AD-A225 486

Identifying Insurgent Infrastructure

A Monograph
by

Major James A. Horris

Special Forces

MENS EST CLAVIS VICTORIAE

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

First Term AY 89/90

90-11/6

05 0

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	Approved for public release; distribution is unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION U.S. Army Command and General Staff College	6b. OFFICE SYMBOL (If applicable) ATZL-SWV	7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS (City, State, and ZIP Code) ATTN: ATZL-SWV Fort Leavenworth, KS 66027-6900	7b. ADDRESS (City, State, and ZIP Code)

8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS			
	PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)

Identifying Insurgent Infrastructure (U)

12. PERSONAL AUTHOR(S)
Major James A. Horris

13a. TYPE OF REPORT Monograph	13b. TIME COVERED FROM 7-89 TO 1-90	14. DATE OF REPORT (Year, Month, Day) 900107	15. PAGE COUNT 49

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Insurgency, Infrastructure, Counterinsurgency, Intelligence operations, Link Analysis, Pattern Analysis, Police intelligence operations. (U)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This monograph examines the nature of insurgent infrastructure and methods of identifying it. It uses a communist mass-based insurgency as a context. The research hypothesis is that current doctrine and service school curricula do not adequately meet the educational needs of analysts or advisors prior to commitment in operational areas today.

The study examines insurgent infrastructure at the local level, and establishes its primacy in the conduct of an insurgency. It describes the use of generic insurgency models, then operational area models in educating personnel prior to deployment. Using the intelligence cycle as a framework, it expands on intelligence doctrine for identifying insurgent cells. It incorporates police intelligence techniques and discusses the operation and administration of an intelligence analysis center. The monograph closes with considerations for targeting and neutralizing infrastructure members.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code)	22c. OFFICE SYMBOL

19. (continued)
The study concludes that intelligence operations in counterinsurgency deserves
its own field manual; that the Military Intelligence School and the Special
Warfare Center should include infrastructure in their curricula which incorporates
police techniques and concepts; and lastly, that the theory of (host nation)
joint fusion and analysis centers similar to those of the Phoenix program should
be part of U.S. counterinsurgency doctrine.

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major James A. Horris

Title of Monograph: Identifying Insurgent Infrastructure

Approved by:

_____   Monograph Director
Lieutenant Colonel Gerald R. Thiessen, MS

_____   Director, School of
Colonel William H. Janes, MA, MMAS   Advanced Military
                                          Studies

_____   Director, Graduate
Philip J. Brookes, Ph.D.   Degree Program

Accepted this ___26th___ day of ___March___ 1990

ABSTRACT

IDENTIFYING INSURGENT INFRASTRUCTURE   by Major   James a.
Horris, USA, 49 pages.

This monograph examines   the   nature   of   insurgent
infrastructure and methods of identifying it.   It uses a
Communist mass-base insurgency as   a context. The research
hypothesis is that current doctrine and service school
curricula do not adequately   meet the educational needs of
analysts or advisors prior to commitment in operational
areas today.

The study defines and examines insurgent infrastructure at
the local level, and establishes its primacy in the conduct
of an insurgency.   It   describes the use of generic
insurgency models, then operational area models in educating
personnel prior to deployment. Using the Intelligence Cycle
as a framework, it expands on intelligence doctrine for
identifying insurgent cells.   It incorporates   police
intelligence techniques and discusses the operation and
administration of an intelligence analysis center.   The
monograph closes with considerations for targeting and
neutralizing infrastructure members.

The study concludes   that intelligence   operations in
counterinsurgency deserves its own field manual; that the
Military Intelligence School and the Special Warfare Center
should include infrastructure identification in their
curricula which incorporates police techniques and concepts;
and lastly, that the theory of [host nation] joint fusion
and analysis centers similar to those of the Phoenix program
should be part of U.S. counterinsurgency doctrine.

iii

TABLE OF CONTENTS

LIST OF FIGURES

SECTION I

INTRODUCTION

The role of insurgent infrastructure is uniquely important in a revolutionary movement. Attacking that infrastructure must therefore be an integral part of any counterinsurgency plan. Unfortunately, the role of infrastructure and the techniques of defeating it are not commonly understood in today's military.

In order to defeat the infrastructure, one must be able to identify it. This is a process of intelligence collection and analysis, facets of which are unique to low-intensity conflict (LIC). The Army currently does not have sufficient doctrine to meet this need. Army field manuals provide some of the necessary information and methods. Generally, however, they fail to sufficiently explain, or completely omit, techniques which are critical to the synthesis of intelligence.

Intelligence analysis in counterinsurgency (COIN) requires a blend of military and police intelligence techniques. The Army's manual for this, FM 34-3 Intelligence Analysis, provides some tools for use in a COIN environment, as well as some insurgent characteristics.

1

However, the manual is less instructive than it is descriptive. Pattern analysis, a primary technique, is only briefly mentioned. Link analysis, a key police method of determining associations, is not defined at all.

Similarly, information storage and retrieval is addressed only in terms of files and overlays. While these are described well, no mention is made of managing information, or how to design an adequate file system. Yet these techniques are readily available from police intelligence units.

Human intelligence (HUMINT) collection, another staple in LIC, is covered in FM 34-60, Counterintelligence, and FM 34-60A (S/NFN), Counterintelligence Operations. Much of the technique and tradecraft discussed in these sources is generic, though with a distinctly NATO flavor. They thus require interpretation to apply to third world insurgencies.

These shortfalls are covered neither by the Military Intelligence School nor by the Special Warfare Center curricula, both of whom have vested interests. Training in these techniques is rare and Army institutional expertise resides mostly in personnel assigned to third-world operational areas. In short, this means that most analysts/advisors were under-prepared when committed unless they had prior, in-country experience in intelligence work.

The purpose of this paper, then, is to define insurgent infrastructure and its role in prosecuting a revolution; to

chart a methodology for identifying that infrastructure; and finally, to present considerations for neutralizing it.

This study expands on the doctrine presented in the above manuals, as well as in FM 34-130 <u>Intelligence Preparation of the Battlefield</u>. It incorporates police intelligence methods and lessons of past wars. These techniques, mostly common sense, are used today by law enforcement agencies as well as by U.S. military personnel in Foreign Internal Defense (FID) programs. A communist, mass-oriented insurgency provides the context for the study.[1]

Background

Infrastructure is an American term coined during the Vietnam War, but never used by the Vietnamese communists.[2] It refers to the individuals and groups which organizationally constitute the "party, civil, and military elements" of the insurgency.[3] (See Figure 1.) Though often used when speaking of political subversion cells, it also includes the local militia and small guerrilla units which respond to those cells. Infrastructure is alternately known as parallel hierarchy,[4] shadow government,[5] and in older references, the underground.[6]

In theory, infrastructure extends from the villages all the way to the national-level Central Committee, and includes the Military High Command as well. Notably,

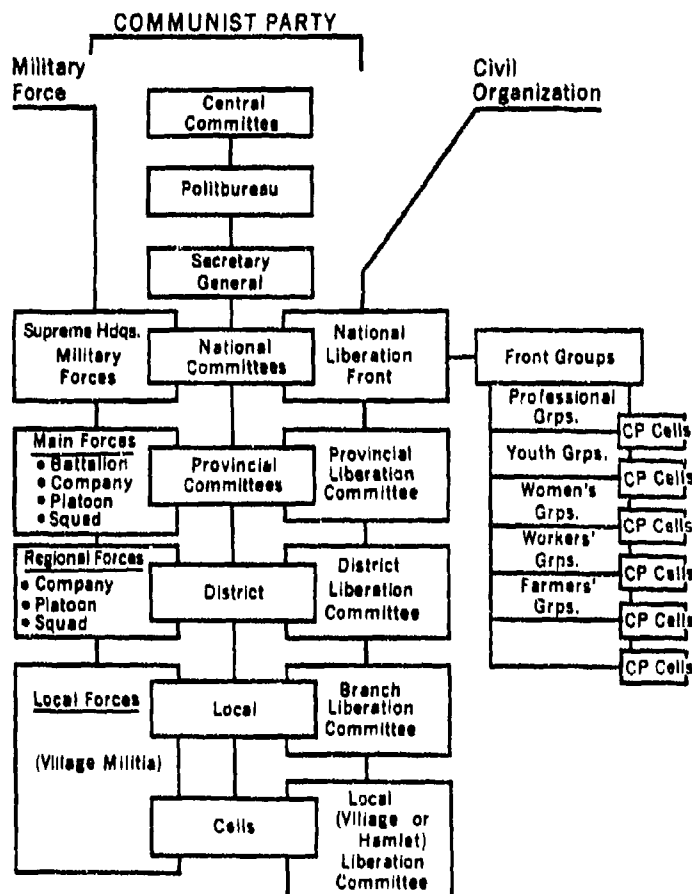however, Main Force guerrilla units are not considered part

Figure 1. [7]

of the insurgent infrastructure. Though highly politicized,

Main Force units are strictly military formations with

combat missions. They do not respond to regional or

district party committees.[8]

This study focuses on infrastructure at the district

level and below. It is these individuals and cells who

4

bring the revolution into the homes of the people, and it is they who subvert the government and coerce popular cooperation. In Vietnam, party and civilian leaders of the infrastructure were called cadres.

In his book Silence Was A Weapon, Stuart Herrington further classifies the party/civil cadres as "legal" and "illegal".[?] A legal cadre is an insurgent who operates covertly as a member of the infrastructure but overtly as a legitimate member of the community. He has been recruited from the community and has an ID card, a family, and a job. An illegal cadre lives in a bunker in the woods by day and operates clandestinely at night, infiltrating and organizing.

Of the various elements of infrastructure, the party and civil cadres are the most dangerous. They are the political subversives who prosecute the insurgency and direct the activities of the local guerrilla units they have recruited. They coordinate the collection of taxes to support these guerrillas as well as Main Force units. In directly attacking the insurgent infrastructure, the established government must give priority to destruction of these cadres over destruction of guerrillas. [10]

In vying for, or coercing, the support of the people, the insurgent takes an indirect approach to displacing the established government. He chooses this path because he does not possess the military power to directly challenge

the established government. He also chooses it because the government has allowed the social, political, and economic conditions to exist which make the people susceptible to his ideology.

In theory, the reverse also is true. That is, if the government worked to eliminate the root causes of the insurgency, it could forego combatting the infrastructure directly.

In practice, this does not work.[11] Most governments conducting counterinsurgency simply do not have the resources and political will to quickly undo the conditions which have fostered the insurgency. Additionally, if not attacked directly, the infrastructure can negate the efforts of the government through terrorism, sabotage, and military action. The government must both attack the infrastructure and work to alleviate the conditions which have allowed the insurgency to develop.[12]

The identification of insurgent infrastructure is actually the threat evaluation/threat integration portion of an intelligence preparation of the battlefield (IPB). FM 34-130, Intelligence Preparation of The Battlefield, provides a format for a low-intensity conflict (LIC) IPB, but mentions only briefly the most important prerequisite for intelligence analysis--a comprehensive knowledge of the insurgent's organization and tactics. Field Manual 34-3, Intelligence Analysis, also addresses this requirement but

6

in only slightly greater detail. To achieve this
comprehensive knowledge, the study of insurgent organization
begins with a generic model and then transitions to an
operational area, or country, model.

Although each insurgency is unique, type-insurgencies
(in this study, Maoist mass-oriented) usually have common
features which allow development of a generic model. (Refer
again to Figure 1. Another version of this model is found
in Appendix D, FM 100-20 Low-Intensity Conflict.[13]) The
broader an analyst/advisor's study of the generic model, the
better his framework for analyzing and assimilating the
theater model.

In order to create the infrastructure shown in the
model, the insurgent operates in units known as cells. The
cell is the basic building block of insurgent
infrastructure. Historically, cells are composed of a
leader and two-seven members.[14] The actual size of the cell
is determined by its mission and the conditions under which
it functions. Security is the principal consideration.
Cells are organized and assigned either by geographic area
or by mission.[15]

In areas where the insurgent is militarily strong and
the government has little popular support, cadres may
operate overtly in a village, or *barangay* (a Philippine term
for village). Some cells may become fairly large.
Conversely, if the government presents an immediate threat

or has the support of the people, greater compartmenting results. Cells are smaller and communications are more formal (written). Under these circumstances, insurgents will use a standard technique of clandestine communications known as a cut-out. A cut-out is a break in the linkage between two persons or cells. It is a security measure taken to prevent disclosure of an association or relationship and may involve the use of an intermediary or mail-drop.

Cell designs vary by mission and usually represent a compromise between the need for organizational efficiency and the need for security.[16] Normally there are three types of generic cells: operational, intelligence and auxiliary.[17]

An operational cell executes one or a variety of missions and members of the cell are usually known to each other. (See Figure 2.) Cell members infiltrate and organize the populace, collect taxes, agitate, propagandize, or
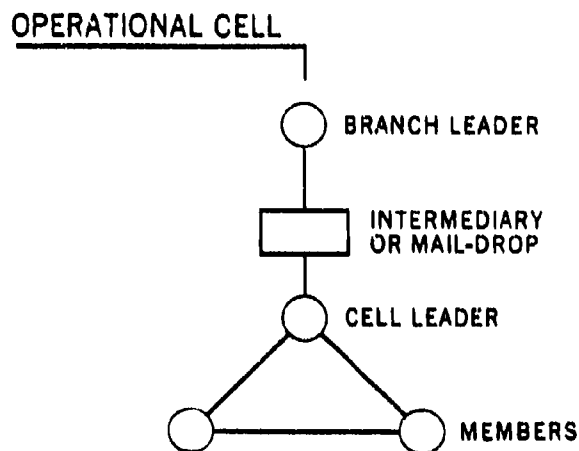
OPERATIONAL CELL

BRANCH LEADER

INTERMEDIARY OR MAIL-DROP

CELL LEADER

MEMBERS

Figure 2.[18]

8

recruit. Some operational cells may specialize in sabotage, terrorism, or traitor elimination, expanding their size as necessary to meet mission requirements.

Intelligence cells are highly compartmented units whose members are not known to the infiltrated agency or community and rarely to each other. (See Figure 3.) This compartmenting preserves the security of the cell if a member is compromised. The use of cut-outs is common here.

