without the prior approval of the agency furnishing the information).

3. Unlike NCIC and many other U.S. computerized crime and criminal information systems, INTERPOL's data files cannot be directly accessed by an agency—requests must be handled by INTERPOL-USNCB staff member

   a. All requests first go to the *Quality Control Unit*

b. If the request meets all quality control criteria, it will be acted on and requesting officer or agency notified

c. Quality Control Unit ensures that requests are consistent with U.S. Law, USNCB regulations, and the INTERPOL constitution and regulations

4. *INTERPOL-USNCB quality control criteria*

a. The request must come from a legitimate domestic law enforcement agency or an INTERPOL member country

b. All requests must be to or from an INTERPOL member country, or a federal, state, or local law enforcement agency

c. The request must involve an international investigation

d. The crime, if it had occurred within the United States, must be considered a violation of U.S. federal or state law, as well as a crime in the country involved

e. The request cannot violate the accepted interpretation of Article 3 of the INTERPOL Constitution which prohibits involvement in matters of a religious, military, political, or racial nature

f. There must be a *link* between the crime and the subject of the case. The person or property must be suspected of specific criminal involvement

g. The reason for the request must be clearly stated, indicating the type of investigation, and the fullest possible identifying details of the subject. If this information is not stated, the requestor is contacted for additional information, including the type of offenses, dates, charges, arrests, convictions, etc.

h. There is no charge for INTERPOL inquiries

5. THE EL PASO INTELLIGENCE CENTER—EPIC

A. Primary purpose is to collect, process, and disseminate information concerning illicit drug trafficking—all tactical intelligence

B. While EPIC's focus is on drug enforcement, it has also intelligence information on crimes traditionally related to drugs, including:

1. Continuing criminal enterprises
2. Organized crime
3. Narco-terrorism
4. Auto theft (particularly along the U.S./Mexico border)
5. Smuggling of guns and contraband other than drugs
6. Smuggling of aliens
7. Other crimes which may arise

C. EPIC is administered by the Drug Enforcement Administration, but has personnel assigned from a total of nine federal agencies:

- Bureau of Alcohol, Tobacco and Firearms (BATF)
- Coast Guard
- Customs Service (USCS)
- Drug Enforcement Administration (DEA)
- Federal Aviation Administration (FAA)
- Federal Bureau of Investigation (FBI)
- Immigration and Naturalization Service (INS)
- Internal Revenue Service (IRS)
- Marshals' Service

D. Besides these participating federal agencies, EPIC has reciprocal agreements with the state police in all states

E. EPIC is comprised of two sections:

1. *Watch Operations* - responsible for handling information requests on a 24-hour basis
2. *Analysis Section* - provides a full range of research, analytical, and data retrieval services on:

   a. Air intelligence

b. Maritime intelligence

c. General intelligence

d. Analysis section also provides:

1) Finished intelligence reports

2) Special operations reports:

a) Organizational profiles on violator organizations and networks

b) Developing law enforcement problems

3) Pre-operational interdiction planning, and

4) Post-operational summation and evaluation

F. Points to remember about EPIC:

1. It is an **intelligence clearinghouse**, not a communications center

2. Information requests are bound by Privacy Act restrictions

3. Information from EPIC can only be distributed to:

a. EPIC affiliate agencies, or

b. Non-affiliated law enforcement agencies with the approval of the nearest EPIC affiliate agency

6. INTELLIGENCE NETWORKS

A. The RISS Projects—Regional Information Sharing System

1. The RISS projects were first funded in the late 1970s—since 1980 support funding has continued through the Department of Justice

2. RISS projects consist of seven regionally grouped states from which state and local law enforcement agencies can become members via:

   a. Contributory payments

   b. Participation in access and input to intelligence data bases

   c. Participation in defining priorities

   d. Participation in administrative direction

3. RISS projects provide, for member agencies, various services such as:

   a. Intelligence data base and communications

   b. Tactical analysis

   c. Strategic analysis

   d. Investigative support

   e. Limited equipment support

   f. Monthly bulletins

4. Each RISS project, while abiding by certain foundation rules, is allowed individuality to target crimes and services to meet regional needs

5. The RISS projects and their crime targets are: (*See* Figure X-1)

   a. **MAGLOCLEN - Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network**

      1) STATES: Michigan, Indiana, Ohio, New York, New Jersey, Pennsylvania, Delaware, Maryland, District of Columbia; Also Canadian provinces of Quebec and Ontario

Figure X-1

REGIONAL INFORMATION SHARING SYSTEM: PROJECTS AND LOCALES

THE SEVEN REGIONAL INFORMATION SHARING PROJECTS

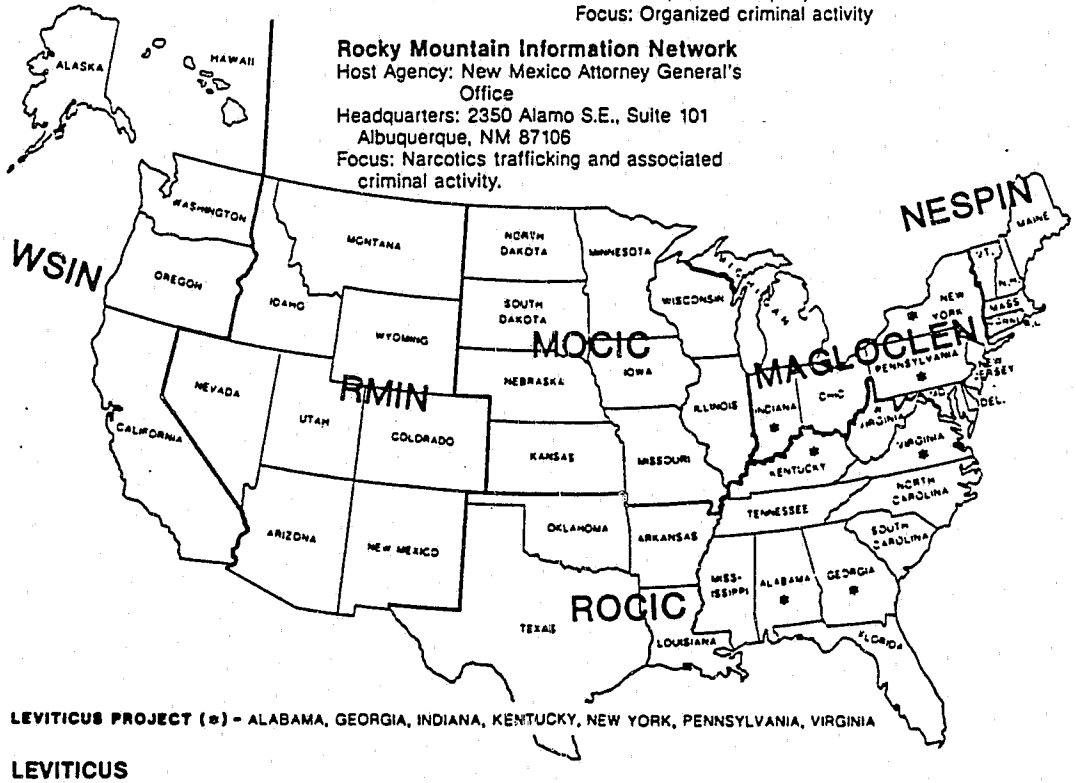
Mid-State Organized Crime Information Center
Host Agency: Missouri Attorney General's Office
Headquarters: No. 2 Corporate Centre Suite 310, Springfield, MO 65804 (417) 883-4383
Focus: Professional traveling criminals, organized crime, and narcotics trafficking

Western States Information Network
Host Agency: California Department of Justice
Headquarters: 1825 Bell St., Suite 205 Sacramento, CA 95825 (916) 924-2606
Focus: Narcotics offenders and offenses

New England State Police Information Network
Host Agency: Massachusetts Department of Public Safety
Headquarters: P. O. Box 786, Randolph, MA 02368 (617) 986-6544
Focus: Organized crime and narcotics trafficking

Middle Atlantic Great Lakes Organized Crime Law Enforcement Network
Host Agency: Pennsylvania Crime Commission
Headquarters: 40 Lloyd Avenue, Suite 206 Malvern, PA 19355 (215) 644-1607
Focus: Organized criminal activity

Rocky Mountain Information Network
Host Agency: New Mexico Attorney General's Office
Headquarters: 2350 Alamo S.E., Suite 101 Albuquerque, NM 87106
Focus: Narcotics trafficking and associated criminal activity.



LEVITICUS PROJECT (*) - ALABAMA, GEORGIA, INDIANA, KENTUCKY, NEW YORK, PENNSYLVANIA, VIRGINIA

LEVITICUS
Host Agency: Virginia Department of Criminal Justice Services
Headquarters: The LEVITICUS Project 6767 Forest Hill Avenue, Suite 318 Richmond, VA 23225 (800) 221-4424
Focus: Coal related crimes and major fraud

Regional Organized Crime Information Center
Host Agency: City of Nashville
Headquarters: Two International Plaza, Suite 901, Nashville, TN 37217 (617) 366-1197
Focus: Professional traveling criminals organized crime, and narcotics violators

2) CRIMES: Outlaw motorcycle gangs, narcotics, pornography, white collar crime, toxic waste disposal, Columbian cocaine cartels, non-traditional organized crime, La Cosa Nostra groups, labor racketeering

b. WSIN - Western States Information Network

1) STATES: California, Washington, Oregon, Alaska, Hawaii

2) CRIMES: Narcotic related cases only

c. NESPIN - New England State Police Information Network

1) STATES: Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut

2) CRIMES: Responds to any crime assistance inquiries from member agencies

d. RMIN - Rocky Mountain Information Network

1) STATES: New Mexico, Utah, Nevada, Arizona, Colorado, Wyoming, Montana, Idaho

2) CRIMES: Narcotics smuggling

e. ROCIC - Regional Organized Crime Information Center

1) STATES: Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, West Virginia

2) CRIMES: Travelling criminals and serial criminals

f. MOCIC - Mid-States Organized Crime Information Center

1) STATES: Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, Wisconsin

2) CRIMES: Major criminal conspiracies which have the probability of crossing state lines

g. **LEVITICUS** - A Special RISS project involving states from various other RISS groups to address crimes of common interest

1) STATES: New York, Pennsylvania, Indiana, Kentucky, Virginia, Alabama, Georgia

2) CRIMES: Coal, oil, natural gas related crimes; major fraud

B. Other intelligence networks include:

1. **Law Enforcement Intelligence Unit** - Represents 275 law enforcement agencies for the coordinated exchange of criminal information between law enforcement agencies in the U.S., Canada, and Australia

a. CRIMES: Bombing, bribery, burglary, extortion, kidnapping, labor racketeering, loansharking, gambling, major fraud, murder, narcotics, pornography, prostitution, receiving stolen property, and other organized crime activity

b. CONTACT: Law Enforcement Intelligence Unit, DOJ/BOCCI, Central Coordinating Agency, PO Box 13357, Sacramento, CA 95813

2. **Australian Bureau of Criminal Intelligence (ABCI)** - formed in 1981 by agreement of all Australian governments and the Northern Territory Government, the ABCI is the center for criminal intelligence collection, analysis, and dissemination for all Australian police forces.

a. CRIMES: Drug trafficking, illicit gambling, fraudulent securities and companies, money laundering, public corruption, loansharking, and all organized crime activity

b. CONTACT: The Executive Officer, Australian Bureau of Criminal Intelligence, GPO Box 1936, Canberra, Australia - ACT 2601

3. **South Pacific Islands Criminal Intelligence Network (SPICIN)** - Seventeen Pacific Rim nations met in America Samoa in 1987 signing agreements to cooperate and share criminal intelligence information.

   a. CRIMES: Drug trafficking, mobile criminals, major crimes of South Pacific interest.

   b. CONTACT: Executive Director, SPICIN, Pago Pago, American Samoa, 96799, FAX 684-633-2679

10. RESOURCES TO ASSIST IN SELECTED INTELLIGENCE ACTIVITIES

Instructional Support and Criteria

GOAL:

> To identify resources and organizations outside of a law enforcement agency which may be useful in information gathering and intelligence analysis.

OBJECTIVES:

1. The student will be able to identify techniques from outside resources useful in support of intelligence activities..
2. The student be able to define various external organizations to assist in intelligence activities and distinguish the types of crimes and assistance available from those various agencies.

STUDY QUESTIONS:

a. Using an illustration of a crime, explain how *criminal profiling* could be a useful tool for the intelligence analyst.

b. Some local law enforcement agencies have been reluctant to use VICAP? Why do you feel this has occurred? Discuss fully.

c. Using your home or jurisdiction as a point of reference, explain a crime or incident wherein INTERPOL may be a useful resource. In your answer, include a discussion of the steps you would have to go through to submit an INTERPOL inquiry.

d. Some criticism has been raised about the RISS projects questioning their effectiveness. Generally discuss the RISS concept and its advantages and disadvantages.

NOTES

CHAPTER 11

COMPUTERIZED INFORMATION AND STATISTICAL SYSTEMS

"Computers will either be our salvation or death—as for me, I can't even figure out how to turn the damn things on".
Statement of a veteran police Sergeant to the Author.

1. COMPUTERIZATION IN LAW ENFORCEMENT

Just as in every other facet of our society, computerization has entered into law enforcement as an important tool to support the management and delivery of police services. The evolution of computer technology has placed computer terminals in police cars and led to computer systems which contain not only information but also images.

While many remarkable advancements in computerized law enforcement have been made, two *caveats* are warranted:

- We have under-utilized the potential of computers
- We have become too reliant on current computer applications

A. Under-Utilization

1. There has been insufficient exploration in the applications of artificial intelligence/expert systems for law enforcement

   EXCEPTIONS:
   - FBI'S Arson Profiling Project
   - Baltimore County, Maryland Computerization Research

2. Use of sophisticated, high volume statistics for projections in strategic intelligence

3. Fully integrating computer information capabilities with:

   a. Intra-departmental communications

b. Inter-jurisdictional communications

B. **Over-Reliance**

1. Using computers as a sole source for conducting background checks of persons

2. Relying only on "canned computer printouts" for strategic intelligence and crime analysis

2. CLASSIFICATION OF COMPUTER SYSTEMS

For both operational reasons and factors related to the Privacy Act requirements, it is important to recognize:

- The *types* of computer systems that exist, and
- The inherent *differences* between these systems

A. **Information Systems** - *Defined*:

> An organized means of collecting, processing, storing, and retrieving information on *individual entities* for purposes of record and reference.

1. **EXAMPLES**: person, vehicle, property

2. Important to recognize that the information is descriptive of the individual person or entity

B. **Statistical System** - *Defined*:

> An organized means of collecting, processing, and storing, and retrieving *aggregate* information for purposes of analysis, research, and reference. No individual records are stored in a statistical system.

1. This is collective information—one cannot get access to anything about an individual entity from a statistical system

2. Particularly used for analytical purposes

C. It is important to understand the differences between these systems because of:

1. *Legal Implications*

a. Information system data has notable legal limitations for access and dissemination

b. Statistical system data has virtually no legal limitations but there may be policy or administrative limitations

2. *Intelligence Use of the System's Data*

a. Information system data mostly used for tactical intelligence

b. Statistical system data mostly used for strategic intelligence

3. *Security of the System*

3. ISSUES AND FACTORS IN COMPUTER SECURITY

A. LAWINT relies increasingly in computer systems to assist in the storage, retrieval, processing, and analysis of types of critical information.

1. The benefits of automation are apparent, however, a constant problem of security remains

2. Intelligence managers and analysts alike must be familiar with the different security issues in order to protect information—for both case integrity and citizens' rights—from improper access or dissemination

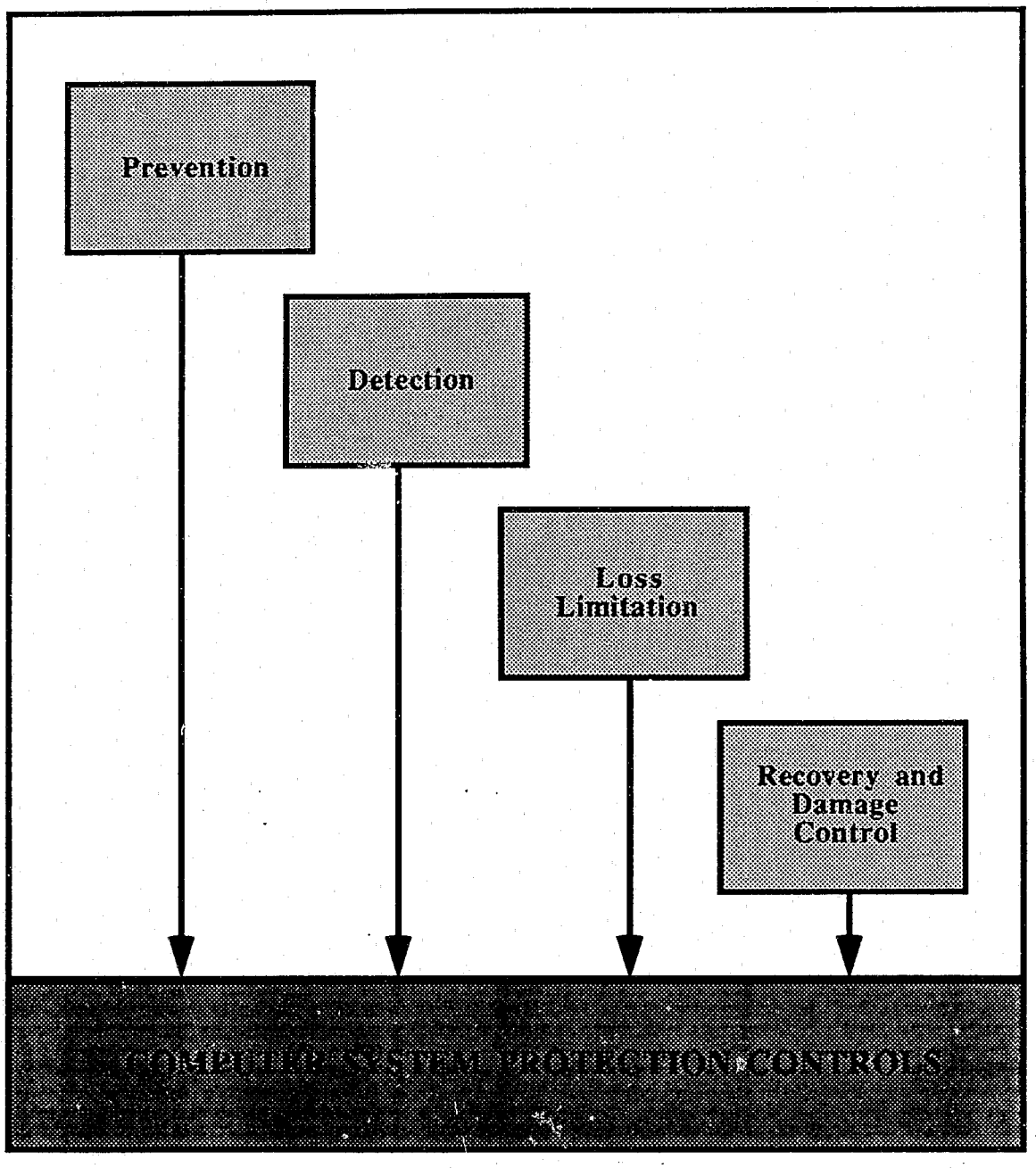
B. Overall, computer security controls must address four levels of protection (*See* Figure XI-1):

1. **Prevention** - Restricting access to information and technology to authorized personnel who perform only authorized functions

2. **Detection** - Providing for early discovery of improper access and abuses if prevention mechanisms are circumvented

Figure XI-1

PROTECTION CONTROLS FOR COMPUTER SYSTEMS



3. **Limitation** - Restricting losses if access occurs despite prevention and detection controls

4. **Recovery and Damage Control** - Provides for efficient information recovery and minimizes the effect of compromised data/information through the use of contingency plans

C. All computer systems (and manual information systems) should have plans and procedures to address these issues with intelligence personnel cognizant of their role

D. In order to effectively address the computer security issues, several points need to be addressed (*See* Figure XI-2):

1. ***Manual Assurance of Data Handling***

a. All data and information in a computer system must, in some way, be handled *manually* in preparation for computerization

b. Similarly, there is manual handling of much of the information which has completed computer processing—as such, computer security must address:

1) Quality control and security of data that is *input* must be maintained—inaccurate or altered input will taint the entire system

2) Quality control and security of system *output*—control who receives system output so data cannot be abused—includes control of access to output

2. ***Physical Security***

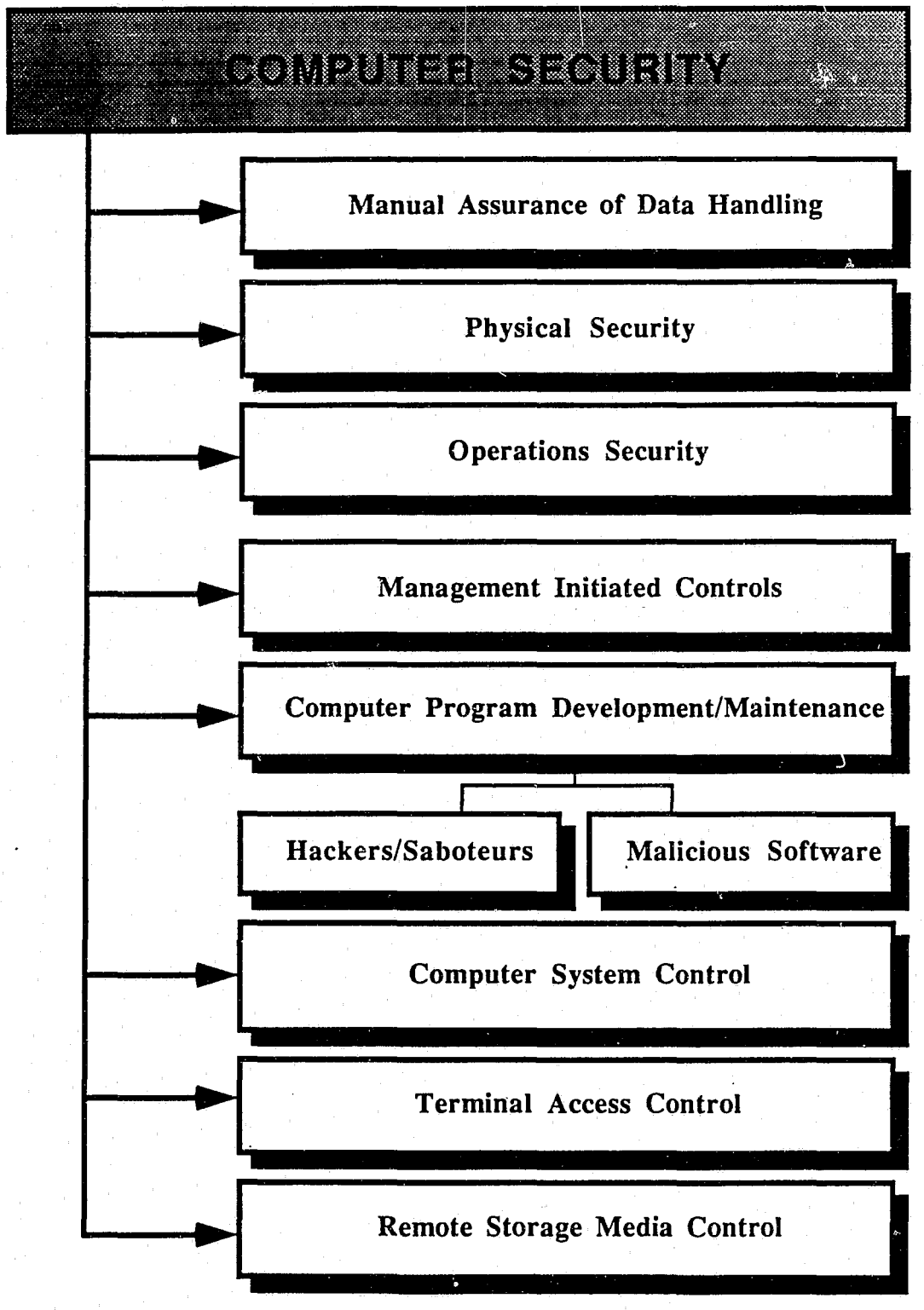
a. Tampering or penetration of hardware and facilities related to computer processing can have both a direct and an indirect impact on the computer output

b. There must be effective measures in place to ensure the security of...

1) The building housing the computer(s),

Figure XI-2

COMPUTER SECURITY ISSUES



2) Remote terminals, and

3) Any other computer hardware and peripheral equipment or facilities

3. ***Operations Security***

a. Even during the course of computer processing, there is the potential for data to be destroyed or altered, either intentionally or by accident

b. As a result, there are several security concerns which must be addressed:

1) *Quality control of personnel* operating mainframe computer

2) *Quality control of jobs production* including isolation of production, to minimize data exposure to unauthorized persons, modification, destruction, and/or unauthorized use

4. ***Management Initiated Controls*** - Includes:

a. Management oversight of computer operations,

b. Administrative policy for computer use,

c. Establishment of a data security management committee,

d. Establishing or contracting for a computer systems auditor,

e. Establishing data classification schemes for control and access, and

f. Establishing a computer security officer

5. ***Computer Program Development and Maintenance***

a. Each computer program—whether commercial or contracted—should be developed with not only an operations/production plan but also a *security plan*;

b. Computer software has become the target of:

1) "***Hackers***" who generally attempt to gain unauthorized access to a computer system for the "challenge";

a) Their *intent* is usually "harmless" causing minor disruptions or nuisances

b) Their *effect* can be more harmful

- Data loss
- Access to restricted/confidential information
- Theft of service
- Loss of resources via reparations to the security breach

2) ***Saboteurs*** whose intent is to...

a) Disrupt or destroy computer operating programs;

b) Consume computer memory to disrupt storage capabilities; or

c) Destroy the contents of the computer memory

c. The actions of Hackers and Saboteurs may be to:

1) Steal ("down load" or copy) information

2) Destroy information

3) Disrupt a processing cycle

4) Alter information

5) Damage or incapacitate hardware through the alteration of programming instructions

6) Slow down processing operations by introducing "bugs" into the software

d. These purposes may be accomplished by:

1) Direct or "on-line" manipulation of programming instructions; or

2) Introduction of a self-contained, interactive piece of malicious software into the operating system or application program

e. The use of ***malicious software*** has increased significantly in recent years and has been directed at virtually all computer types ranging from personal microcomputers to highly secure mainframe computers (*See* Wack and Carnahan, 1989)

1) *Defined*:

> Self-contained yet interactive computer programs which, when introduced into a computer, can cause loss of memory, loss of data, or cause erroneous instructions to be given in a computer program.

2) *Types of Malicious Software*

a) **Trojan Horse**—A computer program, command or procedure which appears to be useful but contains a hidden code that, when invoked, performs some unwanted procedure; the program is *written with the intent* to be disruptive.

EXAMPLE: A microcomputer calculator program which appears to be convenient on which to perform simple calculations. Yet its hidden function, when invoked, may be to delete files.

b) **Computer Virus** - Programs which were written to perform a desired function but have had a hidden code introduced into the command sequence which, when triggered, performs an unwanted or destructive function; it "infects" the computer by spreading through its memory and/or operating system and can "infect" other computers if introduced through shared data media.

EXAMPLE: A word processing program which has a virus that is started when a given date is record or certain amount of memory is used. The triggered virus may consume memory, alter commands, or execute any other type of disruptive function.

c) **Worms** - These programs use computer network connections to spread from system to system, thus worms attack system that are linked via communications lines spreading viruses or Trojan Horses via inter-connected media.

3) In sum, malicious software can be introduced into computers via:

a) Shared software (notably in the case of microcomputers)

b) Access gained to a computer network

c) Physical access to a given computer

f. The threat from malicious software can be reduced by:

1) Developing contingency plans to deal with potential malicious software incidents

2) Maintain regular back-up files of both operating software/application programs and data files

3) Teach users how to protect computer systems and detect evidence of tampering or unusual computer activity

4) Ensure that technically-oriented security and management staff are in place or available through contract to deal with security incidents

5) Maximize the the security options available on current hardware and software

6) Purchase and use software tools to aid in auditing computing activity and detecting the presence of tampering or damage

6. ***Computer System Control***

   a. The general operating system of a computer directs and monitors all activity within the system

   b. Operating system should have:

      1) Access and execution controls

      2) Automatic computer generated reports which records

         a) All operating system activity,

         b) All sub-program access, and

         c) Attempted access to the operating system and sub-programs

7. ***Computer System Terminal Access Controls***

   a. Hardware access to a computer via both remote on-line terminals and modem/telephone access are widely available

   b. As a result, control and auditing of any computer system access protocol must be established, in terms of:

      1) Multiple security steps for "log on"

      2) Generation of internal system reports to monitor:

         a) Transaction privileges,

         b) Output display restrictions,

         c) Output ordered and generated

         d) Terminal identifiers,

         e) Log-in and password protocols, and

         f) Data file access controls

8. ***Floppy Disks, Data Tapes, and Other Remote Storage Media***

   a. Procedures for controls on access need to be established for persons obtaining computer media;

   b. Chain of custody logs maintained on procedures and controls concerning removal of computer media with sensitive information from a secure area with records of:

      1) Name,

      2) Authorization information,

      3) Date, and

      4) Time

4. "COMPUTERS AS INFORMERS"—SPECIAL OBSERVATIONS

This caption was taken from an article by Marx and Reichman (1985) addressing the wide range of applications computers are being used for in todays society. Income tax records, credit bureaus, police offense reports, criminal histories, property tax records, motor vehicle records, drivers' license files and vital statistics are but illustrations of the array of information available with merely the touching of a few keys on a computer terminal.

In support of these concerns, Figure XI-3 presents "Eight Commandments of Data Management" recommended for government entities.

A. How computerized information is used...

1. **Matching**—Comparing people, places, events, property, and behavior to identify similarities on any given criteria

2. **Sorting**—Distinguishing between variables and classifying any defined variables, or combination into specifically identified groups

Figure XI-3

THE EIGHT COMMANDMENTS OF DATA MANAGEMENT†

1. Information is a valuable government asset; it should be managed to benefit the people.
2. The public should have access to government information, unless such access would jeopardize the privacy of any individual.
3. Information belongs to the government as a whole; agencies are only its keepers and should share it widely among themselves.
4. The information technology employed by a government should encourage all branches of the government to communicate freely with one another.
5. Agencies should collect only the information they need, and managers should seek to minimize the burden on those who must provide it.
6. Governments should develop—and adhere to—a clearly stated design of how they intend to handle information.
7. Because most information is time-sensitive, governments should consider how old their data is in deciding what to do with it.
8. Standards serve a purpose. Governments should strive to get the best technology quickly and economically.

†**Source:** "Governing Guide: Managing Information." *Governing*. February (1990), p. 28A.

3. **Developing profiles**—Assessing a wide range of information about persons, places, or things to develop an "average" or composite picture based on parameters one wishes to describe

4. **Describing**—Identifying any given variable or descriptor and quantifying that variable in light of a large population

5. **Verifying**—Accessing information to determine the validity of a statement, claim, status or behavior

B. Because of discussions elsewhere in this monograph (Chapters 3, 14, and 15), suffice it to note at this point that:

1. These use of computerized files can be helpful to law enforcement to both increase efficiency and effectiveness, however,

2. They can also be easily abused—controls must also be instituted to ensure they are not

5. DESCRIPTIONS OF TYPES OF COMPUTER SYSTEMS USED IN LAW ENFORCEMENT INTELLIGENCE

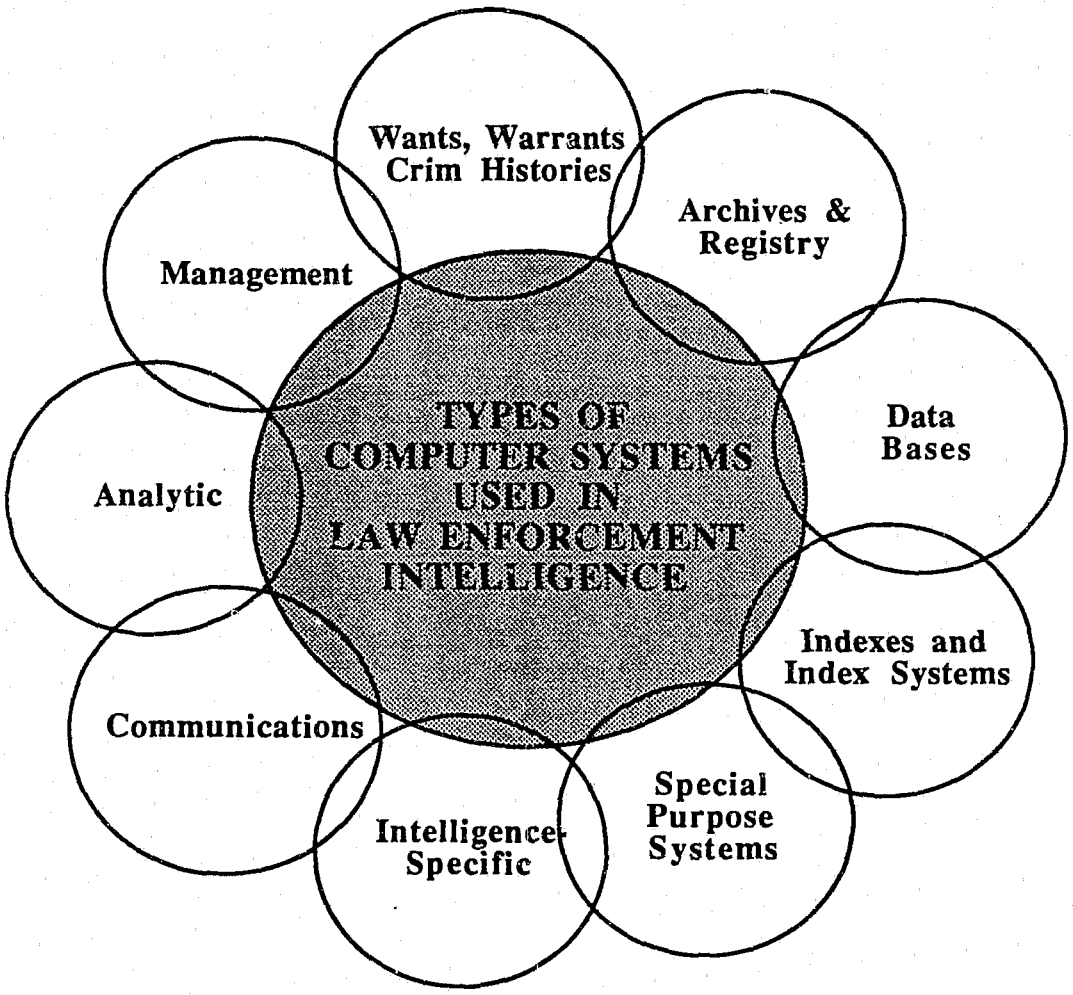
There are a wide range of information and statistical systems which are available to law enforcement agencies in support of the management and operation of LAWINT. This section provides a categorization of the different system types with illustrations of currently available programs. The examples are not meant to be comprehensive or all-inclusive, but simply illustrative of each system category.

Figure XI-4 illustrates the different types of systems noting that the systems should be view *interactively*. That is, while they are structurally independent, the nature of a comprehensive intelligence system is interactive. Thus, the systems should be viewed as mutually supporting different functions within the intelligence cycle.

If the systems are viewed as independent automated intelligence entities, their value is significantly reduced (as discussed in earlier chapters differentiating "information' from "intelligence",.

Figure XI-4

INTELLIGENCE-RELATED COMPUTER SYSTEMS



A. **Management Systems** - broad based systems used in all phases of police management including planning, budgeting, personnel, resource allocation, etc.

EXAMPLES:

- IBM's LEMRAS (Law Enforcement Manpower Resource Allocation System)
- AT&T's "CLUES"
- Command Data System's LEADER (Law Enforcement Automated Data Entry and Retrieval System)
- C.R.I.M.E.A.I.D. (Commercial)

2. **Communications Systems** - Computer assisted/driven systems for inter-law enforcement agency communications of official data and information

EXAMPLES:

- NLETS (National Law Enforcement Telecommunications System)
- LEIN (Law Enforcement Information Network)
- TECS (Treasury Enforcement Communications System)
- INTEL (Intelligence Communications System operated by the U.S. Treasury Department)

3. **Analytic Systems** - used for a wide array of analytic purposes, predominantly statistical system data, in police administration and intelligence

EXAMPLES:

- Criterion Incorporated's "LandTrak" (crime analysis system)
- Command Data System's CAM (Crime Analysis Module)

- TELAN (Telephone Analysis Program; Treasury Department)

- SPSS (Statistical Package for the Social Sciences)

4. **Intelligence-Specific Systems** - computer systems designed specifically to support the functions of law enforcement intelligence

   EXAMPLES:

   - EXODUS - Treasury Department System with company oriented information regarding the export of high technology items; particular emphasis on items going to Soviet bloc countries

   - CACTIS - Customs Automated Cargo Transaction and Intelligence System

   - PATHFINDER - Storage, retrieval, and correlation system for drugs, illegal aliens, and weapons smuggling (DEA)

   - OCIS - Organized Crime Information System (FBI access only)

   - NOMAD - Narcotics and Organized Crime Management and Analytical Data Base (New Jersey Department of Law and Public Safety)

5. **Wants, Warrants, and Criminal Histories** - on-line systems for inquiry to determine if persons or property are wanted; typically these systems will also have a direct interface with criminal histories ("rap sheets") on a person's arrest and conviction record

   EXAMPLES:

   - NCIC/CCH - National Crime Information Center/Computerized Criminal Histories

   - MULES - Missouri Uniform Law Enforcement System

   - VVPS - Vessel Violation Profile System

   - ASIS - Anti-Smuggling Information System (Justice, INS)

6. **Archives and Registry Information** - contains registration information on vehicles, aircraft, marine, and any other registered or licensed person or entity

   EXAMPLES:

   - PAIRS - Private Aircraft Reporting System
   - IMDAL - Immigrant Visa Document Control
   - DACS - Deportation Casework System (Justice, INS)
   - States' motor vehicle registration files
   - States' marine registration files

7. **Data Bases** - contain raw data or information on a specifically defined phenomenon or entity

   EXAMPLES:

   - TDB - Terrorist Data Base (Treasury)
   - UCR - Uniform Crime Report (FBI)
   - NCS - National Crime Survey (Bureau of Justice Statistics and Census Bureau)
   - CLEAR - Customs Law Enforcement Activity Reporting

8. **Indexes and Indexing Systems** - systems which facilitate the indexing of intelligence and investigative information and/or those systems which serve as an index to lead an investigator or analyst to a specific system to obtain defined information

   EXAMPLES:

   - KWIC - Key Word In Context (Commercial)
   - MIRAC - Master Index Remote Access (INS system related to aliens)

- NADDIS - Narcotics and Dangerous Drugs Information System; contains DEA identified subjects and investigative reporting information

9. **Special Purpose Systems** - these are computer systems, either informational or statistical, which have been devised to operate (or "drive") a specific function or activity

EXAMPLES:

- AFIS - Automated Fingerprint Identification System (various commercial systems available)

- Command Data System's MCI (Managing Criminal Investigations)

11. COMPUTERIZED INFORMATION AND STATISTICAL SYSTEMS

Instructional Support and Criteria

GOAL:

> To familiarize the student with a wide range of issues related to the use of computers in tactical and strategic law enforcement intelligence.