INTELLIGENCE CELL

BRANCH LEADER

INTERMEDIARY OR MAIL-DROP

CELL LEADER

INTERMEDIARY OR MAIL-DROP

MEMBERS

Figure 3.[17]

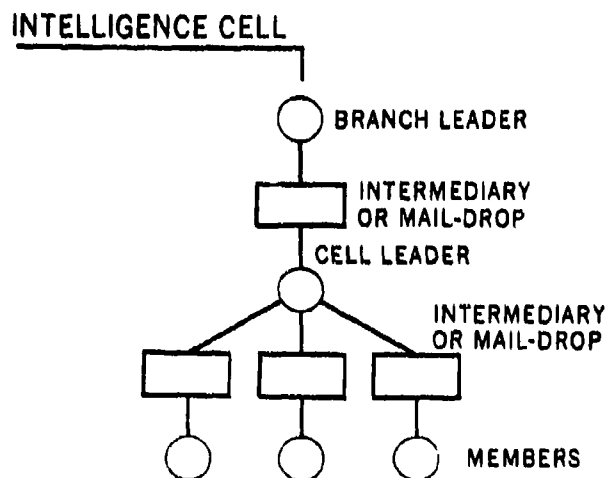Auxiliary cells organize sectoral and functional fronts within a community. (See Figure 4.) Sectoral fronts accomplish social organization such as youth, women's and laborers' groups. Functional fronts (e.g., health, finance, education) accomplish civil administration and logistical support for guerrillas. Operational cells normally recruit auxiliary cell leaders and assistant cell leaders from

within the village, or *barangay*.   Once   indoctrinated and
trained these cell leaders fall into the category of legal
cadre.

AUXILIARY CELL

CELL LEADER

ASSISTANT
CELL LEADERS

MEMBERS
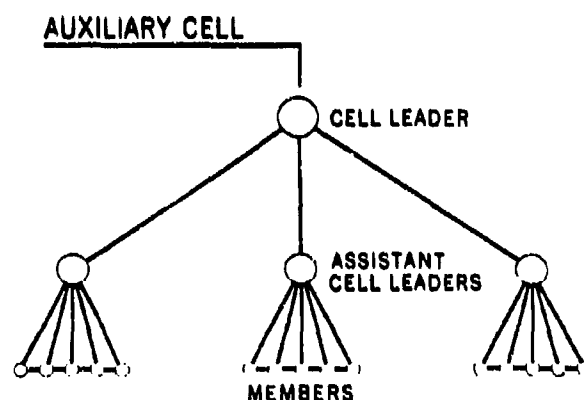
Figure 4.[20]

Although   an intelligence cell may be established
beforehand, an operational cell is normally   the first to
openly contact the local people. An intelligence cell may
remain in place and retain its cover even after arrival of
the operational cell.[21] In this manner it continues to
provide the infrastructure hierarchy with intelligence as
well as progress reports on the operational cell(s).

    Cells may be arranged in parallel, or in series, to
achieve a desired goal or condition. Parallel cells provide
redundancy, a   particularly   important   capability   in
intelligence collection (Fig.5).   The existence of a
parallel cell may be unknown to its counterpart, thereby
preserving capability if one cell is compromised.

10

PARALLEL CELLS

BRANCH LEADER

INTERMEDIARY
OR MAIL-DROP

CELL LEADERS

INTERMEDIARY
OR MAIL-DROP

MEMBERS

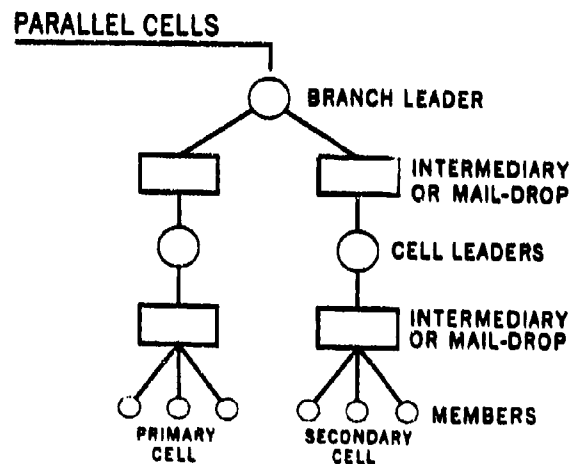PRIMARY
CELL

SECONDARY
CELL

Figure 5.[22]

Insurgents organize cells in series to achieve production
when security for a single centralized operation is
unattainable (Fig.6). Historical examples include small
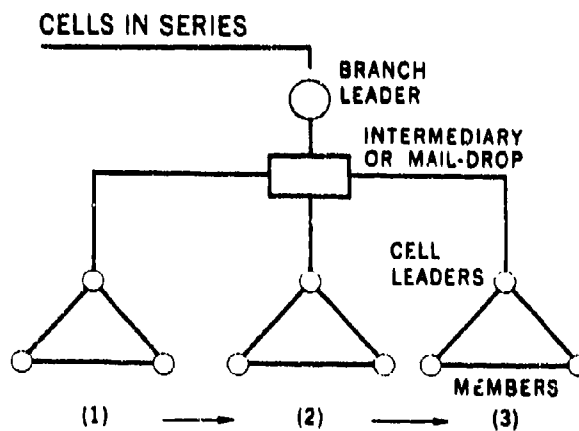arms production as well as newspaper printing and
distribution. [23]

CELLS IN SERIES

BRANCH
LEADER

INTERMEDIARY
OR MAIL-DROP

CELL
LEADERS

MEMBERS

(1) ⟶ (2) ⟶ (3)

Figure 6.[24]

11

The insurgent leadership trains its operational and intelligence cell members well. Cell leaders are ideologues who, in many cases, have attended indoctrination and technical schools, some out-of-country. The production of insurgent cadres who possess an iron resolve is critical to fighting a protracted peoples' war.

When deemed critical, cells include communist party members. The party recruits selectively and membership indicates comprehensive commitment by an individual.[23] Party members in a cell add prestige, reliability and backbone.

To illustrate some of these points, consider the armed propaganda unit (APU), or team. This is an operational cell common to Maoist insurgencies. A Vietnamese invention, APUs have appeared in Thailand, Kampuchea briefly, and in the Philippines. Under its original charter (1944), the APU was to be the element which carried the revolution to the people, infiltrating rural communities and organizing the people. It was to use its weapons only for protection or martial demonstrations. (It would be counterproductive to use the weapons for terror, reasoned Ho Chi Minh.)[24]

This non-violent concept of mobilizing the people changed radically in application, however, and armed terrorism quickly became a standard insurgent tool. By the end of 1963, Viet Cong armed propaganda units had assassinated roughly 13,000 village chiefs, teachers,

12

citizens, and government representatives in South Vietnam.[27]

Generally, insurgent cadres still prefer persuasion to coercion in gaining the support of the people. The initial lack of violence, though, is usually short-lived. The cadres tolerate no opposition and show little compunction for resorting to terror or assassination. In the Philippines, for instance, an APU is employed after a Semi-Legal Team (SLT) has infiltrated a *barangay*. The SLT then calls in an armed propaganda unit to provide "revolutionary justice" and selective coercion.

The insurgent hierarchy geographically divides the country based on its own needs. Boundaries may coincide with those of the government, but generally do not.[28] Boundaries are usually drawn based on the density of infrastructure. If the insurgency is strong in an area, cell density is high and boundaries may be close. Conversely, if the revolution has enjoyed little success cell density will be lower with boundaries farther apart.[29]

A complete study of a generic model would be much longer than my discourse here. However, the value of such a study should be evident. The next step is to correlate the generic model to the country-specific model.

The purpose is to note differences and similarities, while accounting for each function portrayed in the generic model. Appendix A provides an organizational chart of the Communist Party of the Philippines (CPP) for comparison to

Figure 1, the applicable generic model.[30] It contains a description of *modus operandi* as well. Comparative analysis of the two models reveals, for example, that: a Semi-Legal Team functions initially as an intelligence cell; that it becomes an operational cell as it begins organizing the people; and that there is presently no Main Force guerrilla unit which responds to the NPA High Command.

The educational preparation I have described here is essential prior to deployment of the analyst/advisor. Depth of knowledge imparts a broader framework for analysis and a better basis for judgment. Culture and geography are also critically important here. Neither native wit nor conventional background will compensate for a detailed knowledge of the insurgent, his background, or his methods.

SECTION II

IDENTIFICATION

> Gradually the more intelligent officers find
> themselves developing a new set of characteristics
> such as deviousness, patience, and a determination
> to outwit their opponents by all means compatible
> with the achievement of the aim.
> —Frank Kitson[31]

The techniques described here expand on the information in the doctrinal manuals. Since insurgency often resembles organized crime, some police intelligence methods apply.

14

The Intelligence Cycle shown below provides the structure
for a logical presentation of information:[32]

Directing	Recording
Collecting	Evaluating
Processing	Integrating
Disseminating	Interpreting
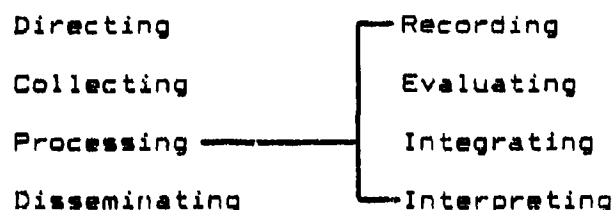
I will discuss Collecting and Processing functions in
detail.

Directing

Simply put, selecting and prioritizing targets is a
"management issue".[33] It requires balancing resources with
the expected utility of the information, the criticality of
the target and the probability of success. The
analyst/advisor must inventory the available collection
assets. Informant operations usually match host-nation
capabilities most closely, though many countries possess a
growing technological capability as well.[34] He should
understand the capabilities of these systems and may request
U.S. asset collection (through U.S. channels) to complement
the host nation's effort.

Collecting

In a counterinsurgency human intelligence (HUMINT) is

15

the key to identifying infrastructure. Signals intelligence
(SIGINT) and imagery intelligence (IMINT) should not be
discounted however. Direction finding, monitoring, and
aerial photo reconnaissance can be significant multipliers
in the intelligence effort.

Collection systems are either covert or overt, the
distinction resting in whether or not the enemy knows he is
being targeted. Most of the SIGINT and IMINT collectors
available to the analyst/advisor will be covert. HUMINT
collectors fall into both categories. In collecting
information, analysts/advisors must adhere to the principle
of systematic targeting. Barring a "big break", this is the
only way to build a threat profile. Military and police
patrols, interrogators, village self-defence groups, and
other official intelligence agencies (military and police)
are overt HUMINT collectors. Some input from other agencies
may come in the form of intelligence but most will be raw
information. The analyst/advisor must impress upon
collectors that every patrol report, every interrogation
report, every captured map, notebook, document, etc. is
important and must be submitted to the analysis center.

Enemy documents have particular importance. Insurgents
keep meticulous records. Highly centralized command and
decentralized execution foster this. Cell or unit rosters,
code names, cache locations, safe deposit box numbers,
infiltration routes, and tax collection tallies are examples

16

of valuable information if submitted in a timely fashion.

The format itself of a captured document may yield
information. By analyzing distribution lists on insurgent
directives the analyst/advisor may be able to infer local
and higher political boundaries as well as committee
hierarchy or chain of command.[35] A clear picture of who-
works-for-whom will be essential later in the neutralization
process.

Population control measures (if any) will provide the
analyst/advisor collection opportunities. Curfews and
identity cards in conjunction with police checkpoints may
reveal patterns of activity indicative of tax/food
collection, messenger traffic, etc. Synchronization of
police and military efforts is a requirement here, as
throughout the counterinsurgency.

Informants are covert collectors. Informant operations
are potentially very lucrative, but require skill on the
parts of all concerned. Recruiting and managing informants
is an art. This is the job of the "case officer".[36]

The analyst/advisor may perform as his own case officer
if he can do so without compromising his informant net.
Ethnic heritage and language skills are common prohibitors.
An indigenous case officer from the host nation military is
a possible solution.

The analyst/advisor must develop his own case officer
selection and training program. The doctrinal reference for

informant operations, development of covers, and clandestine communications is FM 34-60A, Counterintelligence Operations (S/NFN/WNINTEL). The analyst/advisor should look for certain character attributes in addition to trainability. Some skills are instinctive and thus not trainable. The case officer must exhibit reliability and the native wit and interpersonal skills to "make it on the street."

Informants are vulnerable so security is paramount. Covers must be carefully developed and maintained. The case officer must respect this or lose informant confidence.

In recruiting informants, the case officer looks for those with grievances against the insurgents, such as family members of a victim. Other candidates may be relatives of soldiers or government employees. They usually possess a predisposition to work against the insurgency. He also looks to recruit personnel to act as linkage in the informant net. These are people who overlook an activity node such as a market, liquor store or pharmacy. To illustrate: Informants pass spot reports to a local merchant during a weekly visit to the marketplace; the merchant passes the information to the case officer, whose contact with the merchant is situationally plausible; the case officer then relays the information to the analysis center.

Information is perishable. The analyst/advisor should insure he is available to receive the information,

particularly when there is already some inherent delay such as in market visits.

Information often is not free. Paying informants is a problem when corruption is rife, particularly if it must change hands to reach its target. Even with a well established net, however, the real HUMINT payoff historically does not come until an insurgent cadre member rallies to the government.[37] This may occur without notice, or as a result of capture. A sound amnesty program provides the government some leverage here.

The analyst/advisor's main interest in recruiting the insurgent is exploiting his knowledge of the infrastructure. This requires skillful interrogation even if the cadre member is cooperative. He may wish to protect family or himself. In such cases, information from other insurgents can be used to advantage.

When more than one cadre member has been recruited or captured, parallel interrogation can be a significant multiplier.[38] Parallel interrogation involves alternately questioning one insurgent, then the other. Here, information from one insurgent is used to prompt the second. This also provides some depth and allows the interrogator to evaluate the quality of the information.

After analyzing the interrogation results, the analyst/advisor may pursue several options for further exploitation of the captured insurgent. If the insurgent

was a legal cadre, it may be productive to use him in an anti-insurgent propaganda campaign. Alternately, he may be used as the focus of a disinformation program to cause paranoia and de-stabilize the remaining infrastructure. Other options include guiding government forces to caches or base camps, and verifying information gained from subsequent captives. The analyst/advisor must protect his asset, however. Once insurgents realize a former cadre has rallied to the government, they will mark him for elimination.

I have concentrated on HUMINT while discussing Collection because of its primacy in LIC. The potential of technical collection means, however, should not be discounted. As with other elements in the intelligence cycle, the analyst/advisor's imagination and initiative determine the effectiveness of the collection effort.

Recording

A functional information storage and retrieval system is crucial to the intelligence process.[39] Because counterinsurgency is a protracted effort, the analyst/advisor must retain information over a long period of time. The goal then is to establish a system which provides the best balance of accessibility and ease of storage. Chapter Nine of FM 34-3, Intelligence Analysis, describes some types of files required;[40] I will present some techniques for meeting those requirements. Police

intelligence units use the systems described below. They are portrayed as manual systems, but are easily automated.

In technical terms, a storage and retrieval system will always have two components: the index and the file.[41] They are present in manual and automated systems alike, and in both system designs.

The two basic design alternatives are the classification system and the accession system.[42] Both use alphabetical indexes to designate the location of information within the system. The classification system is organized on the concept of classes of information, or data bases. The accession system does not use data bases, but files items serially, or in the order received. The index for the accession system is necessarily more comprehensive than that of the classification system.

Appendix B contains a detailed description of each system and examples. It also includes a design comparison matrix. Some analysts/advisors prefer the classification system because of the data base feature. This is a more intuitive method of storing information and it lends itself well to automation.

The analyst/advisor may create or alter data bases as needed. He should anticipate using the following categories:[43]

Personalities-all names generated by collectors.

Radio Telephone Operators (RTO)

War Names (Nom de Guerre)

Organizations/Guerrilla units (Order of Battle)

Base Camps

Girlfriends/sexual contacts

Propaganda Themes

Cities/Towns

Barangay/Sitio

Data base formats are the preference of the analyst. Suggested formats are at Appendix C. After recording basic information in a given format, the analyst/advisor should record subsequent information chronologically.

In a manual system, each file (each name, camp, RTO, etc.) has its own file folder. An automated system does not require hard copy for each file in a data base (field). Automation, however, does not mitigate the requirement to keep dossiers on all propaganda themes and personalities. (The analyst/advisor should select a cutoff for keeping dossiers; e.g. all cell leaders, all squad leaders and above, all APU members, etc.)

Some analysts consider a chronological master incident file a must. Specific incident files (mines, assassination, etc.) are optional.

In the classification system, retrieving information is faster when a greater number of classes or data bases is used. However as files grow, they require more maintenance. This is a further draft on manpower and another resource

22

consideration for the analyst/advisor.

Overlays provides a second method of storing data. The LIC IPB (FM 34-130, Appendix E) provides a starting point in determining types of overlays needed. These "event template" overlays facilitate analysis but require periodic updating (seasonal drainage changes, new trails, etc.). The intelligence analysis manual (FM 34-3, Chapter 9) also discusses these event overlays and various types of working overlays, as well.

Current field manuals list a number of overlays. Several fall into the event template category.[44]

LOC: Lines of communication. Road, trails, navigable rivers.

Infiltration/Exfiltration Routes: Insurgent avenues of approach/egress.

Cover/Concealment: Should reflect seasonal changes.

Population Status: Reflects tribal, ethnic, religious, and political affiliations. The Philippine government, for example, currently classifies *barangays* as insurgent-controlled, insurgent-influenced, or non-insurgent influenced.

Trap: Likely targets for insurgent sabotage or strike operations. Particularly critical in urban or sub-urban areas where there is a higher density of physical infrastructure (buildings, houses, power stations, radio stations, etc.)

Insurgent Logistics Sustainability: Areas providing food, water and supplies to the guerrillas.

The analyst/advisor can "mix and match" as required to suit his area of operations, the threat, and his staff resources. He should avoid being inundated, however, with unusable

23

information and avoid the pit fall of overlays becoming end in themselves. The section on integration will discuss fuving the information on these overlays to produce Named Areas of Interest (NAI) or target folders.

The incident overlay is the most important one.[45] It provides a visual representation of events in an area over a given period of time. Non-standard symbols should be explained on the overlay. Each incident reflected on the overlay should be accompanied by a date and a reliability/ credibility rating. Lastly, incident overlays should be filed for later use in pattern analysis as a visual record of events.

A variation of the incident overlay is the personalities and contact map.[46] This map (or overlay) is used to track the movements and contacts of individuals, usually in an urban setting. It requires a large scale map as well as a plan of consistent surveillance. It is essentially link analysis on a map. (See Integrating)

Overlays have proven only as useful as the accuracy of the data they reflect. The analyst/advisor should update overlays through aerial/ground reconnaissance and photo imagery.

Another common graphic useful in recording information is the standard line-and-block chart.[47] An example of Viet Cong village infrastructure using the line-and-block method is shown in Figure 7.[48] Line-and-block charts may also be

useful in portraying mature military (guerrilla) units. Each unit block should contain the file location or report serial number which contains the information depicted on the chart.
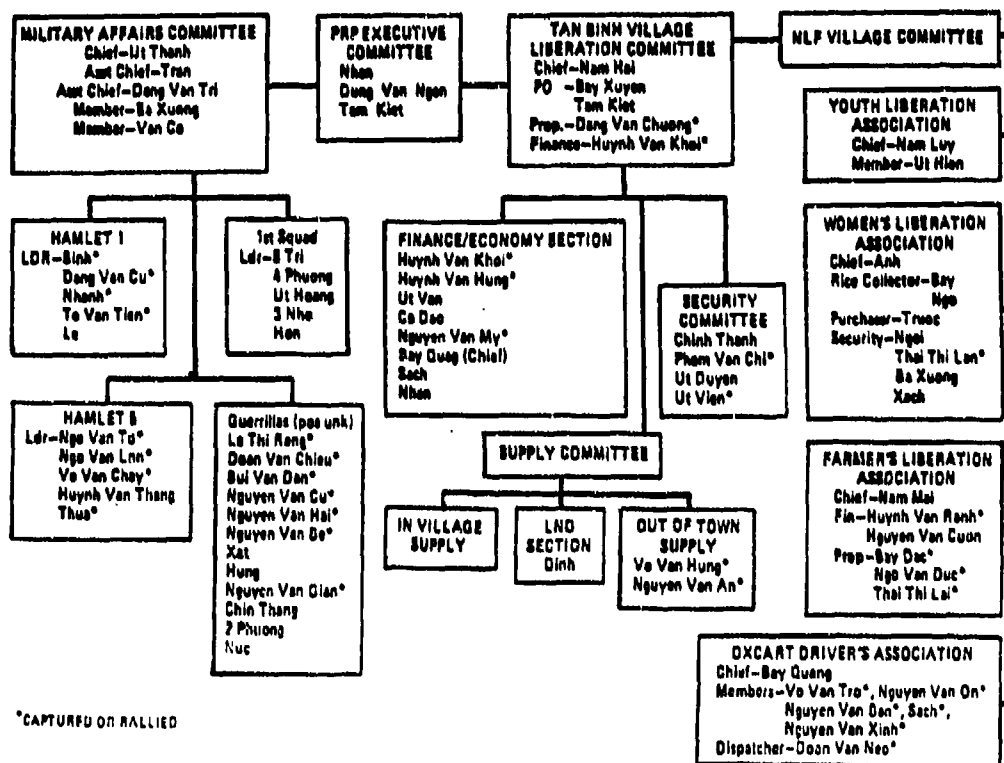
MILITARY AFFAIRS COMMITTEE
Chief—Ut Thanh
Asst Chief—Tran
Asst Chief—Dang Van Tri
Member—Ba Xuang
Member—Van Ce

PRP EXECUTIVE COMMITTEE
Nhan
Dung Van Ngon
Tam Kiet

TAN BINH VILLAGE LIBERATION COMMITTEE
Chief—Nam Hai
PO —Bay Xuyen
Tam Kiet
Prop.—Dang Van Chuong*
Finance—Huynh Van Khoi*

NLF VILLAGE COMMITTEE

YOUTH LIBERATION ASSOCIATION
Chief—Nam Luy
Member—Ut Hien

HAMLET 1
LDR—Binh*
Dang Van Cu*
Nhanh*
To Van Tien*
Le

1st Squad
Ldr—8 Tri
4 Phuong
Ut Hoang
3 Nhe
Hen

FINANCE/ECONOMY SECTION
Huynh Van Khoi*
Huynh Van Hung*
Ut Van
Ca Dao
Nguyen Van My*
Bay Quag (Chiel)
Sach
Nhan

SECURITY COMMITTEE
Chinh Thanh
Pham Van Chi*
Ut Duyen
Ut Vien*

WOMEN'S LIBERATION ASSOCIATION
Chief—Anh
Rice Collector—Bay
Ngo
Purchaser—Truoc
Security—Ngoi
Thai Thi Lan*
Ba Xuang
Xach

HAMLET 8
Ldr—Ngo Van To*
Ngo Van Lnn*
Vo Van Chay*
Huynh Van Thang
Thua*

Guerrillas (pos unk)
Le Thi Reng*
Doan Van Chieu*
Bui Van Dan*
Nguyen Van Cu*
Nguyen Van Hai*
Nguyen Van Be*
Xat
Hung
Nguyen Van Gian*
Chin Thang
2 Phuong
Nuc

SUPPLY COMMITTEE

IN VILLAGE SUPPLY

LNO SECTION
Dinh

OUT OF TOWN SUPPLY
Vo Van Hung*
Nguyen Van An*

FARMER'S LIBERATION ASSOCIATION
Chief—Nam Mai
Fin—Huynh Van Ranh*
Nguyen Van Cuon
Prop—Bay Dac*
Ngo Van Duc*
Thai Thi Lai*

OXCART DRIVER'S ASSOCIATION
Chief—Bay Quang
Members—Vo Van Tro*, Nguyen Van On*
Nguyen Van Dan*, Sach*,
Nguyen Van Xinh*
Dispatcher—Doan Van Neo*

*CAPTURED OR RALLIED

Figure 7.

Evaluating

The analyst/advisor must evaluate all information before the fusion and analysis process. He must have a method of determining the validity of data. Failure to do this improperly weights information and leads to invalid

conclusions.

The U.S. military alphanumeric system for evaluation is simple and commonly used by police agencies and U.S. allies. The system assigns a value to the reliability of the source and the credibility of the information. Chapter 2, FM 34-3, provides a full explanation for the criteria shown below:[49]

A-completely reliable   1-confirmed by other sources
B-usually reliable   2-probably true
C-fairly reliable   3-possibly true
D-not usually reliable   4-doubtfully true
E- unreliable   5-improbable
F-reliability cannot be   6-truth cannot be
    judged   judged

In some situations, the sheer quantity of data may be overwhelming. Here, evaluation ratings act also as discriminators. If the analyst/advisor is dealing with large volumes of information, he may establish _rating minimums_ for posting on incident maps or SITMAPs.

Additional considerations in evaluating information are:[50]

1. Characteristics of the Source

A. Sensory limitation. What was really "seen" or "heard"? All sources, human and technical are limited in various ways.

B. Physical condition. Fatigued? Apathetic? On drugs/alcohol.

C. Bias. How is the source prejudiced?

D. Knowledge and experience

2. How far removed is the evaluator from the source?

3. Does the reported information correlate with other data?

Sifting data to determine false or only partially true information is the objective here. Colby states that during the Phoenix program, he generally required three separate identifications of infrastructure members before they were listed on official rosters.[81] In some cases there will be no determining the accuracy of information. The analyst/advisor, however should correlate the information with other he has received for confirmation. Information-sharing arrangements with other agencies can facilitate this.

Integrating

Next, the analyst/advisor assembles information to make it meaningful. The objective is to collate data which may arrive in volume and may appear to be unrelated. A technique for doing this is link analysis.[82]

Law enforcement units often use link analysis to develop intelligence on gangs and organized crime. Since insurgencies and organized crime share common methods of operation, the analyst/advisor will find link analysis useful in constructing the political order of battle.

Link analysis is a simple, common sense method of sorting information by visually portraying relationships.

27

Over time, lateral and vertical relationships become apparent as activities reveal a hierarchical pattern. The analyst/advisor then templates these organizations against generic cells and his country-specific model. This is the equivalent of doctrinal templating. The activity of the individual insurgents, along with information from captured documents, interrogations, and so forth, reveals cell types (operational, auxiliary, etc.). Thus, the analyst/advisor develops a construct of the insurgent shadow government, or parallel hierarchy. The following example is illustrative of the actual techniques involved:

A hamlet, or *sitio*, resident reports being taxed by the insurgents. Upon questioning, other residents admit to being taxed, but by a different individual. One resident states that she thought one of the tax collectors came from a family in a neighboring hamlet.

The analyst/advisor targets the two tax collectors, as well as the implicated family in the next hamlet, for intelligence collection. He tracks their activities recording contact with other individuals and organizations. Concentrating on repetitive contacts, he tries to determine the flow of money, food, information-anything that indicates hierarchy.

Using a number of link analysis aids, the analyst builds an order of battle (OB), of sorts. He can "wargame" this model, changing it to reflect other possible

arrangements if there is some ambiguity. Appendix D lists a seven step process for constructing a link analysis matrix and diagram.

Before going further in the intelligence process, the analyst now goes back to selecting/prioritizing targets and cues his collectors to highest value targets. As further information comes in, he confirms or changes the link diagram.

Link analysis without benefit of an informant, though valuable, can be a long conjectural process. Consider the difficulty in ferreting out an intelligence cell whose leader is an illegal cadre; whose members are legal cadre (community members) located in different *sitios*; and whose members pass information via drop. (See Figure 8.) If the insurgents communicate properly, the cell may be impossible to fully detect.
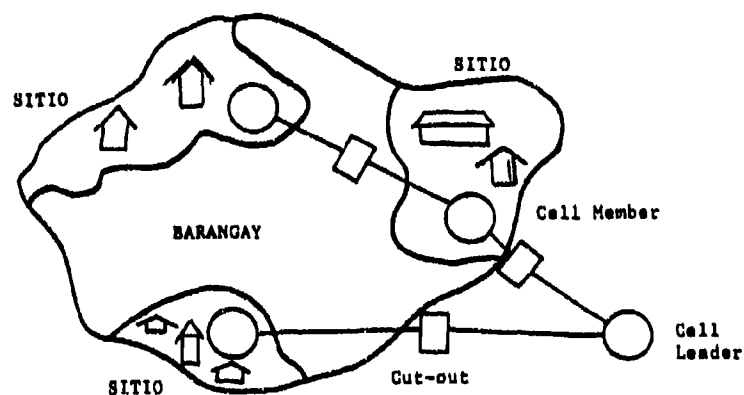

Figure 8.