OBJECTIVES:

1. The student will have a general understanding of a wide range of computerized data systems which may be used in the performance of the intelligence function.
2. The student will have a working knowledge of computer-related issues and concerns for LAWINT including applications, security, and viruses.
3. The student will be able to distinguish between information and statistical systems, their roles in LAWINT, their applications, general differences in legal standards for each type of system, and have a working knowledge of examples of the various system types.

STUDY QUESTIONS:

a. In your own words, describe the difference between an *information* and *statistical* system.

b. To say that law enforcement has both under-utilized and over-relied on computers seems to be inconsistent. How could these opposing factors occur?

c. We have experienced a large number of breaches in computer security in this country affecting both government and industry. Given the complexity of these systems and our security concerns, why would you speculate that so many security breaches have occurred?

d. In your own words, distinguish between a Trojan Horse, Computer Virus, and Network Worm.

f. What do you feel about the concept of "Computers as Informers"? How do you personally feel about having large amounts of information on **you** being stored in computer systems?

NOTES

CHAPTER 12
TECHNOLOGICAL ISSUES AND DEVELOPMENTS

"I wonder where he gets those wonderful toys?!"
"The Joker" in the movie Batman (1989).

1. TECHNOLOGY IN LAW ENFORCEMENT INTELLIGENCE

As noted in previous chapters' presentations, LAWINT relies on growing computer technology in the analysis of information. In addition to computerized information and statistical systems, there are numerous technological applications which are useful in the collection and pursuit of intelligence cases. Along with these applications are a wide range of issues which must be addressed by both those using and those managing the technologies. In this regard, the issues may be categorized as:

- Security of technologies
- Proper utilization of technologies
  - Training and supervision for proper use
  - Issues of privacy
- Types of technology available
- Observations on technological use

"Technologies" for this chapter refer to any electronic instrument or device used for communications, data collection, data transmittal, data storage, or data analysis.

NOTE: It should be remembered that all aspects of technological development utilized in law enforcement intelligence are focused on information: Its *collection*, *analysis*, and *communication*.

2. SECURITY OF TECHNOLOGIES

A. Refer also to the security issues of computers presented in Chapter 11 on Information Systems.

B. Vulnerability of technologies (Office of Technology Assessment (OTA, 1987:23)

1. Today's public communication network is, for the most part, at least as easy to exploit as at any time in the history of telecommunications.

   a. The design of the public switched network is such that some parts of it are vulnerable to relatively easy exploitation (e.g., wiretaps on copper cable, over the air interception),

   b. Others (e.g., fiber optic cable) present greater inherent barriers to exploitation

2. There are, and will likely remain, opportunities for casual, generally "untargeted" eavesdropping of communications.

   a. However, *targeted* and *consistently successful* unauthorized access requires greater resources.

   b. For systems with sophisticated safeguards, the resource requirements may frustrate even the efforts of national security intelligence agencies.

   c. Adversaries with sufficient resources can eventually defeat all barriers except, perhaps, those based on high-quality encryption.

3. Users of communications face a spectrum of vulnerabilities ranging from those which can be exploited by unsophisticated, low-budget adversaries to those that can be exploited by only adversaries with exceptionally high resources and technological expertise.

4. Technological advances may increase the capabilities of adversaries to misuse computer and communications systems

   a. These same advances can also be used to enhance security

b. Proactive steps must be taken, however, to plan for and apply the security measures

5. Increases in computing power and decentralization of functions have increased exposure to some threats. Two types are important...

   a. Abuse by intruders who are not authorized to use or access the system (*See* Chapter 11)

   b. Misuse by authorized users (which frequently poses the greatest problem)

C. It should be emphasized that with the growing emphasis on integrated data, voice, and facsimile communications systems and greater reliance on communications systems to electronically transfer information, rather than via physical delivery, the security vulnerabilities of communications systems becomes even more critical.

D. Security safeguards and practices for technology developments and communications (OTA, 1987:51)

1. Technological safeguards for communications (and computer) systems are still evolving, as are users' understanding of their needs for them. Products and systems are available for controlling access, auditing use, and encrypting data.

   a. For LAWINT, data encryption is not required for daily, operations communications or data transference

   b. Encryption should be reasonably used on "sensitive" and speculative information in the intelligence process

   c. LAWINT encryption does not mean that a cryptographic code is necessary, rather electronic encryption (i.e.,"signal scrambling") will typically suffice when access to the data and decryption systems are controlled

2. Technical safeguards alone cannot protect information systems completely. Effective information security requires an integrated set of safeguard technologies, management policies, and administrative procedures.

3. Information security hinges on the security of each segment of the increasingly intertwined computer and communications network.

4. A number of important techniques are emerging to verify the identities of the senders of messages, authenticate their accuracy, and ensure confidentiality.

E. Evidence exists as a result of investigations of high resource criminal enterprises (notably drug trafficking) that crime cartels are utilizing their own technologies for communications and intruding on law enforcement investigations.

NOTE: Investment in technological security becomes even more critical in light of these developments

3. PROPER UTILIZATION OF TECHNOLOGIES

A. Training and supervision

1. All new technologies introduced require that personnel be trained in its proper and lawful use

   a. Improperly using technology will diminish its validity and reliability

   b. Depending on the nature of the technology, regular in-service training may also be required

2. Supervision is also required to ensure proper use and accountability of use and products of technological applications—supervision includes:

   a. Visual observation of performance

   b. On-going instruction

   c. Report review

   d. Procedural auditing/accounting

   e. Activity review

B. Issues of privacy

1. The U.S. Congress, Office of Technology Assessment identified five principles necessary to ensure the privacy rights of citizens (1986:102-103) (*See* Figure XII-1)

   a. *There must be no personal data system whose very existence is secret.*

      1) This does not mean that access to the contents of the system is universally guaranteed, rather, the presence of the system itself shall not be secret

      2) Poses an ethical problem for an intelligence analyst's personal "system" which may be on a microcomputer but is not an "official" system of the organization

         NOTE: Essentially a "working" system, like working documents or notes are not considered a formal "personal data system"

      3) Also has complications for merged systems which, together, develop "new" information on profiles, matches, etc.

         a) The question to be addressed is whether the generation of new knowledge from two independent systems constitutes a new system if that new knowledge is stored in a an accessible computer file

         b) This is as much an ethical question as a legal one—intelligence professionals should interpret their own systems in light of the spirit of the principle

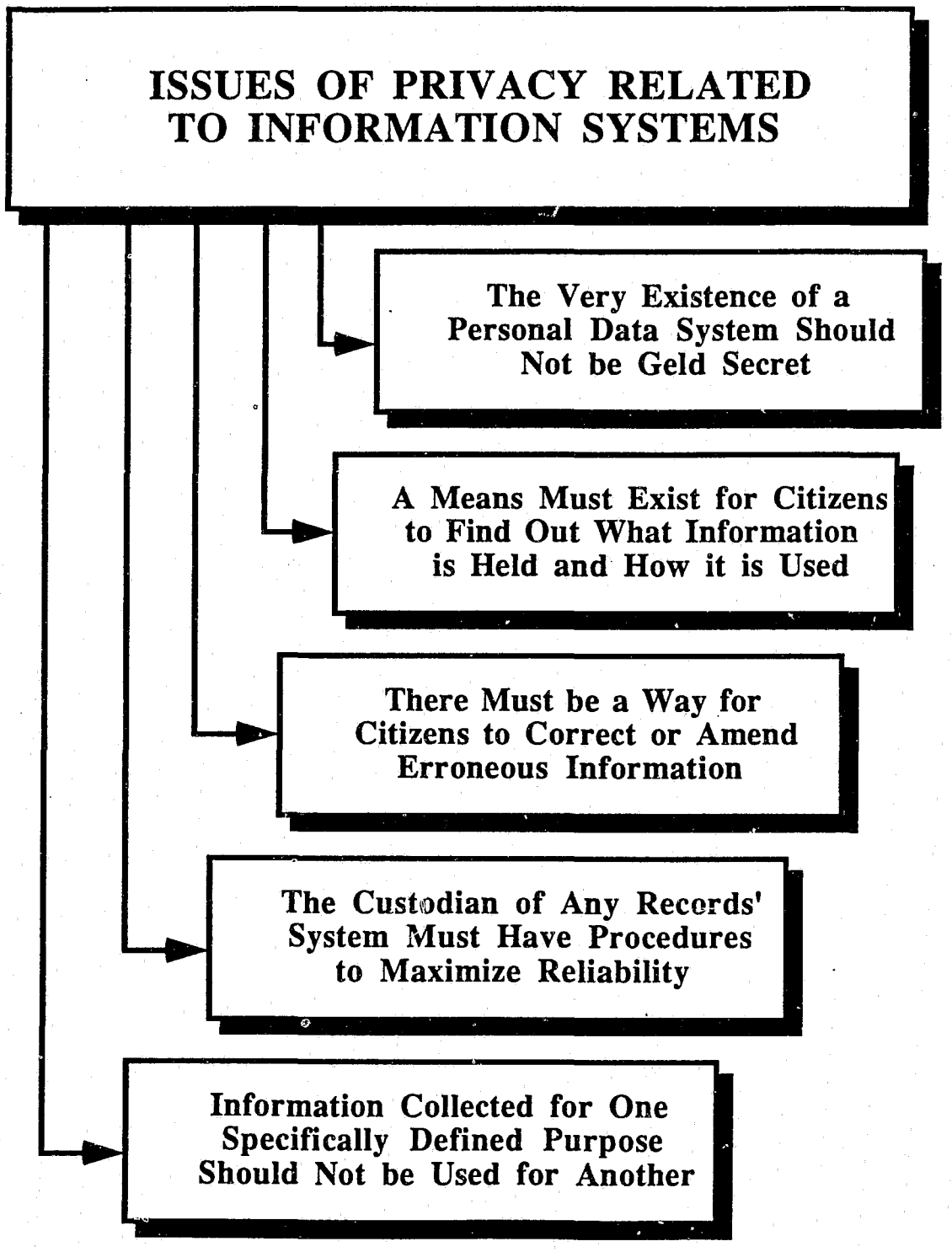
   b. *There must be a way for an individual to find out what information about him or her is in a record and how it is used.*

      1) This is particularly true regarding information that is used in official proceedings

      2) There is obviously a need to keep intelligence records confidential during the course of an investigation

Figure XII-1

PRIVACY ISSUES RELATED TO INFORMATION SYSTEMS



3) It is a case-by-case interpretation by intelligence personnel with respect to

   a) Which information can reasonably remain confidential, and

   b) The duration of time that confidentiality attaches is subject to

4) LAWINT personnel must "self-police" themselves to ensure that information which needs to remain confidential does so, yet balance the constitutional privacy rights of the individual judiciously

c. *There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for another purpose without his or her consent.*

   1) At the outset, this particularly applies to information that a person has voluntary submitted to a public or private organization for a defined purpose

   2) In those cases of submitted information, access of non-public records may have to be by court order

   3) Information independently generated by the law enforcement agency is a different circumstance wherein it can be used in pursuit of the original or related criminal investigation or civil processes (such as asset forfeiture)

d. *There must be a way for an individual to correct or amend a record of identifiable information about him or her.*

   1) This is particularly true for criminal records which are in error

   2) More problematic in LAWINT is when suspected criminal involvement or untrue information is entered in a person's file

   3) Given the nature of the intelligence records, there will be little access for inaccurate information to be corrected

4) Essentially, in LAWINT procedures should be established that monitor information in files and amend the information when inaccuracies are detected

a) At this point, most intelligence systems/units have not developed this process effectively

b) Corrections are usually made based on the memory of an analyst working on a case

c) The process needs to become more systematic

e. *Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.*

1) This includes dissemination of data and information to other law enforcement agencies

2) See discussions in previous information concerning: dissemination (Chapter 5), intelligence records (Chapter 13), and Privacy Act (Chapter 14).

2. These principles are important considerations in information technological developments which are at the disposal of LAWINT

a. It is recognized, however, that LAWINT records fall within unusual circumstances wherein access can be lawfully limited

b. The decisions on information release requires both legal judgement and ethical considerations

3. Privacy and civil liberties are not only a concern of information dissemination, but also during collection.

a. Many LAWINT technologies are intrusive, thus the issue becomes how intrusive can the collection process be without violating the privacy of the target

b. The perspective must be maintained that regardless of the nature of the investigation, the target's privacy rights remain intact—their violation could even jeopardize prosecution of the case

4. The dimensions for balancing interests between intrusive surveillance and privacy/civil liberties are not definitive, but rely on judgments which must be made by decision makers (OTA, 1985:22)

   a. **Civil Liberty Interest**

      1) *Nature of the Information*: The more personal or intimate the information that is to be gathered about a target, the more intrusive the surveillance technique and the greater the threat to civil liberties

      2) *Nature of Place of Communication*: The more "private" the area or place of communication to be placed under surveillance, the more intrusive the surveillance and the greater the threat to civil liberties

      3) *Scope of Surveillance*: The more people and activities that are subject to surveillance, the more intrusive the surveillance and the greater the threat to civil liberties

      4) *Surreptitiousness of the Surveillance*: The less likely it is for the individual to be aware of the surveillance and the harder it is for the individual to detect it, the greater the threat to civil liberties.

   b. **Government Investigative Interest**

      1) *Purpose of the Investigation*: Importance ranked as follows, national security, domestic security, law enforcement, and the proper administration of government programs. This ranking thus infers that national security intelligence may lawfully be more intrusive than LAWINT

      2) *Degree of Individualized Suspicion*: The lower the level of suspicion, the harder it is to justify the use of surveillance devices

      3) *Relative Effectiveness*: More traditional investigative techniques should be used and proven ineffective before using technologically sophisticated techniques

4. CURRENT AND FUTURE HIGH TECHNOLOGY APPLICATIONS TO LAW ENFORCEMENT INTELLIGENCE INCLUDE

There are a wide variety of technological devices currently available or on the horizon for use in law enforcement intelligence. As noted previously, resources for their use are an important limitation: Not only for purchase, but for training, use and maintenance. The nature of the investigation will affect the technology as well as legal restrictions. The listing below describes some of the technological applications.

A. Audio Technology

1. Radiating devices and receivers (e.g., miniaturized transmitters)
2. Non-radiating devices (e.g., wired surveillance systems including telephone taps and concealed microphones)
3. Audio tape recorders
4. Parabolic microphones for long distance reception of conversations
5. Cellular telephones
6. Microwave communications media

B. Optical/Imaging Technology

1. Photographic techniques (including panchromatic, infrared, and ultraviolet)
2. Video recordings and direct video surveillance (closed circuit and cable)
3. Night vision devices
4. Remote sensing (using either airplane or satellite platforms)
5. High resolution facsimile transmission methods
6. High resolution optics

C. Computers and Related Data Surveillance Technologies

1. Microcomputers - machine decentralization, remote access and remote processing
2. Computer networks and accessing patterns
3. Computer encrypted message transmissions and records
4. Bubble storage in computers (more information will be stored at lower cost and less space)
5. Mobile digital terminals
6. Simulation programs for establishing intelligence links and hypotheses
7. Computer enhanced images
8. Artificial intelligence

D. Sensor Technology

1. Magnetic sensors
2. Seismic sensors
3. Infrared sensors
4. Strain sensors
5. Electromagnetic sensors
6. Radar imagery

E. Other Devices and Technologies;

1. Transceiver radio equipment (including UHF, VHF, and CB)
2. Vehicle location systems
3. Aircraft and marine transponders

4. Laser disks for image storage

5. Voiceprint identification

6. Fiber optic technologies for voice, data, and image transmission

7. Identification through DNA

5. OBSERVATIONS ON THE GROWING USE OF TECHNOLOGY FOR INFORMATION COLLECTION AND USE

A. Utilization of technology in information collection grew significantly in the 1980s as a result of...

1. Greater availability of technology at lower costs

2. The undertaking of complex investigations notably large drug trafficking cartels and money laundering systems

B. Observations concerning electronic surveillance and technology...

1. The number of Federal and State court-approved wiretaps and bugs reported in 1984 was the highest since 1973

2. The number of Federal court-approved wiretaps and bugs in 1984 was the highest ever

3. The extent of use of electronic surveillance in the private sector for both legitimate and illegitimate use is unknown, but suspected to have increased dramatically in the 1980s

4. An average of about 25 percent of communications intercepted by law enforcement agencies in 1984 were reported to be incriminating in nature, with 2,393 persons arrested as a result of electronic surveillance

5. The Drug Enforcement Administration, Federal Bureau of Investigation, U.S. Customs Service, and Air Force Office of Special Investigations use the greatest number of different types of electronic surveillance technologies

C. The use of technology in case development should be a joint plan between operational units and intelligence units

   1. Types of desired information can be better targeted

   2. Legal justification, as needed, for the technology can be more effectively developed

   3. Value of seized conversations and information can be maximized

D. Technology is a *tool*, not an *end*

   1. Avoid the tendency to over rely on technological capabilities

   2. The value of the technology can only be measured in terms of its wise use

12. TECHNOLOGICAL ISSUES AND DEVELOPMENTS

Instructional Support and Criteria

GOAL:

To provide an overview and possible abuses of different technologies which are currently available or are emerging to support the effective use of tactical and strategic law enforcement intelligence.

OBJECTIVES:

1. The student will have a general understanding of a wide range of technologies which can be used for information collection, storage, analysis, and retrieval in the performance of the intelligence function.

2. The student will have an understanding of the fundamental privacy issues associated with using intrusive intelligence collection methods.

3. The student will be able to identify contemporary trends in the development of intelligence collection technologies.

STUDY QUESTIONS:

a. Why is security of intelligence collection technologies a fundamental concern?

b. Assume you are responsible for the introduction of new, highly sensitive and intrusive intelligence collection methods/technologies in your LAWINT unit. Describe the steps you would go through to ensure prober use and control of these technologies.

c. Based on your knowledge of the issues and the discussions contained in this document, describe what you think are the greatest concerns associated with high technology intelligence gathering devices. Discuss the reasons on which your concerns are based.

d. Discuss, as you understand them, the difference between the *Civil Liberty Interest* and the *Government Investigative Interest* in the propriety of using intrusive surveillance technologies in gathering intelligence information.

NOTES

CHAPTER 13

INTELLIGENCE RECORDS' SYSTEMS: AN OVERVIEW

"The court said we had to get rid of what we called our Red Files—you know, the records we kept on Commies, fags, activists and people who were generally a pain in the ass. We got rid of 'em—they're in my basement."
Comment of a former law enforcement intelligence officer from a southwestern state to the author.

1. A PERSPECTIVE ON INTELLIGENCE RECORDS

In the previous twelve chapters there has been a significant amount of reference to intelligence records. Written documents represent all the work of current and previous investigations as well as the essential structure for criminal prosecutions. Records have also been the manifest characteristic for which law enforcement intelligence has been criticized on the basis that many such records have violated citizens' rights in the past.

The purpose of this chapter is address many of the issues related to the maintenance of intelligence records from the perspectives of:

- Case Control
- Case Planning
- Case Accountability
- Coordination of Intelligence and Investigative Activities
- Accountability to the Public

Many of the concerns addressed in this section also have particular applicability to the discussions in the following chapter, **Legal Issues.**

2. POLICY GUIDES IN STARTING AN INTELLIGENCE CASE FILE

In order to ensure compliance with all aspects of the law and maintain quality control of the intelligence units case records, policy standards

should be established which dictate the parameters of starting a case file. The following give recommended direction in this regard.

A. Have articulatable facts or information to reasonably indicate that a crime has occurred, is being conspired, or may reasonably occur

B. Have defined targets for the case with some articulatable reason to link the target to the crime(s)

C. Establish a requirement that a supervisor approve the generation of a new case file after reviewing the facts concerning the crime(s) and/or suspected parties

D. A case supervisor should develop a broad plan for pursuing evidence in the case

   1. The plan would include:

      a. The type of information collection methodologies to be used;

      b. Critical milestones or decision points projected in the case's development;

      c. Anticipated issues or problems to be dealt with;

      d. Anticipated needs for outside or supplemental resources;

   2. The plan should be sufficiently specific to permit realistic planning and direction, yet broad enough to be flexible as the case develops and changes

E. If unique or special surveillance or information collection techniques are anticipated, they should be justified based upon:

   1. Legal permissibility

   2. Expected benefits/types of information to be gained

   3. Cost implications

   4. Logistical and coordination issues

F. When a case file is established, have a check sheet to ensure:

1. All proper approvals have been obtained;

2. All required forms and reports have been completed to formally establish the case file;

3. All required information has been entered into applicable intelligence information systems

4. All persons so required have been notified of the case

3. GUIDELINES FOR CONTROL AND MANAGEMENT OF INTELLIGENCE INFORMATION AND RECORDS

In light of the unique nature of intelligence information, constitutional limitations of intelligence information gathering, potential liability associated with improper intelligence information, and elements of the Privacy Act, careful control needs to be made of intelligence file information. The following presents some guidelines in this regard.

A. Dissemination procedures

1. *Dissemination within the agency to other units*

   a. Develop an authorized dissemination list for each category of intelligence information or authorize selected personnel to disseminate the information on a case-by-case basis

   b. Do not make copies of an intelligence file; permit visual inspection of the files or oral briefings to authorized persons

   c. All dissemination outside the intelligence unit should be logged by date, time, persons receiving information, person authorizing dissemination, nature of the information, and rationale for dissemination

2. *Dissemination to other criminal justice agencies*

   a. Disseminate, whenever possible, pursuant to an **Intelligence Mutual Aid Pact (IMAP)** with another agency (*See* Figures XIII-1 and XIII-2 appended to this chapter.)

1) An IMAP shows agencies have agreed to pool resources regarding cases and investigations

2) Specific guidelines on various aspects of cooperation, information sharing, and responsibilities should be in the IMAP

3) The IMAP should be a formal agreement between the applicable agency administrators

b. If no IMAP exists, disseminate to a recognized inter-agency intelligence group rather than an individual agency within the group

c. If no group exists, disseminate only to an intelligence officer

d. Log all information dissemination with the date, time, persons receiving information, person authorizing dissemination, nature of the information, and rationale for dissemination

e. Prohibit recipients from disseminating the information to other agencies or group (the **Third Agency Rule**)—agencies wanting the intelligence should be referred to the source agency

3. *Dissemination outside the criminal justice system*

a. Intelligence information must be restricted to bona fide criminal justice system users

b. Exceptions are when dissemination is required by:

1) Statute (e.g., Freedom of Information Act, Privacy Act)

2) Court order

3) Executive order

B. File/record creation and maintenance

1. Maintain all intelligence information in a physically segregated and secure intelligence section with restricted access

2. Never place intelligence information in Criminal History Record Information (CHRI) files

3. All intelligence files or cases (depending on the unit's organization) should have a designated supervisor or proctor who maintains control of entry, dissemination, purging of information

4. Information should be entered in intelligence records ...

   a. If it is known to be of criminal nature or shed relevant insight on criminal activity

   b. If there is some articulatable reason or pattern to show relevance of the information to the subject, crime, or case

   c. Identified with the source of the information and an evaluation of the validity and reliability of the information source and the information

C. Review and Purging of Intelligence Files

1. All matters relating to case file controls, including file creation, dissemination, review, and purging, should be a matter of written policy and procedure

2. Case file supervisors should perform an annual review of case files with the authority to purge files or delete information no longer relevant to the case/investigation

3. A log noting file review and outcome of the review should be maintained by the case/file supervisor

4. Criteria for purging file may include, but are not limited to:

   a. Reasonable grounds no longer exist connecting the record subject to the criminal behavior

   b. Information in the file was found to be collected in a manner which was inconsistent with either law or policy

   c. The information, on its face, is no longer relevant

d. The statute of limitations for the case under investigation has passed

e. Four years have passed without an entry into a case file or since the subject's contact with the criminal justice system

5. The case/file supervisor, upon entry of new file information, should review the file and delete information no longer pertinent

6. Information purged from intelligence files should be either shred or incinerated under the supervision of a member of the intelligence unit

4. GENERAL OBSERVATIONS ON CRIMINAL HISTORY RECORD INFORMATION (CHRI)

A. Privacy and CHRI are of particular concern to law enforcement agencies because of uncertainty about what information must be released

B. Criminal History Record Information—*Defined*:

> Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does *not* include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

C. The types of records covered in the CHRI definition are generally protected from disclosure except:

1. Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons

2. Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by

law or long standing custom to be made public, if such records are organized on a chronological basis

3. Court records of public judicial proceedings

4. Published court or administrative opinions or public judicial, administrative or legislative proceedings

5. Records of traffic offenses maintained by state departments of transportation, motor vehicles or the equivalent for the purpose of regulating the issuance, suspension, revocation, or renewal or driver's, pilot's, or other operators' licenses

6. Announcements of executive clemency

5. PHYSICAL MAINTENANCE OF RECORDS

A. Records may be stored via:

1. Paper files

2. Computerization (on-line or remote storage)

3. Microforms (Microfilm, microfiche)

B. Regardless of the storage media, there should be:

1. Defined procedures for:

a. Access to the records

b. Accountability for the records placement and use

2. Control procedures for "back-up" or duplicate records

Figure XIII-1

SAMPLE INTELLIGENCE MUTUAL AID PACT (IMAP)

AN AGREEMENT FOR MUTUAL ACCESS AND DISSEMINATION OF LAW ENFORCEMENT INTELLIGENCE INFORMATION

THIS AGREEMENT, made and entered into this_____day of _____, 19___, by and between the (*name of agencies*) which are political subdivisions of the State(s) of _____, who are signatories hereto.

WHEREAS, the political subdivisions named above have determined that the provision of law enforcement mutual aid across jurisdictional lines in multi-jurisdictional crimes will increase their ability to preserve the safety and welfare of the communities; and

WHEREAS, the above political subdivisions have law enforcement intelligence analysis capabilities for identifying crime trends and developing criminal cases against defined suspects,

NOW THEREFORE, the parties hereto do agree as follows:

1. Whenever a multijurisdictional crime occurs or is reasonably suspected between the above jurisdictions and that crime meets the originating agency's requirements as an intelligence target, the Chief Executive of the law enforcement agency or his/her designate shall communicate with the other party or parties about the nature of the crime and/or suspects.

2. When a designated intelligence representative of one of the above law enforcement agencies seeks intelligence information in the development of a bona fide criminal case or for strategic intelligence projections, that representative may formally obtain that information from the other party or parties under the provisions of this agreement.

3. Requests and information exchanges described above shall be rendered according to the procedures established in the operational plans developed and agreed to by all of the parties to this agreement pursuant to the provisions in paragraph 4 herein. Each party shall designate an appropriate official within its jurisdiction who is empowered to request information under this agreement.

4. The mutual assistance to be rendered under this agreement shall be available upon the development and approval of an operational plan developed by the above named parties. The plan shall outline the exact procedures to be followed in responding to a request for information and for notifying a participant agency of a multijurisdictional intelligence target. Upon execution of this agreement, the parties hereto shall designate an appropriate official in each agency to participate in the development of the operational plan. The parties shall meet at least annually to review and, if necessary, to propose amendments to the operational plan. Any proposed amendments shall not be effective until approved in writing by all the parties to this agreement. ***(continued...)***

5. The services performed and expenditures made under this agreement shall be deemed for public and governmental purposes. All immunities from liability enjoyed by the local political subdivision within its boundaries shall extend to its participation in rendering mutual aid under this agreement outside its boundaries unless provided by law.

6. Each party to this agreement shall waive any and all claims against all the other parties hereto which may arise out of their activities affecting direct actions and intelligence activities derived under the provisions of this agreement.

7. Each party shall indemnify and save harmless the other parties to this agreement from all claims by third parties for damage or injury which may arise out of the activities of the other parties of this agreement under mutual aid activities performed under the provisions of this agreement.

8. All the immunities from liabilities and exemptions from laws, ordinances, and regulations which law enforcement employees employed by the various parties hereto have in their own jurisdictions shall be effective in and with the jurisdiction in which they are reciprocating intelligence activities unless otherwise prohibited by law.

9. All compensation and other benefits enjoyed by law enforcement employees in their own jurisdiction shall extend to the services they perform under this agreement.

10. Law enforcement employees rendering assistance under this agreement shall do so under the direction and control of the appropriate official designated by the jurisdiction requesting the aid.

11. The parties shall notify each other of the name, address, and telephone number of the official authorized to direct mutual aid activities within their jurisdiction.

12. The parties to this pact agree to provide safeguards to protect reports, safeguards in data transmission, storage and retrieval, to maintain confidentiality and prevent unauthorized access to the information.

13. The parties agree to abide by all federal, state and local laws and regulations governing criminal investigations and criminal files.

14. The parties agree to abide by the provisions of the Department of Justice "Criminal Intelligence Systems Operating Policies" appended to this agreement.

15. This agreement shall remain in effect until terminated by all the parties hereto upon written notice setting forth the date of such termination. Withdrawal from this agreement by any one party hereto shall be made by thirty days' written notice to all parties but shall not terminate this agreement among the remaining parties.

IN WITNESS THEREOF, the parties hereto have executed this agreement as of the date noted above.

(To be signed by the Chief Executive Officers of the participating agencies.)

Figure XIII-2

CHAPTER 1--DEPARTMENT OF JUSTICE

PART 23—CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

Chapter I—Department of Justice

PART 23—CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

Sec.

AUTHORITY: Pursuant to the authority invested in the Office of Justice Assistance, Research, and Statistics by sections 818(c) and 802(a) of the Omnibus Crime Control and Safe Streets act of 1968, 42 U.S.C. 3701, *et seq.*, as amended by the Omnibus Crime Control Act of 1970, Pub. L. 91-644, 84 Stat., 1880 (Jan. 2, 1971), the Crime Control Act of 1973, Pub. L. 93-83, 87 Stat. 197 (Aug. 6, 1973), the Juvenile Justice and Delinquency Prevention Act of 1974, Pub. L. 93-415, 88 Stat. 1109 (Sept. 7, 1974), the Public Safety Officers' Benefits Act of 1976, Pub. L. 94-430, 90 Stat. 1346 (Sept. 29, 1976), the Crime Control Act of 1976, Pub. L. 94-503, 90 Stat. 2407 (Oct. 15, 1976), the Juvenile Justice Amendments of 1977, Pub. L. 95-155, 91 Stat. 1048 (Oct. 3, 1977), and the Justice System Improvement Act of 1979, Pub. L. 96-157, 93 Stat. 1167.

SOURCE: 45 FR 61613, Sept. 17, 1980, unless otherwise noted.

§23.1 Purpose.

The purpose of these regulations is to assure all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3701, *et seq.*, as amended (Pub. L. 90-351, as amended by Pub. L. 9-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, and Pub. L. 96-157), are utilized to conformance with the privacy and constitutional rights of individuals.

§23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, narcotics, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates. Policy Guidelines for Federally funded projects are required.

§23.3 Applicability.

(a) These standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3701, *et seq.*, as amended (Pub. L. 90-351, as amended by Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-130, Pub. L. 94-503, Pub. L. 95-115, and Pub. L. 96-157) or under the State and Local Drug Strike Force Grant Program (Pub. L. 96-68 and Pub. L. 96-132).

(b) As used in these policies, "Intelligence Systems" means the arrangements equipment, facilities, and procedures used for the continuing storage, exchange and analysis of criminal intelligence data, however, the term does not include modus operandi files; "interjurisdictional Intelligence Systems" means those systems for the continuing exchange of criminal intelligence data between local, county, or larger political subdivisions, including the exchange of data between State or local agencies and units of the Federal Government.

§23.20 Operating principles.

Criminal intelligence information concerning an individual shall be collected and maintained only if it is reasonably suspected that the individual is involved in criminal activity and that the information is relevant to that criminal activity.

(b) No records shall be maintained or collected about political, religious or social views, association or activities of any individual group, association, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

(c) No information which has been obtained in violation of any applicable Federal, State, or local law or ordinance shall be included in any criminal intelligence system.

(d) Intelligence information shall be disseminated only where there is a need to know/right to know the data in the performance of a law enforcement activity.

(e)(1) Except as noted in (e)(2) of this section, intelligence information shall be disseminated only to other law enforcement authorities who shall agree to follow procedures regarding data entry, maintenance, security, and dissemination which are consistent with these standards.

(2) Paragraph (e)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a Government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(f) Agencies maintaining criminal intelligence data shall adopt administrative, technical, and physical safeguards (including audit trails) to insure against unauthorized access and against intentional or unintentional damage. A written record indicating who has been given data, reason for release and date of each dissemination outside the agency is to be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of control agencies and officials. Each agency must establish written standards for need to know/right to know under subsection (d).

(g) Procedures shall be adopted to assure that all information which is retained has relevancy and importance. Such procedures shall provide for the periodic review of data and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Any information that has been retained in the system but has not been reviewed for a period of two (2) years must be reviewed and validated before it can be utilized or disseminated.

(h) If automated equipment for use in connection with a criminal intelligence system is to be obtained with funds under the grant, then:

(1) Direct remote terminal access to data shall not be made available to system users; and

(2) No modifications to system design shall be undertaken without prior LEAA approval.

(i) LEAA shall be notified prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(j) Assurances shall be made that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of Title III of Pub. L. 9-351, as amended, or any applicable state statute related to wiretapping and surveillance.

(k) Assurances shall be made that there shall be no harassment or interference with any lawful political activities as part of the intelligence operation.

(l) Sanctions shall be adopted to control unauthorized access, utilization, or disclosure of information contained in the system.

23.30 Funding guidelines.

(a) LEAA and state criminal justice agencies shall apply the following funding guidelines to all categorical grant applications and formula grant applications, the principal purpose of which is the funding of intelligence systems. Systems shall only be funded where a grantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(1) The proposed collection and exchange of data has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(2) The areas of criminal activity in connection with which intelligence data are to be utilized represents a significant and recognized threat to the population and;

(i) Is either undertaken for the purpose of seeking illegal power or profits or poses a threat to the life and property of citizens;

(ii) Involves a significant degree of permanent criminal organization; and

(iii) Is not limited to one jurisdiction.

(3) Control and supervision of information collection and dissemination for the intelligence system will be retained by the head of a government agency or by an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency. This official shall certify in writing that he takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the standards set forth in §23.20.

(4) Where the system is an interjurisdictional system the governmental agency which exercises control and supervision over the operation of the system shall have the head of that agency or an individual with general

policymaking authority who has been expressly delegated such control and supervision by the head of the agency; (i) officially responsible and accountable for actions taken in the name of the joint entity and (ii) certify in writing that he takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to other agencies will be in compliance with the standards set forth in §23.20. The standards set forth in §23.20 shall be made part of the By-laws or operating procedures for that system. Each member agency, as a condition of membership, must accept in writing these standards which govern the collection, maintenance and dissemination of information included as part of the interjurisdictional system.

(5) Intelligence data will be collected primarily for State and local law enforcement efforts—exceptions being made only for cases involving joint State-Federal efforts.

§23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Grants for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in §23.20. Such plan shall be approved prior to award of funds.

(b) All such grants shall be awarded subject to a Special Condition requiring compliance with standards set forth in §23.20.

(c) An annual notice will be published by OJARS which will indicate the existence and objective of all systems for the continuing interjurisdictional exchange of intelligence data which are funded under the Act.

13. INTELLIGENCE RECORDS' SYSTEMS: AN OVERVIEW

Instructional Support and Criteria

GOAL:

To provide an overview of issues associated with the maintenance, creation, dissemination, and control of intelligence records.

OBJECTIVES:

1. The student will be able to identify the basic issues for which decisions must be made in the control of intelligence records.
2. The student will have a foundation for developing an Intelligence Mutual Aid Pact between law enforcement agencies..
3. The student will be familiar with the structure of Criminal History Records Information..

STUDY QUESTIONS:

a. On what criteria would the decision be based to create an intelligence case file on a target?

b. Why is *dissemination* of intelligence records such a critical issue? What is the value of an Intelligence Mutual Aid Pact?

c. Why would intelligence units ever want to *purge* their records?

d. What is "Criminal History Records Information"? What is its use in intelligence?

NOTES

CHAPTER 14

LEGAL ISSUES AND LAW ENFORCEMENT INTELLIGENCE

"In my experience there are times when we [the police] have to step on a few rights to ferret out the assholes."
Statement of a municipal police manager to the author.