Interpreting

After integrating (collating) available information, the analyst/advisor develops the insurgent's status, intentions, or course of action essentially through inference. Thus the next steps are inference development, inference testing or wargaming, and finalization of inferred enemy situation or course(s) of action.[82] The connection between these steps is inferential logic or reasoning based on the analyst's experience, recall, and powers of correlation.

The analyst/advisor looks primarily for patterns of activity. These patterns will yield contacts, indicate organizations, or reveal intent. Practically speaking, the analyst will constantly move between integration and interpretation, alternately using link and pattern analysis to identify the enemy.

Pattern analysis is a kind of situational templating wherein the analyst/advisor takes the *modus operandi* of the insurgents and lays it over the indicators or patterns reported. He then makes an inference based on these factors.

The current field manuals refer to pattern analysis briefly but don't explain it.[84] It is imprecise and best described through example. It relies on the analyst's judgement, and his facility with the tools of the trade (overlays, files, collection assets). Although pattern analysis is the heart of COIN intelligence production, a

field manual is inadequate for imparting expertise. It is a skill learned best through execution (or practical exercise).

The following examples are offered in illustration of the method. The last example uses a scenario.

Example 1. It is difficult or impossible to track units such as guerrilla squads or armed propaganda teams. They have virtually no signature. It is possible, however, to track the leaders of units (personalities) and the people who move with them. Informants normally report names or numbers of people since unit designations are not apparent. SIGINT usually yields names or callsigns as opposed to unit identities. As the same names and capabilities (e.g., mortars, demolitions) correlate over time (link analysis), the analyst/advisor develops an order of battle with rosters. Thus, when a SIGINT (DF and monitoring) report indicates that two insurgents named Julio and Miguel, and a mortar, are at a given location, the analyst lays this against his data bases. A data base yields Mortar Squad #3, six personnel habitually associated with it, two of whom are named Julio and Miguel. Thus, he infers the unit designation, parent unit, unit commander, etc. He then re-injects this intelligence into the inferential reasoning process to discern a broader scheme or intent.

Example 2. If an insurgent leader is a known womanizer, and has established "patterns" of visiting

particular women, this information should be in a data base. Hence, when the analyst/advisor locates a personality in a given geographical area, the insurgent's "patterns" should indicate a likelihood of contact with a girlfriend in that area. The analyst/advisor then cues surveillance or interception assets to the woman's location which has become, *de facto*, a named area of interest (NAI), or target area of interest (TAI).

Example 3. (Scenario) An insurgent leader travels with his girlfriend and has her function as his RTO. Her voice is distinctive on a radio net, thus allowing SIGINT collectors to track the insurgent's movements. A SIGINT report locates the insurgent leader in the village of Vallarto, near the small city of Santa Lucia. The analyst/advisor checks the personality and Vallarto files to determine when the insurgent last visited Vallarto. The answer: three times in the last 12 months. The analyst then retrieves the incident overlays which correspond to those dates. The overlays reflect two terrorist bombings in Santa Lucia, on military or police facilities, on dates corresponding to two of the insurgent's three appearances in Vallarto. The analyst then checks the data bases to see if the insurgent's movements correspond to other terror bombings. If so, it will reinforce the conclusion that a terrorist bombing is imminent in Santa Lucia. The analyst then notifies the appropriate agencies or military units.

Lastly, the analyst may find **flow charting** a valuable tool.[88] Whereas link analysis provides a snapshot of associations, flow charting depicts a progression of events or commodities over time or distance. It is a general purpose aid to analysis, and is appropriate for use as needed at any time in the process. Flow charting normally falls into two categories: **Event Flow Analysis** and **Commodity Flow Analysis**. Appendix E gives a description of the techniques and a fuller appreciation of their utility.

Disseminating

Ideally joint fusion and analysis centers should exist to bring together representatives of all military, paramilitary, and police organizations concerned with intelligence analysis. This aids information-sharing among all parties. If there is no joint effort, then the analyst/advisor must determine which intelligence products go out and to whom. Basic security and dissemination fundamentals such as "need to know" should be observed.

Dissemination has several principal considerations: security, timeliness, and packaging. Security is normally a matter of standard procedure while timeliness is matter of production and delivery. The format and quality of the product, however, is all-important. The goal of the identification process, then, is to produce Tactical Intelligence Support Packages, commonly known as target

folders. [34]

Target folders should include all intelligence available to the analyst/advisor pertinent to the target in a format useable by host nation forces. Creating a target folder necessarily means fusing intelligence from overlays, databases, files, and dossiers. An example will serve best to illustrate:

A number of prominent, district-level insurgent leaders meet in a remote guerrilla campsite. The camp has been occupied for purposes of the meeting. Ideally, the target folder would include such intelligence as:

--Updated maps and/or aerial photographs of the area and the camp.

--Strength/Disposition of security forces and automatic weapons.

--Locations in the camp area where mines have been encountered. Other obstacle locations.

--Optimal direction of attack for host nation forces.

--Optimal routes into the camp where the meeting will be held.

--Anticipated actions of insurgent leaders upon initiation of attack.

--Likely guerrilla egress routes.

--Likely destinations for escapees.

--Photos and pertinent dossier extracts on insurgent

leaders.

--Target windows.

--Optimal time of attack based on enemy habits/ discipline.

Target folders for other situations will obviously have different information. The goal is to fuse as much intelligence as possible into the most useable product.

Intelligence Center

The preceding discussion on tactical intelligence support packages implies a sophisticated and well-staffed analysis center. More probably the analyst/advisor will find himself in an austere situation, assisting a host nation staff with various levels of training. A grasp of the administrative organization of the intelligence center is thus essential.

The three critical functions of an intelligence center are collection, information storage and retrieval, and analysis. [87] In line with these, the analyst/advisor should work to insure the following conditions:

First, he must establish the center formally "in the net". In other words, there must be a permanent system, or tasking, to insure the flow of information into the center. This pertains to sources which he does not immediately control.

Second, the intelligence files must be comprehensive
and functional. The systems described in Appendix B
suffice.

Third, he must specifically designate personnel as
analysts.** Though this seems obvious, without personnel
dedicated to the task of analysis, the quality of the
product quickly deteriorates.

Each of these functions must be present, regardless of
unit size. At the lowest tactical levels, a small operating
staff may be the norm. In such a case, jobs should be
shared. If a single individual is selecting intelligence
targets, analyzing, or doing both, the impact of personal
bias may be substantial. The analyst/advisor should be
alert to this in himself and in the intelligence staff.
Reviewing collection plans or wargaming analysis with this
in mind can help overcome it. Finally, the analyst/advisor
should establish liaison with other intelligence agencies.

In a broader context, the development of joint fusion
and analysis centers is a better solution than a single-
service intelligence center. All the principles of
organization, collection, and analysis still apply. The
objective is to unify the capabilities of police and
military units which would otherwise conduct unilateral
operations against the insurgent infrastructure. The idea is
not new. This was the charter of both the Intelligence
Coordination and Exploitation Program (ICEX) and its

successor, the *Phung Hoang* program, in Vietnam. The American name for *Phung Hoang* was Phoenix.

Contrary to its sensational reputation, Phoenix was an overt program. It was established by [South Vietnamese] presidential decree in an effort to centralize intelligence collection, analysis, and dissemination on the Viet Cong infrastructure. American advisors were assigned to it. Although Phoenix had committees at province and national levels, the district-level center was the principal intelligence coordination and operations element. Phoenix itself commanded no combat or police units.

> Each [district] Phoenix office was supposed to
> house representatives of the national police; the
> district S-2 (intelligence officer); the Military
> Security Service (MSS, the military intelligence
> organization responsible for ... counterespionage
> and countersubversion); the Rural Development
> cadre (...[its] members frequently learned...about
> Vietcong activity as they built schools and dikes
> in the villages); and finally, the S-3 (the
> operations section of the district staff which-in
> theory-planned military operations based upon the
> targets generated by the Phoenix effort).[49]

Phoenix was to produce, then disseminate its products to the organization best suited to neutralizing a given target. After the war, former Viet Cong cadre members testified to Phoenix's devastating effectiveness.[40] Conversely, its founder, Robert Komer, and its initial director, William Colby, have stated that Phoenix was only partially effective, never reaching its potential. Corruption, turf battles, quotas, and lack of cooperation among agencies all

37

worked to hamstring the program. As a result, some district Phoenix centers functioned well, others did not.

Phoenix's problems and its reputation not withstanding, the concept is sound. But rather than merely have police, paramilitary, and military representatives, it must be a truly joint intelligence effort. All host nation collection assets, regardless of ownership, would feed and respond to the center. Analysts and clerical personnel as well would come from the various services. Target intelligence support packages would be forwarded to an executing unit by a senior joint commander specifically empowered to task these missions.

The identification of infrastructure is the most critical aspect of a sound, well-executed counterinsurgency. I have couched the techniques presented here inside an established doctrinal framework because it is both appropriate and familiar to the military reader. Undeniably the flavor of police operations is present, as it should be, given the nature of insurgent infrastructure and the role of police in fighting it.

SECTION III

CONSIDERATIONS IN THE
REDUCTION OF INFRASTRUCTURE

Targeting and reducing infrastructure are two of the most controversial aspects of a counterinsurgency.   In this

38

section I will briefly present considerations for the
analyst/advisor in targeting and neutralizing insurgent
cadre members.

Targeting

Based on his own predetermined indicators, the
analyst/advisor will decide that he has identified enough
infrastructure to do a target analysis. The criteria shown
is derived primarily from the target analysis acronym,
CARVER (criticality, accessibility, recuperability,
vulnerability, effect on the population, recognizability).[1]
Additional planning considerations are added for
completeness.

1. How much of the infrastructure is known? Yet to be
identified?

2. What is the criticality (importance) of the targeted
infrastructure members? The Phoenix program assigned
suspects "to one of three categories: "A" for leaders and
...party members, "B" for holders of other responsible jobs-
cadre-and "C" for rank-and-file members and followers."[2]
Colby, as the director of Phoenix, decided not to target "C"
members since they were relatively unimportant.

3. How accessible is the target(s)? Is target
accessibility time sensitive ?

4. How recuperable is the target(s)? If the target
can be replaced quickly, is it worth taking out?

39

5. How vulnerable is the target(s)? This is a question of forces available. What type of forces are most appropriate- police, paramilitary, or military? Are there enough troops available? Are they sufficiently trained?

6. How much of the identified infrastructure should be neutralized? Is there an "A,B,C" criteria established? What is the criteria for local and district guerrilla units (vice party, civil infrastructure)? Should "As" and "Bs" be neutralized as soon as identified or only when a complete cell is known? Should any part be left intact? This is particularly critical if recuperatory ability is high. If only a percentage of targets can be neutralized before others are alerted, which are most important (criticality)?

7. Can the government protect the people from reprisals ?

8. Is identification of the target a problem? Are informants, ralliers available to identify insurgents and to act as guides?

Practically, the analyst/advisor will often target individuals. Politically, the semantics of targeting an insurgent unit instead of an individual may present a better option.

Neutralization

Neutralization means to kill, capture, or recruit.

Like "infrastructure", "neutralization" is a uniquely American term. Like Phoenix, it usually conjures up draconian images. "Reduction" may be a better choice in the future since it is somewhat neutral in connotation and sufficiently vague. However, it will mean kill, capture, or recruit.

In keeping with current U.S. military assistance policy, neutralization is the responsibility of the host nation. That much is clear. Beyond this, little is clear. The moral, ethical, and legal issues in a neutralization policy are extensive and go well beyond the scope of this paper. There are several points worth mentioning, however.

The first is the nature of the ideologue. Infrastructure members who fit into categories A and B may be called ideologues. Certainly party members qualify for that title.

Ideologues are true believers. They are more than converts. Ideologues have been schooled in the philosophy of the revolution, often in another country. Their susceptibility to an amnesty program is very low. So too is the likelihood of their informing, if captured. The government must kill or incarcerate them until the insurgency has been eradicated.[43]

The second point is the issue of objective. At every decision point, the analyst/advisor must focus on the objective. The objective is to enhance the legitimacy of

41

the host nation's government. This must take precedence
over convenience in neutralizing infrastructure. Put
plainly, there are times when overwhelming military force is
appropriate to the target. There are also times when
capture by police better serves the government. The arrest
of communist civil cadre on charges of murder, for example,
rather than terrorism accomplishes the objective without
creating a revolutionary martyr.

The analyst/advisor's role here is difficult. He must
understand existing emergency legislation and other
politically sensitive issues. He should have clear guidance
as to his role beyond the preparation of a target folder.
(This role should be defined by the host nation and the
analyst/advisor's chain of command.) And finally, if he has
credibility among his host nation counterparts, even his
unofficial opinions will have effect. Whatever he says or
does must enhance achievement of the objective.

SECTION IV

CONCLUSIONS

The purpose of this monograph was to examine a
perceived weakness in the education of intelligence and
special operations personnel. Based on their high
likelihood of commitment as analysts or advisors worldwide,

42

these personnel have a particular need to understand the process of identifying insurgent infrastructure. The procedures outlined in this study highlight and fill those areas where current manuals fall short.

Intelligence operations in low-intensity conflict deserves its own field manual. This mandates a thoughtful compilation of analysis, information management, and counterintelligence techniques in an insurgency context. Generic insurgency study manuals should accompany it. Several Department of the Army Pamphlets published in the late 1960s (see Bibliography) need little revision to meet this requirement.

The Special Warfare Center and the Military Intelligence School should include infrastructure identification in their curricula for officers and senior NCOs. Both schools teach much of the material, or related subjects, already. None of the concepts are new. In order to incorporate the best law enforcement experience, the schools should obtain programs of instruction from police organized crime information centers.