1. LEGAL ISSUES ASSOCIATED WITH THE MANAGEMENT OF INVESTIGATIVE AND INTELLIGENCE ACTIVITIES

Information contained in intelligence must be collected, managed, protected, and disseminated in a lawful manner. The issues of law are wide-ranging in the fulfillment of these legal requirements and span the continuum of substantive criminal law, criminal procedure, civil rights, and liability, among others. Furthermore, there are Federal legal mandates in these areas as well as mandates by state laws (and sometimes local ordinances) all of which are conceptually similar, yet have minor procedural differences. The information contained herein is to provide an overview of the issues and alternatives. Since many state laws on these issues are modeled after Federal legislation, Federal laws are presented as a guidepost to the issues. Topics of law to be addressed are:

- Maintenance of Intelligence Records
- Civil Liberties and Intelligence Records
- Liability
- Freedom of Information Act (FOIA)
- Privacy Act
- Racketeering Influence Corrupt Organizations (RICO) and Continuing Criminal Enterprises
- Asset Forfeiture

2. AN OVERVIEW OF LAW RELATING TO THE MAINTENANCE OF AND USE OF INTELLIGENCE AND INVESTIGATIVE RECORDS/FILES

A. The Duty to Adhere to Substantive Law Mandates

1. Intelligence information collected and maintained regarding suspected criminal activity must involve the violation of a defined substantive criminal law for which the parent agency of the intelligence organization has jurisdiction to investigate

2. Collection and maintenance of intelligence records in support of non-criminal legal action (such as civil asset forfeiture) must be within the statutory empowering authority of the parent agency

3. Collection, maintenance, and dissemination of information or records maintained by the intelligence unit must be done so in a manner consistent with statutory records requirements including, but not limited to, Privacy Acts and Freedom of Information Acts

4. Actions of persons collecting, analyzing, and disseminating intelligence information must be consistent with provisions of the Civil Rights Act (as well as any provisions of applicable state tort law)

B. The Duty to Adhere to Procedural Law Mandates

1. Intelligence information must be collected so as not to violate the constitutional rights of any person

2. Of particular concern is:

   a. Fourth Amendment prohibition against *unreasonable searches and seizures*

   b. Fifth Amendment *privilege against self-incrimination*

   c. Fifth and Fourteenth Amendments guarantees of *due process of law*

   d. Case law decisions and articulated statutory *rights of privacy*

3. Covert information collection methodologies are of particular concern

4. ***General Rule***: Assume that any information collected may be needed for introduction into a criminal trial, thus the procedures used to collect it must be able to withstand judicial scrutiny

C. The Duty to Maintain Accurate and Current Records

1. An agency which has the responsibility for the operation and management of a records or information system which has multi-jurisdictional contributors has the duty to take reasonable steps to help ensure the accuracy of the information because:

   a. It keeps the information in an organized file; and

   b. Disseminates the information

2. The function of maintaining and disseminating records carries with it as a corollary the responsibility to discharge that function reliably and responsibly and without unnecessary harm to individuals whose rights have been invaded

3. Agencies contributing to records systems have the duty to:

   a. Maintain reasonably accurate and current information; and

   b. Establish reasonable administrative mechanisms designed to minimize the risk of inaccuracy by requiring that the records be constantly updated

4. Breaches of the duty to make reasonable efforts to maintain accurate records ...

   a. May result in civil liability on the part of the agency, its officials, and applicable employees

   b. Invalidate arrests based upon reliance of inaccurate information and the suppression of evidence seized after such arrests

D. Liability for Record Mismanagement or Mishandling

1. Personal liability may be incurred through either intentional or negligent conduct in the maintenance, dissemination, use, or inaccuracy of criminal justice records

2. Various state and federal statutes permit that liability including the far reaching 42 U.S.C. 1983, Deprivation of Civil Rights

3. Most records management is a "discretionary act"

   a. That is, there is no explicit statutory or regulatory guidance and discretion is used in the management of the system

   b. If discretionary acts are performed in good faith then one may be protected by qualified immunity

4. If records systems users ...

   a. Act in good faith;

   b. Reasonably confirm information obtained in the records system before taking official action; and

   c. Believe the records system to be reliable; then

   d. They will be better protected from liability—or at least be in a more defensible position

5. Case law varies on liability and courts have sustained civil judgements for records malpractice at every stage of the process: record entry, records maintenance, and records utilization

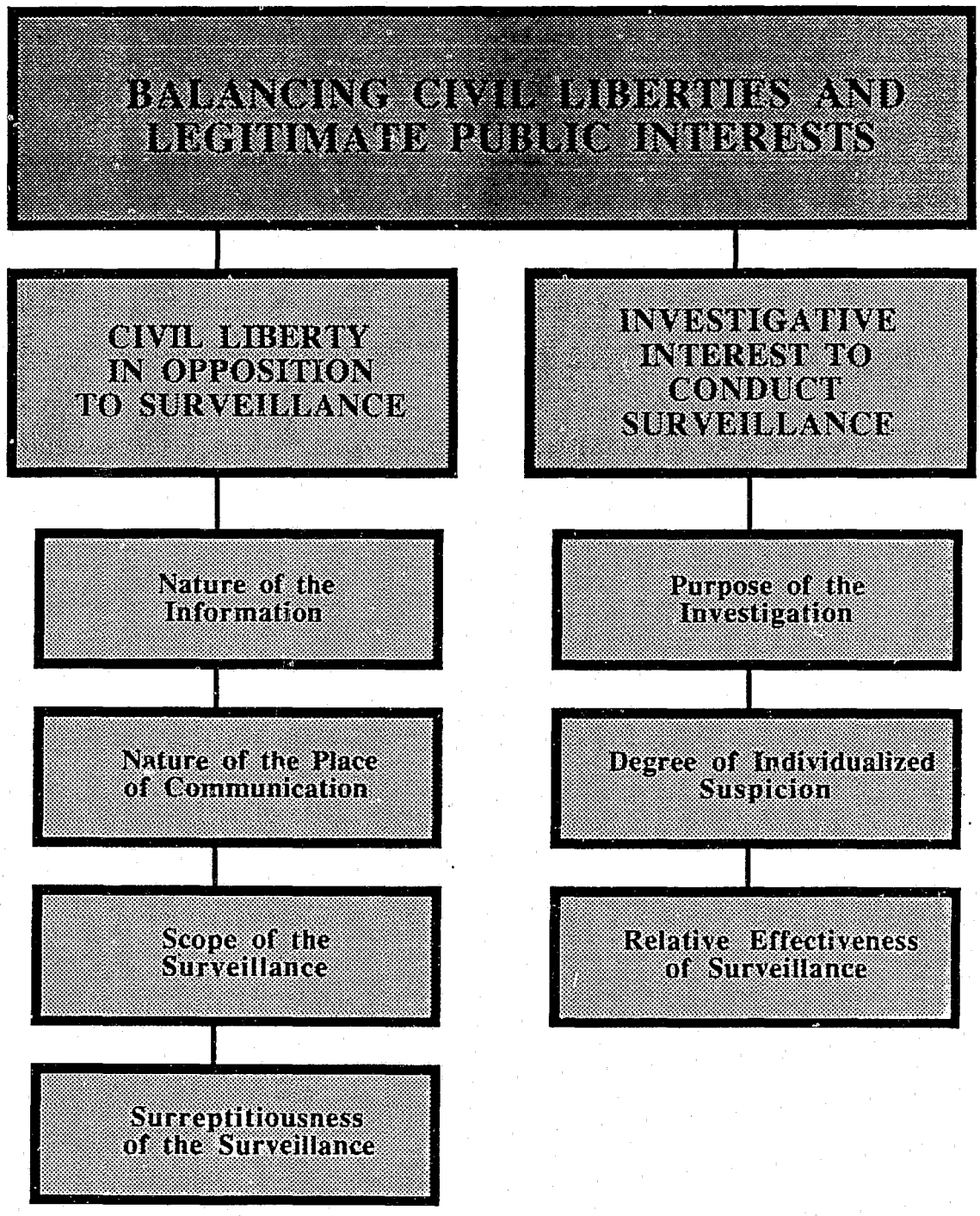
6. Certainly, liability would attach if improperly seized information was placed in an intelligence records system as part of a case file

3. BALANCING INDIVIDUAL CIVIL LIBERTIES AND THE LEGITIMATE PUBLIC INTEREST

When seeking a court order to obtain certain types of information—such as conducting some form of covert, intrusive surveillance or access private and confidential records of a person—a judicial officer must frequently "balance" the individual rights of a person versus the legitimate public interest served by the collected information. In making the decision whether to grant the request for surveillance or information collection, the court considers various issues and standards. If the intelligence and investigative officers can anticipate some of these issues with documented rationale and/or sound logic, permission to collect the desired information is more likely to be granted. The following outlines some of the more critical factors in the "balancing" decision (*See* Figure XIV-1):

Figure XIV-1

BALANCING INDIVIDUAL CIVIL LIBERTIES AND PUBLIC INTERESTS FOR SURVEILLANCE



A. Civil Liberty Interest in Opposition to the Surveillance

1. ***Nature of the Information*** - The more personal or intimate the information that is to be gathered about a target, the more intrusive the surveillance technique and the greater the threat to civil liberties

   CASE ARGUMENT:

   a. Indicate in the strongest terms possible the importance of the information to the case

   b. Present any facts, evidence, or analytic hypothesis in support of the argument

2. ***Nature of the Place or Communication*** - The more "private" the area or type of communication to be placed under surveillance, the more intrusive the surveillance and the greater the threat to civil liberties

   CASE ARGUMENT:

   a. Indicate the rationale for the particular surveillance being sought

   b. In private places, logic may focus on the fact that relevant and incriminating conversations are believed to only occur in strictly limited settings

   c. Regarding private communications, logic may focus on the fact that the target's communications of an incriminating or evidentiary nature are typically limited to a rigidly defined circle of confidants

   d. Support this rationale with information from informants, undercover agents, or other available documentation (including deductions from the intelligence analyst)

3. ***Scope of the Surveillance*** - The more people and activities that are subject to surveillance, the more intrusive the surveillance and the greater the threat to civil liberties

CASE ARGUMENT:

a. Each person or activity for which surveillance is planned should be justified individually with respect to the need for the surveillance

b. The arguments may be strengthened by also showing the relationships between the persons and activities

4. **Surreptitiousness of the Surveillance** - The less likely it is for the individual to be aware of the surveillance and the harder it is for the individual to detect it, the greater the threat to civil liberties.

CASE ARGUMENT:

a. Rationale for the surveillance may indicate that surreptitious surveillance methodologies are virtually the only means by which to obtain the evidentiary or incriminating information

b. Arguments might also draw on the support used for item 2 above regarding the privacy of the place and the communication

B. Government Investigative Interest to Conduct the Surveillance

1. ***Purpose of the Investigation*** - In law enforcement intelligence it must be shown that the target under investigation is reasonable suspected of a specific crime

CASE ARGUMENT:

a. Evidence must be submitted to support this claim

b. The federal government and states will have different statutory law governing the use of electronic surveillance devices

c. Information must be submitted to show that statutory provisions have been met

2. ***Degree of Individualized Suspicion*** - The lower the level of suspicion, the more difficult it is to justify the use of surveillance devices

CASE ARGUMENT:

a. Specific evidence and reasonably inferred facts must be presented as they relate to a specific person's involvement in the crime being investigated

b. The argument that it is believed the target is deeply involved in a criminal enterprise and the surveillance is to obtain evidence to confirm that involvement may not be used—there must be independent evidence individualizing the suspicion

3. ***The Relative Effectiveness of Surveillance*** - More traditional investigative techniques should be used and proven ineffective before using technologically sophisticated methodologies

CASE ARGUMENT:

a. Types of techniques used and nature of the results should be articulate

b. Indicate why it is believed the surveillance methodologies would yield better information

c. Indicate general types of information expected to be collected through electronic surveillance and the basis for those reasons

4. THE FEDERAL FREEDOM OF INFORMATION ACT (FOIA)

The Freedom of Information Act (FOIA), 5 U.S.C. 552, *Defined*:

> Enacted in 1966 generally provides, as a statutory right, that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

A major purpose of the FOIA is to *maintain an informed citizenry about the actions of government officials and agencies*. Yet achieving an informed citizenry is a goal often counterpoised against other vital societal aims. Society's interest in an open government can conflict with its interest in protecting personal privacy rights and with the overriding public need for persevering the confidentiality of national defense, criminal investigation matters, and other concerns. Though tensions among these competing

interests are characteristic of a democratic society, their resolution lies in providing a workable formula which encompasses, balances, and appropriately protects all interests, while placing emphasis on fully responsible disclosure. It is the task of accommodating opposing concerns, with disclosure as the primary objective, that the FOIA seeks to accomplish.

The following outline addresses the critical components of the FOIA based on its statutory content and case law on issues. While the outline is fairly comprehensive, it is not meant to be all-inclusive of the issues involved in FOIA litigation.

A. The FOIA provisions for disclosure include:

1. Requires automatic disclosure of the following:

   a. Publication in the Federal Register of information such as descriptions of agency organization, functions, procedures, substantive rules, and statements of general policy

   b. Final opinions in the adjudication of cases, specific policy statements, and certain administrative staff manuals, all of which must be indexed, and routinely be made available for public inspection—this disclosure is to prevent the promulgation of any "secret law".

2. The most commonly utilized portion of FOIA requires disclosure of all records upon an agency's receipt of a specific and proper access request from any person unless the information is exempted from disclosure

3. To deal with the public's official governmental representatives—Congress—the FOIA requires that Congress (as a body, not as individual congressional members) cannot be denied access to information on the grounds of FOIA exemptions

4. The Act also requires that each federal agency submit an annual report to Congress regarding its FOIA operations and an annual report from the Attorney General regarding FOIA litigation and the efforts of the Department of Justice to encourage agency compliance with the FOIA

B. Procedural requirements of the FOIA include:

1. The act only applies to "records" maintained by "agencies" within the Executive Branch of the federal government

2. *Excluded* under the federal FOIA are:

   a. Records maintained by state governments (although states may enact a state FOIA for those records)

   b. Records maintained by the courts

   c. Records maintained by Congress

   d. Records of organizations that are neither chartered by the federal government nor controlled by it

   e. Records of the personal staff of the President and units within the Executive Office of the President whose sole function is to advise and assist the President

   f. Personal notes of an agency employee or official typically may not be considered a "record" for disclosure

   g. Certain internal communications may not be deemed to be discloseable records—these may be determined on a case-by-case basis

3. Each federal agency is required to publish its FOIA procedural regulations in the Federal Register

4. FOIA requests may be made by "any person" which includes individuals (including foreign citizens), partnerships, corporations, associations, and foreign, state, and local governments

5. FOIA requests may be made for any reason with no showing of relevancy or purpose required

6. The FOIA has only two requirements for access to records:

   a. The request "reasonably describe" the records sought (It is reasonable if it enables a professional agency employee familiar with the subject area to locate the record with a "reasonable amount of effort"

   b. The request be made in accordance with the agency's published procedural regulations

7. The agency, upon receipt of a valid request, must inform the requester of its decision to grant or deny access to the information within ten working days—the information does not have to be provided within ten days, but "promptly thereafter"

8. Extensions for time limits can be made if:

   a. There is a need to search for and collect records from different offices;

   b. There is a need to examine a voluminous amount of records required by the request; and

   c. There is a need to consult with another agency or agency component

9. The FOIA requires that any "reasonably segregated portion of a record" must be released after appropriate application of the nine exemptions

10. Notifications to requesters should contain information such as:

    a. *Time* and *location* when records will be available

    b. Amount of *fees*, if any, which must be paid prior to the granting of access to the records

    c. *Which records* are or are not responsive to the request

    d. The *date of receipt* of the request (or appeal)

    e. The *reason for denial* of request

f. Where appropriate, the agency's *interpretation* of a request or appeal

11. Miscellaneous characteristics of the FOIA (*See* Figure XIV-2):

a. The FOIA applies only to *records*, not to tangible or evidentiary objects

b. Agencies are *not* required to *create records* in order to respond to FOIA requests

c. Agencies are not bound to answer questions *disguised as FOIA* requests

d. FOIA does *not* permit *degrees of disclosure* such as permitting viewing, but not copying of documents

e. Disclosure is of the records, *interpretations or inferences* from the records are *not required* of the agency

f. There is *no damage remedy* available to FOIA requesters for non-disclosure—actions are only reviewable and enforceable by the courts

g. Requesters *cannot require* agencies to make *automatic releases* of records as they are created; non-automatic disclosures must be a result of valid requests

h. Agencies *may charge reasonable fees* for responding to requests—fees may include labor, supplies, computer time, photocopying, and similar expenses necessary to produce the records

C. Exemptions to the FOIA—*Defined*:

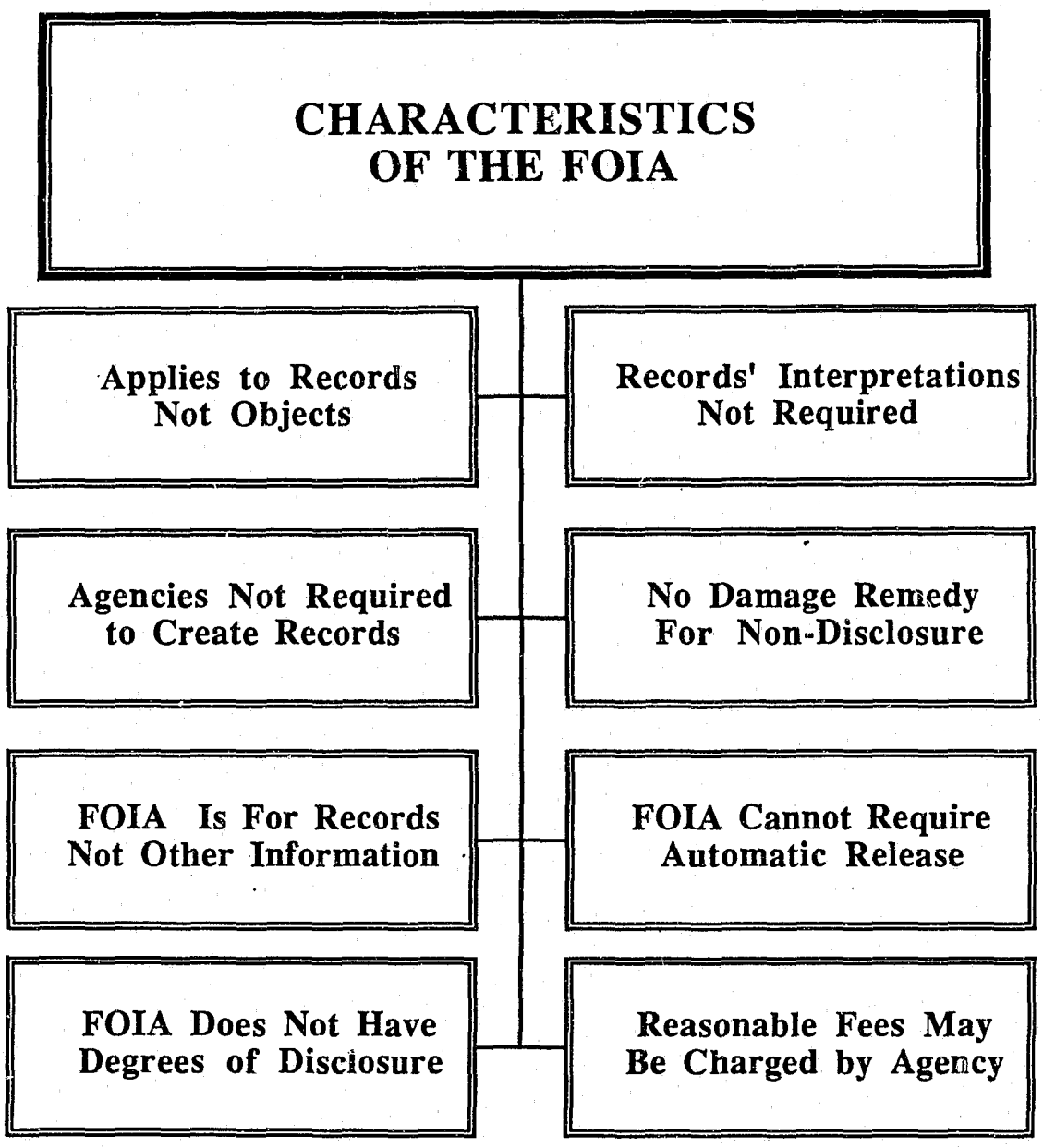
> Exemptions are the circumstances wherein an agency is not required to disclose information from a FOIA request.

1. Exemptions have been established via statutory law

2. Court interpretations have verified and clarified the exemptions

Figure XIV-2

CHARACTERISTICS OF THE FREEDOM OF INFORMATION ACT



3. The following description of exemptions is a summary of the critical law

D. EXEMPTION 1

Protects from disclosure national security information concerning the national defense or foreign relations, provided that the information/records has been properly classified in accordance with the substantive and procedural requirements of an Executive Order.

E. EXEMPTION 2

Exempts from disclosure records "related solely to the internal personnel rules and practices of an agency." This exemption has been interpreted to encompass two distinct categories of information:

1. Internal matters of a relatively trivial nature; and

2. More substantial internal matters which, if disclosed, would allow circumvention of a statute or agency regulation

F. EXEMPTION 3

Allows the withholding of information which is prohibited from disclosure by statute only if that statute:

1. Requires that the records/information which are to be withheld from the public are done so in such a manner as to leave no discretion on the issue; or

2. Establishes particular criteria for withholding or refers to particular types of matters to be withheld

G. EXEMPTION 4

The intent of this exemption is to protect both the interests of commercial organizations that submit proprietary information to the government and the interests of the government in receiving continued access to such information. The exemption covers two broad categories of information in federal agency records:

1. Trade secrets

2. Information which is:

   a. Commercial or financial, and

   b. Obtained from a person (as opposed to information independently generated by the government through investigation), and

   c. Privileged or confidential

H. EXEMPTION 5

This exemption includes "inter-agency or intra-agency memorandums or letters which would not be available by law to a party ... in litigation with the agency." The courts have interpreted this exemption to exempt those documents, and only those documents, normally privileged in the civil discovery context. The exemption is quite broad, however, the three most frequently invoked privileges which have been held to be incorporated in the exemption are:

1. The "deliberative process" privilege or "executive privilege"—reasons:

   a. To encourage open, frank discussions on matters of policy between subordinates and superiors;

   b. To protect against premature disclosure of proposed policies before they are officially/formally adopted; and

   c. To protect against public confusion that might result from disclosure of reasons and rationales that were not, in fact, ultimately the grounds for the agency's actions

2. The attorney work-product privilege

   a. Protects documents and other materials prepared by an attorney in preparation for litigation

   b. Its purpose is to protect the adversary trial process by insulating the attorney's preparation from scrutiny

3. The attorney-client privilege

   a. Incorporates confidential communications between an attorney and his/her client relating to a legal matter for which the client has sought professional advice

   b. Includes both facts given by the client to the attorney and the attorney's opinions based on those facts

I. EXEMPTION 6

Provides protection for personal privacy through the withholding of all information about individuals in personnel files, medical files, and similar files if its disclosure would constitute a clearly unwarranted invasion of personal privacy.

1. This exemption cannot be invoked by an agency when a requester is seeking disclosure of private information about him/herself

2. In determining if the disclosure was an unwarranted invasion of personal privacy, one must balance the rights of the public interest versus the privacy right (such as a public official's violation of the public trust)

J. EXEMPTION 7

Protects from disclosure "*investigatory records* compiled for law enforcement purposes, but only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the the life or physical safety of law enforcement personnel." Generally ...

- *Investigatory records* are those records which reflect or result from specifically focused inquiries by the agency

- For the records to be exempt, they typically must be part of a compilation on a specific case or criminal enterprise, not a routine compilation of information or a general inquiry

- When records not initially compiled for law enforcement purposes become an important part of the record compiled for an ongoing investigation, then the exemption attaches

1. ***Exemption 7(A)***

   a. Authorizes the withholding of investigatory records compiled for law enforcement purposes if their disclosure would interfere with pending or prospective law enforcement proceedings

   b. An important element to this exemption is whether the records' disclosure would cause some articulatable harm

   c. Only a generalized showing of "interference" typically would need to be made

   d. Dormancy of an investigation does not negate the exemption

2. ***Exemption 7(B)***

   This exemption, which is aimed at avoiding prejudicial pretrial publicity, is rarely asserted and has not been the subject of any significant judicial interpretation

3. ***Exemption 7(C)***

   a. Investigatory records may be withheld if the records would produce an unwarranted invasion of personal privacy

   b. While similar to Exemption 6, the burden of proof to withhold records under this exemption is lower

   c. Several courts have implicitly recognized a public interest favoring non-disclosure of personal privacy information, particularly the public interest element, in avoiding impairment of ongoing and future criminal investigations

4. ***Exemption 7(D)***

   a. Provides protection for confidential sources in all law enforcement investigations

b. Permits withholding of all information provided by a confidential source

c. The exemption focuses on the circumstances and source(s) under which the information is provided, not exclusively on the harm resulting from disclosure of the information

d. Informants' identities are protected whenever they have provided information either:

1) Under an expressed promise of confidentiality; or

2) Under circumstances from which such an assurance could be reasonably inferred

5. ***Exemption 7(E)***

a. Investigatory records reflecting special techniques or procedures of investigation may be withheld where necessary to prevent harm to the investigatory process

b. Commonly known procedures may be protected when their use in concert with other elements of an investigation and in their totality directed toward a specific investigative goal constitute a "technique" which merits protection to insure its future effectiveness

c. Where an agency's law enforcement mandate is preventative rather than investigative, protective techniques and procedures may be exempt from disclosure

6. ***Exemption 7(F)***

a. Protects information in investigatory records if the disclosure would endanger the life of physical safety of law enforcement personnel (regardless of the agency or level of government)

b. The exemption extends to retired law enforcement officers

K. EXEMPTION 8

1. Covers matters that are "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions"

2. Bank examination reports and related documents prepared by state regulatory agencies have been found to be protected under this exemption

L. EXEMPTION 9

1. This exemption covers "geological and geophysical information and data, including maps, concerning wells"

2. The exemption appears to be primarily focused to protect security and proprietary interests in energy sources such as oil and uranium

M. MISCELLANEOUS ISSUES ASSOCIATED WITH THE FOIA

1. The FOIA authorizes agencies to waive or reduce the customary charges for document search and duplication where agencies determine that such action is in the public interest because furnishing the information can be considered as primarily benefiting the general public

2. Jurisdiction in cases where an agency has not complied with the FOIA or a point is at issue regarding the agency's response to a valid request ...

   a. Jurisdiction to hear FOIA cases rests with the U.S. District Courts

   b. Jurisdiction is predicated upon the plaintiff showing that an agency has

      - Improperly,
      - Withheld,
      - Agency records

3. If an FOIA complaint is filed in District Court regarding an agency's response (or lack thereof), the agency has 30 days to answer the complaint

4. Requester's exhaustion of remedies ...

   a. The general FOIA rule is that *administrative remedies must be exhausted prior to judicial review*

   b. Depending on published agency procedures, most agency's have some form of internal review or appeal regarding FOIA requests

   c. The Act permits requesters to treat an agency's failure to comply with its specific time limits as the full exhaustion of administrative remedies

5. Regarding the adequacy of the search for records ...

   a. To prevail in a FOIA suit, the defendant agency must prove that each document ...

      • Has been produced,
      • Is unidentifiable, or
      • Is wholly exempt from the Act's inspection requirements

   b. The issue is not whether there might be additional documents which are possibly responsive to the request, but whether the search for those documents was adequate

6. If it is found that an agency has fully responded to a valid FOIA request, the issue is moot and litigation should be dismissed

7. The **Vaughn Index**

   a. *Defined*:

> In *Vaughn v. Rosen*, 484 F.2d 826, the court required agencies to prepare an itemized index, correlating each withheld document (or portion) with a specific FOIA exemption and the relevant part of an agency's non-disclosure justification.

b. The degree of specificity of itemization, justification, and correlation required in a particular case will depend on the nature of the document at issue and the particular exemption asserted

8. Judges may make *in camera* (in chambers) inspection of records to make determinations of whether records should be exempt

9. Discovery is extremely restricted in FOIA actions except with respect to the scope of an agency's search, its indexing, and classification procedures, and similar factual matters

10. The trial court may award reasonable attorney's fees and litigation costs if the plaintiff has substantially prevailed in litigation under the FOIA

11. The FOIA provides that, in certain narrowly prescribed circumstances, agency employees who act arbitrarily or capriciously in withholding information may be subject to disciplinary action

12. A "reverse" FOIA action is one in which the submitter of information (such as a business) seeks to enjoin an agency from releasing that information in response to a third-party FOIA request

    a. Such "reverse" actions cannot be based on the FOIA or the Trade Secrets Act

    b. The action may be brought under the Administrative Procedures Act

5. THE FEDERAL PRIVACY ACT

With the passage of the Privacy Act, 5 U.S.C. 552a, Congress gave a comprehensive statutory recognition to privacy. The Act extends a premise of the FOIA: That government, in its role as custodian of information, is accountable to those it serves. Both acts provide for access to government records. The difference, however, is that the FOIA is designed to be used by individuals seeking many kinds of government agency records while the Privacy Act is intended to *assist individuals in obtaining information about themselves.*

The Privacy Act—*Defined*:

> Legislation which allows an individual to review almost all Federal files (and state files under the auspices of the respective state privacy acts) pertaining to him/herself; places restrictions on the disclosure of personally identifiable information; specifies that there be no secret records systems on individuals; and compels the government to reveal its information sources.

A key element of the Privacy Act is that it gives the individual significant control over how information concerning him/her is used. With certain exceptions, it specifies that records containing personal information about individuals be disclosed to others only with the consent of the individual to whom the record pertains. As with the FOIA, civil remedies are available if an agency refuses access or declines to amend or correct a file.

The *essential difference between the FOIA and the Privacy Act* is that the latter **requires the disclosure of records** containing personal information to the individual who is the subject of the record but **restricts the disclosure** of these records to others. Conversely, the FOIA requires that all types of information be released to anyone making a request provided that (among other exemptions) it does not violate the privacy of any individual.

A. Provisions of the Privacy Act which controls the collection and use of information about individuals

1. It requires agencies to publicly report the existence of all systems of records maintained on individuals

2. It **requires** that *information contained in agency record systems* be:

   - Accurate
   - Complete
   - Relevant
   - Current

3. It provides procedures whereby individuals can inspect and correct inaccuracies in almost all Federal files about themselves

4. It specifies that information gathered about an individual for one purpose cannot be used for another without the person's consent

5. It requires agency's to keep an accurate accounting of the disclosure of records and, with certain exceptions, make these disclosures available to the subject of the record

B. Sanctions are included in the act to enforce these provisions

C. Information available under the Privacy Act:

1. Applies only to *personal records maintained by the executive branch* of the Federal government concerning individual citizens

2. State privacy laws generally apply to personal records in the executive branch of the state government and records held by local government executive agencies

3. The federal act *does not apply* to:

   a. State government records

   b. Local government records

   c. Records of private organizations

4. Federal agencies covered by the Privacy Act include executive departments and offices, military departments, government corporations, government controlled corporations, and independent regulatory agencies

5. Individualized files held by these agencies records' systems must be made available to the individual subject of the record upon request, subject to specified exceptions

6. Only U.S. citizens and lawful resident aliens may make records requests under the Privacy Act

D. Under the Privacy Act, a system of records is—*Defined*:

> A group of records from which information is retrieved by reference to a name or other personal identifier such as a social security number.

E. Exemptions from the Privacy Act mean that certain systems of records may be exempted from disclosing records—such exemptions are classified under the act as being either "general" or "specific"

1. **General exemptions** - these agencies' records can be exempt from more provisions of the act than those maintained by other agencies

   a. These apply only to the Central Intelligence Agency (CIA) and criminal law enforcement agencies

   b. These agencies are subject to certain basic provisions:

      1) The *existence* and *characteristics* of all records systems must be *publicly reported*;

      2) Subject to specified exceptions, *no personal records can be disclosed to other agencies or persons* without the prior consent of the individual to whom the record pertains

      3) All *disclosures* must be *accurately accounted* for

      4) Records which are disclosed must be *accurate*, *relevant*, *current*, and *complete*

      5) No records *describing how an individual exercises his/her First Amendment rights can be maintained* unless such maintenance is authorized by statute or by the individual to whom it pertains or unless it is relevant to and within the scope of an authorized law enforcement activity

   c. General Exemption (j) (1) covers files maintained by the CIA essentially due to information being classified on grounds relating to *national security*

d. General Exemption (j) (2) refers to files maintained by federal criminal law enforcement agencies

1) Specifically, the exemption applies to:

a) Records maintained by police/law enforcement agencies,

b) Prosecuting attorneys offices

c) Corrections agencies including probation, pardon, and parole

2) Moreover, to be exempt, the records of those agencies must consist of ...

a) Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and probation and parole status;

b) Information compiled for the purpose of criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or

c) Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision

2. **Specific exemptions** - there are seven specific exemptions which apply to all agencies

a. Exemption (k) (1) - Classified documents concerning national defense and foreign policy

b. Exemption (k) (2) - Investigatory material compiled for law enforcement purposes—under certain conditions this exemption may not be used if the records are used to deny a person of a benefit, right, or privilege entitled by federal law

c. Exemption (k) (3) - Secret Service intelligence files

d. Exemption (k) (4) - Files used solely for statistical purposes

e. Exemption (k) (5) - Investigatory material used in making decisions concerning federal employment, military service, federal contracts, and security clearances

f. Exemption (k) (6) - Testing or examination material used solely for employment purposes

g. Exemption (k) (7) - Evaluation material used in making decisions regarding promotions in the armed services

F. Miscellaneous factors of the Privacy Act

1. Upon request from a subject, an agency is required to inform the requester whether they have files on the individual, however, the substance of those files may be exempt from disclosure

2. Requests can be made by individuals either in writing, by telephone, or in person

3. Most agencies require proof of identity before the release of records

4. Anyone who "knowingly and willfully" requests or receives access to a record about an individual "under false pretenses" is subject to criminal penalties

5. The Privacy Act permits agencies to charge fees to cover actual costs of copying records but are not allowed to charge for time spent in locating records or preparing them for inspection

6. The Privacy Act imposes no time limits for agency responses to requests, however, the judicial history indicates that the time for response should be "reasonable"

7. Records that are released must be in a form that is "comprehensible" to the requester

8. Generally, records may be either examined in person or a copy may be made

6. RICO—RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS AND CONTINUING CRIMINAL ENTERPRISES

The federal RICO statute was enacted as Title IX of the Organized Crime Control Act of 1970 (18 U.S.C. Sections 1961-1968). The statute provides civil and criminal penalties for persons who engage in a "pattern of racketeering activity" or "collection of an unlawful debt" that has a specified relationship to an "enterprise" that affects interstate commerce.

A. *Definitions*:

Racketeering activity - state felonies involving murder, robbery, extortion, and several other serious offenses, and more than thirty serious federal offenses including extortion, interstate theft offenses, narcotics violations, mail fraud, and securities fraud

Enterprise - includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity

Pattern of racketeering activity - consists of two or more of the defined state or federal crimes within a statutorily prescribed time period

Unlawful debt - is a debt that arises from illegal gambling or loansharking activities

B. Laws passed on these crimes—both at the federal and state levels—are intended to establish a basis for prosecution of persons who either:

1. Infiltrate or integrate criminal wrong-doing and racketeering with "legitimate" business enterprises, (RICO) or

2. Involved in on-going criminal activity over an extended time period rather than one or a series of independent crimes (Continuing Criminal Enterprise)

C. Continuing Criminal Enterprise

1. *Defined*:

> Any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity which are involved in a continuing or perpetuating criminal event.

2. **EXAMPLES**: Drug trafficking, gun running, White Slavery (prostitution rings), loan sharking, etc.

3. Rather than collect evidence and prosecute on one or a few criminal incidents, the statutes require the showing that many criminal incidents occur by the same principal persons who have the intent to perpetuate the criminal activity

4. Such statutes have significantly harsher penalties than individual criminal incidents

5. To establish cases on continuing criminal enterprises requires a notable time investment, careful evidence collection, and comprehensive evidence to prove the on-going nature of the criminal activity

D. RICO—The Federal Organized Crime Control Act

1. Many states have RICO statutes modeled after the federal law—examining the federal statute provides an overview

2. The essential crimes available for prosecution under the Federal RICO statute are:

   a. The acquisition of an enterprise with any income derived from an illegal activity;

   b. The illegal acquisition or maintenance of an interest in, or control of, any enterprise through criminal activity;

   c. The use of an enterprise to commit illegal activities; or

   d. A conspiracy to commit any of the above three crimes

3. As noted previously, an "enterprise" with respect to the statute ...

   a. Is not limited solely to the traditional concept of a corporation or other legal entity

   b. It may include an informally gathered group banded together to permit illegal activities

4. The illegal means involved in either acquiring or using the enterprise may include ...

   a. A pattern of racketeering activity; or

   b. The collection of an unlawful debt (such as the collection of a gambling debt or loan sharking)

5. For a RICO violation to occur, at least two offenses, connected by a common scheme or motive, must occur in order for a pattern to exist

   a. The offenses in the pattern may be of either state or federal law

   b. The key element is that the offenses must have an effect on either interstate or foreign commerce

6. Additional unique elements of RICO:

   a. Civil remedies are available to RICO victims in order for them to recover their losses to the RICO enterprise

   b. The law can be used to divest the criminals from a lawful enterprise and restore the enterprise to a lawful operation

   c. The RICO forfeiture provisions allow the government to reach the illegally accumulated assets of a criminal enterprise

      1) The intent is to strike at the heart of the enterprise eliminating its value, seizing fruits of unlawful gain, and making the continuation of the enterprise difficult

      2) RICO forfeitures may only be made pursuant to a court order following the conviction on a RICO statute

E. Federal policy on prosecution of cases under RICO recognizes that all cases meeting the "technical requirements" of the statute do not warrant such severe prosecution—furthermore, "injudicious" use of the statute would reduce its use

F. Department of Justice policy states that U.S. Attorneys should seek a RICO violation in an indictment *only if one or more* of the following requirements are present:

1. RICO is necessary to ensure that the indictment adequately reflects the nature and extent of the criminal conduct involved in a way that prosecution only on the underlying charges would not

2. A RICO prosecution would provide the basis for an appropriate sentence under all of the circumstances of the case;

3. A RICO charge would combine related offenses which would otherwise have to be prosecuted separately in different jurisdictions;

4. RICO is necessary for a successful prosecution of the government's case against the defendant or a co-defendant;

5. Use of RICO would provide a reasonable expectation of forfeiture which is proportionate to the underlying criminal conduct;

6. The case consists of violations of state law, but local law enforcement officials are unlikely or unable to successfully prosecute the case, in which the federal government has significant interest;

7. The case involves violations of state law, but involves prosecution of significant political or government individuals, which may pose special problems for the local prosecutor (SOURCE: RICO Manual for Federal Prosecutors, U.S. Department of Justice, 1988.)

G. State law enforcement officials should review comparable state policy on prosecuting continuing criminal enterprises/RICO prior to beginning an intelligence operation on a RICO case.

NOTE: Within the context of this policy, see also Chapter 9, *Targeting Crimes for Intelligence*

H. The implications for RICO statues for intelligence analysts are important—familiarity with law and policy and the evidence required for a RICO prosecution must be inherent in all aspects of the analytic activities

7. ASSET SEIZURE AND FORFEITURE SANCTIONS IN DRUG CASES

Forfeiture can be simply defined as "the divestiture without compensation of property used in a manner contrary to the laws of the sovereign" [*U.S. v. Eight Rhodesian Stone Statues*, 449 F.Supp. 193, 195 n.1 (C.D. Cal. 1978)]. The mere fact that property has been used illegally does not give the government the right to seize it. Rather, the forfeiture and processes must be specifically authorized by statute. This is done through both federal and state laws using both criminal and civil procedures. This section provides an overview of the asset forfeiture law.

A. Forfeiture refers to the legal practice of government seizure of property used in criminal activity

1. Initial forfeiture statute was a provision of the 1970 RICO law described above

2. In 1978 forfeiture statutes were expanded when Congress authorized civil forfeiture of any proceeds derived from narcotics trafficking in violation of federal law [21 U.S.C. Section 881(6)]

3. Since the initial federal RICO law every state, with the exception of Vermont, has passed state level forfeiture laws for drug-related offenses.

4. The benefits of asset forfeiture laws—whether under state or federal statutes—include:

   a. They provide another tool for prosecuting major law violators

   b. They allow for a comprehensive crippling assault on major offenders allowing their illicit investment assets to be seized

   c. Seizing and eliminating illicit business assets of major offenders strengthens the legitimate business community by reducing unfair competition

d. Seized assets can be used (and are sometimes mandated) to go to law enforcement for investigation and prosecution of other criminals

B. Crimes for which forfeitures apply

1. The federal law and virtually all states permit asset seizure in connection with illicit drug trafficking and manufacture

2. Some states permit forfeiture with drug cultivation

3. Some states also permit forfeiture with other crimes such as gambling and hazardous waste violations

C. Types of property which may be seized are based on individual state law

1. All states permit the seizure of the drugs and contraband involved

2. Other property which is seizable is defined by statute and usually includes property that was either:

a. An "instrumentality"—that is, used to commit the crime; or

b. A "fruit of the crime"; some asset obtained as a result of the criminal activity (i.e., property purchased from the proceeds of a drug transaction)

3. Common statutory provisions permit seizure of:

a. Conveyance (vehicles, aircraft, vessels) used to transport, conceal, or facilitate the crime

b. Cash used for or with the intent to be used for the purchase of drugs; or cash derived from the proceeds of an illegal drug transaction

c. Raw materials, products, and equipment used in manufacturing, trafficking, or cultivation

d. Containers used to store or transport drugs

e. Drug paraphernalia used to consume or administer the controlled substance

f. Criminal research and records, including formulas, microfilm, tapes, and data that can be used to violate the drug laws

g. Some states permit pursuit of "traceable assets" purchased from drug profits such as real estate, jewelry, personal property, etc.