Lastly, the concept of joint intelligence centers modeled after the Phoenix program is one worth pursuing and putting into doctrine. The realities of police forces and police operations in each nation will uniquely vary the application, yet the concept can only enhance the attack on insurgent infrastructure.

43

ENDNOTES

1. FM 100-20, Low-Intensity Conflict, Final Draft (Fort Leavenworth: USACGSC, March,1989), p. 2-11.

2. Douglas Pike, PAVN: People's Army of Vietnam (Novato: Presidio, 1986), p.59.

3. Department of the Army Pamphlet 550-106,The Communist Infrastructure in South Vietnam: A Study of Organization and Strategy (Washington, D.C.: Headquarters, Department of the Army, March 1967), p. 20.

4. General Jean Marchand, L'Indochine en Guerre (Paris: Les Presses Modernes, 1954), p. 181; cited by John J.McCuen, The Art of Counter-Revolutionary War (Harrisburg: Stackpole Books, 1966), pp. 98-99. Parallel hierarchy is a French concept/term fundamental to French theories of revolutionary and counter-revolutionary war. See Roger Trinquier, Modern Warfare, translated from French by Daniel Lee (New York: Frederick A. Praeger, Inc., 1964), p. 30. Trinquier uses the term "parallel organizations".

5. DA PAM 550-106, Communist Insurgent Infrastructure, p.31. See also Department of the Army Pamphlet 550-104 Human Factors Considerations of Undergrounds in Insurgencies (Washington, D.C.: Headquarters, Department of the Army, September 1966), p. 19. The term "shadow government" is in common use today, particularly among Philippine military officers.

6. DA PAM 550-106, Communist Insurgent Infrastructure, p. 20-22. Also DA Pam 550-104, Undergrounds.

7. DA PAM 550-104, Undergrounds, p. 52.

8. DA PAM 550-106, Communist Insurgent Infrastructure, p. 145. Also, LTC Rolando Garcia, Philippine Constabulary, interviews by author, 7 and 13 November 1989, Fort Leavenworth, KS.

9. Stuart A. Herrington, Silence Was A Weapon (Novato: Presidio Press, 1982), p. 13.

10. Sir Robert Thompson, Defeating Communist Insurgency (New York: Praeger, 1966), p. 55.

11. Ibid., p.56.

12. Frank Kitson, Low Intensity Operations: Subversion, Insurgency, Peace-Keeping (Hamden: Archon,1974), p. 49.

13. FM 100-20, Low-Intensity Conflict, p. D-8.

14. Department of the Army Pamphlet 550-104 Human Factors Considerations of Undergrounds in Insurgencies (Washington, D.C.: Headquarters, Department of the Army, September 1966), p. 21.

15. Ibid., p. 20.

16. Ibid.

17. Ibid., p. 19-23.

18. Ibid., p.21.

19. Ibid., p. 22.

20. Ibid., p. 23.

21. Ibid., p. 24.

22. Ibid., p. 25.

23. Ibid., p. 24-25.

24. Ibid., p.26.

25. Ibid., p. 42.

26. Pike, PAVN, p. 30.

27. DA PAM 550-106, Communist Insurgent Infrastructure, p. 120.

28. DA PAM 550-104, Undergrounds, p. 27.

29. FM 34-60 Counterintelligence (Washington, D.C.: Headquarters, Department of the Army, August 1985), p. 6-2.

30. LTC Rolando Garcia, Philippine Constabulary, interviews by author, 7 and 13 November 1989, Fort Leavenworth, KS. The CPP model was drawn from materials and information received in these interviews.

31. Kitson, Low Intensity Operations, p. 200.

32. FM 34-3 Intelligence Analysis (Washington, D.C.: Headquarters, Department of the Army, August 1985), p. 2-0 to 2-1.

33. Mid-States Organized Crime Information Center (MOCIC) Program of Instruction (POI), The Intelligence Model, p. 2.

34. BG John F. Stewart, USA, "Military Intelligence Operations in Low-Intensity Conflict: An Organizational Model," Military Review 68 (January 1988): 22.

35. FM 34-60 Counterintelligence, p. 6-11.

36. Peter M. Ossorio, Assistant U.S. Attorney, U.S. Department of Justice, Western District of Missouri, interview by author, Kansas City, MO, 16 October 1989. The Army's doctrinal term for this is "source handler"(U), though "case officer" is firmly established in the vernacular. See FM 34-60A Counterintelligence Operations (S/NFN/WNINTEL) (Washington, D.C.: Headquarters, Department of the Army, June 1989), p. 6-5.

37. Herrington, Silence, p. 103. See also Kitson, Low-Intensity Operations, p.117.

38. Herrington, Silence Was A Weapon, p. 20.

39. MOCIC POI, Intelligence Information Storage and Retrieval System, p. 1.

40. FM 34-3, Intelligence Analysis, p. 9-3 to 9-5.

41. MOCIC POI, Intelligence Information Storage and Retrieval System, p. 1.

42. Ibid., p. 2.

43. FM 34-3 Intelligence Analysis (Washington, D.C.: Headquarters, Department of the Army, January 1986), p. 9-3. Some of the categories mentioned in the text are discussed here and on p. 9-10.

44. FM 34-130 Intelligence Preparation of the Battlefield (Washington D.C.: Headquarters, Department of the Army, May 1989), Appendix E, p. E-4 to E-8.

45. FM 34-3, Intelligence Analysis, p. 9-2.

46. FM 34-3 Intelligence Analysis, p. 9-3.

47. FM 34-60, Counterintelligence, p. 6-3.

48. Andrew P. O'Meara, "Infrastructure and the Power Seizure: A Structural Functional Analysis of the Bolshevik and Chinese Communist Models of Revolution" (Master's thesis, USACGSC, 1970), p. 143.

49. FM 34-3, Intelligence Analysis, p. 2-11 to 2-12.

50. MOCIC POI, Data Evaluation, p. 4.

51. William Colby and Peter Forbath, Honorable Men: My Life in the CIA (New York: Simon and Schuster, 1978), p. 268.

52. MOCIC POI, Link Analysis Techniques, p. 1.

53. MOCIC POI, The Intelligence Process, p. 7.

54. FM 34-3 Intelligence Analysis, p. 9-5: Briefly states use of patterns in integrating information; p. 10-12: Cites FM 34-60A Counterintelligence Operations as describing pattern analysis. However, the June 1989 edition of FM 34-60A does not list or contain a description of pattern analysis. See also FM 34-60 Counterintelligence, p. 3-12.

55. MOCIC POI, Flow Charting Techniques, p. 1.

56. U.S. Army Military Intelligence Officer Advanced Course (MIOAC) Program of Instruction (POI), Department of Tactical Intelligence and Military Science (DTIMS), Low-Intensity Conflict block of instruction: El Salvadoran Case Study; IPB block of instruction. This is not, as yet, a doctrinal term. It is in common use in some parts of the intelligence community. "Target folder" is in the vernacular throughout the intelligence and special operations communities.

57. MOCIC POI, Building The Intelligence System, p. 4.

58. Ibid.

59. Herrington, Silence Was A Weapon, p. 12-13.

60. Stanley Karnow, Vietnam (New York: Viking Press, 1983), p. 602.

61. U.S. Army, Special Operations Targeting Handbook (FOUO) (Fort Bragg, NC: SFOD-I, DCSINT, USA 1st SOCOM Edition 5), p. 3.

62. Colby, Honorable Men, p. 268.

APPENDIX A

COMMUNIST PARTY OF THE PHILIPPINES
METHODOLOGY[1]

Militarily and politically, the CPP/NPA[2] has been most successful in the countryside. It follows a simple but persistent methodology for establishing its infrastructure in rural areas. The CPP/NPA begins by sending a SemiLegal Team (SLT) into a *barangay*, or village. The SLT is a 3-5 person cell which uses any number of cover stories to penetrate a *barangay* and begin its social investigation.

To create legitimacy, it may pose as representatives of pharmaceutical or medical equipment companies conducting a survey; similarly, it may profess to represent the Bureau of Fisheries, or Forestry, or other government agencies.

The SLT quietly ingratiates itself to the local people and begins to compile data. It acts without noticeable

---

[1] James A. Horris, "U.S. Military Assistance to Philippine Ground Forces" (thesis, USACGSC, 1989), 24-30. Some of the thesis research is used in this appendix. It has been updated/corrected through recent interviews.

[2] The Communist Party of the Philippines (CPP) is conducting an insurgency to overthrow the Aquino government. The New Peoples Army (NPA) is the military arm of the CPP. At the lower levels, however, the lines are not cleanly drawn. Thus the insurgents are commonly called the CPP/NPA.

A1

malicious intent. Depending on its cover story and other circumstances, the SLT may remain in the *barangay* continuously, or depart and return later to resume its social investigation.

The SLT pursues such information as grievances against local and national government, grievances against landowners, prevalence of disease and illness, and the number of school drop-outs. It also recruits villagers for guerrilla training at an NPA training camp. Often this training is couched in terms of a "job offer" and school drop-outs are a favorite target.

The SLT identifies future leaders from within the *barangay* population, as well as those who may prove troublesome. Dossiers are compiled. Through informal discussions, these local leaders are gradually indoctrinated and together with the SLT form a *Barangay* Liaison Group (BLG). See Figure A1. The BLG usually grows to include


```
                    ┌──────────────────────────────────┐
                    │   ┌──────────────────────────┐   │
   ╭─────╮          │   │ BARANGAY        BLG      │   │
   │ SLT │──────────────│ LIAISON                  │   │
   ╰─────╯          │   │ GROUP                    │   │
 Infiltrates        │   └──────────────────────────┘   │
 Conducts Soc Invest│                                  │
 Establishes BLG    │          BARANGAY                │
                    └──────────────────────────────────┘
```
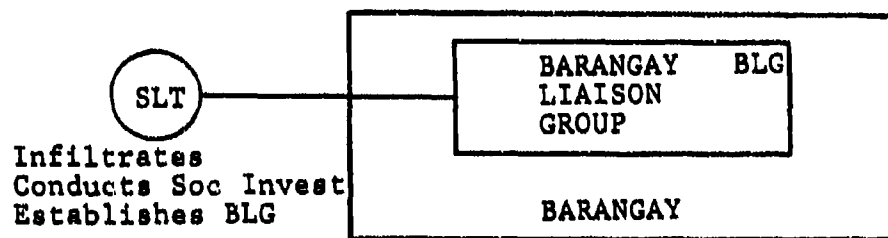
Figure A1.

relatives and close friends of the core group of leaders. At this point the SLT begins conducting teach-ins.

A 2

As numbers grow, the Liaison Group becomes known as a *Barangay* Organizing Group (BOG). See Figure A2. In this phase the SLT organizes the people into sectoral groups such as peasants, men, women, youth, and laborers. A variation on this theme is for members of the BOG to begin influencing members of already-existing sectoral groups to which they belong. The BOG also begins forming a militia.
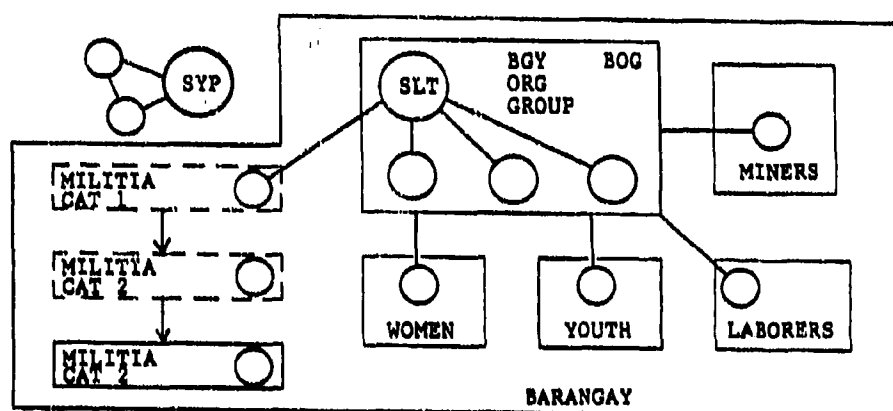

Figure A2.

Formal training is now injected. Using classroom lectures, the SLT indoctrinates villagers in such subjects as ideology and simple Marxist economics. Meanwhile informal training through discussion and teach-ins continues.

It is important to note how the *barangay* is organized. Men, women, and youths are all placed in different groups with different leaders. In this way, the communists unobtrusively subvert traditional family cohesiveness and

A3

further create vulnerability to their teachings.

The militia usually consists of 10-14 local males, and
undergoes an evolution of its own. Each phase is called a
category. In the first category, the militia men are new,
unarmed, and used in local intelligence or early warning
nets. In the second category, they are given some small
arms; these are usually few and often crude. Missions are
usually defensive in nature. As they become better trained,
they will be fully armed and considered category three.
They will conduct offensive operations and may be placed
under the operational control (OPCON) of the District
Guerrilla Unit for selected missions.

Once in the third category, five to seven individuals
from the militia will be formed into a *Sandatahang Yunit
Pangpropaganda*, (SYP). On the direction of the SLT and
approval of District headquarters, the SYP will brutalize or
kill selected inhabitants to enhance the propaganda effort.
This may mean meting out "revolutionary justice" to a local
criminal, AFP collaborator, or offending landowner; or it
may simply mean shooting an individual who resists
indoctrination. The NPA is rarely arbitrary in selecting
its initial victims. It establishes legitimacy in the eyes
of the people by providing visible relief to an immediate
problem, with an astute eye toward its propaganda value.

Again there are variations to this methodology. It may
not be wise to use a SYP against the people of its own

A4

barangay or *sitio*.[x] In this event, the SLT contacts the District Party Committee (DPC) and imports a SYP from a different area with no allegiance to the local populace. The SYP is a familiar feature of communist, mass-based insurgencies, more commonly known as an Armed Propaganda Team or Unit, (APT or APU).