D. Disposition of forfeited property

1. Most states first require that outstanding liens on property first be paid

2. Administrative costs (e.g., storing, maintaining, etc.) of forfeiture are next paid

3. Some states then require the costs of law enforcement and prosecution be reimbursed

4. Most states require that remaining proceeds and monies go into the seizing jurisdictions treasury

5. Some states stipulate the monies must go to law enforcement and cannot be used as a basis to reduce funding allocations to law enforcement

E. Forfeiture/assets seizure can be accomplished via:

1. Criminal proceedings wherein assets are seized incidental to arrest for crimes where forfeiture sanctions apply

a. Since the proceeding is part of a criminal prosecution, the burden of proof in showing that the targeted property is seizable is "proof beyond a reasonable doubt"

b. There must be a conviction of the accused and a special verdict or finding for the forfeiture

2. Civil proceedings ...

a. In civil forfeitures, the proceedings are brought against the property, rather than the "wrong-doer"

b. Evidence exists to show assets are the fruits and/or instrumentalities of criminal activity (usually drug trafficking); and

c. Civil proceedings require only a burden of proof "within the preponderance of the evidence"

F. During the course of case development via intelligence analysis, the analyst should remain aware of the statutes permitting assets forfeiture and the processes required for such forfeitures

1. The analyst may hold a key role in the ultimate decision of whether civil or criminal proceedings will be used

2. The analyst may also have the best perspective on the nature of applicable assets and directions for the investigation to maximize seizures

3. Thus, intelligence activities in cases potentially involving asset forfeitures, the analyst must keep these statutes in perspective as well as evidentiary development for criminal prosecution

8. SUMMARY OBSERVATIONS ON LAW

The purpose of this chapter was to provide an overview of legal issues with which the intelligence analyst must be concerned. *Importantly*, it must be recognized that intelligence activities have legal responsibilities which go beyond the traditional criminal law knowledge afforded law enforcement officers in training.

14. LEGAL ISSUES AND LAW ENFORCEMENT INTELLIGENCE

Instructional Support and Criteria

GOAL:

To provide an overview of selected statutory legal issues fundamental to law enforcement intelligence activities.

OBJECTIVES:

1. The student will have a general understanding of the provisions and exemptions of the Freedom of Information Act.
2. The student will have a general understanding of the provisions and exceptions of the Privacy Act.
3. The student will have a working knowledge of the Racketeering Influence Corrupt Organization Act.

STUDY QUESTIONS:

a. Generally discuss the relationship between procedural law mandates and the collection of intelligence information.

b. How might an intelligence unit be liable for the deprivation of a citizen's civil rights.

c. What is the intent of the Freedom of Information Act? How do the provisions of the the act serve to fulfill this intent?

d. Describe the intent of the Privacy Act and how that intent relates to law enforcement intelligence.

e. Why is there a need for having exemptions to the FOIA and exceptions to the Privacy Act?

f. Discuss the role of law enforcement intelligence as it relates to RICO cases.

NOTES

CHAPTER 15

MAINTAINING CONTROL OF THE INTELLIGENCE FUNCTION

"The police have a lot of power and we've got to make sure they use it legally, fairly, ethically, and with humanity."
Comment of a Police Chief to the author.

1. A PERSPECTIVE ON MAINTAINING CONTROL

This is somewhat of an eclectic section addressing issues which range from the pragmatic to the philosophical. Concern for control is essential because of the potential for abuse in law enforcement intelligence (LAWINT); the rather nondescript rules which govern LAWINT activities; the impact intelligence activities can have on citizens; and the surreptitious nature of LAWINT. All aspects of control apply to tactical intelligence (TACTINT), operational intelligence (OPINT), and strategic intelligence (STRATINT) although the applications will vary somewhat. In order to comprehensively deal with these concerns, this section addresses *four dimensions* of control:

- Evaluation of the Intelligence Process
- Quality Control of Intelligence Information
- Maintenance of Legal Standards
- Ethics and Values in the Intelligence Function

2. DIMENSION ONE: EVALUATION OF THE INTELLIGENCE PROCESS

A. Evaluation has been defined in many ways—regardless of this multiplicity it can basically be categorized as having two components:

1. **Outcome evaluation**: Are you accomplishing what you want?

2. **Process evaluation:** Are the methods for accomplishing outcomes working with maximum utility?

B. *Definitions*:

1. **Outcome Evaluation:**

> The process of determining the value or amount of success in achieving a predetermined objective through:
>
> • Defining the objective in some qualitative or quantitative measurable terms;
>
> • Identifying the proper criteria (or variables) to be used in measuring the success toward attaining the objective;
>
> • Determination and explanation of the degree of success; and
>
> • Recommendations for further program actions to attain the desired objectives/outcomes

2. **Process Evaluation:**

> The assessment of procedures used to attain objectives within the following criteria:
>
> a. Do the procedures substantively contribute to the objective?
>
> b. Do the procedures effectively utilize resources?
>
> c. Are the procedures coordinated with other elements in the intelligence process?
>
> d. Are staff members properly trained to execute the procedures?

C. Essentially, evaluation involves making comparisons between conditions—evaluative comparisons which are made in LAWINT include:

1. **"Real" versus "Expected" Outcomes** - Serves as a means to assess the accuracy of STRATINT projections and forecasts. Can be used in TACTINT to assess the accuracy of hypotheses, conclusions, and recommendations.

2. **"Before" versus "After" Status** - Examines whether the intelligence functions (either TACTINT or STRATINT) have had an impact or contributed to a change in the intelligence target or activity peripheral to the target.

3. **Comparison of Intelligence Reactions to Operations and Administrative Reactions** - Determines the consistency of perceptions and quality (value) of TACTINT and STRATINT to the expectations of administrative and operational consumers of intelligence.

4. **Contributory Value** - With respect to TACTINT, this attempts to assess the degree to which the intelligence contributed to case prosecution or other intended tactical objectives (e.g., assets forfeiture, contraband interdiction, etc.). In STRATINT, this evaluation assesses the value of STRATINT analysis in the decision-making process for resource allocation and deployment.

5. **Quality Control Assessment** - This is an overall, broad-based assessment of the utility, accuracy, general value, orientation, and need of TACTINT and STRATINT activities.

6. **Processes and Outputs** - An internal assessment of the correlation of expended efforts and procedures in comparison to the type and quality of output produced in TACINT and STRATINT analysis

D. While sophisticated evaluation techniques should be used, they should be limited to conditions and times that demand the need

1. Effective "evaluative sensing" in LAWINT can be done informally by supervisors or designated evaluators

2. When problems appear to exist, then formalized evaluation may be warranted

3. Importantly, evaluation should be viewed as a positive, constructive activity to make the intelligence function more valuable to the organization—evaluation should not be viewed as "fault-finding"

4. For informal evaluation to work, it must be performed:

   a. Purposely

   b. Routinely

   c. Comprehensively

   d. Critically

E. At the heart of any evaluative effort is the identification and assessment (measurement) of relevant variables

1. In a formal evaluation the variables must be critically selected from the particular activity being assessed

2. Informal intelligence evaluation can take a more generalized approach

F. Types of variables and questions to ask during the informal TACTINT and STRATINT evaluations include:

1. **Collection Protocols...**

   a. Are the proper or best methodologies and media being selected for the designated intelligence needs?

   b. Are personnel properly trained to utilize and interpret the data being collected via the protocol used?

   c. Are the protocols fully within the agency's capability or are resources and expertise being stretched?

2. **Information Processing...**

   a. Is collected information being adequately assessed for the contribution to the intelligence goal?

   b. Is the quality of information being adequately assessed?

c. Is too much raw, non-contributory (i.e., high interest but low utility) information being introduced into the intelligence process?

d. Is information being effectively and logically categorized and indexed?

e. Is too much or too little information being introduced into the intelligence cycle?

3. **Analysis...**

a. Are the best and most appropriate analytic techniques being used?

b. Are logical conclusions being drawn?

c. How accurate are hypotheses and interpretations?

d. Are suspected TACTINT links, associations, and commodity flows accurate?

e. Are STRATINT projections and pattern analysis proving to be "on target"?

4. **Reporting...**

a. Are the LAWINT reports being produced in a substantively understandable manner (i.e., are the interpretations and findings clear)?

b. Are the reports comprehensive?

c. Are the reports fulfilling their intended role?

5. **Intelligence Dissemination...**

a. Are the right people receiving the needed information?

b. Are investigators and decision makers receiving the information needed to fulfill their responsibilities?

c. Is the intelligence being disseminated on a timely basis?

d. Are intelligence recipients able to use the information they receive?

e. Is security of the intelligence being maintained?

6. **Personnel...**

a. Are intelligence staff members properly trained for their tasks?

b. Is there proper supervision within the unit?

c. Is the expertise of the staff sufficiently diverse to meet the intelligence unit's needs?

d. Do personnel have effective relations and communications with other organizational units which contribute to and consume LAWINT reports?

G. Among the more common problems found in intelligence unit operations which should be examined as part of the evaluation process are:

1. The unit becomes too enmeshed in daily activities with difficulty in changing procedures to respond to fast breaking or special needs.

2. Little feedback, positive or negative, is given to the intelligence unit on the quality and value of LAWINT reports—without feedback the *status quo* is maintained.

3. Commonly used methods of information collection and analysis become institutionalized with limited creativity.

a. More attention should be given to aligning the collection methods with information needs.

b. Analysts should discuss case alternatives and hypotheses among themselves and with investigators to bring in alternate perspectives.

4. In complex cases where there is disagreement about the interpretation of intelligence, the disagreements are frequently compromised in reports rather than have both positions and

supporting arguments presented in the reports for consumption by users

5. In the process of analyzing cases of a multi-jurisdictional nature there must be on-going communications with intelligence units or investigators from other participant agencies.

   a. The communications must be two-way

   b. Units must share information, thoughts, and ideas

6. Assumptions and interpretations are too frequently made based on the life experiences of the analyst.

   a. Analysts must force critical thinking of the experiences of persons from other backgrounds and cultures

   b. Introspection must be given in light of the case and individuals involved in order to challenge assumptions

7. LAWINT personnel must avoid "circularity" in facts—that is, not loose perspective and believe that earlier made assumptions are now fact.

8. It must be ensured that all personnel use words and phrases which have a consistent and clear meaning by all analysts and consumers of intelligence information.

H. In sum, evaluation of the intelligence process is to ensure that the process is:

1. **Effective**—it is accomplishing what we want it to do

2. **Efficient**—it is being effective without waste or undue expenditures of resources

3. **Accurate**—the products of the intelligence process are valid and reliable

4. **Timely**—information is being produced within time frames which make the information useful for decision making

5. **Relevant**—information is contributing to the goals of the police organization

3. DIMENSION TWO: MAINTAINING CONTROL OF INTELLIGENCE INFORMATION

The second dimension of maintaining control focuses on the quality of intelligence information. Information is the essence of all LAWINT activities. As such, the need for maintaining control of all phases of information processing and use is essential. In this regard, control of intelligence information is concerned with four elements:

- Data Quality Standards
- Records' Status (Sealing, purging, and archiving)
- Intelligence Data Format
- Security of Intelligence Information

While these issues are also part of intelligence records management as well as intelligence unit management, the importance of maintaining control of intelligence information is such that it warrants special attention.

A. Data Quality Standards

1. "Data quality" has become a significant concern in recent years as a result of:

   a. Computerization of records

   b. Lawsuits concerning information in the possession of law enforcement agencies (as well as government agencies in general)

   c. Statutory law (e.g., Privacy Act and Freedom of Information Act)

   d. The need for effective records for successful prosecutions—particularly in complex criminal cases?

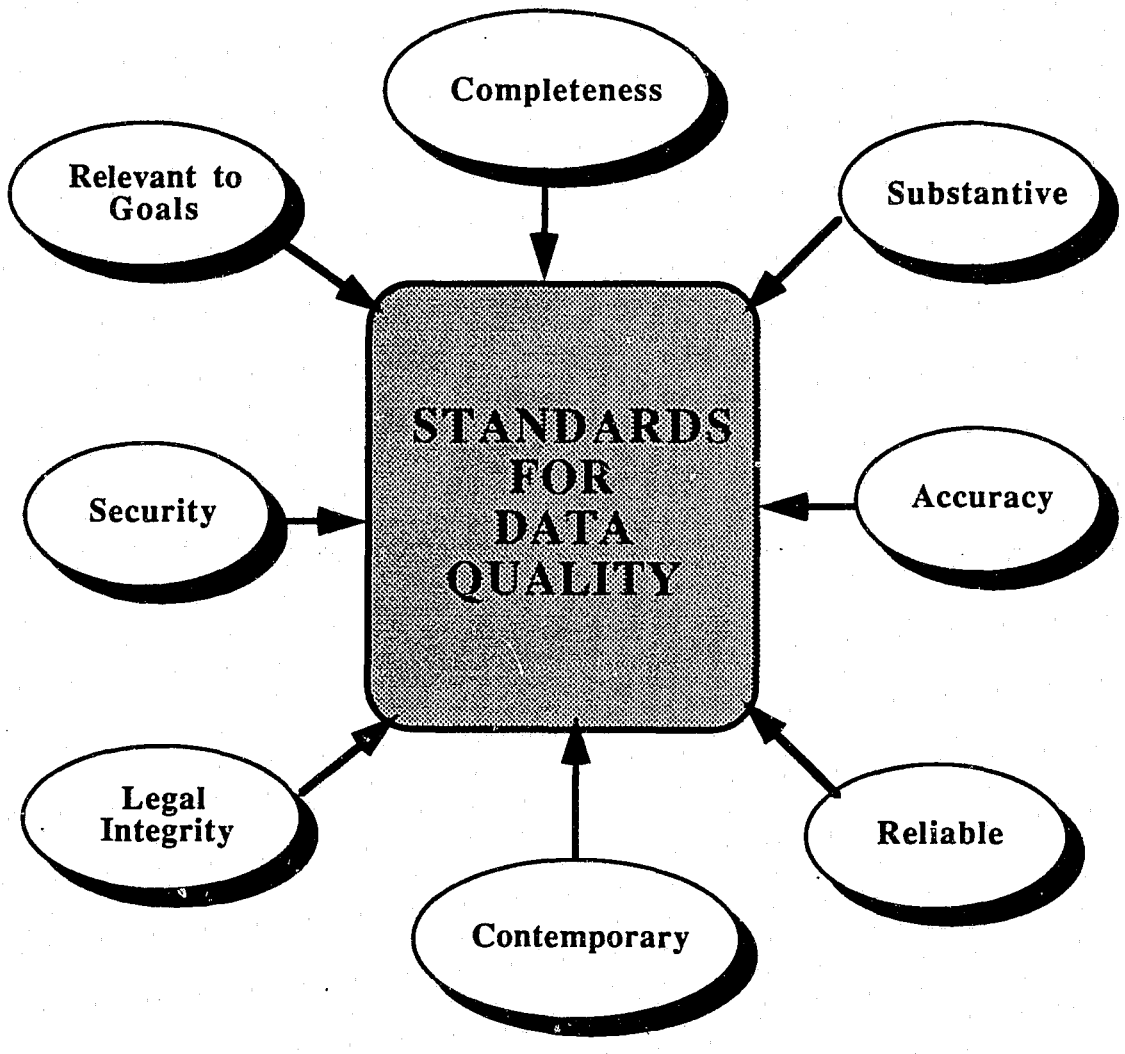
2. Data quality is concerned with several factors, including (*See* Figure XV-1):

   a. Insuring records are *complete*

   b. Insuring records are *accurate*

Figure XV-1

STANDARDS FOR DATA QUALITY



c. Insuring records are *secure* ...

1) Protected against intentional destruction or modification

2) Protected against accidental destruction or modification

3) Protection against release to unauthorized persons

d. Insuring *legal integrity* of the records is maintained

e. Insuring that records contain *substantive information*, not frivolous or irrelevant information

f. Insuring the data and information is *contemporary*

g. Insuring that the data and information is *relevant to a lawful law enforcement interest or function*

h. Insuring the *reliability of the data* or information

3. While these standards apply to all law enforcement information, it is more difficult to maintain the standards with LAWINT information because:

a. Much of the information is "raw" awaiting analysis and placement in a role affecting a case

b. Much of the information is developmental and inferential—thus its continued value and role is sometimes vague

4. Despite this difficulty, it is recommended that:

a. Agencies provide for periodic reviews of data and the destruction of any information that is misleading, obsolete, or otherwise unreliable (See BJS, 1975)

b. Information that remains in intelligence files should be corroborated to the extent possible

c. Purge information that is not...

1) Relevant

2) Accurate

3) Reliable

5. Regardless of the difficulty, it is the best interest of the LAWINT function to maintain data quality

B. **Records' Status** (Sealing, Purging, Archiving)

1. ***Archiving—Defined***:

> The maintenance of records in remote storage after a case has been closed or disposed of as a matter of contingency should the records be needed for later reference.

a. Archived records may be:

1) Paper records which are stored

2) Microfilmed records

3) Placed on computer tape or other remotely stored computer medium

b. Archiving is done because of:

1) Potential future need of the records,

2) Sometimes as a matter of historical record, and

3) The compulsive nature of law enforcement organizations

c. In reality, the need to archive records for extended periods of time meets with waste except for a few extraordinary cases

NOTE: This is particularly true with intelligence information since much of it is time-specific

d. Most agencies make their own rules about archiving, although some laws exist

1) **EXAMPLE:** The state of Alaska has a statute requiring expungement of records one year after an arrest or police investigation results favorably for an individual

2) There are other states and cities with similar laws

e. Archived records are available for later research and reference

2. ***Sealing***—*Defined*:

> Records are stored by the agency but cannot be accessed, referenced, or used without a court order based on a showing of evidence that there is a legitimate government interest to review the sealed information.

a. The circumstances under which records are sealed may be a function of:

1) Statute,

2) Policy, or

3) Court order

b. The chain of custody for sealed records must be verified

c. Records are sealed to

1) Protect the identity of people, and

2) To give people a "second chance"

3. ***Purging***—*Defined*:

> Records are removed from files and destroyed because they are deemed to be of no further value or further access to the records would serve no legitimate government interest. means records are removed and destroyed.

a. Just as in the case of sealing, the records may be purged as a result of:

1) Statute,

2) Policy, or

3) Court order

b. The obvious difference is that there is a legal or factual basis to believe that future access to the records would be useless or inappropriate

4. Perhaps the best—and most conservative—standards to evaluate intelligence records on these criteria comes from *Paton v. LaPrade* 524 F.2d 862 (3rd Cir. 1975): The appellate court's finding stated ...

The benefits to the government to maintain records must be held in relationship to the subject's rights with respect to:

a. The accuracy and adverse nature of the information

b. The availability and scope of dissemination;

c. The legality of the collection methods;

d. The existence of relevant statutory standards to have such records; and

e. The value of the information to the government (e.g., Can a compelling state interest be shown?)

5. Administrative policies and procedures must be established and enforced to control intelligence information through archiving, sealing, and purging

C. Intelligence Data Format

1. Format deals with the media on which the details are recorded

2. Format includes:

a. Paper records

1) Formal or official records

2) Informal or unofficial records

b. Computer and machine readable forms

c. Microforms

d. Audio and video record storing media

3. Format is important for maintaining control of records because of the accessibility to the information

ISSUES:

a. Access to computer intelligence records should be restricted to LAWINT personnel

1) Computer records stored on remote media (e.g., tape, disks) should have special security access

2) Security protocols for access to intelligence records should be unique, not have general accessibility

b. Access to formal records of the intelligence unit should be controlled by:

1) Physical security, and

2) An access policy stating who may have access, the conditions for access, and the chain of custody/accountability of records

c. Policy should also exist for "informal" intelligence records

1) These generally include notes, thoughts, and observations kept by LAWINT personnel

2) They are critical because they may contain accusatory information or information which cannot be released

3) Such informal records typically have no formal controls and are kept in the custody of the individual analyst/officer

4) While it is difficult to stipulate restrictive policies and procedures for individual writings, some control mechanisms should be in place dependent on the nature of the information and unique characteristics of the agency

D. Security of Intelligence Information

1. As inferred above, security of intelligence information is important because:

   a. Intelligence information, per se, is frequently inconclusive

   b. Insecure intelligence information could be damaging to a person's character (defamation)

   c. Insecure intelligence could lead to problems in case building if obtained by the targets

2. It would be advisable for LAWINT to develop security methods which will control:

   a. Access

   b. Alteration to records/information

   c. Misuse of records/information

   d. Provide a "damage assessment" if secure information is released

4. DIMENSION THREE: MAINTENANCE OF LEGAL STANDARDS

While specific issues of law and legal procedure are discussed elsewhere, the importance of this issue deserves special emphasis. It cannot be over-stressed that the integrity of the intelligence unit—and its ultimate effectiveness—is directly correlated to the maintenance of legal standards. Unfortunately, there is still a tendency in some cases to claim that the "means is justified by the end." This is compounded when the law enforcement agency tolerates some of the legal abuses. Thus, the need for maintaining control of legal processes becomes an important issue.

A. Lawful information collection is an inherent need in order to:

1. Maintain the integrity of citizens' rights

2. Be able to use the information in court as necessary

3. Protect analysts, investigators, and the agency from liability

B. Concern for lawful collection and control of information is evidenced by the history of problems experienced by the law enforcement intelligence function

C. Legal controls can be viewed in terms of substantive and procedural due process—*Definitions*:

1. **Due Process**

> Fundamental fairness during the course of the criminal justice process, includes adherence to legal standards and the civil rights of the police constituency; the adherence to principles which are fundamental to justice.

2. **Substantive Due Process**

> Guarantees persons against arbitrary, unreasonable, or capricious laws and it acts as a limitation against arbitrary governmental actions so that no government agency may exercise powers beyond those authorized by the Constitution (Lewis and Peoples, 1978).

a. While typically not a direct concern of LAWINT, the knowledge of substantive due process is important for understanding the parameters of due process law

b. For example, there have been cases of municipal ordinances and some state laws which permitted the collection of intelligence information on "suspicious persons"

1) Such laws are typically violative of substantive due process

2) The violation, depending on how the law is written, is based on either that the law was "overbreadth" or "void or vagueness"

3. **Procedural Due Process**

> Mandates and guarantees of law which ensure that the procedures employed to deprive a person of life, liberty, or property during the course of the criminal justice process meet constitutional standards.

a. For example, with respect to LAWINT:

1) It ensures that property and evidence seized by the police is consistent with Fourth Amendment standards

2) It ensures incriminating statements are made within the confines of Fifth Amendment guarantees

b. Procedural due process is of particular importance during intelligence collection

D. The due process issues are fundamental to all legal processes associated with LAWINT whether the issue is statutory (e.g., releasing information under the Freedom of Information Act) or a matter of case law (e.g., not violating a person's reasonable expectation of privacy)

E. In LAWINT it is difficult to maintain rigid control of legal standards because of (*See* Figure XV-2):

1. The *surreptitious or secret nature* of many intelligence activities

2. The *working autonomy* of analysts and investigators

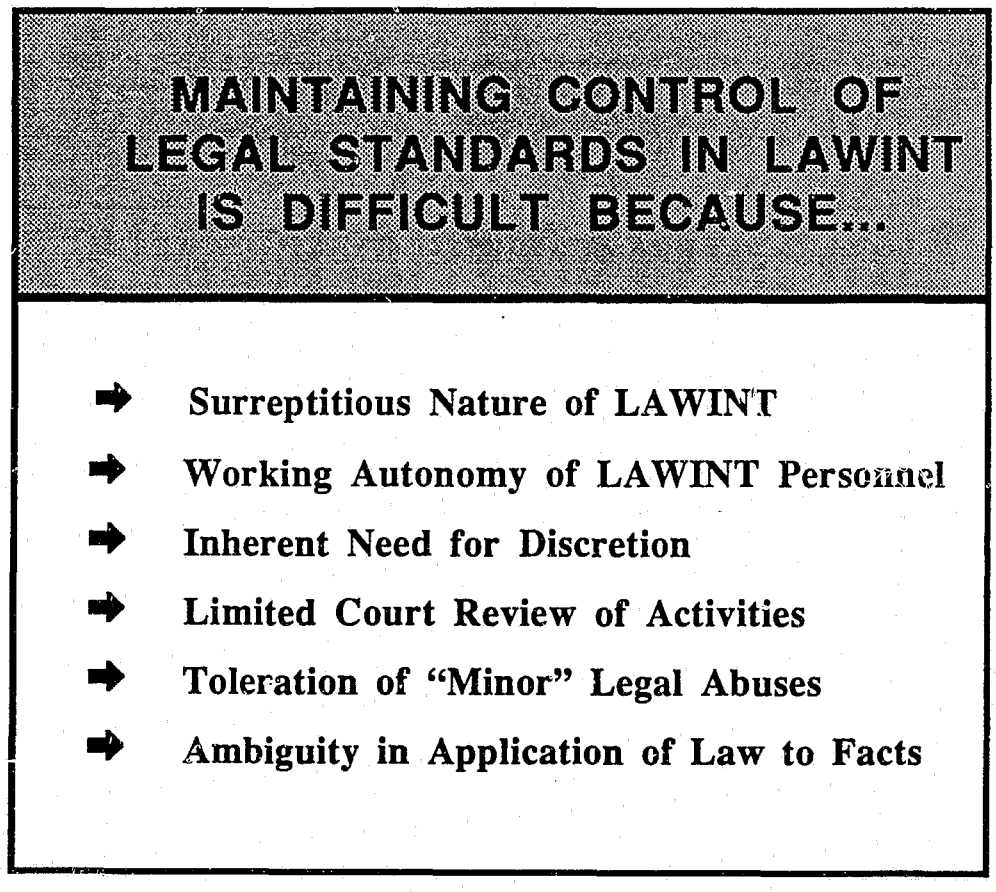
3. *Discretion* inherent in law enforcement activities

4. The *limited court review* of many LAWINT activities

5. The tendency of law enforcement to *tolerate "minor" legal abuses*, particularly in an investigation of a "known" criminal

Figure XV-2

LEGAL CONTROL LIMITATIONS OF LAWINT



6. The *inherent ambiguity* when attempting to apply the concepts of case law to factual situations

F. Adherence to legal standards can be assessed via:

1. Policies requiring self-evaluation of activities

2. Observations of activities of subordinates by intelligence supervisors

3. Careful, substantive report review

4. Examination of evidence in intelligence case files to determine the nature and amount of evidence/information which cannot be admitted in court

G. Proactive legal controls may include:

1. Having training sessions, reinforced by policy, emphasizing the importance of legal integrity

2. Taking administrative/disciplinary action against personnel who violate policies and procedures on matters of legal integrity

3. Establish an authorization protocol for information collection

4. Enhance supervision in the LAWINT unit, particularly on collection activities

5. Administrators and managers must directly affirm their support of legal integrity regardless of the nature of the case or the suspected criminal

6. In-service training should be provided as a refresher and to provide updates with respect to criminal law and procedure and legal issues of particular unique application to LAWINT

5. DIMENSION FOUR: ETHICS AND VALUES IN THE INTELLIGENCE FUNCTION

Because of the intrusive and frequently surreptitious nature of intelligence, the notable absence of definitive rules for intelligence collection, and the subjective nature of the analytic process, the potential for abuse clearly

exists. In many cases, abuse may occur within the technical parameters of the law—the so-called "letter of the law"—however, the actions of the personnel and their propriety from an operational perspective may be subject to debate—notably on issues concerning the "spirit of the law." As a result of the ever-present potential for abuse, not to mention the legacy for intelligence abuses in the 1960s and 1970s, it is essential that some form of "moral control" be part of the intelligence unit's operating philosophy. As such, ethics and values should be inculcated as obligations inherent in the total operation of the intelligence unit.

NOTE: Ethical factors are inherent in the value-based philosophy described in Chapter 3)

A. Ethics—in summary—addresses the moral propriety of our actions

B. The ethics in one's work deals with the philosophy and beliefs relied on when:

   1. Making decisions

   2. Using discretion

   3. Interpreting and applying the law

   4. Interpreting and applying organizational policies, procedures, and rules

C. All ethical principles are founded in philosophies which are moral, legal, and social in character

   1. This means that these differing factors must be balanced to derive the "right" decision in a situation

   2. Determining the "right" decision in law enforcement is difficult because there may be a conflict between:

      a. What is "legally right"

      b. What is "morally right"

3. **EXAMPLE:**

   a. You are investigating an organized crime case where the suspects are involved in drug trafficking, extortion, and murder

   b. You receive a fairly reliable tip that the suspects are going to order the murder of someone, however, no further information is received

   c. The only way you can see to obtain additional information is to electronically eavesdrop on the suspects, however, you do not have sufficient legal grounds to get a court order, *what do you do*?

      1) Adhere to the legal mandate and protect the suspects' rights by not eavesdropping?

      2) Violate the suspects' rights and unlawfully eavesdrop with the sole purpose of obtaining information about he "hit" to save the victim's life?

      3) Would your decision be affected by whether the intended victim was a citizen who witnessed something as opposed to the "hit of a drug dealer"?

4. How do you justify your answer? Are you comfortable with your decision?

D. There are no easy answers to our ethical dilemmas

   1. Ethical direction does not exist in policies and procedures

   2. Ethical direction does not exist in law: In the above example, law *compounded* the dilemma

E. Some ethical guidance, although limited, is provided in the Law Enforcement Code of Ethics (*See* Figure XV-3)

Figure XV-3

LAW ENFORCEMENT CODE OF ETHICS

As a law enforcement officer, my fundamental duty is to serve mankind; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against violence or disorder; and to respect the Constitutional rights of all men to liberty, equality, and justice.

I will keep my private life unsullied as an example to all; maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed in both my personal and official life, I will be exemplary in obeying the laws of the land and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided in me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, animosities, or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or ill will, never employing unnecessary force or violence and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith, and I accept it is a public trust to be held so long as I am true to the ethics of the police service. I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession ... law enforcement.

1. The Code of Ethics...

> "is a pledge [to be made by each law enforcement officer] to discharge fundamental law enforcement duties to the best of ability, to conduct personal affairs so as to reflect credit on one's Department, to enforce the law impartially, and to recognize the public trust implied in the job." (Felkenes, 1984:212)

2. While the Code of Ethics is somewhat superfluous it nonetheless provides some standard of ethical behavior for LAWINT by stipulating, among other things:

   a. Adherence to Constitutional standards

   b. Pursuance of criminals for prosecution

   c. Courteous and "appropriate" enforcement of laws

   d. Maintenance of confidentiality

F. Ethical dilemmas often surface when there is conflict between "legal rights" and "moral rights"

1. In the pursuit of "justice" there is frequently the belief that the "means is justified by the end" if it is to get the criminals "off the street"—ridding a criminal from society supports our moral rights of the community to be "crime-free"

2. However, if the suspect's rights are violated not only is there a violation of legal rights but also a violation of the moral philosophy of our democratic society

G. Areas of ethical concern in LAWINT frequently include:

1. Surveillance and intelligence of a person merely suspected of unlawful behavior simply due to their:

   a. Lifestyle

   b. Political philosophy

c. Behavior that is incongruent with accepted social norms but is not unlawful

2. Unlawful surveillance methods on "known criminals" notably violating a person's reasonable expectation of privacy

3. Maintaining unauthorized intelligence files whether they are part of LAWINT unit's records' system or, even more problematic, "private" files the analyst/investigator keeps

4. "Deceptions" in the law enforcement process, such as:

   a. Deceptions during investigative interviews

   b. Use of "storefronts" to lure in thieves who seek to sell stolen property

   c. Undercover operations and the borderline issues of entrapment (e.g., ABSCAM)

   d. Perjury during a trial notably to convict a "known criminal"

5. Misleading public information (disinformation) to:

   a. Avoid publicity of a problem

   b. Avoid publicity on a matter the "public would not understand"

   c. Avoid tipping criminal suspects that they are under investigation

H. Realistically, one must consider both the moral and legal ramifications

I. Marx (1988) discusses the "complexity of virtue" in using undercover operations and, by extension, the intelligence process

   a. In discussing these issues he attempts to provide a "compass, not a map" to aid in ethical decision making

   b. This analogy refers to the fact that such decisions are subjective and qualitative—definitive procedures to follow cannot be given (i.e., the map), but general guidelines for direction can be presented (i.e., the compass).

c. These principles are presented in modified form in Figure XV-4.

J. Some police organizations have opted for adopting organizational values

1. With values the police department must infuse a belief system among its officers to accept certain responsibilities and standards of conduct as being proper

2. Importantly, the process of inculcating values cannot be coercive, rather it must be consensual

3. To be effective it is a long term process which integrates ethics, the departmental mission, professional responsibility, fairness, due process, and empathy

4. Subscribed values enhance the quality of organizational life not only because of their "moral" implications but also because they induce people to behave in a certain manner because it is "right"

5. Compliant behavior—subscribing to the values—is far more desirable than complete reliance on negative control mechanisms (i.e., the threat of the disciplinary process)

6. Figure XV-5 has an illustration of the values statement of the Newport News, Virginia Police Department

   a. Among the values stipulated by the department, with respect to personnel behavior are:

      1) Protecting and preserving citizen rights

      2) Aggressively pursuing criminals

      3) Police personnel integrity and community trust

   b. These values, as well as others, have direct implications for LAWINT

   c. While not providing personnel with decisions in critical situations they do provide guidance and a statement of the department's position on various issues

Figure XV-4

A "COMPASS" OF ETHICAL GUIDELINES FOR INTELLIGENCE OPERATIONS

Seriousness: Does the seriousness of the crimes warrant the methods and resources being used?

Alternatives: What alternate means could be used to accomplish the crime control goals?

Spirit of the Law: Are the means being used consistent with the spirit of the law as well as the letter of the law?

Prosecution: Is the goal of the intelligence activity to prosecute criminals or simply gain information? If the latter, does this goal warrant the means being employed?

Crime Occurrence: Are there reasonable grounds for concluding that the crime that occurs is not a product of the undercover or intelligence intervention?

Grounds for Suspicion: Are there sufficient grounds to believe that the intelligence target has been involved in criminal activity?

Prevention: Are there grounds to believe that the investigation will prevent future crimes from occurring?

Autonomy: How much supervision will investigators have in their decisions relating to the progression of the investigation?

Degree of Deception: Do the tactics to be employed involve a minimal or extensive degree of deception? Is the degree of deception only that which is necessary to carry out the investigation?

Privacy and Expression: Will use of the information collection methods sufficiently respect the sanctity of private places, intimate and professional relations, and the right to freedom of expression and action?

Collateral Harm: How great is the potential for exploitation, corruption, perjury, or abuses and harm to the police, informers, and unwitting third parties? Can these be adequately controlled and compensated for?

Equitable Target Selection: Are the criteria for target selection equitable, free of bias based on lifestyle, race, ethnicity, religion, and political belief?

Realism: Do the tactics represent, to the degree possible, real world scenes and interactions?

Relevance of Charges: Are the charges to be brought against a target directly connected to criminal harm or are they merely procedural violations?

Actors: To what extent are sworn police officers being used as opposed to informers?

J. An important axiom, borrowed from medical ethics, which can be used in ethical decision making in LAWINT is "do no harm"

6. CLOSING OBSERVATIONS

Much of this section has had a caustic tone dealing with the potential for abuse in LAWINT. The reason for that tone is ingrained in the history of intelligence. It is assumed that most intelligence staff members will earnestly perform their work in an attempt to deal with crime problems and criminals within the charge of the unit. In the zeal of working on a case and recognizing the wide array of criminal activity in which intelligence targets may be involved, it becomes too easy to take "short cuts" in case development. Most LAWINT personnel recognize this at some point in their persona, however, the need to be reminded of the importance of "maintaining control" still exists. Had such concerns been exercised in the 1960s and 1970s, LAWINT may not have the controversial legacy and the difficult task of rebuilding that it is currently experiencing.

Figure XV-5

NEWPORT NEWS, VIRGINIA POLICE DEPARTMENT STATEMENT OF VALUES

VALUE #1—The Newport News Police Department is committed to protecting and preserving the rights of individuals as guaranteed by the Constitution.

VALUE #2—While the Newport News Police Department believes the prevention of crime is its primary responsibility, it aggressively pursues those who commit serious offenses.

VALUE #3—The Newport News Police Department believes integrity and professionalism are the foundation for trust in the community.

VALUE #4—The Newport News Police Department is committed to an open and honest relationship with the community.

VALUE #5—The Newport News Police Department is committed to effectively managing its resources for optimal service delivery.

VALUE #6—The Newport News Police Department is committed to participating in programs which incorporate the concept of a shared responsibility with the community in the delivery of police services.

VALUE #7—The Newport News Police Department actively solicits citizen participation in the development of police activities and programs which impact their neighborhood.

VALUE #8—The Newport News Police Department believes that it achieves its greatest potential through the active participation of its employees in the development and implementation of policies and programs.

VALUE #9—The Newport News Police Department recognizes and supports academic achievement of employees and promotes their pursuit of higher education.

15. MAINTAINING CONTROL

Instructional Support and Criteria

GOAL:

> To provide an overview of the types of technologies which are currently available or are emerging to support the effective use of tactical and strategic law enforcement intelligence.

OBJECTIVES:

1. The student will have a general understanding of a wide range of technologies which can be used for information collection, storage, analysis, and retrieval in the performance of the intelligence function.

2. The student will have a working knowledge of computer-related issues and concerns for LAWINT including applications, security, and viruses.

3. The student will be able to distinguish between information and statistical systems, their roles in LAWINT, their applications, general differences in legal standards for each type of system, and have a working knowledge of examples of the various system types.

STUDY QUESTIONS:

a. Distinguish between "process evaluation" and "outcome evaluation" and their roles in maintaining control of the intelligence function.

b. "For informal evaluation to work, it must be performed purposely, routinely, comprehensively, and critically." Discuss the meaning of this statement as it relates to LAWINT.

c. Describe what is meant by "data quality" and the importance of data quality with respect to (a) intelligence effectiveness and (b) maintenance of citizens' rights.

d. Discuss the issues associated with the need for security of *intelligence* information.

e. In your own words, describe the difference between *substantive* and *procedural* due process.

f. What is the role of ethics in the law enforcement intelligence function?

NOTES

APPENDIX A
SAMPLE LINK ANALYSIS

This illustration is to show how a link analysis is used in intelligence analysis. The contents herein are not meant to be a comprehensive analysis of a case, rather they serve as an illustration of the processes and elements used in the analysis component of the intelligence cycle with specific attention to diagrammatic analytic techniques.

The case presented is completely hypothetical. The crime, names of individuals, names of companies/corporations, addresses, and phone numbers have been randomly selected for this illustration. Similarly, the facts and hypotheses described are contrived simply for instructional purposes. Any similarities to real persons, companies, and/or events are completely accidental and unintended.

Attachments to this Handout are (in order):

1. A description of the *crime problem* being analyzed.

2. Two *association matrices* illustrating links between organizations.

3. A *link analysis* between persons and organizations based on the association matrices and other evidence collected and analyzed by the intelligence unit.