As the communist hold over the *barangay* grows tighter, the BOG, growing ever larger, becomes known as a *Barangay* Organizing Committee, or BOC. See Figure A3. The BOC is a
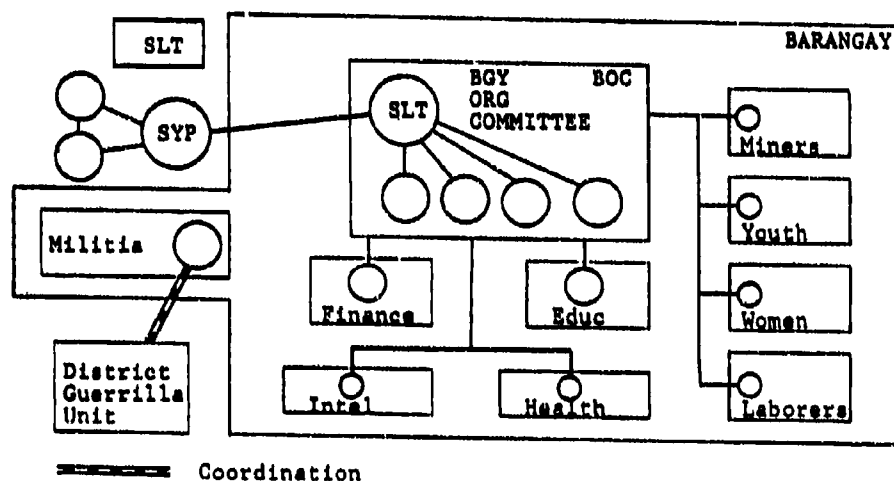

Figure A3.

further step in the progression toward a full-fledged shadow government. Using auxiliary cells, it organizes

---

[x] A *sitio* is a small community located within the geographic area of a *barangay*. It is analogous to the Vietnamese hamlet. Just as there are several hamlets in a village, so, too, there are usually several *sitios* in a *barangay*.

functional groups (e.g.,Health, Finance, Education) to co-opt the civil administration of the barangay. The BOC continues to infiltrate and direct the sectoral groups previously established, while expanding its activities in other areas. Cell leaders step up recruiting for NPA training camps, form intelligence (spotter) networks, and develop logistical support cells for the guerrillas.

The recruiting mandate placed upon cell leaders never ceases. Recruits either remain in the *barangay* militia, or go to guerrilla training camps. Graduates of the training camps are sent to either a DGU or Regional Mobile Unit (RMP). The District Guerrilla Unit responds to the District Party Committee (DPC) and is not subordinate to the RMP. Similarly, the Regional Party Committee alone directs the activities of the Regional Mobile Unit, if one exists. The NPA High Command draws forces as needed from the RMPs, but only for special purpose units (e.g., Sparrow teams). It does not command the RMPs. And as of this writing, there are no known Main Force units.

As the *Barangay* Organizing Committee matures, the government's control deteriorates. The BOC extracts revolutionary taxes from the people and protection money from plantation owners and local businesses. Having set the wheels in motion, the original SLT forms a new nucleus from within the community itself. It then moves on at the direction of the DPC to organize another *barangay*. All

these steps portend the final evolution of the *barangay* into a *Barangay* Revolutionary Committee (BRC). See Figure A4.
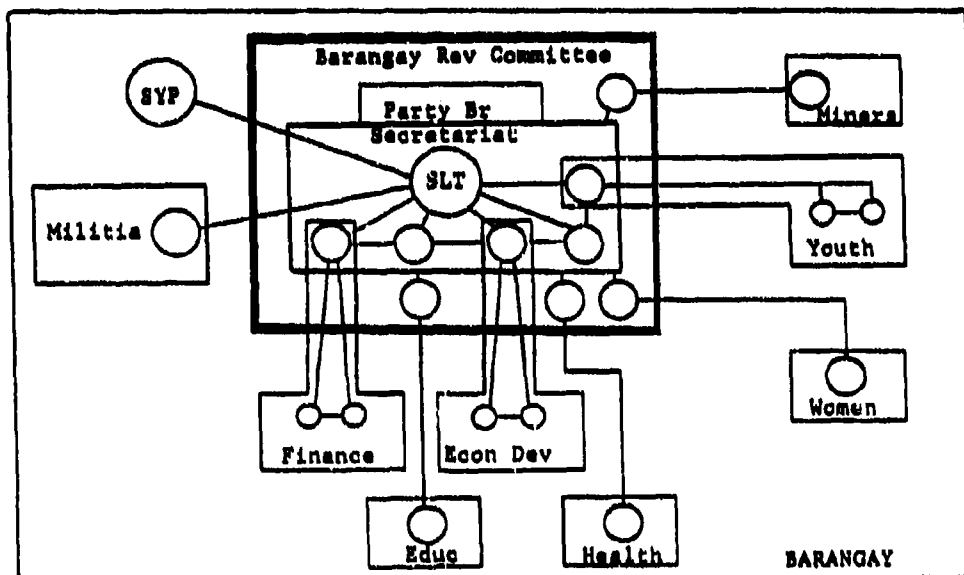

Figure A4.

The *Barangay* Revolutionary Committee is the highest form of political organization that the CPP/NPA will pursue in a *barangay*. It is a parallel hierarchy which theoretically co-opts every function of the established government. The BRC is composed of a Secretariat and cell leaders from the various front (sectoral/functional) groups. The Secretariat is the executive committee for the BRC. It includes the SemiLegal Team, selected front group leaders, and a communist party cell if one is located in that *barangay*.

The communist party cell is known as a Party Branch.

A 7

This is a generic term and Party Branches exist in every tier of the infrastructure. A Party Branch collocates with a BRC to exercise greater control over it. Another variation has the Party Branch centrally located within a portion of a district to manage the activities of several *barangays*. See Figure A5.
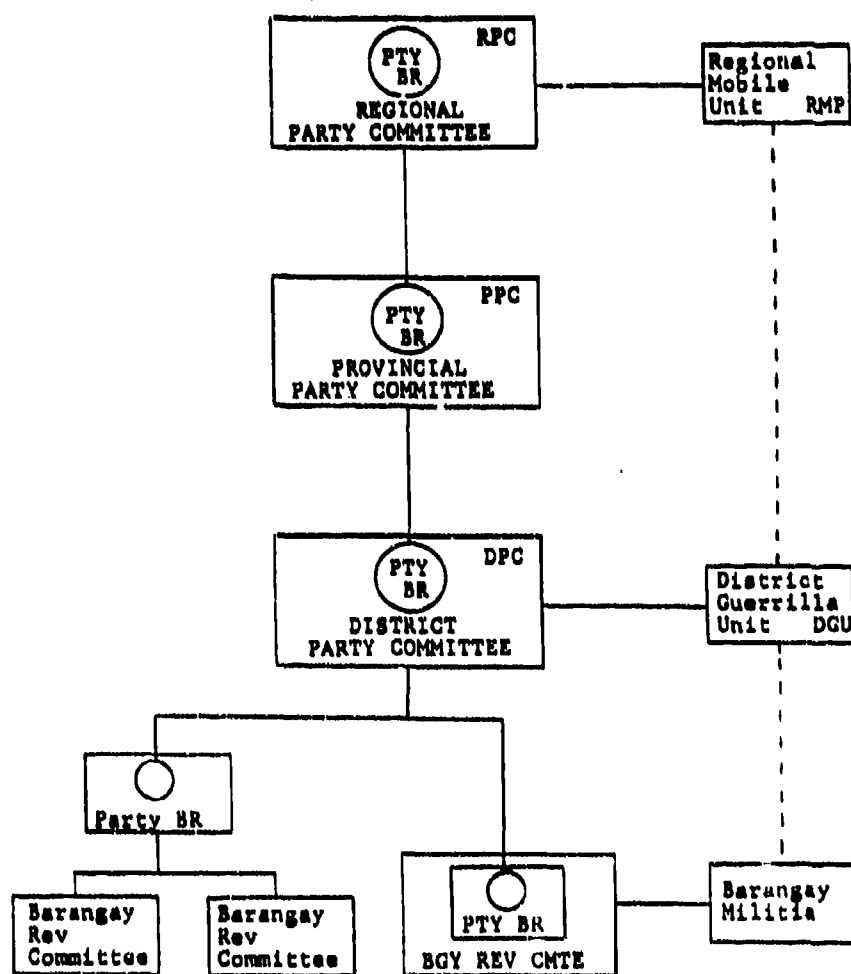
Figure A5.

In reality, the number of Party Branches is not as great as the reader might infer. In some areas, the hierarchy of Regional/Provincial/District Party Committees does not fully exist. In these cases, a single Party Branch and its Party Committee must fulfill the roles of several.

The influence of the CPP/NPA is by no means pervasive in the Philippines. However, it is crucial to grasp the point that the CPP/NPA has, in some cases, governed some portions of the country for nearly two decades. In these areas, legitimacy lies with the insurgents, and the federal government is an intruder.

INFORMATION STORAGE AND RETRIEVAL SYSTEMS[1]

Classification

The classification system operates on the simple concept of categories of information, or data bases. It uses a decimal system of numbering to provide for expansion and accommodates nested classes of information. The index may use 3x5 cards, or any other medium as long as it is physically, or electronically, expandable. Maintenance of the index is critical to prevent the loss of information.
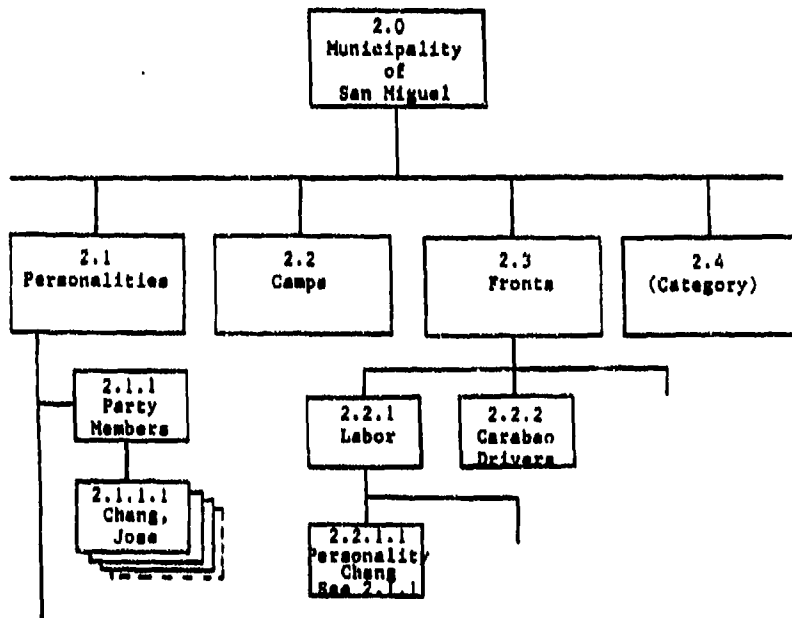
Figure B1. [2]

Accession

This system stores information (e.g., reports, documents) serially. When an analyst receives an item of information, he identifies individuals, organizations, etc., for indexing. He then fills out new index cards, or annotates existing ones. The analyst assigns a sequential accession number to the item and notes it on the appropriate index cards. He then files the item by serial number and index cards alphabetically.

To retrieve the information, the analyst searches the index for the subject. He then goes to the numbered files indicated on the index card.
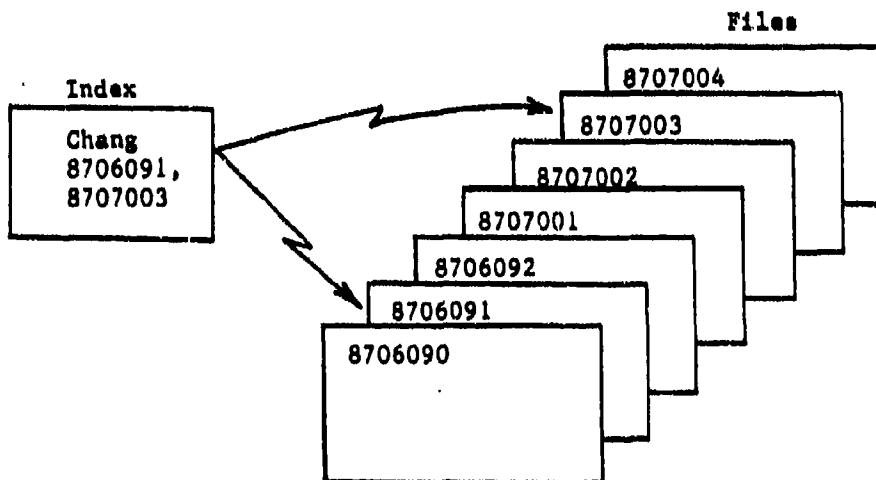
Figure B2. ᵔ

The serial number system shown below (Figure B3.) is used by the Mid-States Organized Crime Information Center for

several of its intelligence files. This system has the
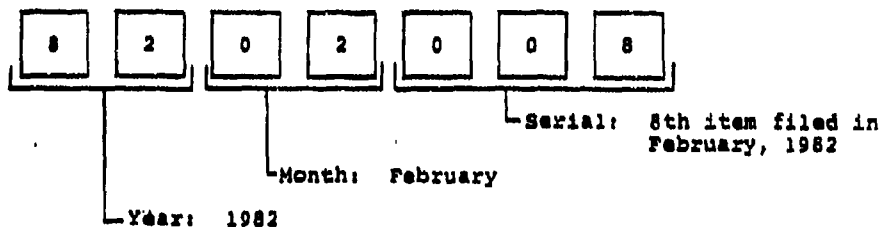advantage of simplifying a physical audit.

Figure B3. *

The following comparison matrix allows the analyst to
determine which system best suits his needs.

COMPARISON CRITERIA	CLASSIFICATION SYSTEM	ACCESSION SYSTEM
Ease of storage	Filed by decimal number after classification assigned. File summary, if used, must be updated. Multiple copies may be needed.	Filed directly by accession (serial) number No classification or updating required at time of entry. No copies needed.
Ease of indexing	Classifications selected and decimal numbers put on index cards.	Accession number put on index cards.
Ease of retrieval	Quick access to collections of information; slow access to individual items.	Quick access to individual item; slow access to collections of information.
Selectivity of retrieval	Less selective--must search through entire folders to find relevant items.	More selective--each item is numbered and indexed.
Facilitation of analysis	Analysis is hampered by less selectivity and slower access to individual items.	Analysis is facilitated by greater selectivity and faster access to individual items.
Security from compromise	Assembled information (e.g., file on Black Panthers) is easier to define and get to by outsiders. Lost or misplaced items cannot be identified.	Unassembled information (there is no file on Black Panthers) is more difficult to define and get to by outsiders. Missing items are easily identified.
Ease of expansion	Unlimited.	Unlimited.
Ease of purging	Since every file must be reviewed, purging is necessarily difficult.	Application of recency or activity-level purging criteria is relatively easy.