4. A statement of the *summary hypothesis* and, from the analysis, a *conclusion*, *prediction*, and *estimate*.

5. The *process hypotheses* used to develop the summary hypothesis.

6. A *commodity flow* diagram illustrating the process hypotheses.

THE CRIME PROBLEM AT ISSUE:

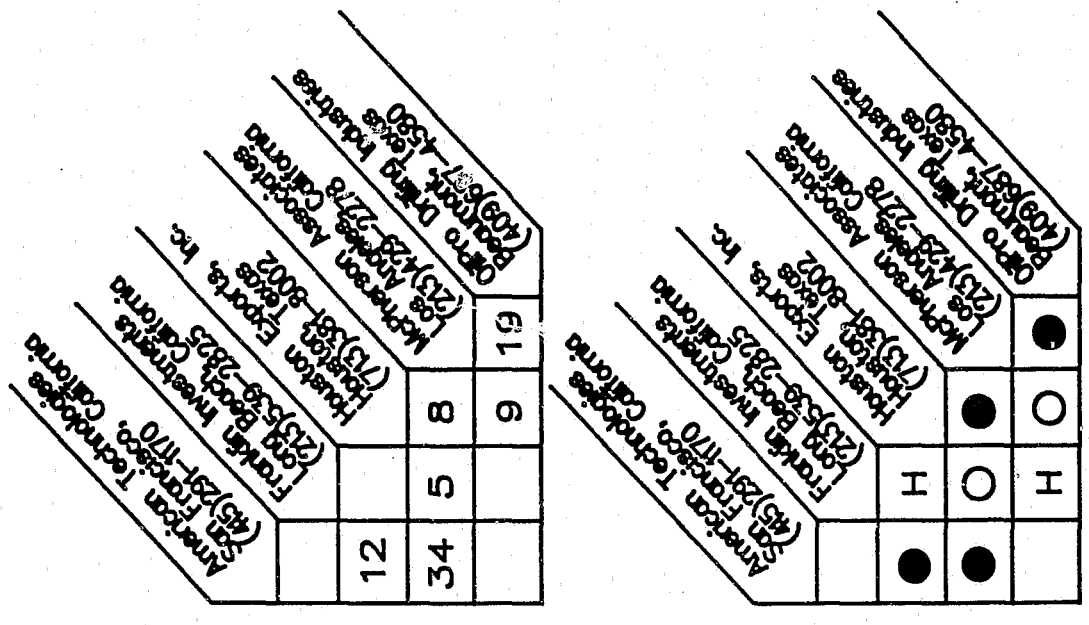
It is unlawful to sell certain forms of high technology items to Soviet bloc countries because of the potential for those technologies to be used in weaponry, military equipment, and intelligence activities. Since such technologies are in high demand and their trade is forbidden, the black market sale of high technology materials yields high profit.

Information received through a wide variety of generally reliable sources have indicated that a man named **FRANK WHITE** may be deeply involved in the sale of high technology to Soviet bloc countries. Preliminary intelligence indicates that **WHITE** uses an elaborate multi-corporate scheme which includes independent brokers, international monetary exchange and laundering, and fraudulent sales and shipping manifests to make the sales and earn substantial profits.

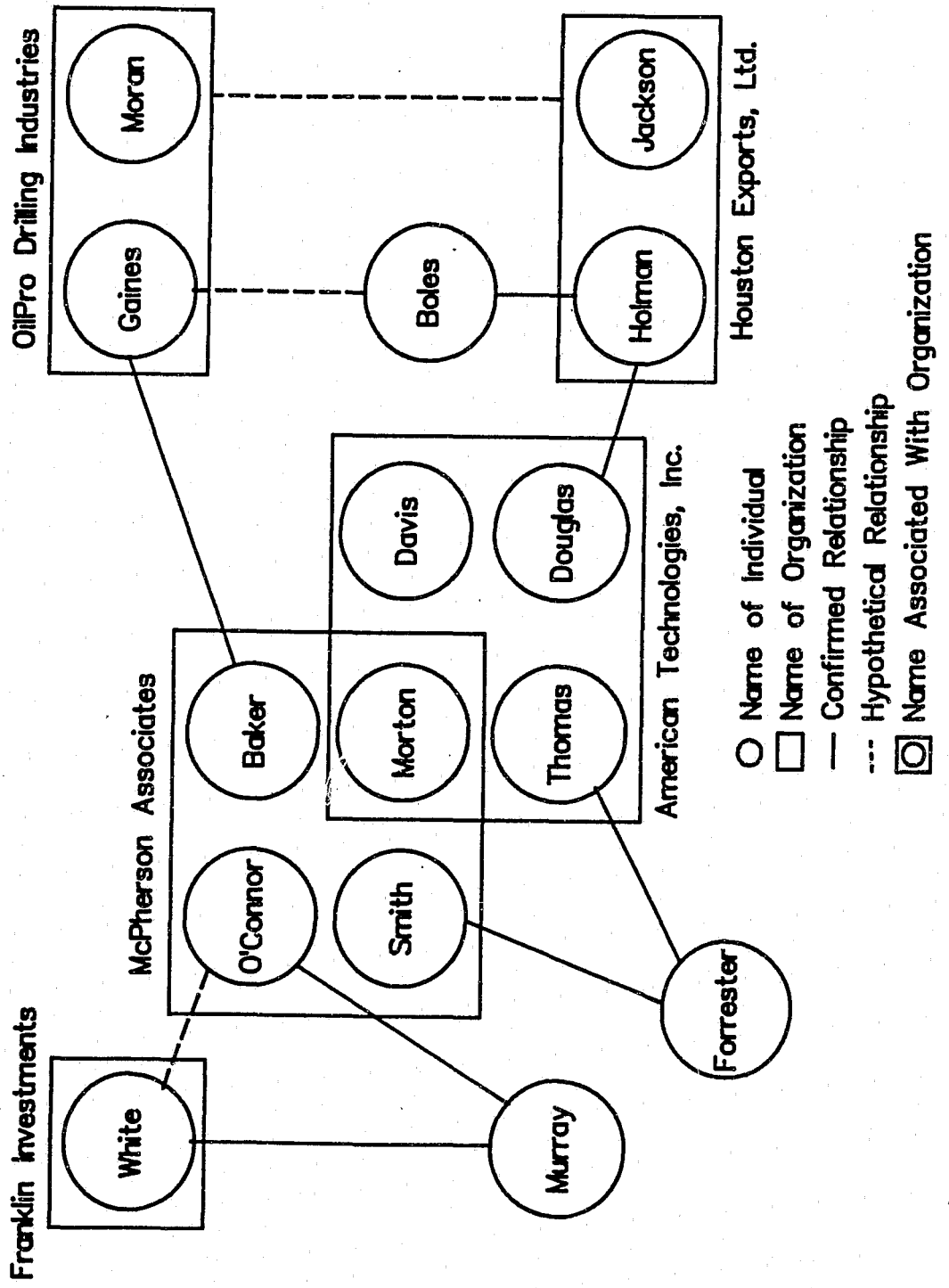
It appears that the companies involved have legitimate business enterprises, however, there are key figures in the top corporate structure of each company which knows of the scheme, helps facilitate the sales, and reaps profits from the illicit high tech sales.

Analysis of a wide variety of business reports, telephone calls, government reports, and associated materials produced the results contained herein.

ILLUSTRATIONS OF ASSOCIATION MATRICES



ILLUSTRATIONS OF LINK DIAGRAM



PROCESS HYPOTHESES

NOTE: A "process hypothesis" represents a hypothesized link, procedure, or behavior throughout a criminal enterprise which is the basis for the logic to make summary hypotheses, conclusions, estimates, and/or predictions.

1. **FRANKLIN INVESTMENTS** (wholly owned by **FRANK WHITE**) makes substantial "investments" through independent broker **MURRAY.**

2. **MURRAY** invests **FRANKLIN's** money in a diversified holding and distribution company called **McPHERSON ASSOCIATES.**

3. **McPHERSON** purchases a wide variety of materials including high technology computers, microcomputer chips, and components from **AMERICAN TECHNOLOGIES, INC.**

4. **McPHERSON** sells the high technology materials to **OILPRO DRILLING INDUSTRIES** for the stated purposes of manufacturing a wide range of oil seismology, drilling, and production equipment.

5. **OILPRO** sells contraband high technology (computers, chips, and components) under disguise and false bills of lading labelled "oil exploration and production equipment".

6. Because the cost of the contraband high technology is more than the manifest of oil supplies, the Soviet bloc countries pay **OILPRO** in German marks through an established and diversified rollover account at the Bank of Switzerland.

7. **HOUSTON EXPORTS, LTD.** has access to the Swiss account through their wide range of international businesses.

8. **HOUSTON EXPORTS** withdraws the Soviet money in dollars and converts the money to cash through a wide range of currency exchange houses and duty free stations.

9. Cash payments are made to **AMERICAN TECHNOLOGIES** for the high technology merchandise sold to **McPHERSON ASSOCIATES** plus "bonuses".

10. The cash is further transferred to **McPHERSON ASSOCIATES** for their "investment bonus" through intermediary investment broker **FORRESTER.**

11. **McPHERSON ASSOCIATES** pays cash dividends to investment broker **MURRAY** who in turn pays **FRANKLIN INVESTMENTS** its "dividends".

RESULTS OF THE ANALYSIS

Summary Hypothesis...

> "**FRANK WHITE** of **FRANKLIN INVESTMENTS**, invested, planned, and finances the entire purchase and distribution network involving unlawful sale of high technology microcomputer chips and components to Soviet bloc countries."

Conclusion...

> "**FRANK WHITE** sells sensitive microcomputer chips and components to Soviet bloc countries using legitimate front companies."

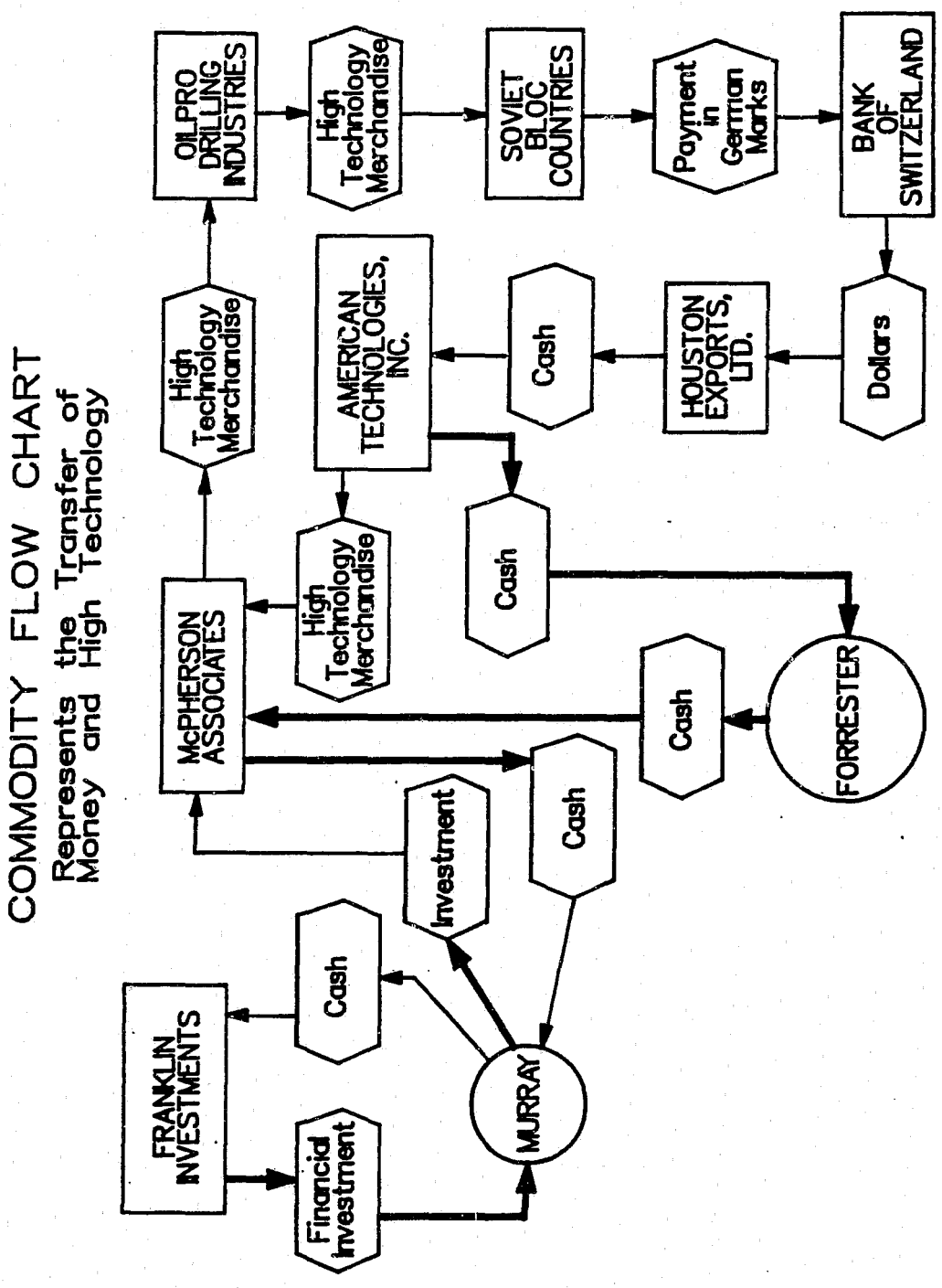
Prediction...

> "A change in the shipment of microcomputer chips and components will be routing through the Port of Houston mixed with overseas oil drilling equipment supplies instead of through the presently used Ports of New York and Los Angeles."

Estimate...

> "**FRANK WHITE**'s illegal gross income from sale of microcomputer chips to Soviet bloc countries is estimated to be $8.5 to $10 million during the next 12 months."

ILLUSTRATIONS OF A COMMODITY FLOW CHART



NOTES

APPENDIX B

ACCREDITATION STANDARDS FOR INTELLIGENCE UNITS

FROM: Commission on Accreditation, *Standards for Law Enforcement*, "Chapter 51: Intelligence"

As intelligence relates to law enforcement agencies, it is an activity principally concerned with collecting, processing, and disseminating information in specified problem areas. These areas of concern vary widely among law enforcement jurisdictions but typically include the following:

- Organized crime activities
- Subversive activities
- Vice activities
- Terrorism
- Civil disorders

Ordinarily, the intelligence component should not perform enforcement activities but should be a source of information to operational units.

The standards in this topical area address the basic concerns of a law enforcement agency in carrying out the intelligence functions. The standards do not include the intelligence-gathering activities associated with special events experienced in routinely scheduled activities such as sporting events or visiting dignitaries.

These standards are presented in the four major areas of administration, operations, personnel, and facilities and equipment as they related to the intelligence function.

51.1 Administration

51.1.1 *A Written directive specifies the intelligence activities performed by the agency.*

Commentary: Intelligence activities are important in all agencies, regardless of size. Certain essential activities should be accomplished, although in small agencies there may be a less formal and structured process than in large agencies. The intelligence activities should include information gathering, analysis, and dissemination to proper sources.

51.1.2 *A written directive sets forth procedures for ensuring the legality and integrity of the intelligence effort, to include:*

- *methods for ensuring informants are secure in their anonymity;*
- *procedures for ensuring information collected is limited to criminal conduct and relates to activities that present a threat to the community;*

• *procedures for the utilization of intelligence personnel, equipment, and techniques;*

• *descriptions of the types of quality of information that may be included in the system; and*

• *methods for purging the records of out-of-date information.*

Commentary: Activities undertaken in the intelligence effort should avoid indiscriminate collection or distribution of information.

51.1.3 *The agency has a full-time intelligence component with accountability designated in an identifiable person.*

Commentary: The purpose of this standard is to ensure accountability and provide for unity of command. Since intelligence activities are essential to effective law enforcement, a full-time organizational component should be established in those agencies where justified by workload. Certain essential activities should be accomplished by an intelligence component, to include: (1) a procedure that permits the continuous flow of raw data into a central point from all sources; (2) a secure records system where evaluated data are properly cross-referenced to reflect relationships and to ensure complete and rapid retrieval; (3) a system of analysis capable of developing intelligence from both the records' system and other data sources; and (4) a system for dissemination of information to appropriate sources.

51.1.4 *When an agency establishes a confidential fund, an accounting system is maintained.*

Commentary: A confidential fund is important to intelligence activities. Among other purposes, such a fund pays informants and helps support other intelligence operations. The accounting system should be carefully structured and audited due to the confidentiality of information. A coding system for identifying individuals is frequently used for this purpose. An accounting system should provide for internal monitoring as well as after-the-fact auditing.

51.1.5 *Intelligence records are maintained under the control of the intelligence component.*

Commentary: Responsibility for the security of intelligence records should be vested in the intelligence component. Access to intelligence records should be limited to individuals approved by the agency's chief executive officer. In those agencies not having a specialized intelligence component, the records should be maintained under the immediate control of the agency's chief executive officer. This represents an exception to the centralization of the records.

51.1.6 *A written directive governs procedures for the safeguarding of intelligence information.*

Commentary: Intelligence information should be distributed only to criminal justice agencies and on a need-to-know basis. Intelligence information should be collated and analyzed in a secure environment. If a computer is used for intelligence purposes, there should be a secure system that protects against unauthorized attempts to access, modify, remove, or destroy stored information.

51.1 Operations

51.2.1 *A written directive stipulates that the agency maintain liaison with federal, state, and local agencies for the exchange of intelligence information.*

Commentary: The exchange of information as well as the coordination of effort between the agency's intelligence

component and other governmental agencies having similar responsibilities enhances the preparedness of each. A specific position or person should be designated as responsible for this liaison.

51.2.2 *A written directive governs the exchange of information between the intelligence component and other agency components.*

Commentary: Information developed through intelligence activities should be provided to operational units to increase the effectiveness of their enforcement and deterrent efforts. The written directive should establish procedures to ensure adequate feedback on the utility and timeliness of intelligence information. It should be recognized that patrol officers have a significant opportunity to gather intelligence information.

51.3 Facilities and Equipment

51.3.1 *The agency maintains or has access to specialized equipment to support the intelligence function.*

Commentary: The intent of the standard is to require the availability of equipment specifically designed for the intelligence function. This may include audio-visual monitoring equipment, night vision equipment, and specially designed surveillance vehicles.

51.3.2 *A secure area separate form the agency's records center is utilized for the storage of intelligence records.*

Commentary: The highly sensitive nature of intelligence files requires that they be maintained separately from other agency records to prevent compromise and protect the integrity of the system.

NOTES

APPENDIX C

NATIONAL ADVISORY COMMISSION INTELLIGENCE STANDARDS

EXCERPTS FROM: National Advisory Commission on Criminal Justice Standards and Goals (1973) *Police*, PP 250—254.

Standard 9.11

Intelligence Operations

(page 250)

Every police agency and every State immediately should establish and maintain the capability to gather and evaluate information and to disseminate intelligence in a manner which protects every individual's right to privacy while it curtails organized crime and public disorder.

1. Every State should establish a central gathering, analysis and storage capability, and intelligence dissemination system.

a. Every police agency should actively participate in providing information and receiving intelligence from this system.

b. Every police agency should designate at least one person to be liaison with the State intelligence system.

c. Every State intelligence system should disseminate specific intelligence to local agencies according to local needs and should disseminate general information throughout the State.

2. Every local agency should participate, where appropriate, in the establishment of regional intelligence systems. Every regional intelligence system should participate actively in the State system.

3. Every police agency with more than 75 personnel should have a full-time intelligence capability.

a. The number of personnel assigned to this operation should be based on local conditions.

b. The intelligence operation should be centralized; however, intelligence specialists may be assigned, where appropriate, to major transportation centers.

c. When the size of the intelligence operation permits, organized crime intelligence should be separate from civil disorder intelligence.

d. In smaller agencies the intelligence specialist should be required to take direct enforcement action only

when limited agency resources make it absolutely necessary. In larger agencies the intelligence specialists should be required to take direct enforcement action only where a serious threat to life or property makes it absolutely necessary.

e. The intelligence operation should include an independent and well-secured reporting and record system.

4. Every police agency should insure exchange of information and coordination of the intelligence operation and all other operational entities of the agency and with other government services.

5. Every police agency could supply its intelligence operation with the funds, vehicles, vision devices, and other specialized equipment necessary to implement an effective intelligence operation.

Commentary (page 251)

Intelligence, in the police sense, is awareness. Awareness of community conditions, potential problems, and criminal activity—past, present, and proposed—is vital to the effective operation of law enforcement agencies and continued community safety and security.

Intelligence should be carefully guarded. Above all, every individual's right to privacy must be protected. Dissemination of information on suspected offenders or of other intelligence that would not be admissible in a court should be restricted exclusively to officers needing such information to achieve the goals of their police agency lawfully. Informants should be secure in their anonymity and should be assured that their covert contributions will not be revealed. Specific safeguards should be built into the police intelligence system to prevent any information from being disseminated to unauthorized persons, or to any person for uses not consistent with the role of the police agencies maintaining or participating in the system.

... Intelligence activities must be continual, and they must constitute a system. When the system is effective, it always produces action programs.

The deployment of intelligence operations will be determined, of course, by the activities that present a threat to the community. Operations may be concentrated on organized predatory criminal groups, or other groups that are violence-oriented or inclined toward activity that unlawfully disrupts the community and its citizens. ...

Dissemination of Intelligence (page 253)

It is frequently charged, sometimes justifiably, that intelligence elements neglect to pass along information that could be valuable to other elements, particularly the patrol force. It is also true that intelligence operations are carried out in such isolation that only when they are concluded is it discovered that they were of little or no value. Too often intelligence operations become so enmeshed in the information gathering process that they omit evaluation and dissemination.

...

Coordination of efforts and exchange of information between a policy agency's intelligence operation and other governmental agencies with similar operational responsibilities increases operation effectiveness.

There is no known, thoroughly reliable method for evaluating the performance of an intelligence operation. The criteria for other investigatory performance techniques are not valid for intelligence. Invariably, when an attempt is made to evaluate the performance of an intelligence operation, members of the unit are diverted to tasks designed to proves they are productive—such tasks as increasing the number of items of information received and disseminated or the number of cases developed.

Perhaps a valid measurement of performance of an intelligence operation is whether it answers the following questions: Does the intelligence operation provide the police chief executive with useful intelligence in a timely manner? Does this intelligence form a foundation upon which [the chief] can implement effective action programs?

NOTES

GLOSSARY

Allocation - The long-term assignment of personnel by function, geography, and shift/duty tour along with the commitment of required supporting resources to deal with crime and police service demands in the most efficient and effective manner.

Analysis - That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information.

Archiving (Records) - The maintenance of records in remote storage after a case has been closed or disposed of as a matter of contingency should the records be needed for later reference.

Authority - The right to act or command others to act toward the attainment of organizational goals.

Bias/Hate Crime - Any criminal act directed toward any person as a result of that person's race, ethnicity, religious affiliation, or sexual preference.

Black Chamber - One of the earliest (1919) scientific applications to intelligence, this was a working group responsible for deciphering codes used to encrypt communications between foreign powers' diplomatic posts.

C^3 - An intelligence applications concept initially used by military intelligence which means command, control, and communications as the hallmarks for effective intelligence operations.

Clandestine Activities - An activity which is usually extensive and goal-oriented, planned and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation. "Storefront" operations, "stings", and certain concentrated undercover investigations (such as ABSCAM) can be classified as clandestine LAWINT collection.

Collation (of intelligence information) - A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system which permits easy and rapid access and retrieval.

Collection (of information) - The identification, location, and recording of unanalyzed information, typically from an original source and using both human and technological means, for input into the intelligence cycle to determine its usefulness in meeting a defined tactical or strategic intelligence goal.

Commodity - Any item or substance which is inherently unlawful to possess (contraband) or materials which, if not contraband, are themselves being distributed, transacted or marketed in an unlawful manner.

Communications Intelligence (COMINT) - This is the capture of information—either encrypted or in "plaintext"—exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between inter-communicating parties or groups, and/or analysis of the substantive meaning of the communication.

Computer Virus - Programs which were written to perform a desired function but have had a hidden code introduced into the command sequence which, when triggered, performs an unwanted or destructive function; it "infects" the computer by spreading through its memory and/or operating system and can "infect" other computers if introduced through shared data media or via a communications medium.

Conclusion - A definitive statement about a suspect, action, or state of nature based on the analysis of information.

Continuing Criminal Enterprise - Any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity which are involved in a continuing or perpetuating criminal event.

Coordination - The processes of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

Counterintelligence - A National Security intelligence activity which involves the countering of similar intelligence activities by other groups, governments, or individuals through the identification, neutralization, and manipulation of other states or groups intelligence services.

Covert Intelligence - A covert activity is planned and executed to conceal the collection of information and/or the identity of any officer or agent participating in the activity. Undercover operations, electronic eavesdropping, and "closed" surveillance of an intelligence target would fall within this category.

Crime Analysis - The process of analyzing information collected on crime and police service delivery variables in order to give direction for police officer deployment, resource allocation, and policing strategies as a means to maximize crime prevention activities and the cost-effective operation of the police department.

Criminal History Record Information (CHRI) - Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does *not* include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

Criminal Informant - *See* Informant

Cryptanalysis - The process of deciphering encrypted communications of an intelligence target.

Cryptography - The creation of a communications code/encryption system for communication transmission with the intent of precluding the consumption and interpretation of one's own messages.

Cryptology - the study of communications encryption methods which deal with the development of "codes" and the "scrambling" of communications in order to prevent the interception of the communications by an unauthorized or unintended party.

Data Quality - Refers to police records to ensure all information in the records is complete, accurate, and secure.

Deployment - The short-term assignment of personnel to address specific crime problems or police service demands.

Discrete Intelligence - A collection activity which must be conducted cautiously to avoid undue curiosity and public interest, to minimize interference with the collection activity, and to minimize the suspicions of the

intelligence target. Discrete activities may be acknowledged by and attributed to its agency/sponsor.

Dissemination (of intelligence) - This is the process of effectively distributing analyzed intelligence information in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

Division of Labor - Tasks within the organization are divided among personnel based on expertise required to perform the tasks, demand for the tasks to be performed, or, due to the inherent nature of the tasks, there is a need for close supervision and/or security; specialization of duties is part of the division of labor.

Due Process - Fundamental fairness during the course of the criminal justice process, includes adherence to legal standards and the civil rights of the police constituency; the adherence to principles which are fundamental to justice.

Effective - Doing the *right job*. It is performing the tasks and expending the effort to accomplish the specifically defined goal of the task(s) at hand.

Efficient - Doing the *job right*. It is concerned with the judicious use of resources and effort to accomplish the intended tasks without expending undue time, money, or effort.

El Paso Intelligence Center (EPIC) - Operated by the Drug Enforcement Administration; a cooperative intelligence center serving as a clearinghouse and intelligence resource for local, state, and federal law enforcement agencies. Primary concern is drug trafficking, however intelligence information on other crimes is also dealt with.

Enterprise - Any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.

Estimate - Strategic projections on the economic, human, and/or quantitative criminal impact of the crime or issue subject to analysis.

Evaluation (of intelligence information) - All information collected for the intelligence cycle is reviewed for its *quality* with an assessment of the validity and reliability of the information.

Exemptions (to the FOIA) - Circumstances wherein the agency is not required to disclose information from a FOIA request.

Freedom of Information Act (FOIA) - The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966 generally provides, as a statutory right, that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

General intelligence - Intelligence unit will collect information on crimes in general in support of an agency's investigative responsibility—typically associated with a municipal, county, or state law enforcement agency with general law enforcement responsibilities

Goal - A goal is the end to which all activity in the unit is directed.

Human Intelligence (HUMINT) - Intelligence gathering methods which require human interaction or observation of the target or targeted environment. The intelligence is collected through the use of one's direct senses or the optical and/or audio enhancement of the senses.

Hypothesis - A proposed relationship between persons, events, and/or commodities based on the accumulation and analysis of intelligence information.

Imagery - The representation of an object or locale produced on any medium by optical or electronic means. The nature of the image will be dependent on the sensing media and sensing platform.

Inductive logic - The reasoning process of taking diverse pieces of specific information and inferring to a broader meaning of the information through the course of hypothesis development.

Informant - The interaction with persons not affiliated with a law enforcement agency to solicit information for purposes of gathering incriminating information on the intelligence target or information which will further the investigation.

Information System - An organized means of collecting, processing, storing, and retrieving information on *individual entities* for purposes of record and reference.

Intelligence Analyst - A person who takes the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a crime and places them into a logical and related framework for the purpose of developing a criminal case, explaining a criminal phenomenon, or describing crime and crime trends.

Intelligence Community - Customarily refers to those agencies which gather National Security intelligence information.

Intelligence Cycle - An organized process by which information is *gathered*, *assessed*, and *distributed* in order to fulfill the goals of the intelligence function—it is a method of performing analytic activities and placing the analysis in a useable form.

Intelligence Mutual Aid Pact (IMAP) - A formal agreement between law enforcement agencies designed to expedite the process of sharing information in intelligence records.

International Criminal Police Organization (INTERPOL) - INTERPOL is a world wide association of national police forces established for mutual assistance in the detection and deterrence of international crimes; it is an information clearinghouse for nonpolitical, international criminals, international transportation of stolen properties, and international trade of contraband.

Key Word In Context (KWIC) - An automated system which indexes selected key words which represent the evidence or information being stored.

Law Enforcement Intelligence (LAWINT) - The end product (output) of an analytic process which collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgements and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends.

Macro-intelligence - An overall view of general demographic, social, and crime trends which indicate environments and types of crimes which are emerging or projected to emerge.

Malicious Software - Self-contained yet interactive computer programs which, when introduced into a computer, can cause loss of memory, loss of data, or cause erroneous instructions to be given in a computer program.

Micro-intelligence - Intelligence activities focusing on current problems and crimes for either case development or resource allocation.

Mission - The mission is the *role* which the unit fulfills in support of the overall mission of the agency—it specifies in general language *what* the unit is intended to accomplish.

Motion Sensing - Various methods exist to detect the presence, direction, and nature of moving people, vehicles, or objects. Motion sensors may be on either a fixed or mobile platform and include acoustic, seismic and disturbance sensors.

National Central Bureau (NCB or USNCB) - The United States Headquarters of INTERPOL located in Washington, DC.

National Security Intelligence - The collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States' sovereign principles.

Office of Strategic Services (OSS) - Created by President Roosevelt in 1942, the OSS was the precursor agency to the Central Intelligence Agency (CIA) and established the model for contemporary national security intelligence applications.

Open Communications (OPCOM) - The collection of open or publicly available communications, broadcasts, audio or video recordings, propaganda, published statements, and other distributed written or recorded material for purposes of analyzing the information.

Operational intelligence - Intelligence information is evaluated and systematically organized on an active or potential target. This process is developmental in nature wherein there is sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information in order to develop a case for arrest or indictment.

Organizing - The rational coordination of the activities of a number of people for the achievement of some common explicit purpose or goal through division of labor and function and through a hierarchy of authority and responsibility.

Outcome Evaluation - The process of determining the value or amount of success in achieving a predetermined objective through defining the objective in some qualitative or quantitative measurable terms; identifying the proper criteria (or variables) to be used in measuring the success toward attaining the objective; determination and explanation of the degree of success; and recommendations for further program actions to attain the desired objectives/outcomes.

Overt Intelligence - A collection activity which is conducted openly and may be acknowledged by and attributed to its agency/sponsor and participants. Interviewing criminal suspects or witnesses and accessing public records are examples of overt LAWINT collection.

Physical Intrusion - The interception of communications as a result of a physical intrusion into the communications medium such as opening mail; seizure of non-public written communications or documents; tapping telephone lines; interception of cable communications; or accessing computer-driven communications systems through direct or remote surreptitious access to the system.

Planning - Planning is the anticipation of future situations, estimating organizational demands and resources needed to attend to those situations, and initiating strategies to respond to those situations.

Policy - The principles and values which guide the performance of a duty. A policy is *not* a statement of what must be done in a particular situation. Rather, it is a statement of *guiding principles* which should be followed in activities which are directed toward the attainment of goals.

Policy Intelligence - *See* National Security Intelligence.

Prediction - Projection of future criminal actions or changes in the nature of crime trends based on analysis of intelligence information.

Privacy Act - Legislation which allows an individual to review almost all Federal files (and state files under the auspices of the respective state privacy acts) pertaining to him/herself; places restrictions on the disclosure of personally identifiable information; specifies that there be no secret records systems on individuals; and compels the government to reveal its information sources.

Procedural Due Process - Mandates and guarantees of law which ensure that the procedures employed to deprive a person of life, liberty, or property during the course of the criminal justice process meet constitutional standards.

Procedures - A method of performing an operation or a manner of proceeding on a course of action. It differs from policy in that it directs action in a particular situation to perform a specific task within the guidelines of policy. Both policies and procedures are goal oriented. However, policy establishes limits to action while procedure *directs responses* within those limits.

Process Evaluation - The assessment of procedures used to attain objectives within the following criteria of substantive contribution, effectiveness of resources; coordination with other activities; and properly trained staff.

Process Hypothesis - Represents a hypothesized link, procedure, or behavior throughout a criminal enterprise which is the basis for the logic to make summary hypotheses, conclusions, estimates, and/or prediction.

Profile/Criminal Profile - An investigative technique by which to identify and define the major personality and behavioral characteristics of the [criminal] offender based upon an analysis of the crime(s) he or she has committed.

Protocol (of Intelligence Collection) - Information collection *procedures* employed to obtain verbal and written information, actions of people, and physical evidence required for strategic and tactical intelligence analysis.

Purging (Records) - Records are removed from files and destroyed because they are deemed to be of no further value or further access to the records would serve no legitimate government interest. means records are removed and destroyed.

Qualitative (Methods) - Research methods that collect and analyze information which are described in narrative or rhetorical form and conclusions drawn based on the cumulative interpreted meaning of that information.

Quantitative (Methods) - Research methods that collect and analyze information which can be "counted" or placed on a scale of measurement which can be statistically analyzed.

Racketeering activity - state felonies involving murder, robbery, extortion, and several other serious offenses, and more than thirty serious federal offenses including extortion, interstate theft offenses, narcotics violations, mail fraud, and securities fraud.

Racketeering Influenced Corrupt Organization (RICO) - The statute provides civil and criminal penalties for persons who engage in a "pattern of racketeering activity" or "collection of an unlawful debt" that has a specified relationship to an "enterprise" that affects interstate commerce. Title IX of the Organized Crime Control Act of 1970 (18 U.S.C. Sections 1961-1968)

Records System (Privacy Act) - A group of records from which information is retrieved by reference to a name or other personal identifier such as a social security number.

Regional Information Sharing System (RISS) - RISS projects consist of seven regionally grouped states from which state and local law enforcement agencies can become members to share intelligence information and have a clearinghouse for information and resources for targeted crimes.

Reliability - Asks the question, "Is the *source* of the information consistent and dependable?"

Remote Sensing (REMSEN) - The collection of information which is typically not communications but can be viewed or interpreted by intelligence personnel to learn more about the intelligence target and provide support for case preparation.

Reporting - The process of taking the analyzed information and placing it in the proper form for the most effective consumption of that information as dependent on the type of intelligence.

Responsibility - Responsibility reflects how the authority of a unit or individual is used and determining if goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority.

Rules - A specific requirement or prohibition which is stated to prevent deviations from policy or procedure. A violation of a rule typically results in an internal investigation and may result in disciplinary action.

Sealing (Records) - Records are stored by the agency but cannot be accessed, referenced, or used without a court order based on a showing of evidence that there is a legitimate government interest to review the sealed information.

Signal Intelligence (SIGINT) - The interception of various radio frequency signals, microwave signals, satellite audio communications, nonimagery infrared and coherent light signals, and transmissions from surreptitiously placed audio micro-transmitters in support of the COMINT activity.

Specialized intelligence - Intelligence unit (or section within a unit) focuses on an exclusive issue whether it is a crime (e.g., narcotics, terrorism, etc.) or entity (e.g., organized crime, right wing extremist groups, etc.).

Statistical System - An organized means of collecting, processing, and storing, and retrieving *aggregate* information for purposes of analysis, research, and reference. No individual records are stored in a statistical system.

Strategic Intelligence - An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making and resource allocation; and the focused examination of unique, pervasive, and/or complex crime problems.

Substantive Due Process - Guarantees persons against arbitrary, unreasonable, or capricious laws and it acts as a limitation against arbitrary governmental actions so that no government agency may exercise powers beyond those authorized by the Constitution.

Surveillance - The observation of activities, behaviors, and associations of a LAWINT target (individual or group) with the intent to gather incriminating information or "lead" information which is used for the furtherance of a criminal investigation.

Tactical intelligence - Evaluated information on which immediate enforcement action can be based;

intelligence activity focused specifically on developing an active case.

Target - Any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis.

Target - For purposes of LAWINT a target is the person(s), crime(s), and criminal enterprises identified as the subject of a criminal investigation utilizing law enforcement intelligence analysis.

Targeting - The identification of crimes, crime trends, and crime patterns which have discernable characteristics that make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

Technology - As used in this monograph, refers to any electronic instrument or device used for communications, data collection, data transmittal, data storage, or data analysis.

Telemetry - The collection and processing of information derived from noncommunications electromagnetic radiations emitting from sources such as radio navigation systems (e.g., transponders); radar systems, and information/data signals emitted from monitoring equipment in a vehicle or device.

Third Agency Rule - An agreement wherein a source agency releases information under the condition that the receiving agency *does not* release the information to any other agency—that is, a "third agency".

Trojan Horse - A computer program, command or procedure which appears to be useful but contains a hidden code that, when invoked, performs some unwanted procedure; the program is *written with the intent* to be disruptive.

Undercover Investigation - Active infiltration (or attempting to infiltrate) a group believed to be involved in criminal activity and/or the interaction with a LAWINT target with the intent to gather incriminating information or "lead" information which is used for the furtherance of a criminal investigation.

Unity of Command - The principle of organization referred to as "one man, one boss". Each person within the organization should be operationally and functionally responsible to *only one* supervisor.

Validity - Asks the question, "Does the information *actually represent* what we believe it represents?"

Value-Based Philosophy - LAWINT activities which are clearly designed in support of legitimate organizational goals and performed in a manner which is consistent with law and ethical standards.

Variable - Any characteristic on which individuals, groups, items, or incidents differ.

Vaughn Index - In *Vaughn v. Rosen*, 484 F.2d 826, the court required agencies to prepare an itemized index, correlating each withheld document (or portion) with a specific Freedom of Information Act exemption and the relevant part of an agency's nondisclosure justification.

Violent Criminal Apprehension Program (VICAP) - A nationwide data information center operated by the FBI's National Center for the Analysis of Violent Crime, designed to collect, collate, and analyze specific crimes of violence.

Worms (Computer) - These programs use computer network connections to spread from system to system, thus worms attack system that are linked via communications lines spreading viruses or Trojan Horses via inter-connected media.

NOTES

BIBLIOGRAPHY

Baines, John M., et al. (1973). *Mutual Aid Planning*. Washington: National Sheriffs' Association.

Baltimore County (MD) Police Department. (1988). *Policy and Procedures for the Handling of Racial, Religious, and Ethnic Incidents*. Towson, MD: Baltimore County Police Department.

Bamford, James. (1986). *The Puzzle Palace*. New York: Penguin Press.

Bayse, William A. and Carolyn G. Morris. (1988). "Developing Artificial Intelligence Applications for National Investigative Programs." *Federal Criminal Investigator*. (Summer) Vol. 6, No.1, pp. 37-41.

Best, A. George. (1987). *Forfeiture Sanctions*. Detroit: Wayne County (MI) Office of the Prosecuting Attorney.

Blakey, G. Robert, Ronald Goldstock, and Charles Rogovin. (1978). *Racket Bureaus: Investigation and Prosecution of Organized Crime*. Washington: National Institute for Law Enforcement and Criminal Justice.

Booth, Frank R. (1988). *Asset Forfeiture: Public Record and Other Information on Hidden Assets*. Washington: Police Executive Research Forum/Bureau of Justice Assistance.

Bouza, Anthony V. (1976). *Police Intelligence: The Operations of an Investigative Unit*. New York: AMS Press, Inc.

Brantingham, Paul and Patricia Brantingham. (1984). *Patterns in Crime*. New York: Macmillan.

Brooks, Pierce R., et al. (1988). *Multi-Agency Investigative Team Manual*. Washington: National Institute of Justice.

Buck, George A., et al. (1973). *Police Crime Analysis Unit Handbook*. Washington: National Institute of Law Enforcement and Criminal Justice.

Bureau of Justice Statistics. (Undated). *Criminal Justice Information Policy: Research Access to Criminal Justice Data*. Washington: U.S. Department of Justice.

Clavell, James. (ed.). (1988). *The Art of War: Transcriptions of Chinese Philosopher Sun Tzu*. New York: Dell Publishing.

Colton, Kent W., et al. (1982). *Computer Crime: Electronic Fund Transfer Systems and Crime*. Washington: Bureau of Justice Statistics.

Commission on Accreditation for Law Enforcement Agencies. (1988). *Standards for Law Enforcement Manual.* (Text Edition) Alexandria, VA: CALEA.

Commission to Review Department of Defense Security Policies and Practices. (1985). *Keeping the Nation's Secrets.* Washington: U.S. Department of Defense.

Committee on Government Operations. (1987). *A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records.* Washington: U.S. House of Representatives.

Couper, David C. (1983). *How to Rate Your Local Police.* Washington: Police Executive Research Forum.

Criminal Division. (1988). *Asset Forfeiture Law, Practice, and Policy.* Washington: U.S. Department of Justice.

Dintino, Justin J. and Frederick T. Martens. (1983). *Police Intelligence Systems in Crime Control.* Springfield, IL: Charles C. Thomas, Publisher.

Dowling, Jerry. (1979). *Criminal Investigation.* New York: Harcourt, Brace, Jovanovich.

Drug Enforcement Administration, Office of Intelligence. (Undated) *Source Debriefing Guide.* Washington: U.S. Department of Justice.

Eck, John E. (1979). *Managing Case Assignments: The Burglary Investigation Decision Model Replication.* Washington: Police Executive Research Forum.

Edelhertz, Herbert. (ed.). (1987). *Major Issues in Organized Crime Control.* Washington: National Institute of Justice.

Executive Order 12333. (1981) *United States Intelligence Activities.* Washington: Office of the President of the United States.

Fairfax County (VA) Police Department, Crime Analysis Unit. (1987). *Crime Analysis Unit Operations Manual.* Mimeographed document of the Fairfax County Police Department.

Federal Bureau of Investigation. (1985). *Counterintelligence Awareness Seminar: Proceedings.* Washington: U.S Department of Justice/FBI.

Fital, Robert A. (1988). "The Electronic Communications Privacy Act." *FBI Law Enforcement Bulletin.* (Part 1: February, pp. 25-30); (Part 2: March, pp. 26-30); (Part 3: April, pp. 24-30).

Fooner, Michael. (1985). *A Guide to INTERPOL: The International Criminal Police Organization in the United States.* Washington: National Institute of Justice.

Gallagher, G. Patrick. (1988). *Asset Forfeiture: The Management and Disposition of Seized Assets.* Washington: Police Executive Research Forum/Bureau of Justice Assistance.

Gardiner, John A. (1970). *The Politics of Corruption: Organized Crime in An American City*. New York: Russell Sage Foundation.

Godson, Roy. (ed.). (1980). *Intelligence Requirements for the 1980s: Analysis and Estimates*. Washington: National Strategic Information Center, Inc.

Godson, Roy. (ed.). (1983). *Intelligence Requirements for the 1980s: Elements of Intelligence*. (Revised edition). Washington: National Strategic Information Center, Inc.

Godson, Roy. (ed.). (1986). *Intelligence Requirements for the 1980s: Domestic Intelligence*. Washington: National Strategic Information Center, Inc.

Godson, Roy. (ed.). (1986). *Intelligence Requirements for the 1980s: Intelligence and Policy*. Washington: National Strategic Information Center, Inc.

Goldsmith, Michael. (1988). *Asset Forfeiture: Civil Forfeiture—Tracing the Proceeds of Narcotics Trafficking*. Washington: Police Executive Research Forum/Bureau of Justice Assistance.

"Governing Guide: Managing Information." (1990) *Governing*. (February), p. 28A.

Harper, Walter R., et al. (1977). *A Study Report: Immigration and Naturalization Service Intelligence System Concept*. Santa Barbara, CA: ANACAPA Sciences, Inc.

Harris, Don R. (1976). *Basic Elements of Intelligence*. Washington: Law Enforcement Assistance Administration.

Hicks, John W. (1988). "DNA Profiling: A Tool for Law Enforcement." *FBI Law Enforcement Bulletin*. (August), pp. 1-5.

Immigration and Naturalization Service. (1988). *Anti-Smuggling Program*. INS Mimeographed internal report.

Immigration and Naturalization Service. (1988). *Asset Forfeiture Program: Equitable Sharing*. INS Mimeographed internal report.

Immigration and Naturalization Service. (Undated). *Intelligence Officer Handbook*. Mimeographed handbook produced by the INS Office of the Assistant Commissioner for Intelligence.

Institute of Law and Justice. (1989) Managing Confidential Funds. Alexandria, VA: Institute of Law and Justice.

International Association of Chiefs of Police. (1985). Law Enforcement Police on the Management of Criminal Intelligence. Gaithersburg, MD: IACP.

International Association of Chiefs of Police. (1990). "Models for Management: Confidential Informants". *The Police Chief*. (January), pp. 56—7.

Karchmer, Cliff. (1988). *Illegal Money Laundering: A Strategy and Resource Guide for Law Enforcement Agencies.* Washington: Police Executive Research Forum.

Kelley, Clarence M. (1987) *Kelley: The Story of An FBI Director.* Kansas City, MO: Andrews, McMeel and Parker.

Kinney, Jack and Douglas Harris. (1980). *Study Report: Alcohol, Tobacco and Firearms Intelligence Systems Study.* Santa Barbara, CA: ANACAPA Sciences, Inc.

Kleiman, Mark A.R. (1984). *Evaluation of the Lynn Drug Task Force.* Cambridge, MA: Harvard University, John F. Kennedy School of Government.

Kleiman, Mark A.R. et al. (1988) *Street-Level Drug Enforcement: Examining the Issues.* Washington: National Institute of Justice.

Levine, Emil H. (1979). *Information Science: Law Enforcement Applications.* Cincinnati: Anderson Publishing Company.

Martens, Frederick T. (1982). "The Essence of the Intelligence Process: Analysis." *Issues of Interest to Law Enforcement Intelligence.* Sacramento, CA: Law Enforcement Intelligence Unit.

Martens, Frederick T. (1987). "The Intelligence Function." In Herbert Edelhertz. (ed.). *Major Issues in Organized Crime Control.* Washington: National Institute of Justice.

Marx, Gary T. (1987). "Restoring Realism and Logic to the Covert Facilitation Debate." *Journal of Social Issues.* 43:3, pp. 43-55.

Marx, Gary T. (1987). "The Interweaving of Public and Private Police in Undercover Work." In Clifford Shearing and Philip Stenning, *Private Policing.* New York: Sage Publications, pp. 172-193.

Marx, Gary T. (1988). *Undercover: Police Surveillance in America.* Berkeley, CA: University of California Press.

Marx, Gary T. (1989). "Commentary: Some Trends and Issues in Citizen Involvement in the Law Enforcement Process." *Crime & Delinquency.* 35:3(July):500-519.

Marx, Gary T. and Nancy Reichman. (1985). "Routinizing the Discovery of Secrets: Computers as Informants." *Software Law Journal.* Vol.1:pp 95-121.

McEwen, J. Thomas. (1989) *Dedicated Computer Crime Units.* Washington: National Institute of Justice.

Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network. (1986). *Annual Report.* Malvern, PA: MAGLOCLEN.

Miller, George I. (1987). "Observations on Police Undercover Work." *Criminology.* 25:1, pp. 27-46.

Miron, Murray S. and John E. Douglas. (1979). "Threat Analysis: The Psycholinguistic Approach." *FBI Law Enforcement Bulletin.* (September).

Moore, Mark. (1977). *Buy and Bust.* Lexington, MA: D.C. Heath, Publisher.

National Advisory Commission on Criminal Justice Standards and Goals. (1973). *Police.* Washington: U.S. Government Printing Office.

National Commission on the Causes and Prevention of Violence. (1969). *Crimes of Violence.* Washington: U.S. Government Printing Office.

National Intelligence Academy. (1987) *Technical Intelligence.* 3rd ed. Ft. Lauderdale, FL: National Intelligence Academy.

Naval Education and Training Command. (1983). *Intelligence Specialist Training Manual.* Washington: United States Navy.

New Jersey Department of Law and Public Safety. (1988). *Narcotics and Organized Crime Management and Analytical Data Base: Policy Manual.* Trenton, NJ: State of New Jersey, Office of Attorney General.

Office of National Drug Control Policy. (1989) *National Drug Control Strategy.* Volume 1. Washington: U.S. Government Printing Office.

Office of National Drug Control Policy. (1990) *National Drug Control Strategy.* Volume 2. Washington: U.S. Government Printing Office.

Office of Technology Assessment (OTA). (1987a). *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information.* Washington: Congress of the United States.

Office of Technology Assessment. (1985). *Electronic Surveillance and Civil Liberties.* Washington: Congress of the United States.

Office of Technology Assessment. (1986). *Electronic Records Systems and Individual Privacy.* Washington: Congress of the United States.

Office of Technology Assessment. (1987). *The Border War on Drugs.* Washington: Congress of the United States.

Office of Technology Assessment. (1987b). *Science, Technology, and the Constitution: Background Paper.* Washington: Congress of the United States.

Office of Technology Assessment. (1988). *Science, Technology, and the First Amendment: Special Report.* Washington: Congress of the United States.

Organized Crime and Racketeering Section. (1988). *Racketeer Influenced and Corrupt Organizations: A Manual for Federal Prosecutors.* Washington: U.S. Department of Justice.

Parker, Donn B., et al. (Undated). *Computer Crime: Computer Security Techniques.* Washington: Bureau of Justice Statistics.

President's Commission on Law Enforcement and Administration of Justice. (1967). *Task Force Report: Organized Crime.* Washington: U.S. Government Printing Office.

President's Commission on Law Enforcement and Administration of Justice. (1967). *Task Force Report: The Police.* Washington: U.S. Government Printing Office.

President's Commission on Organized Crime. (1986). *America's Habit: Drug Abuse, Drug Trafficking, and Organized Crime.* Washington: U.S. Government Printing Office.

President's Council on Integrity and Efficiency. (1986). *Computers: Crimes, Clues and Controls.* Washington: U.S. Government Printing Office.

Quirk, John P. (1988). *The Intelligence Community.* Guilford, CT: Foreign Intelligence Press.

Reid, Sue Titus. (1982). *Crime and Criminology.* 2d ed. New York: Holt, Rinehart and Winston/CBS College Publishing.

Reuter, Peter. (1983). *Disorganized Crime.* Cambridge, MA: M.I.T. Press.

Riggin, Stephen P. (1984). "U.S. Information Access Laws: Are They a Threat to Law Enforcement?" *FBI Law Enforcement Bulletin.* (July), pp. 13-19.

Robbins, Stephen. (1976). *The Administrative Process.* New York: Prentice-Hall, Publisher.

Sadighian, Joseph. (1989) *Drug Courier Profiles After Sokolow: Legal Review and Analysis.* (Mimeographed Report). Washington: Police Executive Research Forum.

SEARCH Group, Inc. (1985). *Intelligence and Investigative Records.* Washington: Bureau of Justice Statistics.

SEARCH Group, Inc. (1988). *Public Access to Criminal History and Record Information.* Washington: Bureau of Justice Statistics.

SEARCH Group, Inc./Bureau of Justice Statistics. (1986). *Data Quality Policies and Procedures: Conference Proceedings.* Washington: SEARCH Group, Inc.

Select Committee on Intelligence. (1986). *Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs.* Washington: United States Senate.

Sommers, Marilyn P. (1986). "Law Enforcement Intelligence: A New Look." *International Journal of Intelligence and Counter Intelligence.* Vol. 1, No. 3. pp. 25-40.

SRI International. (1979). *Computer Crime: Criminal Justice Resource Manual.* Washington: Bureau of Justice Statistics.

Stellwagen, Lindsey D. (1985). "Use of Forfeiture Sanctions in Drug Cases". *Research in Brief*. Washington: National Institute of Justice.

Subcommittee on Civil and Constitutional Rights of the Committee of the Judiciary. (1984). *FBI Undercover Operations*. U.S. House of Representatives.

U.S. Army Intelligence and Security Command. (1984). *Military Intelligence: A Pictoral History*. Washington: United States Army.

U.S. Customs Service. (Undated). *Training Manual for Customs Intelligence Analysts*. Mimeographed handbook produced for training at the Federal Law Enforcement Training Center, Glynco, GA.

U.S. Drug Enforcement Administration. (1988). *Enforcement at the Source*. Project descriptive paper.

U.S. House of Representatives. (1987). *FBI Undercover Operations*. Report of the Subcommittee on Civil and Constitutional Rights, House Committee on the Judiciary.

U.S. Marine Corps. (1983) *Counterintelligence*. Washington: U.S. Government Printing Office.

United States Attorney General. (1988) *RICO Manual for Federal Prosecutors*. Washington: U.S. Department of Justice.

Wack, John P. and Lisa J. Camahan. (1989). *Computer Viruses and Related Threats: A Management Guide*. Washington: U.S. Department of Commerce, National Institute of Standards and Technology.

Wasserman, Robert and Mark H. Moore. (1988). "Values in Policing." *Perspectives on Policing*. Washington: National Institute of Justice.

White House Conference for a Drug Free America. (1988) *Final Report*. Washington: U.S. Government Printing Office.

Wilson, James Q. (1978). *The Investigators*. New York: Basic Books.

Wilson, Thomas F. and Paul L. Woodward. (1986). *Criminal Justice Information Policy: Criminal Justice "Hot" Files*. Washington: SEARCH Group, Inc./Bureau of Justice Statistics.

Wilson, Thomas F. and Paul L. Woodward. (1987). *Automated Fingerprint Identification Systems: Technology and Policy Issues*. Washington: Bureau of Justice Statistics.

NOTES

History of Law Enforcement Intelligence

The Special Case of Organized Crime

A PERSPECTIVE

THE SPECIAL ROLE OF ORGANIZED CRIME IN THE DEVELOPMENT OF INTELLIGENCE

"As a wiseguy you can lie, you can cheat, you can steal, you can kill people—legitimately. *You can do any goddamn thing you want, and nobody can say any thing about it. Who wouldn't want to be a wiseguy?."*
"Made" New York Mobster Lefty Ruggiero

A. The initial applications of LAWINT—while influenced by many factors—was particularly influenced by "traditional" organized crime: The Mafia or La Cosa Nostra. Conversely, the largest factor affecting the growth of organized crime "families" was **prohibition.**

A Definition of Organized Crime

Organized crime is a nonideological enterprise that involves a number of persons in close social interaction, organized on a hierarchical basis for the purpose of securing profit and power by engaging in illegal and legal activities. Positions in the hierarchy and positions involving functional specialization may be assigned on the basis of kinship or friendship, or rationally assigned according to skill. ... [Organized crime] eschews competition and strives for monopoly over particular activities on an industry or territorial basis. There is a willingness to use violence and/or bribery to achieve ends or to maintain discipline. Membership is restricted, although nonmembers may be involved on a contingency basis. (Abadinsky, 1985)

B. Prohibition provided an opportunity for bootleggers to provide a product (i.e., alcohol) which had been outlawed yet remained in great demand by virtually all strata of society. As a result, crime groups, which were largely ethnically based, took advantage of this capitulation by Americans and supplied the alcohol they craved. The profits were tremendous, and in order to keep their lifestyles and continuing profits, politicians and police officials were corrupted.

Taking Notice of La Cosa Nostra

Our understanding and perception of organized crime—in particular the La Cosa Nostra—has several developmental phases:

- Virtually no recognition of the organized crime concept before 1920

(continued)

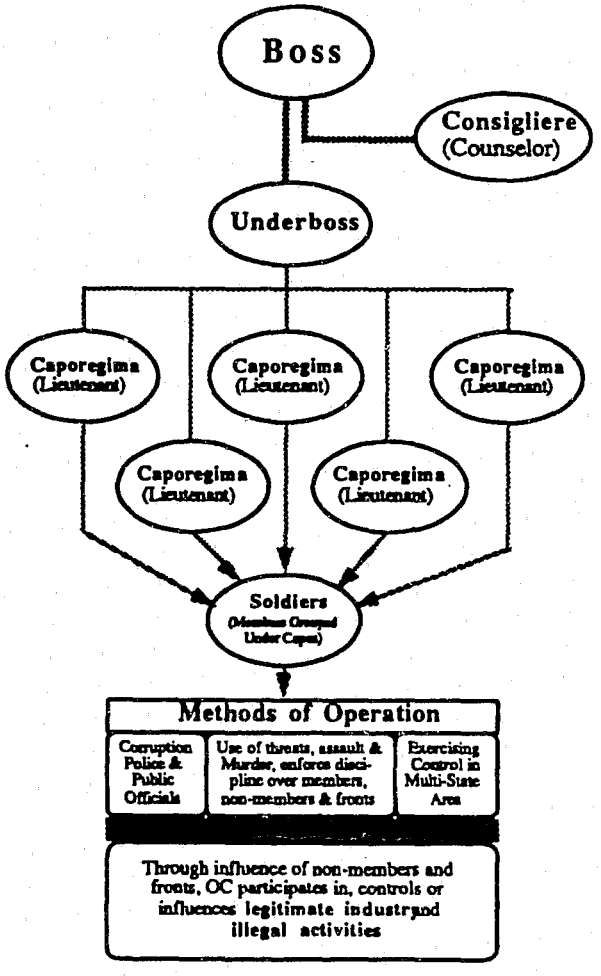
- Period of denial that there was any type of crime networks beginning during 1920s with Prohibition going into the 1950s.

- Overt recognition of organized crime after the Apalachin New York meeting (1957) and the Valachi Hearings with continuing interest into the 1960s when interest diminished in light of the influence of other socio-political events of the 1960s.
- Second period of denial with some romanticization (notably in the 1970s following *The Godfather* movie, the interest on "self", and the fairly widespread acceptance of recreational drug use
- Since around 1980 serious recognition of organized crime along with several significant federal prosecutions, and including "new" types of organized crime (notably South American, Jamaican, Asian crime groups)

C. During Prohibition, the organized crime families continued earlier criminal enterprises and expanded them with their new-found capital—Gambling, prostitution, and racketeering were given particular attention.

D. Following Prohibition, organized crime became more diversified.

- The Chicago "Accardo Family" and the New York "Bonanno Family" (along with some of their subordinate families) focused great attention to gaming operations in Las Vegas in order to "skim" gambling proceeds from casinos.
- Most of the families continued their prostitution, gambling, loan sharking, and racketeering operations only in expanded form
- Many of the families expanded into narcotics trafficking because of the lucrative profits, despite some of the earlier family prohibitions against involvement with drugs.
- A number of the smaller family enterprises continued to steal virtually anything that could be fenced as a means to bring in income—as long as the appropriate "cuts" were shared throughout the family's



rudimentary organizational structure.

- Increasingly, organized crime families (notably at the upper echelons) invested their illegitimate profits into legitimate businesses.

E. These evolutionary steps not only made the organized crime families more structured, it made them more difficult to investigate and prosecute.

F. The growth and diversity of organized crime along with its impact on government (via corruption) and its violence drew the attention of law enforcement—and the need for law enforcement intelligence

The Commission

May 1929 was the first national meeting of organized crime leaders—to become known as The Commission—in Atlantic City. (Some of the attendees included Al Capone, Lucky Luciano, Frank Costello, Meyer Lansky, and Bugsy Siegel.

"The Commission" met as such for the first time in 1931 and included the leaders from the five New York families and the head of the families in Chicago and Buffalo. The Commission was not discovered until 1957 in a special meeting at Apalachin, New York quite by accident when the suspicions of a New York state trooper were aroused by the presence of the incoming mobsters.

The Commission was not a governing board, per se, but more like a forum where common issues or problems could be discussed and resolved. While The Commission had not formally written rules, there was an understood code of conduct which was abided by and typically decisions of the The Commission were also adhered to.

G. There have been many people involved in the development of organized crime in the United States. The following is not meant to be comprehensive list, but to provide a perspective of some selected figures in OC and illustrate how growth occurred. Among some of the more notable persons involved in the development of organized crime in the United States:

- **Al Capone**—one of the most infamous mobsters—was a "strong arm" from Brooklyn was sent to Chicago to serve as "muscle" in growing bootlegging operations

  - Capone was noted for his violence; this contributed largely to his growth as a bootlegger and growth of the Capone Family

- **Meyer Lansky** was the **Charles "Lucky" Luciano** mob's (New York) financial advisor who had set up casinos and skimming operations in Havana Cuba (with the cooperation of former Cuban president Fulgencio Batista) in 1933

- **Lansky** was recruited by **Tony Accardo** (Chicago) to take the gaming and skimming expertise he had developed in Cuba to Las Vegas

- **Benjamin "Bugsy" Siegel**, under the direction of the Accardo Family in Chicago, in the 1930s was operating in the Casino business in Las Vegas

- In the early 1940s **Bugsy Siegel** was working to develop the Flamingo Hotel—opened December 26, 1946—to be the ultimate adult entertainment center with the best of everything

- **Morris "Moe" Dalitz**, a former Prohibition rum runner with a tough reputation, went to Las Vegas in 1946—he was destined to become the "godfather of Las Vegas"

- Meyer Lansky had sent Dalitz to Las Vegas to straighten out operations at the Flamingo because Bugsy Siegel was not doing the job he was supposed to and, it was thought, Siegel was skimming money from the Family

- Dalitz became a permanent fixture in Vegas in 1949 when he and others took over the Desert Inn's (DI) final construction after the owner, Wilbur Clark, ran into financial trouble. Dalitz and fellow family members would be the owners of the DI while Clark's name was the "front"

- The New York mob had opened several casinos in Las Vegas:

  - Flamingo 1946
  - Thunderbird 1948
  - Sands 1952

- The Chicago Accardo Family got into Vegas by taking over the Stardust in 1955 after the death of its original owner, a gangster from Los Angeles

- Accardo hired Dalitz from the Desert Inn to run the Stardust

H. Some of the "Good Guys"—The following people were among those who recognized and influenced the investigation of Organized Crime Families in the United States

- **Frank J. Loesch** was concerned with the growth of organized crime during Prohibition and was central figure in starting the Chicago Crime Commission i the 1920s.

- **Harry J. Anslinger** was Director of the Bureau of Narcotics 1930-1962 and was the first federal law enforcement official to recognized organized crime cartels

- Senator **Royal S. Copeland** of New York started the first Congressional hearings on organized crime in 1931

  NOTE: Other major national inquiries of organized crime included:

  —The **Senate Special Committee to Investigate Organized Crime in Interstate Commerce** (known as the Kefauver Commission, 1951)

  —The President's **Commission on Law Enforcement and Administration of Justice, Task Force on Organized Crime** (1967)

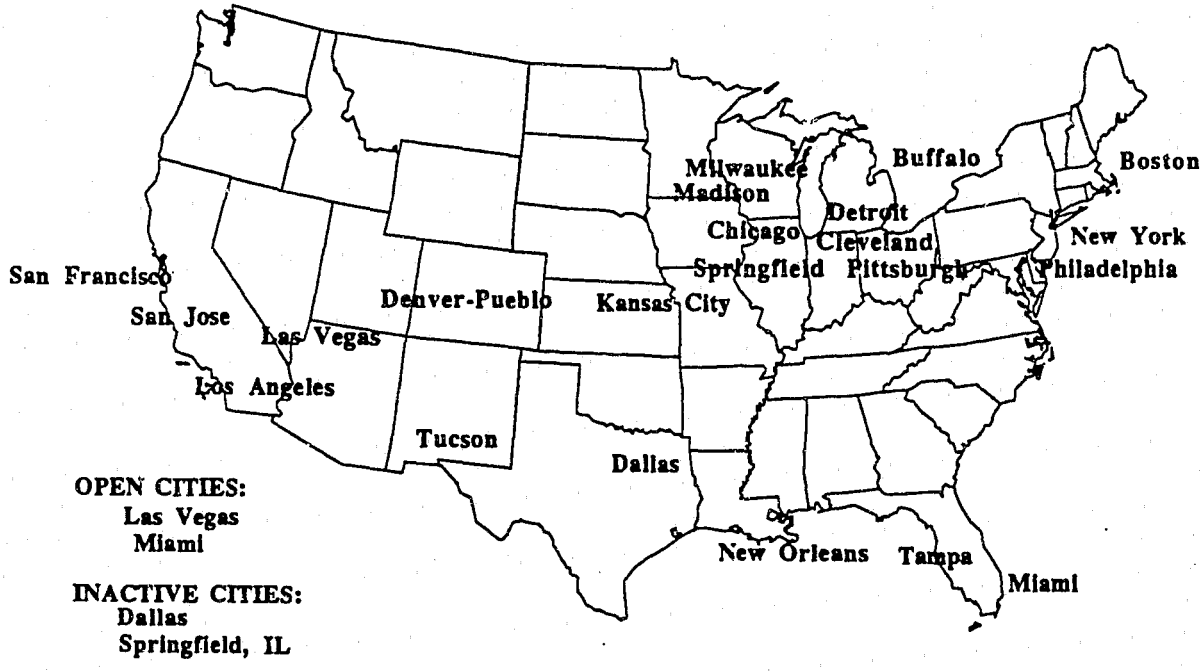
  —The **President's Commission on Organized Crime** (1986)

- Former Chief Justice of the U.S. Supreme Court **Earl Warren** was an active District Attorney in Oakland, California who aggressively investigated and prosecuted organized crime

- **Thomas E. Dewey,** most famous for his narrow, lost minute loss of the Presidential election to Harry S. Truman, was an aggressive and thorough prosecutor in New York working exclusively on organized crime

- **J. Edgar Hoover,** Director of the FBI, refused to believe there was any type of national network of organized crime. This was changed in 1957 with the meeting of The Commission in Apalachin, NY and following a series of organized crime battles and fighting over turf in Las Vegas. With Hoover's acknowledgment of large scale organized crime syndicates he initiated the Top Hoodlum Program (THP) which was to be the first nation-wide effort to fight organized crime

Cities With Italian-American Crime Families



CRIMINAL CASE PATHOLOGY

A PERSPECTIVE
CRIMINAL CASE PATHOLOGY

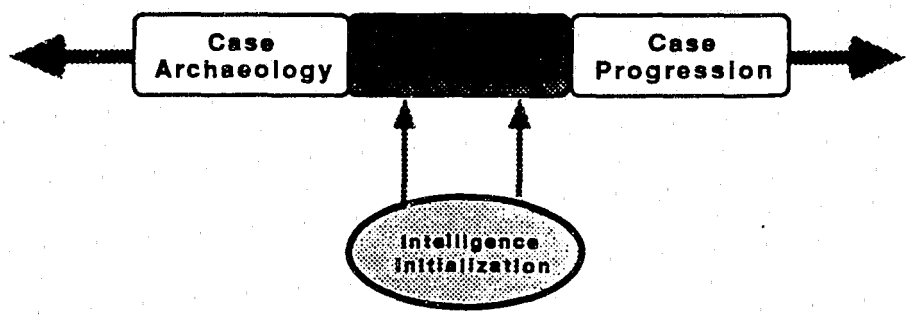
"You've got to have substantiated details to take the case to court. But you also need a well thought out plan—the big picture—to organize those details so the case will end in a successful prosecution."
New York City Drug Prosecutor

When beginning the intelligence cycle an analyst should have a clear picture of the progression in case development. The intelligence cycle is an application of the scientific method to assess and control information for the application of logic to develop a criminal case. By case pathology, one must recognize that the parameters of inquiry expand in diverse directions. As a result there is a somewhat different mind set needed, particularly for information collection.

When one enters a case for intelligence applications, it is because of the case's seriousness or complexity as well as an undeveloped foundation of information indicating the presence of crime and potential criminal suspects. The intelligence casefile is initialized at some point in the midst of the criminal enterprise. Because of this there are two **conceptual** strategies which must be employed with their subsequently developed information "entered" into the intelligence cycle. These strategies may be classified as **case archaeology** and **case progression.**

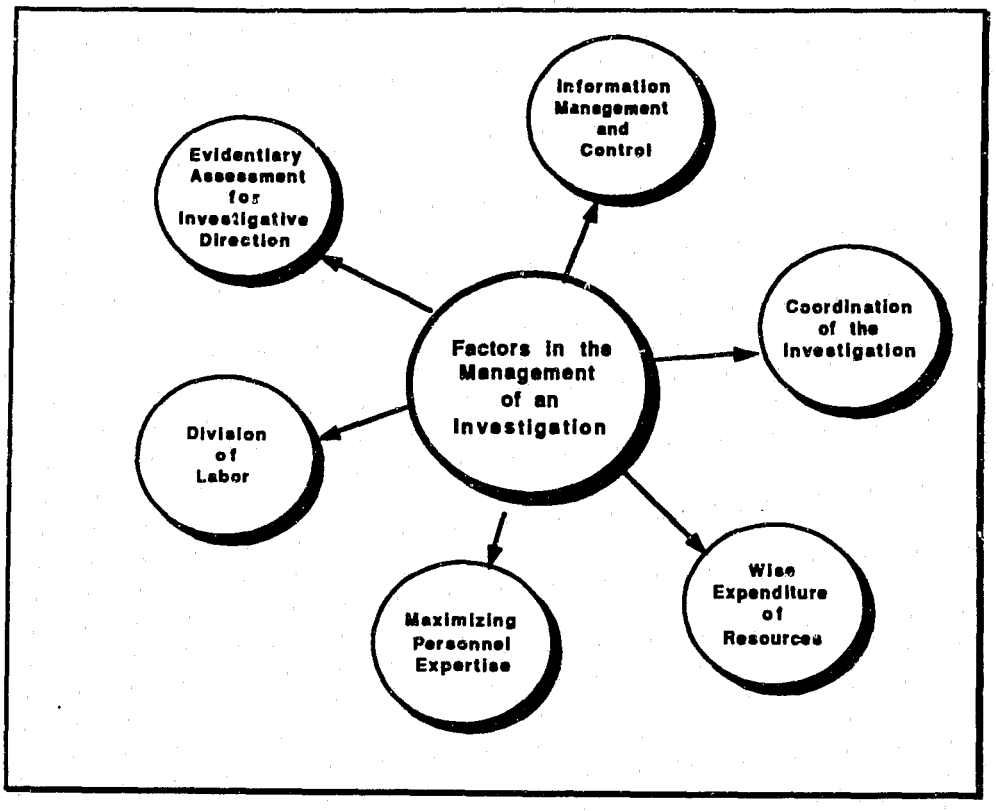
Case archaeology is looking back at the origins and characteristics of the case to understand its dynamics. Archaeology is the scientific study of cultures through examination of artifacts. The analogy for criminal investigation is that there is a scientific inquiry into the criminal enterprise (i.e., the culture) through examination of records, victims, and related evidence (i.e., the artifacts of the criminality). Thus, **case archaeology** is concerned with developing an understanding of the environment and practices surrounding the criminal enterprise which led to the decision to target the case for intelligence analysis. Obviously, this purpose is to establish an evidentiary foundation, identify the direction for further investigation, and to hone the criminal target(s).

While archaeology looks back, **case progression** looks forward from the point of initialization toward the goals of the inquiry. It relies on what is known and, more importantly, what is learned from the archaeological exercise to take the case further. Developing an undercover or sting operation, cultivating informants, and conducting surveillance all illustrations of activities which are used to take the case forward to ensure that there is suffi-



cient evidence of reliable quality to sustain the burden of proof in the case.

This pathology should be viewed on a continuum so that the investigation no only transcends the two perspectives but also integrates them. This conceptual exercise is a planning tool which can help manage the investigation to enhance efficiency and effectiveness. Management of the investigation involves a variety of activities as noted in the figure below.



CIPA:

CLASSIFIED INFORMATION PROCEDURES ACT

A PERSPECTIVE
CLASSIFIED INFORMATION PROCEDURES ACT

"I got some great information on dope coming into our airport from a guy in Customs—then he says I can't use it because it's classified. Why the hell did he even tell me?"
Statement of a Florida police officer

Since the days of Watergate, complexities became apparent when criminal investigations and prosecutions were pursued in cases where relevant information had been classified by the U.S. Intelligence Community for national security reasons. This problem has become even more prevalent since President Reagan declared narcotics and drugs to be a national security threat. Previously, this problem had been handled through informal agreement and plea negotiations. In order to deal with this more effectively, Congress passed the **Classified Information Procedures Act** [Public Law 96-456, 94 Stat. 2025, Codified at 18 U.S.C. App. (1982)].

"Graymail" refers to the situation where a criminal defendant threatens to disclose classified information during the course of a trial in the hope that the government would rather forego prosecution than suffer disclosure of the information [*United States v. Smith*, 780 F.2d 1102, 1105 (4th Cir. 1985)]. So long as the threat of disclosure is a real one, the defendant may enjoy immunity from prosecution [*United States v. Collins*, 720 F.2d 1195, 1197 (11th Cir. 1983)]. "Sensitive regard for national security was seen as having resulted in foregoing prosecutions for serious crimes, even in cases where the chances were great that, properly handled prior to trial, a defendant could well have been accorded due process without any cost in public revelation of classified information" [13 A.J.Crim.Law 277 (1986)].

The Classified Information Procedures Act (CIPA) was enacted by Congress in 1980 to deal with the growing graymail problem. CIPA is an omnibus act containing pretrial and trial procedures to be applied whenever classified information may be involved in a criminal case. In its effort to combat graymail, CIPA must reconcile two conflicting interests:

- The defendant's right to a fair trial, and
- The government's need to protect national security information involved in the trial.

"Classified information", for purposes of the act, means "any information or material that has been determined by the United States Government pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data as defined in ... the Atomic Energy Act of 1954." "National security", as defined in the act, means "the national defense and foreign relations of the United States."

CIPA statutory elements address:

- Pretrial Conferences
- Protective Orders Against Disclosure of Classified Information
- Discovery of Classified Information by Defendants Based Upon a "Sufficient Showing" of need
- Notice of Defendant's Intention to Disclose Classified Information
- Procedures and Hearings for Cases Involving Classified Information
- Interlocutory (Intervening/Provisional) Appeal Procedures
- Introduction of Classified Information as Evidence
- Security Procedures

Future Issues In

Intelligence Applications

FUTURE ISSUES IN INTELLIGENCE APPLICATIONS

AN ADDENDUM TO THE MONOGRAPH

LAW ENFORCEMENT INTELLIGENCE OPERATIONS

Prepared by:

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University
East Lansing, MI 48824-1118

(517) 355-2197

A PERSPECTIVE

FUTURE ISSUES IN INTELLIGENCE APPLICATIONS

"Our destiny rules over us, even when we are not yet aware of it; it is the future that makes our laws for today."
Nietzsche

It has been said that "the only way to predict the future is to have the power to shape it". Any work which attempts to forecast occurrences and needs for the future is obviously limited by spurious events—whether they are social, political, economic, or technological—that effect logical reasoning in the extrapolation of known trends. We can solidify the future by anticipating, as best we can, factors which will affect us and then make plans to deal with those anticipated events. The future issues discussed below are both logical and reasonable. Their "roots" already exist in law enforcement and we need only to look at our evolving socio-political culture to acknowledge their realistic potential as concerns for law enforcement intelligence. The forecasts are offered as milestones for introspection and planning in order to deal with the changing world of crime and law enforcement.

A Perspective on Preparing for the Future

Looking at trends and examining the future gives us a **target of opportunity** to identify and solve problems. It requires a willingness to be open to alternate ideas; creativity; flexibility; and acceptance of propositions which may be counter to long-held beliefs. It is not easy to be on the forefront of change—it is frequently an uphill battle requiring one to battle the *status quo*. Because changes in our techno-socio-political-world-economy are occurring at such a rapid pace, law enforcement must be willing to leap ahead instead of lagging behind. In law enforcement, we were behind the private sector in the use of motor vehicles; in the adoption of radio communications; in the application of contemporary management principles; in the adoption of computers; in keeping up with the evolution of computer technology; in adopting a regional perspective of responsibilities; and in the recognition of international influences on local problems. Capitalizing on **targets of opportunity** for the future will permit law enforcement to better prepare for changing crime problems.

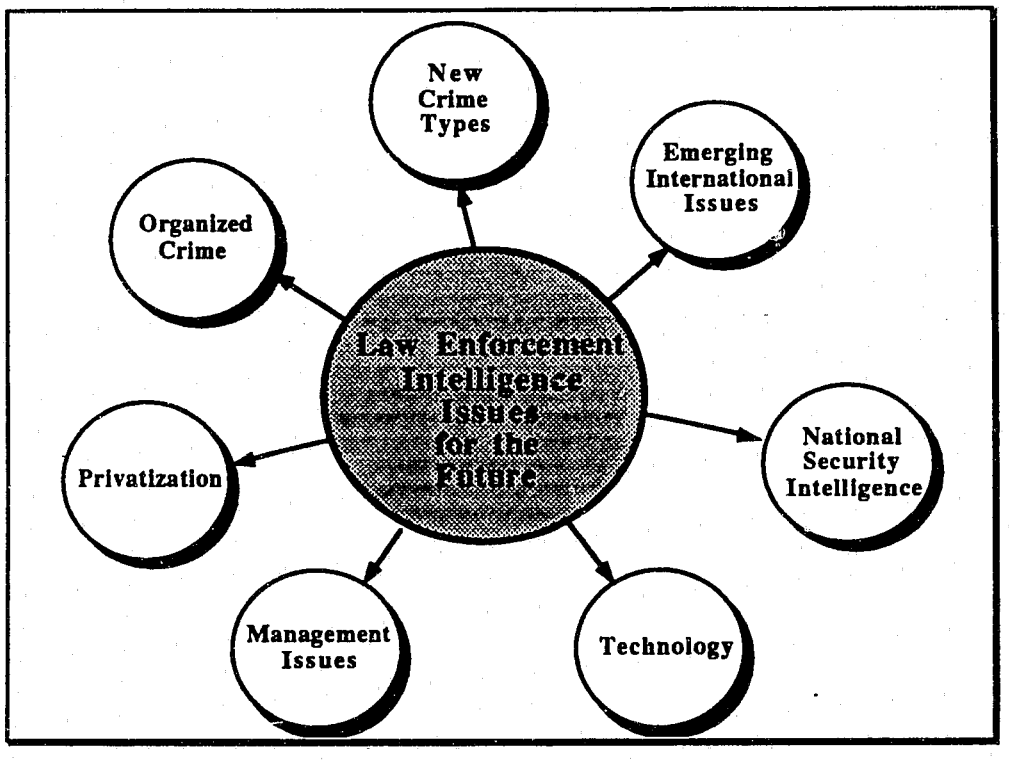
A. Just as important—perhaps more so—as looking at how we can improve intelligence operations today, is looking at the future

B. LAWINT operations will be affected by social and technological changes just as the rest of society—we need to look ahead and point our goals, and expertise toward future intelligence needs

C. Future Crime Issues

1. **Organized Crime (OC)**

a. More sophistication (more college graduates)



b. Line between legitimate and illegitimate activities more difficult to determine

c. Ventures into "nontraditional" crime areas (as described below)

A Perspective on Changes in Organized Crime

Just as Prohibition was a watershed for the development of "traditional" organized crime, information and technological developments as well as environmental issues and concerns shall be the stimulus for changing

criminal enterprises—albeit less violent, the economic impact and the number of potential victims (both proportionately and numerically) from these "nontraditional" crimes will dwarf Prohibition.

d. Ethnic Based Organized Crime Cartels

1) Italian/Sicilian (Traditional Organized Crime)

2) South American/Hispanic (Notably drug trafficking)

3) Caribbean (Notably drug trafficking and money laundering)

4) Asian (Asian Triads, tongs, and street gangs involved in drug trafficking, extortion, and "protection")

5) Slavic Crime groups (Strong potential for black marketing)

A Perspective on Ethnic-Based Organized Crime

Ethnic-based organized crime emerged as a "force" in criminality in the late 1800s and early 1900s. The most noted ethnic crime groups were Italian, Sicilian, and Irish; in many cases, first generation immigrants. Criminality was *not* a function of ethnicity. Rather, ethnicity—culture, language, kinship—served as a *bond*: it was a foundation for trust and camaraderie. This will become more pronounced as other ethnic-based organized crime groups emerge. Moreover, because of La Cosa Nostra's experience with informers, lingual differences, and physical attributes, the "new" ethnic-based organized crime cartels will be more difficult for law enforcement to penetrate.