Figure B4. *

B 3

1. Mid-States Organized Crime Information Center (MOCIC) POI, _Intelligence Information Storage and Retrieval System_, p. 1-5. All information in this appendix is drawn directly from the MOCIC POI. These are Police Intelligence techniques.

2. Illustration adapted from MOCIC POI, _Intelligence Information Storage and Retrieval System_, p. 3.

3. IBID., p. 4.

4. Ibid.

5. Ibid., p. 6.

APPENDIX C

SELECTED DATA BASE FORMATS

The formats shown here illustrate the types of information needed in a data base/file. They are the author's suggestion. Actual formats are the analyst's choice.

Personality

Name:

Alias/War name:

Rank:

Assignment/position:

Cover/job:

Education:

Appearance, skills, character traits:

Family Locations: (immediate family, relatives)

Girlfriends, wife(s):

RTO: (identification, callsign)

Reports: (chronological entries listing date, source
identification and evaluation rating, content of
report)

Order of Battle Card

Field Manual 34-3 _Intelligence Analysis_ devotes an entire chapter to developing enemy Order of Battle (OB). It prescribes an array of methods for documenting enemy units. It is clearly oriented toward a conventional foe. Nevertheless, many of the techniques may be modified for counterinsurgency, and will be particularly applicable to Main Force guerrilla units.

Guerrillas often remain dispersed until a mission dictates massing. Only during missions then will the company, platoon or squad exist as a unit. In any case, a formation considered a unit by the insurgent should be so considered by the analyst, and entered in the data base regardless of size. The format below comes from FM 34-3, with a chronological record added to aid in pattern analysis:

Unit I.D.: (numerical designation, type)

Subordination: (parent/subordinate units)

Code name: (assigned by enemy)

Nickname: (unofficial popular name)

Commander:

Subordinate Leaders: (a full unit roster also may be kept
                      here or in another file)

Signature equipment/insignia: (items which distinguish the
                               unit from other guerrillas,
                               if any)

Combat performance/effectiveness: (analyst's estimate)

Location: (date)   (grid)   (place name)   (remarks)
             "   "   "   "

C 2

Camp File

Name/number: (include index number or file location of
sketch or overlay)

Location: (include map sheet number)

Description: (buildings, type construction)

Reports:

Propaganda Themes

Theme: (salient topic; include file location of dossier)

Date(s):

Location:

Description:

Results:

Correlation to Significant Event:

APPENDIX D

LINK ANALYSIS TECHNIQUES [1]

Use the following process to construct link diagrams:

1. Assemble all raw data and put in some organized form (such as a log). Necessary since basic data or information may come from many different sources such as files, patrol reports, SIGINT/wire-tap records, informants, etc.

2. Choose the data points (such as names and/or organizations) important to the analysis and abstract from the narrative.

3. Construct an association matrix and list data points (names, business, phone numbers, etc,), as headings on the diagonal axis in alphabetical order.

4. Enter the "association" points on the matrix. Where there is strong evidence of a link between the individuals enter a dark dot (o) in the matrix, where there is less than strong evidence, enter an open circle (o).
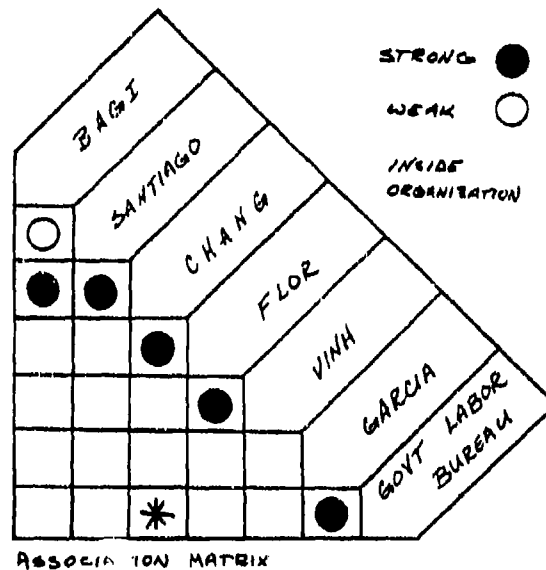
Figure D1. Association Matrix [2]

5.   Determine the number of links associated with each
individual. (Count the number of times an item appears in
each cell in the matrix.)

6.   Draw a draft diagram of the links between individuals
starting from the individual with the most associations.
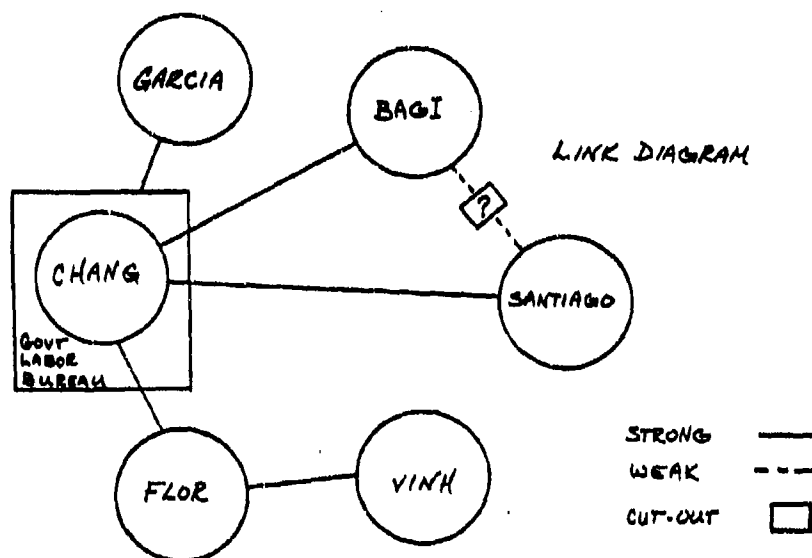(Dark dots are shown as solid lines; open circles are shown
as dotted lines.)

Figure D2.

7.   Clarify and re-plot the diagram. (Avoid crossing lines
Use straight lines.) Relate individuals to organizations by
enclosing the circles (individuals) in large rectangles
(organizations).

     Shown below are further techniques to assist the
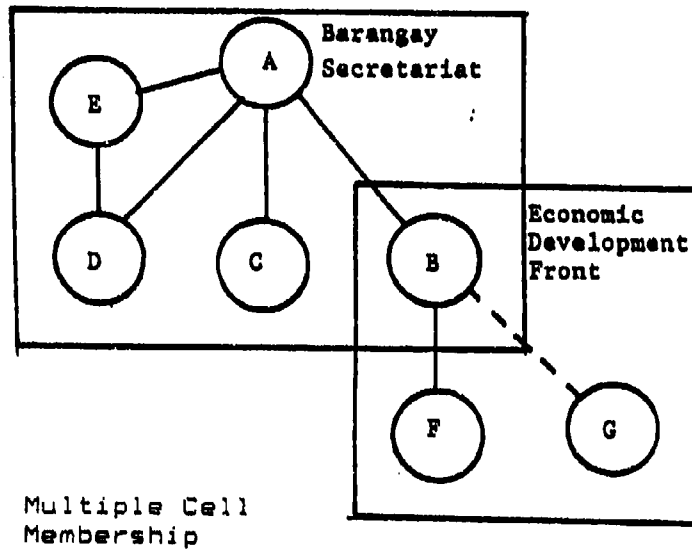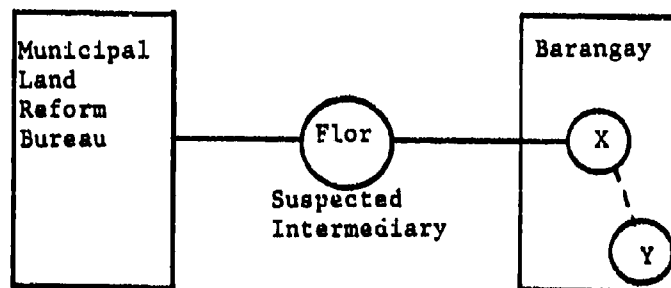
analyst in displaying infrastructure associations.

Multiple
Organization
Membership

Figure D3.

Barangay
Secretariat

Economic
Development
Front

Multiple Cell
Membership
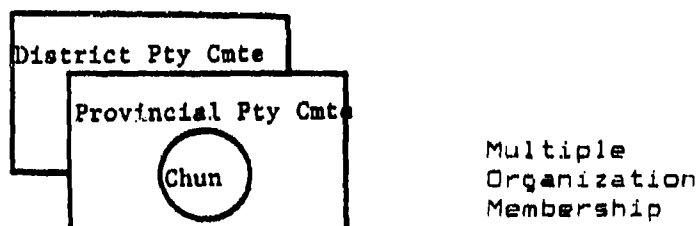
Figure D4.

Association between subject
and organization/business

Municipal
Land
Reform
Bureau

Barangay

Flor

Suspected
Intermediary

Association between a subject
and subject in a community

Figure D5. *

ENDNOTES
APPENDIX D

1. Mid-States Organized Crime Information Center (MOCIC) POI, <u>Link Analysis Techniques</u>, p. 2.

2. Ibid., p.

3. Ibid., p. 4.

4. Ibid., p. 9.

5. Illustration adapted from MOCIC POI, <u>Link Analysis Techniques</u>, p. 13.

APPENDIX E

FLOW CHARTING [1]

Flow charting has few, if any, rules. The analyst uses symbols of his own choosing, however he should be consistent. He should use arrows to indicate flow. Charts should generally run top-to-bottom, and left-to-right.

Event flow charts consist of a description of each event enclosed by a circle or rectangle. These are connected by arrows showing progression or direction of flow. Arrows may annotate time or distance. In the figure below, circles represent events, and boxes represent results. Dashed lines indicate suspected or possible flow/events.
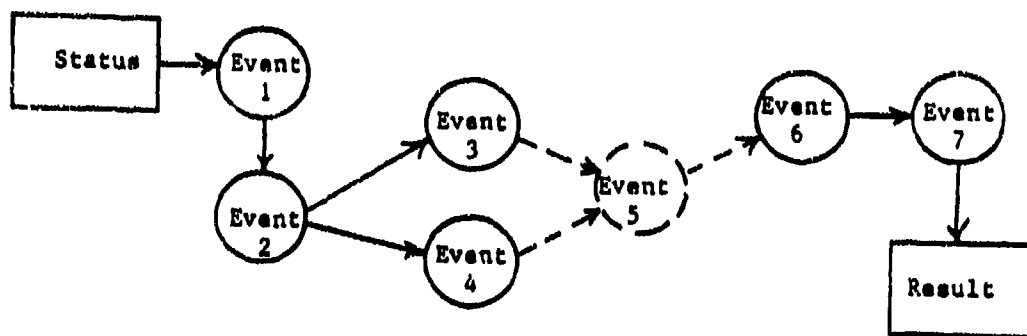
Figure E1. Event Flow Analysis[2]

A single flow chart will not establish a pattern. However, event flow charts constructed for each barangay depicting a particular process (such as initial contact and social investigation by SemiLegal Teams) will assist in defining a modus operandi when compared (pattern analysis).

Commodity flow analysis is a similar process but uses different parameters. It is useful in identifying the persons, organizations, and time involved in the flow of commodities. These include money, narcotics, food, arms, and so forth. Currency flow usually runs parallel but opposite to the commodity itself. Both should be traced to identify key persons and organizations. [3]

The following example is a common scenario in the Philippines today: International church organizations contribute money to a Christian relief organization in country. The relief organization is a front for the insurgency. The party siphons off most funds and gives the remainder to selected churches/parishes in rural areas where the clergy are members of the Church for National Liberation (CNL). The clergy's orders are to buy rice and store it with other supplies while contracting transportation to remote barangays. The contractor is legitimate but the barangays are communist influenced. Insurgent cadre receive the supplies. Most is sent up-country to NPA training camps. Some is used to "repay" villagers for food previously taken by guerrillas, amid much proselytizing.

E 2

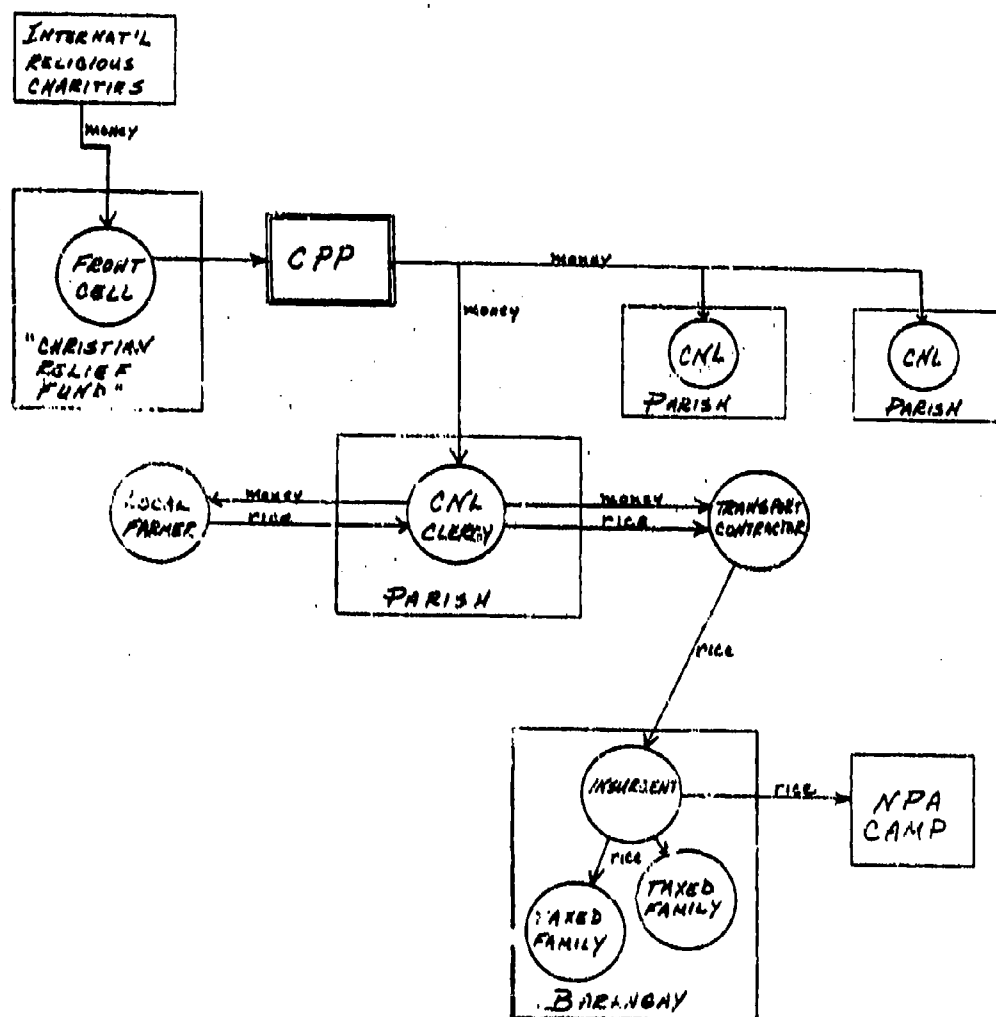In the illustration below, circles represent individuals, boxes represent organizations.