2. Types of Crime

a. Environmental Crime

1) Pollutants, improper refuse disposal, improper hazardous waste disposal, involvement of OC in environmental crime

2) Water-related Crime (bootleg water cleansing, water diversion, corruption)

b. Money Laundering

c. Theft by computer—a study by the Florida Department of Law Enforcement (FDLE) found that 25% of the businesses surveyed in that state *reported* that they had been the victim of some type of

involved in such crimes. FBI Futurist William Tafoya asks, "What type of message do these penalties send to potential computer criminals."

f. Counterfeiting (merchandise and such things as computer hardware, computer software, any type of material item—jeans, watches, etc.)

g. Stock and securities manipulation and fraud

A Perspective on "Enterprise Crime"

Money laundering, computer crimes, information crimes, counterfeiting, "white collar crime", and drug trafficking are increasingly being referred to as **enterprise crime**—particularly on an international basis—because of their characteristics that:

- The motive of the crime is **profiteering**
- On a large scale, the crimes require **organizations** or **networks**
- The crimes are typically of an **on-going nature**
- The crimes are **multi-jurisdictional**; frequently **multi-national**
- The crimes involve some type of "**marketing**" directed toward clientele

h. Riots & civil disorders

A Perspective From The National Advisory Commission on Civil Disorders

"Police departments must develop means to obtain adequate intelligence for planning purposes, as well as on-the-scene information for use in police operations during a disorder".

i. Violence

j. Bias/Hate crimes (including "domestic terrorism" as discussed below)

k. Kidnapping for "Slavery"

A Perspective on Kidnapping for "Slavery"

According to research by Dr. William Tafoya of the FBI's Behavioral Science Unit, there appears to be increases in the kidnapping of young men and women for sexual pleasure and servitude. The "clients" are generally wealthy foreign "benefactors" in other countries (notably Germany, Thailand, and the Middle East). The possibility should be explored that some young people listed as missing or as "runaways" could be victims of these types of kidnapping.

computer crime. It is important to note that different approaches to investigating computer offenses must be developed to look at offenses committed both by employees and persons outside of the organization.

A Perspective on Computer Crime Investigations

As a result of the FDLE study, a training program was developed to specifically address the issues and idiosyncrasies of these investigations. As an outgrowth of these training sessions a new organization was formed: The Florida Association of Computer Crime Investigators (FACCI).

d. Information Crime (e.g., Theft of Trade Secrets)

A Perspective on Information Crime

- The impetus for the growth in drug trafficking has been the **"big dollar"** benefit—it is an econometric phenomenon
- Information on rapidly *growing technologies* and *trade secrets* is worth **"big dollars"**
- This information is no longer just locked in vaults—it is stored as electronic impulses in computers
- These computers are frequently accessible from virtually any telephone with a personal computer and modem and the information is blocked from the thief by only some keystrokes in the security protocol
- The information could also be easily be removed by an "inside man" on easily concealed disks
- Tracing this lost information—even *detecting* that the information has been copied and stolen—can be almost impossible
- Information crime is costing us **millions—if not billions—of dollars** in addition to putting both our **personal security** and **national security** at risk (BloomBecker, 1990).

e. Computer systems' sabotage through the use of "malicious software" (e.g., Trojan Horses, Worms, Viruses)

A Perspective on Computer Crime "Justice"

The relatively few people who have been convicted of computer crimes—particularly "hacking" and "malicious software" types of crimes—typically receive light sentences. The lack of violence or a clearly discernable victim apparently contributes to this, despite the cost and wide-ranging effects

1. Terrorism

1) There are a number of definitions—one which addresses virtually all of the elements is from an Army publication:

> **Terrorism** is the calculated use of violence or the threat of violence to attain goals, often political, religious, or ideological in nature, through instilling fear, intimidation, or coercion. It involves a criminal act, often symbolic in nature, intended to influence an audience beyond the intended victim (U.S. Army, n.d.).

2) Important elements to recognize in terrorism include:

- Violence or threat of violence
- It is ideologically based

3) Terrorism can be from either end of the political spectrum—it can also be...

- Domestic terrorism, or
- Transnational terrorism

4) Comparatively speaking, we in the United States have been relatively free from terroristic threats and acts

5) Our "targeting hardening" for potential terroristic acts have traditionally been based on what **we intuitively** believe would be targets

6) LAWINT needs to develop a strong **cultural understanding** of groups posing terroristic threats and harden targets in light of that cultural perspective

7) With respect to the future of terroristic threats, we need to carefully examine the threat in the months following the Persian Gulf War

a) Recognizing that the cultural dynamics are different in Islam

b) It is the nature of Islamic culture that **insults and injury are neither easily forgiven nor forgotten**

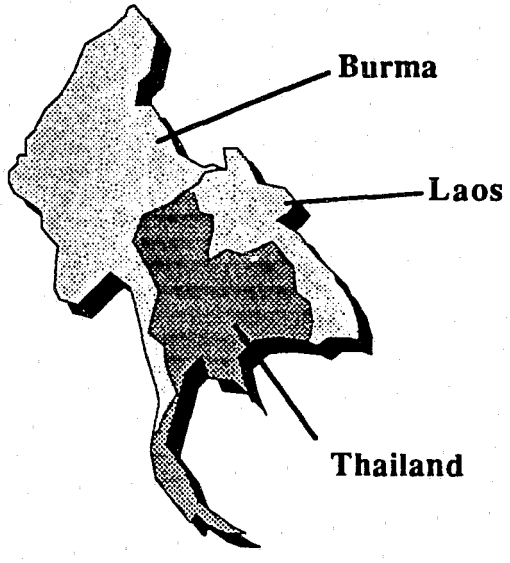
a) A report from the United Nations Economic and Social Council of February 1991 noted "the recent upsurge in the involvement of nationals of other regions...in illicit traffic in heroin from Asia and the Pacific" (UN, *Commission on Narcotics*, Report # E/CN.7/1991/4, 1991).

b) The same report also noted that...

- "the illicit production of heroin was on the increase in the 'Golden Triangle' and in the 'Golden Crescent' ";
- And that "...the quality of heroin seized was increasing..."

c) Strategic intelligence reports of the Drug Enforcement Administration predicted these quantitative and qualitative changes in heroin trafficking in 1988 (Westrate, 1988).

Countries of the "Golden Triangle"
Primary Sources of Opium Production for Heroin



Countries of the "Golden Crescent"
Heroin Source Countries of Growing Activity

D. The Emerging International Perspective in LAWINT

1. International crimes and criminal transactions as a result of:

   a. Communications technologies

   b. Computer transfers of information

   c. Satellite data, text, and image transmissions

   d. Increased ease of travel worldwide

A Perspective on World Travel

Currently we can travel from Los Angeles to Tokyo in 12 hours or New York to London in 6 hours on a Boeing 747. When the "stratojet"—an airliner traveling just above the earth's atmosphere—comes on line, it will make the Los Angeles-Tokyo flight in 4 hours and the trip between New York and London in 2 hours. Because of aircraft size and efficiency, the costs will comparable to, or less than, current jet air fares to these locations.

2. European Economic Community (New types and dimensions of economic crimes and information crimes; greater flow of criminals through the European Community)

   a. The "Trevi Process"—so named for the meeting of the EEC Council of Ministers in Trevi, Italy—expressed concern for international crime as it relates to the EEC

   b. Specifically the Ministers:

      1) Went on record emphasizing the need for law enforcement intelligence

      2) Expressed the need for integration of national security intelligence issues with LAWINT

      3) Developed for EEC working groups to deal with:

         • Drug trafficking
         • Crime
         • Terrorism
         • Illegal immigration

c) It is because of this, that future terroristic acts at targets consistent with "fear generation" be incorporated into any related intelligence activities

8) Potential terroristic targets which bear particular scrutiny include **Apple Pie Targets**—those which are symbolic of important things in American life (e.g., entertainment, auto production, fast food restaurants, etc.)—Reasons:

- They have important symbolic status
- They typically have less security than "high profile" targets such as airports or power plants

A Perspective on Terroristic Targets

A 1991 survey by Guardsmark, Inc. of corporate security directors and senior executives in 100 of the Fortune 500 companies asked about terroristic targets. More than one-half fear their companies will be a target of terrorism. Almost three-fifths believe such an attack will occur in the United States in the next few weeks and more than one-third believe terrorists will strike the cities in which their companies are headquartered.

m. Drugs

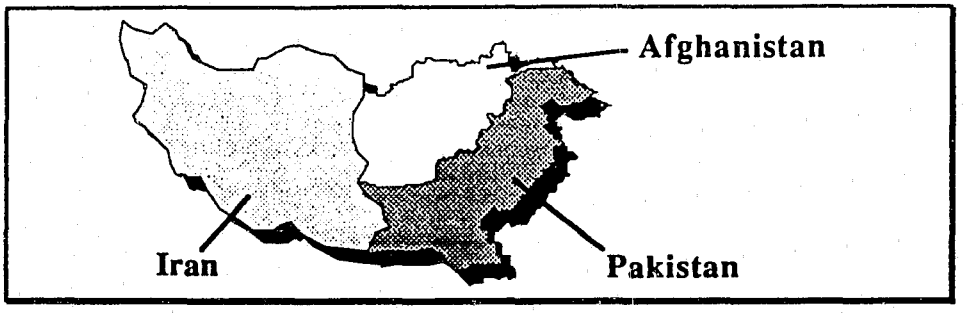
1) Drugs will continue to be a problem for law enforcement

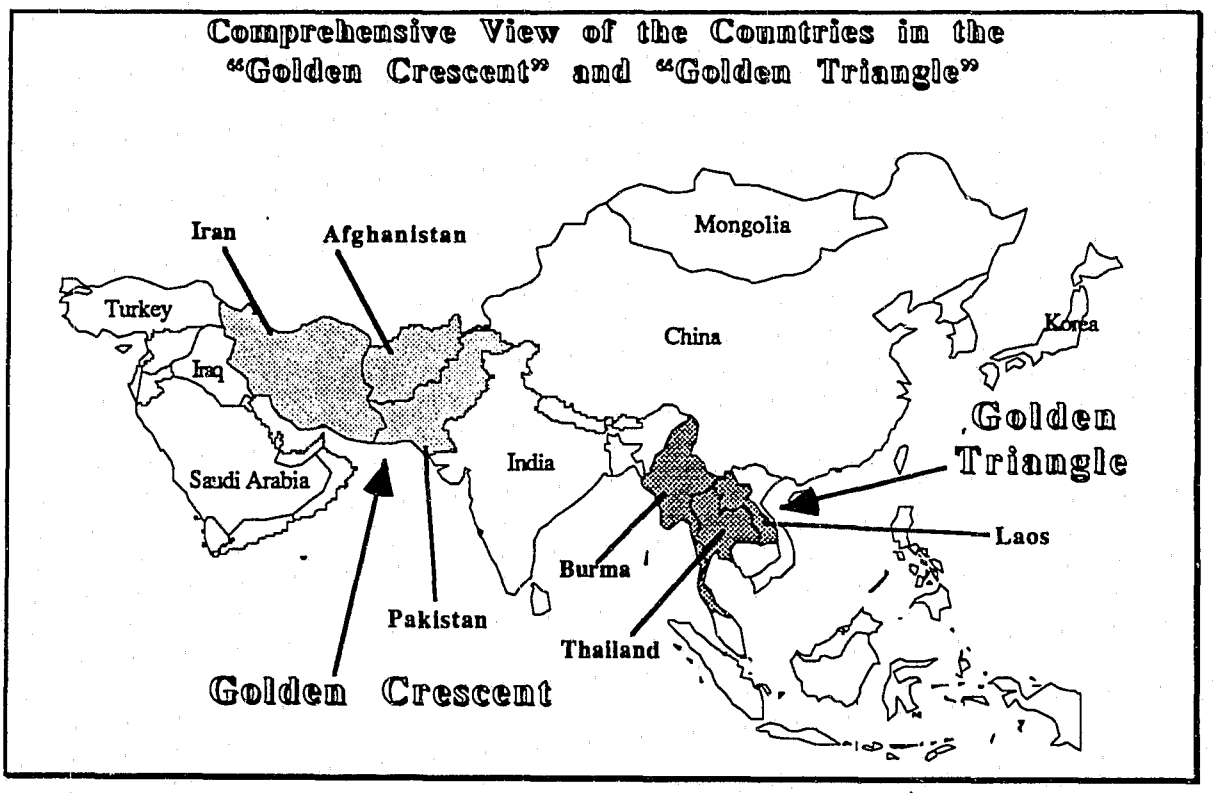
2) We must be prepared to deal with **changes** in drug trafficking patterns—not get caught in a recurring pattern

3) Look for changing trends in drug trafficking and use in your area—via **strategic intelligence**—and prepare for emerging changes

4) One useful approach is econometric market analysis—dope is **big business**, thus look at it as such

5) Particularly keep your eye on **heroin**





d) The challenge for LAWINT is to:

- Look ahead for new avenues and techniques of heroin trafficking
- Examine the potential impact of heroin trafficking on current enforcement efforts, resources, and personnel
- Identify the changing distribution markets which will have to be understood and penetrated for successful investigations

4) Britain is urging the EEC Council of Ministers to develop regulations to permit inspections of bank accounts and confiscate their contents where there is reasonable suspicion that the monies are used to finance terrorism (Germany and France are the most reluctant EEC members to approve this)

c. The motivation for creating the EEC was to enhance Europe's economy and industry—this will effect bot legitimate and illegitimate (criminal) economic motivations

E. National Security Intelligence (NASINT)

1. Greater integration of NASINT with LAWINT even at the local level

2. This will...

a. Create greater problems of information sharing

b. Create problems for evidence admissibility

3. Greater need for state and local law enforcement to become familiar with the Classified Information Procedures Act (CIPA)

4. Require the greater use of multi-agency task forces which includes all levels of government (the Organized Crime Drug Enforcement Task Forces may serve as a model for other areas)

5. The following portion of a Presidential Order serves as an example of the recognition of NASINT and LAWINT interaction:

A Perspective on NASINT
Executive Order 12333
United States Intelligence Activities (Excerpt)

2.6 *Assistance to Law Enforcement Authorities*: Agencies within the Intelligence Community are authorized to:
(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community;
(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or intentional terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency; and
(d) Render any other assistance and cooperation to law enforcement agencies not precluded by applicable law.

F. Technological Applications

1. Artificial Intelligence for...

   a. Analysis

   b. Profiling

   c. Information Identification (The "Knowledge Navigator" where Artificial Intelligence/Expert Systems helps identify sources for the type of information you need)

      NOTE: This could be most helpful for LAWINT to find the diverse types of archive, registry, vital statistics, and similar information needed in a wide range of files maintained by various organizations and agencies

2. Inter-AFIS Communications

3. DNA Computer files

4. Bar coding

5. Compact Digital Disk image storage

6. Cellular phone scanners

7. Tempest systems

8. Computer-chip driven radiating and non-radiating listening devices

9. Computer enhanced audio and video surveillance technologies

G. Management Issues

1. A "rediscovery" of intelligence by managers—a renaissance of intelligence this has largely been influence by drugs, RICO, and Asset Seizures

2. Greater use of strategic intelligence (need to develop this expertise if it is not developed already)

A Perspective on Strategic Intelligence

"President Kennedy's assassination in 1963 occasioned a critical review of the intelligence capabilities of the Secret Service, the FBI, and the CIA as well as many state and local criminal justice agencies. The Warren Commission Report criticized the FBI in particular, and called for expansion of **preventive intelligence** capabilities" (Emphasis added). **NOTE:** After nearly twenty years, preventive/strategic intelligence is still getting relatively little attention.

3. Greater policy structure and control—influenced by CALEA, Liability cases, recent restrictions imposed on police records as a result of court cases and DOJ rules; FOIA, Privacy Act

4. Wider application of intelligence (beyond OC, racketeering, drugs, outlaw motorcycle gangs, etc)

5. Reciprocal integration of intelligence activities with Community/Problem-Oriented Policing

6. Greater use of regional intelligence task forces and Intelligence Mutual Aid Pacts between agencies within defined regions

7. The use of Task Forces to address complex investigations

A Perspective on Task Forces

As crimes become more multi-jurisdictional and more substantively complex (e.g., computers, accounting, corporate covers, etc.), task forces will become not only the best, but perhaps the only, way to conduct effective investigations. Such task forces would be made up investigative specialists who can address the legal, technological, and methodological dynamics of these crimes.

8. Future Personnel Needs

   a. Bilingual personnel

b. Bicultural understanding (e.g., culture, norms, beliefs)

c. Computer Tracing and Analysis

d. Accounting

e. Economic systems and the stock market

f. Image interpretation

g. Crime analysis

h. Forecasting

i. Empirical research

j. Long range planning

G. Privatization Issues

1. Increased "private policing"

2. Significantly growing sophistication and expertise

3. Private policing industry is currently growing dramatically in many dimensions

A Perspective on Private vs. Public Police

In many areas—such as, computer crime investigations, executive threat assessment, theft of trade secrets—"private police" organizations are probably *more* sophisticated and aware of the problems than most public law enforcement agencies. One reason is the economic motivation, but it also involves the ability to laterally develop personnel expertise and to more easily apply innovation, creativity, and flexibility in program areas.

4. EXAMPLES:

- **Ford Motor Company**

- Facility and resource protection (including computer systems, satellite)
- Trade secrets
- Executive protection

• **Aerospace Industry**
- Significant technological developments
- Significant national security issues in weapons systems

5. Incredible amounts of information available on

   a. Employees

   b. Clients

6. Organizations like **Guardsmark™** already perform intelligence analysis—many organizations perform strategic intelligence

   a. Law enforcement needs to become more familiar with the myriad of organizations—many very subtle—which perform intelligence work

   b. Many of these private organizations' concerns cross between LAWINT and NASINT

7. Law enforcement needs to begin opening doors and coordinate efforts—don't look at these groups as simply "rent-a-cops"

8. Law enforcement also needs to develop policies and standards to *share* information; not just receive it

A Perspective on
Public and Private Police Cooperation

Recognizing that "The police cannot provide all the protection and enforcement necessary to maintain safe and orderly communities", the New York Police Department created a program called **APPL—Area Police-Private Security Liaison Program**. The APPL program encourages personal contact at all levels of the chain of command between the public and private police to share information on crimes, criminals, and crime-related issues (Voelker, 1991).

H. Principles for the Future—Elements for Planning and Change

1. **Progress is most likely when all players believe they have received what they need**

   - Are your goals and objectives in place?
   - Are you meeting the intelligence needs of your jurisdiction and agency?
   - Have you made changes in your target focus?
   - Have you kept up with changes in crime and crime trends in your jurisdiction?
   - Have you kept up with changes in the criminal enterprises of targets (notably organized crime groups)?
   - Are you keeping up with the most current resources and techniques for collection and analysis?

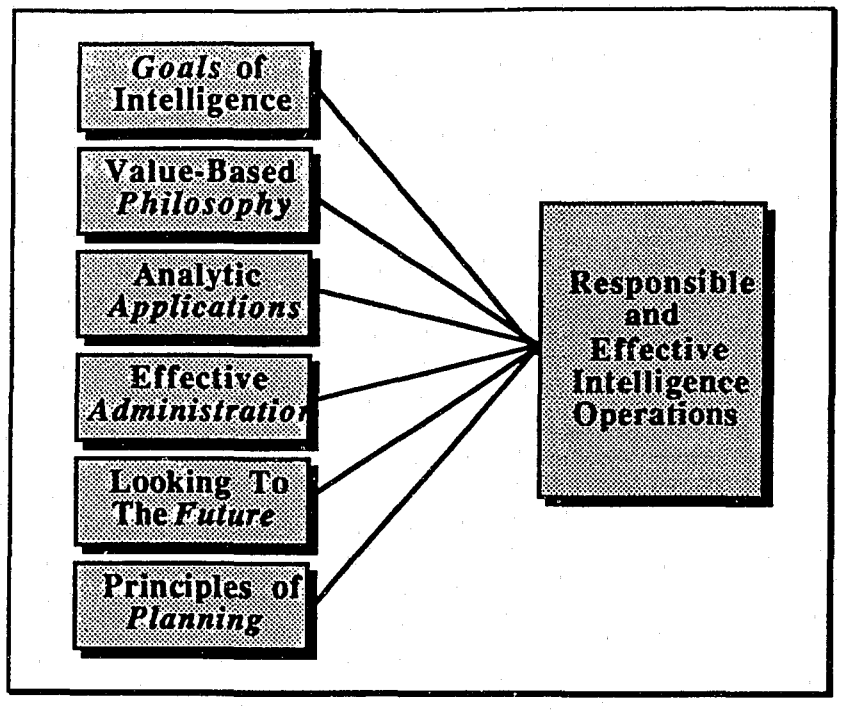
2. **All players do not need the same things, but all players need something**

   - Are you providing the right kind of information to investigators?
   - Are you providing the right kind of information to administrators?
   - Are you providing the right kind of information to outside agencies?
   - Are you providing diverse analytic techniques?

3. **No matter how comprehensive your intelligence unit is, it will have limitations**

   - Not all cases, no matter how "big" or important will produce sufficient evidence for successful prosecution
   - Not all important crimes and events will be identified or projected by strategic intelligence.
   - Because of economic, political, or jurisdictional limitations, not all crimes or criminals can be pursued by the intelligence unit regardless of the desire of the unit's personnel.
   - Because of the nature of the intelligence function, criticisms of the unit's activities and its effectiveness will undoubtedly surface periodically.
   - The effectiveness of the intelligence function will always be influenced by the quality of its personnel and the amount of support received from the department's administration.
   - Have you assessed success or failure—are efforts and activities subject to periodic evaluation?

4. **The future of law enforcement intelligence must be viewed interactively with all intelligence responsibilities**


Goals of Intelligence
Value-Based Philosophy
Analytic Applications
Effective Administration
Looking To The Future
Principles of Planning
Responsible and Effective Intelligence Operations

BIBLIOGRAPHY

Bennett, G. (1991). "Cultural Lag in Law Enforcement: Preparing Police for the CrimeWarps of the Future." *American Journal of Police.* Vol. XI, No.3:pp 81–126.

BloomBecker, B. (1990). *Spectacular Computer Crimes.* Homewood, IL: Dow Jobes-Irwin.

Bureau of Justice Statistics. (1990). *Criminal Justice in the 1990s: The Future of Information Management.* Washington: U.S. Government Printing Office.

"Saddam Hussein's Second Front: Terrorism." (1991) *The Lipman Report.* Memphis, TN: Guardsmark, Inc.

Owen, R. and M. Dynes. (1990). *The Times Guide to 1992: Britain in a Europe Without Frontiers.* 2d ed. London: Times Books, Ltd.

Tafoya, W.L. (1990a). "Forward". *Computers in Criminal Justice.* Bristol, IN: Wyndham Hall Press.

Tafoya, W.L. (1991). "Understanding Resistance to Change: Implications for the Future of Policing." *American Journal of Police.* Vol. XI, No.3:pp 183–88.

Tafoya, W.L. (1990b). "Rioting in the Streets: Deja' Vu?" *C.J. the Americas.* Vol. 2, No. 6:1, 19—23.

Tafoya, W.L. (1988). *A Delphi Forecast of the Future of Law Enforcement.* Doctoral dissertation (Criminology and Criminal Justice, University of Maryland, College Park MD.

United Nations. *Report of Commission on Narcotic Drugs.* Report # E/CN.7/1991/4, Vienna, Austria.

United States Army (n.d.). "Countering Terrorism and Other Major disruptions on Military Installation." *Army Regulation 190–52* Washington, DC: U.S. Army.

Voelker, A.M. (1991). "NYPD's APPL Program: A New Partnership." FBI Law Enforcement Bulletin. (February, pp. 1–4).

Westrate, D.L. (1988). "Projected Changes in Drug Trafficking Patterns". Presentation to the *Attorney General's Working Group on Reducing Violence in America.*". Washington, DC.

ASSET FORFEITURE

ASSET FORFEITURE

Bulletin

August 1988

Funded by
Bureau of Justice Assistance

INSIDE:

FOLLOW THE MONEY

Three New BJA Asset Forfeiture Reports Show How

"Follow the money" was Deep Throat's advice to a reporter trying to get to the bottom of the Watergate scandal. The phrase since has become a slogan for investigators trying to unravel complex racketeering and narcotics conspiracies. It's good advice for law enforcement agencies seeking to seize the assets of elusive drug dealers.

Three recent reports show how to follow the money—and other assets—of drug traffickers through mazes of banking and public records. The reports are products of the Asset Forfeiture Training and Technical Assistance Project operated under a cooperative agreement between the Bureau of Justice Assistance and the Police Executive Research Forum.

Financial Institutions

"Bank records are probably the single most important source of leads to assets that can be seized" under RICO (racketeer influence and corrupt organizations) statutes and kindred federal laws and their clones at the state level, according to Charles H. Morley. A former investigator for the Internal Revenue Service and the U. S. Senate, Morley is author of the Asset Forfeiture Project's *Tracing Money Flows Through Financial Institutions.* He writes that the "more you know about tracing transactions through banks, the better you will be able to use these laws in your investigations."

Morley's guide to money flows rests on this proposition: "Tracing transactions through a bank is like any other asset-tracing procedure—you search for the ultimate source of funds coming into the bank and you search for the ultimate disposition of funds leaving the bank. Both ends of the transaction can lead you to hidden sources of income, hidden assets, previously unknown witnesses, and other principals."

> Bank records are probably the single most important source of leads to assets that can be seized

But first investigators have to know how transactions move through bank accounts. The accompanying diagram from Morley's report provides basic information to help investigators analyze bank accounts (Diagram on page 2).

Bank Deposit Patterns

"Look for larger deposits," Morley says, "particularly if your subject is part of a large narcotics organization.... Be alert for business deposits that appear to be out of the ordinary, such as large, even amounts deposited in an account of a retail business where receipts are normally received in small, uneven amounts."

According to Morley, here are deposit patterns to look for: "At least two transaction of $10,000 or more on the same day; large deposits in rounded numbers; and repeated deposits of the same amounts, especially when they are deposited with noticeable regularity....

(cont'd on p. 2)

A GUIDE TO THE ASSET FORFEITURE PROGRAM

Asset Forfeiture Bulletin is one product of several from a cooperative agreement between the Bureau of Justice Assistance (BJA) and the Police Executive Research Forum. The agreement launched the Asset Forfeiture Training and Technical Assistance Project. Its purpose is to enable state and local criminal justice agencies to use their own laws, rather than federal statutes, to attack and seize the huge amounts of wealth that drug traffickers accumulate.

BJA, a part of the Office of Justice Programs in the U. S. Department of Justice, initiated the project in 1986 with $249,000 and added $1.625 million in late 1987. The latter funds were awarded under state and local assistance provisions of the Anti-Drug Abuse Act of 1986.

The new funding increased from four to 16 the number of states that can participate in a model forfeiture training program. The project also yields:

- Technical resource and reference guides on key aspects of asset forfeiture such as the role of financial institutions in money laundering and the use of undercover and other investigative techniques to identify assets liable to forfeiture.
- Funds for four state and local criminal justice agencies to begin or expand innovative forfeiture programs. The goal of the pilot grant program is to increase the forfeiture of valuable, often hidden, underworld assets such as bank and securities accounts, real estate, and legitimate businesses.

(cont'd on p. 5)

Follow the Money (cont'd from p.1)

Look for patterns in the timing of the transactions, such as deposits that occur shortly after an observed narcotics transaction. These patterns are not only indicative of criminal activity, but may provide probable cause for search or arrest warrants or for civil seizure of assets."

He says that an account may warrant a complete search if it is obviously used for money laundering or if it is a hidden account.

"There are some classic examples of cases that have been broken by detection of small, seemingly insignificant items in a bank account," Morley says. "Hidden real estate in another town has been discovered by small payments on utility bills, phone bills, retail charges out of town, taxes or insurance. Hidden brokerage accounts either in or out of town have been discovered by similar small payments of interest on a margin account paid from a known bank account."

Loans, Cash, Wires

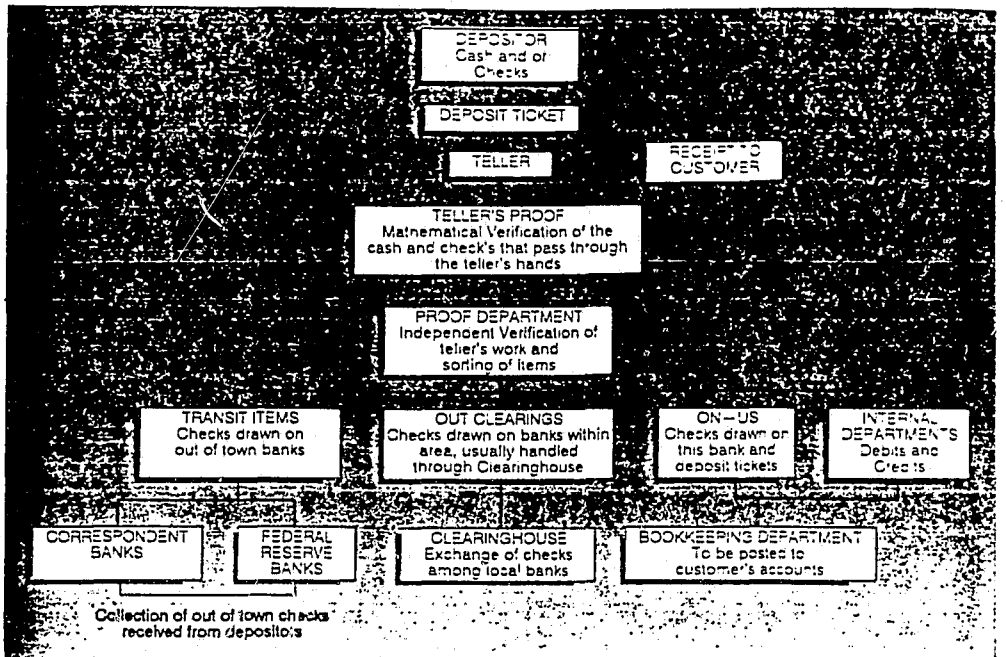
Besides bank accounts, other bank-related transactions can be fertile sources of information about hidden assets.

Loans. Banks usually maintain three types of loan documents: the loan ledger, the loan application, and the loan correspondence file. Morley advises investigators first to analyze loan ledger entries. He says "this analysis will help ... determine which follow-up records to request, if any. For instance, a normal business operating loan with regular repayments from the business bank account may require no follow-up. On the other hand, unusual loans should be traced from beginning to end."

Unusual loans include those where no record exists of loan proceeds going to the subject's bank account. This is contrary to normal banking practice and investigators may find "the funds went to another account and were used to purchase an undisclosed asset," according to Morley who includes this other advice about loans:

- Loan records can show when a bank in collusion with a subject. Examples are loans that are long overdue or loans that violate bank policy.
- A loan that appears far beyond a subject's ability to repay may also indicate collusion.
- Lump sum loan repayments, loan payments in odd amounts, payments that are consistently late, and payments that do not come from a subject's bank account also should raise investigators' suspicions.

In many loan cases, investigators "are looking for leads to other people or to other assets," Morley says. "You may find hidden accounts where the loan proceeds went or accounts that were used to make loan payments. Loans are frequently secured by hidden assets or may be cosigned by previously unknown associates."



Tracing Transactions Through Bank Accounts

1. Transaction entry points start with tellers who receive customer deposits directly, through the mail or from automatic teller machine; with a memo entry from another bank department; or with input from a bank's cash services department which handles large cash deposits from customers such as retail stores.
2. Transactions next go to the proof department where a bank (a) assigns each item an encoded number so that it can be located in record systems; (b) encodes each item with an MICR number (the series of computerized numbers that appear at the bottom of checks); (c) microfilms each item; and (d) enters each item into bank computer systems. Items that enter a bank are generally filmed together in the order in which they entered.
3. Next high speed computers, reading the encoded numbers, batch all entered items to facilitate processing. Items generally are batched in four or more categories: (a) "on-us" items are those that can be cleared completely within a bank; (b) clearinghouse items must clear through other local banks and thus use a central, local clearinghouse; (c) transit items are drawn on out-of-town banks and thus are processed outside a bank's area through correspondent banks and Federal Reserve banks; (d) items that require special bank handling, which include cashier's checks, debit and credit memos, certificates of deposits, loan transactions, and wire transfers.
4. The final step in account transaction processing involves the bookkeeping department where all items eventually end up and are filed in a way that allows quick retrieval. Bookkeeping maintains all files, searches them for other departments, and often contains a bank's error resolution unit.

Source: *Tracing Money Flows Through Financial Institutions*

[redacted]h. Investigators who believe a sub- [redacted]s using cash-for-cash transactions have to rely primarily on bank branch personnel where the transactions take place. "Pure cash-for-cash transactions are normally very hard to document," Morley says. "They generally require a search of all teller tapes and proof film by date, and even this isn't conclusive." But some banks now require customers to make deposits and withdrawals rather than exchanges and "this leaves a paper trail ... to follow."

Wire Transfers. "Once the bad guys think they have their money safe in a bank, they tend to attempt to launder their funds by wire transfers to other banks in the United States or abroad," Morley writes. But wire transfers hold no mysteries. "If you see a memo entry in the account pertaining to the wire, the bank can generally easily retrieve the documents pertaining to the wire," he says. These documents show who sent the wire and to which bank, along with the date and the amount.

Effective use of state regulatory agencies is [redacted]argely untapped investigative tool

Morley's report includes details on obtaining bank records, what records to request, specific steps on analyzing bank records, tracing disbursements, certificates of deposit, and cashier's checks.

Public Records

Besides banks, there exists another fertile source of information for uncovering the assets of narcotics traffickers. "Government records are probably the most accessible records ... available to assist in the hidden – asset investigation as it relates to real estate purchases or investments in a business enterprise," according to Frank R. Booth, a Pennsylvania – based law enforcement consultant. His report for the Asset Forfeiture Project is *Finding Public Record and Other Information on Hidden Assets.*

Particularly valuable are records kept at the county and state level. For example, a mortgage document filed at [redacted]e county recorder of deeds office [redacted]ntifies a lending institution that has [redacted]greed to finance the purchase of property," Booth notes. "This leads the investigation to possible sources of documentation and witnesses who know and have done business with the target of the investigation."

The county taxing authority provides another example. It identifies "who pays taxes on a property and where the billing notice is mailed," Booth says. "If the billing notice is mailed to a practitioner associated with the hidden owner, rather than the owner of record, a key lead has just been developed."

State Agencies

A valuable state-level ally for investigators seeking hidden assets can be the corporation bureau or office of corporate registry. Most states at a minimum require that a corporation provide this information: name and purpose of a corporation, names of corporate officers and directors, stock distribution, date of incorporation, and registered agent if any.

"In reality," Booth writes, "the sophisticated major offender will not file information that will aid the investigation effort. But all avenues must be thoroughly examined in seeking even the slightest opening of the corporate veil. For example, if filed information can be shown to be false, the investigation could use the corporation bureau's regulatory authority to revoke the charter of the front corporation. If this action is fought by the corporation counsel or other representative, the resulting conflict could further remove the veil of secrecy."

State licensing board and regulatory agencies require information that can provide a wealth of data about sources of business financing and bonding and insurance which, in turn, can be traced to hidden ownership. The same boards and agencies collect useful information about employment and occupations and the names of accountants and attorneys. In addition, a "regulatory or licensing authority may do more than license," Booth says. "It also may exercise the authority to suspend, fine or even revoke the license necessary for a business to operate – a powerful legal weapon. Effective use of state regulatory agencies is a largely untapped investigative tool."

Others Sources of Information

Besides public records, Booth examines other sources of information on hidden assets. Former property owners or lessors, realtors, title companies, accountants, vendors, tenants, and former employees can be vital to hidden-asset investigations.

As an example, Booth cites a company that "supplied a variety of vending machines to a bar and restaurant owned by a major criminal figure but fronted by an associate. The vending company offered an interest-free loan to the business for using their vending machines, with the loan being paid on a monthly basis from 50 percent of the vending machine receipts."

"The loan was substantial and of major concern to the hidden owner. As a result, he negotiated the loan repayment agreement and his name and a record of his involvement appeared in the vending company records. This was not conclusive evidence on its own, but served as a critical element that subsequently was combined with other investigative evidence in a successful hidden-asset investigation."

The Legal Basis

Michael Goldsmith, a law professor at Brigham Young University, takes a different approach to following the money and other assets of narcotics traffickers. In *Civil Forfeiture: Tracing the Proceeds of Narcotics Trafficking*, he provides an overview of the legal principles that have to be considered in achieving successful asset forfeiture.

Tracing an asset to narcotics trafficking is not an insurmountable task.

"Tracing an asset to narcotics trafficking is not an insurmountable task," Goldsmith writes. "Federal courts have identified a number of factors that may be sufficient to achieve the required linkage.... The factors themselves transcend federal grounds. They are equally applicable to state litigation. Moreover, relying upon analyses comparable to 'net worth' proof used in tax litigation, imaginative investigators may

(cont'd on p. 4)

low the Money (cont'd from p. 3)

be able to develop new avenues for attacking this problem."

Goldsmith stresses that the procedural benefits of civil process enhance the prospects for successful forfeiture. "The most obvious feature is the lower burden of proof confronting enforcement officials: proof by preponderance of the evidence rather than beyond a reasonable doubt. Furthermore, under federal law and some state legislation, the burden of proof is placed on the claimant rather than the government." So officials do not have to achieve certainty in their tracing efforts.

Flourishing Federally

Federal standards and procedures facilitate the civil forfeiture of proceeds and "civil forfeitures have flourished federally," according to Goldsmith who cites these recent cases to make his point:

"In *United States v. 33,000 United States Currency*, probable cause for forfeiture was satisfied by the following evidence: (1) claimant's guilty plea to conspiracy to distribute marijuana and evade taxes; (2) the seizure of $33,000 located in a brown paper bag in claimant's home; (3) the presence of drugs on the premises; and (4) claimant's lack of legitimate employment. Although claimant presented evidence that he had received $21,915 from the recent sale of a horse, the court found that his burden of proof had not been met because of his failure to explain his cash transactions at a time when he had no apparent source of income."

"In *United States v. Brock*, the government sought forfeiture of jewelry, valued at $120,000, which was found in a bag in claimant's attic. Despite the absence of any direct evidence connecting the jewelry with claimant's narcotics activity, the Court of Appeals concluded probable cause was present: 'The circumstances were sufficient to warrant a conclusion that there was no other way Brock could have acquired the jewelry than ... by proceeds of the alleged narcotics violation.'"

Survey of States

In preparing his report, Goldsmith surveyed cases and statues in Arizona, Colorado, Florida, Georgia, Illinois, Michigan, New Jersey, New Mexico, and Pennsylvania and drew three generalizations.

1. "Some states have adopted the federal approach to civil forfeiture."

2. "Fortunately, state courts have not raised the civil forfeiture standard to proof beyond a reasonable doubt.... (and) most state laws place the burden of proof on the claimant to establish any available statutory exemptions."

3. "Many state statutes establish presumptions providing that money or negotiable instruments found in 'close proximity' to controlled substances are presumed to be forfeitable."

Goldsmith also examines common evidentiary factors and net worth analysis involved in civil forfeiture. He concludes:

"Asset forfeiture continues to hold great potential for attacking large scale narcotics trafficking. Using the benefits of civil discovery and a lower burden of proof, law enforcement has an important opportunity to strike at the profits generated by such criminality. Thus far, most civil forfeitures have been accomplished by federal authorities. Although federal law is admittedly preferable to most state statutes, the states do have adequate legal tools to achieve comparable success...."

To Obtain Reports

Public Record and Other Sources of Information on Hidden Assets and *Civil Forfeiture: Tracking the Proceeds of Narcotics Trafficking* may be obtained by sending your request and a check for $5 for postage and handling to the

BJA Asset Forfeiture ProjectRPolice
Executive Research Forum
2300 M St., N. W.
Suite 910
Washington, DC 20037.

Tracing Money Flows Through Financial Institutions is scheduled to be available soon from the Forum..

FEDS CAN SEIZE $20 MILLION IN ASSETS OF HEROIN RING

In what is said to be one of the largest-ever asset forfeitures, the federal government has obtained a verdict allowing it to seize more than $20 million in property from two brothers convicted of being kingpins of a major heroin operation in the New York City borough of the Bronx.

The assets include $900,000 in cash, $120,000 in jewelry, and a $160,000 Lamborghini sports car among several luxury automobiles plus these properties in Puerto Rico: a shopping center and bowling alley complex, three gasoline stations, and seven homes.

Rudolph W. Giuliani, the U. S. attorney in Manhattan, said the jury verdict involves one of the largest forfeitures ever obtained under federal narcotics law and estimated the value of the property at between $20 million and $30 million. The government will sell the seized property and give some of the proceeds to New York law enforcement agencies that took part in the investigation, Giuliani said.

> ...selling heroin at a rate of $40,000 a day...

Victor and Jorge Torres, the two brothers, and Nelson Flores, their top aide, face mandatory sentences of life in prison with no parole because of their conviction as leaders of the heroin operation, according to *The New York Times*. A prosecutor in the case said documents obtained in the investigation indicated the Torres organization had been selling heroin at a rate of $40,000 a day on South Bronx streets, *The Times* said. The prosecutor was quoted as saying that Victor Torres, 26, and Jorge Torres, 26, invested their profits in Puerto Rican businesses.

The brothers and eight other convicted defendants in the case are scheduled for sentencing in September.

FIN CEN:

FINANCIAL CRIMES ENFORCEMENT NETWORK

NCIAL CRIMES
RCEMENT NETWORK

fact sheet

U.S. DEPARTMENT OF
THE TREASURY

Financial Crimes Enforcement Network

* The financial Crimes Enforcement Network (FinCEN) is a multi-source financial intelligence, analysis and targeting network.

* Using advanced technology and analytical processes FinCEN will generate new leads relative to the financial aspects of criminal activity. FinCEN will also support on-going criminal investigations, prosecutions and forfeiture actions conducted by law enforcement officers in the field on all crimes including money laundering.

* FinCEN will integrate data from Federal and State law enforcement and regulatory agencies, State, and local governments, cooperating foreign governments, and the private sector.

* FinCEN will use artificial intelligence and other analysis methods to identify and report on potential targets as well as existing and emerging methods, patterns, and trends.

* FinCEN will incorporate, review and analyze affidavits, reports of investigations and other information related to the financial aspects of all criminal activity.

* FinCEN will conduct studies using financial data to help law enforcement and regulatory agencies work together more efficiently.

* FinCEN will be available to advise Federal, State, regional, and local law enforcement agencies on financial intelligence management and dissemination as well as investigative techniques and procedures.

* FinCEN will conduct research and develop efforts in technological, economic and other areas associated with the financial aspects of criminal investigations.

* FinCEN will conduct issue-specific seminars related to money laundering. The seminars will identify and assess the impact of these issues and provide recommended actions to law enforcement and regulatory agencies.

* FinCEN will develop and coordinate effective liaison relationships with participating Federal, State and local governments, cooperating foreign governments and the private sector.

1-800-SOS-BUCK

[redacted]er 1990

Funded by
Bureau of Justice Assistance

FROM:
Police Executive Research Forum, Asset Foreiture Bulletin.

FinCEN's Director: Definite State-Local Role

Interview with Brian Bruh

Editor's Note: In April of this year, Secretary of the Treasury Nicholas Brady created the Financial Crimes Enforcement Network (FinCEN) to attack the economic roots of drug trafficking [redacted]ther profit-motivated crimes. To [redacted] this ambitious program, Secretary Brady chose Brian Bruh, a former Deputy Assistant Commissioner of IRS for Investigation and a career financial investigator. PERF contacted Bruh to arrange this interview, hoping to clarify the relationship of FinCEN to the state and local law enforcement community. Among other promising benefits, FinCEN's concentration on money laundering could result in greater forfeiture activity throughout all levels of government. An edited version of our questions and Brian Bruh's answers follows.

Question: FinCEN appears to be designed to bring together *Federal* investigative resources on money laundering and other financial crimes. In general, does FinCEN have a role in assisting *state* and *local* law enforcement?

Response: FinCEN's mission includes providing support to Federal, state, and local law enforcement in the war on drugs. The FinCEN network currently is [redacted]orting two major multi-agency task [redacted]s that include state and local police agencies. As our services expand, assistance to state and local agencies will increase. Some of this assistance will be provided via existing systems, including the High Intensity Drug Trafficking Area (HIDTA) task forces, the Organized Crime Drug Enforcement Task Forces (OCDETF), financial task forces, and other Federal grand jury investigative processes that may involve state and local agencies. For high-profile investigations in which state and local agencies are not party to a Federal grand jury, FinCEN most likely will provide support through procedures similar to those being used to obtain information from Interpol and EPIC. We understand that most, if not all, states have at least a designated official through whom inquiries are directed to EPIC and Interpol. In addition, FinCEN may use the Regional Information Sharing Systems (RISS) program of the Department of Justice as a vehicle to assist state and local agencies.

[redacted]

FinCEN
continued from page 1

> **"We do not forsee FinCEN as a substitute for . . . existing investigative relationships."**

FinCEN encourages state and local agencies to continue their liaison and working relationships with the various Federal agencies in their geographic area. *We do not foresee FinCEN as a substitute for, but a complement to, existing investigative relationships.* A primary goal of FinCEN is to provide quality service to all agencies, state and local as well as Federal, as resources permit. The methods for achieving this goal will evolve as FinCEN becomes fully staffed and operational. We expect to phase in direct support to law enforcement agencies, starting with the Federal sector.

We solicit your suggestions as to the best means of serving your operational needs. One idea we are considering is for FinCEN to hold a conference during fiscal year 1991—after we have gained more experience in dealing with all FinCEN customers. The conference would feature a blue ribbon panel, including representatives from state and local agencies. Relationships with all participating agencies would be reviewed, and revisions of our procedures would be welcomed.

Question: Can FinCEN provide operational assistance to state and local law enforcement agencies? If so, what types of assistance can it provide, and how should state/local agencies begin the process for obtaining that assistance?

Response: FinCEN plans to provide an array of assistance, both tactical and strategic. We are in the process of reaching agreements with numerous Federal law enforcement and regulatory agencies to obtain access to their investigative files. In addition, FinCEN will have access to Bank Secrecy Act information, other Federal financial data bases, and information from private and public sources. We encourage state and local agencies to consult initially with appropriate Federal authorities for access to their respective data bases. Assistance from FinCEN should be sought in urgent situations, and also when inquiries to local Federal agencies may not provide the desired information.

> **FinCEN plans to provide an array of assistance, both tactical and strategic."**

We will be devising a system to provide direct access to FinCEN information. As noted earlier, we are considering adoption of procedures similar to those used to access information from EPIC and Interpol. FinCEN has an Operations Center, similar to the EPIC Watch, to provide immediate support to field activities. Currently, the Center is open to the two multi-agency task forces mentioned earlier, and to a U.S. Postal Inspection Service operation. The hours of operation are now 7 a.m. to midnight. *By October 1990 we will be operating 24 hours a day, seven days a week.* FinCEN can also provide strategic

lysis of emerging trends and patterns as they relate to enforcement. Further, FinCEN will be conducting seminars on specific enforcement problems. FinCEN recently held its first such seminar—on the issue of unregulated money exchange houses (*casa de cambios*) on the Southwest border. Many participants in the conference were state and local enforcement and regulatory personnel.

Question: Does FinCEN want input from state/local agencies on the financial aspects of their drug investigations? For example, do you want agencies to provide you with documentary leads and evidence, or should the agencies continue to go to the individual enforcement agency (e.g., the local IRS field office)?

Response: Certainly, we value the input of state and local enforcement agencies. Our main goal is to create a data base containing financial information not available elsewhere. Examples of the types of Federal, state, and local information to be included in the FinCEN data base are affidavits for search, seize, and arrest warrants; financial documents seized during execution of warrants; analytical information provided by FinCEN to agencies; and other financial information not currently captured and indexed by enforcement agencies. FinCEN will be developing procedures and criteria for submission of information to the data base.

Question: We understand that FinCEN now has authority to service state and local agency requests for Bank Secrecy Act (BSA) information, such as CTR and CMIR reports. If that is so, under what conditions should an agency request the BSA information directly from FinCEN rather than through IRS, Customs, or the Treasury Department?

Response: FinCEN is authorized to disseminate BSA information to state and local law enforcement agencies. Nevertheless, we prefer that routine requests for BSA information be made to local IRS or Customs offices. We see our role as one of fulfilling *unique* requests, for example, using our artificial intelligence capability to identify targets or to analyze links among criminals and their organizations.

Question: Please give an example or two of assistance FinCEN has given to state or local investigations that has made a difference in the outcomes of those cases. Are they typical examples, and can readers of the Bulletin who have ideas for enhancing their investigations expect the same type of assistance—and outcome?

Response: FinCEN has been in operation for only four months. We have provided limited assistance directly to state and local agencies. Regarding the two multi-agency task forces being supported by our Operations Center and other multi-agency investigations being supported by the Tactical Division, we have received little feedback. Feedback relative to direct requests has been good. For example, a target for whom a bench warrant had been issued was located immediately, and fugitives were located for the Bureau of Alcohol, Tobacco and Firearms. In another instance, a money laundering investigation was initiated on the basis of our analysis of financial data base information.

FinCEN is authorized to disseminate Bank Secrecy Act information to state and local agencies.

Question: Suppose an agency wants help setting up a computer program or adapting software to manage and analyze financial transactions. Can FinCEN provide any specific assistance to the agency, and, if so, what type of assistance?

Response: We will have standard computer software available for analyzing such information and evidence as seized records and telephone calls. When unique needs arise, FinCEN will have the expertise to develop the needed computer software or to assist local Federal agencies in their efforts.

Question: What kinds of information is FinCEN developing to help state and local agencies understand money laundering and related problems?

Response: FinCEN routinely studies patterns and trends in currency flow between the Federal Reserve and its member institutions. FinCEN also analyzes, and has reports on, Bank Secrecy Act data. This information is available to state and local agencies on written request. We also have a pamphlet and other resource material on money laundering methods and possible investigative remedies. As mentioned, FinCEN recently held a seminar on *casa de cambios*. We will be preparing a white paper setting forth the scope of that problem and suggested solutions. The paper likely will include recommendations for state and local legislative and regulatory initiatives, as well as heightened enforcement efforts.

Question: How should agencies contact FinCEN for assistance?

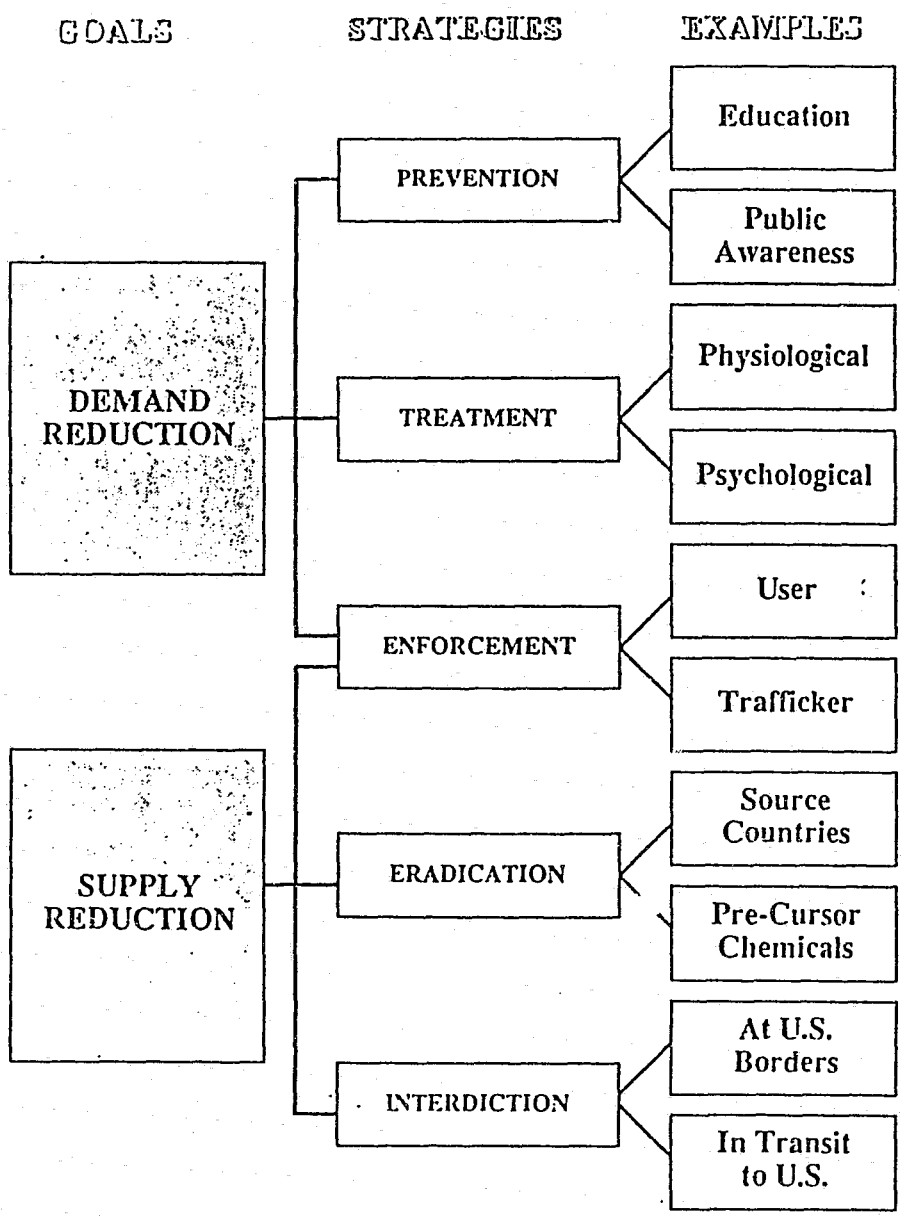
Response: As mentioned earlier, FinCEN expects to provide assistance to state and local enforcement agencies primarily through existing Federal task force efforts and other established lines of communication. Direct requests should be made in writing, either by letter or by FAX. Our mailing address is *FinCEN, 3833 N. Fairfax Drive, Arlington, VA 22203*. Our FAX number is (703) 235-0526.

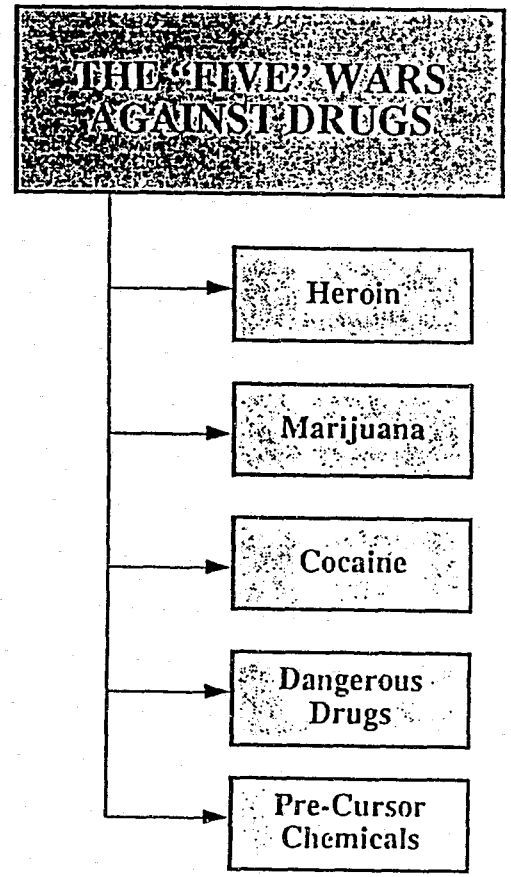
Question: Is there anything else about FinCEN, its mission, plans, or other matters, that you would like to share with Bulletin readers?

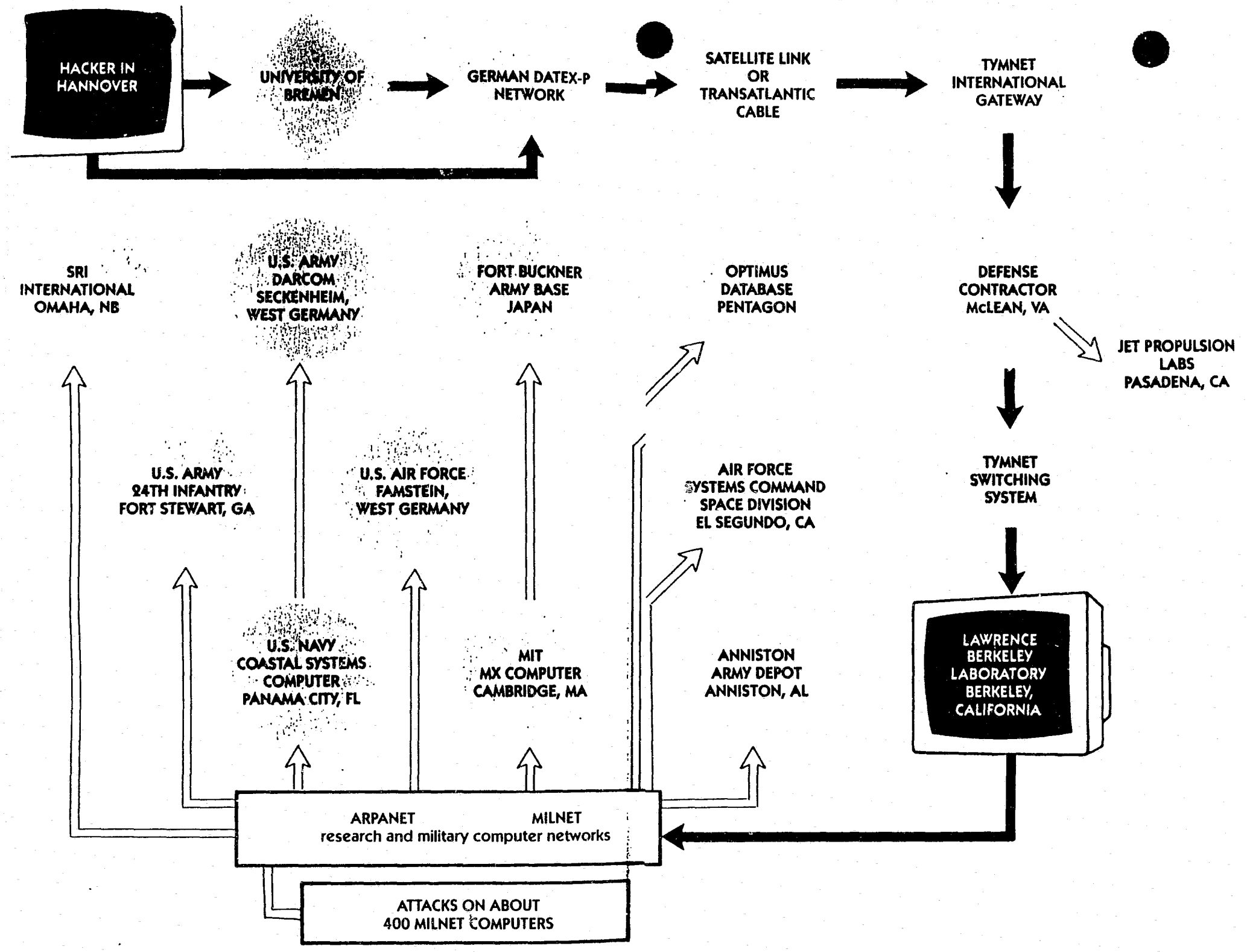
Response: FinCEN's mission is to obtain access to and/or collect all available and relevant financial information. FinCEN will analyze, target, and disseminate this information in support of law enforcement efforts directed toward money laundering and other financial crimes. FinCEN accepts this challenge and commits itself to providing high-quality services to all customers. FinCEN's goal is to help Federal, state, and local law enforcement disrupt and dismantle money laundering and drug trafficking organizations. I encourage feedback on ways FinCEN can assist state and local agencies. I appreciate this opportunity to inform your readers of our mission and goals, and I eagerly await your suggestions.

MISCELLANEOUS:

- ✔DRUG STRATEGY CHART
- ✔COMPUTER CRIME NETWORK
- ✔TERRORISM DEFINITIONS
- ✔TERRORIST ORGANIZATIONS


GOALS
STRATEGIES
EXAMPLES
DEMAND REDUCTION
SUPPLY REDUCTION
PREVENTION
TREATMENT
ENFORCEMENT
ERADICATION
INTERDICTION
Education
Public Awareness
Physiological
Psychological
User
Trafficker
Source Countries
Pre-Cursor Chemicals
At U.S. Borders
In Transit to U.S.


"THE "FIVE" WARS AGAINST DRUGS
Heroin
Marijuana
Cocaine
Dangerous Drugs
Pre-Cursor Chemicals


HACKER IN HANNOVER
UNIVERSITY OF BREMEN
GERMAN DATEX-P NETWORK
SATELLITE LINK OR TRANSATLANTIC CABLE
TYMNET INTERNATIONAL GATEWAY
SRI INTERNATIONAL OMAHA, NB
U.S. ARMY DARCOM SECKENHEIM, WEST GERMANY
FORT BUCKNER ARMY BASE JAPAN
OPTIMUS DATABASE PENTAGON
DEFENSE CONTRACTOR McLEAN, VA
JET PROPULSION LABS PASADENA, CA
U.S. ARMY 24TH INFANTRY FORT STEWART, GA
U.S. AIR FORCE FAMSTEIN, WEST GERMANY
AIR FORCE SYSTEMS COMMAND SPACE DIVISION EL SEGUNDO, CA
TYMNET SWITCHING SYSTEM
U.S. NAVY COASTAL SYSTEMS COMPUTER PANAMA CITY, FL
MIT MX COMPUTER CAMBRIDGE, MA
ANNISTON ARMY DEPOT ANNISTON, AL
LAWRENCE BERKELEY LABORATORY BERKELEY, CALIFORNIA
ARPANET
MILNET
research and military computer networks
ATTACKS ON ABOUT 400 MILNET COMPUTERS

BASIC DEFINITIONS OF TERRORISM

CJ-402

The politically, socially, and/or religiously motivated criminal intimidation of the innocent.

FBI

The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

CIA

Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine state agents, usually intended to influence and audience.

Risks International

The threatened or actual use of force and violence to attain a political goal through fear, coercion and intimidation.

INTERNATIONAL TERRORISM

Terrorism involving citizens or territory of more than one country. (CIA)

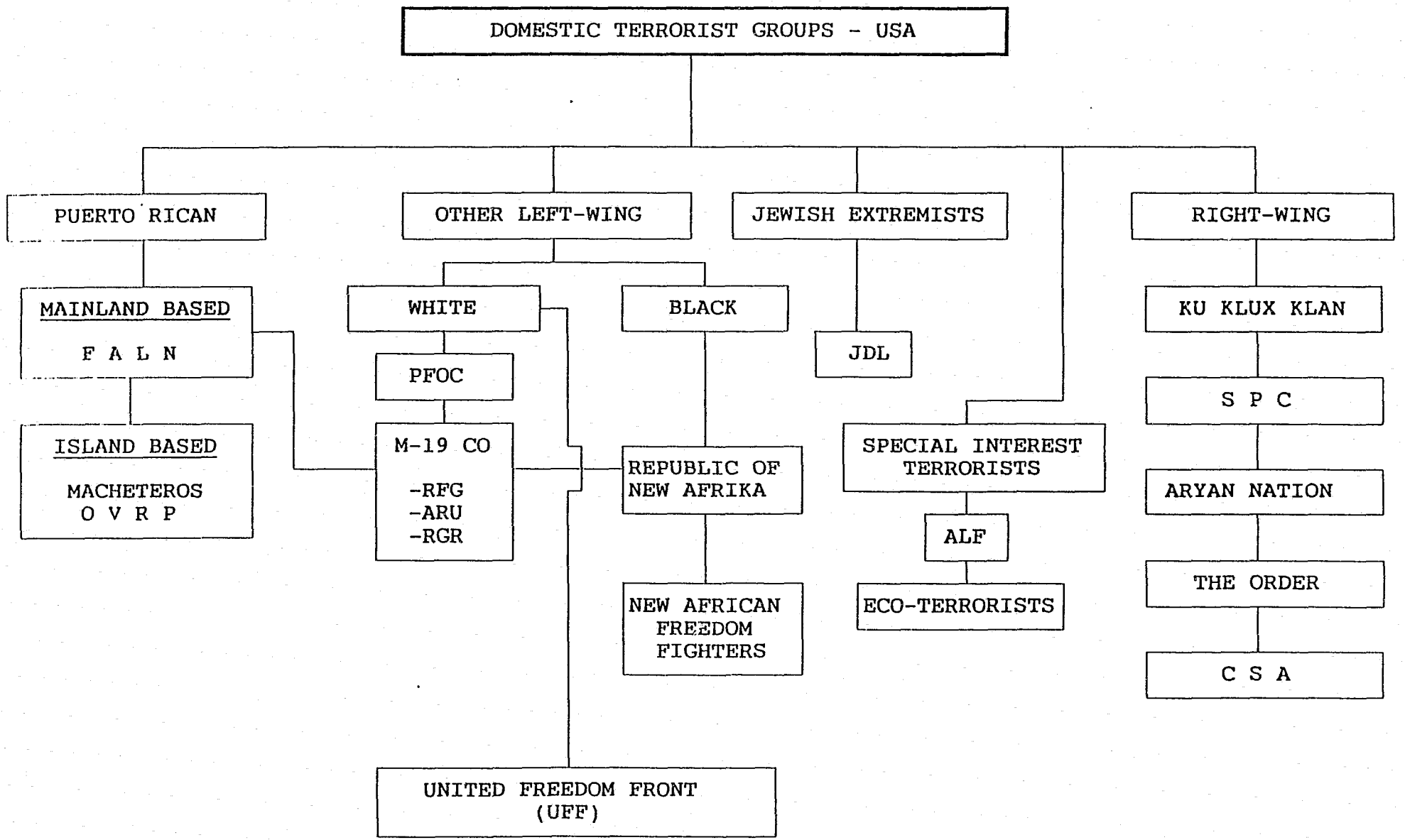
TRANSNATIONAL TERRORISM

Terrorism carried out by non state actors, operating across national borders whether or not they enjoy some degree of support from sympathetic states.

STATE SPONSORED TERRORISM

The deliberate and unlawful use of force or violence by a sovereign state or its surrogates against a non combatant population in furtherance of political objectives.

CLASSROOM USE ONLY



STELLA™

COMPUTER SIMULATION PROGRAM

COMPUTER SIMULATION AS A MEANS OF FORECASTING

PREPARED BY:

DAVID L. CARTER, PH.D.
BEHAVIORAL SCIENCE UNIT, FBI ACADEMY
SCHOOL OF CRIMINAL JUSTICE, MICHIGAN STATE UNIVERSITY

The use of models and simulations are means to look to the future to anticipate problems, issues, or events and anticipate policy alternatives. Typically this has been a complex and expensive process.

Recent technological advancements have led to the practical application of computer programs which can simulate social systems and associated social patterns or trends. STELLA™ is one such program that couples a systems approach with computer modeling to forecast qualitative and quantitative dynamics. The systems approach has long been recognized as having great potential for prediction (Knight, Curtis & Fogel, 1970).

A primary function of simulation research is to forecast the behavior of dynamic social systems. Simulation is "a way of tracing out the dynamic behavior that's implied by the particular arrangement of assumptions (and associated numerical values) that you've mapped out" (Richmond, Vescuso & Peterson, 1987, p. 2). By employing this technology, researchers and police personnel can now "handle complex non—linear relationships, and...model the system realistically" (Levine & Perkins, in press, p. 20). Furthermore, by employing this technology, parameters can be easily manipulated to check for the possible implications of various law enforcement policies. According to Levine and Fitzgerald (in press),

> ...this process involves first a descriptive and then a normative emphasis. In the descriptive phase, feedback mechanisms and the flow of information through the system are identified and mapped to build a model that simulates the behavior of the current problem. In the normative phase, the model is used as a tool for predicting, at least qualitatively, the impacts of proposed solutions and policies (p. 21).

The illustrations in this handout represent a project on which the author is currently working. The intent of the project is to forecast violence in the United States based on a series of social, economic, and political variables.

The first step in building the model is identifying the critical variables. This is done both intuitively and logically. One should then attempt to document the validity of the variables through a review of research or logical argument. While this is not an absolute necessity for the model to work, per se, it gives greater meaning to the logic of the process.

Both quantitative and qualitative variables can be used in the model. Quantitative variables rely on time series data which can be entered into the model. Qualitative variables can rely on "dummy" values, estimations, or can be manipulated to reflect different states of nature.

Since STELLA™ is based on systems theory, a basic systems model must first be developed. Essentially, one must explore the relationships of the critical variables as they are hypothesized to interact. Figure ! illustrates the basic systems loop structure hypothesized for the study of violence trends. This is used as the blueprint to develop the actual STELLA™ systems model, which is illustrated in Figure 3. (Figure 2 illustrates the legend of symbols used in the STELLA™ systems structure.)

Following the foundation established in the loop structure the researcher builds on the model adding critical variables as deemed necessary. Figure 3 shows the STELLA™ model program for the violence research. As can be seen, the basic loop structure is intact, but has been expanded with data and variables.

As variables and their relationships are created in STELLA™, the software creates an algebraic formula. The researcher simply needs to input data or give values to these algebraic components.

To enhance reliability, once the model is developed, the researcher attempts to place the model in a state of "equilibrium" Figure 4 gives two illustrations where variables are compared and placed in a state of equilibrium after year 1991. Basically, the state of equilibrium represents a mean linear interactive projection of each variable. Variables can then be modified, quantitatively or qualitatively, for projections to the time desired. Conversely, any combination of the models can be explored to determine their interactive effects.

Conclusions are drawn based on multiple exploration of the variable interactions as based on the system's projections. While certainly not foolproof, the system provides a foundation for making projections.

Any model is only as good as its structure and the information entered into it. The term **isomorphism** refers to the degree a model reflects reality. Thus, as isomorphism increases, so does the representation of reality. STELLA™ reflects this phenomenon. As the quality of the data, complexity of the model, and validity of the logic increases, so does the reliability of its projections.

REFERENCES CITED

Knight, D. E., Curtis, H. W. & Fogel, L. J. (1971). Cybernetics, simulation and conflict resolution. New York, NY: Spartan.

Richmond, B., Vescuso, P., & Peterson, S. (1987). An academic users guide to STELLA™. Lyme, NH: High Performance Systems.

Levine, R. J. & Perkins, D. V. (in press). Analyses of dynamic psychological systems. New York: Plenum Press.

Figure 1. Loop Structure

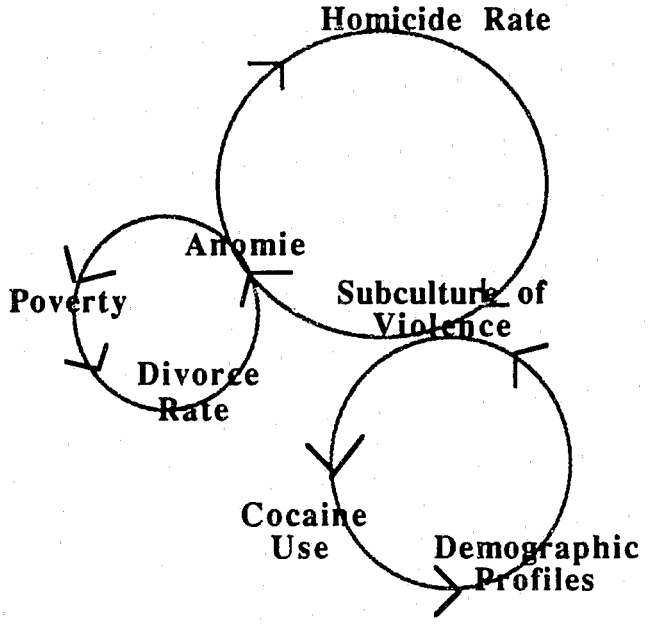


Figure 2. Icon Legend for STELLA™ Model

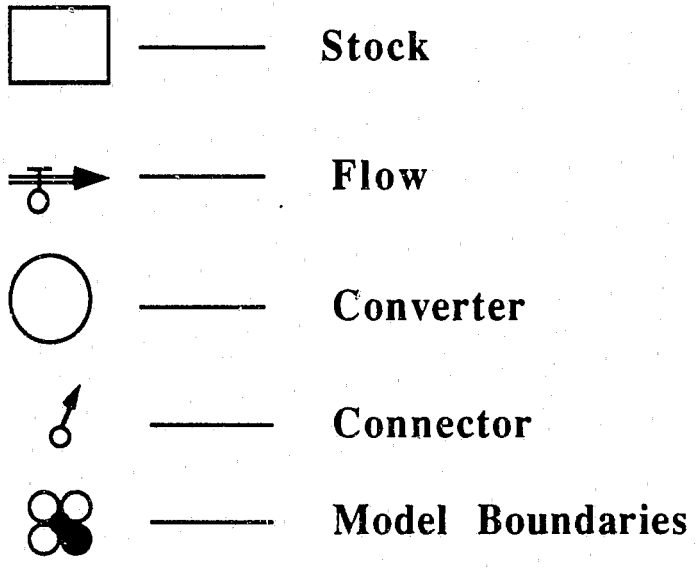


Figure 3. Flow Diagram

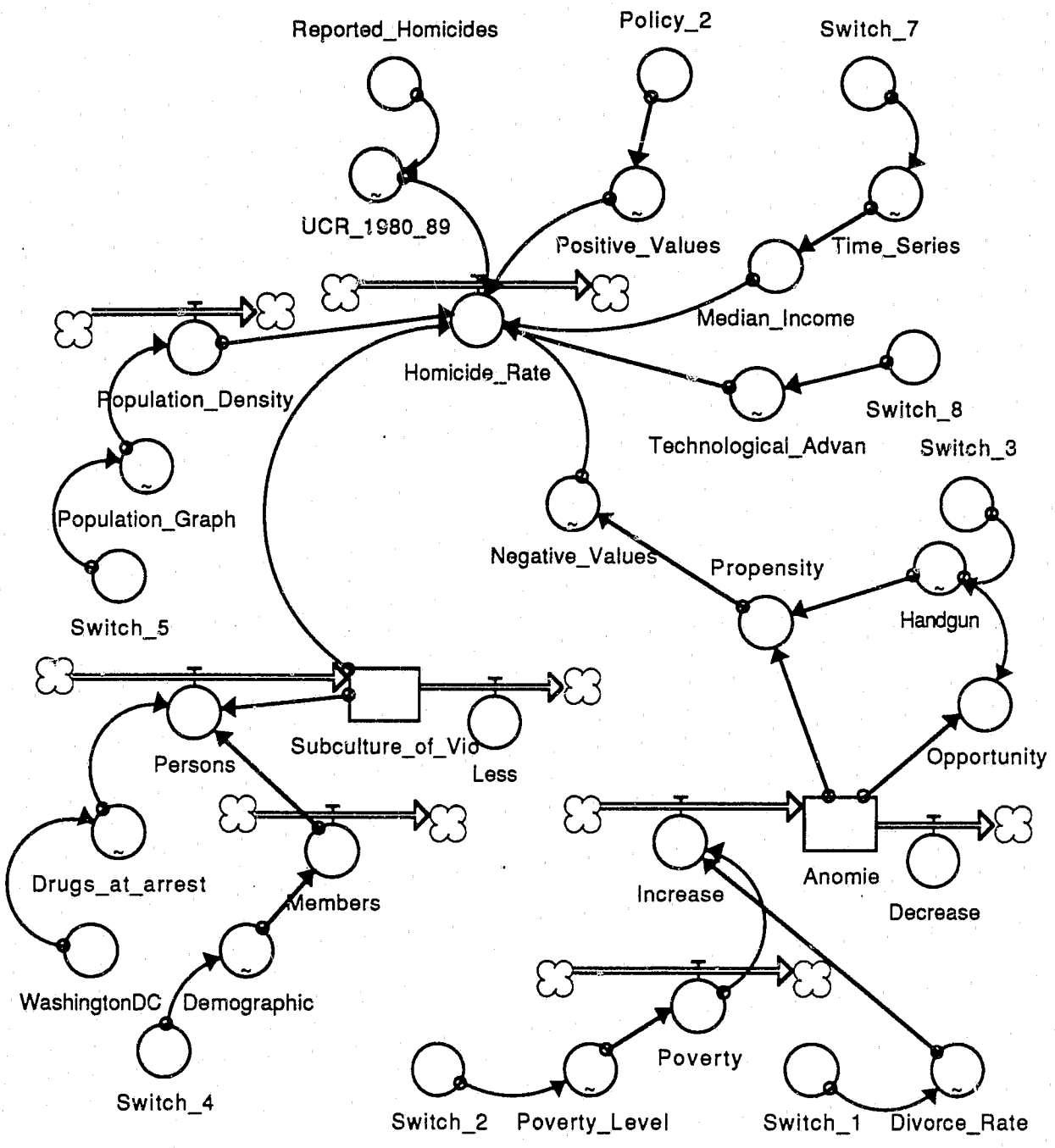


Figure 4. Equilibrium Represented in the Model