Figure E2. Commodity Flow Analysis

ENDNOTES
APPENDIX E

1. Mid-States Organized Crime Information Center (MOCIC) POI, _Flow Charting Techniques_, p. 1.

2. Ibid., p. 6. Illustration adapted from that cited here.

3. Ibid., p. 7.

APPENDIX F

INTELLIGENCE CENTER ADMINSTRATION

The analyst/advisor should evaluate host nation
operations before recommending changes. The following
points, however, have proven useful in the past and are
offered here for the analyst/advisor's consideration.

1. Use maps with a scale of 1:50,000. These are fairly
common and will suffice for most intelligence operations.
Additionally, if the host nation is supported by U.S.
assets, it helps to achieve compatibility. Urban operations
will require maps of a much larger scale (1:12,500 or
greater). Annotate overlays with map sheet numbers,scale,
and dates before storing..

2. Low staff personnel turbulence in the host nation
unit is important. Longevity and continuity are significant
multipliers, particularly in analysts and photo imagery
interpreters.

3. Host-nation analysts should be organized by
geographic area, not by source. That is, rather than have
one analyst work all SIGINT, another all interrogation,
etc., assign the analyst an area (district or barangay) and

F 1

have him fuse all reports on that area. This develops area
expertise. The U.S. analyst/advisor must be alert to bias,
however.

4. Locate specialists such as photo interpreters and
computer technicians. Longevity is important here also. If
these people are not already assigned, or available for
assignment, seek habitual working relationships.

5. Require analysts and specialists to work together.
For example, an analyst with a SIGINT (DF) report should be
talking to the photo interpreter, looking for additional
indicators from photographs.

6. In some insurgencies, the urban infrastructure
employs high-technology. If the government seizes
communications or computer equipment (as happened in Manila
in early 1988), a technician should be on hand to prevent
the loss of electronic information.

7. Use host-nation treasury agents to assist in
tracking the transmission of funds through legitimate banks
and financial institutions. This may lead to infrastructure
contacts at the local level.

8. The analyst/advisor should establish liaison with
other intelligence agencies. Arrange for exchange of
information and intelligence products.

The following illustration depicts an intelligence unit with
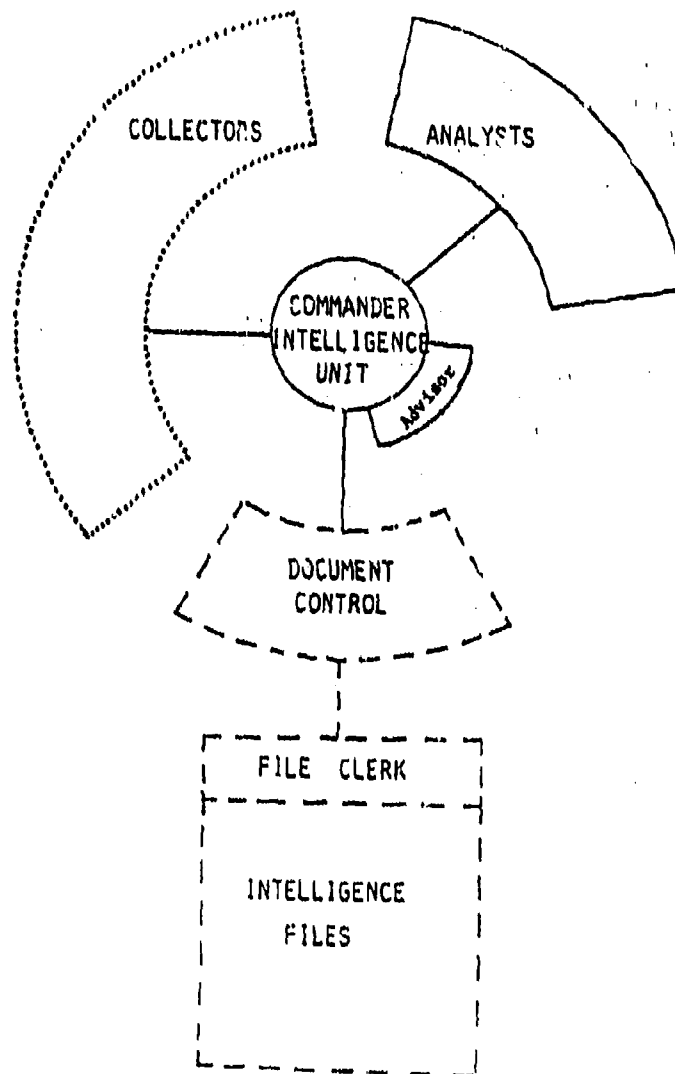enough staff to segregate responsibility (Figure F1).

F 2

Figure F1. ¹

The last illustration depicts a well-staffed, modernized unit of the type found at a senior command or national level (Figure F2).
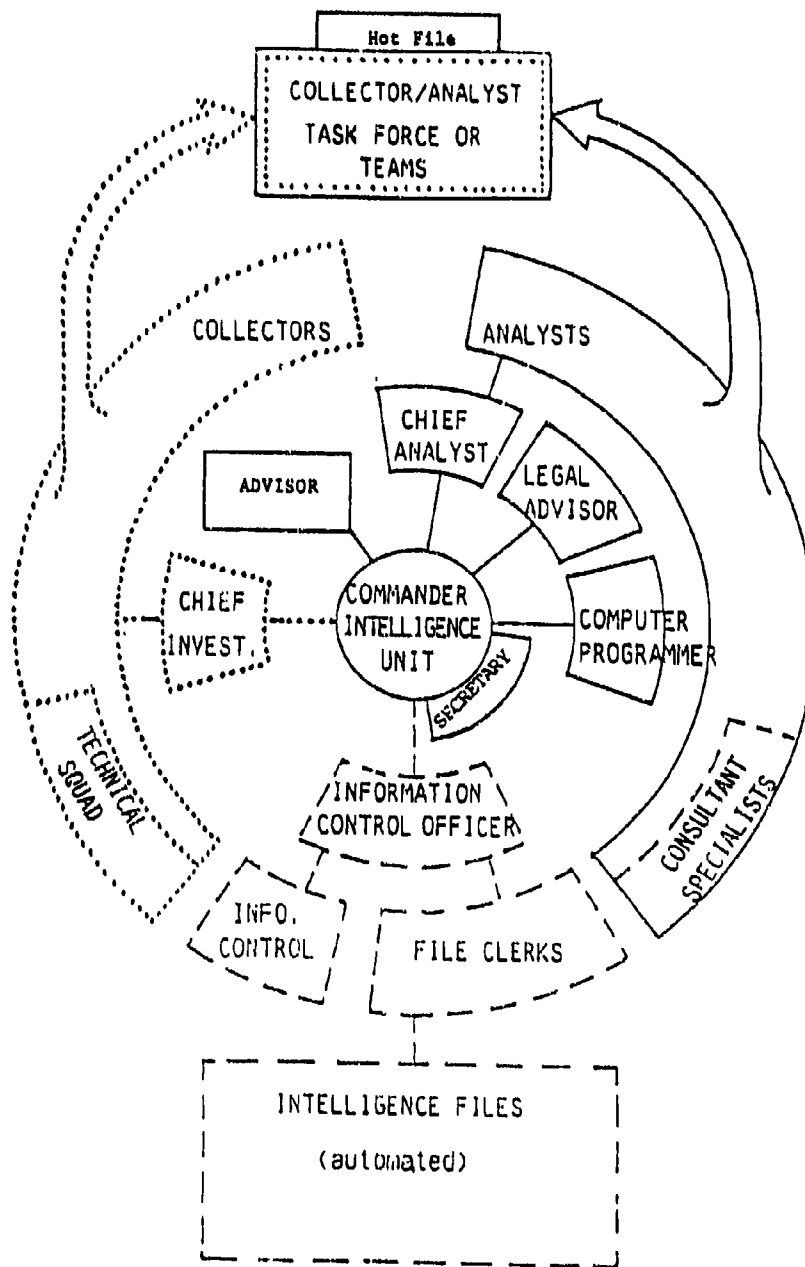
Figure F2.²

ENDNOTES
APPENDIX F

1. Mid-States Organized Crime Information Center (MOCIC) PDI, <u>Building the Intelligence System</u>, p. 8x.

2. Ibid., p. 11x.

BIBLIOGRAPHY

1. ARTICLES

Stewart, John F., Brigadier General, USA. "Military
    Intelligence Operations in Low-Intensity Conflict: An
    Organizational Model." Military Review 68 (January
    1988): 17-27.

2. BOOKS

Colby, William and Peter Forbath. Honorable Men: My Life in
    the CIA. New York: Simon and Schuster, 1978.

Herrington, Stuart A. Silence Was A Weapon. Novato:
    Presidio Press, 1982.

Karnow, Stanley. Vietnam. New York: Viking Press, 1983.

Kitson, Frank. Low Intensity Operations: Subversion,
    Insurgency, Peacekeeping. Hamden: Archon, 1974.

Krepinevich, Andrew F., Jr. The Army and Vietnam.
    Baltimore: The Johns Hopkins University Press, 1986.

Lipsman, Samuel and Edward Doyle. Fighting For Time. The
    Vietnam Experience Series. Boston: Boston Publishing
    Company, 1983.

McCuen, John J., Lieutenant Colonel, U.S. Army. The Art of
    Counterrevolutionary War: A Psycho-Politico-Military
    Strategy of Counterinsurgency. Harrisburg: Stackpole
    Books, 1966.

Thompson, Robert. Defeating Communist Insurgency. New
    York: Praeger Press, 1966.

Trinquier, Roger. Modern Warfare. Translated from the
    French by Daniel Lee. New York: Frederick A. Praeger,
    Inc, 1964.

O'Neill, Bard E., William R. Heaton, and Donald J. Alberts,
    editors. Insurgency in the Modern World. Boulder:
    Westview Press, 1980.

Pike, Douglas. PAVN: People's Army of Vietnam. Novato:
    Presidio Press, 1986.

3. GOVERNMENT PUBLICATIONS

Scoville, Thomas W. _Reorganizing For Pacification Support_. Washington, D.C.: U.S. Government Printing Office, 1982.

U.S. Army. _FM 34-3 Intelligence Analysis_. Washington, D.C.: Headquarters, Department of the Army, January 1986.

U.S. Army. _FM 34-60 Counterintelligence_. Washington, D.C.: Headquarters, Department of the Army, August, 1985.

U.S. Army. _FM 34-60A (S/NFN) Counterintelligence Operations_. Washington, D.C.: Headquarters, Department of the Army, June 1989.

U.S. Army. _FM 34-130 Intelligence Preparation of the Battlefield_. Washington, D.C.: Headquarters, Department of the Army, May 1989.

U.S. Army. _FM 100-20 Low-Intensity Conflict_. Final Draft. Fort Leavenworth, Kansas: USACGSC, March 1989.

U.S. Army. _DA PAM 550-104 Human Factors Considerations of Undergrounds in Insurgencies_. Washington, D.C.: Headquarters, Department of the Army, September 1966.

U.S. Army. _DA PAM 550-106 The Communist Infrastructure in South Vietnam: A Study of Organization and Strategy_. Washington, D.C.: Headquarters, Department of the Army, March 1967.

U.S. Army. _Special Operations Targeting Handbook_ (FOUO). Fort Bragg, NC: SFOD-I, DCSINT, USA 1st SOCOM. Edition 5.

U.S. Marine Corps. _NAVMC 2890 Small Wars Manual_. Washington, D.C.: Headquarters, Department of the Navy, April 1987 (Reprint of the 1940 edition).

4. INTERVIEWS

Ossorio, Peter M. Assistant U.S. Attorney, U.S. Department of Justice, Western District of Missouri. Interview by author. Kansas City, Missouri. 16 October 1989.

Garcia, Rolando. Lieutenant Colone., Philippine Constabulary. Interviews by author. Fort Leavenworth, Kansas. 7,13 November 1989.

5. UNPUBLISHED DISSERTATIONS, THESES, and PAPERS

Knapp, William L. "Phoenix/Phung Hoang and the Future: A Critical Analysis of the US/GVN Program to Neutralize the Viet Cong Infrastructure." Carlisle Barracks, Pennsylvania: U.S. Army War College, 8 March 1971.

Mid-States Organized Crime Information Center (MOCIC). Intelligence Analyst Program of Instruction. Course material provided to the author by Patricia Koetting, Intelligence Analyst, Drug Enforcement Unit, Kansas City Missouri Police Department. October 1989.

Military Advisory Command Civil Operations and Revolutionary Development Supports (MACCORDS). Phoenix Coordinators' Orientation Course. Seminary Camp, Vung Tau, RVN: MACV, March 1970.

O'Meara, Andrew P., Jr. "Infrastructure and the Power Seizure: A Structural and Functional Analysis of the Bolshevik and Chinese Communist Models of Revolution." MMAS thesis, U.S. Army Command and General Staff College, 1970.